Shanghai Fudan Microelectronics Group Company Limited

复旦微电子

FM24NC512T1/T2/T3/T4
NFC Serial EEPROM

Data Sheet

Feb. 2017

1 Description

FM24NC512Tx is a 512Kbit dual interface EEPROM with flexible tag function. The 512kbit data memory and the dedicated tag memory can be accessed by both two wire serial interface and ISO/IEC 14443A compatible RF interface. When tag memory accessed by RF interface, the device is fully compatible with NFC Forum Type 2 tag. The device can also access tag memory through the conventional address by two wire serial interface. This feature ensures a flexible NFC tag application.

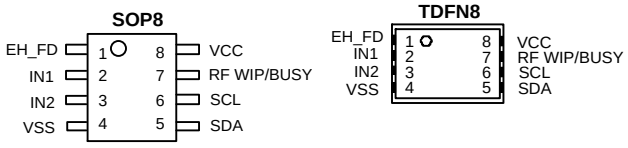
2 Features

- **Contact Interface**
  - 1.7V~5.5V single power supply
  - Typical standby current <1uA
  - Two wire serial interface
  - 1MHz (2.5V~5.5V) and 400 kHz (1.7V~5.5V) compatibility
  - Byte and Page Write (up to 128 bytes) for data memory
  - Byte and Page Write (up to 16 bytes) for tag memory
  - Random and Sequential read
  - Contact interface timeout
- **RF Interface**
  - ISO/IEC 14443A compatible
  - Contactless data transmission
  - Enhanced RF performance using contact power
  - Carrier frequency: 13.56 MHz
  - Data transfer rate: 106/212/424/848 kbit/s
  - UID & Counter ASCII Mirror for automatic serialization NDEF messages
  - Originality signature
  - True anticollision
  - Tag operation: 4 bytes Write, 16 bytes /Fast Read
  - Data Memory operation: Byte and Page Write (up to 128 bytes), Random read (up to 256 bytes)
  - Support sleep mode
- **Memory**
  - Data Memory: 64K bytes organized in 512 pages of 128 bytes each
  - Tag Memory:

Part number	Tag memory - user data
FM24NC512T1	144 bytes
FM24NC512T2	504 bytes
FM24NC512T3	888 bytes
FM24NC512T4	1884 bytes

  - Self-timed write cycle (5 ms max)
  - Endurance: 1 million write cycles
  - Data retention: 40 years
- **Security**
  - Write protection register of whole data memory both in two wire serial interface and RF interface
  - Write protection of tag memory by page in two wire serial interface
  - Password protection for lock and system configuration and RF data write
  - Unique ID for each device
- **User configurable General purpose output**
- **Energy harvesting and Field detection**
  - Configurable Energy harvesting(EH) or Field detection(FD) output
  - Configurable EH output voltage: 1.5V, 1.8V，2.5V and 3.3V
  - Configurable EH limited current:: 0.5mA, 1mA, 2mA and no limit
  - Configurable FD output voltage: 1.5V, 1.8V，2.5V and 3.3V
  - Configurable FD trigger action: upon any RF field presence, upon the selection of the tag, upon start of frame and upon halt with previous read operation
- **Green Package**
  - RoHS Compliant and Halogen-free

3 Packaging Type



4 Pin Configurations

Pin Name	Function
EH_FD	Energy harvesting and Field Detection Output
SDA	Serial Data Input/Output
SCL	Serial Clock Input
GPO	General purpose output
IN1/IN2	Antenna connection
VCC	Power Supply
VSS	Ground

5 Block Diagram

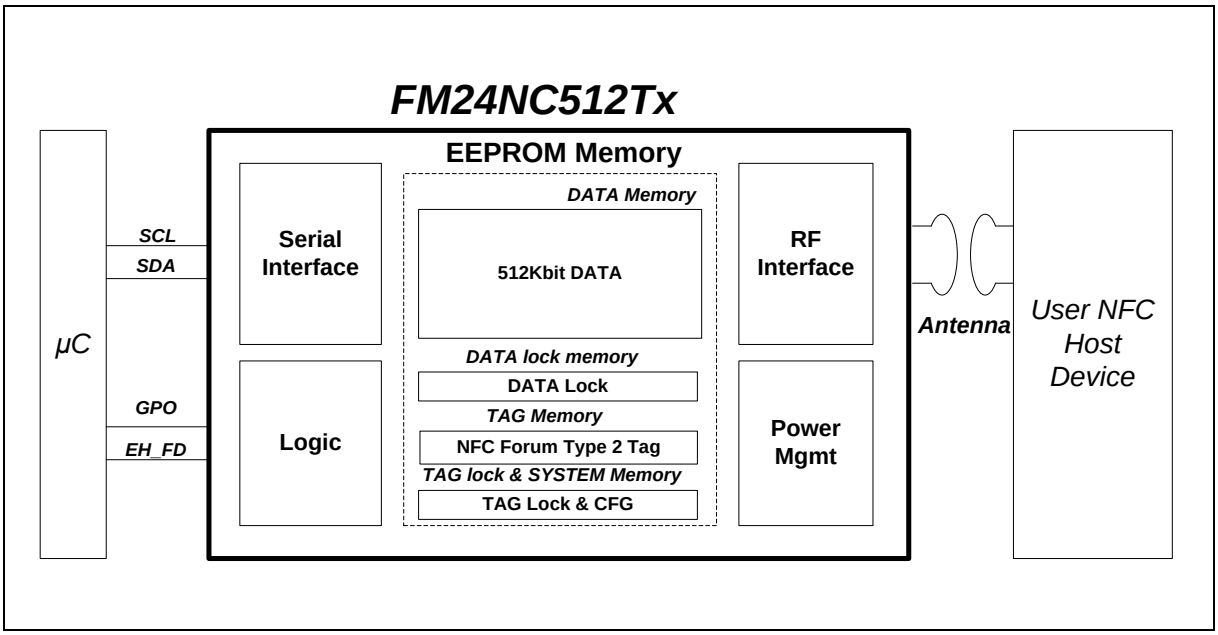


Figure 1 Block Diagram of FM24NC512Tx

6 Pin Descriptions

6.1 SERIAL CLOCK (SCL)

This input signal is used to strobe all data in and out of the device. In applications where this signal is used by slave devices to synchronize the bus to a slower clock, the bus master must have an open drain output, and a pull-up resistor must be connected from Serial Clock (SCL) to VCC. In most applications, though, this method of synchronization is not employed, and so the pull-up resistor is not necessary, provided that the bus master has a push-pull (rather than open drain) output.

6.2 SERIAL DATA (SDA)

This bidirectional signal is used to transfer data in or out of the device. It is an open drain output that may be wire-OR'ed with other open drain or open collector signals on the bus. A pull up resistor must be connected from Serial Data (SDA) to VCC.

6.3 Antenna Connection (IN1, IN2)

These input pins are used to connect the device to an external coil exclusively. It is advised to not connect any other DC or AC path to IN1 and IN2 pads. When correctly tuned, the coil is used to access the device using the ISO/IEC 14443A protocol and NFC Forum Type 2 Tag Operation Specification.

6.4 Energy Harvesting and Field Detection Output (EH_FD)

This output pin is used to deliver the analog voltage available when the RF field strength is sufficient. The output voltage and the drive current can be configured.

This pin is also used as RF field detection and to interrupt source to e.g. wake up an embedded microcontroller or trigger further actions. Typical applications are Bluetooth and Wi-Fi pairing.

6.5 General purpose Output (GPO)

This configurable output signal is used either to indicate that the FM24NC512Tx is executing an internal write cycle of data or tag memory via RF interface or than an RF command is in progress. It is an open drain output that may be wire-OR'ed with other open drain or open collector signals on the bus. A pull up resistor must be connected from GPO to system power.

6.6 Ground (VSS)

VSS is the reference for the VCC supply voltage.

6.7 Supply voltage (VCC)

This pin can be connected to an external DC supply voltage not only in two-wire serial interface, but also in RF interface.

Prior to selecting the memory and issuing command to it, a valid and stable VCC voltage within the specified [VCC(min), VCC(max)] range must be applied. To maintain a stable DC supply voltage, it is recommended to decouple the VCC line with a suitable capacitor (usually of the order of 10 nF) close to the VCC/VSS package pins. This voltage must remain stable and valid until the end of the transmission of the command and, for a write command, until the completion of the internal write cycle (t_{WR}).

7 Memory Organization

The FM24NC512Tx memory consists of four parts: Data memory, Data lock, Tag memory, and Tag System. Each part can be accessed by two wire serial interface or RF interface or both.

Table 1 Memory organization of FM24NC512Tx

Data memory organization

Contact Interface	RF Interface	Address		Byte number inside page			Description
		Page	Byte	0	…	127	
Device address 1010000	Data memory command	000h	0000h	Data memory (512 page X 128 byte)			Data memory
		001h	0080h				
		…	…				
		1FFh	FFFFh				

Data system, TAG and TAG system memory organization

Contact Interface	RF Interface	Address		Byte number inside page			Description
		Page	Byte	0	…	15	
Device address 1010001	NA	040h	0400h	CT_DATA_PWD & CT_DATA_WR_LOCK			Data lock
	Data lock command	041h	0410h	RF_DATA_WR_LOCK &RF_DATA_RD_LOCK			
	Data pwd command	042h	0420h	RF_DATA_PWD			
Device address 1010001	TAG memory command	080h	0800h	TAG memory (12 page X 16 byte for FM24NC512T1 34 page X 16 byte for FM24NC512T2 58 page X 16 byte for FM24NC512T3 120 page X 16 byte for FM24NC512T4)			TAG memory
		081h	0810h				
		…	…				
		0F7h	0F70h				
	NA	0F8h	0F80h	CT_TAG_WR_LOCK			TAG lock & system
		0F9h	0F90h	CT_TAG_PWD & EH_FD_CFG & GPO_CFG			
		0FAh	0FA0h	UID			
		0FFh	0FF0h	NULL		RF_SLEEP	

Remark: The address not mentioned is NULL, which indicates the empty address. When accessed by contact interface, the readout data is always 00h. The write operation in this area receives the response of ACK and will trigger internal write cycle, but it cannot change the readout data.

7.1 Data memory

The data memory of FM24NC512Tx is organized in 512 pages of 128 bytes each. When accessed by two wire serial interface, with device address set to 1010000b, each byte can be individually read or write using 2 bytes of byte address which address range is from 0000h to FFFFh. When accessed by RF interface, with data memory command, each byte can be individually read or write using 2 bytes of byte address which address range is from 0000h to FFFFh.

There is a special mechanism to protect data memory from unexpected write operation. For command from two wire serial interface, the whole data memory is protected by the CT_DATA_WR_LOCK register. The write operation is permitted if only the register=0. For command from RF interface, the whole data memory is protected by the RF_DATA_WR_LOCK register and RF_DATA_PWD authentication action. The write operation is permitted if only the

register=0 and a previously RF_DATA_PWD authentication.

The default value of the data memory at delivery is FFh.

7.2 Data lock memory

7.2.1 CT_DATA_WR_LOCK(0400h)

CT_DATA_WR_LOCK is a register that locks the write access of data memory in contact interface.

The detail is shown as below

CT_DATA_WR_LOCK register

Byte addr.	Bit number inside byte							
	7	6	5	4	3	2	1	0
0400h	CT_DATA_WR_LOCK	RFU						

- 0b indicates to unlock data memory
- 1b indicates to lock data memory

In contact interface, the read access of CT_DATA_WR_LOCK doesn't need authentication of contact password (CT_DATA_PWD). However, the write access must be in CT_DATA_PWD authenticated state.

CT_DATA_WR_LOCK does not impact write access of RF interface, and it couldn't be accessed in RF interface.

The default value of each bit of CT_DATA_WR_LOCK at delivery is 0b.

7.2.2 CT_DATA_PWD(0408h~040Bh)

CT_DATA_PWD is password of contact interface. It has 32 bits organized in 4 bytes, which byte address is from 0408h to 040Bh in contact interface. CT_PWD is used to password authentication in contact interface.

CT_DATA_PWD can be read and write in password authenticated state of contact interface.

CT_DATA_PWD cannot be accessed by RF interface.

The default value of each byte of CT_PWD at delivery is 00h.

7.2.3 RF_DATA_WR_LOCK(0418h)

RF_DATA_WR_LOCK is a register that locks the write access of data memory in RF interface. The detail is shown as below

CT_DATA_WR_LOCK register

Byte addr.	Bit number inside byte							
	7	6	5	4	3	2	1	0
0418h	RF_DATA_WR_LOCK	RFU						

- 0b indicates to unlock data memory
- 1b indicates to lock data memory

In RF interface, the read access of RF_DATA_WR_LOCK doesn't need authentication of RF password (RF_DATA_PWD). However, the write access must be in RF_DATA_PWD authenticated state.

RF_DATA_WR_LOCK does not impact write access of contact interface.

The default value of each bit of RF_DATA_WR_LOCK at delivery is 0b.

7.2.4 RF_DATA_RD_LOCK(0410h)

RF_DATA_RD_LOCK is a register that locks the read access of data memory in RF interface.

The detail is shown as below

CT_DATA_WR_LOCK register

Byte addr.	Bit number inside byte							
	7	6	5	4	3	2	1	0
0410h	RF_DATA_RD_LOCK	RFU						

- 0b indicates to unlock data memory
- 1b indicates to lock data memory

In RF interface, the read access of RF_DATA_WR_LOCK doesn't need authentication of RF password (RF_DATA_PWD). However, the write access must be in RF_DATA_PWD authenticated state.

RF_DATA_RD_LOCK does not impact read access of contact interface.

The default value of each bit of RF_DATA_RD_LOCK at delivery is 0b.

7.2.5 RF_DATA_PWD(0420h~0423h)

RF_DATA_PWD is password of RF interface. It has 32 bits organized in 4 bytes, which byte address is from 0420h to 0423h in contact interface. RF_PWD is used to password authentication in RF interface.

RF_DATA_PWD can be read and write in password authenticated state of contact interface.

RF_DATA_PWD can not be accessed by RF interface.

The default value of each byte of RF_DATA_PWD at delivery is 00h.

7.3 Tag memory

In FM24NC512Tx, there's a tag memory to ensure NFC Forum Type 2 Tag operation. It can be accessed by two wire serial interface, with device address set to 1010001b, using 2 bytes of byte address. The address range varies according to tag type, refers to Table 2-5.

The tag memory is organized in pages of 16 bytes each when accessed by two wire serial interface. Meanwhile, the tag memory is organized in blocks of 4 bytes each when accessed by RF interface. Each block can be individually accessed by tag command.

For FM24NC512T1 variant, the tag memory size is 180 bytes, including 144 bytes user memory. NFC Tag is organized in blocks with 4 bytes. Each block can be individually accessed by tag command.

Table 2 Tag memory organization of FM24NC512T1

Contact CMD	Tag CMD	Byte number inside block	Description

Device addr	Page addr.	Byte addr.	Block addr. Hex.	Block addr. Dec.	0	1	2	3	
1010001	080h ~ 083h	0800h	00h	0	UID0/RFU	UID1/RFU	UID2/RFU	BCC0/RFU	UID and static lock bytes
		0804h	01h	1	UID3/RFU	UID4/RFU	UID5/RFU	UID6/RFU	
		0808h	02h	2	BCC1/RFU	Internal/RFU	Lock_byte[0]	Lock_byte[1]	
		080Ch	03h	3	Capability Container (CC)				CC
		0810h	04h	4	Static Data Area (Block 04h-0Fh, total 12 blocks)				User data
		…	…	…					
		083Ch	0Fh	15					
	084h ~ 08Bh	0840h	10h	16	Dynamic Data Area (Block 10h~2Bh, total 24 blocks)				
		…	…	…					
		089Ch	27h	39					
		08A0h	28h	40	Dynamic Lock Bytes				Dynamic Lock Bytes
		08A4h	29h	41	FDP & MIRROR	RFU	MIRROR_BLOCK	AUTH0	Configuration
		08A8h	2Ah	42	ACCESS	RFU			
		08ACh	2Bh	43	PWD				
		08B0h	2Ch	44	PACK		RFU		
See 7.4			2Dh	45	EH_FD_CFG	GPO_CFG	RFU		Tag system

For FM24NC512T2, the tag memory size is 540 bytes, including 504 bytes user memory. NFC Tag is organized in blocks with 4 bytes. Each block can be individually accessed by tag command.

Table 3 Tag memory organization of FM24NC512T2

Contact CMD			Tag CMD		Byte number inside block				Description
Device addr	Page addr.	Byte addr.	Block addr. Hex.	Block addr. Dec.	0	1	2	3	
1010001	080h ~ 083h	0800h	00h	0	UID0/RFU	UID1/RFU	UID2/RFU	BCC0/RFU	UID and static lock bytes
		0804h	01h	1	UID3/RFU	UID4/RFU	UID5/RFU	UID6/RFU	
		0808h	02h	2	BCC1/RFU	Internal/RFU	Lock_byte[0]	Lock_byte[1]	
		080Ch	03h	3	Capability Container (CC)				CC
		0810h	04h	4	Static Data Area (Block 04h-0Fh, total 12 blocks)				User data
		…	…	…					
		083Ch	0Fh	15					
	084h ~ 0A1h	0840h	10h	16	Dynamic Data Area (Block 10h~81h, total 114 blocks)				
		…	…	…					
		0A04h	81h	129					
		0A08h	82h	130	Dynamic Lock Bytes				Dynamic Lock Bytes
		0A0Ch	83h	131	FDP & MIRROR	RFU	MIRROR_BLOCK	AUTH0	Configuration
		0A10h	84h	132	ACCESS	RFU			
		0A14h	85h	133	PWD				

Contact CMD			Tag CMD		Byte number inside block				Description
Device addr	Page addr.	Byte addr.	Block addr.		0	1	2	3	
			Hex.	Dec.					
		0A18h	86h	134	PACK		RFU		
See 7.4			87h	135	EH_FD_CFG	GPO_CFG	RFU		Tag system

For FM24NC512T3, the tag memory size is 924 bytes, including 888 bytes user memory. NFC Tag is organized in blocks with 4 bytes. Each block can be individually accessed by tag command.

Table 4 Tag memory organization of FM24NC512T3

Contact CMD			Tag CMD		Byte number inside block				Description
Device addr	Page addr.	Byte addr.	Block addr.		0	1	2	3	
			Hex.	Dec.					
1010001	080h ~ 083h	0800h	00h	0	UID0/RFU	UID1/RFU	UID2/RFU	BCC0/RFU	UID and static lock bytes
		0804h	01h	1	UID3/RFU	UID4/RFU	UID5/RFU	UID6/RFU	
		0808h	02h	2	BCC1/RFU	Internal/RFU	Lock_byte[0]	Lock_byte[1]	
		080Ch	03h	3	Capability Container (CC)				CC
		0810h	04h	4	Static Data Area (Block 04h-0Fh, total 12 blocks)				User data
		…	…	…					
		083Ch	0Fh	15					
	084h ~ 0B9h	0840h	10h	16	Dynamic Data Area (Block 10h~E1h, total 210 blocks)				
		…	…	…					
		0B84h	E1h	225					
		0B88h	E2h	226	Dynamic Lock Bytes				Dynamic Lock Bytes
		0B8Ch	E3h	227	FDP & MIRROR	RFU	MIRROR_BLOCK	AUTH0	Configuration
		0B90h	E4h	228	ACCESS	RFU			
		0B94h	E5h	229	PWD				
		0B98h	E6h	230	PACK		RFU		
See 7.4			E7h	231	EH_FD_CFG	GPO_CFG	RFU		Tag system

For FM24NC512T4, the tag memory size is 1920 bytes, including 1884 bytes user memory. NFC Tag is organized in blocks with 4 bytes. Each block can be individually accessed by tag command.

Table 5 Tag memory organization of FM24NC512T4

Contact CMD			Tag CMD			Byte number inside block				Description
Device addr	Page addr.	Byte addr.	Sector addr.	Block addr.		0	1	2	3	
				Hex.	Dec.					
1010001	080h ~	0800h	0	00h	0	UID0/RFU	UID1/RFU	UID2/RFU	BCC0/RFU	UID and static lock

Contact CMD			Tag CMD			Byte number inside block				Description
Device addr	Page addr.	Byte addr.	Sector addr.	Block addr.		0	1	2	3	
				Hex.	Dec.					
	083h	0804h		01h	1	UID3/RFU	UID4/RFU	UID5/RFU	UID6/RFU	bytes
		0808h		02h	2	BCC1/RFU	Internal/ RFU	Lock_byte[0]	Lock_byte[1]	
		080Ch		03h	3	Capability Container (CC)				CC
		0810h		04h	4	Static Data Area (Block 04h-0Fh, total 12 blocks)				User data
		…		…	…					
		083Ch		0Fh	15					
	084h ~ 0F7h	0840h		10h	16	Dynamic Data Area (Sector 0 Block 10h~Sector 1 Block DAh, total 459 Blocks)				
		…		…	…					
		0BFCh		FFh	255					
		0C00h	1	00h	0					
		…		…	…					
		0F68h		DAh	218					
		0F6Ch		DBh	219	Dynamic Lock Bytes				Dynamic Lock Bytes
		0F70h		DCh	220	FDP & MIRROR	RFU	MIRROR_BLOCK	AUTH0	Configuration
		0F74h		DDh	221	ACCESS	RFU		SEC_CFG	
		0F78h		DEh	222	PWD				
		0F7Ch		DFh	223	PACK		RFU		
See 7.4				E0h	224	EH_FD_CFG	GPO_CFG	RFU		Tag system

7.3.1 Read only bytes(0800h~0809h)

In RF interface, these 10 bytes are the mirror of UID, which are read only. Any read operation replies UID which defined in UID (0FA0h~0FA9h). In contact interface, these 10 bytes can be written to any data, and be readout. But it can not change the reply of read operation of RF interface.

Remark: The real UID and anticollision operation will not be influenced if these bytes are changed by contact interface.

7.3.2 Static lock bytes(080Ah~080Bh)

In RF interface, the bits of byte 2 and byte 3 of block 02h represent the field programmable read-only locking mechanism. Each block from 03h (CC) to 0Fh can be individually locked by setting the corresponding locking bit Lx to logic 1 to prevent further write access. After locking, the corresponding block becomes read-only memory.

The three least significant bits of lock byte 0 are the block-locking bits. Bit 2 deals with block 0Ah to 0Fh, bit 1 deals with block 04h to 09h and bit 0 deals with block 03h (CC). Once the block-locking bits are set Logic 1, the locking configuration for the corresponding memory area is frozen.

Table 6 Static lock bytes of FM24NC512Tx

Field	Byte	Bit number inside byte

	No.	7	6	5	4	3	2	1	0
Static lock bytes	0	L7	L6	L5	L4	LCC	BL15-10	BL9-4	BLCC
	1	L15	L14	L13	L12	L11	L10	L9	L8

Remark: Lx locks Block x to read-only; BLx-y blocks further locking for the memory area x-y.

For example if BL15-10 is set to logic 1, then bits L15 to L10 (lock byte 1, bit [7:2]) can no longer be changed.

The so called static locking and block-locking bits are set by a WRITE or COMPATIBILITY_WRITE command to block 02h. Bytes 2 and 3 of the WRITE or COMPATIBILITY_WRITE command and the contents of the lock bytes are bit-wise OR'ed and the result then becomes the new content of the lock bytes. This process is irreversible. If a bit is set to logic 1, it cannot be changed back to logic 0. The contents of bytes 0 and 1 of block 02h are unaffected by the corresponding data bytes of the WRITE or COMPATIBILITY_WRITE command.

In contact interface, static lock bytes don't affect the write access of tag memory.

The default value of the static lock bytes at delivery is 00h.

7.3.3 Dynamic Lock Bytes

In RF interface, to lock the blocks starting at block address 10h and onwards, the so called dynamic lock bytes are used.

For FM24NC512T1 variant, those three lock bytes cover the memory area of 96 data bytes. The granularity is 2 blocks, compared to a single block for the first 64 bytes as shown in Table 7.

For FM24NC512T2 variant, those four lock bytes cover the memory area of 456 data bytes. The granularity is 16 blocks, compared to a single block for the first 64 bytes as shown in Table 8.

For FM24NC512T3 variant, those four lock bytes cover the memory area of 840 data bytes. The granularity is 16 blocks, compared to a single block for the first 64 bytes as shown in Table 9.

For FM24NC512T4 variant, those four lock bytes cover the memory area of 1884 data bytes. The granularity is 16 blocks, compared to a single block for the first 64 bytes as shown in Table 10.

Remark: Set all bits marked with RFU to 0, when writing to the dynamic lock bytes.

Table 7 Dynamic Lock Byte of FM24NC512T1

Field	Byte No.	Bit number inside byte							
		7	6	5	4	3	2	1	0
Dynamic lock byte	0	L30-31	L28-29	L26-27	L24-25	L22-23	L20-21	L18-19	L16-17
	1	RFU	RFU	RFU	RFU	L38-39	L36-37	L34-35	L32-33
	2	RFU	RFU	BL36-39	BL32-25	BL28-31	BL24-27	BL20-23	BL16-19
	3	RFU							

Remark: Lx-y locks Block x-y to read-only; BLx-y blocks further locking for Block x-y.

Table 8 Dynamic Lock Byte of FM24NC512T2

Field	Byte No.	Bit number inside byte							
		7	6	5	4	3	2	1	0
Dynamic lock byte	0	L128-129	L112-127	L96-111	L80-95	L64-79	L48-63	L32-47	L16-31
	1	RFU							
	2	RFU				BL112-129	BL80-111	BL48-79	BL16-47
	3	RFU							

Remark: Lx-y locks Block x-y to read-only. BLx-y blocks further locking for Block x-y.

Table 9 Dynamic Lock Byte of FM24NC512T3

Field	Byte No.	Bit number inside byte							
		7	6	5	4	3	2	1	0
Dynamic lock byte	0	L128-143	L112-127	L96-111	L80-95	L64-79	L48-63	L32-47	L16-31
	1	RFU		L224-225	L208-223	L192-207	L176-191	L160-175	L144-159
	2	RFU	BL208-225	BL176-207	BL144-175	BL112-143	BL80-111	BL48-79	BL16-47
	3	RFU							

Remark: Lx-y locks Block x-y to read-only; BLx-y blocks further locking for Block x-y.

Table 10 Dynamic Lock Byte of FM24NC512T4

Field	Byte No.	Bit number inside byte							
		7	6	5	4	3	2	1	0
Dynamic lock byte	0	L240-271	L208-239	L176-207	L144-175	L112-143	L80-111	L48-79	L16-47
	1	RFU	L464-474	L432-463	L400-431	L368-399	L336-367	L304-335	L272-303
	2	BL464-474	BL400-463	BL336-399	BL272-335	BL208-271	BL144-207	BL80-143	BL16-79
	3	RFU							

Remark: Lx-y locks Block x-y to read-only; BLx-y blocks further locking for Block x-y. There are 459 dynamic data blocks, 240 blocks in sector 0 and 219 blocks in sector 1, respectively.

Dynamic lock bytes of the WRITE or COMPATIBILITY_WRITE command and the current contents of the dynamic lock bytes is bit-wise OR'ed. The result is the new dynamic lock bytes contents. This process is irreversible. Once a bit is set to logic 1, it cannot be changed back to logic 0.

In contact interface, dynamic lock bytes don't affect the write access of tag memory.

The default value of dynamic lock bytes at delivery is 00h.

7.3.4 Capability Container (CC) bytes(080Ch~080Fh)

The Capability Container CC (block 3) is programmed during the IC production according to the NFC Forum Type 2 Tag specification. These bytes may be bit-wise modified by a WRITE or COMPATIBILITY_WRITE command.

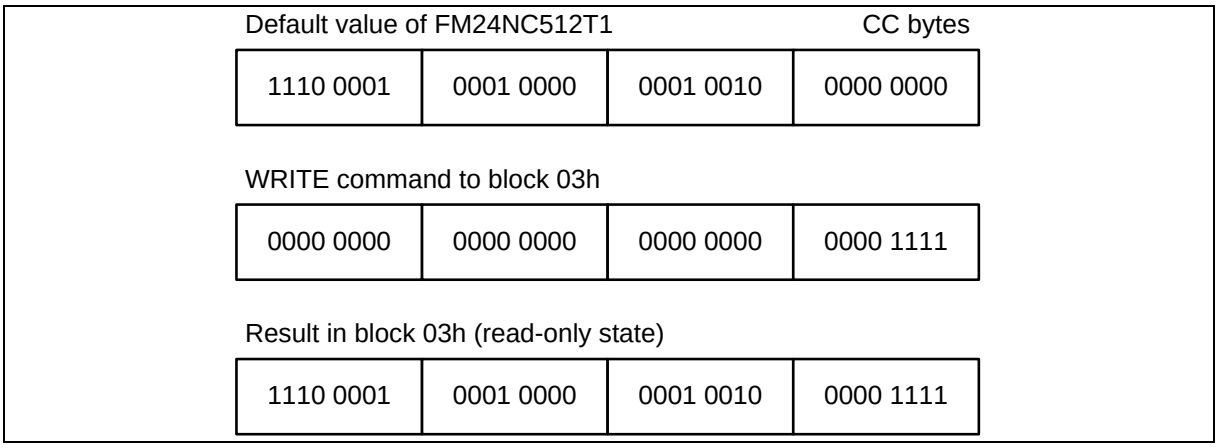


Figure 2 the example of CC bytes write

The parameter bytes of the WRITE command and the current contents of the CC bytes are bit-wise OR'ed. The result is the new CC byte contents. This process is irreversible. Once a bit is set to logic 1, it cannot be changed back to logic 0.

The default values of the CC bytes at delivery are defined in Section 7.3.6.

7.3.5 Data blocks

Blocks 04h to 27h for FM24NC512T1, blocks 04h to 81h for FM24NC512T2, blocks 04h to E1h for FM24NC512T3 and blocks 04h of sector 0 to DAh of sector 1 for FM24NC512T4 are the user memory read/write area. The access to a part of the user memory area can be restricted using password verification. See Section 7.3.7 for further details.

The default values of the data blocks at delivery are defined in Section 7.3.6.

7.3.6 CC and Data blocks content at delivery

The tag memory of FM24NC512Tx are pre-programmed to the initialized state according to the NFC Forum Type 2 Tag specification as defined in Table 11, Table 12, Table 13 and Table 14.

Table 11 Memory content at delivery of FM24NC512T1

Contact CMD		Tag CMD	Byte number inside block			
Page addr.	Byte addr.	Block addr.	0	1	2	3
080h	080Ch	03h	E1h	10h	12h	00h
	0810h	04h	01h	03h	A0h	0Ch
	0814h	05h	34h	03h	03h	D0h
	0818h	06h	00h	00h	FEh	00h

Table 12 Memory content at delivery of FM24NC512T2

Contact CMD		Tag CMD	Byte number inside block			
Page addr.	Byte addr.	Block addr.	0	1	2	3
080h	080Ch	03h	E1h	10h	3Fh	00h
	0810h	04h	01h	03h	88h	08h
	0814h	05h	66h	03h	03h	D0h
	0818h	06h	00h	00h	FEh	00h

Table 13 Memory content at delivery of FM24NC512T3

Contact CMD		Tag CMD	Byte number inside block			
Page addr.	Byte addr.	Block addr.	0	1	2	3
080h	080Ch	03h	E1h	10h	6Fh	00h
	0810h	04h	01h	03h	E8h	0Eh
	0814h	05h	66h	03h	03h	D0h
	0818h	06h	00h	00h	FEh	00h

Table 14 Memory content at delivery of FM24NC512T4

Contact CMD		Tag CMD	Byte number inside block			
Page addr.	Byte addr.	Block addr.	0	1	2	3
080h	080Ch	03h	E1h	10h	6Fh	00h
	0810h	04h	01h	03h	E8h	0Eh
	0814h	05h	66h	03h	03h	D0h

Contact CMD		Tag CMD	Byte number inside block			
Page addr.	Byte addr.	Block addr.	0	1	2	3
	0818h	06h	00h	00h	FEh	00h

The access to a part of the user memory area of tag memory can be restricted using password verification. Please see Section 7 for further details.

7.3.7 Configuration

Blocks 29h to 2Ah for FM24NC512T1 variant, blocks 83h to 84h for FM24NC512T2 variant, blocks E3h to E4h for FM24NC512T3 variant and blocks DCh to DDh of sector 1 variant are used to configure the memory access restriction and to configure the UID ASCII mirror feature.

Blocks 2Bh to 2Ch for FM24NC512T1 variant, blocks 85h to 86h for FM24NC512T2 variant, blocks E5h to E6h for FM24NC512T3 variant and blocks DEh to DFh of sector 1 variant are used as password and PACK.

Table 15 MIRROR_BYTE configuration

Byte address	Block address	Field	Bit number inside byte							
			7	6	5	4	3	2	1	0
08A4h/ 0A0Ch/ 0B8Ch/ 0F70h	29h/ 83h/ E3h/ DCh (Sector1)	FDP & MIRROR	MIRROR_CONF		MIRROR_BYTE		SLEEP_EN	STRG_MOD_EN	FDP_CONF	

Remark: Byte/Block address is for FM24NC512T1, FM24NC512T2, FM24NC512T3 and FM24NC512T4 individually.

Table 16 ACCESS configuration

Byte address	Block address	Field	Bit number inside byte							
			7	6	5	4	3	2	1	0
08A8h 0A10h 0B90h 0F74h	2Ah 84h E4h DDh	ACCESS	PROT	CFGLCK	RFU	NFC_CNT_EN	NFC_CNT_PWD_PROT_EN	AUTHLIM		

Remark: Byte/Block address is for FM24NC512T1, FM24NC512T2, FM24NC512T3 and FM24NC512T4 individually.

Table 17 SEC_CFG configuration

Byte address	Block address	Field	Bit number inside byte							
			7	6	5	4	3	2	1	0
0F77h	DDh	ACCESS	RFU						MIRRORS	AUTHS

Remark: Byte/Block address is for FM24NC512T4, this configuration makes sense only for FM24NC512T4.

Table 18 TAG configuration parameter description

FM24NC512T1

Part number	Byte address	Block address	Field	Bit	Default values	description

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC512T1	08A4h	29h	MIRROR_CONF	2	00b	Defines which ASCII mirror shall be used, if the ASCII mirror is enabled by a valid MIRROR_BLOCK byte 00b ... no ASCII mirror 01b ... UID ASCII mirror 10b … Counter mirror 11b … UID & counter mirror
FM24NC512T1	08A4h	29h	MIRROR_BYTE	2	00b	The 2 bits define the byte position within the block defined by the MIRROR_BLOCK byte (beginning of ASCII mirror)
FM24NC512T1	08A4h	29h	SLEEP_EN	1	0b	Enables the SLEEP mode function
FM24NC512T1	08A4h	29h	STRG_MOD_EN	1	0b	Controls the tag modulation strength - by default strong modulation is enabled
FM24NC512T1	08A4h	29h	FDP_CONF	2	11h	FDP CONF defines the configuration of the Field detect pin 00b ... enabled by first State-of-Frame (start of communication) 01b... enabled by halt with previous read operation 10b... enabled by selection of the tag 11b... enabled by field presence
FM24NC512T1	08A6h	29h	MIRROR_BLOCK	8	00h	MIRROR_BLOCK defines the block for the beginning of the ASCII mirroring A value >03h enables the ASCII mirror feature 04h-24h ... valid MIRROR_BLOCK values for FM24NC512T1 (UID ASCII mirror) 04h-26h ... valid MIRROR_BLOCK values for FM24NC512T1 (NFC counter mirror only) 04h-22h ... valid MIRROR_BLOCK values for FM24NC512T1 (both UID and NFC counter mirror)
FM24NC512T1	08A7h	29h	AUTH0	8	FFh	AUTH0 defines the block address from which the password verification is required. Valid address range for byte AUTH0 is from 00h to FFh.

Part number	Byte address	Block address	Field	Bit	Default values	description
						If AUTH0 is set to a block address which is higher than the last block from the user configuration, the password protection is effectively disabled.
FM24NC512T1	08A8h	2Ah	PROT	1	0b	One bit inside the ACCESS byte defining the memory protection 0b ... write access is protected by the password verification 1b ... read and write access is protected by the password verification
FM24NC512T1	08A8h	2Ah	CFGLCK	1	0b	Write locking bit for the user configuration excluding the PWD and PACK 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access
FM24NC512T1	08A8h	2Ah	NFC_CNT_EN	1	0b	Enables the NFC counter 0b ... disabled 1b ... enabled
FM24NC512T1	08A8h	2Ah	NFC_CNT_PWD_PROT_EN	1	0b	enables the password protection to read out and mirror the NFC counter 0b ... the protection is disabled 1b ... the protection is enabled
FM24NC512T1	08A8h	2Ah	AUTHLIM	3	000b	Limitation of negative password verification attempts 000b ... limiting of negative password verification attempts disabled 001b-111b ... maximum number of negative password verification attempts

FM24NC512T2

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC512T2	0A0Ch	83h	MIRROR_CONF	2	00b	Defines which ASCII mirror shall be used, if the ASCII mirror is enabled by a valid MIRROR_BLOCK byte 00b ... no ASCII mirror 01b ... UID ASCII mirror 10b … Counter mirror 11b … UID & counter mirror

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC512T2	0A0Ch	83h	MIRROR_BYTE	2	00b	The 2 bits define the byte position within the block defined by the MIRROR_BLOCK byte (beginning of ASCII mirror)
FM24NC512T2	0A0Ch	83h	SLEEP_EN	1	0b	Enables the SLEEP mode function
FM24NC512T2	0A0Ch	83h	STRG_MOD_EN	1	0b	Controls the tag modulation strength - by default strong modulation is enabled
FM24NC512T2	0A0Ch	83h	FDP_CONF	2	11h	FDP CONF defines the configuration of the Field detect pin 00b ... enabled by first State-of-Frame (start of communication) 01b... enabled by halt with previous read operation 10b... enabled by selection of the tag 11b... enabled by field presence
FM24NC512T2	0A0Eh	83h	MIRROR_BLOCK	8	00h	MIRROR_BLOCK defines the block for the beginning of the ASCII mirroring A value >03h enables the ASCII mirror feature 04h-7Eh ... valid MIRROR_BLOCK values for FM24NC512T2 (UID ASCII mirror) 04h-80h ... valid MIRROR_BLOCK values for FM24NC512T2 (NFC counter mirror only) 04h-7Ch ... valid MIRROR_BLOCK values for FM24NC512T2 (both UID and NFC counter mirror)
FM24NC512T2	0A0Fh	83h	AUTH0	8	FFh	AUTH0 defines the block address from which the password verification is required. Valid address range for byte AUTH0 is from 00h to FFh. If AUTH0 is set to a block address which is higher than the last block from the user configuration, the password protection is effectively disabled.
FM24NC512T2	0A10h	84h	PROT	1	0b	One bit inside the ACCESS byte defining the memory

Part number	Byte address	Block address	Field	Bit	Default values	description
						protection 0b ... write access is protected by the password verification 1b ... read and write access is protected by the password verification
FM24NC512T2	0A10h	84h	CFGLCK	1	0b	Write locking bit for the user configuration excluding the PWD and PACK 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access
FM24NC512T2	0A10h	84h	NFC_CNT_EN	1	0b	Enables the NFC counter 0b ... disabled 1b ... enabled
FM24NC512T2	0A10h	84h	NFC_CNT_PWD_PROT_EN	1	0b	enables the password protection to read out and mirror the NFC counter 0b ... the protection is disabled 1b ... the protection is enabled
FM24NC512T2	0A10h	84h	AUTHLIM	3	000b	Limitation of negative password verification attempts 000b ... limiting of negative password verification attempts disabled 001b-111b ... maximum number of negative password verification attempts

FM24NC512T3

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC512T3	0B8Ch	E3h	MIRROR_CONF	2	00b	Defines which ASCII mirror shall be used, if the ASCII mirror is enabled by a valid MIRROR_BLOCK byte 00b ... no ASCII mirror 01b ... UID ASCII mirror 10b … Counter mirror 11b … UID & counter mirror
FM24NC512T3	0B8Ch	E3h	MIRROR_BYTE	2	00b	The 2 bits define the byte position within the block defined by the MIRROR_BLOCK byte (beginning of ASCII mirror)
FM24NC512T3	0B8Ch	E3h	SLEEP_EN	1	0b	Enables the SLEEP mode function
FM24NC512T3	0B8Ch	E3h	STRG_MOD_E	1	0b	Controls the tag modulation

Part number	Byte address	Block address	Field	Bit	Default values	description
			N			strength - by default strong modulation is enabled
FM24NC512T3	0B8Ch	E3h	FDP_CONF	2	11h	FDP CONF defines the configuration of the Field detect pin 00b ... e enabled by first State-of-Frame (start of communication) 01b... enabled by halt with previous read operation 10b... enabled by selection of the tag 11b... enabled by field presence
FM24NC512T3	0B8Eh	E3h	MIRROR_BLOCK	8	00h	MIRROR_BLOCK defines the block for the beginning of the ASCII mirroring A value >03h enables the ASCII mirror feature 04h-DEh ... valid MIRROR_BLOCK values for FM24NC512T3 (UID ASCII mirror) 04h-E0h ... valid MIRROR_BLOCK values for FM24NC512T3 (NFC counter mirror only) 04h-DCh ... valid MIRROR_BLOCK values for FM24NC512T3 (both UID and NFC counter mirror)
FM24NC512T3	0B8Fh	E3h	AUTH0	8	FFh	AUTH0 defines the block address from which the password verification is required. Valid address range for byte AUTH0 is from 00h to FFh. If AUTH0 is set to a block address which is higher than the last block from the user configuration, the password protection is effectively disabled.
FM24NC512T3	0B90h	E4h	PROT	1	0b	One bit inside the ACCESS byte defining the memory protection 0b ... write access is protected by the password verification 1b ... read and write access is protected by the password verification
FM24NC512T3	0B90h	E4h	CFGLCK	1	0b	Write locking bit for the user

Part number	Byte address	Block address	Field	Bit	Default values	description
						configuration excluding the PWD and PACK 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access
FM24NC512T3	0B90h	E4h	NFC_CNT_EN	1	0b	Enables the NFC counter 0b ... disabled 1b ... enabled
FM24NC512T3	0B90h	E4h	NFC_CNT_PWD_PROT_EN	1	0b	enables the password protection to read out and mirror the NFC counter 0b ... the protection is disabled 1b ... the protection is enabled
FM24NC512T3	0B90h	E4h	AUTHLIM	3	000b	Limitation of negative password verification attempts 000b ... limiting of negative password verification attempts disabled 001b-111b ... maximum number of negative password verification attempts

FM24NC512T4

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC512T4	0F70h	DCh(Sector1)	MIRROR_CONF	2	00b	Defines which ASCII mirror shall be used, if the ASCII mirror is enabled by a valid MIRROR_BLOCK byte 00b ... no ASCII mirror 01b ... UID ASCII mirror 10b … Counter mirror 11b … UID & counter mirror
FM24NC512T4	0F70h	DCh(Sector1)	MIRROR_BYTE	2	00b	The 2 bits define the byte position within the block defined by the MIRROR_BLOCK byte (beginning of ASCII mirror)
FM24NC512T4	0F70h	DCh(Sector1)	SLEEP_EN	1	0b	Enables the SLEEP mode function
FM24NC512T4	0F70h	DCh(Sector1)	STRG_MOD_EN	1	0b	Controls the tag modulation strength - by default strong modulation is enabled
FM24NC512T4	0F70h	DCh(Sector1)	FDP_CONF	2	11h	FDP CONF defines the configuration of the Field detect pin 00b ... e enabled by first State-of-Frame (start of communication)

Part number	Byte address	Block address	Field	Bit	Default values	description
						01b... enabled by halt with previous read operation 10b... enabled by selection of the tag 11b... enabled by field presence
FM24NC512T4	0F70h	DCh(Sector1)	MIRROR_BLOCK	8	00h	MIRROR_BLOCK defines the block for the beginning of the ASCII mirroring A value >03h enables the ASCII mirror feature 04h-DEh ... valid MIRROR_BLOCK values for FM24NC512T4 (UID ASCII mirror) 04h-E0h ... valid MIRROR_BLOCK values for FM24NC512T4 (NFC counter mirror only) 04h-DCh ... valid MIRROR_BLOCK values for FM24NC512T4 (both UID and NFC counter mirror)
FM24NC512T4	0F73h	DCh	AUTH0	8	FFh	AUTH0 defines the block address from which the password verification is required. Valid address range for byte AUTH0 is from 00h to FFh. If AUTH0 is set to a block address which is higher than the last block from the user configuration, the password protection is effectively disabled.
FM24NC512T4	0F74h	DDh	PROT	1	0b	One bit inside the ACCESS byte defining the memory protection 0b ... write access is protected by the password verification 1b ... read and write access is protected by the password verification
FM24NC512T4	0F74h	DDh	CFGLCK	1	0b	Write locking bit for the user configuration excluding the PWD and PACK 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access
FM24NC512T4	0F74h	DDh	NFC_CNT_EN	1	0b	Enables the NFC counter

Part number	Byte address	Block address	Field	Bit	Default values	description
						0b ... disabled 1b ... enabled
FM24NC512T4	0F74h	DDh	NFC_CNT_PWD_PROT_EN	1	0b	enables the password protection to read out and mirror the NFC counter 0b ... the protection is disabled 1b ... the protection is enabled
FM24NC512T4	0F74h	DDh	AUTHLIM	3	000b	Limitation of negative password verification attempts 000b ... limiting of negative password verification attempts disabled 001b-111b ... maximum number of negative password verification attempts
FM24NC512T4	0F77h	DDh	MIRRORS	1	0b	MIRRORS defines the sector address for the beginning of the ASCII mirroring 0b … sector 0 1b … sector1
FM24NC512T4	0F77h	DDh	AUTHS	1	0b	AUTH0 defines the sector address from which the password verification is required. 0b … sector 0 1b … sector1

Remark: The CFGLCK bit activates the permanent write protection of two blocks of configuration. The write lock is only activated after a power cycle of FM24NC512Tx. If write protection is enabled, each write attempt leads to a NAK response.

Table 19 TAG password and PACK description

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC512T1	08ACh~08AFh	2Bh	PWD	32	all 1b	32-bit password used for memory access protection
FM24NC512T2	0A14h~0A17h	85h				
FM24NC512T3	0B94h~0B97h	E5h				
FM24NC512T4	0F78h~0F7Bh	DEh				
FM24NC512T1	08B0h~08B1h	2Ch	PACK	16	0000h	16-bit password acknowledge used during the password verification process
FM24NC512T2	0A18h~0A19h	86h				
FM24NC512T3	0B98h~0B99h	E6h				
FM24NC512T4	0F7Ch~0F7Dh	DFh				

7.4 TAG Lock & System memory

Table 20 TAG System memory organization of FM24NC512T1

Contact address		byte number			
Page addr.	Byte addr.	0	1	2	3
0F8h	0F80h	CT_TAG_WR_LOCK<11:0>		RFU	
	0F84h	RFU			
	0F88h	RFU			
	0F8Ch	RFU			
0F9h	0F90h	CT_TAG_PWD			
	0F94h	EH_FD_CFG	GPO_CFG	RFU	
	0F98h	RFU			
	0F9Ch	RFU			
0FAh	0FA0h	UID0	UID1	UID2	BCC1
	0FA4h	UID3	UID4	UID5	UID6
	0FA8h	BCC2	Internal		
	0FACh	Internal			

Table 21 TAG System memory organization of FM24NC512T2

Contact address		byte number			
Page addr.	Byte addr.	0	1	2	3
0F8h	0F80h	CT_TAG_WR_LOCK<31:0>			
	0F84h	CT_TAG_WR_LOCK<33:32>	RFU		
	0F88h	RFU			
	0F8Ch	RFU			
0F9h	0F90h	CT_TAG_PWD			
	0F94h	EH_FD_CFG	GPO_CFG	RFU	
	0F98h	RFU			
	0F9Ch	RFU			
0FAh	0FA0h	UID0	UID1	UID2	BCC1
	0FA4h	UID3	UID4	UID5	UID6
	0FA8h	BCC2	Internal		
	0FACh	Internal			

Table 22 TAG System memory organization of FM24NC512T3

Contact address		byte number			
Page addr.	Byte addr.	0	1	2	3
0F8h	0F80h	CT_TAG_WR_LOCK<31:0>			
	0F84h	CT_TAG_WR_LOCK<57:32>			
	0F88h	RFU			
	0F8Ch	RFU			
0F9h	0F90h	CT_TAG_PWD			
	0F94h	EH_FD_CFG	GPO_CFG	RFU	
	0F98h	RFU			

Contact address		byte number			
Page addr.	Byte addr.	0	1	2	3
	0F9Ch	RFU			
0FAh	0FA0h	UID0	UID1	UID2	BCC1
	0FA4h	UID3	UID4	UID5	UID6
	0FA8h	BCC2	Internal		
	0FACh	Internal			

Table 23 TAG System memory organization of FM24NC512T4

Contact address		byte number			
Page addr.	Byte addr.	0	1	2	3
0F8h	0F80h	CT_TAG_WR_LOCK<31:0>			
	0F84h	CT_TAG_WR_LOCK<63:32>			
	0F88h	CT_TAG_WR_LOCK<95:64>			
	0F8Ch	CT_TAG_WR_LOCK<119:96>			RFU
0F9h	0F90h	CT_TAG_PWD			
	0F94h	EH_FD_CFG	GPO_CFG	RFU	
	0F98h	RFU			
	0F9Ch	RFU			
0FAh	0FA0h	UID0	UID1	UID2	BCC1
	0FA4h	UID3	UID4	UID5	UID6
	0FA8h	BCC2	Internal		
	0FACh	Internal			

Remark 1: RFU is reserved for future use. The default value at delivery is 00h.

Remark 2: Internal is the internal data of Fudan microelectronics, and they are read only. The write operation in this area receives the response of ACK and will trigger internal write cycle, but it cannot change the readout data.

7.4.1 CT_TAG_WR_LOCK(0F80h~0F8Fh)

CT_DATA_WR_LOCK has 12/34/58/120 bits organized in 2/5/8/15 bytes. Each bit locks the write access of one page of tag memory in contact interface. CT_TAG_WR_LOCK[0] is used to lock Page 000h of tag memory, and CT_DATA_WR_LOCK[1] locks Page 001h, and so on. Logic 1 indicates lock, Logic 0 indicates unlock.

In contact interface, the read access of CT_TAG_WR_LOCK doesn't need authentication of contact password (CT_TAG_PWD). However, the write access must be in CT_PWD authenticated state.

CT_TAG_WR_LOCK does not impact write access of RF interface, and it couldn't be accessed in RF interface.

The default value of each bit of CT_TAG_WR_LOCK at delivery is 0b.

7.4.2 CT_TAG_PWD(0F90h~0F93h)

CT_TAG_PWD is password of contact interface. It has 32 bits organized in 4 bytes, which byte

address is from 0790h to 0793h in contact interface. CT_PWD is used to password authentication in contact interface.

CT_TAG_PWD can be read and write in password authenticated state of contact interface.

CT_TAG_PWD cannot be accessed by RF interface.

The default value of each byte of CT_PWD at delivery is 00h.

7.4.3 EH_FD_CFG(0F94h)

PIN_CFG is used to configure EH_FD pin. The detail is shown in Table 24.

Table 24 PIN_CFG configuration

Byte addr.	Field	Bit number inside byte							
		7	6	5	4	3	2	1	0
0F94h	EH_FD_CFG	RFU		EH_FD_CFG		EH_ILIM		EH_FD_VOUT	

EH_FD_CFG is used to configure the function of EH_FD pin. The default value at delivery is 00b.

- 00b indicates energy harvesting with 100% current drive strength
- 01b indicates energy harvesting with 26% current drive strength
- 10b indicates FD function
- 11b indicates no function (EH_FD pin high Z)

EH_ILIM is used to configure the limited current of energy harvesting function. The default value at delivery is 00b.

- 00b indicates no limit.
- 01b indicates I_{LIM}=2mA
- 10b indicates I_{LIM}=1mA
- 11b indicates I_{LIM}=0.5mA

EH_FD_VOUT is used to configure the output voltage of energy harvesting and FD function. The default value at delivery is 00b.

- 00b indicates Vout=1.8V
- 01b indicates Vout=1.5V
- 10b indicates Vout=2.5V
- 11b indicates Vout=3.3V

In contact interface, EH_FD_CFG can be read, and be written in CT_TAG_PWD authenticated state.

In RF interface, EH_FD_CFG can be read or written by tag command.

7.4.4 GPO_CFG(0F95h)

GPO_CFG is used to configure GPO pin. The detail is shown in Table 25.

Table 25 PIN_CFG configuration

Byte addr.	Field	Bit number inside byte							
		7	6	5	4	3	2	1	0
0F95h	PIN_CFG	GPO_CFG							

GPO_CFG is used to configure the function of GPO pin. The default value at delivery is 000b.

- 000b indicates RF access tag busy
- 001b indicates RF access tag WIP

- 010b indicates RF access data busy
- 011b indicates RF access data WIP
- 100b indicates RF in Data memory active status
- 101b indicates FD function
- 110b reserve for future use
- 111b indicates no function

In contact interface, GPO_CFG can be read, and be written in CT_TAG_PWD authenticated state.
In RF interface, GPO_CFG can be read or written by tag command.

7.4.5 UID(0FA0h~0FABh)

FM24NC512Tx provides read-only 9 bytes Unique Identification (UID), which byte address is from 07A0h to 07A8h in contact interface.

In accordance with ISO/IEC 14443-3 check byte 0 (BCC0) is defined as CT⊕UID0⊕UID1⊕UID2 and check byte 1 (BCC1) is defined as UID3⊕UID4⊕UID5⊕UID6. CT is Cascade Tag (value 88h) as defined in ISO/IEC 14443-3 Type A. UID0 holds the Manufacturer ID for Fudan microelectronics (1Dh) in accordance with ISO/IEC 14443-3.

In contact interface, UID in TAG system memory is read-only. The content of UID cannot be changed by write command whether in password authenticated state or not. The response of write access on UID in TAG system memory is No ACK.

In RF interface UID can be accessed by anticollision operation and read operation of the first tenth bytes of tag memory, which are the mirror of UID.

7.5 RF_SLEEP(0FFFh)

FM24NC512Tx provides RF_SLEEP register, which byte address is 0FFFh in contact interface. It is volatile. The detail is shown in Table 26.

Table 26 RF_SLEEP register

Byte addr.	Bit number inside byte							
	7	6	5	4	3	2	1	0
0FFFh	RF_SLEEP	RFU					FD_CLR	FD_SEL

RF_SLEEP is used to configure RF sleep function.
- 1b indicates to enable the sleep mode function of RF interface
- 0b indicates to disable the sleep mode function of RF interface
- The default value after power up is 0b

FD_SEL is used to configure the duration of GPO PIN in FD configuration (GPO_CFG=101b)
- 0b indicates to disable GPO PIN after RF power down
- 1b indicates to disable GPO PIN after FD_CLR set to 1
- The default value after power up is 0b

FD_CLR is used to disable GPO PIN when FD_SEL is set to 1 and GPO PIN in FD configuration (GPO_CFG=101b)
- 0b indicates to enable GPO PIN
- 1b indicates to disable GPO PIN
- The default value after power up is 0b

8 Contact Interface

FM24NC512Tx supports the two wire serial interface access. Any device that sends data to the bus is defined as a transmitter, and any device that reads data is defined as a receiver. The device that controls the data transfer is known as the bus master, and the other as the slave device. A data transfer can only be initiated by the bus master, which also provides the serial clock for synchronization. FM24NC512Tx is a slave in all communications.

8.1 Two wire serial operation

8.1.1 Data Operation

FM24NC512Tx supports data read and write operation of the conventional two wire serial interface. The detail commands can see section8.4.2 and section8.4.3. In addition, the write access of data can be locked by page through configuring CT_DATA_WR_LOCK in system memory.

8.1.2 Password protection

To protect DATA lock and TAG lock & system memory from unexpected write operation, a password protection mechanism is applied. Before any write operation to system memory, successful password verification must be applied first. Otherwise the device replies No ACK and the internal write cycle will not be triggered.

Password verification can be enabled using password verification enable command. The verification state is effective until power down or a password verification disable command.

8.1.3 Two wire serial interface timeout

During the execution of a two wire operation, the memory which is occupied by contact interface can not be accessed by RF interface.

To prevent RF communication freezing due to inadvertent un-terminated commands sent to the two wire serial bus, the FM24NC512Tx features a timeout mechanism that automatically resets the two wire logic block.

8.1.3.1 Timeout on start condition

Two wire serial communication with the FM24NC512Tx starts with a valid Start condition, followed by a device select code.

If the delay between the Start condition and the following rising edge of the Serial Clock (SCL) that samples the most significant of the Device Select exceeds the t_{START_OUT} time (see Table 66), the two wire logic block is reset and further incoming data transfer is ignored until the next valid Start condition.

8.1.3.2 Timeout on clock period

During data transfer on the two wire serial bus, if the serial clock pulse width high (t_{HIGH}) or serial clock pulse width low (t_{LOW}) exceeds the maximum value specified in Table 66, the two wire logic block is reset and any further incoming data transfer is ignored until the next valid Start condition.

8.2 Field Detection and Energy Harvesting

FM24NC512Tx features a field detection function. The field detection can be used as interrupt signal. The FD function and the output voltage can be enabled by EH_FD_CFG in TAG system memory and the trigger condition can be configured by configuration in tag memory.

This pin also features an energy harvesting function. The general purpose of the Energy harvesting is to deliver a part of the non-necessary RF power received by FM24NC512Tx on the IN1-IN2 RF input in order to supply an external device. The current consumption on EH_FD pin is limited to ensure that the FM24NC512Tx is correctly supplied during the powering of the external

device.

When the Energy harvesting mode is enabled and the power delivered on the IN1-IN2 RF input exceeds the minimum required $P_{IN1\text{-}IN2\_min}$, the FM24NC512Tx is able to deliver a regulated voltage on EH_FD pin. The output voltage and the drive current can be configured by PIN_CFG in TAG system memory. The current consumption on the EH_FD cannot exceed the configured value of IOUT in EH_FD_CFG. Otherwise, the output voltage cannot meet the configured voltage value of EH_FD_CFG.

8.3 GPO Output

FM24NC512Tx features a configurable open drain output GPO pin used to provide RF activity information to an external device. The pin functionality depends on the value of bit[7:5] of GPO_CFG in TAG system memory.

8.3.1 RF data memory Write in progress

When bit[7:5] of GPO_CFG is set to 011b, the pin is configured in RF write data memory in progress mode. The purpose of this mode is to indicate to two wire serial bus master that some data of data memory has been changed in RF interface.

In this mode, the GPO pin is tied to 0 for the duration of an internal write operation to data memory (i.e. between the end of a valid RF write command and the beginning of the RF answer).

During the execution of two wire serial write operations, the GPO pin remains in high-Z state.

8.3.2 RF data memory busy

When bit[7:5] of GPO_CFG is set to 010b, the GPO pin is configured in RF access data memory busy mode. The purpose of this mode is to indicate to two wire serial bus master whether the data memory of FM24NC512Tx is busy in RF interface or not.

In this mode, the GPO pin is tied to 0 from the RF command Start Of Frame (SOF) until the end of the command execution. If a bad RF command is received, the GPO pin is tied to 0 from the RF command SOF until the reception of the RF command CRC. Otherwise, the GPO pin is in high-Z state. When tied to 0, the GPO signal returns to High-Z state if the RF field is cut-off.

During the execution of two wire serial commands, the GPO pin remains in high-Z state.

8.3.3 RF tag memory Write in progress

When bit[7:5] of GPO_CFG is set to 001b, the pin is configured in RF write tag memory in progress mode. The purpose of this mode is to indicate to two wire serial bus master that some data of tag memory has been changed in RF interface.

In this mode, the GPO pin is tied to 0 for the duration of an internal write operation to tag memory (i.e. between the end of a valid RF write command and the beginning of the RF answer).

During the execution of two wire serial write operations, the GPO pin remains in high-Z state.

8.3.4 RF tag memory busy

When bit[7:5] of GPO_CFG is set to 000b, the GPO pin is configured in RF access tag memory busy mode. The purpose of this mode is to indicate to two wire serial bus master whether the tag memory of FM24NC512Tx is busy in RF interface or not.

In this mode, the GPO pin is tied to 0 from the RF command Start Of Frame (SOF) until the end of the command execution. If a bad RF command is received, the GPO pin is tied to 0 from the RF command SOF until the reception of the RF command CRC. Otherwise, the GPO pin is in high-Z state. When tied to 0, the GPO signal returns to High-Z state if the RF field is cut-off.

During the execution of two wire serial commands, the GPO pin remains in high-Z state.

8.3.5 RF Data memory active status

When bit[7:5] of GPO_CFG is set to 100b, the GPO pin is configured in RF data memory active mode. The purpose of this mode is to indicate to two wire serial bus master whether the device is

in data memory active status.

In this mode, the GPO pin is tied to 0 after receiving Rats command and returns to High-Z state if the RF field is cut-off.

8.3.6 Field detection

When bit[7:5] of GPO_CFG is set to 101b, the GPO pin is configured in field detect function which can be used as interrupt signal. In this configuration, GPO pin performs the same function as the EH_FD pin in FD configuration, except for GPO pin's open drain feature, while EH_FD features a configurable output voltage. This provides flexible solution for system design.

8.3.7 No function

When bit[7:5] of GPO_CFG is set to 111b, the GPO pin has no function and remains in high-Z state.

8.4 Command

8.4.1 Command Overview

8.4.1.1 Command Set

Table 27 command set of two wire serial interface

Command	Device Address	Address	Data
Data memory Write	A0h	0000h~FFFFh	1~128 bytes
Data memory Read	A1h	-	Output n bytes
Data memory Password authentication	A2h (un-authenticated state)	0408h	4 bytes PWD
Data memory Password write	A2h (authenticated state)	0408h	4 bytes new PWD
Data memory Password read	A3h (authenticated state)	- (1)	Output 4 bytes PWD
Data memory Password de-authentication	A3h (authenticated state)	- (1)	-
TAG memory Write	A2h	0800h~08BFh for FM24NC512T4 0800h~0A1Fh for FM24NC512T4 0800h~0B9Fh for FM24NC512T4 0800h~0F7Fh for FM24NC512T4	1~16 bytes
TAG memory Read	A3h		Output n bytes
TAG memory Password authentication	A2h (un-authenticated state)	0F90h	4 bytes PWD
TAG memory Password write	A2h (authenticated state)	0F90h	4 bytes new PWD
TAG memory Password read	A3h (authenticated state)	- (1)	Output 4 bytes PWD
TAG memory Password de-authentication	A3h (authenticated state)	- (1)	-

Note: 1. The current address of read operation is the address of CT_DATA_PWD or CT_TAG_PWD.

8.4.1.2 Timing

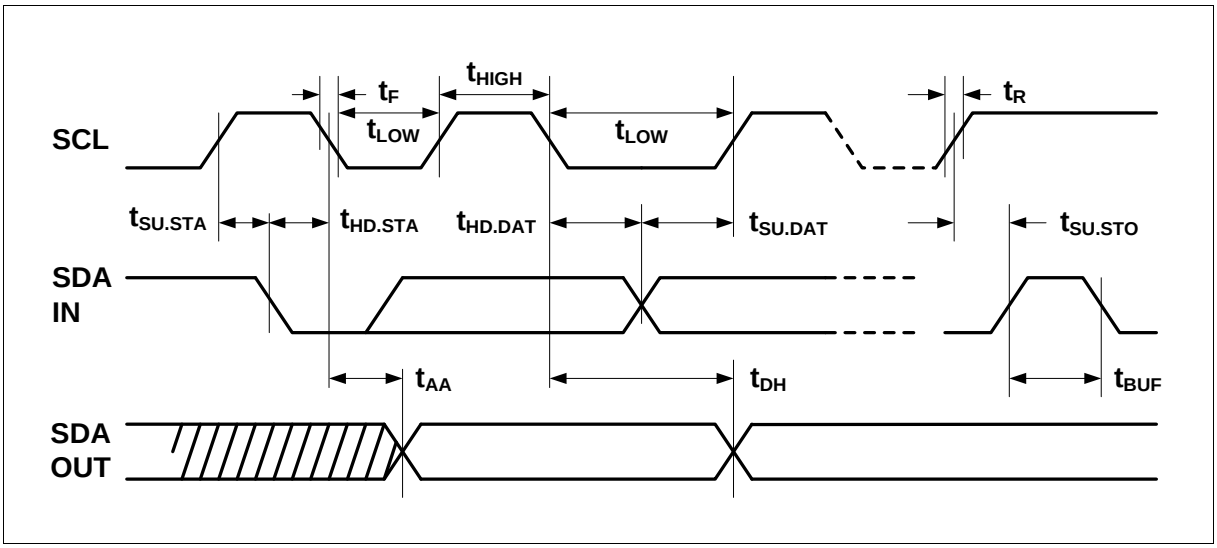


Figure 3 Two-wire Series Interface Bus Timing

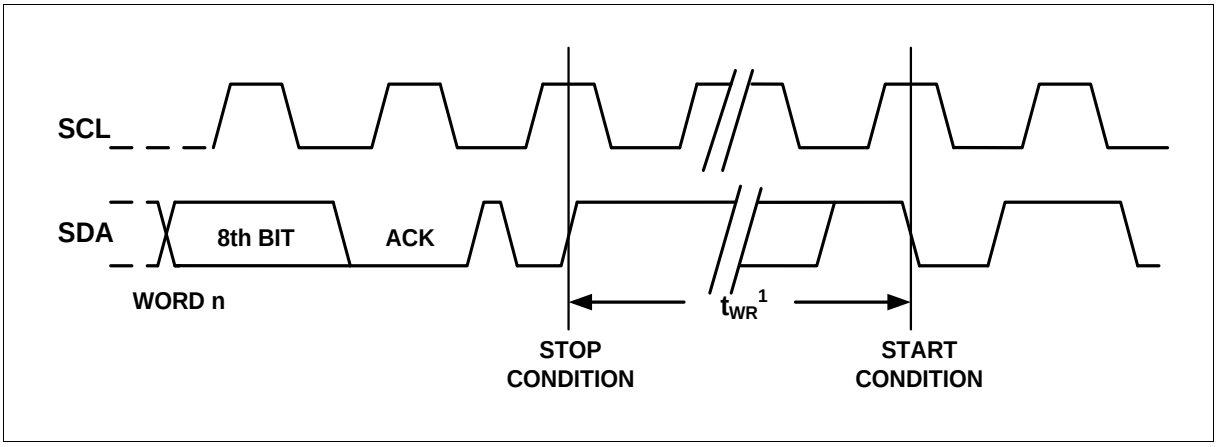


Figure 4 Writing Cycle Timing

Note: 1. The writing cycle time, t_{WR}, is the time from a valid stop condition of a writing sequence to the end of the internal erase/program cycle.

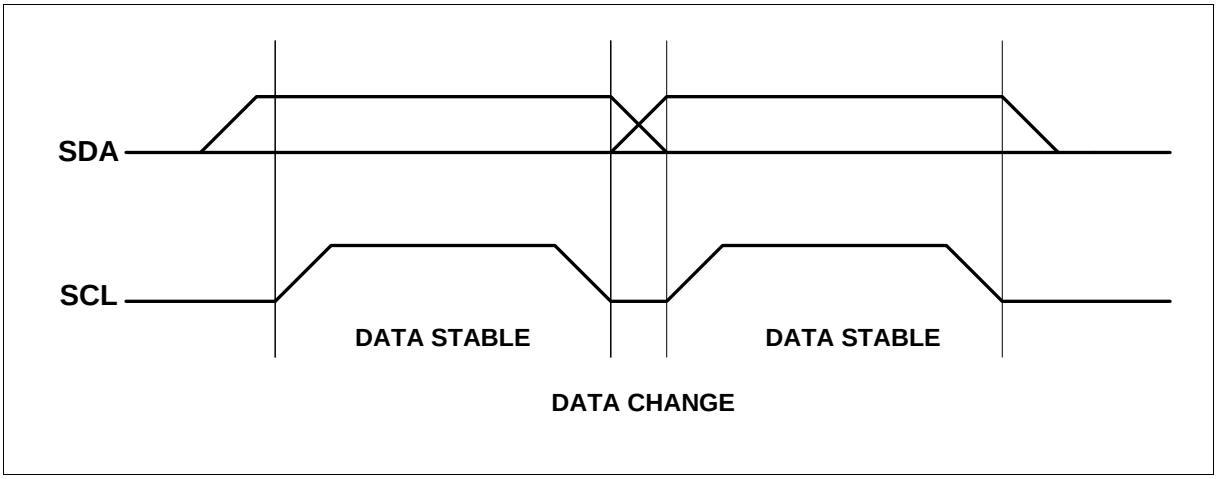


Figure 5 Data Validity

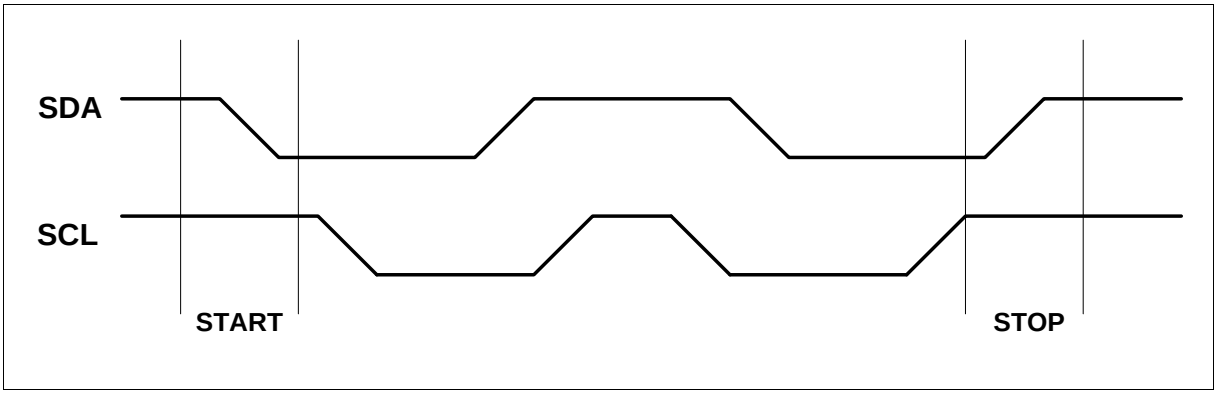


Figure 6 Start and Stop Definition

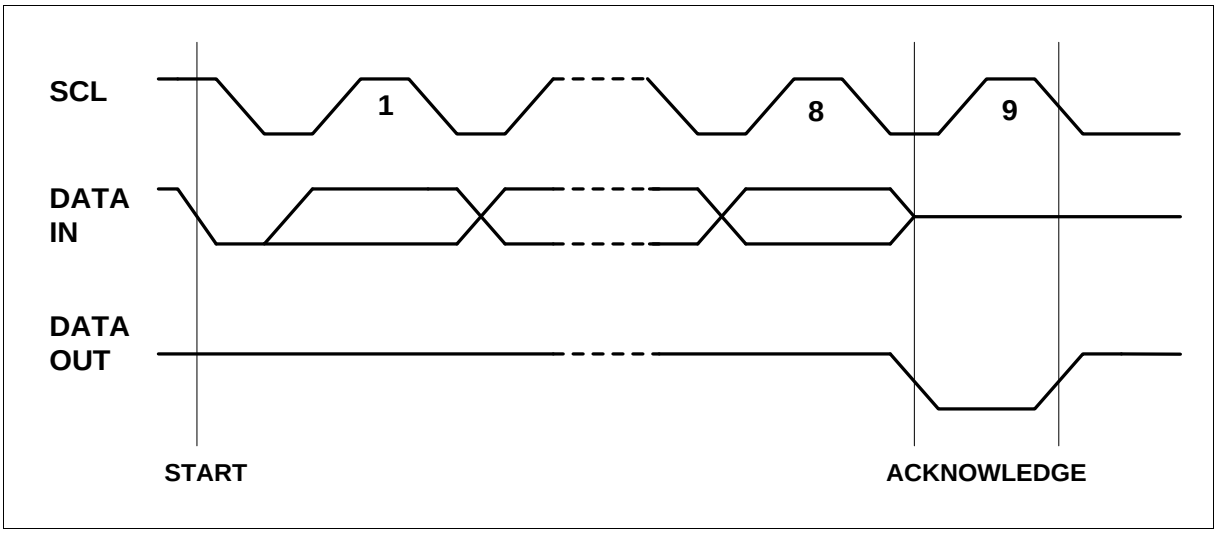


Figure 7 Output Acknowledge

8.4.1.3 Start condition

Start is identified by a falling edge of serial data (SDA) while the serial clock (SCL) is stable in the high state. A Start condition must precede any data transfer command. The device continuously monitors (except during a write cycle) the SDA and the SCL for a Start condition, and does not respond unless one is given.

8.4.1.4 Stop condition

Stop is identified by a rising edge of serial data (SDA) while the serial clock (SCL) is stable and driven high. A Stop condition terminates communication between the device and the bus master. A Read command that is followed by No Ack can be followed by a Stop condition to force the device into the Standby mode. A Stop condition at the end of a Write command triggers the internal write cycle.

8.4.1.5 Acknowledge bit (ACK)

The acknowledge bit is used to indicate a successful byte transfer. The bus transmitter, whether a bus master or a slave device, releases the serial data (SDA) after sending eight bits of data. During the 9th clock pulse period, the receiver pulls the SDA low to acknowledge the receipt of the eight data bits.

Table 28 ACK response in contact interface

Operation	Area	State	Response
Write	Data memory	un-locked	ACK
		locked	ACK
	Tag memory	un-locked	ACK
		locked	No ACK (from data byte)
	Lock byte, CT_PWD & PIN_CFG in DATA & TGA System memory	Relative CT_PWD authenticated	ACK
		Relative CT_PWD un-authenticated	No ACK (from data byte)
	UID in TAG System memory	CT_TAG_PWD authenticated	No ACK (from data byte)
		CT_TAG_PWD un-authenticated	No ACK (from data byte)
	Internal	CT_TAG_PWD authenticated	No ACK (from data byte)
		CT_TAG_PWD un-authenticated	No ACK (from data byte)
	NULL	-	ACK (no data refreshed)
	RFU		Same response as the contents in the same page
Password authentication	CT_PWD in DATA or TAG System memory	Relative CT_PWD un-authenticated	AUTH pass: ACK AUTH failure: No ACK

8.4.1.6 Data input

During data input, the device samples serial data (SDA) on the rising edge of the serial clock (SCL). For correct device operation, the SDA must be stable during the rising edge of the SCL, and the SDA signal must change only when the SCL is driven low.

8.4.1.7 Device addressing

To start a communication between the bus master and the slave device, the bus master must initiate a Start condition. Following this, the bus master sends the device address word, shown in Figure 8(on Serial Data (SDA), the most significant bit first).

The device address consists of a 4-bit device type identifier which should be 1010b and a 3-bit Chip Enable “Address” (000b for data, 001b for data system, tag and tag system).

The eighth bit is the Read/Write bit (R/W). It is set to 1 for Read and to 0 for Write operations.

If a match occurs on the device select code, the corresponding device gives an acknowledgment on serial data (SDA) during the ninth bit time. If the device does not match the device select code, it deselects itself from the bus, and enters Standby mode.

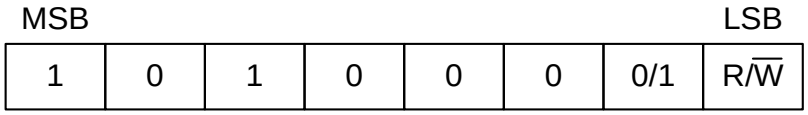


Figure 8 Device address of two wire serial interface

8.4.2 Write command

Following a Start condition, the bus master sends a device select code with the Read/Write bit (RW) reset to 0. The device acknowledges this and waits for two address bytes and data bytes. The device responds to each address byte and data byte with an acknowledge bit if memory is not locked.

When the bus master generates a Stop condition immediately after the Ack bit (in the tenth bit time slot), either at the end of a byte write or a page write, the internal write cycle is triggered and all inputs are disabled during this write cycle and the EEPROM will not respond until the write is complete. A Stop condition at any other time slot does not trigger the internal write cycle.

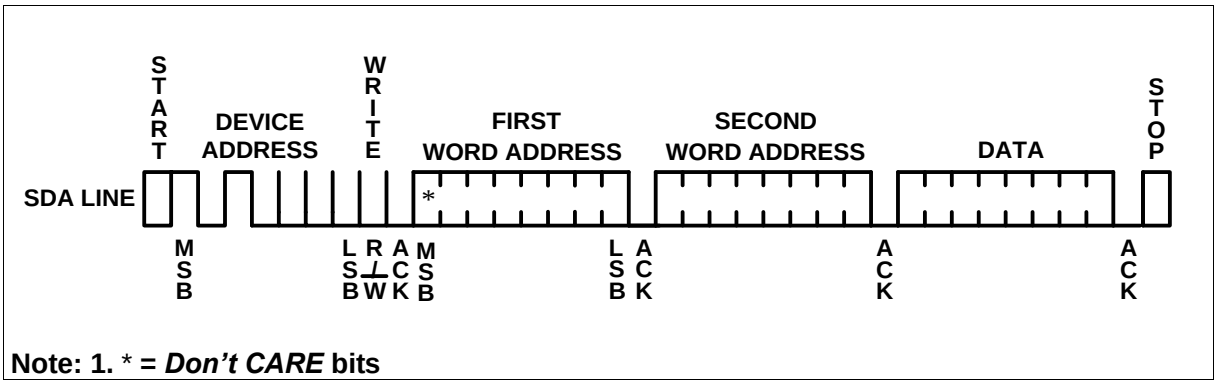
Writing to data memory may be inhibited if the write protect register CT_DATA_WR_LOCK=1. In this situation, device replies No Ack from data bytes and internal write cycle is not triggered.

Writing to tag memory may be inhibited if corresponding lock bit=1 (CT_TAG_WR_LOCK). In this situation, device replies No Ack from data bytes and internal write cycle is not triggered.

Writing to DATA lock or TAG lock & system memory needs relative password verification. Without verification, device replies No Ack from data bytes and internal write cycle is not triggered.

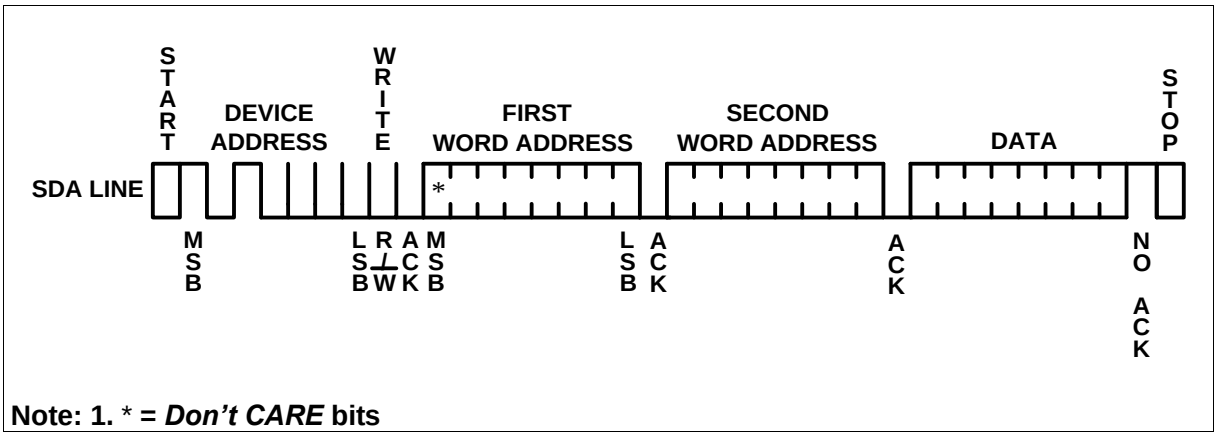
8.4.2.1 Byte write

After the device select code and the address bytes, the bus master sends one data byte, following a stop condition to trigger the internal write cycle.



Note: 1. * = *Don't CARE* bits

Figure 9 Byte write with lock bit/register =0



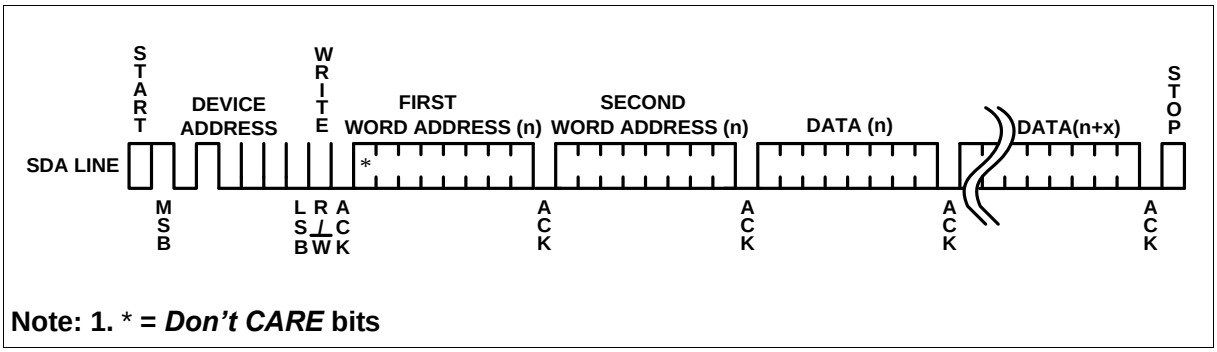
Note: 1. * = *Don't CARE* bits

Figure 10 Byte write with or lock bit/ register =1

8.4.2.2 Page write

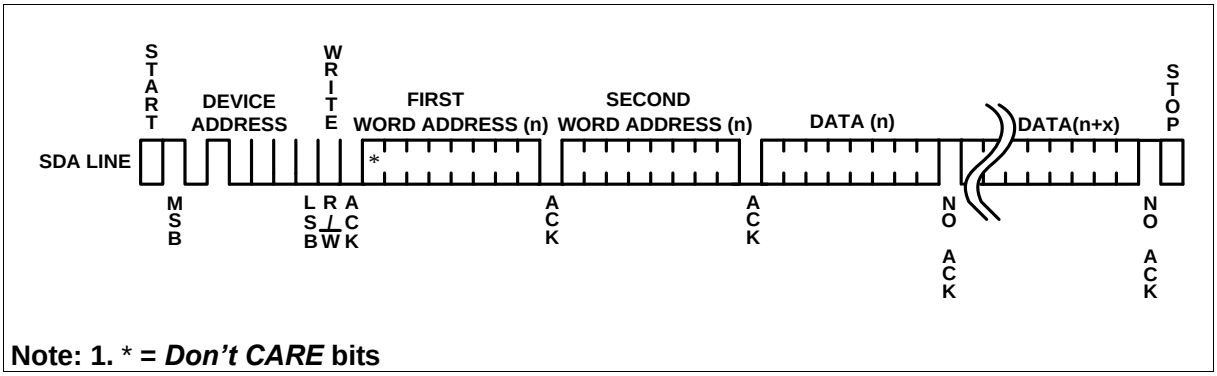
A page write is initiated the same way as a byte write, but the master does not send a stop condition after the first data word is clocked in. Instead, after the EEPROM acknowledges receipt of the first data word, the master can transmit up to 127 more data words for data memory or 15 more data words for data system, tag and tag system memory. The EEPROM responds to each data byte with an acknowledge bit. After sending all data bytes, the master sends a stop condition to trigger the internal write cycle.

The data word address lower seven bits for data memory access or lower four bits for tag memory access are internally incremented following the receipt of each data word. The higher data word address bits are not incremented, retaining the memory page row location. When the word address, internally generated, reaches the page boundary, the following byte is placed at the beginning of the same page. If more than 128 data words for data or 16 bytes for tag and tag system are transmitted to the EEPROM, the data word address will “roll over” and previous data will be overwritten.



Note: 1. * = *Don’t CARE* bits

Figure 11 Page write with lock bit/register =0



Note: 1. * = *Don’t CARE* bits

Figure 12 Page write with WP_DATA=1 or lock bit/ register =1

8.4.2.3 ACKNOWLEDGE POLLING

Once the internally timed write cycle has started and the EEPROM inputs are disabled, acknowledge polling can be initiated. This involves sending a start condition followed by the device address word. The read/write bit is representative of the operation desired. Only if the internal write cycle has completed will the EEPROM respond with a zero allowing the read or write sequence to continue.

8.4.3 Read command

Read operations are initiated the same way as write operations with the write command exception that the read/write select bit in the device address word is set to one. There are three

read operations: current address read, random address read and sequential read.

8.4.3.1 Current address read

For the Current Address Read operation, following a Start condition, the bus master only sends a device select code with the Read/Write bit (RW) set to 1. The device acknowledges this, and outputs the byte addressed by the internal address counter which maintains the last address accessed during the last read or write operation, incremented by one. This address stays valid between operations as long as the chip power is maintained. The counter is then incremented. The bus master terminates the transfer with a Stop condition.

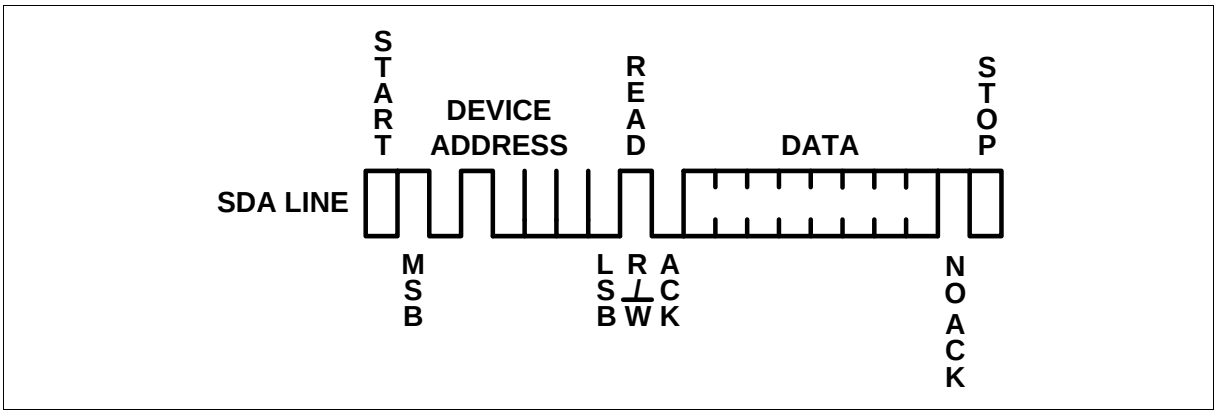
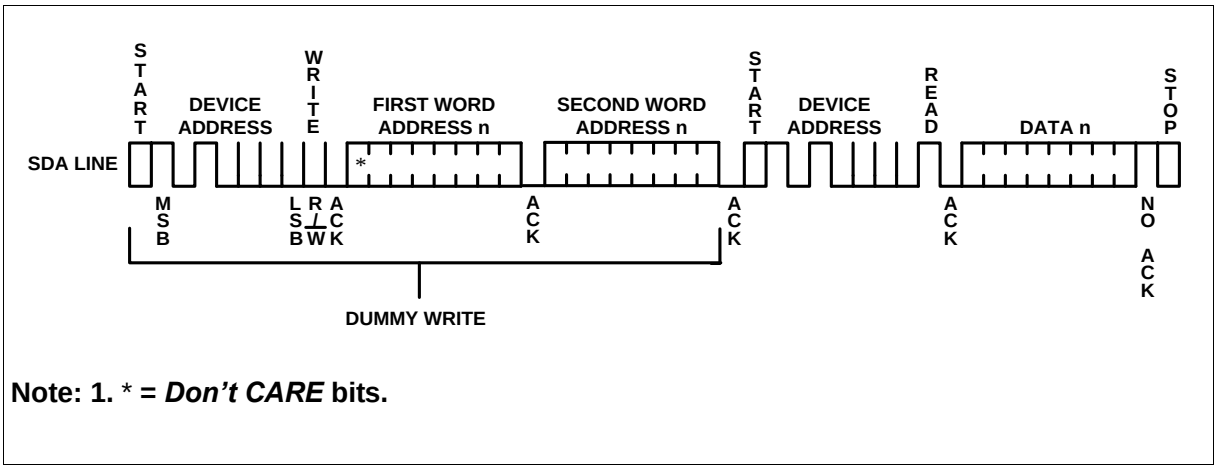


Figure 13 Current address read

8.4.3.2 Random read

A dummy write is first performed to load the address into this address counter but without sending a Stop condition. After device address byte, the bus master sends another Start condition, and repeats the device select code, with the Read/Write bit (RW) set to 1. The device acknowledges this, and outputs the contents of the addressed byte. The bus master must not acknowledge the byte, and terminates the transfer with a Stop condition.



Note: 1. * = *Don't CARE* bits.

Figure 14 random read

8.4.3.3 Sequential read

This operation can be used after a Current Address Read or a Random Address Read. The bus master does acknowledge the data byte output, and sends additional clock pulses so that the device continues to output the next byte in sequence. To terminate the stream of bytes, the bus master must not acknowledge the last byte, and must generate a Stop condition.

The output data comes from consecutive addresses, with the internal address counter automatically incremented after each byte output. After the last memory address, the address counter “rolls over”, and the device continues to output data from memory address 00h.

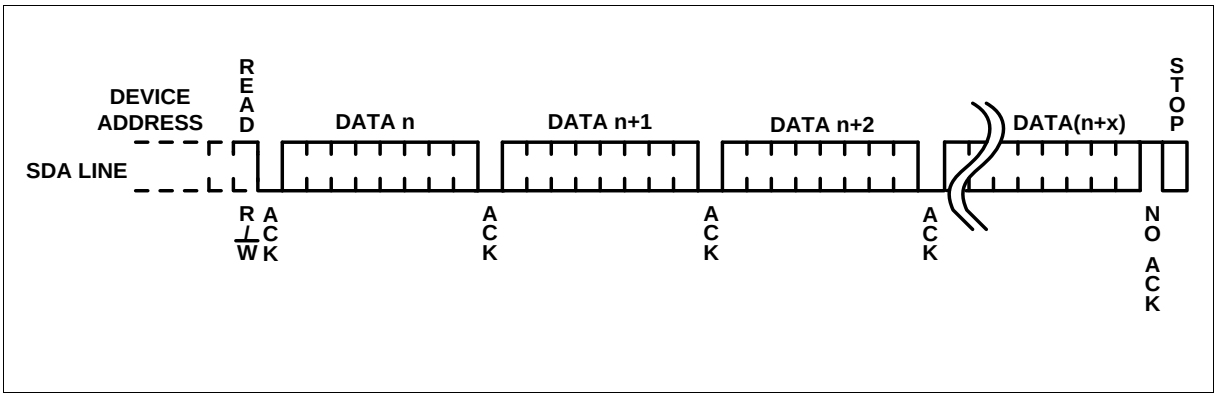


Figure 15 sequential read

8.4.4 Password command

For write operation, the device has two status, verified status in which lock and system memory can be modified using write command and unverified status in which system memory cannot be modified. The status is determined by password verification operation.

There are four password operations: password authentication, password write, password read and password de-authentication.

After power up, the device is in unverified status. A successful password verification operation makes the device enter verified status. In this status, password can be read or write. After a password verification disable command, the device returns to unverified status.

8.4.4.1 Password authentication

Password authentication operation must be performed in unauthenticated status. Otherwise, it is regarded as password write refer to section 9.1.5.2.

It is initiated the same way as write operations, with the exception that the address must be the starting address of CT_DATA_PWD or CT_TAG_PWD and the following data must be 4 bytes. After a stop condition, an internal comparison progress is triggered. The internal logic unit compares the 4 bytes input data and the 4 bytes password stored in memory. If the input data matches the password, the password authentication operation is successful and the device enters relative authenticated status (For DATA password authentication, enters DATA authenticated status, For TAG password authentication, enters TAG authenticated status). If the input data does not match password, the password authentication operation is fail and the device remains unauthenticated state.

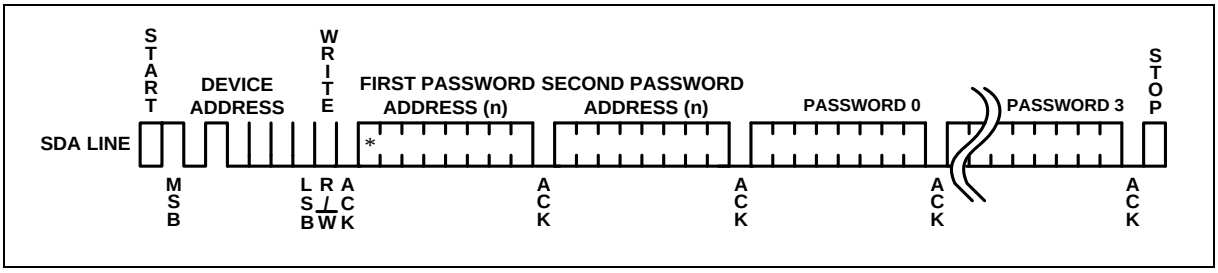


Figure 16 password authentication

8.4.4.2 Password write

Password write command is same as password authentication. If the device is already in authenticated status, this command will be regarded as password write command. After a stop condition, internal write cycle is trigged and the password stored in memory is refreshed according to the input data.

8.4.4.3 Password read

In authenticated state, password can be read. It is initiated the same way as random read.

After stop or next start, the device returns to unauthenticated status.

If device receives password read command in unauthenticated status, it replies ACK but the output data is all logic 0.

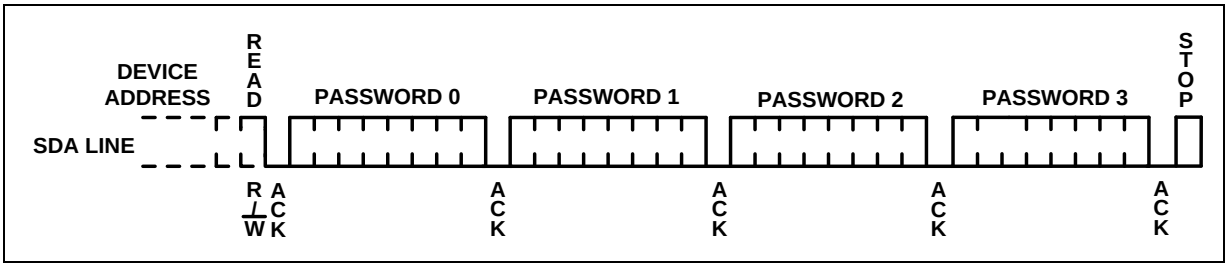


Figure 17 password read in authenticated state

8.4.4.4 Password de-authentication

If read operation reaches the boundary of password bytes, after stop or next start, the device returns to unauthenticated state.

9 RF interface

The RF-interface is based on the ISO/IEC 14443 Type A standard.

During operation, the NFC device generates an RF field. The RF field must always be present (with short pauses for data communication) as it is used for both communication and as power supply for the Digital Control Unit of tag. During RF interface operation, contact power supply pin (VCC) must be power on, because the power of EEPROM memory is supplied by Vcc pin. The harvested energy of EH_FD pin comes from RF field.

For both directions of data communication, there is one start bit at the beginning of each frame. Each byte is transmitted with an odd parity bit at the end. The LSB of the byte with the lowest address of the selected block is transmitted first. The maximum length of a NFC device to FM24NC512Tx frame is 2369 bits (1 PCB byte + 1 INS byte + 2 address bytes + 1 Lc byte + 256 data bytes + 2 CRC bytes + 1 start bit). The maximum length of a FM24NC512Tx to NFC device frame is 2326 bits (256 data bytes + 2 CRC bytes + 1 start bit). The TAG FAST_READ command has a variable frame length depending on the start and end address parameters. The maximum frame length supported by the NFC device needs to be taken into account when issuing this command.

For a multi-byte parameter, the least significant byte is always transmitted first. As an example, when reading from the memory using the READ command, byte 0 from the addressed block is transmitted first, followed by byte 1 to byte 3 out of this block. The same sequence continues for the next block and all subsequent blocks.

9.1 Communication principle

The commands are initiated by the NFC device and controlled by the Digital Control Unit of the FM24NC512Tx. The command response is depending on the state of the IC and for memory operations also on the access conditions valid for the corresponding page.

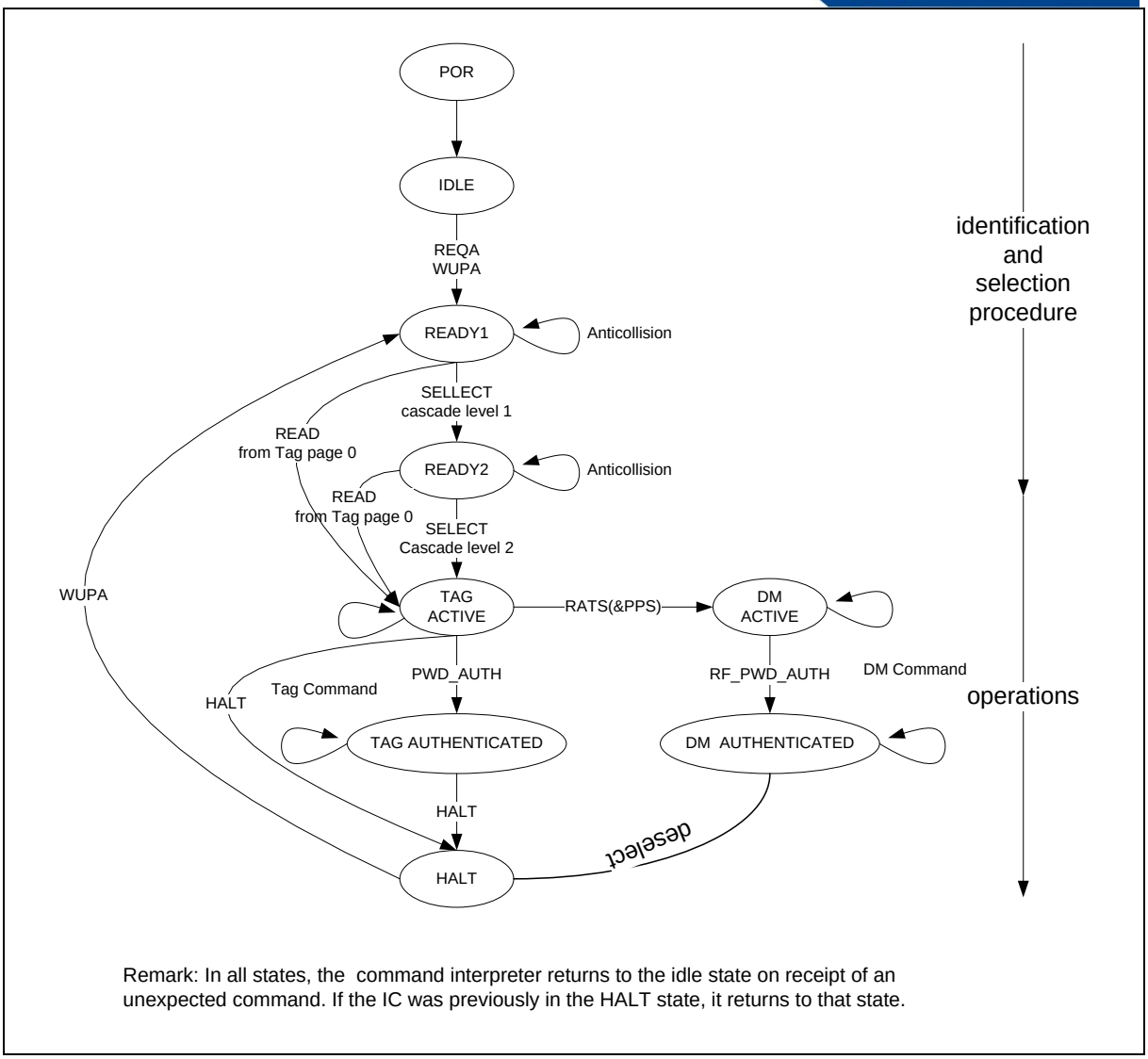


Figure 18 state diagram of RF interface

9.1.1 IDLE state

After a power-on reset (POR), FM24NC512Tx switches to the IDLE state. It only exits this state when a REQA or a WUPA command is received from the NFC device. Any other data received while in this state is interpreted as an error and FM24NC512Tx remains in the IDLE state.

After a correctly executed HLTA command i.e. out of the ACTIVE or AUTHENTICATED state, the default waiting state changes from the IDLE state to the HALT state. This state can then be exited with a WUPA command only.

9.1.2 READY1 state

In this state, the NFC device resolves the first part of the UID (3 bytes) using the ANTICOLLISION or SELECT commands in cascade level 1. This state is correctly exited after execution of either of the following commands:

• SELECT command from cascade level 1: the NFC device switches FM24NC512Tx into READY2 state where the second part of the UID is resolved.

• READ command (from address 0): all anticollision mechanisms are bypassed and the FM24NC512Tx switches directly to the ACTIVE state.

Remark: If more than one tag is in the NFC device field, a READ command from address 0 selects all FM24NC512Tx devices. In this case, a collision occurs due to different serial numbers. Any other data received in the READY1 state is interpreted as an error and depending on its previous state FM24NC512Tx returns to the IDLE or HALT state.

9.1.3 READY2 state

In this state, FM24NC512Tx supports the NFC device in resolving the second part of its UID (4 bytes) with the cascade level 2 ANTICOLLISION command. This state is usually exited using the cascade level 2 SELECT command.

Alternatively, READY2 state can be skipped using a READ command (from address 0) as described for the READY1 state.

Remark: The response of FM24NC512Tx to the cascade level-2 SELECT command is the Select Acknowledge (SAK) byte. In accordance with ISO/IEC 14443, this byte indicates if the anticollision cascade procedure has finished. FM24NC512Tx is now uniquely selected and only this device will communicate with the NFC device even when other contactless devices are present in the NFC device field. If more than one FM24NC512Tx is in the NFC device field, a READ command from address 0 selects all FM24NC512Tx devices. In this case, a collision occurs due to the different serial numbers. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state the FM24NC512Tx returns to either the IDLE state or HALT state.

9.1.4 TAG ACTIVE state

All tag operations and other functions like the originality check are operated in this state.

The ACTIVE state is exited with the HLTA command and upon reception FM24NC512Tx transits to the HALT state. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state, FM24NC512Tx returns to either the IDLE state or HALT state.

FM24NC512Tx transits to the TAG AUTHENTICATED state after successful password verification using the PWD_AUTH command.

9.1.5 TAG AUTHENTICATED state

In this state, all operations on TAG memory blocks, which are configured as password verification protected, can be accessed.

The TAG AUTHENTICATED state is exited with the HLTA command and upon reception FM24NC512Tx transits to the HALT state. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state, FM24NC512Tx returns to either the IDLE state or HALT state.

9.1.6 Data Memory (DM) ACTIVE state

In this state, data memory can be read and authentication can be performed. Any write command to data memory is not permitted and replies NAK.

Any other data received when the device is in this state is interpreted as an error and FM24NC512Tx returns to HALT state.

FM24NC512Tx transits to the DM AUTHENTICATED state after successful RF password verification using the RF_PWD_AUTH command.

9.1.7 Data Memory (DM) AUTHENTICATED state

In this state, all operations on RF read/write data memory and lock bits can be accessed.

Any other data received when the device is in this state is interpreted as an error and FM24NC512Tx returns to HALT state.

9.1.8 HALT state

HALT and IDLE states constitute the two wait states implemented in FM24NC512Tx. An already processed FM24NC512Tx can be set into the HALT state using the HLTA or deselect command. In the anti-collision phase, this state helps the NFC device to distinguish between processed tags and tags yet to be selected. FM24NC512Tx can only exit this state on execution of the WUPA command. Any other data received when the device is in this state is interpreted as an error and FM24NC512Tx state remains unchanged.

9.2 RF operation

9.2.1 Data operation

9.2.1.1 Tag Memory Operation

Using RF tag memory command, RF interface can access tag memory. Tag memory command can see section 9.3.2. These commands are used to read or write data in tag memory.

9.2.1.2 Data Memory Operation

Using RF data memory command, RF interface can access 512Kbit data memory. Data memory command includes READ and WRITE. These two commands are used to read or write data in data memory. The number of data bytes can be configured, using 1 Lc byte for write operation and 1 Le byte for read operation, respectively. That is, for read operation, 1~256 bytes can be transferred in one command. For write operation, because of the limitation of page size, if more than 128 data words are transmitted, the data word address will “roll over” and previous data will be overwritten.

Read and writing access of data memory in RF interface could be restricted by RF_DATA_RD_LOCK, RF_DATA_WR_LOCK or Data memory unauthenticated status. If RF_DATA_RD_LOCK register is 1, read operation to data memory by RF interface is restricted and the response is NAK. If the device is in Data memory unauthenticated status or RF_DATA_WR_LOCK register is 1, write operation to data memory by RF interface is restricted and the response is NAK.

9.2.1.3 Data Memory Lock Operation

Using RF lock command, the read and writing access in RF interface could be read and changed.

READ_RF_DATA_RD_LOCK and READ_RF_DATA_WR_LOCK commands are used to read RF_DATA_RD_LOCK and RF_DATA_WR_LOCK register individually. These two commands doesn’t need RF_PWD authentication. They can operate not only in DM ACTIVE state, but also in DM AUTHENTICATED state.

WRITE_RF_DATA_RD_LOCK and WRITE_RF_DATA_WR_LOCK commands are used to Lock RF_DATA_RD_LOCK and RF_DATA_WR_LOCK individually. These two commands need RF_PWD authentication. They can operate only in DM AUTHENTICATED state.

WRITE_RF_DATA_RD_LOCK and WRITE_RF_DATA_WR_LOCK commands are bit-wise OR’ed. It can change lock bit to logic 1, but cannot change back to logic 0.

9.2.2 Data integrity

Following mechanisms are implemented in the contactless communication link between NFC device and FM24NC512Tx to ensure very reliable data transmission:

- 16 bits CRC per block
- parity bits for each byte
- bit count checking
- bit coding to distinguish between “1”, “0” and “no information”
- channel monitoring (protocol sequence and bit stream analysis)

9.2.3 ASCII mirror function

FM24NC512Tx features a ASCII mirror function. This function enables FM24NC512Tx to virtually mirror

- 7 byte UID
- 3 byte NFC counter value
- both, 7 byte UID and 3 byte NFC counter value with a sepration byte

into the physical tag memory of the IC. On the READ or FAST READ command to the involved user memory blocks, FM24NC512Tx will respond with the virtual memory content of the UID in ASCII code.

The required length of the reserved physical memory for the mirror functions is specified as below.

- UID mirror 14 bytes
- NFC counter mirror 6 bytes
- UID + counter mirror 21 bytes (14 bytes UID + 1 byte separation + 6 byte counter)

The position within the user memory where the mirroring of the UID shall start is defined by the MIRROR_BLOCK and MIRROR_BYTE values.

The MIRROR_BLOCK value defines the block where the UID ASCII mirror shall start and the MIRROR_BYTE value defines the starting byte within the defined block.

9.2.3.1 UID ASCII mirror function

This function enables FM24NC512Tx to virtually mirror the 7 byte UID in ASCII code into the physical memory of the IC. The length of the UID ASCII mirror requires 14 bytes to mirror the UID in ASCII code. On the READ or FAST READ command to the involved user memory blocks, FM24NC512Tx will respond with the virtual memory content of the UID in ASCII code.

The position within the user memory where the mirroring of the UID shall start is defined by the MIRROR_BLOCK and MIRROR_BYTE values.

The MIRROR_BLOCK value defines the block where the UID ASCII mirror shall start and the MIRROR_BYTE value defines the starting byte within the defined block.

The UID ASCII mirror function is enabled with a MIRROR_BLOCK value >03h and the MIRROR_CONF bits are set to 01b.

Remark: Please note that the 14 bytes of the UID ASCII mirror shall not exceed the boundary of the tag user memory. Therefore it is required to use only valid values for MIRROR_BYTE and MIRROR_BLOCK to ensure a proper functionality.

Table 29 Configuration parameter descriptions

	MIRROR_BLOCK	MIRROR_BYTE bits
Minimum values	04h	00 - 11b
Maximum values	last user memory block - 3	10b

9.2.3.2 NFC counter mirror function

This function enables FM24NC512Tx to virtually mirror the 3 byte NFC counter value in ASCII code into the physical memory of the IC. The length of the NFC counter mirror requires 6 bytes to mirror the NFC counter value in ASCII code. On the READ or FAST READ command to the involved user memory blocks, FM24NC512Tx will respond with the virtual memory content of the NFC counter in ASCII code.

The position within the user memory where the mirroring of the NFC counter shall start is defined by the MIRROR_BLOCK and MIRROR_BYTE values.

The MIRROR_BLOCK value defines the block where the NFC counter mirror shall start and the MIRROR_BYTE value defines the starting byte within the defined block.

The NFC counter mirror function is enabled with a MIRROR_BLOCK and MIRROR_BYTE value according to Table 30 and the MIRROR_CONF bits are set to 10b.

If the NFC counter is password protected with the NFC_CNT_PWD_PROT bit set to 1b (see Section 8.5.7), the NFC counter will only be mirrored into the physical memory, if avalid password authentication has been executed before.

The NFC counter ASCII mirror function is enabled with a MIRROR_BLOCK value >03h and the MIRROR_CONF bits are set to 10b.

Remark: Please note that the 6 bytes of the NFC counter mirror shall not exceed the boundary of the tag user memory. Therefore it is required to use only valid values for MIRROR_BYTE and MIRROR_BLOCK to ensure a proper functionality.

Table 30 Configuration parameter descriptions

	MIRROR_BLOCK	MIRROR_BYTE bits
Minimum values	04h	00 - 11b
Maximum values	last user memory block - 1	10b

9.2.3.3 UID and NFC counter mirror function

This function enables FM24NC512Tx to virtually mirror the 7 byte UID and 3byte NFC counter value in ASCII code into the physical memory of the IC separated by 1 byte (“x” character, 78h). The length of the mirror requires 21 bytes to mirror the UID, NFC counter value and the separation byte in ASCII code. On the READ or FAST READ command to the involved user memory blocks, FM24NC512Tx will respond with the virtual memory content of the UID and NFC counter in ASCII code.

The position within the user memory where the mirroring shall start is defined by the MIRROR_BLOCK and MIRROR_BYTE values.

The MIRROR_BLOCK value defines the block where the mirror shall start and the MIRROR_BYTE value defines the starting byte within the defined block.

The UID and NFC counter mirror function is enabled with a MIRROR_BLOCK and a MIRROR_BYTE value according to Table 31 and the MIRROR_CONF bits are set to 11b.

If the NFC counter is password protected with the NFC_CNT_PWD_PROT bit set to 1b (see Section 8.5.7), the NFC counter will only be mirrored into the physical memory, if a valid password authentication has been executed before.

The UID and NFC counter ASCII mirror function is enabled with a MIRROR_BLOCK value >03h and the MIRROR_CONF bits are set to 11b.

Remark: Please note that the 21 bytes of the UID and NFC counter mirror shall not exceed the boundary of the tag user memory. Therefore it is required to use only valid values for MIRROR_BYTE and MIRROR_BLOCK to ensure a proper functionality.

Table 31 Configuration parameter descriptions

	MIRROR_BLOCK	MIRROR_BYTE bits
Minimum values	04h	00 - 11b
Maximum values	last user memory block - 5	10b

9.2.4 RF tag Password verification protection

The memory write or read/write access to a configurable part of the tag memory by RF interface can be constrained to a positive password verification. The 32-bit secret password (PWD) and the 16-bit password acknowledge (PACK) responses are typically programmed into the configuration blocks at the tag personalization stage. The AUTHLIM parameter specified in Section 7.3.7 can be used to limit the negative verification attempts.

In the initial state of FM24NC512Tx, password protection is disabled by a AUTH0 value of FFh. PWD and PACK are freely writable in this state. Access to the configuration blocks and any part of the user memory can be restricted by setting AUTH0 to a block address within the available memory space. This block address is the first one protected.

Remark: The password protection method provided in FM24NC512Tx has to be intended as an easy and convenient way to prevent unauthorized memory accesses. If a higher level of protection is required, cryptographic methods can be implemented at application layer to increase overall system security.

9.2.4.1 Programming of Tag PWD and PACK

The 32-bit PWD and the 16-bit PACK need to be programmed into the configuration pages, see Section 7.3.7. The password as well as the password acknowledge are written LSByte first. This byte order is the same as the byte order used during the PWD_AUTH command and its response.

The PWD and PACK bytes can never be read out of the memory. Instead of transmitting the real value on any valid READ or FAST_READ command, only 00h bytes are replied.

If the password verification does not protect the configuration pages, PWD and PACK can be written with normal WRITE and COMPATIBILITY_WRITE commands.

If the configuration blocks are protected by the password configuration, PWD and PACK can be written after a successful PWD_AUTH command.

The PWD and PACK are writable even if the CFGLCK bit is set to 1b. Therefore it is strongly recommended to set AUTH0 to the block where the PWD is located after the password has been written. This block is 2Bh for FM24NC512T1, 85h for FM24NC512T2 and E5h for FM24NC512T3.

Remark: To improve the overall system security, it is advisable to diversify the password and the password acknowledge using a die individual parameter, that is the 7-byte UID available on FM24NC512Tx.

9.2.4.2 Limiting negative verification attempts

To prevent brute-force attacks on the password, the maximum allowed number of negative password verification attempts can be set using AUTHLIM. This mechanism is disabled by setting AUTHLIM to a value of 000b, which is also the initial state of FM24NC512Tx.

If AUTHLIM is not equal to 000b, each of negative verification is internally counted. As soon as this internal counter reaches the number specified in AUTHLIM, any further negative password verification leads to a permanent locking of the protected part of the memory for the specified access modes. Specifically, whether the provided password is correct or not, each subsequent PWD_AUTH fails. Any successful password verification, before reaching the limit of negative password verification attempts, resets the internal counter to zero.

9.2.4.3 Protection of special memory segments

The configuration blocks can be protected by the password authentication as well. The protection level is defined with the PROT bit.The protection is enabled by setting the AUTH0 byte to a value that is within the addressable memory space.

9.2.5 Originality signature

FM24NC512Tx features a cryptographically supported originality check. With this feature, it is possible to verify with a certain confidence that the tag is using an IC manufactured by Fudan microelectronics. This check can be performed on personalized tags as well. If you need further information, please contact us.

9.3 Command

9.3.1 Overview

NFC tag of FM24NC512Tx activation follows the ISO/IEC 14443 Type A. After tag has been selected, it can either be deactivated using the ISO/IEC 14443 HLTA command, or the NFC tag commands (e.g. READ or WRITE) can be performed.

In RF interface command, the LSB of the byte is transmitted first.

9.3.1.1 Command Set

All available commands for FM24NC512Tx are shown in Table 32.

Table 32 FM24NC512Tx RF Command Set

Command category	Command	ISO/IEC 14443	NFC Forum	Command Code (hexadecimal)
Anticollision	Request	REQA	SENS_REQ	26h (7 bit)
	Wake-up	WUPA	ALL_REQ	52h (7 bit)
	Anticollision CL1	Anticollision CL1	SDD_REQ CL1	93h 20h
	Select CL1	Select CL1	SEL_REQ CL1	93h 70h
	Anticollision CL2	Anticollision CL2	SDD_REQ CL2	95h 20h
	Select CL2	Select CL2	SEL_REQ CL2	95h 70h
	Halt	HLTA	SLP_REQ	50h 00h
Tag	READ	-	READ	30h
	FAST_READ	-	-	3Ah

Command category	Command	ISO/IEC 14443	NFC Forum	Command Code (hexadecimal)
	WRITE	-	WRITE	A2h
	COMP_WRITE	-	-	A0h
	PWD_AUTH	-	-	1Bh
	READ_SIG	-	-	3Ch
Data memory	READ	-	-	03h
	WRITE	-	-	02h
Data memory Lock	READ_RF_DATA_RD_LOCK	-	-	65h
	READ_RF_DATA_WR_LOCK	-	-	63h
	WRITE_RF_DATA_RD_LOCK	-	-	66h
	WRITE_RF_DATA_WR_LOCK	-	-	64h
	RF_PWD_AUTH	-	-	61h

9.3.1.2 Timing

The command and response timings shown in this document are not to scale and values are rounded to 1µs.

All given command and response times refer to the data frames including start of communication and end of communication. They do not include the encoding (like the Miller pulses). A NFC device data frame contains the start of communication (1 “start bit”) and the end of communication (one logic 0 + 1 bit length of unmodulated carrier). A NFC tag data frame contains the start of communication (1 “start bit”) and the end of communication (1 bit length of no subcarrier).

The minimum command response time is specified as an integer n which specifies the NFC device to NFC tag frame delay time. The frame delay time from NFC tag to NFC device is at least 87µs. The maximum command response time is specified as a time-out value. Depending on the command, the TACK value specified for command responses defines the NFC device to NFC tag frame delay time. It does it for either the 4-bit ACK value specified in Section 9.3.1.3 or for a data frame.

All timing can be measured according to ISO/IEC 14443-3 frame specification as shown for the Frame Delay Time in Figure 19.

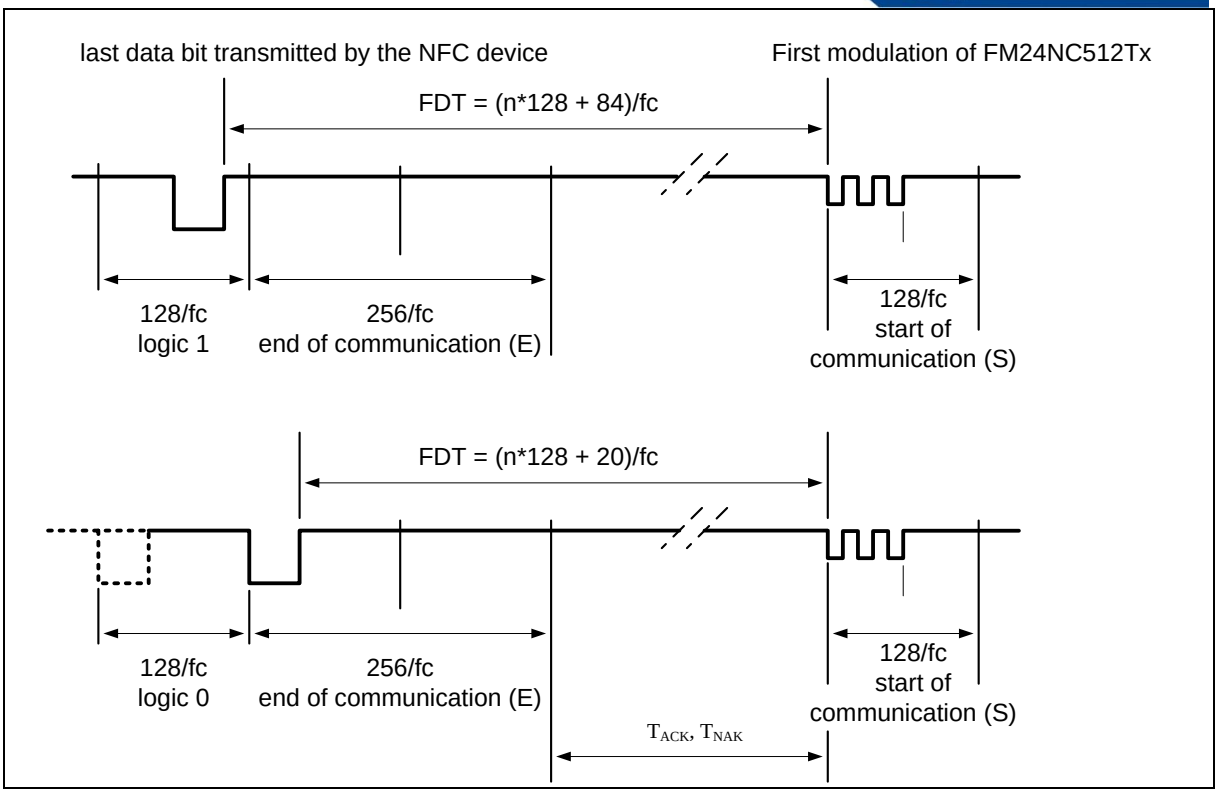


Figure 19 Frame Delay Time (from NFC device to FM24NC512Tx), T_{ACK} and T_{NAK}

Remark: Due to the coding of commands, the measured timings usually excludes (a part of) the end of communication. Considered this factor when comparing the specified with the measured times.

9.3.1.3 ACK and NAK

When TAG memory is accessed, the device uses a 4 bit ACK / NAK as shown in Table 33.

Table 33 ACK and NAK values for TAG memory

Code (4-bit)	ACK/NAK
Ah	Acknowledge (ACK)
0h	NAK for invalid argument (i.e. invalid block address)
1h	NAK for parity or CRC error
5h	NAK for EEPROM write error

When DATA memory is accessed, the device uses a 1 byte ACK and 2 bytes NAK as shown in Table 34.

Table 34 ACK and NAK values for DATA memory

Code	ACK/NAK
0Ah	Acknowledge (ACK)
B2B2h	NAK

9.3.1.4 ATQA and SAK responses

FM24NC512Tx replies to a REQA or WUPA command with the ATQA. It replies to a Select CL2 command with the SAK. The 2-byte ATQA value is transmitted with the least significant byte first (44h).

Table 35 ATQA response of the FM24NC512Tx

Field	Value	Bit number															
		16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ATQA	00 44h	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0

Table 36 SAK response of the FM24NC512Tx

Field	Value	Bit number							
		8	7	6	5	4	3	2	1
SAK1	04h	0	0	0	0	0	1	0	0
SAK2	00h	0	0	0	0	0	0	0	0

Remark: The ATQA coding in bits 7 and 8 indicate the UID size according to ISO/IEC 14443 independent from the settings of the UID usage.

Remark: The bit numbering in the ISO/IEC 14443 starts with LSB = bit 1 and not with LSB = bit 0. So 1 byte counts bit 1 to bit 8 instead of bit 0 to 7.

9.3.2 Tag Memory command

9.3.2.1 READ(30h)

The READ command requires a start block address, and returns the 16 bytes of four blocks. For example, if address (Addr) is 03h then blocks 03h, 04h, 05h, 06h are returned. Special conditions apply if the READ command address is near the end of the accessible memory area. The special conditions also apply if at least part of the addressed blocks is within a password protected area. For details on those cases and the command structure refers to Figure 20 and Table 37.

Table 38 shows the required timing.

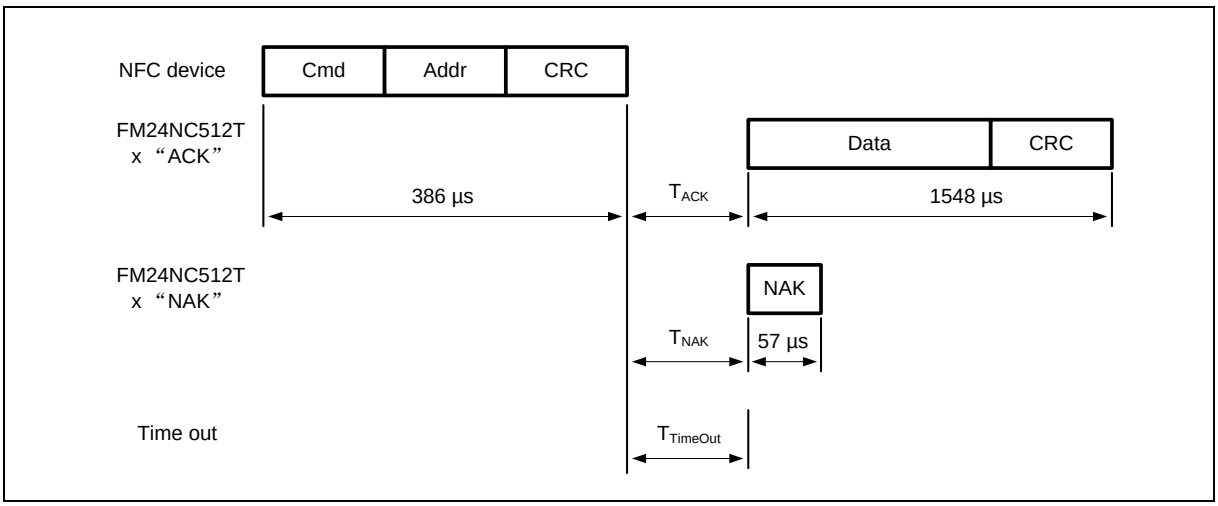


Figure 20 READ command

Table 37 READ command

Name	Code	Description	Length
Cmd	30h	read out blocks	1 byte
Addr	-	Start block address	1 byte
CRC	-	CRC	2 bytes
Data	-	Data content of the addressed blocks	16 bytes
NAK	see Table 33	see Section 9.3.1.3	4-bit

Table 38 READ timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
READ	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

In the initial state of FM24NC512Tx, all memory blocks are allowed as Addr parameter to the READ command.
- block address 00h to 2Ch for FM24NC512T1
- block address 00h to 86h for FM24NC512T2
- block address 00h to E6h for FM24NC512T3

Addressing a memory block beyond the limits above results in a NAK response from FM24NC512Tx.

A roll-over mechanism is implemented to continue reading from page 00h once the end of the accessible memory is reached. Reading from block address 2Ah on FM24NC512Tx results in blocks 2Ah, 2Bh, 2Ch and 00h being returned.

The following conditions apply if part of the memory is password protected for read access:
- if FM24NC512Tx is in the ACTIVE state
  - addressing a block which is equal or higher than AUTH0 results in a NAK response
  - addressing a block lower than AUTH0 results in data being returned with the roll-over mechanism occurring just before the AUTH0 defined block

- if FM24NC512Tx is in the AUTHENTICATED state
  - the READ command behaves like on a FM24NC512Tx without access protection

Remark: PWD and PACK values can never be read out of the memory. When reading from the blocks holding those two values, all 00h bytes are replied to the NFC device instead.

9.3.2.2 FAST READ(3Ah)

The FAST_READ command requires a start block address and an end block address and returns the all n*4 bytes of the addressed blocks. For example if the start address is 03h and the end address is 07h then blocks 03h, 04h, 05h, 06h and 07h are returned. If the addressed block is outside of accessible area, FM24NC512Tx replies a NAK. For details on those cases and the command structure, refer to Figure 21 and Table 39.

Table 40 shows the required timing.

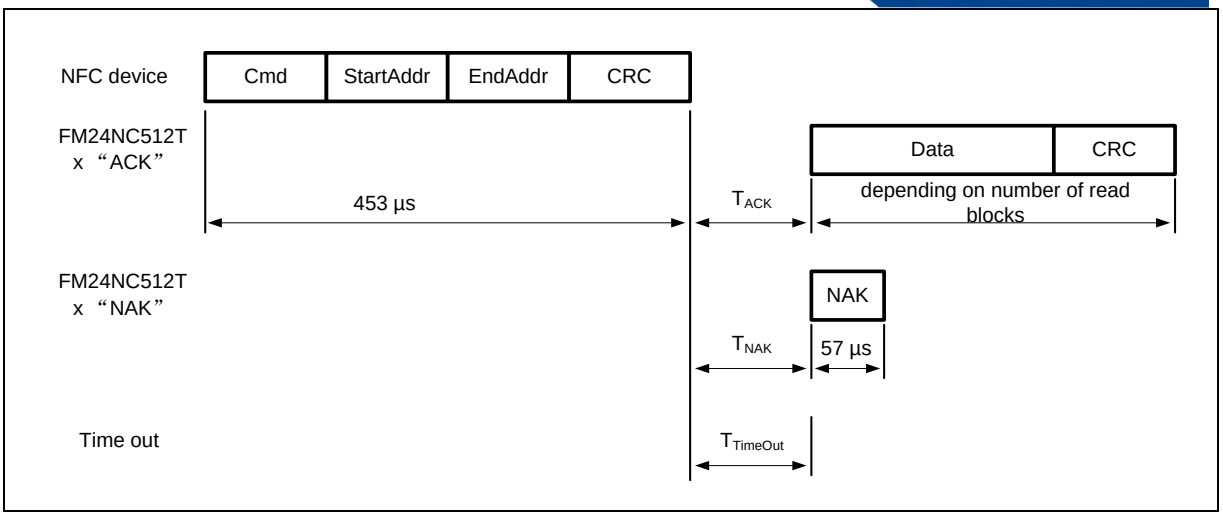


Figure 21 FAST_READ command

Table 39 FAST_READ command

Name	Code	Description	Length
Cmd	3Ah	read out multiple blocks	1 byte
StartAddr	-	start block address	1 byte
EndAddr	-	end block address	1 byte
CRC	-	CRC	2 bytes
Data	-	Data content of the addressed blocks	N*4 bytes
NAK	see Table 33	see Section 9.3.1.3	4-bit

Table 40 FAST_READ timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
FAST_READ	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

In the initial state of FM24NC512Tx, all memory blocks are allowed as StartAddr parameter to the FAST_READ command.
- block address 00h to 2Ch for FM24NC512T1
- block address 00h to 86h for FM24NC512T2
- block address 00h to E6h for FM24NC512T3

Addressing a memory block beyond the limits above results in a NAK response from FM24NC512Tx.

The EndAddr parameter must be equal to or higher than the StartAddr.

The following conditions apply if part of the memory is password protected for read access:
- if FM24NC512Tx is in the ACTIVE state
  – if any requested page address is equal or higher than AUTH0 a NAK is replied
- if FM24NC512Tx is in the AUTHENTICATED state
  – the FAST_READ command behaves like on a FM24NC512Tx without access protection

Remark: PWD and PACK values can never be read out of the memory. When reading from the blocks holding those two values, all 00h bytes are replied to the NFC device instead.

Remark: The FAST_READ command is able to read out the whole memory with one command. Nevertheless, receive buffer of the NFC device must be able to handle the requested amount of data as there is no chaining possibility.

9.3.2.3 WRITE(A2)

The WRITE command requires a block address of tag memory, and writes 4 bytes of data into the addressed FM24NC512Tx block. The WRITE command is shown in Figure 22 and Table 41. Table 42 shows the required timing.

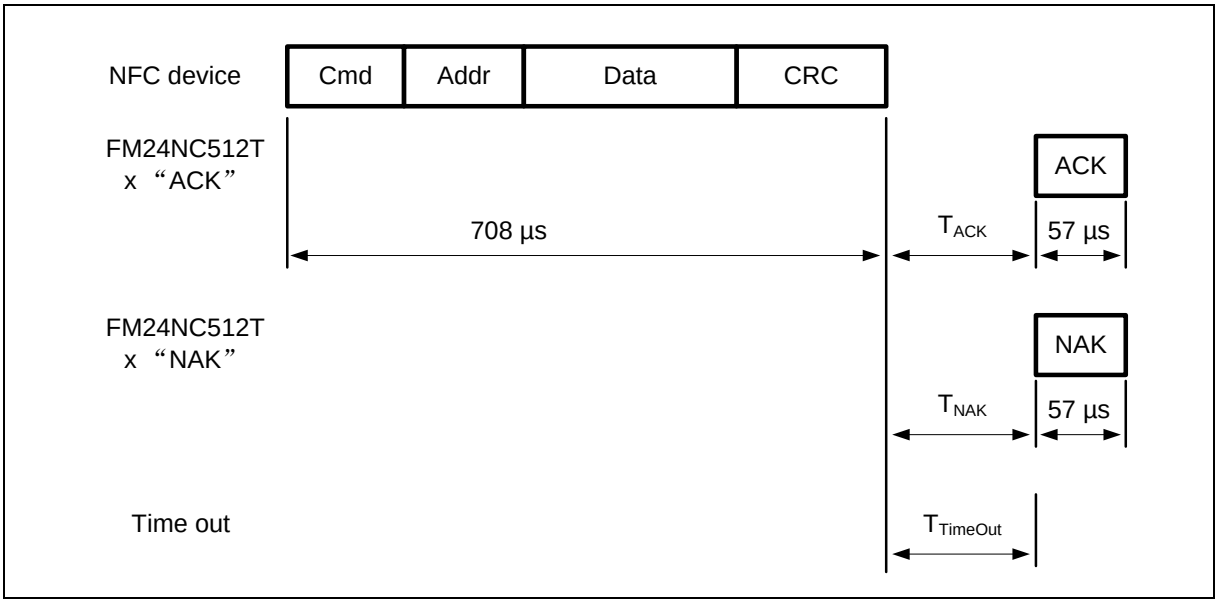


Figure 22 WRITE command

Table 41 WRITE command

Name	Code	Description	Length
Cmd	A2h	write one block	1 byte
Addr	-	block address	1 byte
CRC	-	CRC	2 bytes
Data	-	data	4 bytes
ACK	Ah	Acknowledge (ACK)	4 bit
NAK	see Table 33	see Section 9.3.1.3	4-bit

Table 42 WRITE timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
WRITE	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

In the initial state of FM24NC512Tx, the following memory blocks are valid Addr parameters to the WRITE command.
- block address 00h to 2Ch for FM24NC512T1
- block address 00h to 86h for FM24NC512T2
- block address 00h to E6h for FM24NC512T3
- block address 00h of sector 0 to DFh of sector 1 for FM24NC512T4

Addressing a memory block beyond the limits above results in a NAK response from FM24NC512Tx. Blocks which are locked against writing cannot be reprogrammed using any write command. The locking mechanisms include static and dynamic lock bits as well as the locking of the configuration blocks.

The following conditions apply if part of the memory is password protected for write access:
• if FM24NC512Tx is in the ACTIVE state
– writing to a blocks which address is equal or higher than AUTH0 results in a NAK response
• if FM24NC512Tx is in the AUTHENTICATED state
– the WRITE command behaves like on a FM24NC512Tx without access protection

FM24NC512Tx features tearing protected write operations to specific memory content. The following blocks are protected against tearing events during a WRITE operation:
• block 2 containing static lock bits
• block 3 containing CC bits
•block 28h containing the additional dynamic lock bits for FM24NC512T1
•block 82h containing the additional dynamic lock bits for FM24NC512T2
•block E2h containing the additional dynamic lock bits for FM24NC512T3
•block DBh of sector 1 containing the additional dynamic lock bits for FM24NC512T4

9.3.2.4 COMPATIBILITY WRITE(A0h)

The COMPATIBILITY_WRITE command is implemented to guarantee interoperability with the established MIFARE Classic PCD infrastructure, in case of coexistence of ticketing and NFC applications. Even though 16 bytes are transferred to FM24NC512Tx, only the least significant 4 bytes (bytes 0 to 3) are written to the specified address. Set all the remaining bytes, 04h to 0Fh, to logic 00h. The COMPATIBILITY_WRITE command is shown in Figure 23, Figure 24 and Table 43.

Table 44 shows the required timing.

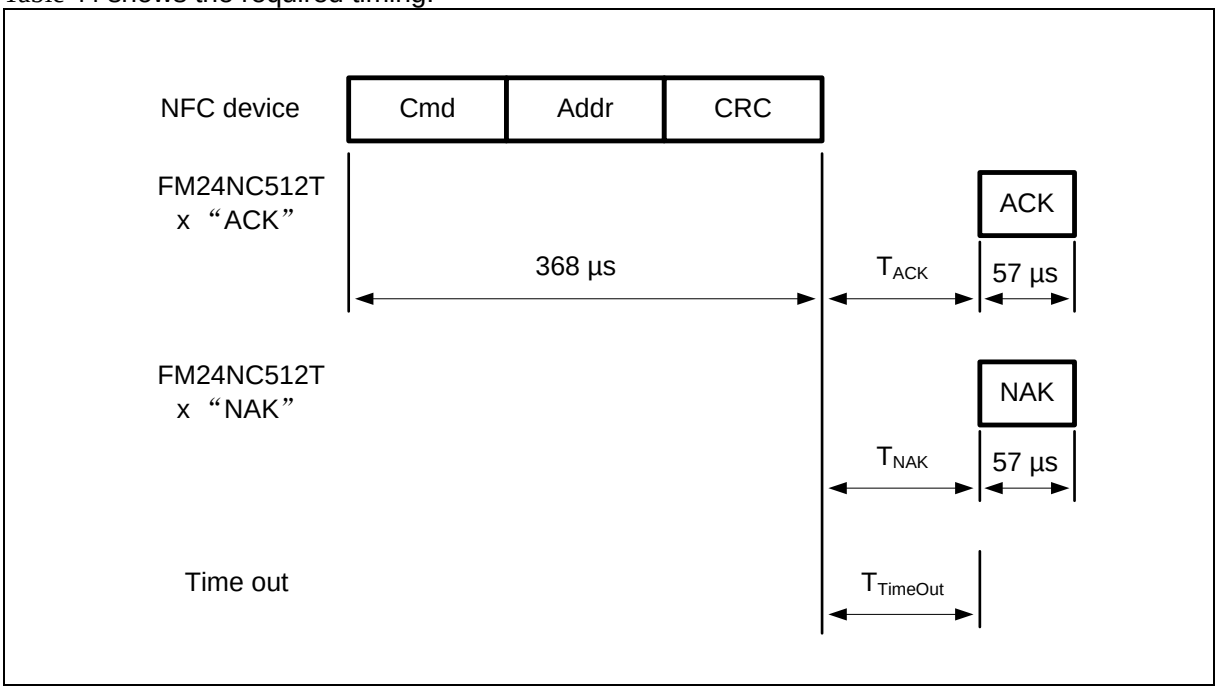


Figure 23 COMPATIBILITY_WRITE command part 1

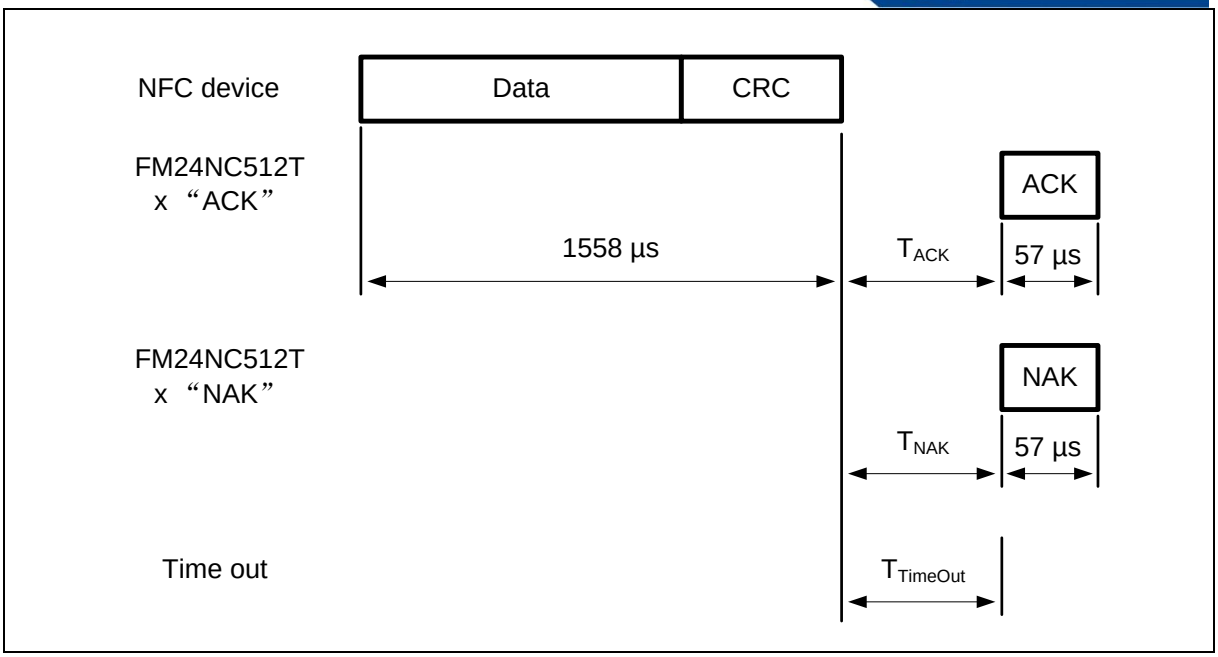


Figure 24 COMPATIBILITY_WRITE command part 2

Table 43 COMPATIBILITY_WRITE command

Name	Code	Description	Length
Cmd	A0h	Compatibility write	1 byte
Addr	-	block address	1 byte
CRC	-	CRC	2 bytes
Data	-	16-byte data, only least significant 4 bytes are written	16 bytes
ACK	Ah	Acknowledge (ACK)	4 bit
NAK	see Table 33	see Section 9.3.1.3	4-bit

Table 44 COMPATIBILITY_WRITE timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
COMPATIBILITY_WRITE part 1	n=9(1)	$T_{TimeOut}$	5ms
COMPATIBILITY_WRITE part 2	n=9(1)	$T_{TimeOut}$	10ms

Note: 1. Refer to Section 9.3.1.2.

In the initial state of FM24NC512Tx, the following memory pages are valid Addr parameters to the COMPATIBILITY_WRITE command.

- block address 00h to 2Ch for FM24NC512T1
- block address 00h to 86h for FM24NC512T2
- block address 00h to E6h for FM24NC512T3
- block address 00h of sector 0 to DFh of sector 1 for FM24NC512T4

Addressing a memory block, that beyond the limits above, results in a NAK response from FM24NC512Tx.

Blocks which are locked against writing cannot be reprogrammed using any write command. The locking mechanisms include static and dynamic lock bits as well as the locking of the configuration pages.

The following conditions apply if part of the memory is password protected for write access:

- If FM24NC512Tx is in the ACTIVE state
  – Writing to a block which address is equal or higher than AUTH0 results in a NAK response
- If FM24NC512Tx is in the AUTHENTICATED state
  – The COMPATIBILITY_WRITE command behaves the same as on a FM24NC512Tx without access protection

FM24NC512Tx features tearing protected write operations to specific memory content. The following pages are protected against tearing events during a COMPATIBILITY_WRITE operation:

- block 02h containing static lock bits
- block 03h containing CC bits
- block 28h containing the additional dynamic lock bits for FM24NC512T1
- block 82h containing the additional dynamic lock bits for FM24NC512T2
- block E2h containing the additional dynamic lock bits for FM24NC512T3
- block DBh of sector 1 containing the additional dynamic lock bits for FM24NC512T4

9.3.2.5 PWD AUTH(1Bh)

A protected tag memory area can be accessed only after a successful password verification using the PWD_AUTH command. The AUTH0 configuration byte defines the protected area. It specifies the first block that the password mechanism protects. The level of protection can be configured using the PROT bit either for write protection or read/write protection. The PWD_AUTH command takes the password as parameter and, if successful, returns the password authentication acknowledge, PACK. By setting the AUTHLIM configuration bits to a value larger than 000b, the number of unsuccessful password verifications can be limited. Each unsuccessful authentication is then counted in a counter featuring anti-tearing support. After reaching the limit of unsuccessful attempts, the memory access specified in PROT, is no longer possible. The PWD_AUTH command is shown in Figure 25 and Table 45.

Table 46 shows the required timing.

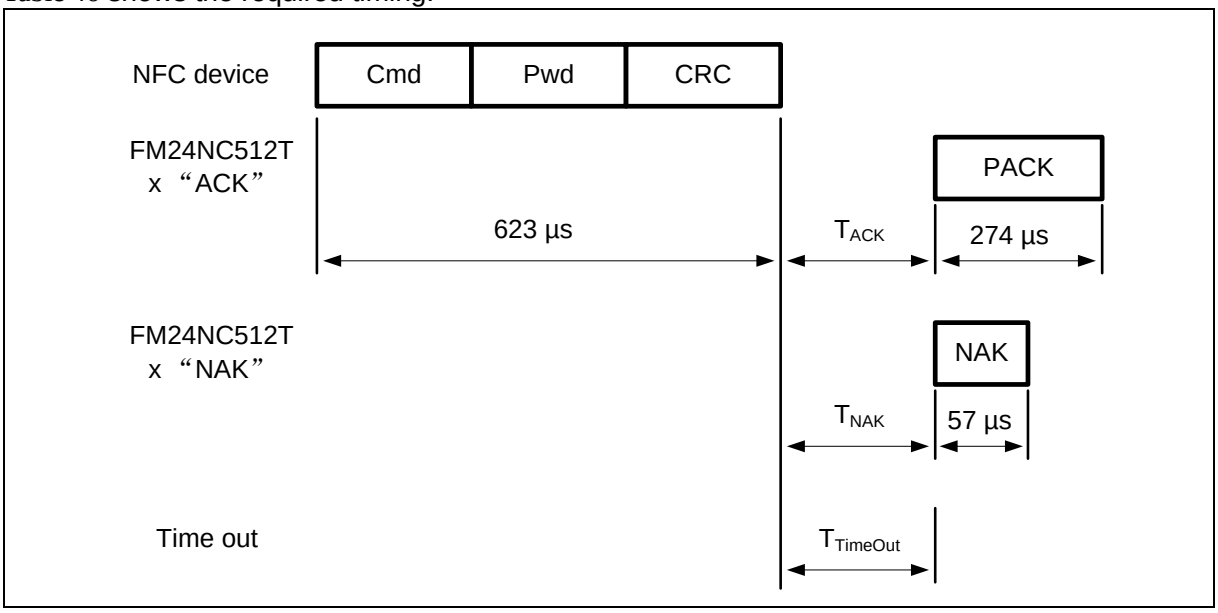


Figure 25 PWD_AUTH command

Table 45 PWD_AUTH command

Name	Code	Description	Length
Cmd	1Bh	Password authentication	1 byte
Pwd	-	password	4 byte

Name	Code	Description	Length
CRC	-	CRC	2 bytes
PACK	-	Password authentication acknowledge	2 bytes
NAK	see Table 33	see Section 9.3.1.3	4-bit

Table 46 PWD_AUTH timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
PWD_AUTH	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

Remark: It is strongly recommended to change the password from its delivery state at tag issuing and set the AUTH0 value to the PWD block.

9.3.3 Data Memory Command

9.3.3.1 READ (03h)

The READ command consists of PCB, INS (03h), P1P2, Le byte and two CRC bytes. The first two bytes are preamble and command code that start the frame. The following two bytes P1 & P2 identify the starting address of the read operation while Le byte configures the number of data bytes to be read out. For example, if the starting address is 0100h and Le byte is 0Fh, 15 bytes data from 0100h are returned.

If the accessed memory is protected by RF_DATA_RD_LOCK, the response is NAK. The command structure is shown in Figure 26 and Table 47.

Table 48 shows the required timing.

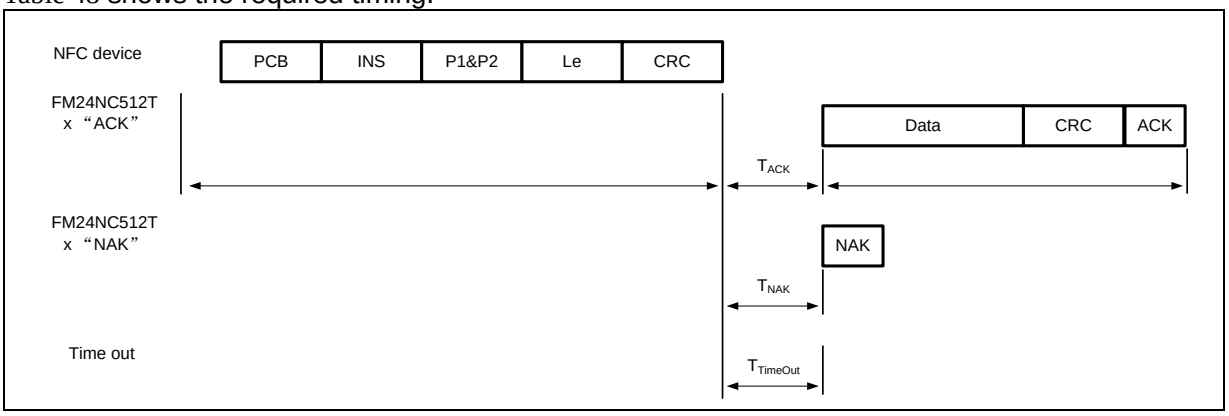


Figure 26 READ command

Table 47 READ command

Name	*Code*	*Description*	*Length*
PCB			1 byte
INS	03h	Read command	1 byte
P1 P2	-	Byte address	2 bytes
Le	-	Data length(1)	1 byte
CRC	-	CRC	2 bytes
Data	-	Data output	1~256 bytes
ACK	0Ah		1 byte

Name	Code	Description	Length
NAK	B2B2h		2 byte

Note: 1. The number of data byte to be read is Le+1.

Table 48 READ timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
READ	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

9.3.3.2 WRITE (02h)

The WRITE command consists of PCB, INS (02h), P1P2, Lc byte, data bytes and two CRC bytes. The first two bytes are a preamble and command code that start the frame. The following two bytes P1 & P2 identify the starting address of the write operation while Lc byte configures the number of data bytes to be written in. When data is transferred in, the data word address lower seven bits are internally incremented following the receipt of each data word. The higher data word address bits are not incremented, retaining the memory page row location. When the word address, internally generated, reaches the page boundary, the following byte is placed at the beginning of the same page. If more than 128 data words are transmitted to the EEPROM, the data word address will “roll over” and previous data will be overwritten. That is, only the last 128 bytes are effective.

If the data memory is protected by RF_DATA_WR_LOCK, the response is NAK. The command structure is shown in Figure 27 and Table 49.

Table 50 shows the required timing.

Figure 27 WRITE command

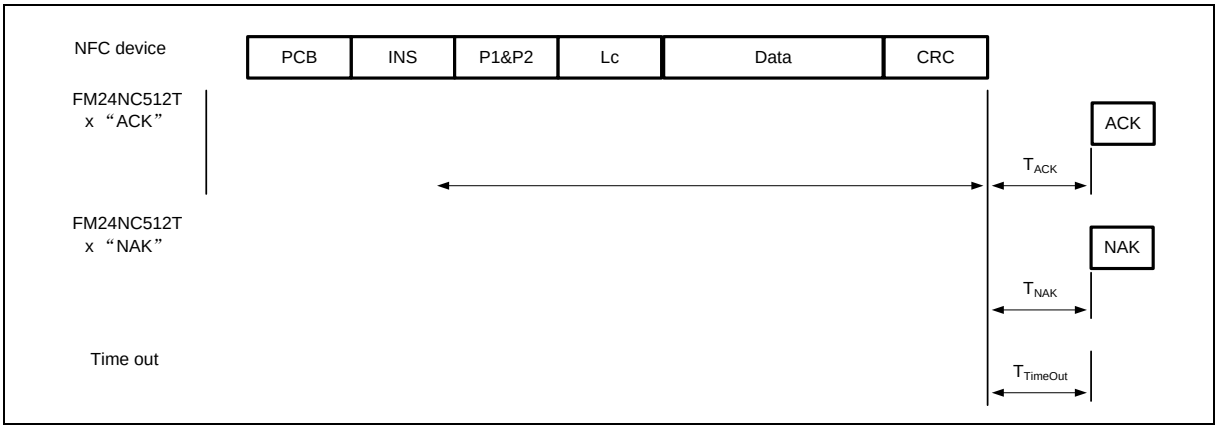


Table 49 WRITE command

Name	Code	Description	Length
PCB			1 byte
INS	02h	Write command	1 byte
P1 P2	-	Byte address	2 bytes
Lc	-	Data length(1)	1 byte
Data	-	Data input	1~256 bytes（only last 128 bytes effective if Lc > 7Fh）

Name	Code	Description	Length
CRC	-	CRC	2 bytes
ACK	A2h		1 byte
NAK	B2B2h		2 byte

Note: 1. The number of data byte to be written is Lc+1.

Table 50 WRITE timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
WRITE	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

9.3.4 Data Memory Lock Command

9.3.4.1 READ_RF_DATA_RD_LOCK (65h)

The READ_RF_DATA_RD_LOCK command is used to read the byte of RF_DATA_RD_ LOCK. 32 bytes of data would be transferred but only bit 7 of the first byte makes sense, all the following bits are 00h. The command structure is shown in Figure 28 and Table 51.

Table 52 shows the required timing.

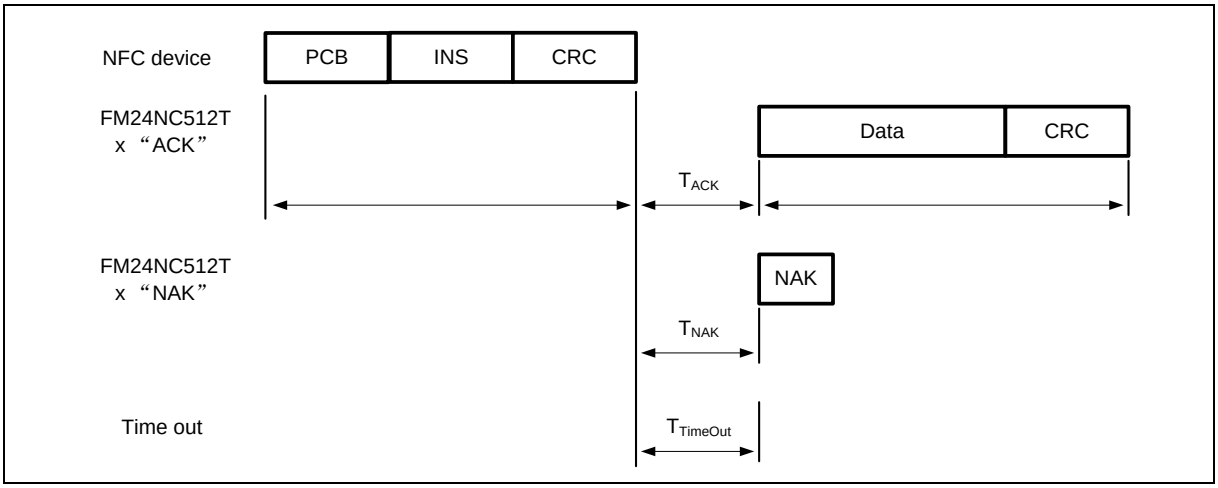


Figure 28 READ_RF_DATA_RD_LOCK command

Table 51 READ_RF_DATA_RD_LOCK command

Name	Code	Description	Length
PCB			1 byte
Cmd	65h	Read RF_DATA_RD_LOCK data	1 byte
CRC	-	CRC	2 bytes
Data	-	data	32 bytes, only bit7 of the first byte makes sense
NAK	B2B2h		2 byte

Table 52 READ_RF_DATA_RD_LOCK timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
READ_RF_DATA_RD_LOCK	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

9.3.4.2 READ_RF_DATA_WR_LOCK (63h)

The READ_RF_DATA_WR_LOCK command is used to read byte of RF_DATA_WR_LOCK. 32 bytes of data would be transferred but only the bit7 of first byte makes sense, all the following bits are 00h. The command structure is shown in Figure 29 and Table 53.

Table 54 shows the required timing.

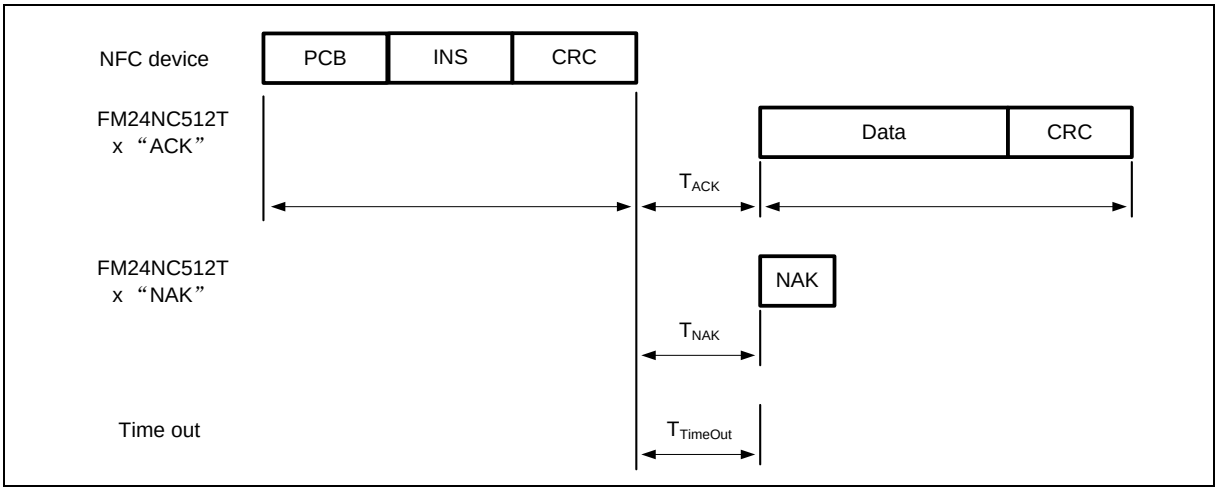


Figure 29 READ_RF_DATA_WR_LOCK command

Table 53 READ_RF_DATA_WR_LOCK command

Name	Code	Description	Length
PCB			1 byte
Cmd	63h	Read RF_DATA_WR_LOCK data	1 byte
CRC	-	CRC	2 bytes
Data	-	data	32 bytes, only bit7 of the first byte makes sense
NAK	B2B2h		2 byte

Table 54 READ_RF_DATA_WR_LOCK timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
READ_RF_DATA_WR_LOCK	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

9.3.4.3 WRITE_RF_DATA_RD_LOCK (66h)

The WRITE_RF_DATA_RD_LOCK command writes 32 bytes of data into the RF_DATA_RD_LOCK in Data lock. Only bit 7 of the first byte makes sense, the following bits can be any value. This command is executed in DM AUTHENTICATED state. If the RF_DATA_PWD is not authenticated, the response of this command is NAK. The WRITE_RF_DATA_RD_LOCK command is bit-wise OR'ed. It can change lock bit to logic 1, but cannot change back to logic 0.The WRITE_RF_DATA_RD_LOCK command is shown in Figure 30 and Table 55.

Table 56 shows the required timing.

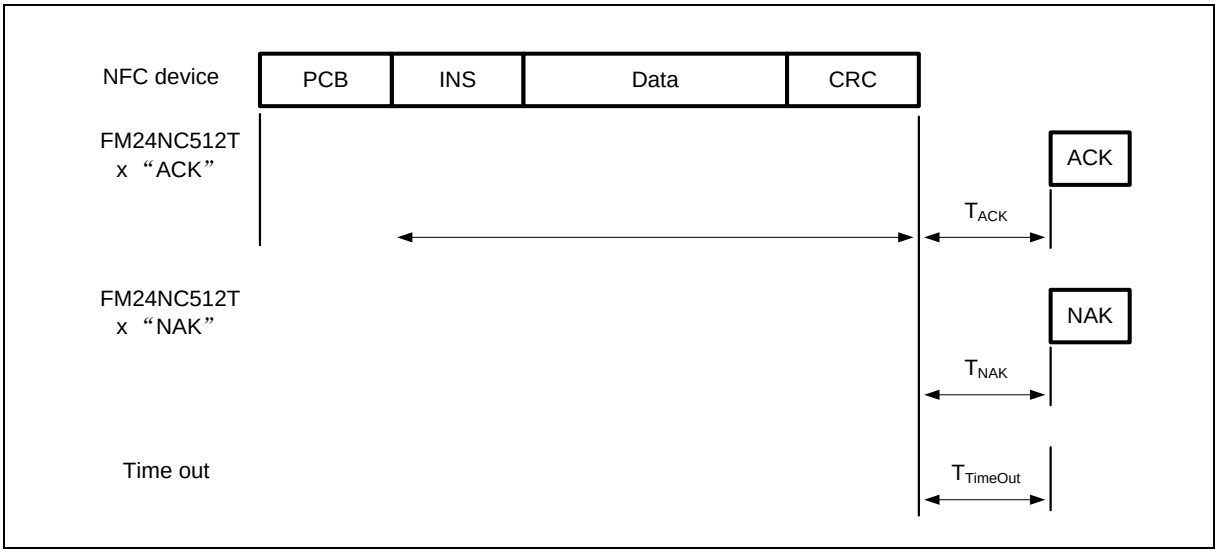


Figure 30 WRITE_RF_DATA_RD_LOCK command

Table 55 WRITE_RF_DATA_RD_LOCK command

Name	Code	Description	Length
PCB			1 byte
Cmd	66h	write RF_DATA_RD_LOCK data	1 byte
Data	-	data	32 bytes, only bit 7 of the first byte makes sense
CRC	-	CRC	2 bytes
ACK	A2h		1 byte
NAK	B2B2h		2 byte

Table 56 WRITE_RF_DATA_RD_LOCK timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
WRITE_RF_DATA_RD_LOCK	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

9.3.4.4 WRITE_RF_DATA_WR_LOCK (64h)

The WRITE_RF_DATA_WR_LOCK command writes 32 bytes of data into the RF_DATA_WR_LOCK in Data lock. Only bit 7 of the first byte makes sense, the following bits can be any value. This command is executed in DM AUTHENTICATED state. If the RF_DATA_PWD is not authenticated, the response of this command is NAK. This command is bit-wise OR'ed. It

can change lock bit to logic 1, but cannot change back to logic 0. The WRITE_RF_DATA_WR_LOCK command is shown in Figure 31 and Table 57.Figure 31 WRITE_RF_DATA_WR_LOCK command

.

Table 58 shows the required timing.

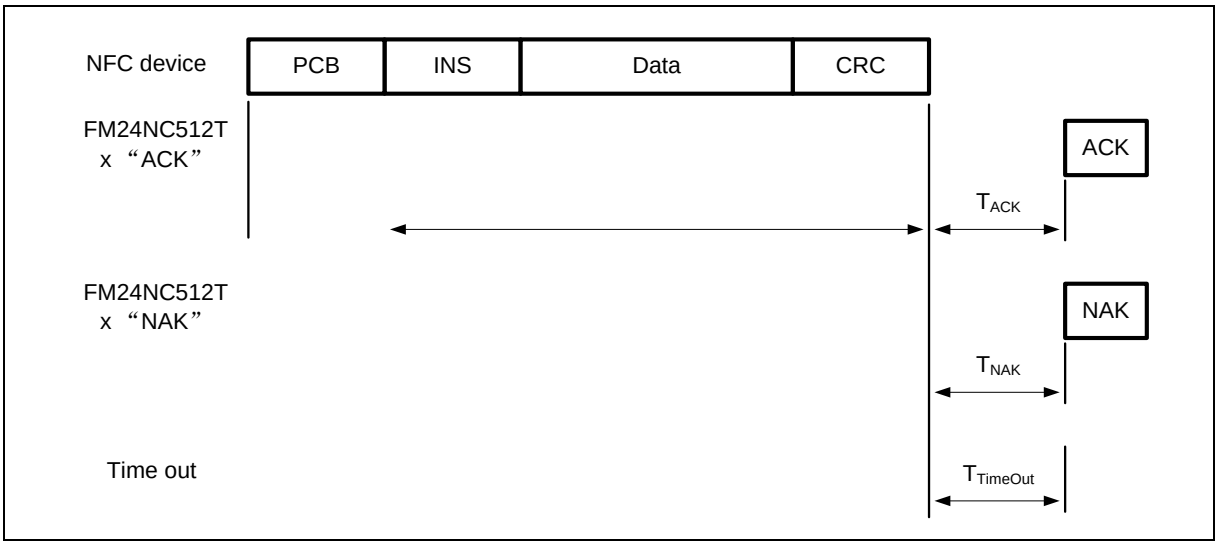


Figure 31 WRITE_RF_DATA_WR_LOCK command

Table 57 WRITE_RF_DATA_WR_LOCK command

Name	Code	Description	Length
PCB			1 byte
Cmd	64h	write RF_DATA_WR_LOCK data	1 byte
Data	-	data	32 bytes, only bit 7 of the first byte makes sense
CRC	-	CRC	2 bytes
ACK	A2h		1 byte
NAK	B2B2h		2 byte

Table 58 WRITE_RF_DATA_WR_LOCK timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
WRITE_RF_DATA_WR_LOCK	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

9.3.4.5 RF_PWD_AUTH (61h)

RF_DATA_RD_LOCK & RF_DATA_WR_LOCK in Data lock can be changed only after a successful password verification using the RF_PWD_AUTH command. The RF_PWD_AUTH command takes the password as parameter and, if successful, returns ACK. The RF_PWD_AUTH command is shown in Figure 32 and Table 59.

Table 60 shows the required timing.

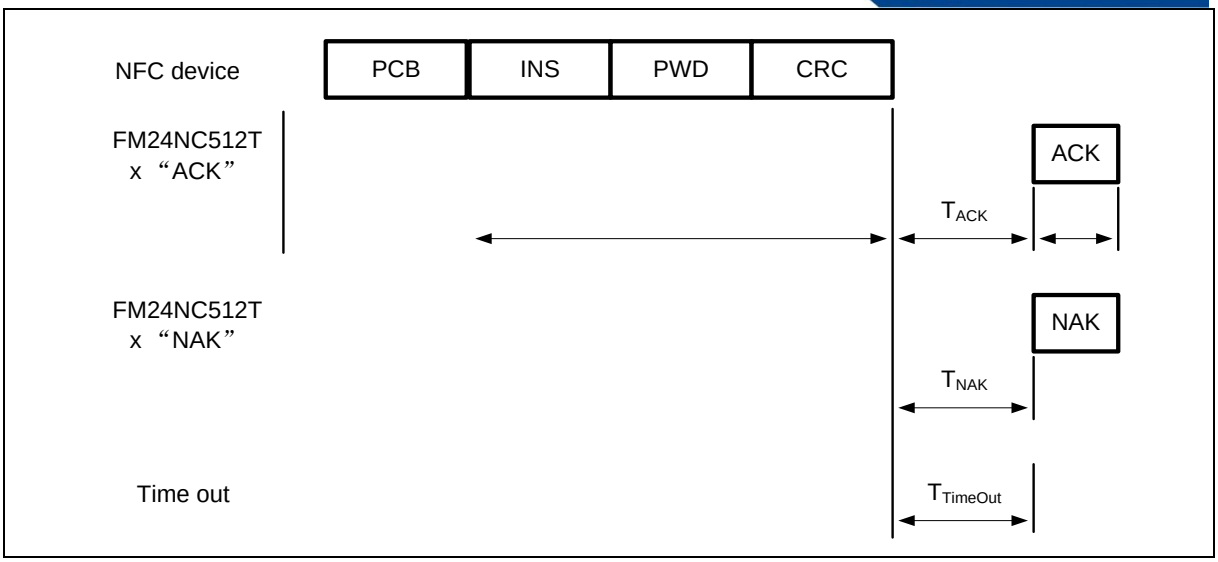


Figure 32 RF_PWD_AUTH command

Table 59 RF_PWD_AUTH command

Name	Code	Description	Length
PCB			1 byte
Cmd	61h	RF password authentication	1 byte
PWD	-	RF_DATA_PWD	4 bytes
CRC	-	CRC	2 bytes
ACK	A2h		1 byte
NAK	B2B2h		2 byte

Table 60 RF_PWD_AUTH timing

These times exclude the end of communication of the NFC device.

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
RF_PWD_AUTH	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

10 Dual-interface Arbitrating

FM24NC512Tx can be accessed by two wire serial (contact) interface or RF interface. There are four parts of memory in the device, which are data memory, data lock, tag memory and tag lock & system. In some condition, simultaneous access from two interfaces is allowed.

- Data memory and one of the rest three parts can be simultaneously accessed by two interfaces respectively.
- Data lock and one of tag memory or tag lock & system can be simultaneously accessed by two interfaces respectively except for both write operation.

In other conditions, collision happens when two interfaces access the device at same time, and a 'First come, first serve' strategy is performed.

EH_FD and GPO pin help the master of two wire serial interface understand RF interface operation in order to select the right time to send command.

11 Electrical Characteristics

11.1 Absolute Maximum Ratings

Table 61 Absolute maximum ratings

Symbol	Parameter	Min	Max	Unit
Top	Operating temperature	-55	125	°C
T_{STG}	Storage temperature	-65	150	°C
V_{IO}	Contact input or output range	-1.0	7.0	V
V_{CC}	Contact supply voltage	-1.0	7.0	V
V_{IN_1}	RF input voltage amplitude peak to peak between IN1 and IN2, VSS pin left floating		15	V
V_{IN_2}	AC voltage between IN1 and VSS, or IN2 and VSS	-1	15	V
I_{IN}	RF supply current IN1 – IN2		40	mA
V_{OP}	Maximum operating voltage		6.25	V
Io	DC output current on pin SDA or GPO		5.0	mA

Remark: Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification are not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

11.2 Contact interface

11.2.1 Pin Capacitance

Table 62 Input capacitance of contact pin

Symbol	Parameter	Condition	Min	Max	Unit
$C_{IN}^{(1)}$	Input capacitance (input pin)	V_{IN} = 0V, f = 1MHz		6	pF
	Input capacitance (I/O pin)	$V_{I/O}$ = 0V, f = 1MHz		8	pF

Note: 1. This parameter is characterized and is not 100% tested.

11.2.2 DC Characteristics

Table 63 Operating conditions of contact interface

Symbol	Parameter	Min	Max	Unit
V_{CC}	Supply Voltage	1.6	5.5	V
T_A	Ambient operating temperature	-40	85	℃

Table 64 DC characteristics of contact interface

Applicable over recommended operating range from: T_A = -40℃ to +85℃, V_{CC} = +1.7V to +5.5V, (unless otherwise noted).

Symbol	Parameter	Condition	Min	Typ	Max	Unit
I_{CC1}	Supply Current	V_{CC} = 5.5V, Read at 1MHz			1.0	mA
I_{CC2}	Supply Current	V_{CC} = 5.5V, Write at 1MHz			3.0	mA
I_{SB1}	Standby Current	V_{CC} = 1.7V, V_{IN} = V_{CC}/ V_{SS}			1.0	μA

Symbol	Parameter	Condition	Min	Typ	Max	Unit
I_{SB2}	Standby Current	V_{CC} = 5.5V, V_{IN} = V_{CC}/ V_{SS}			6.0	µA
I_{LI}	Input Leakage Current	V_{IN} = V_{CC}/V_{SS}		0.10	3.0	µA
I_{LO}	Output Leakage Current	V_{OUT} = V_{CC}/V_{SS}		0.05	3.0	µA
V_{IL}(1)	Input Low Level		-0.6		V_{CC} x 0.3	V
V_{IH}(1)	Input High Level		V_{CC} x 0.7		V_{CC} + 0.5	V
V_{OL2}	Output Low Level 2	V_{CC} = 3.0V, I_{OL} = 2.1 mA			0.4	V
V_{OL1}	Output Low Level 1	V_{CC} =1.7V, I_{OL} = 0.15 mA			0.2	V

Note: 1. V_{IL} min and V_{IH} max are reference only and are not tested.

11.2.3 AC Characteristics

Table 65 AC measurement conditions of contact interface

Symbol	Parameter	Min	Max	Unit
C_L	Load capacitance	100		pF
R_L	Load resistor connected to V_{CC}	1.3		kΩ
t_R, t_F	Input rise and fall times		50	ns
V_{IN}	Input levels	0.2V_{CC} to 0.8V_{CC}		V
$V_{REF(t)}$	Input and output timing reference levels	0.5V_{CC}		V

Table 66 AC characteristics of contact interface

Applicable over recommended operating range from: T_A = -40℃ to +85℃, V_{CC} = +1.7V to +5.5V, CL = 100 pF (unless otherwise noted).

Symbol	Parameter	1.6-volt		2.5-volt		5.5-volt		Unit
		Min	Max	Min	Max	Min	Max	
f_{SCL}	Clock Frequency, SCL		400		1000		1000	kHz
t_{LOW}	Clock Pulse Width Low	1.3	20000(2)	0.4	20000(2)	0.4	20000(2)	µs
t_{HIGH}	Clock Pulse Width High	0.6	20000(2)	0.4	20000(2)	0.4	20000(2)	µs
t_{START_OUT}	Contact interface timeout on start condition	40		40		40		ms
t_I(1)	Noise Suppression Time		100		50		50	ns
t_{AA}	Clock Low to Data Out Valid	0.02	0.9	0.02	0.55	0.02	0.55	µs
t_{BUF}(1)	Time the bus must be free before a new transmission can start	1.3		0.5		0.5		µs
$t_{HD.STA}$	Start Hold Time	0.6		0.25		0.25		µs
$t_{SU.STA}$	Start Setup Time	0.6		0.25		0.25		µs
$t_{HD.DAT}$	Data In Hold Time	0		0		0		µs
$t_{SU.DAT}$	Data In Setup Time	100		100		100		ns
t_R(1)	Inputs Rise Time		0.3		0.3		0.3	µs
t_F(1)	Inputs Fall Time		300		100		100	ns
$t_{SU.STO}$	Stop Setup Time	0.6		0.25		0.25		µs
t_{DH}	Data Out Hold Time	20		20		20		ns

Symbol	Parameter	1.6-volt		2.5-volt		5.5-volt		Unit
		Min	Max	Min	Max	Min	Max	
t_{WR}	Write Cycle Time		5		5		5	ms
Endurance(1)	3.3V, 25°C, Page Mode	1,000,000						Write Cycles

Note: 1. This parameter is characterized and is not 100% tested.

2. Two wire serial interface timeout.

11.3 RF interface

Table 67 characteristics of RF interface

Applicable over recommended operating range from: T_A = -40℃ to +85℃, V_{CC} = +1.7V to +5.5V, (unless otherwise noted).

Symbol	Parameter	Condition	Min	Typ	Max	Unit
f_C	RF carrier frequency		13.553	13.560	13.567	MHz
H_ISO	Operating field according to ISO	T_A= -40℃ to 85℃	1.5		7.5	A/m
Ci	Input capacitance(IN1 to IN2)	(1)			6	pF
V_{FD1}	Field detect output voltage	EH_FD_VOUT=00		1.5		V
V_{FD2}	Field detect output voltage	EH_FD_VOUT=01		1.8		V
V_{FD3}	Field detect output voltage	EH_FD_VOUT=10		2.5		V
V_{FD4}	Field detect output voltage	EH_FD_VOUT=11		3.3		V
V_{EH1}	Energy harvesting output voltage	EH_FD_VOUT=00		1.5		V
V_{EH2}	Energy harvesting output voltage	EH_ FD_VOUT=01		1.8		V
V_{EH3}	Energy harvesting output voltage	EH_ FD_VOUT=10		2.5		V
V_{EH4}	Energy harvesting output voltage	EH_ FD_VOUT=11		3.3		V
I_{EH1}	Energy harvesting output current	EH_ILIM=00		no limit		mA
I_{EH2}	Energy harvesting output current	EH_ILIM=01		2		mA
I_{EH3}	Energy harvesting output current	EH_ILIM=10		1		mA
I_{EH4}	Energy harvesting output current	EH_ILIM=11		0.5		mA

Note: 1. LCR meter, TA = 25°C, fi =13.56MHz, 2V RMS.

12 Ordering Information

FM 24NC 512 TX -PP -C -H

Company Prefix

FM = Fudan Microelectronics Group Co.,ltd

Product Family

24NC = NFC EEPROM

Product Density

512 = 512K-bit

Tag Density

T1 = 144 Bytes
T2 = 504 Bytes
T3 = 888 Bytes
T4 = 1884 Bytes

Package Type (1)

SO = 8-pin SOP
DN = 8-pin TDFN

Product Carrier

U = Tube
T = Tape and Reel

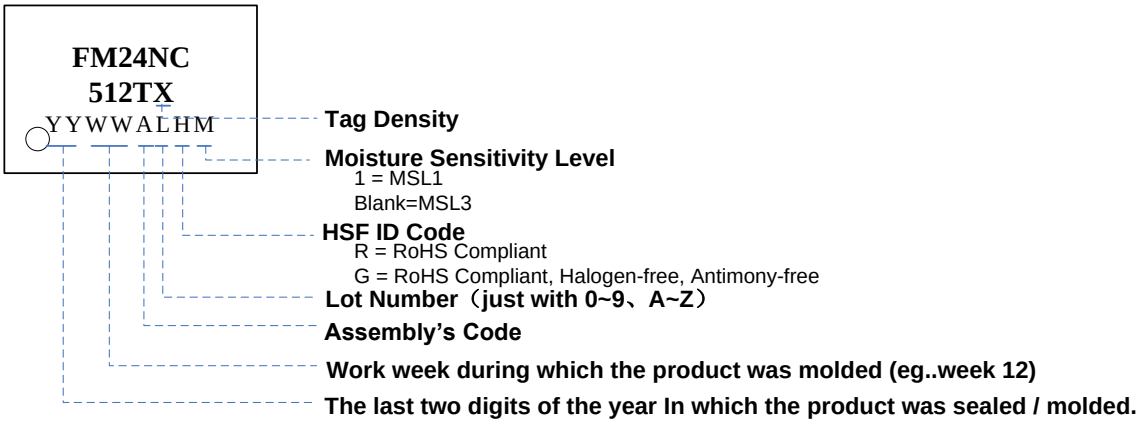
HSF ID Code

G = RoHS Compliant, Halogen-free, Antimony-free

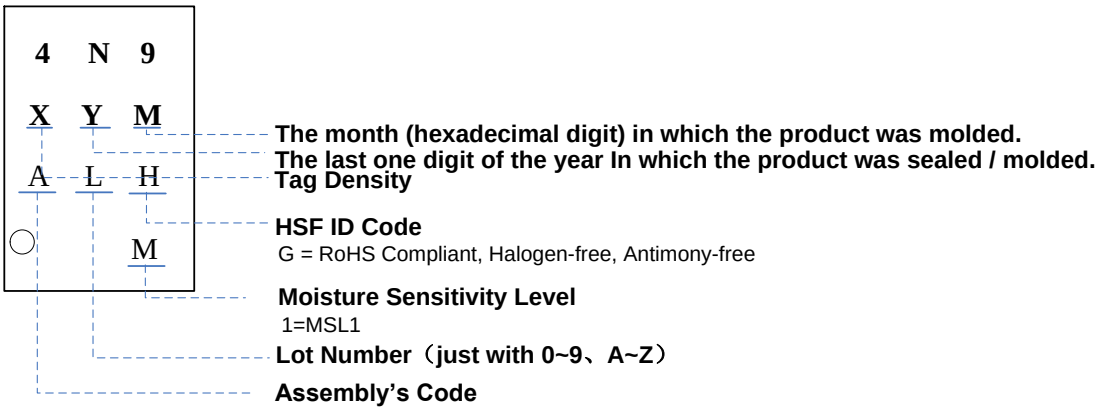
Note:
1. For SO, DN package, MSL1 package are available, for detail please contact local sales office.

13 Part Marking Scheme

13.1 SOP8

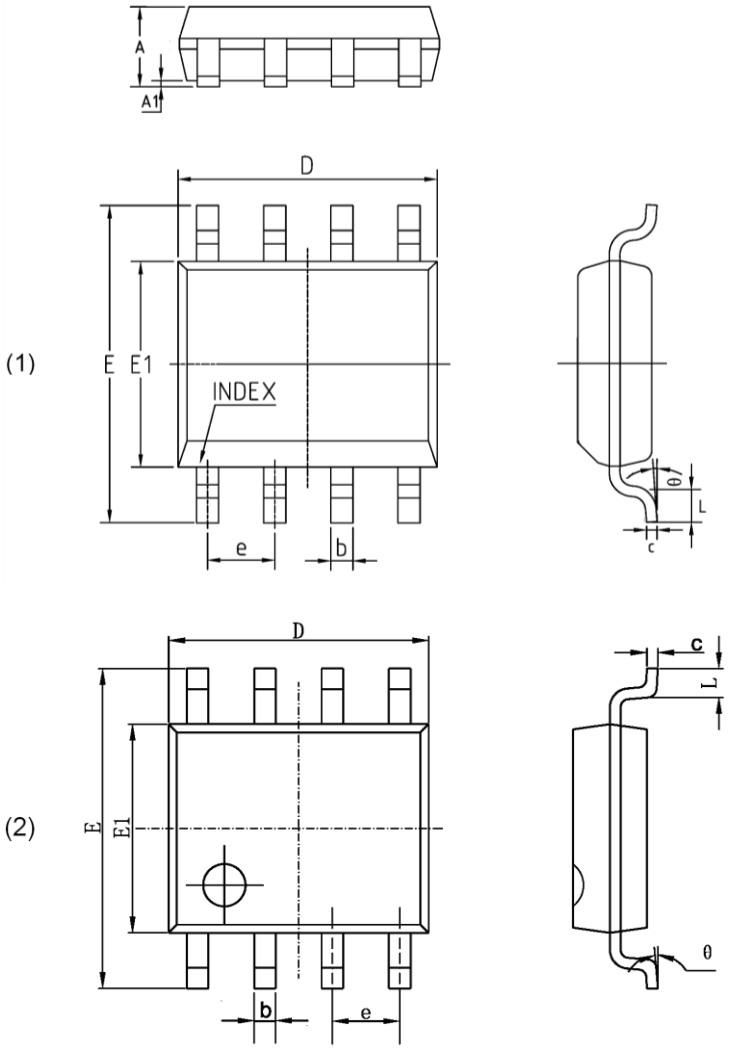


13.2 TDFN8



14 Packaging Information

SOP 8

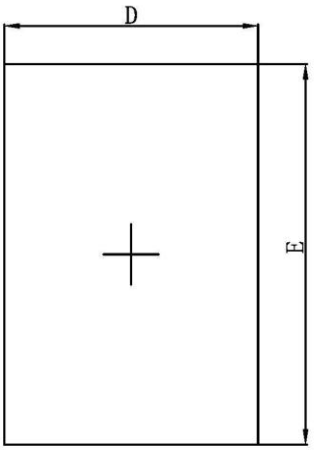


Symbol	MIN	MAX
A	1.350	1.750
A1	0.050	0.250
b	0.330	0.510
c	0.150	0.260
D	4.700	5.150
E1	3.700	4.100
E	5.800	6.200
e	1.270(BSC)	
L	0.400	1.270
θ	0°	8°

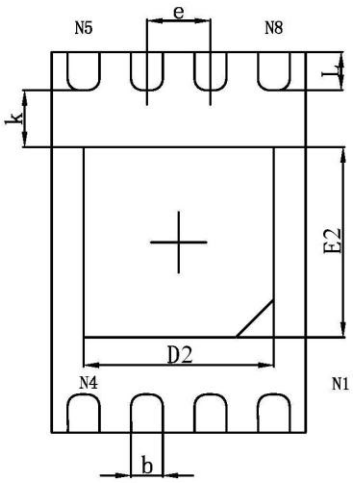
NOTE:

1. Dimensions are in Millimeters.

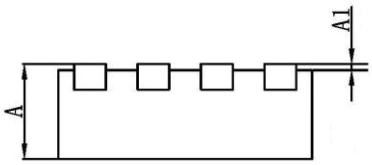
TDFN8



Top View



Bottom View



Side View

Symbol	MIN	MAX
A	0.700	0.800
A1	0.000	0.050
D	1.900	2.100
E	2.900	3.100
D2	1.400	1.600
E2	1.400	1.700
k	0.150(MIN)	
b	0.200	0.300
e	0.500(TYP)	
L	0.200	0.500

NOTE:

1. **Dimensions are in Millimeters.**

15 Revision History

Version	Publication date	Pages	Revise Description
Preliminary	Apr. 2016	74	Initial Document Release.
0.1	Sep. 2016	73	Updated the chapter of 7.3, 9.3.1.3, 9.3.3。
0.2	Feb. 2017	72	Removed TSSOP8 package offering.

Sales and Service

Shanghai Fudan Microelectronics Group Co., Ltd.
Address: Bldg No. 4, 127 Guotai Rd,
Shanghai City China.
Postcode: 200433
Tel: (86-021) 6565 5050
Fax: (86-021) 6565 9115

Shanghai Fudan Microelectronics (HK) Co., Ltd.
Address: Unit 506, 5/F., East Ocean Centre, 98 Granville Road,
Tsimshatsui East, Kowloon, Hong Kong
Tel: (852) 2116 3288 2116 3338
Fax: (852) 2116 0882

Beijing Office
Address: Room 423, Bldg B, Gehua Building,
1 QingLong Hutong, Dongzhimen Alley north Street,
Dongcheng District, Beijing City, China.
Postcode: 100007
Tel: (86-010) 8418 6608
Fax: (86-010) 8418 6211

Shenzhen Office
Address: Room.1301, Century Bldg, No. 4002, Shengtingyuan Hotel,
Huaqiang Rd (North),
Shenzhen City, China.
Postcode: 518028
Tel: (86-0755) 8335 0911 8335 1011 8335 2011 8335 0611
Fax: (86-0755) 8335 9011

Shanghai Fudan Microelectronics (HK) Ltd Taiwan Representative Office
Address: Unit 1225, 12F., No 252, Sec.1 Neihu Rd., Neihu Dist.,
Taipei City 114, Taiwan
Tel : (886-2) 7721 1890 (886-2) 7721 1889
Fax: (886-2) 7722 3888

Shanghai Fudan Microelectronics (HK) Ltd Singapore Representative Office
Address : 237, Alexandra Road, #07-01 The Alexcier, Singapore 159929
Tel : (65) 6472 3688
Fax: (65) 6472 3669

Shanghai Fudan Microelectronics Group Co., Ltd NA Office
Address: 2490 W. Ray Road Suite#2
Chandler, AZ 85224 USA
Tel : (480) 857-6500 ext 18

Web Site: http://www.fmsh.com/