FM24NC32T1/T2/T3
NFC Serial EEPROM

Data Sheet

Jun. 2017

1 Description

FM24NC32Tx is a 32Kbit dual interface EEPROM with flexible tag function. The 32kbit data memory and the dedicated tag memory can be accessed by both two wire serial interface and ISO/IEC 14443A compatible RF interface. When 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

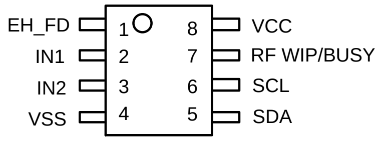
- **Contact Interface**
  - 1.6V~5.5V single power supply
  - Typical standby current <1uA
  - Two wire serial interface
  - 1MHz (2.5V~5.5V) and 400 kHz (1.6V~5.5V) compatibility
  - Byte and Page Write (up to 32 bytes)
  - Random and Sequential read
  - Contact interface timeout
- **RF Interface**
  - 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 ASCII Mirror for automatic serialization NDEF messages
  - Originality signature
  - True anticollision
  - Tag operation: 4 bytes Write, 16 bytes /Fast Read
  - Data Memory operation: 64 bytes Read and 64 bytes Write
  - Support sleep mode
- **Memory**
  - Data Memory: 4K bytes organized in 128 pages of 32 bytes each
  - Security Memory: 256 bytes in 8 pages of 32 bytes each
  - Tag Memory:

Part number	Tag memory - user data
FM24NC32T1	144 bytes
FM24NC32T2	504 bytes
FM24NC32T3	888 bytes

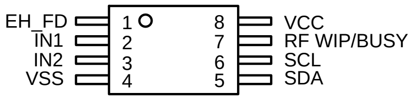
  - Self-timed write cycle (5 ms max)
  - Endurance: 1 million write cycles
  - Data retention: 40 years
- **Security**
  - Write protection of data memory by page in two wire serial interface
  - Write and read protection of data memory by 64 bytes in RF interface
  - Password protection for system configuration
  - Unique ID for each device
- **User configurable RF write in progress or RF busy 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 trigger action: upon any RF field presence, upon the selection of the tag and upon halt with previous read operation
  - FD output voltage: 1.5V
- **Green Package**
  - RoHS Compliant and Halogen-free

3 Packaging Type

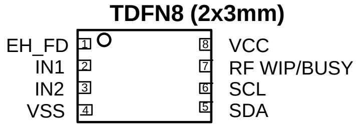
SOP8



TSSOP8



TDFN8 (2x3mm)



4 Pin Configurations

Pin Name	Function
EH_FD	Energy harvesting and Field Detection Output
SDA	Serial Data Input/Output
SCL	Serial Clock Input
RF WIP/BUSY	RF Write in Progress /RF Busy Output
IN1/IN2	Antenna connection
VCC	Power Supply
VSS	Ground

5 Block Diagram

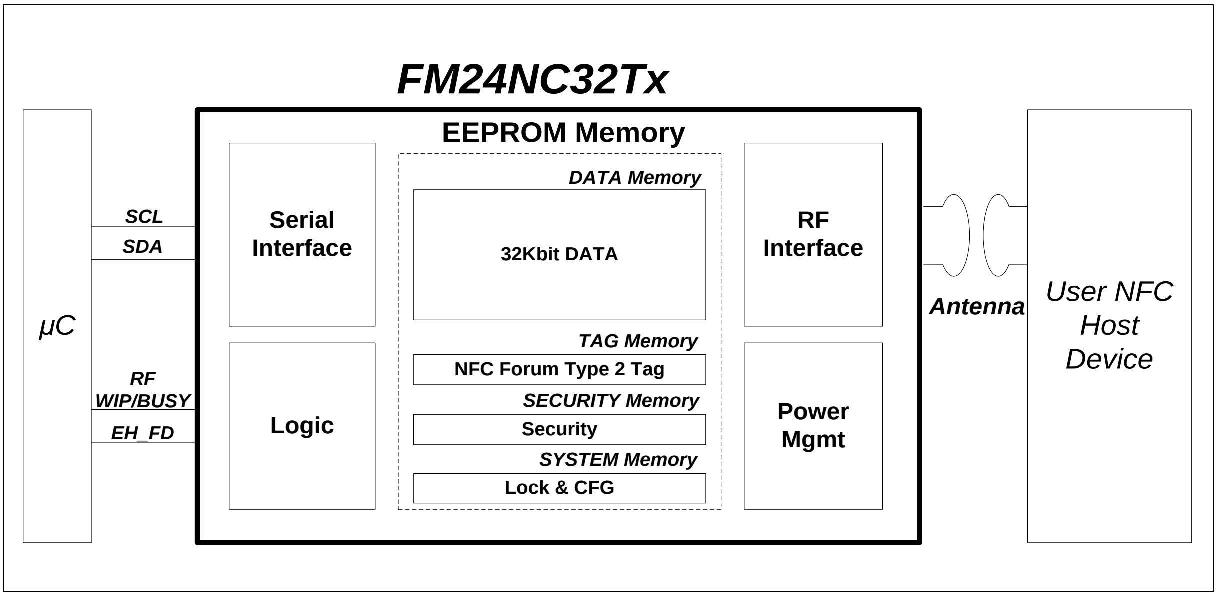


Figure 1 Block Diagram of FM24NC32Tx

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 RF Write in Progress/Busy (RF WIP/BUSY)

This configurable output signal is used either to indicate that the FM24NC32Tx is executing an internal write cycle 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 RF WIP/BUSY 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 FM24NC32Tx memory consists of four parts: Data memory, Tag memory, Security memory and System memory. Each part can be accessed by two wire serial interface or RF interface or both.

Table 1 Memory organization of FM24NC32Tx.

Contact Interface	RF Interface	Address		Byte number inside page			Description
		Page	Byte	0	…	31	
Address: 0000h ~ 0FE0h	Data memory command	00h	0000h	Data memory (128 page X 32 byte)			Data memory
		01h	0020h				
		…	…				
		7Fh	0FE0h				
Address: 1000h ~ 1FFFh	Tag command	80h	1000h	Tag memory			Tag memory
		…	…				
		9Dh	13A0h				
	N/A	9Eh	13C0h	NULL			-
		9Fh	13E0h				
		A0h	1400h	Security memory			Security memory
		…	…				
		A7h	14E0h				
		A8h	1500h	NULL			-
		…	…				
		BFh	17E0h				
		C0h	1800h	CT_DATA_WR_LOCK			System memory
		C1h	1820h	RFU			
		C2h	1840h	CT_TAG_WR_LOCK & CT_SCT_WR_LOCK			
		C3h	1860h	RFU			
	LOCK command	C4h	1880h	RF_DATA_RD_LOCK			
		C5h	18A0h	RFU			

Contact Interface	RF Interface	Address Page	Address Byte	Byte number inside page 0	…	31	Description
		C6h	18C0h	RF_DATA_WR_LOCK			
		C7h	18E0h	RFU			
	N/A	C8h	1900h	SYSTEM CFG			
		C9h	1920h	RFU			
		CAh	1940h	UID			
		CBh	1960h	NULL			-
		…	…				
		0FFh	1FE0h			RF_SLEEP	

Remark: NULL 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 FM24NC32Tx is organized in 128 pages of 32 bytes each. When accessed by two wire serial interface, each byte can be individually read or write using 2 bytes of byte address which address range is from 0000h to 0FFFh. When accessed by RF interface, each 64 bytes can be individually read or write using 1 byte of address.

There is a special mechanism to protect data memory from unexpected read and write operation. For command from two wire serial interface, each page is protected by 1 bit of CT_DATA_WR_LOCK. For command from RF interface, each 64 bytes is protected by 1 bit of RF_DATA_RD_LOCK and 1 bit of RF_DATA_WR_LOCK. Read and write operations are possible if the addressed memory is not protected.

The default value of the data memory at delivery is 00h.

7.2 Tag memory

In FM24NC32Tx, there's a tag memory to ensure NFC Forum Type 2 Tag operation. It can be accessed by two wire serial interface using 2 bytes of byte address which address range is from 1000h to 13BFh.

The tag memory is organized in 30 pages of 32 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 FM24NC32T1 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 FM24NC32T1

Contact CMD Page addr.	Contact CMD Byte addr.	Tag CMD Block addr. Hex.	Tag CMD Block addr. Dec.	Byte number inside block 0	1	2	3	Description
80h ~ 81h	1000h	00h	0	UID0/RFU	UID1/RFU	UID2/RFU	BCC0/RFU	UID and static lock bytes
	1004h	01h	1	UID4/RFU	UID5/RFU	UID6/RFU	UID7/RFU	
	1008h	02h	2	BCC1/RFU	Internal/RFU	Lock_byte[0]	Lock_byte[1]	
	100Ch	03h	3	Capability Container (CC)				CC
	1010h	04h	4	Static Data Area (Block 04h-0Fh, total 12 blocks)				User data
	…	…	…					
	103Ch	0Fh	15					

Contact CMD		Tag CMD		Byte number inside block				Description
Page addr.	Byte addr.	Block addr. Hex.	Block addr. Dec.	0	1	2	3	
82h ~ 87h	1040h	10h	16	Dynamic Data Area (Block 10h~27h, total 24 blocks)				
	…	…	…					
	109Ch	27h	39					
	10A0h	28h	40	Dynamic Lock Bytes				Dynamic Lock Bytes
	10A4h	29h	41	FDP & MIRROR	RFU	MIRROR_BLOCK	AUTH0	Configuration
	10A8h	2Ah	42	ACCESS	RFU			
	10ACh	2Bh	43	PWD				
	10B0h	2Ch	44	PACK		RFU		

For FM24NC32T2, 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 FM24NC32T2

Contact CMD		Tag CMD		Byte number inside block				Description
Page addr.	Byte addr.	Block addr. Hex.	Block addr. Dec.	0	1	2	3	
80h ~ 81h	1000h	00h	0	UID0/RFU	UID1/RFU	UID2/RFU	BCC0/RFU	UID and static lock bytes
	1004h	01h	1	UID4/RFU	UID5/RFU	UID6/RFU	UID7/RFU	
	1008h	02h	2	BCC1/RFU	Internal/RFU	Lock_byte[0]	Lock_byte[1]	
	100Ch	03h	3	Capability Container (CC)				CC
	1010h	04h	4	Static Data Area (Block 04h-0Fh, total 12 blocks)				User data
	…	…	…					
	103Ch	0Fh	15					
82h ~ 91h	1040h	10h	16	Dynamic Data Area (Block 10h~81h, total 114 blocks)				
	…	…	…					
	1204h	81h	129					
	1208h	82h	130	Dynamic Lock Bytes				Dynamic Lock Bytes
	120Ch	83h	131	FDP & MIRROR	RFU	MIRROR_BLOCK	AUTH0	Configuration
	1210h	84h	132	ACCESS	RFU			
	1214h	85h	133	PWD				
	1218h	86h	134	PACK		RFU		

For FM24NC32T3, 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 FM24NC32T3

Contact CMD		Tag CMD		Byte number inside block				Description
Page addr.	Byte addr.	Block addr. Hex.	Dec.	0	1	2	3	
80h ~ 81h	1000h	00h	0	UID0/RFU	UID1/RFU	UID2/RFU	BCC0/RFU	UID and static lock bytes
	1004h	01h	1	UID4/RFU	UID5/RFU	UID6/RFU	UID7/RFU	
	1008h	02h	2	BCC1/RFU	Internal/RFU	Lock_byte[0]	Lock_byte[1]	
	100Ch	03h	3	Capability Container (CC)				CC
	1010h	04h	4	Static Data Area (Block 04h-0Fh, total 12 blocks)				User data
	…	…	…					
	103Ch	0Fh	15					
82h ~ 9Dh	1040h	10h	16	Dynamic Data Area (Block 10h~E1h, total 210 blocks)				
	…	…	…					
	1384h	E1h	225					
	1388h	E2h	226	Dynamic Lock Bytes				Dynamic Lock Bytes
	138Ch	E3h	227	FDP & MIRROR	RFU	MIRROR_BLOCK	AUTH0	Configuration
	1390h	E4h	228	ACCESS	RFU			
	1394h	E5h	229	PWD				
	1398h	E6h	230	PACK		RFU		

7.2.1 Read only bytes(1000h~1009h)

In RF interface, these 10 bytes are read only. In contact interface, these 10 bytes can be written to any data, and be readout.

The default value of the first 9 bytes is as same as UID, see section 7.4.9 for further information, and the tenth byte is for internal use. This is for compatibility consideration because the first 9 bytes of NFC Forum Type2 Tag are defined as tag UID. The default value can help NFC host get UID information, for example using a read command from block 0 of tag memory.

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

7.2.2 Static lock bytes(100Ah~100Bh)

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 5 Static lock bytes of FM24NC32Tx

Field	Byte No.	Bit number inside byte							
		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.

7.2.3 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 FM24NC32T1 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 6.

For FM24NC32T2 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 7.

For FM24NC32T3 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 8.

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

Table 6 Dynamic Lock Byte of FM24NC32T1

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 7 Dynamic Lock Byte of FM24NC32T2

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 8 Dynamic Lock Byte of FM24NC32T3

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.

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.

7.2.4 Capability Container (CC) bytes(100Ch~100Fh)

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.

Default value of FM24NC32T1 CC bytes

1110 0001	0001 0000	0001 0010	0000 0000

WRITE command to block 03h

0000 0000	0000 0000	0000 0000	0000 1111

Result in block 03h (read-only state)

1110 0001	0001 0000	0001 0010	0000 1111

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 7.2.6.

7.2.5 Data blocks

Blocks 04h to 27h for FM24NC32T1, blocks 04h to 81h for FM24NC32T2 and blocks 04h to E1h for FM24NC32T3 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 7.2.7 for further details.

The default values of the data blocks at delivery are defined in Section 7.2.6.

7.2.6 CC and Data blocks content at delivery

The tag memory of FM24NC32Tx are pre-programmed to the initialized state according to the NFC

Forum Type 2 Tag specification as defined in Table 9,
Table 10 and
Table 11.

Table 9 Memory content at delivery of FM24NC32T1

Contact CMD		Tag CMD	Byte number inside block			
Page addr.	Byte addr.	Block addr.	0	1	2	3
80h	100Ch	03h	E1h	10h	12h	00h
	1010h	04h	01h	03h	A0h	0Ch
	1014h	05h	34h	03h	03h	D0h
	1018h	06h	00h	00h	FEh	00h

Table 10 Memory content at delivery of FM24NC32T2

Contact CMD		Tag CMD	Byte number inside block			
Page addr.	Byte addr.	Block addr.	0	1	2	3
80h	100Ch	03h	E1h	10h	3Fh	00h
	1010h	04h	01h	03h	88h	08h
	1014h	05h	66h	03h	03h	D0h
	1018h	06h	00h	00h	FEh	00h

Table 11 Memory content at delivery of FM24NC32T3

Contact CMD		Tag CMD	Byte number inside block			
Page addr.	Byte addr.	Block addr.	0	1	2	3
8h	100Ch	03h	E1h	10h	6Fh	00h
	1010h	04h	01h	03h	E8h	0Eh
	1014h	05h	66h	03h	03h	D0h
	1018h	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.

7.2.7 Configuration

Blocks 29h to 2Ah for FM24NC32T1 variant, blocks 83h to 84h for FM24NC32T2 variant and blocks E3h to E4h for FM24NC32T3 variant are used to conFigure the memory access restriction and to conFigure the UID ASCII mirror feature.

Blocks 2Bh to 2Ch for FM24NC32T1 variant, blocks 85h to 86h for FM24NC32T2 variant and blocks E5h to E6h for FM24NC32T3 variant are used as password and PACK.

Table 12 MIRROR_BYTE configuration

Byte address	Block address	Field	Bit number inside byte							
			7	6	5	4	3	2	1	0
10A4h/ 120Ch/ 138Ch	29h/ 83h/ E3h	FDP & MIRROR	MIRROR_CONF		MIRROR_BYTE		SLEEP_EN	STRG_MOD_EN	FDP_CONF	

Remark: Byte/Block address is for FM24NC32T1, FM24NC32T2 and FM24NC32T3 individually.

Table 13 ACCESS configuration

Byte address for FM24NC32T1	Block address	Field	Bit number inside byte							
			7	6	5	4	3	2	1	0
10A8h	2Ah	ACCESS	PROT	RFU	CFGLCK1	CFGLCK0	RFU	AUTHLIM		

Byte address for FM24NC32T2	Block address	Field	Bit number inside byte							
			7	6	5	4	3	2	1	0
1210h	84h	ACCESS	PROT &CFGLCK	RFU	RFU	RFU	RFU	AUTHLIM		

Byte address for FM24NC32T3	Block address	Field	Bit number inside byte							
			7	6	5	4	3	2	1	0
1390h	E4h	ACCESS	PROT	RFU	CFGLCK	RFU	RFU	AUTHLIM		

Remark: Byte/Block address is for FM24NC32T1, FM24NC32T2 and FM24NC32T3 individually.

Table 14 TAG configuration parameter description

FM24NC32T1

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC32T1	10A4h	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 10/11b ... not permitted
FM24NC32T1	10A4h	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)
FM24NC32T1	10A4h	29h	SLEEP_EN	1	0b	Enables the SLEEP mode function
FM24NC32T1	10A4h	29h	STRG_MOD_EN	1	0b	Controls the tag modulation strength - by default strong modulation is enabled
FM24NC32T1	10A4h	29h	FDP_CONF	2	01b	FDP CONF defines the configuration of the Field detect pin 00b ... no field detect 01b... enabled by halt with previous read operation 10b... enabled by selection of the tag 11b... enabled by field presence

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC32T1	10A6h	29h	MIRROR_BLOCK	8	00h	MIRROR_BLOCK defines the page for the beginning of the ASCII mirroring A value >03h enables the ASCII mirror feature 04h-24h ... valid values for FM24NC32T1 04h-7Eh ... valid values for FM24NC32T2 04h-DEh ... valid values for FM24NC32T3
FM24NC32T1	10A7h	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. If AUTH0 is set to a page address which is higher than the last page from the user configuration, the password protection is effectively disabled.
FM24NC32T1	10A8h	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
FM24NC32T1	10A8h	2Ah	CFGLCK1	1	0b	Write locking bit for the user configuration block 2Ah 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access
FM24NC32T1	10A8h	2Ah	CFGLCK0	1	0b	Write locking bit for the user configuration block 29h 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access
FM24NC32T1	10A8h	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

FM24NC32T2

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC32T2	120Ch	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 10/11b ... not permitted
FM24NC32T2	120Ch	83h	MIRROR_BYTE	2	00b	The 2 bits define the byte position within the page defined by the MIRROR_BLOCK byte (beginning of ASCII mirror)
FM24NC32T2	120Ch			1	0b	Enables the SLEEP mode function
FM24NC32T2	120Ch	83h	STRG_MOD_EN	1	0b	Controls the tag modulation strength - by default strong modulation is enabled
FM24NC32T2	120Ch	83h	FDP_CONF	2	01b	FDP CONF defines the configuration of the Field detect pin 00b ... no field detect 01b... enabled by halt with previous read operation 10b... enabled by selection of the tag 11b... enabled by field presence
FM24NC32T2	120Eh	83h	MIRROR_BLOCK	8	00h	MIRROR_BLOCK defines the page for the beginning of the ASCII mirroring A value >03h enables the ASCII mirror feature 04h-24h ... valid values for FM24NC32T1 04h-7Eh ... valid values for FM24NC32T2 04h-DEh ... valid values for FM24NC32T3
FM24NC32T2	120Fh	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 page address which is higher than the last page from the user configuration, the password protection is effectively disabled.
FM24NC32T2	1210h	84h	PROT&CFGLCK	1	0b	One bit inside the ACCESS byte defining the memory protection and write locking

Part number	Byte address	Block address	Field	Bit	Default values	description
						bit for the user configuration block 83h~84h 0b ... write access is protected by the password verification and user configuration open to write access 1b ... read and write access is protected by the password verification and user configuration permanently locked against write access
FM24NC32T2	1210h	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

FM24NC32T3

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC32T3	138Ch	E3h	MIRROR_CON F	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 10/11b ... not permitted
FM24NC32T3	138Ch	E3h	MIRROR_BYT E	2	00b	The 2 bits define the byte position within the page defined by the MIRROR_BLOCK byte (beginning of ASCII mirror)
FM24NC32T3	138Ch	E3h	SLEEP_EN	1	0b	Enables the SLEEP mode function
FM24NC32T3	138Ch	E3h	STRG_MOD_E N	1	0b	Controls the tag modulation strength - by default strong modulation is enabled
FM24NC32T3	138Ch	E3h	FDP_CONF	2	01b	FDP CONF defines the configuration of the Field detect pin 00b ... no field detect 01b... enabled by halt with previous read operation 10b... enabled by selection of the tag 11b... enabled by field presence
FM24NC32T3	138Eh	E3h	MIRROR_BLO	8	00h	MIRROR_BLOCK defines the

Part number	Byte address	Block address	Field	Bit	Default values	description
			CK			page for the beginning of the ASCII mirroring A value >03h enables the ASCII mirror feature 04h-24h ... valid values for FM24NC32T1 04h-7Eh ... valid values for FM24NC32T2 04h-DEh ... valid values for FM24NC32T3
FM24NC32T3	138Fh	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 page address which is higher than the last page from the user configuration, the password protection is effectively disabled.
FM24NC32T3	1390h	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
FM24NC32T3	1390h	E4h	CFGLCK	1	0b	Write locking bit for the user configuration block E3h~E4h 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access
FM24NC32T3	1390h	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

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 FM24NC32Tx. If write protection is enabled, each write attempt leads to a NAK response.

Table 15 TAG password and PACK description

Part number	Byte address	Block address	Field	Bit	Default values	description
FM24NC32T1	10BCh~10BFh	2Bh	PWD	32	all 1b	32-bit password used for memory access protection
FM24NC32T2	1214h~1217h	85h				
FM24NC32T3	1394h~1397h	E5h				
FM24NC32T1	10C0h~10C1h	2Ch	PACK	16	0000h	16-bit password acknowledge used during the password verification process
FM24NC32T2	1218h~1219h	86h				
FM24NC32T3	1398h~1399h	E6h				

7.3 Security memory

FM24NC32Tx provides 256 bytes security memory, which byte address is from 1400h to 14FFh in contact interface. Security memory is organized in 8 pages of 32 bytes each.

Security memory can be written freely when CT_SCT_WR_LOCK is set logic 0. Once CT_SCT_WR_LOCK is set logic 1, the write access to security memory is locked. CT_SCT_WR_LOCK has 8 bits, and each bit locks one page of security memory individually. The response of writing on the locked security memory is NAK, and the data of security memory couldn't be changed.

CT_SCT_WR_LOCK is only modified from logic 0 to logic 1. The process is irreversible. If a bit is set to logic 1, it cannot be changed back to logic 0.

Security memory cannot be accessed by RF interface.

The default value of the security memory at delivery is 00h.

7.4 System memory

Table 16 System memory organization of FM24NC32Tx

Contact address		byte number			
Page addr.	Byte addr.	0	1	2	3
C0h	1800h	CT_DATA_WR_LOCK[31:0]			
	…	…			
	180Ch	CT_DATA_WR_LOCK[127:96]			
	1810h	RFU			
	…				
	181Ch				
C1h	1820h	RFU			
	…				
	183Ch				
C2h	1840h	CT_TAG_WR_LOCK[29:0]			
	1844h	CT_SCT_WR_LOCK[7:0]			
	1845h	RFU			
	…				
	185Fh				
C3h	1860h	RFU			
	…				
	187Fh				
C4h	1880h	RF_DATA_RD_LOCK[31:0]			
	1884h	RF_DATA_RD_LOCK[63:32]			
	1888h	RFU			
	…				

Contact address		byte number			
Page addr.	Byte addr.	0	1	2	3
	189Ch				
C5h	18A0h … 18BCh	RFU			
C6h	18C0h	RF_DATA_WR_LOCK[31:0]			
	18C4h	RF_DATA_WR_LOCK[63:32]			
	18C8h … 18DCh	RFU			
C7h	18E0h … 18FCh	RFU			
C8h	1900h	CT_PWD			
	1904h	RF_PWD			
	1908h	PIN_CFG	RFU		
	190Ch … 191Ch	RFU			
C9h	1920h … 193Ch	RFU			
125h	1940h	UID0	UID1	UID2	BCC1
	1944h	UID3	UID4	UID5	UID6
	1948h	BCC2	Internal		
	194Ch … 195Ch	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_DATA_WR_LOCK(1800h~180Fh)

CT_DATA_WR_LOCK has 128 bits organized in 16 bytes, which byte address is from 1800h to 180Fh in contact interface. Each bit locks the write access of one page of data memory in contact interface. CT_DATA_WR_LOCK[0] is used to lock Page 000h of data 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_DATA_WR_LOCK doesn't need authentication of contact password (CT_PWD). However, the write access must be in CT_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.

7.4.2 CT_TAG_WR_LOCK(1840h~1843h)

CT_TAG_WR_LOCK has 30 bits, which byte address is from 1840h to 1843h. The definitions see Table 17.

Table 17 CT_TAG_WR_LOCK configuration

Byte address	Field	Bit number inside byte							
		7	6	5	4	3	2	1	0
1840h	CT_TAG_WR_LOCK	CT_TAG_WR_LOCK[7:0]							
1841h		CT_TAG_WR_LOCK[15:8]							
1842h		CT_TAG_WR_LOCK[23:16]							
1843h		RFU		CT_TAG_WR_LOCK[29:24]					

Each bit locks write access of one page in tag memory in contact interface. CT_TAG_WR_LOCK[0] is used to lock Page 100h of tag memory, and CT_TAG_WR_LOCK[1] locks Page 101h, and so on. Logic 1 indicates lock, Logic 0 indicates unlock.

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

CT_TAG_WR_LOCK does not affect the 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.

7.4.3 CT_SCT_WR_LOCK(1844h)

CT_SCT_WR_LOCK has 8 bits which byte address is 1844h. Each bit locks the write access of one page of security memory in contact interface. CT_SCT_WR_LOCK[0] is used to lock page A0h of security memory, and CT_SCT_WR_LOCK[1] locks page A1h, and so on. Logic 1 indicates lock, Logic 0 indicates unlock.

Table 18 CT_SCT_WR_LOCK configuration

Byte address	Field	Bit number inside byte							
		7	6	5	4	3	2	1	0
1844h	CT_SCT_WR_LOCK	CT_SCT_WR_LOCK[7:0]							

Remark: RFU is reserved for future use. The default value of each bit is 0b.

The read access of CT_SCT_WR_LOCK doesn't need authentication of CT_PWD. However, the write access must be in CT_PWD authenticated state.

By using write command in contact interface, the content change of CT_SCT_WR_LOCK is bit-wise OR'ed. This process is irreversible. If a bit is set to logic 1, it cannot be changed back to logic 0.

CT_SCT_WR_LOCK cannot be accessed by RF interface.

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

7.4.4 RF_DATA_RD_LOCK(1880h~1887h)

RF_DATA_RD_LOCK has 64 bits organized in 8 bytes which byte address is from 1880h to 1887h in contact interface. Each bit locks the read access of 64 bytes of data memory in RF interface. RF_DATA_RD_LOCK[0] is used to lock byte[63:0] of data memory, and RF_DATA_RD_LOCK[1] locks byte[127:64], and so on. Logic 1 indicates lock, Logic 0 indicates unlock.

In contact interface, the read access of RF_DATA_RD_LOCK doesn't need authentication of CT_PWD. However, the write access must be in CT_PWD authenticated state.

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

In RF interface, in RF_PWD authenticated state, by using RF LOCK command, the content change of RF_DATA_RD_LOCK is bit-wise OR'ed. This process is irreversible. If a bit is set to logic 1, it cannot be changed back to logic 0.

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

7.4.5 RF_DATA_WR_LOCK(18C0h~18C7h)

RF_DATA_WR_LOCK has 64 bits organized in 8 bytes which byte address is from 18C0h to 18C7h. Each bit locks the write access of one page of data memory in RF interface. RF_DATA_WR_LOCK[0] is used to lock Page 000h of data memory, and RF_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 RF_DATA_WR_LOCK doesn't need authentication of CT_PWD. However, the write access must be in CT_PWD authenticated state.

In RF interface, the read access of RF_DATA_RD_LOCK doesn't need authentication of RF_PWD. However, the write access must be in RF_PWD authenticated state.

In RF interface, after RF_PWD authentication, by using RF LOCK command, the content change of RF_DATA_WR_LOCK is bit-wise OR'ed. This process is irreversible. If a bit is set to logic 1, it cannot be changed back to logic 0.

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

7.4.6 CT_PWD(1900h~1903h)

CT_PWD is password of contact interface. It has 32 bits organized in 4 bytes, which byte address is from 1900h to 1903h in contact interface. CT_PWD is used to password authentication in contact interface.

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

CT_PWD cannot be accessed by RF interface.

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

7.4.7 RF_PWD(1904h~1907h)

RF_PWD is password of RF interface. It has 32 bits organized in 4 bytes, which byte address is from 1904h to 1907h in contact interface. RF_PWD is used to data memory (DM) authentication in RF interface.

In contact interface, RF_PWD can be read whether in CT_PWD authenticated state or not, but it can be written only in CT_PWD authenticated state.

RF_PWD cannot read or write by RF interface.

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

7.4.8 PIN_CFG(1908h)

PIN_CFG is used to conFigure EH_FD pin and RF WIP/BUSY pin. The detail is shown in Table 19.

Table 19 PIN_CFG configuration

Byte addr.	Field	Bit number inside byte							
		7	6	5	4	3	2	1	0
1908h	PIN_CFG	RF_WIP/BUSY	RFU	EH_IOUT		EH_ILIM		EH_VOUT	

RF_WIP/BUSY is used to conFigure the output signal of RF WIP/BUSY pin. Logic 1 indicates to output RF WIP signal; Logic 0 indicates to output RF BUSY signal. The default value at delivery is 0b.

EH_IOUT is used to conFigure the drive strength of energy harvesting function. The default value at delivery is 00b.

- 00b indicates 100% current drive strength
- 01b indicates 26% current drive strength
- 10b indicates 2% current drive strength
- 11b indicates to disable energy harvesting and enable field detect function

The default value at delivery varies according to the option of ordering information, 00b for –E3 and 11b for –F0, respectively.

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

The default value at delivery is 00b.

EH_VOUT is used to conFigure the output voltage of energy harvesting function. The default value at delivery is 00b.

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

The default value at delivery varies according to the option of ordering information, 11b for –E3 and 00b for –F0, respectively.

In contact interface, PIN_CFG can be read, and be written in CT_PWD authenticated state.

In RF interface, PIN_CFG cannot be read or written whether RF password is authenticated or not.

7.4.9 UID(1940h~1948h)

FM24NC32Tx provides read-only 9 bytes Unique Identification (UID), which byte address is from 1940h to 1948h 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 system memory is read-only. The content of UID cannot change by write command whether in password authenticated state or not. The response of write access on UID in system memory is No ACK.

In RF interface UID in system memory cannot be accessed directly except for anticollision operation.

7.5 RF_SLEEP(1FFFh)

FM24NC32Tx provides RF_SLEEP register, which byte address is 1FFFh in contact interface. It is volatile. The detail is shown in Table 20.

Table 20 RF_SLEEP register

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

RF_SLEEP is used to conFigure RF sleep function.

- 10b indicates to enable the sleep mode function of RF interface
- Other configurations indicate to disable the sleep mode function of RF interface

8 Contact Interface

FM24NC32Tx 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. FM24NC32Tx is a slave in all communications.

8.1 Two wire serial operation

8.1.1 Data Operation

FM24NC32Tx 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 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, RF communications are not possible.

To prevent RF communication freezing due to inadvertent un-terminated commands sent to the two wire serial bus, the FM24NC32Tx 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 FM24NC32Tx 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 57), 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 57, 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

FM24NC32Tx features a field detection function. The field detection can be used as interrupt signal. The FD function can be enabled by PIN_CFG in 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 FM24NC32Tx 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 FM24NC32Tx 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 $P_{IN1-IN2\_min}$, the FM24NC32Tx 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 system memory. The current consumption on the EH_FD cannot exceed the configured value of IOUT in PIN_CFG. Otherwise, the output voltage cannot meet the configured voltage value of PIN_CFG.

8.3 RF WIP/BUSY Output

FM24NC32Tx features a configurable open drain output RF WIP/BUSY pin used to provide RF activity information to an external device. The RF WIP/BUSY pin functionality depends on the value of bit[7] of PIN_CFG in system memory.

8.3.1 RF Write in progress

When bit[7] of PIN_CFG is set to 1, the RF WIP/BUSY pin is configured in RF write in progress mode. The purpose of this mode is to indicate to two wire serial bus master that some data has been changed in RF interface.

In this mode, the RF WIP/BUSY pin is tied to 0 for the duration of an internal write operation (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 RF WIP/BUSY pin remains in high-Z state.

8.3.2 RF busy

When bit[7] of PIN_CFG is set to 0, the RF WIP/BUSY pin is configured in RF busy mode. The purpose of this mode is to indicate to two wire serial bus master whether FM24NC32Tx is busy in RF interface or not.

In this mode, the RF WIP/BUSY 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 RF WIP/BUSY pin is tied to 0 from the RF command SOF until the reception of the RF command CRC. Otherwise, the RF WIP/BUSY pin is in high-Z state. When tied to 0, the RF WIP/BUSY signal returns to High-Z state if the RF field is cut-off.

During the execution of two wire serial commands, the RF WIP/BUSY pin remains in high-Z state.

8.4 Command

8.4.1 Command Overview

8.4.1.1 Command Set

Table 21 command set of two wire serial interface

Command	Device Address	Address	Data
Data memory Write	A0h	0000h~0FFFh	1~32 bytes
Data memory Read	A1h	-	Output n bytes
Tag, Security or System Write	A0h	1000h~195Fh	1~32 bytes
Tag, Security or System Read	A1h	-	Output n bytes
Password authentication	A0h (un-authenticated state)	1900h	4 bytes PWD
Password write	A0h (authenticated state)	1900h	4 bytes new PWD
Password read	A1h (authenticated state)	- (1)	Output 4 bytes PWD
Password de-authentication	A1h (authenticated state)	- (1)	-

Note: 1. The current address of read operation is the starting address of CT_PWD (1900h).

8.4.1.2 Timing

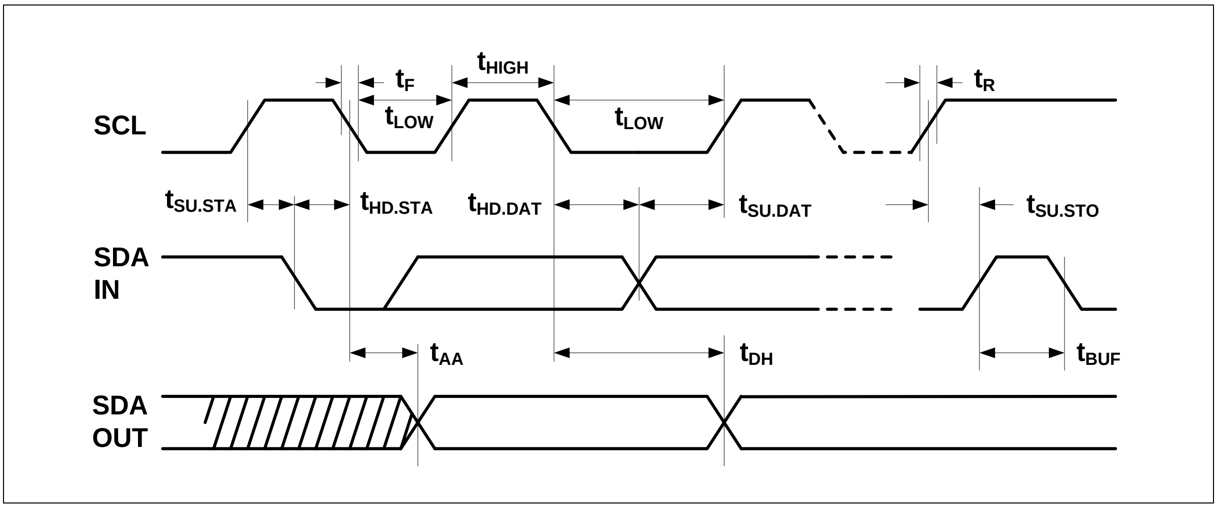


Figure 3 Two-wire Series Interface Bus Timing

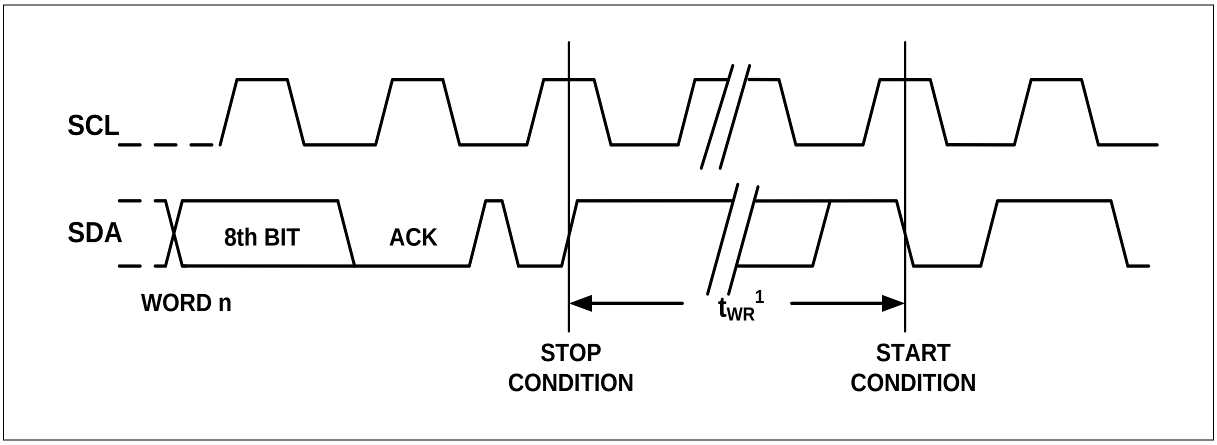


Figure 4 Writing Cycle Timing

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.

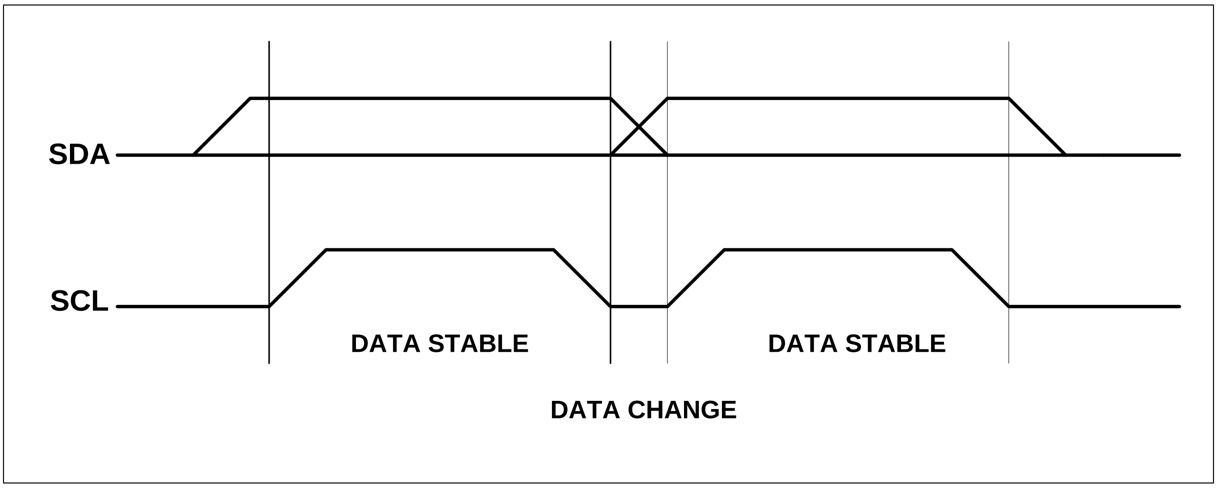


Figure 5 Data Validity

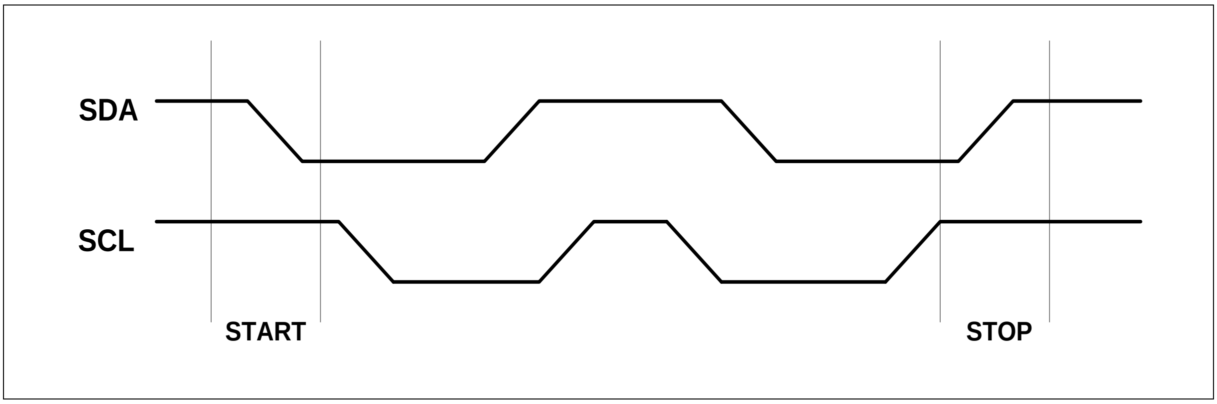


Figure 6 Start and Stop Definition

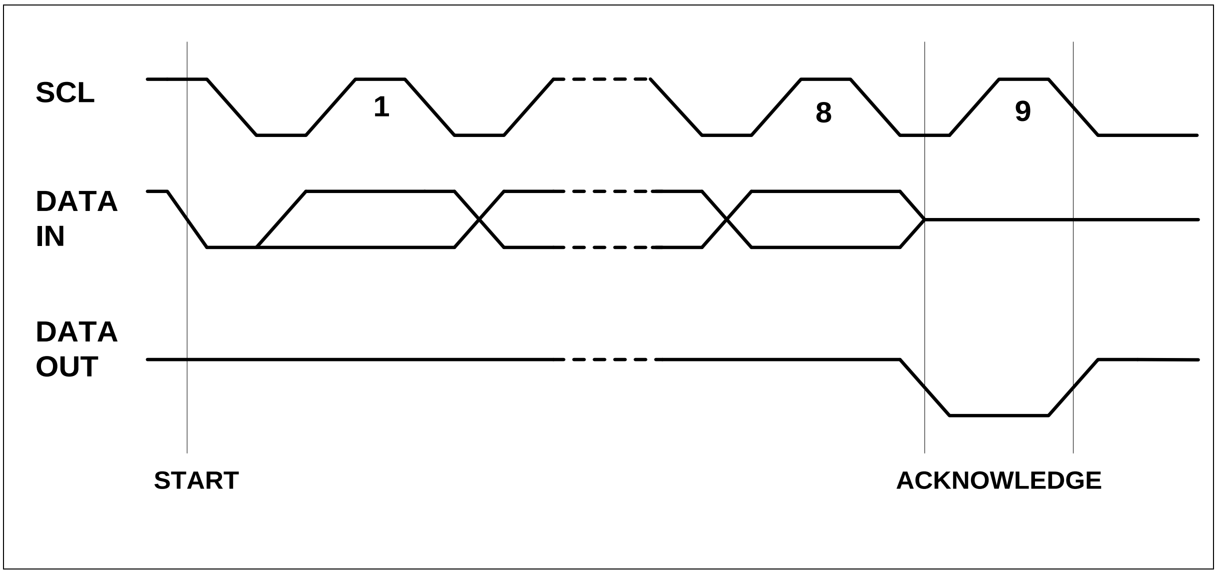


Figure 7 Output Acknowledge

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 9^{th} clock pulse period, the receiver pulls the SDA low to acknowledge the receipt of the eight data bits.

Table 22 ACK response in contact interface

Operation	Area	State	Response
Write	Data memory	un-locked	ACK
		locked	No ACK
	Tag memory	un-locked	ACK
		locked	No ACK
	Security memory	un-locked	ACK
		locked	No ACK
	Lock byte, RF_PWD & PIN_CFG in System memory	CT_PWD authenticated	ACK
		CT_PWD un-authenticated	No ACK
	UID in System memory	CT_PWD authenticated	No ACK
		CT_PWD un-authenticated	No ACK
	Internal	CT_PWD authenticated	No ACK
		CT_PWD un-authenticated	No ACK
	NULL	-	ACK (no data refreshed)
Password authentication	CT_PWD in System memory	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).

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.

MSB							LSB
1	0	1	0	0	0	0	$R/\overline{W}$

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 corresponding lock bit=0.

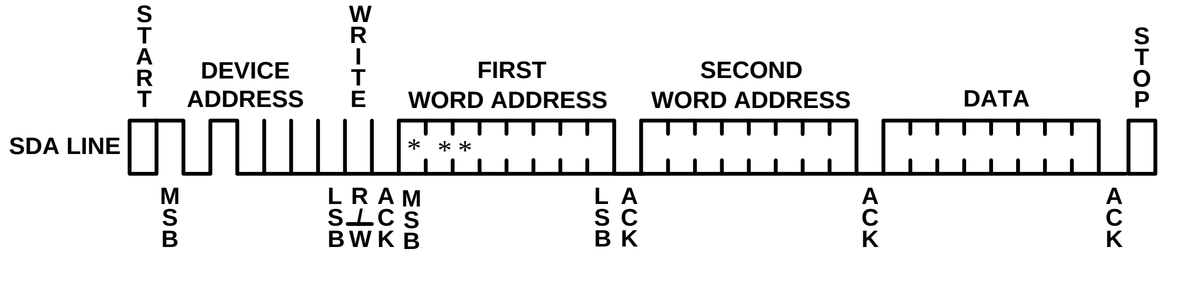
When the bus master generates a Stop condition immediately after the Ack bit (in the tenth bit time slot), either at the end of a byte write or a page write, the internal write cycle is triggered and all inputs are disabled during this write cycle and the EEPROM will not respond until the write is complete.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

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

Writing to system memory needs password verification. Without verification, device responds NAK, and no internal write cycle is triggered.

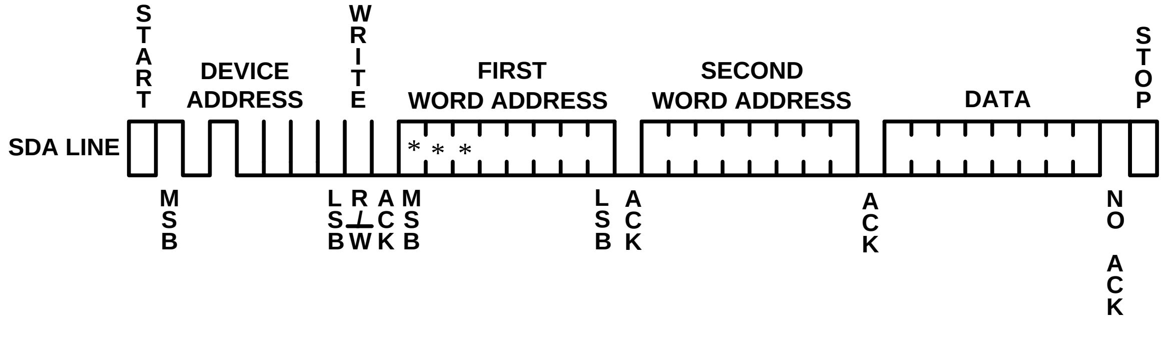
8.4.2.1 Byte write

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=0



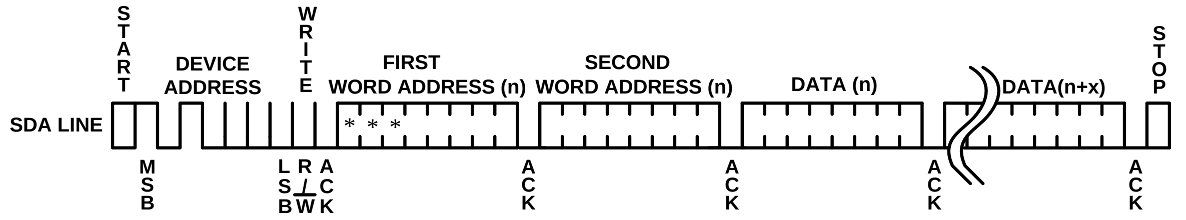
Note: 1. * = *Don't CARE* bits

Figure 10 Byte write with lock bit=1

8.4.2.2 Page write

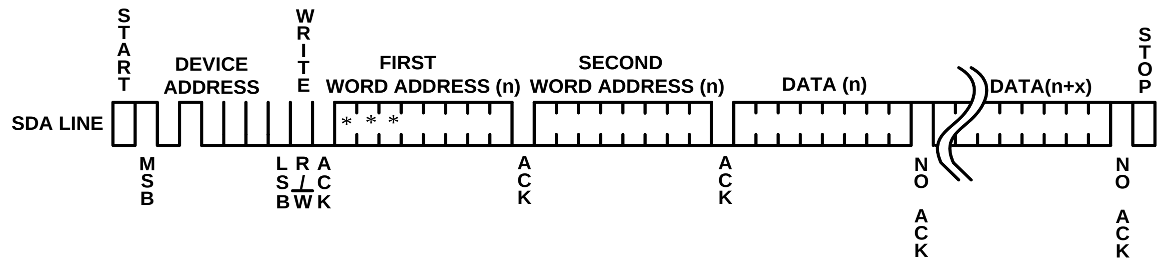
A page write is initiated the same way as a byte write, but the master does not send a stop condition after the first data word is clocked in. Instead, after the EEPROM acknowledges receipt of the first data word, the master can transmit up to 31 more data words. The EEPROM responds to each data byte 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 six 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 64 data words 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=0



Note: 1. * = ***Don’t CARE*** bits

Figure 12 Page write with lock bit=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 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.

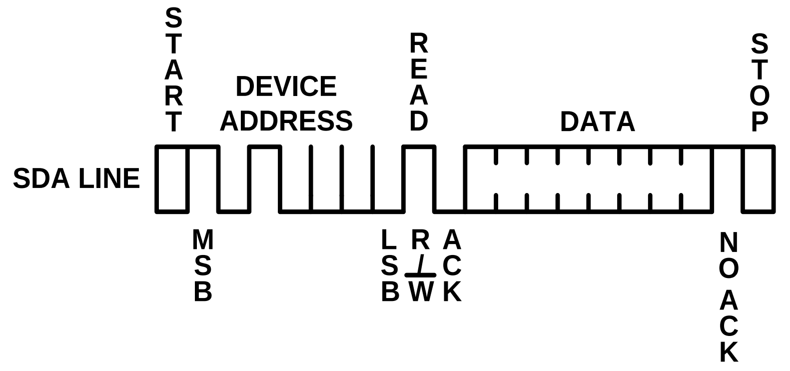


Figure 13 Current address read

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. If the addressed memory is write protected, the device will not acknowledge the device address byte. But it has no impact to the following process. 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.

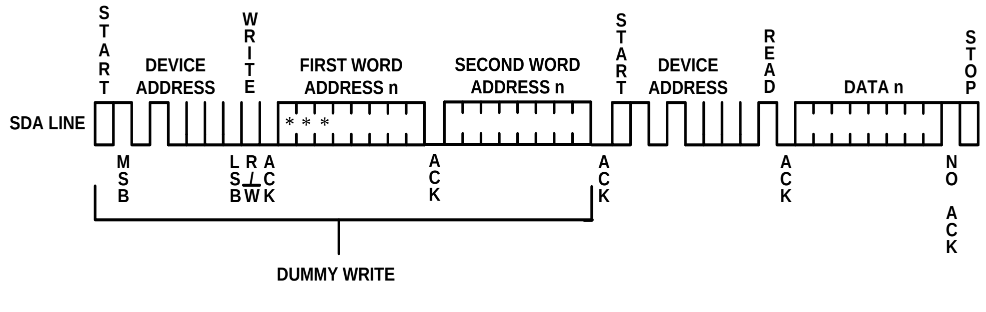


Figure 14 random read

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.

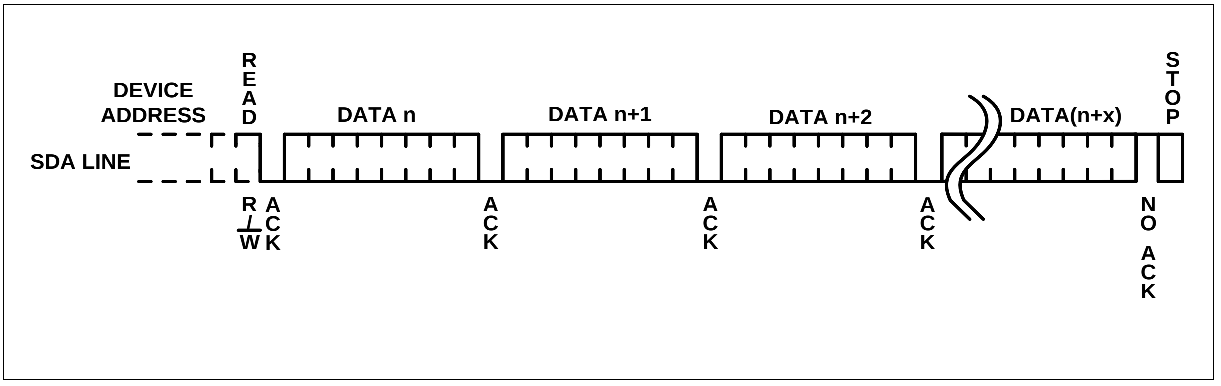


Figure 15 sequential read

8.4.4 Password command

The device has two status, verified status in which 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_PWD (xxx11001 00000000b) 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 authenticated status. If the input data does not match password, the password authentication operation is fail and the device remains unauthenticated state.

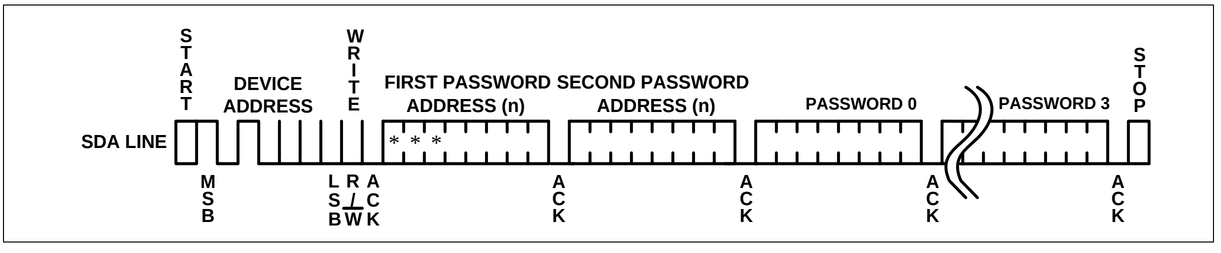


Figure 16 password authentication

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, with the exception that the start address must be CT password address (word address=xxx11001 00000000b).

After stop, the device returns to unauthenticated status.

If device receives password read command in unauthenticated status, it replies No ACK and the output data is all logic 1.

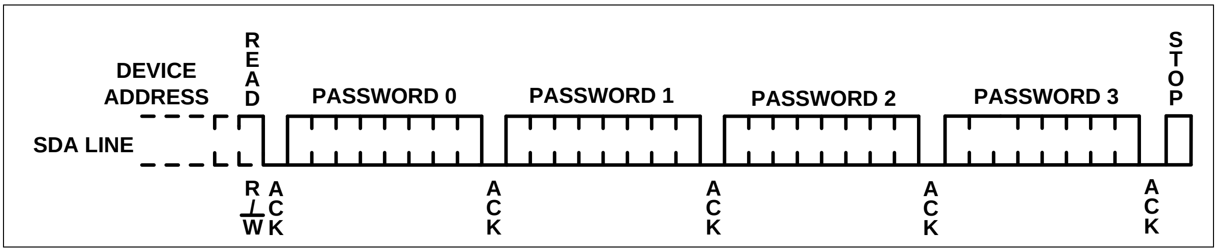


Figure 17 password read in authenticated state

8.4.4.4 Password de-authentication

After password read command, 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 VOUT 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 tag frame is 604 bits (1 cmd byte + 64 data bytes + 2 CRC bytes = 1×9+64×9+2×9+ 1 start bit). The maximum length of a fixed size tag to NFC device frame is 595 bits (64 data bytes + 2 CRC bytes = 64×9+2×9+ 1 start bit). The 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 FM24NC32Tx. 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.

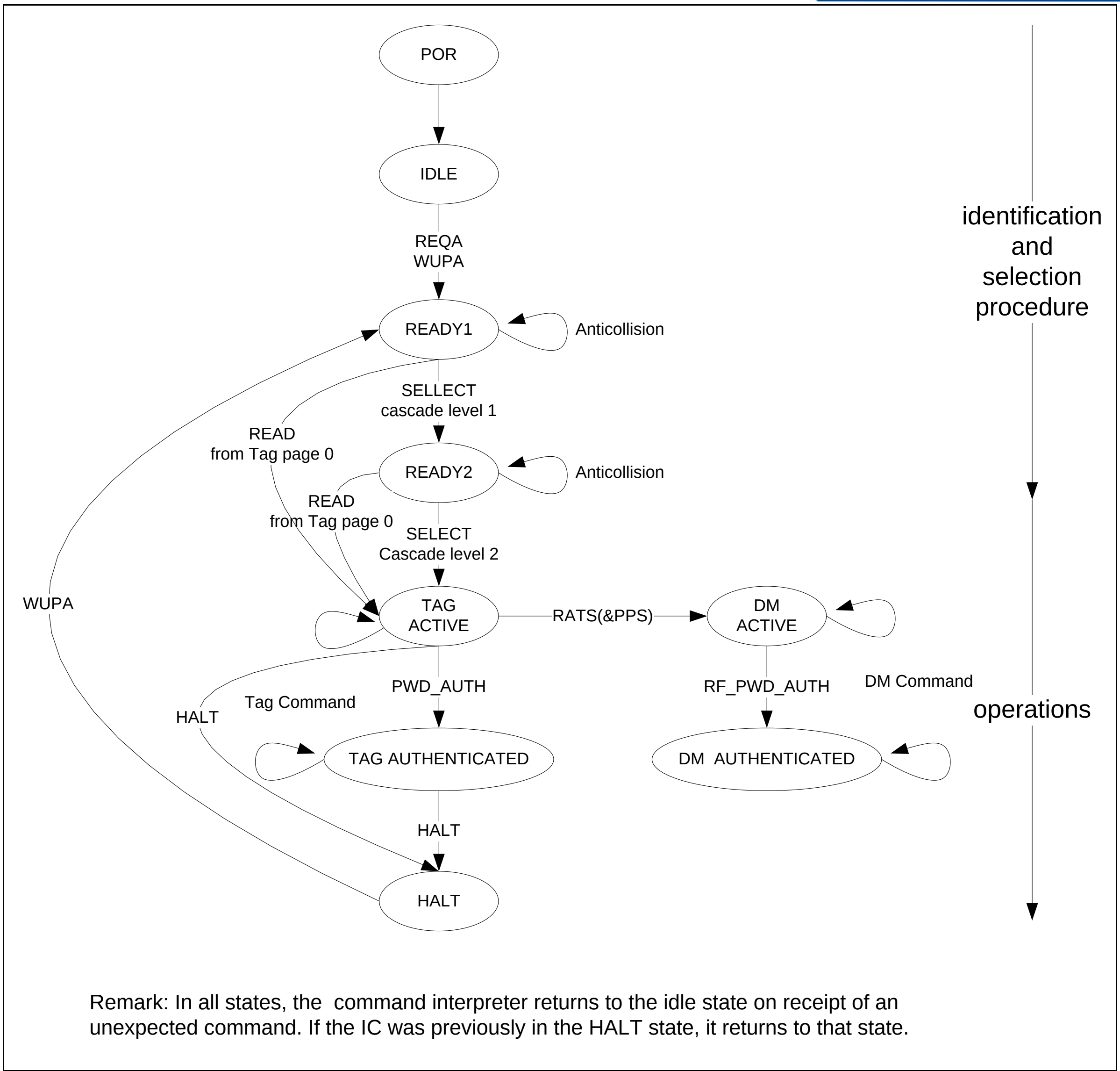


Figure 18 state diagram of RF interface

9.1.1 IDLE state

After a power-on reset (POR), FM24NC32Tx 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 FM24NC32Tx 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 FM24NC32Tx into READY2 state where the second part of the UID is resolved.

• READ command (from address 0): all anticollision mechanisms are bypassed and the FM24NC32Tx 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 FM24NC32Tx 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 FM24NC32Tx returns to the IDLE or HALT state.

9.1.3 READY2 state

In this state, FM24NC32Tx 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 FM24NC32Tx 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. FM24NC32Tx 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 FM24NC32Tx is in the NFC device field, a READ command from address 0 selects all FM24NC32Tx 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 FM24NC32Tx 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 FM24NC32Tx 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, FM24NC32Tx returns to either the IDLE state or HALT state.

FM24NC32Tx transits to the TAG AUTHENTICATED state after successful password verification using the PWD_AUTH command.

9.1.5 Data Memory (DM) ACTIVE state

All Data Memory (DM) operations are operated in this state.

Any other data received when the device is in this state is interpreted as an error and FM24NC32Tx returns to the IDLE state.

FM24NC32Tx transits to the DM AUTHENTICATED state after successful RF password verification using the RF_PWD_AUTH command.

9.1.6 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 FM24NC32Tx 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, FM24NC32Tx returns to either the IDLE state or HALT state.

9.1.7 Data Memory (DM) AUTHENTICATED state

In this state, all operations on RF read/write lock pages, which are configured as RF password verification protected, can be accessed.

Any other data received when the device is in this state is interpreted as an error and FM24NC32Tx returns to the IDLE state.

9.1.8 HALT state

HALT and IDLE states constitute the two wait states implemented in FM24NC32Tx. An already processed FM24NC32Tx can be set into the HALT state using the HLTA command. In the anti-collision phase, this state helps the NFC device to distinguish between processed tags and tags yet to be selected. FM24NC32Tx 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 FM24NC32Tx 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 32kbit data memory. Data memory command includes READ64B and WRITE64B. These two commands are used to read or write 64 bytes data in data memory.

Read and writing access of data memory in RF interface could be restricted by RF_DATA_RD_LOCK and RF_DATA_WR_LOCK individually. One bit of RF_DATA_RD_LOCK or RF_DATA_WR_LOCK protects 64 bytes read or writing access. When lock bit is logic 1, the 64 bytes locked by that bit cannot be read out or written, and the response of READ64B or WRITE64B command 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 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. For example, RF_DATA_RD_LOCK[7:0] is 1111 0000b originally. After writing 0000 0101b by WRITE_RF_DATA_RD_LOCK, RF_DATA_RD_LOCK[7:0] becomes 1111 0101b.

9.2.2 Data integrity

Following mechanisms are implemented in the contactless communication link between NFC device and FM24NC32Tx 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 UID ASCII mirror function

FM24NC32Tx features a UID ASCII mirror function. This function enables FM24NC32Tx to virtually mirror the 7 byte UID in ASCII code into the physical tag 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, FM24NC32Tx 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 23 Configuration parameter descriptions

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

9.2.4 Tag Password verification protection

The memory write or read/write access to a configurable part of the memory 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 7.2.7 can be used to limit the negative verification attempts.

In the initial state of FM24NC32Tx, 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 FM24NC32Tx 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 7.2.7. 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 FM24NC32T1, 85h for FM24NC32T2 and E5h for FM24NC32T3.

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 FM24NC32Tx.

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 FM24NC32Tx.

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

FM24NC32Tx 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 FM24NC32Tx 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 FM24NC32Tx are shown in Table 24.

Table 24 FM24NC32Tx 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

Command category	Command	ISO/IEC 14443	NFC Forum	Command Code (hexadecimal)
	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
	WRITE	-	WRITE	A2h
	COMP_WRITE	-	-	A0h
	PWD_AUTH	-	-	1Bh
	READ_SIG	-	-	3Ch
Data memory	READ64B	-	-	51h
	WRITE64B	-	-	54h
Data memory Lock	READ_RF_DATA_RD_LOCK	-	-	6Ah
	READ_RF_DATA_WR_LOCK	-	-	6Ch
	WRITE_RF_DATA_RD_LOCK	-	-	7Fh
	WRITE_RF_DATA_WR_LOCK	-	-	7Eh
	RF_PWD_AUTH	-	-	40h

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.

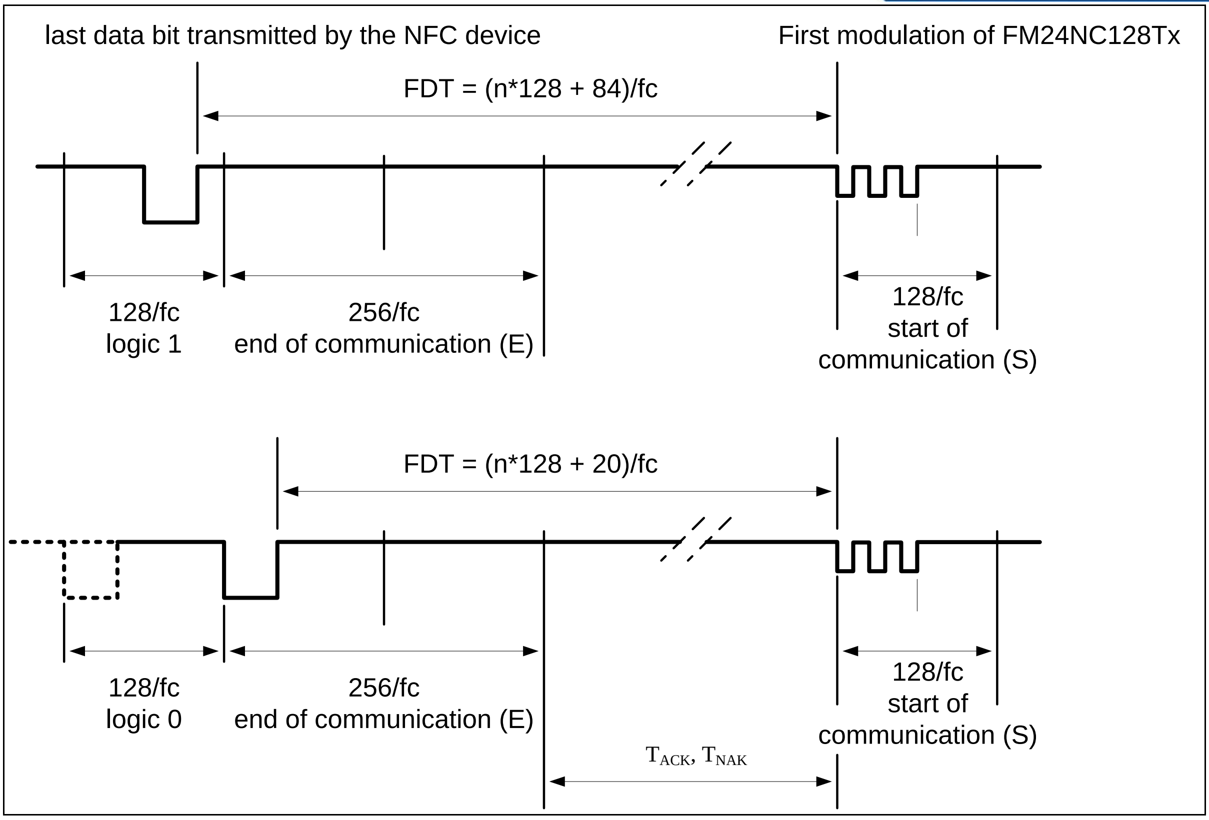


Figure 19 Frame Delay Time (from NFC device to FM24NC32Tx), T_{ACK} and T_{NAK}

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

NFC TAG uses a 4 bit ACK / NAK as shown in Table 25.

Table 25 ACK and NAK values

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

9.3.1.4 ATQA and SAK responses

FM24NC32Tx 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 26 ATQA response of the FM24NC32Tx

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 27 SAK response of the FM24NC32Tx

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 28.

Table 28 shows the required timing.

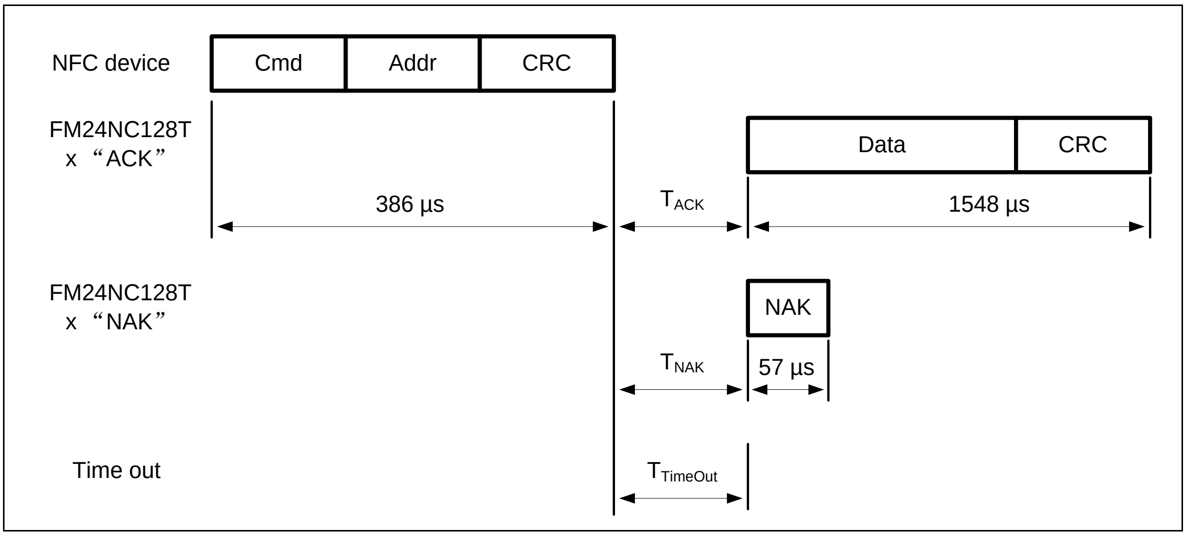


Figure 20 READ command

Table 28 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 25	see Section 9.3.1.3	4-bit

Table 29 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 FM24NC32Tx, all memory blocks are allowed as Addr parameter to the READ command.
• block address 00h to 2Ch for FM24NC32T1
• block address 00h to 86h for FM24NC32T2
• block address 00h to E6h for FM24NC32T3

Addressing a memory block beyond the limits above results in a NAK response from FM24NC32Tx.

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 FM24NC32Tx 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 FM24NC32Tx 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 FM24NC32Tx is in the AUTHENTICATED state
– the READ command behaves like on a FM24NC32Tx 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, FM24NC32Tx replies a NAK. For details on those cases and the command structure, refer to

Figure 21 and Table 30.

Table 31 shows the required timing.

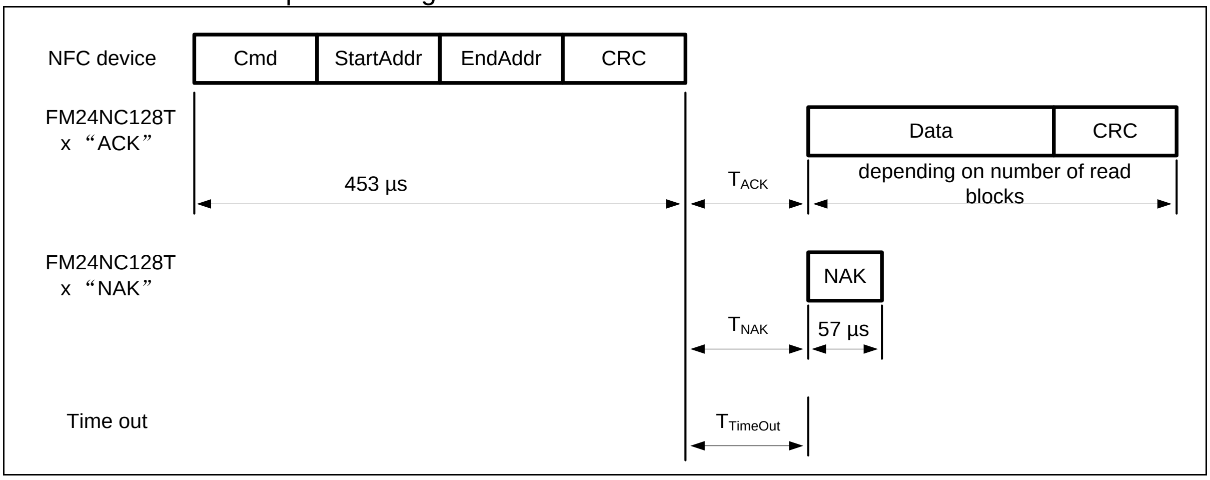


Figure 21 FAST_READ command

Table 30 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 25	see Section 9.3.1.3	4-bit

Table 31 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 FM24NC32Tx, all memory blocks are allowed as StartAddr parameter to the FAST_READ command.
• block address 00h to 2Ch for FM24NC32T1
• block address 00h to 86h for FM24NC32T2
• block address 00h to E6h for FM24NC32T3

Addressing a memory block beyond the limits above results in a NAK response from FM24NC32Tx.

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 FM24NC32Tx is in the ACTIVE state
– if any requested page address is equal or higher than AUTH0 a NAK is replied
• if FM24NC32Tx is in the AUTHENTICATED state
– the FAST_READ command behaves like on a FM24NC32Tx 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 FM24NC32Tx block. The WRITE command is shown in
Figure 22 and Table 32.

Table 33 shows the required timing.

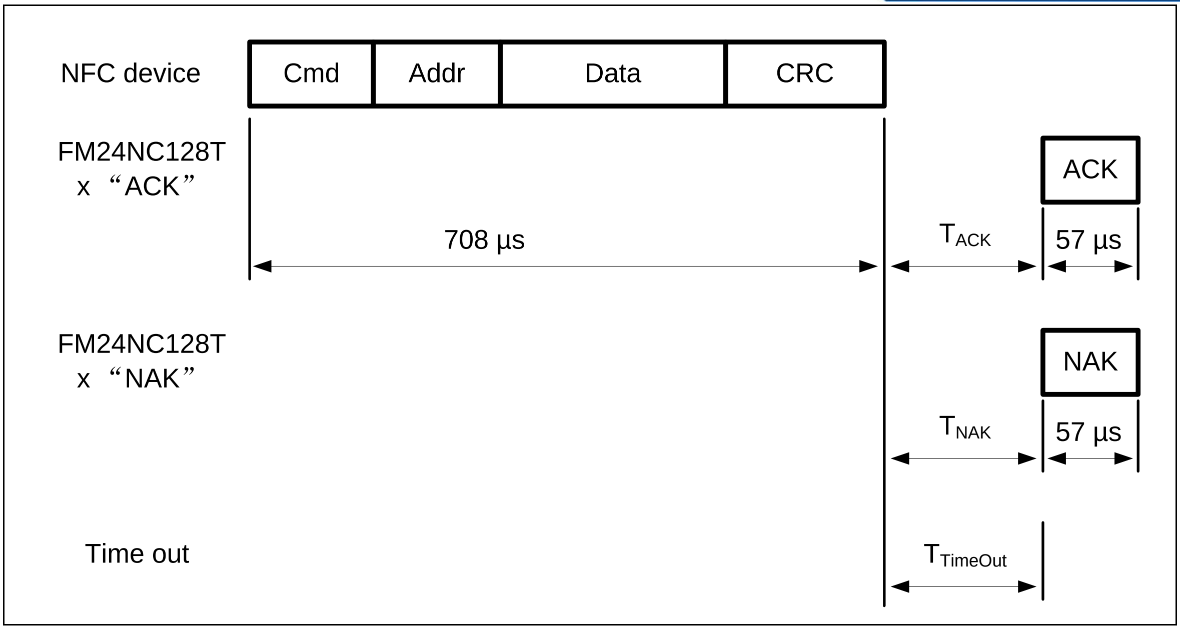


Figure 22 WRITE command

Table 32 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 25	see Section 9.3.1.3	4-bit

Table 33 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 FM24NC32Tx, the following memory blocks are valid Addr parameters to the WRITE command.

- block address 00h to 2Ch for FM24NC32T1
- block address 00h to 86h for FM24NC32T2
- block address 00h to E6h for FM24NC32T3

Addressing a memory block beyond the limits above results in a NAK response from FM24NC32Tx. 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 FM24NC32Tx is in the ACTIVE state
  – writing to a blocks which address is equal or higher than AUTH0 results in a NAK response
- if FM24NC32Tx is in the AUTHENTICATED state
  – the WRITE command behaves like on a FM24NC32Tx without access protection

FM24NC32Tx 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 FM24NC32T1
- block 82h containing the additional dynamic lock bits for FM24NC32T2
- block E2h containing the additional dynamic lock bits for FM24NC32T3

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 FM24NC32Tx, 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 34.

Table 35 shows the required timing.

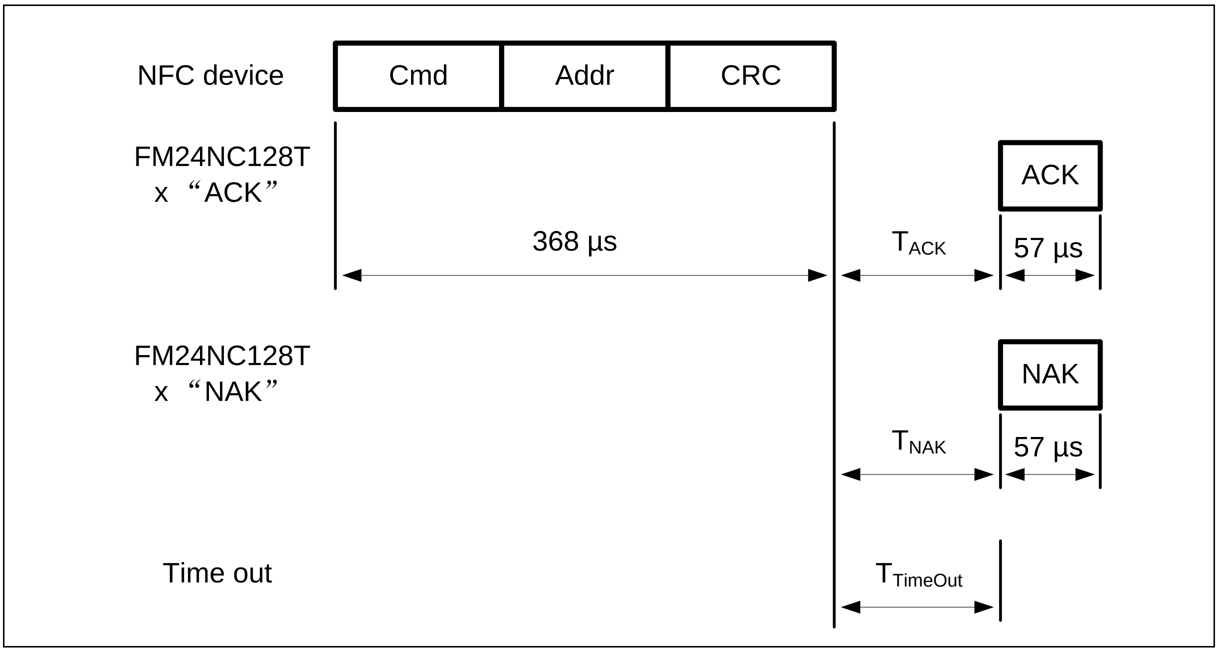


Figure 23 COMPATIBILITY_WRITE command part 1

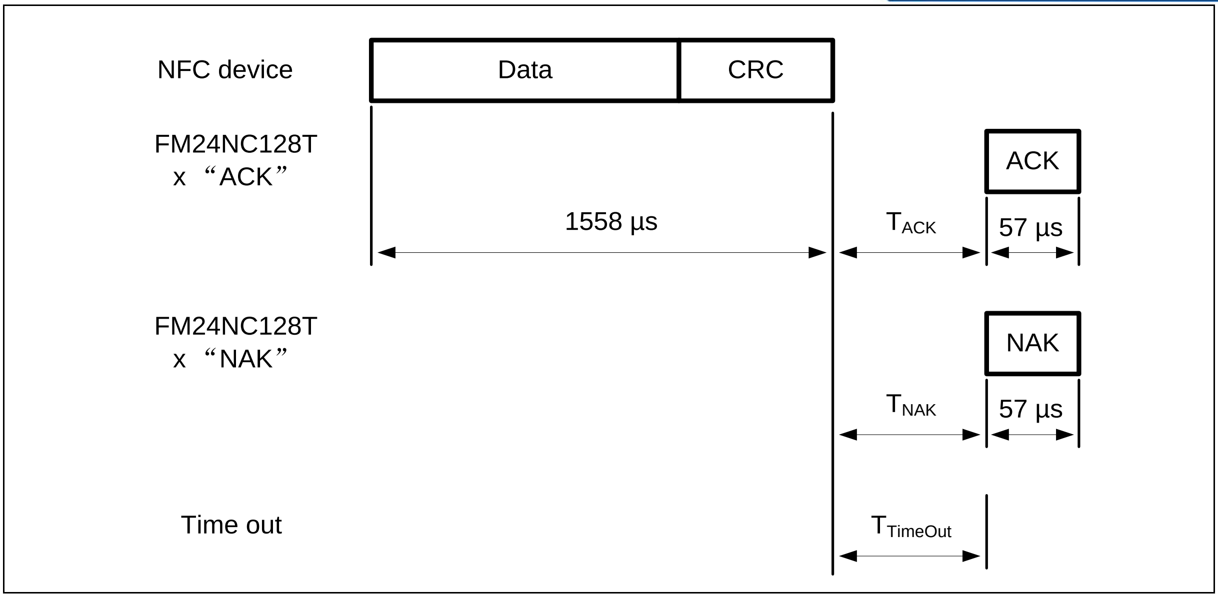


Figure 24 COMPATIBILITY_WRITE command part 2

Table 34 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 25	see Section 9.3.1.3	4-bit

Table 35 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 FM24NC32Tx, the following memory pages are valid Addr parameters to the COMPATIBILITY_WRITE command.

- block address 00h to 2Ch for FM24NC32T1
- block address 00h to 86h for FM24NC32T2
- block address 00h to E6h for FM24NC32T3

Addressing a memory block, that beyond the limits above, results in a NAK response from FM24NC32Tx.

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 FM24NC32Tx is in the ACTIVE state
  – Writing to a block which address is equal or higher than AUTH0 results in a NAK response
- If FM24NC32Tx is in the AUTHENTICATED state

– The COMPATIBILITY_WRITE command behaves the same as on a FM24NC32Tx without access protection

FM24NC32Tx 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 FM24NC32T1
- block 82h containing the additional dynamic lock bits for FM24NC32T2
- block E2h containing the additional dynamic lock bits for FM24NC32T3

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 36.

Table 37 shows the required timing.

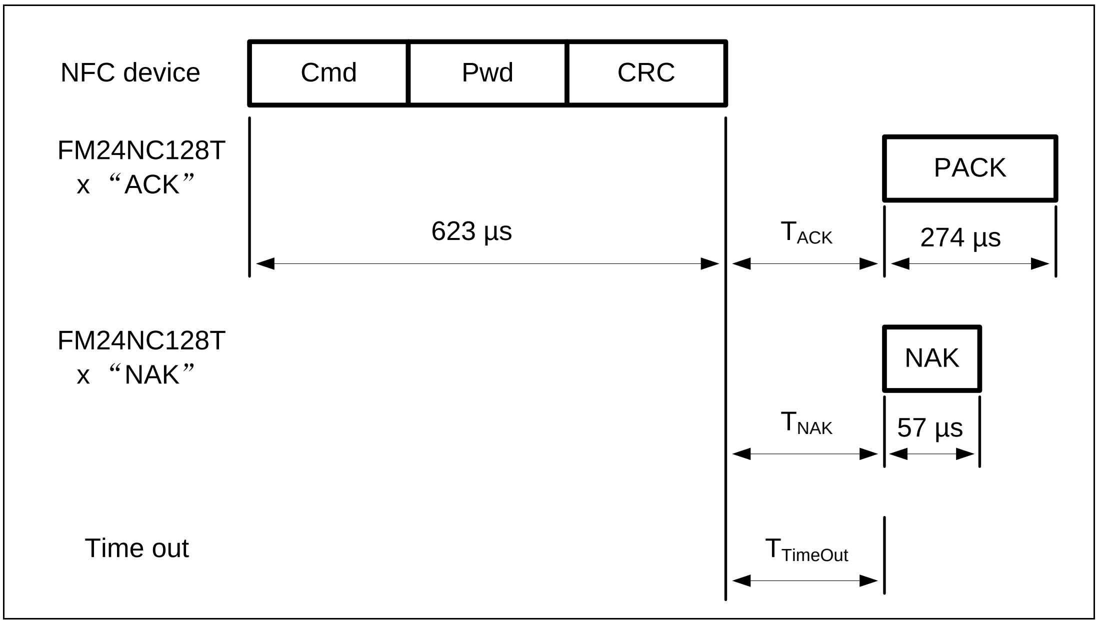


Figure 25 PWD_AUTH command

Table 36 PWD_AUTH command

Name	Code	Description	Length
Cmd	1Bh	Password authentication	1 byte
Pwd	-	password	4 byte
CRC	-	CRC	2 bytes
PACK	-	Password authentication acknowledge	2 bytes
NAK	see Table 25	see Section 9.3.1.3	4-bit

Table 37 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 READ64B (51h)

The READ64B command requires a page address of data memory, and returns the 64 bytes of one page. For example, if page address is 10h then the 64 bytes data of page 10h are returned. If the read access of the addressed page is protected by RF_DATA_RD_LOCK, the response of this command is NAK. The command structure is shown in Figure 26 and Table 38.

Table 39 shows the required timing.

Figure 26 READ64B command

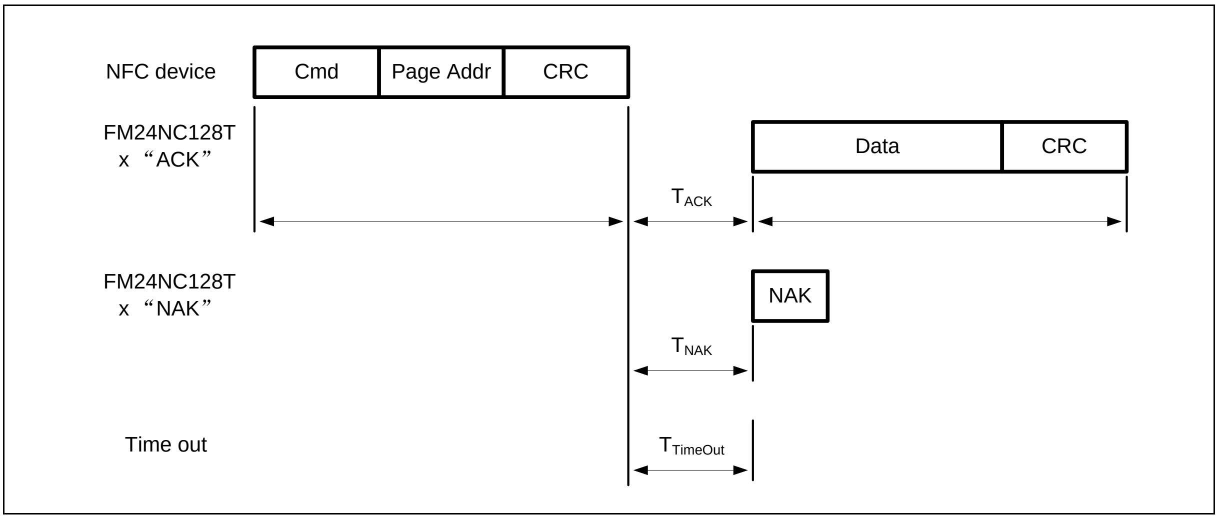


Table 38 READ64B command

Name	Code	Description	Length
Cmd	51h	Read one page of Data memory	1 byte
Page Addr	-	Page address of Data memory	1 byte
CRC	-	CRC	2 bytes
Data	-	data	64 bytes
NAK	see Table 25	see Section 9.3.1.3	4 bit

Table 39 READ64B timing

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

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
READ64B	n=9(1)	$T_{TimeOut}$	5ms

Note: 1. Refer to Section 9.3.1.2.

9.3.3.2 WRITE64B (54h)

The WRITE64B command requires a page address of data memory, and writes 64 bytes of data into the addressed page. If the write access of the page is protected by RF_DATA_WR_LOCK, the response of this command is NAK. The WRITE64B command is shown in Figure 27 and Table 40.

Table 41 shows the required timing.

Figure 27 WRITE64B command

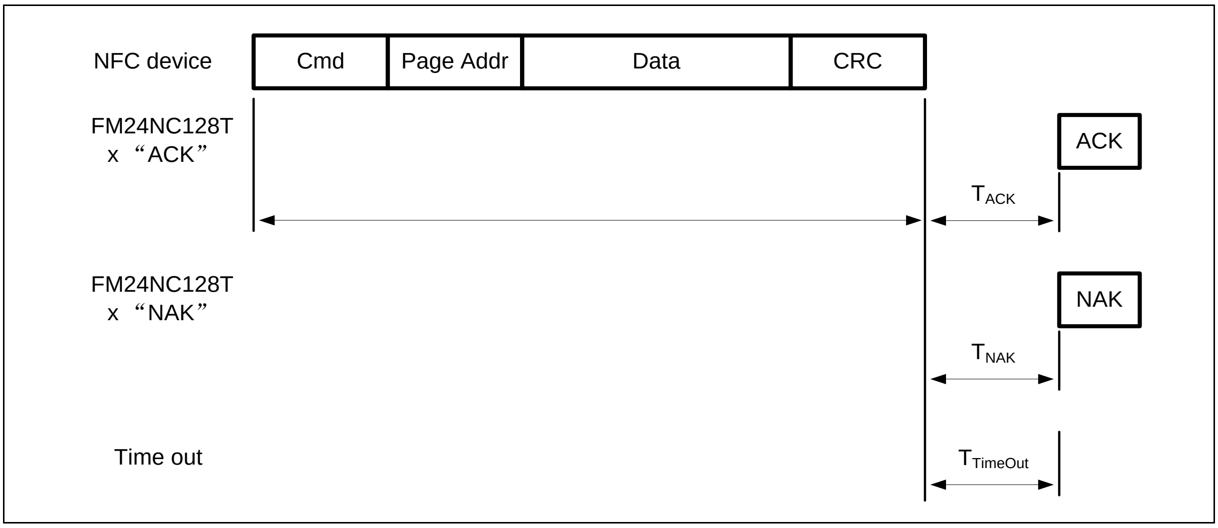


Table 40 WRITE64B command

Name	Code	Description	Length
Cmd	54h	Write one page of data memory	1 byte
Page Addr	-	Page address of data memory	1 byte
Data	-	data	64 bytes
CRC	-	CRC	2 bytes
ACK	Ah	Acknowledge (ACK)	4 bit
NAK	see Table 25	see Section 9.3.1.3	4 bit

Table 41 WRITE64B timing

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

Cmd	$T_{ACK/NAK}$ min	$T_{ACK/NAK}$ max	$T_{TimeOut}$
WRITE64B	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 (6Ah)

The READ_RF_DATA_RD_LOCK command is used to read the 8 bytes of RF_DATA_RD_LOCK and following 24 bytes of RFU. The command structure is shown in

Figure 28 and Table 42.

Table 43 shows the required timing.

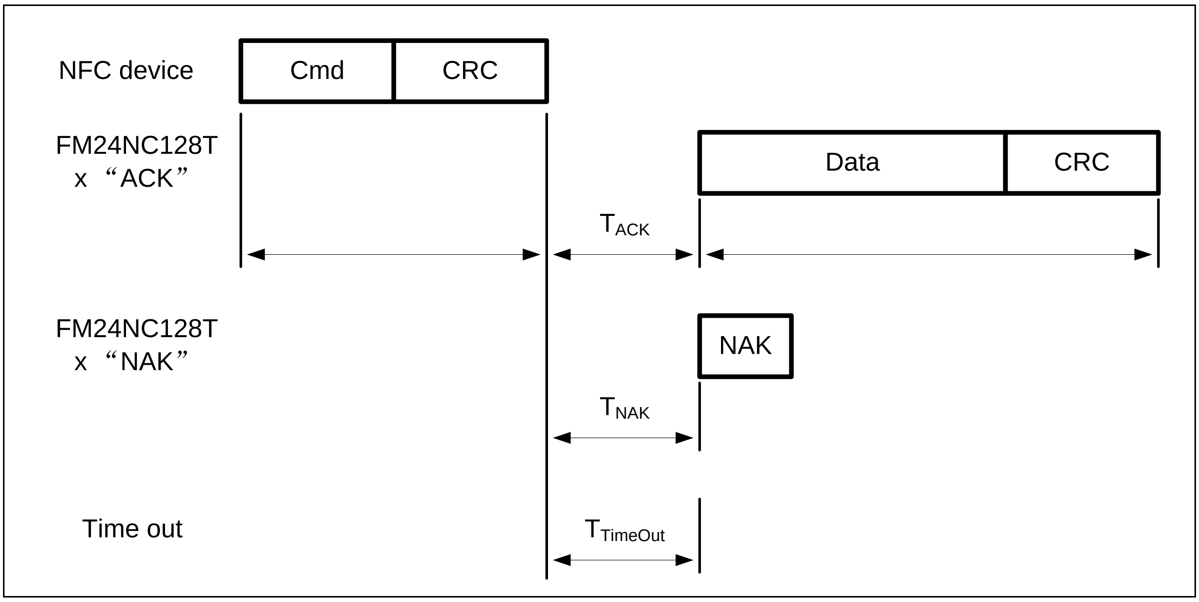


Figure 28 READ_RF_DATA_RD_LOCK command

Table 42 READ_RF_DATA_RD_LOCK command

Name	Code	Description	Length
Cmd	6Ah	Read RF_DATA_RD_LOCK data	1 byte
CRC	-	CRC	2 bytes
Data	-	data	32 bytes
NAK	see Table 25	see Section 9.3.1.3	4 bit

Table 43 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 (6Ch)

The READ_RF_DATA_WR_LOCK command is used to read the 8 bytes of RF_DATA_WR_LOCK and following 24 bytes of RFU. The command structure is shown in Figure 29 and Table 44.

Table 45 shows the required timing.

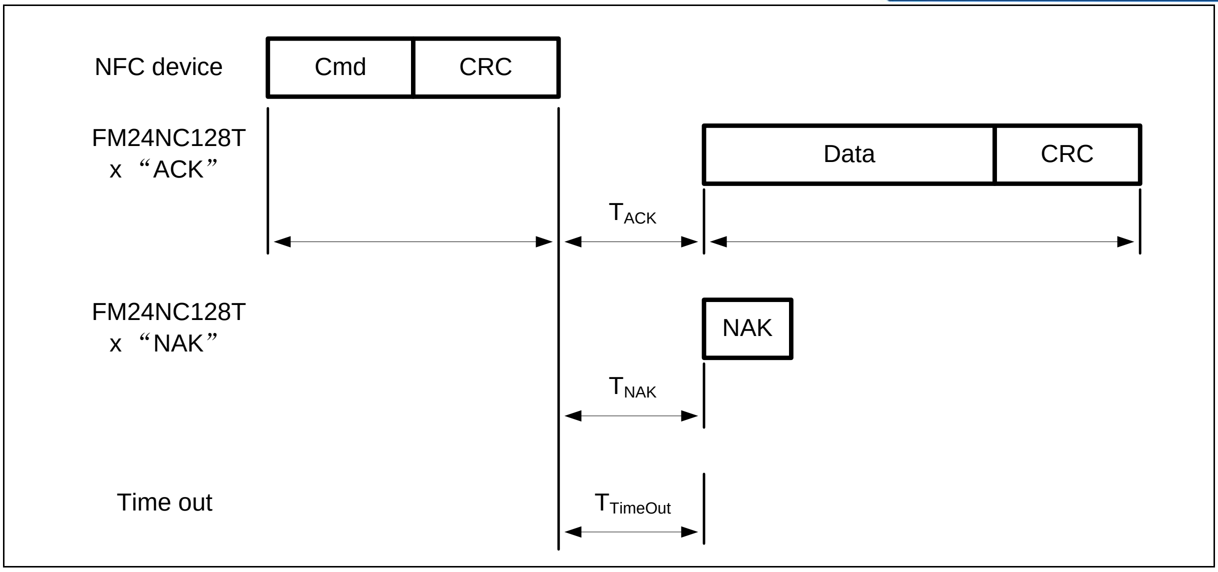


Figure 29 READ_RF_DATA_WR_LOCK command

Table 44 READ_RF_DATA_WR_LOCK command

Name	Code	Description	Length
Cmd	6Ch	Read RF_DATA_WR_LOCK data	1 byte
CRC	-	CRC	2 bytes
Data	-	data	32 bytes
NAK	see Table 25	see Section 9.3.1.3	4 bit

Table 45 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 (7Fh)

The WRITE_RF_DATA_RD_LOCK command writes 32 bytes of data into the 8 bytes of RF_DATA_RD_LOCK and following 24 bytes of RFU in system memory. This command is executed in DM AUTHENTICATED state. If the RF_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 46.

Table 47 shows the required timing.

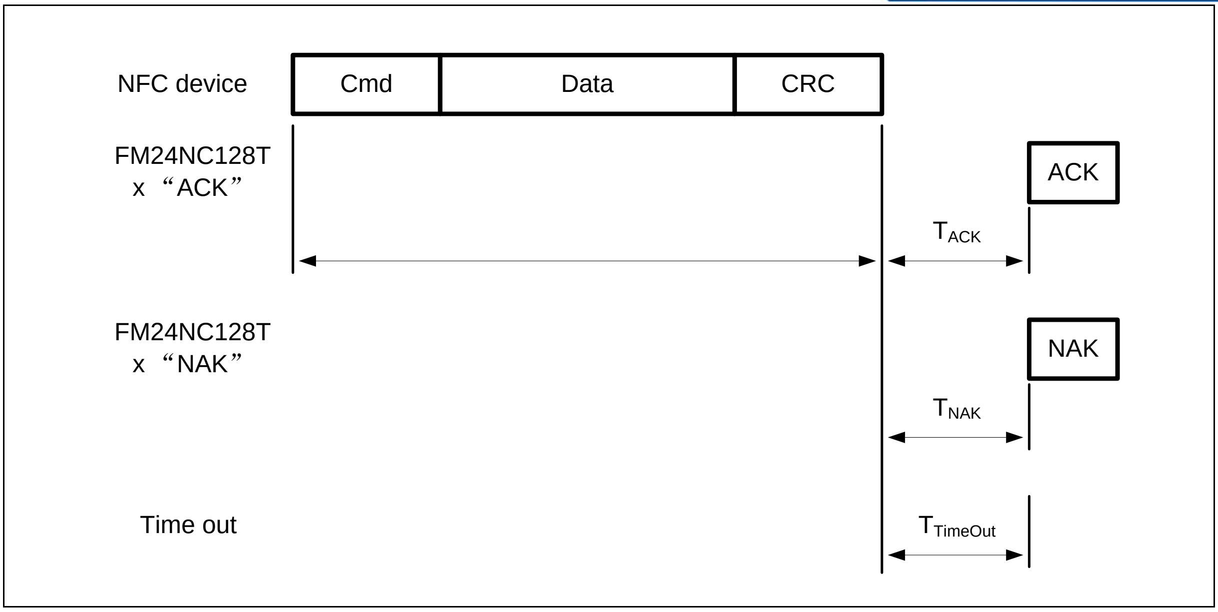


Figure 30 WRITE_RF_DATA_RD_LOCK command

Table 46 WRITE_RF_DATA_RD_LOCK command

Name	Code	Description	Length
Cmd	7Fh	write RF_DATA_RD_LOCK data	1 byte
Data	-	data	32 bytes
CRC	-	CRC	2 bytes
ACK	Ah	Acknowledge (ACK)	4 bit
NAK	see Table 25	see Section 9.3.1.3	4 bit

Table 47 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 (7Eh)

The WRITE_RF_DATA_WR_LOCK command writes 32 bytes of data into the RF_DATA_WR_LOCK in system memory. This command is executed in DM AUTHENTICATED state. If the RF_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 48.

Table 49 shows the required timing.

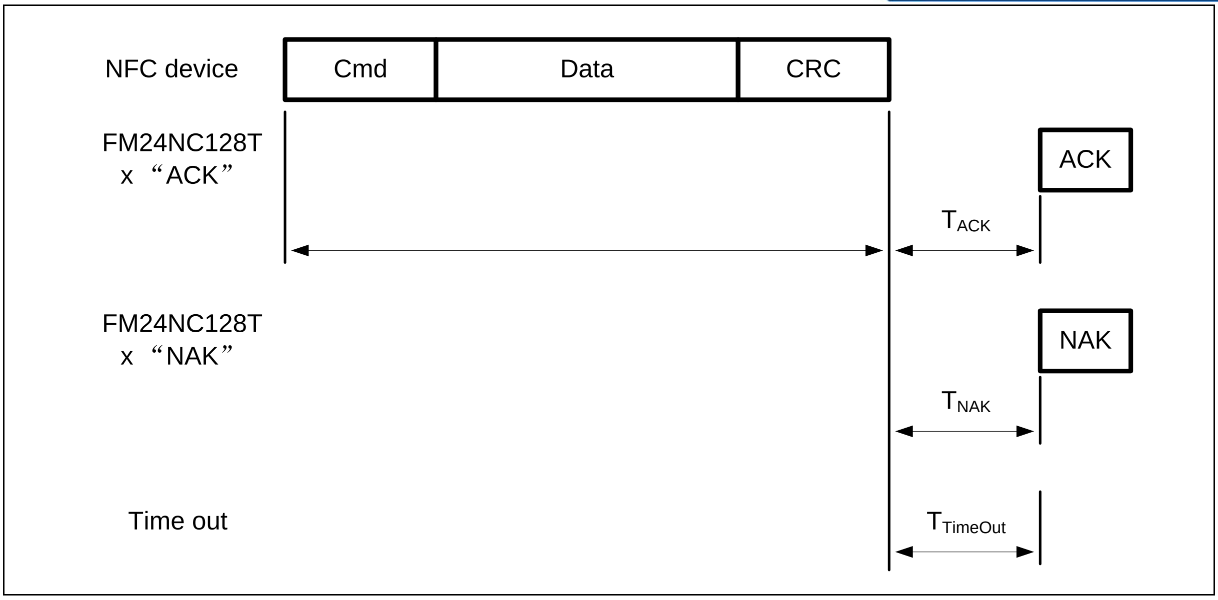


Figure 31 WRITE_RF_DATA_WR_LOCK command

Table 48 WRITE_RF_DATA_WR_LOCK command

Name	Code	Description	Length
Cmd	7Eh	write RF_DATA_WR_LOCK data	1 byte
Data	-	data	32 bytes
CRC	-	CRC	2 bytes
ACK	Ah	Acknowledge (ACK)	4 bit
NAK	see Table 25	see Section 9.3.1.3	4 bit

Table 49 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 (40h)

RF_DATA_RD_LOCK & RF_DATA_WR_LOCK in system memory 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 50.

Table 51 shows the required timing.

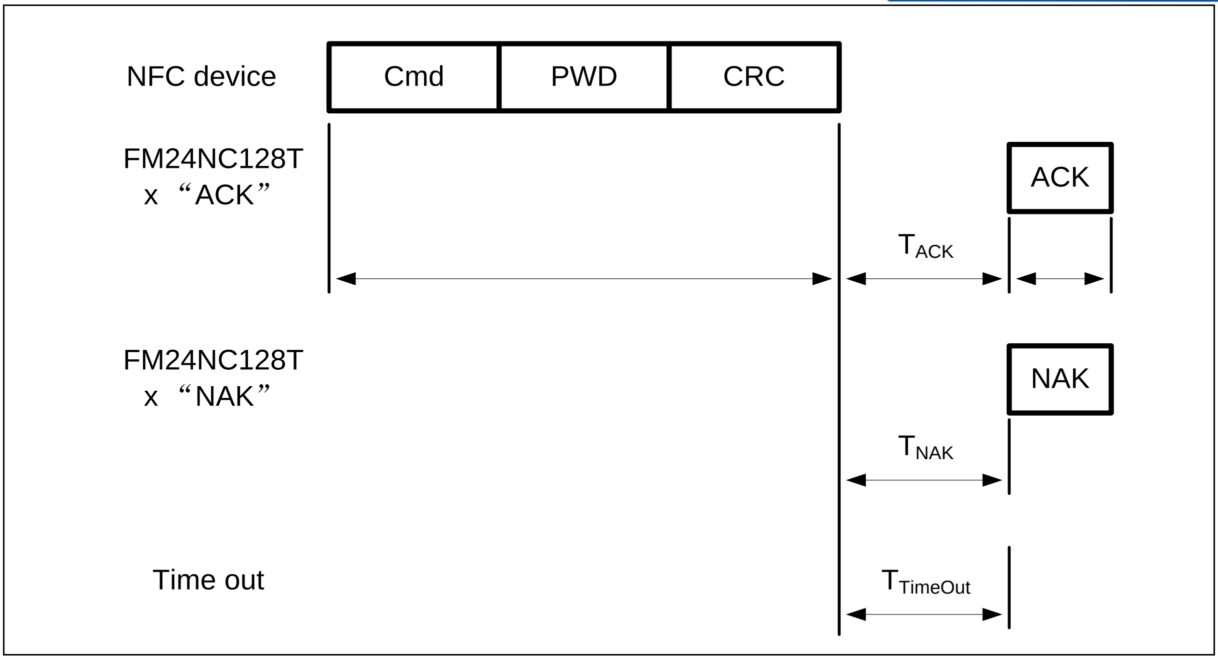


Figure 32 RF_PWD_AUTH command

Table 50 RF_PWD_AUTH command

Name	Code	Description	Length
Cmd	40h	RF password authentication	1 byte
PWD	-	RF_PWD	4 bytes
CRC	-	CRC	2 bytes
ACK	-	ACK	4 bit
NAK	see Table 25	see Section 9.3.1.3	4 bit

Table 51 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

FM24NC32Tx can be accessed by two wire serial (contact) interface or RF interface. If one interface accesses the device and the other keep silent, no collision occurs. But if both of the two interfaces access the device at same time, collision occurs and internal arbiter mechanism is necessary.

The internal arbiter mechanism gives two wire serial interface priority except for RF write cycle. That means if the device receives two wire serial interface command first, it does not respond to subsequent RF command until two wire serial operation is finished. If the device receives two wire serial interface command when RF command is in progress but internal write cycle has not been triggered, it will terminate RF operation and start two wire serial command procedure. But if internal write cycle of RF command has been triggered when receiving two wire serial command, the device will not respond to two wire serial command until write operation is finished.

Because two wire serial interface has priority, a timeout mechanism is applied to prevent RF communication freezing which refer to section 8.1.3.

EH_FD and RF WIP/RF BUSY 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 52 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 RF WIP/BUSY		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 53 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 54 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 55 DC characteristics of contact interface

Applicable over recommended operating range from: T_A = -40℃ to +85℃, V_{CC} = +1.6V to +5.5V, (unless otherwise noted).

Symbol	Parameter	Condition	Min	Typ	Max	Unit
I_{CC1}	Supply Current	V_{CC} = 5.5V, Read at 1MHz		0.4	1.0	mA
I_{CC2}	Supply Current	V_{CC} = 5.5V, Write at 1MHz		2.0	3.0	mA
I_{SB1}	Standby Current	V_{CC} = 1.6V, V_{IN} = V_{CC}/V_{SS}			1.0	μA
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 56 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

Symbol	Parameter	Min	Max	Unit
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 57 AC characteristics of contact interface

Applicable over recommended operating range from: T_A = -40℃ to +85℃, V_{CC} = +1.6V 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
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 58 characteristics of RF interface

Applicable over recommended operating range from: T_A = -40℃ to +85℃, V_{CC} = +1.6V 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_{FD}	Field detect output voltage		1.4	1.5	1.8	V
V_{EH1}	Energy harvesting output voltage	EH_VOUT=00		1.5		V

Symbol	Parameter	Condition	Min	Typ	Max	Unit
V_{EH2}	Energy harvesting output voltage	EH_VOUT=01		1.8		V
V_{EH3}	Energy harvesting output voltage	EH_VOUT=10		2.5		V
V_{EH4}	Energy harvesting output voltage	EH_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 32 TX -PP -C -H -OP

Company Prefix

FM = Fudan Microelectronics Group Co.,ltd

Product Family

24NC = NFC EEPROM

Product Density

32 = 32K-bit

Tag Density

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

Package Type (1)

SO = 8-pin SOP
TS = 8-pin TSSOP
DN = 8-pin TDFN (2x3mm)

Product Carrier

U = Tube
T = Tape and Reel

HSF ID Code

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

OPTION

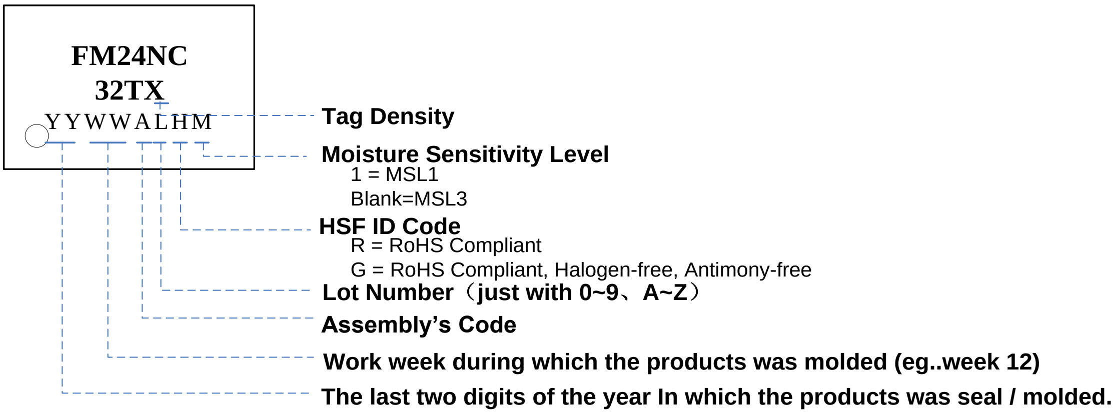
E3 = Enable energy harvesting function, output voltage 3.3V (Default)
F0 = Enable field detect function, output voltage 1.5V (Default)

Note:

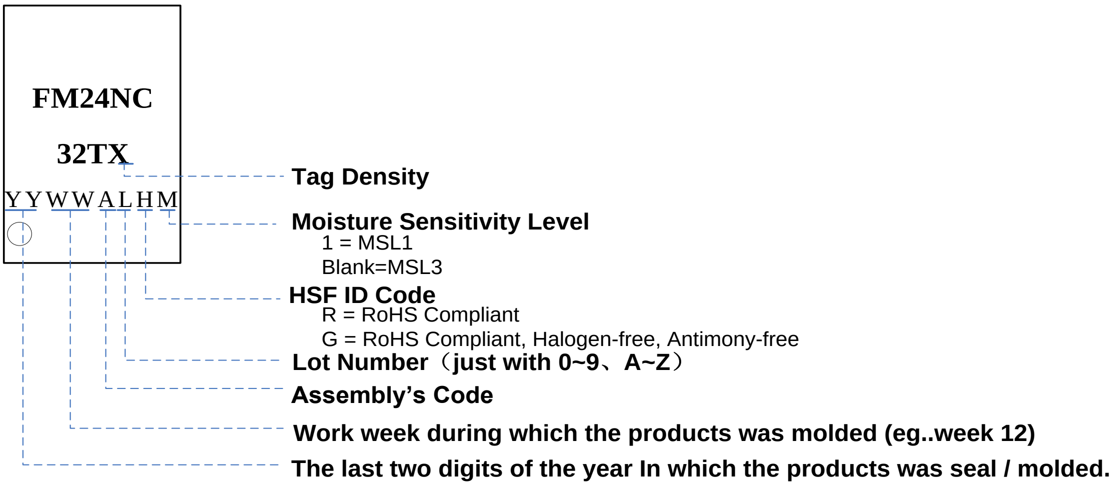
1. For SO, TS, DN package, MSL1 package are available, for detail please contact local sales office.

13 Part Marking Scheme

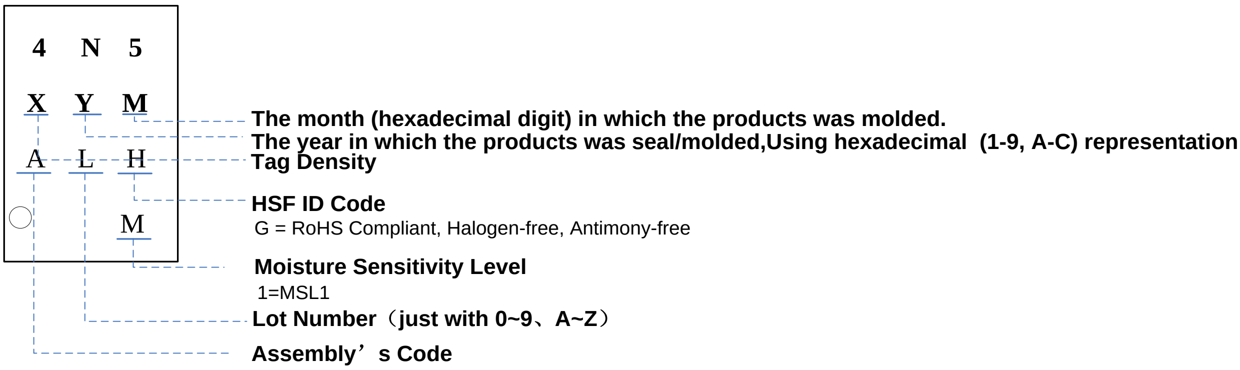
13.1 SOP8



13.2 TSSOP8

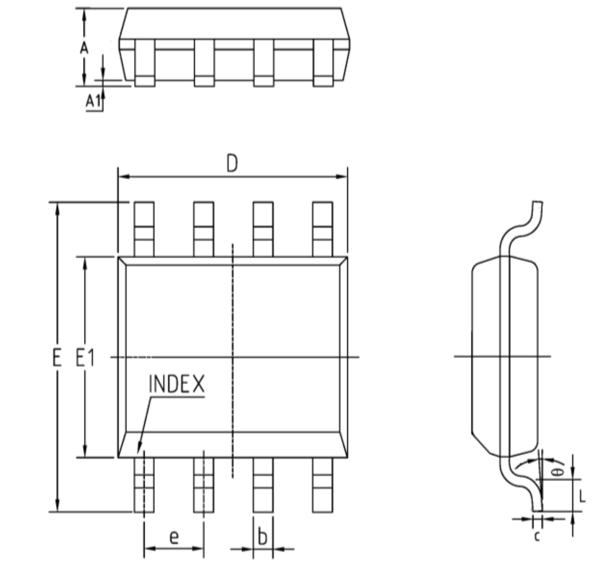


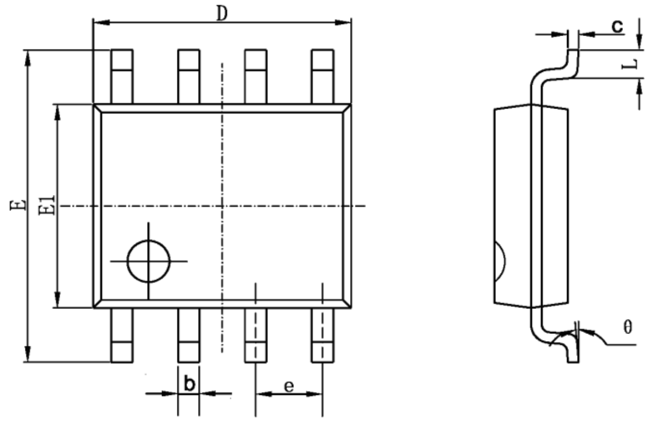
13.3 TDFN8 (2x3mm)



14 Packaging Information

SOP 8

(1)


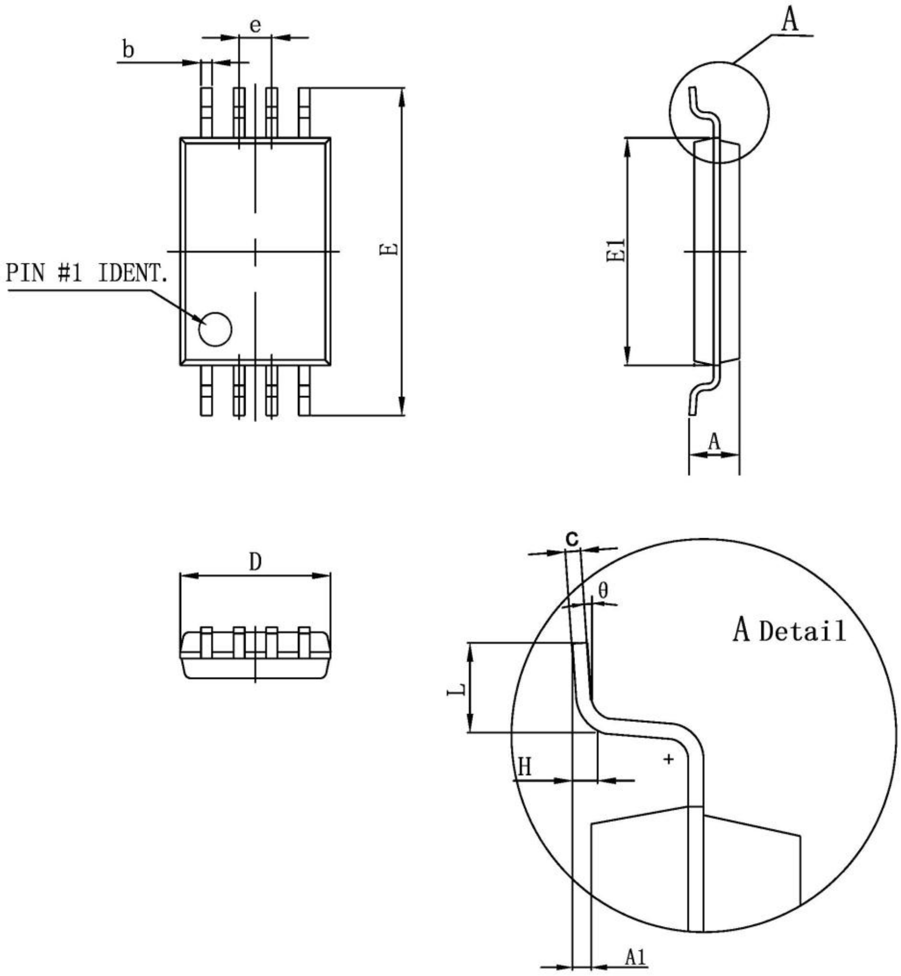
(2)


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.

TSSOP8

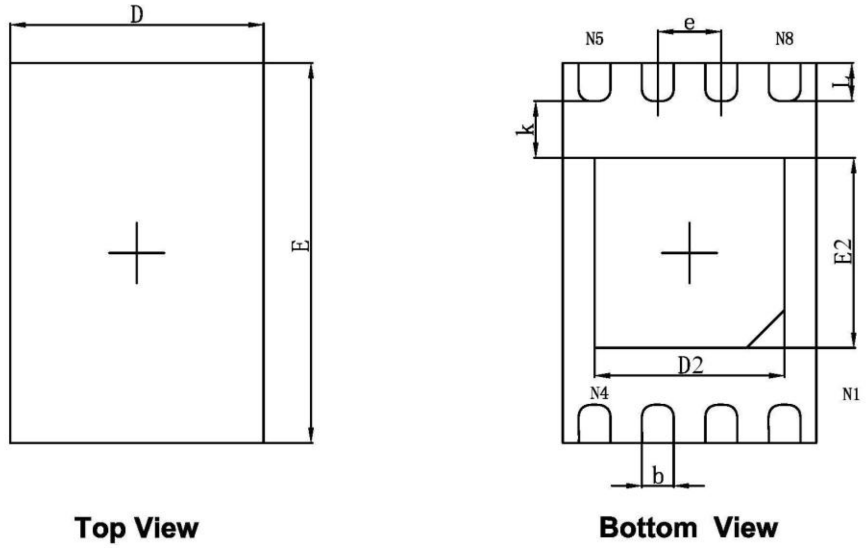


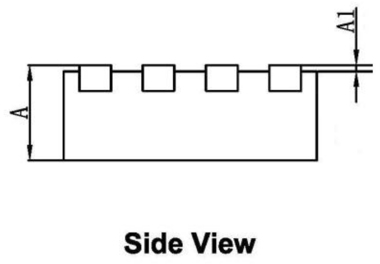
Symbol	MIN	MAX
D	2.900	3.100
E1	4.300	4.500
b	0.190	0.300
c	0.090	0.200
E	6.200	6.600
A		1.200
A1	0.050	0.150
e	0.650 (BSC)	
L	0.450	0.750
θ	0°	8°

NOTE:

1. Dimensions are in Millimeters.

TDFN8(2x3mm)





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	Mar. 2014	64	Initial Document Release.
1.0	Jun. 2014	64	1. Update ch.7.2.6. 2. Update ch.7.4.9. 3. Update ch.9.3.1.1
1.1	Dec. 2014	64	1. Removed TDFN8 Package offering 2. Added UDFN8 Package offering 3. Updated Features 4. Updated Figure2 and Table14
1.2	Oct. 2015	65	1. Add option in ordering information of 12 2. Add the default value of PIN_CFG, 7.4.8 3. Updated the Packaging Information.
1.3	Jun. 2017	64	1. Removed UDFN8 Package offering. 2. Added TDFN8 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 1889 (886-2) 7721 1890
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/