Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

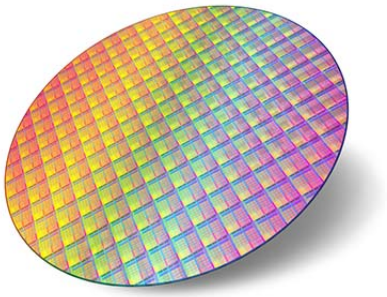
Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

ST25TA512

NFC Forum Type 4 Tag IC with 512-bit EEPROM

Datasheet - production data



Wafer (SB12I)

Description

The ST25TA512 device is an NFC tag IC.

It embeds an EEPROM memory, and can be operated from a 13.56 MHz RFID reader or an NFC phone.

The ST25TA512 is an NFC Forum Type 4 Tag; it communicates using the ISO/IEC 14443 Type A protocol.

Features

Contactless interface

- NFC Forum Type 4 Tag
- ISO/IEC 14443 Type A
- 106 Kbps data rate
- Internal tuning capacitance: 50 pF

Memory

- 64-byte (512 bits) EEPROM
- Supports NDEF data structure
- Data retention: 200 years
- Endurance: 1 million erase-write cycles
- Reads up to 64 bytes in a single command
- Writes up to 54 bytes in a single command
- Chaining capability
- 7-byte unique identifier (UID)
- 128-bit passwords protection
- 20-bit event counter with anti-tearing

Contents

List of tables

List of figures

1 Functional description

The ST25TA512 device is an NFC tag that can be accessed from the RF interface, based on the ISO/IEC 14443 Type A standard. The ST25TA512 is compatible with the NFC Forum Type 4 Tag specifications and supports all corresponding commands.

Figure 1 displays the block diagram of the ST25TA512 device.

Figure 1. ST25TA512 block diagram

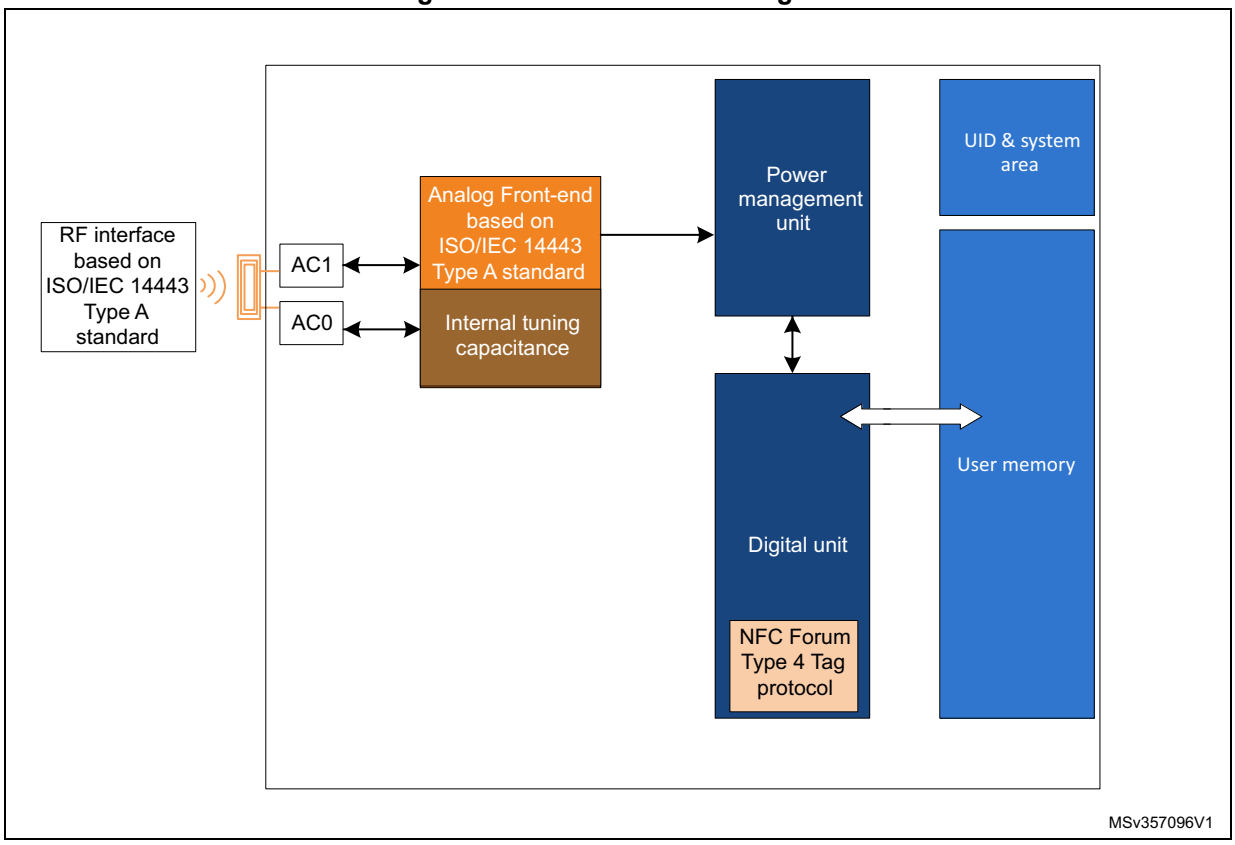


Table 1. Signal names

Signal name	Function	Direction
AC0, AC1	Antenna coils	-

1.1 Functional mode

The ST25TA512 has just one functional mode available (see *Table 2*).

Table 2. Functional mode

Mode	Supply source	Comments
Tag mode	RF field only	The RF interface operates only when RF field level is sufficient.

1.1.1 Tag mode

The ST25TA512 is supplied by the RF field and can communicate with an RF host (RFID reader or an NFC phone). The User memory can be accessed by the RF commands.

2 Signal descriptions

2.1 Antenna coil (AC0, AC1)

These inputs are used to connect the device to an external coil exclusively. It is advised not to connect any other DC or AC path to AC0 or AC1.

When correctly tuned, the coil is used to access the device using NFC Forum Type 4 commands.

3 ST25TA512 memory management

3.1 Memory structure

The ST25TA512 supports the NDEF Tag Application as defined in the NFC Forum Type 4 Tag. The ST25TA512 is composed of three files:

- One Capability Container file
- One NDEF file
- One System file: this file is an ST-proprietary file

The System file contains some information on the configuration of the ST25TA512 device. The CC file gives some information about the ST25TA512 itself and the NDEF file. The NDEF file contains the User data.

3.1.1 File identifier

The file identifier is the value used in the Select command to select a file.

Table 3. File identifier

File identifier	Meaning
0xE101	System file
0xE103	CC file
0x0001	NDEF file

3.1.2 CC file layout

The CC file gives some information about the ST25TA512 and the NDEF file. This file is a read-only file for the RF host and cannot be modified by issuing a write command.

The T field, Read Access and Write Access fields can be changed by the RF host by issuing a specific process (refer to *Section 7: Functional procedures*).

Table 4. CC file layout for 1 NDEF file

File offset	Meaning	Value	Comments
0x0000	Length CC file	0x000F	15 bytes
0x0002	Mapping version(1)	0x20 or 0x10	V 2.0 or V 1.0
0x0003	Maximum number of bytes that can be read	0x0040	64 bytes
0x0005	Maximum number of bytes that can be written	0x0036	54 bytes

Table 4. CC file layout for 1 NDEF file (continued)

File offset	Meaning	Value	Comments
0x0007	NDEF file control TLV	0x04 (2)	T field
0x0008		0x06	L field
0x0009		0x0001	FileID
0x000B		0x0040	Maximum NDEF file size in Bytes
0x000D		0x00 (2)	Read access
0x000E		0x00 (2)	Write access

1. According to the reader command format ST25TA512 will automatically align to the corresponding NFC Forum version.
2. Delivery state.

3.1.3 NDEF file layout

The NDEF file contains the NDEF message which contains the User data. The RF host can read and write data inside the file. The first two bytes named NDEF Message Length define the size of the NDEF message. The NDEF Message Length shall be managed by the application and the ST25TA512 device does not check if its value is relevant vs the data written by the RF host. The ST25TA512 device uses the NDEF Message Length, e. g. the standard read can be processed only inside the NDEF message; otherwise, the ST25TA512 device returns an error code. For more details about the read command, refer to *Section 5.6.7: ReadBinary command*.

Table 5. NDEF file layout

File offset	Byte 0	Byte 1	Byte 2	Byte 3
0x0000	NDEF Message Length		User data	User data
0x0004	User data	User data	User data	User data
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...
0x003C	...	...	...	User data

3.1.4 System file layout

The system file specifies the configuration of the ST25TA512. *Table 6* lists the different fields.

Table 6. Field list

File offset	Field name	No. of bytes	Read access	Write access	Delivery state
0x0000	Length system file	2	Yes	-	0x0012
0x0002	ST reserved	1	Yes	None	0x80
0x0003	Event Counter Config	1	Yes	Yes(1)	0x00
0x0004	20 bits counter (MS nibble 0x0)	3	Yes	None	0x000000
0x0007	Product version	1	Yes	None	0x13(2)
0x0008	UID	7	Yes	None	0x02E5 xx xx xx xx xx(3)
0x000F	Memory Size - 1	2	Yes	None	0x003F
0x0011	Product Code	1	Yes	None	0xE5

1. Configuration bytes can be locked by setting the Most significant bit to 1. Once locked, these bytes cannot be changed anymore.
2. ST reserved.
3. x values are defined by ST to ensure UID unicity.

Table 7. Details about the Counter config field

File offset	b7	b6-b2	b1	b0
0x0003	Counter config lock bit: 0b0: unlocked 0b1: locked	0b00000: ST reserved	Counter enable: 0b0: disable 0b1: enable	Counter increment: 0b0: on Read 0b1: on Write

3.2 Read and write access rights to the NDEF File

The NDEF file can be locked for read or write accesses. It is also protected by a 128-bit password that the host shall present before accessing the NDEF file. There are two 128-bit passwords, one for the read access and the other one for the write access.

An NDEF file can be permanently locked for read or write accesses. Thus, the host cannot access the NDEF file.

The read password shall be sent to the ST25TA512 device before reading a read-locked NDEF file.

The write password shall be present on the ST25TA512 device before writing a write-locked NDEF file. The write password shall be sent to change the read or write access. The read or write access right is defined for the NDEF file.

3.2.1 State of the Read and Write access rights

Two bytes in the CC file are used to define the Read and Write access rights to the NDEF file. For more details, refer to *Section 3.1.2: CC file layout*.

Table 8. Read access right

Value	Meaning
0x00	Read access without any security
0x80	Locked (1)
0xFE	Read not authorized

1. The read password shall be sent before reading in the NDEF file.

Table 9. Write access right

Value	Meaning
0x00	Write access without any security
0x80	Locked (1)
0xFF	Write not authorized

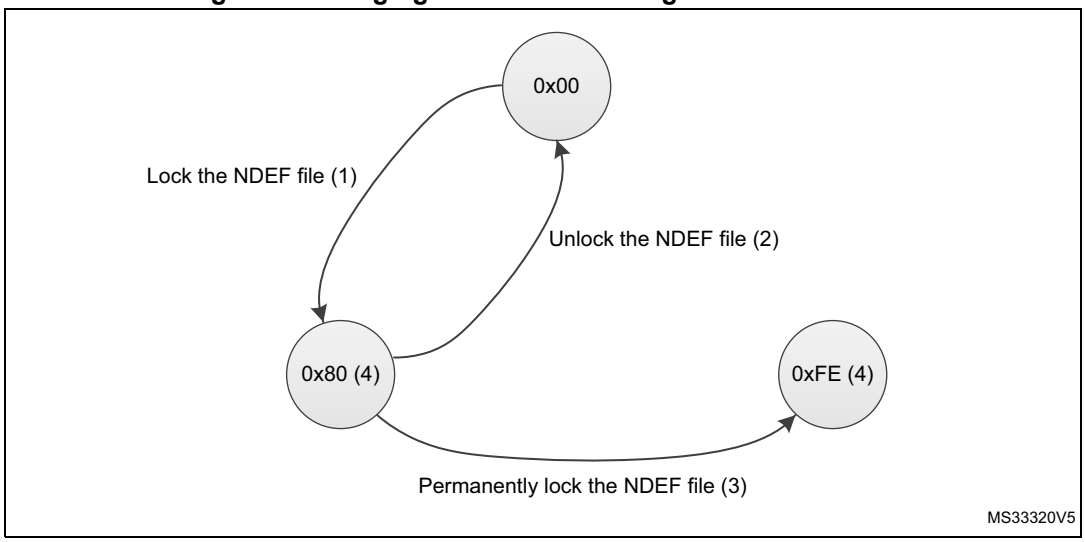
1. The write password shall be sent before writing in the NDEF file.

The state 0xFF and 0xFE cannot be changed by using the Read or Write passwords.

3.2.2 Changing the read access right to NDEF files

The state diagram of *Figure 2* shows how to change the access right to read an NDEF file.

Figure 2. Changing the read access right to an NDEF file

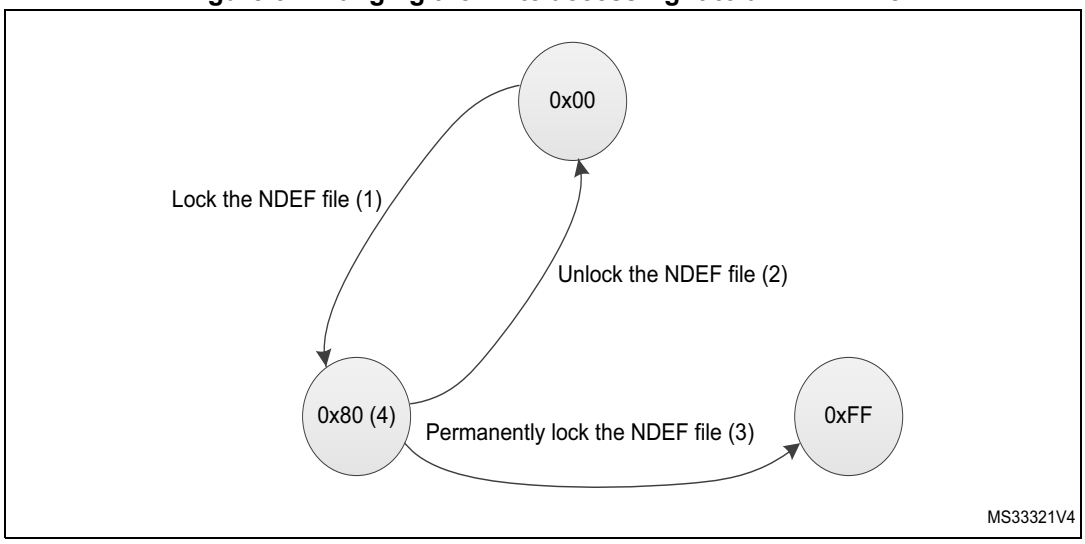


1. See the procedure to lock the read access (*Section 7.4: Locking an NDEF file*).
2. See the procedure to unlock the read access (*Section 7.5: Unlocking an NDEF file*).
3. See the procedure to permanently lock the read access (*Section 7.6: Reaching the read-only state for an NDEF file*).
4. Proprietary state, not defined by NFC Forum Type 4 Tag.

3.2.3 Changing the write access right to NDEF files

The state diagram on *Figure 3* shows how to change the write access right to an NDEF file.

Figure 3. Changing the write access right to an NDEF file



1. See the procedure to lock the write access.
2. See the procedure to unlock the write access.
3. See the procedure to permanently lock the write access (*Section 7.6: Reaching the read-only state for an NDEF file*).
4. Proprietary state, not defined by NFC Forum Type 4 Tag.

3.3 Access right life time

The access right life time is validated while the NDEF file is selected or until the end of the RF session. Once the read or write access right is granted, the host can send one or more ReadBinary or UpdateBinary commands.

At the end of a session or when the host selects another file, the read and write access rights are initialized.

3.4 NDEF file passwords

The NDEF file passwords protect the read or write access from an RF interface from/to an NDEF file.

Two NDEF file passwords are available for each NDEF file:

- Read password
- Write password

The length of a password is 128 bits (16 bytes).

Note: The delivery state for all passwords = 0x00000000000000000000000000000000.

3.5 Read/Write counter

A 20 bits counter can track the read or write events on the NDEF file.

It benefits from an anti-tearing mechanism, that ensures the consistency of the counter, even if there has been an electrical problem during its increment.

The value of the Read/Write counter can be checked by any application, by reading suitable bytes in System file (see *Section 3.1.4*).

If enabled, the Read/Write counter will be incremented on first event (exclusively Read or Write) which is performed on the NDEF File, inside an RF session (an RF session is entered when ST25TA512 receives a valid "Select Application" command).

The counter is reset when it is disabled.

Apart from these procedures, there is no way to act on the value of this counter.

The Read/Write counter can be configured through a specific byte in System file (see *Section 3.1.4*).

This configuration byte allows to:

- Enable or disable this counter
- Define if the counter must be incremented on a read or write sequence
- Definitively lock this configuration byte

Warning: Once this configuration byte is locked, it cannot be changed anymore: the counter will behave accordingly.

If enabled, the Read/Write counter will have an impact on the execution time of the event which is countered: the counter increment needs some write cycles of specific EEPROM cells automatically managed by ST25TA512, which increase the total time before the response is sent to the reader.

As a consequence, an S(WTX) request can be issued on the command that will increment the counter (see *Section 5.4: S-Block format*).

4 Communication mechanism

This section describes the principle of communication between an RF host and the ST25TA512 device.

4.1 Master and slave

The ST25TA512 acts as a slave device on the RF channel and therefore waits for a command from the RF host before sending its response.

The RF host shall generate the RF field and the RF commands.

5 RF command sets

This section describes the ST25TA512 command sets that can be issued by the RF host.

There are three command families:

- the NFC Forum Type 4 Tag command set
- the ISO/IEC 7816-4 command set
- the proprietary command set

The NFC Forum Type 4 Tag command set and the ISO/IEC 7816-4 command set use the I-Block format. For more details about the I-Block format, refer to *Section 5.2: I-Block format*.

Two other command formats exist:

- the commands using the R-Block format
- the commands using the S-Block format

For more details about these formats, refer to *Section 5.3: R-Block format* and to *Section 5.4: S-Block format*.

This section gives a brief description of the RF host commands. The format of these command sets is the I-Block format.

Table 10 lists the RF command sets.

Table 10. RF command sets

Family command set	Command name	Class byte	Instruction code	Brief description
NFC Forum Type 4 Tag	NDEF Tag Application Select	0x00	0xA4	NDEF Tag Application Select
	CC select	0x00	0xA4	Selects the CC file
	NDEF select	0x00	0xA4	Selects the NDEF file
	System select	0x00	0xA4	Selects the system file
	ReadBinary	0x00	0xB0	Reads data from file
	UpdateBinary	0x00	0xD6	Writes or erases data to a NDEF file
ISO/IEC 7816-4	Verify	0x00	0x20	Checks the right access of a NDEF file or sends a password
	ChangeReferenceData	0x00	0x24	Changes a Read or write password
	EnableVerificationRequirement	0x00	0x28	Activates the password security
	DisableVerificationRequirement	0x00	0x26	Disables the password security
ST proprietary	EnablePermanentState	0xA2	0x28	Enables the Read Only or Write Only security state
	ExtendedReadBinary	0xA2	0xB0	Reads data from file
	UpdateFileType	0xA2	0xD6	Sets file type to NDEF or proprietary

5.1 Structure of the command sets

The exchange of data between the RF host and the ST25TA512 uses three kinds of data formats, called blocks:

- I-Block (Information block): to exchange the command and the response
- R-Block (Receive ready block): to exchange positive or negative acknowledgment
- S-Block (Supervisory block): to use either the Deselect command or the Frame Waiting eXtension (WTX) command or response

This section describes the structure of I-Block, R-block and S-Block. This format is used for the application command set.

5.2 I-Block format

The I-Block is used to exchange data between the RF host and the ST25TA512. It is composed of three fields. *Table 11* details the I-Block format.

Table 11. I-Block format

Name	SoD		Payload	EoD
	PCB	DID	-	CRC
Length	1 byte	1 byte	1 to 251 bytes	2 bytes
PCB field				
DID field (optional)				
RF host to ST25TA512: C-APDU ST25TA512 to RF host: R-APDU				
2 CRC bytes				

Table 12. PCB field of the I-Block format

	b7-b6	b5	b4	b3	b2	b1	b0
	0b00	0	0	X	0	1	X
I-Block							
RFU							
Must be set to 0							
DID field is present, if bit is set							
Must be set to 0							
Must be set to 1							
Block number(1)							

1. Follow ISO 14443_4 Block numbering rules (see note)

Note: Block numbering rules:

Reader rules:

Rule A: The Reader block number shall be initialized to 0.

Rule B: When an I-block or an R(ACK) block with a block number equal to the current block number is received, the Reader shall toggle the current block number before optionally sending a block to the ST25TA512.

ST25TA512 rules:

Rule C. The ST25TA512 block number shall be initialized to 1 at activation.

Rule D. When an I-block is received, the ST25TA512 shall toggle its block number before sending a block.

Note: The ST25TA512 may check if the received block number is not in compliance with Reader rules to decide neither to toggle its internal block number nor to send a response block.

Rule E. When an R(ACK) block with a block number not equal to the current ST25TA512 block number is received, the ST25TA512 shall toggle its block number before sending a block.

Note: There is no block number toggling when an R(NAK) block is received.

When the RF host sends a command to the ST25TA512 the format of the payload is the C-APDU.

When the ST25TA512 sends a command to the RF host, the format of the payload is the R-APDU.

5.2.1 C-APDU: payload format of a command

The C-APDU format is used by the RF host to send a command to the ST25TA512. *Table 13* describes its format.

Table 13. C-APDU format

Name	Payload field						
	CLA	INS	P1	P2	L_C	Data	Le
Length	1 byte	1 byte	1 byte	1 byte	1 byte	Lc byte	1 byte
Class byte - 0x00: standard command - 0xA2: ST command(1)							
Instruction byte							
Param Byte 1							
Param Byte 2							
Number of bytes of the Data field							
Data bytes							
Number of bytes to be read in the ST25TA512 memory							

1. See *Table 10*

5.2.2 R-APDU: payload format of a response

the ST25TA512 uses the I-Block format to reply to a command which used the I-Block format. This format is described in *Table 14*.

Table 14. R-APDU format

Name	Payload field		
	Data (optional)	SW1	SW2
Length	Le byte	1 byte	1 byte
Data			
Status byte 1			
Status byte 2			

5.3 R-Block format

The R-Block is used to convey positive or negative acknowledgment between the RF host and the ST25TA512.

Table 15. R-Block format

NFC frame	SoD		-	EoD
	PCB	DID	Payload	CRC
Length	1 byte	1 byte	0 byte	2 bytes
R(ACK) without the DID field: 0xA2 or 0xA3 R(ACK) with the DID field: 0xAA or 0xAB R(NAK) without the DID field: 0xB2 or 0xB3 R(NAK) with the DID field: 0xBA or 0xBB				
DID field (optional)				
-				
2 CRC bytes				

There are two kinds of R-Blocks:

- R(ACK): the acknowledgment block sent by the RF host or by the ST25TA512
- R(NAK): the non-acknowledgment block sent by the RF host

Table 16. R-Block detailed format

	b7-b6	b5	b4	b3	b2	b1	b0
	0b10	1	X	X	0	0	X
R-Block							
Must be set to 1.							
0: NAK 1: ACK							
0: DID field is not present 1: DID field is present							
Must be set to 0							
Must be set to 0							
Block number							

5.4 S-Block format

The S-Block is used to exchange control information between a reader and a contactless tag.

Table 17. S-Block format

NFC frame	SoD		-	EoD
	PCB	DID	Payload	CRC
Length	1 byte	1 byte	1 byte	2 bytes
0xC2: for S(DES) when the DID field is not present 0xCA: for S(DES) when the DID field is present 0xF2: for S(WTX) when the DID field is not present 0xFA: for S(WTX) when the DID field is present				
DID field (optional)				
WTX field (optional)(1)				
2 CRC bytes				

1. This field is present when b5-b4 bits are set to 0b11 (S-Block is a WTX). see *Table 18: S-Block detailed format*.

There are two requests using the S-Block format:

- S(DES): the deselect command
- S(WTX): the Waiting Frame eXtension command or response.

  A Waiting Time eXtension request occurs in RF when the operating time needed by ST25TA512 is greater than 19.2 ms.

  The WTX field indicates the increase time factor to be used in this command execution (FDTtemp = WTX * 19.2 ms). WTX depends on FWI.

Table 18. S-Block detailed format

	b7-b6	b5-b4	b3	b2	b1	b0
	0b11	X	X	0	1	0
S-Block						
0b00: Deselect 0b11: WTX						
0: DID field is not present 1: DID field is present						
Must be set to 0						
Must be set to 1						
Must be set to 0						

Note: After receiving the deselect command, the session is released and ST25TA512 enters the Standby power mode.

*In response to a RATS command, ST25TA512 returns FWI parameter (default frame waiting time used); when ST25TA512 needs more time for a command execution, it requests a frame waiting time extension by responding 0xF2 0xWTX (Request waiting time = FWI * WTX). If the reader accepts ST25TA512 request, it acknowledges by sending the command 0xF2 0xWTX. The frame waiting time becomes FWI * WTX for the current command only.*

5.5 CRC of the RF frame

The two CRC bytes check the data transmission between the RF host and the ST25TA512. For the RF frame, the CRC is computed on all the data bits in the frame, excluding parity bits, SOF and EOF, and the CRC itself.

The CRC is as defined in ISO/IEC 13239. The initial register content shall be 0x6363 and the register content shall not be inverted after calculation.

5.6 NFC Forum Type 4 Tag protocol

5.6.1 Commands set

ST25TA512 command set is built to easily support the NFC Forum Type 4 Tag protocol.

Table 19. Command set overview

Command name	Brief description
NDEF Tag Application Select	Select the NDEF Tag Application
Capability Container Select	Select the capability container (CC) file using the Select command
NDEF Select	Select the NDEF file using the Select command.
System File Select	Select the system file using the Select command.
ReadBinary	Read data from a file
UpdateBinary	Write new data to a file

5.6.2 Status and error codes

This section lists the status and the error code of the ST25TA512.

Table 20. Status code of the ST25TA512

	SW1	SW2	Comment
Value	0x90	0x00	Command completed successfully