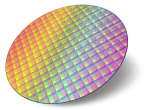
ST25TA-E

Data brief

NFC Type 4/RFID tag IC with up to 2.0 Kbits flash, trusted product authentication and digitization



Product status link
ST25TA-E

Product summary	
Temperature range	-25 °C to 85 °C
Package	Bumped and sawn inkless wafer

Features

Includes state-of-the-art patented technology

Contactless interface

- Compliant with ISO/IEC 14443 Type A
- NFC Forum Type 4 tag certified by the NFC Forum
- Up to 106 kbps data-rate
- Internal tuning capacitance: 68 pF +/- 4 pF

Memory

- Up to 2048 bits (256 bytes) of user flash memory
- Support NDEF data structure
- Data retention: 25 years
- Minimum endurance: 500 k write cycles
- Page erase time down to 0.8 ms
- Chaining capability
- Augmented NDEF (contextual automatic NDEF message)
- 4-digit unique tap code
- 24-bit general purpose counter with antitearing

Data protection

- Permanent lock file protection for read/write access
- 64-bit password-based file protection for read/write access with diagnosis and mitigation services.

Chip identification and protection

- 7-byte unique identifier (UID)
- TruST25 digital signature (off-chip ECDSA)

Product authentication and digitization

- Up to 2-slot secure key storage
- Edge TruST25 digital signature (on-chip ECDSA)
- Compliant with blockchain-backed evidence of authenticity

Security features

- SESIP level 1 certified, with Physical Attacker Resistance
- Active shield and protection against state-of-the-art attacks
- A unique serial number on each die

Privacy

- Scalable NFC-enabled privacy modes
  - Kill mode and anonymous with untraceable UID (fixed or random ID)
  - Configurable kill mode for permanent deactivation of the tag

1 Description

The ST25TA-E devices are NFC/RFID tag ICs with solid security and privacy features.

The ST25TA-E devices hold a unique off-chip generated digital signature through TruST25 (a set of software and procedures) used to prove the origin of the chip UID in identification detection.

The ST25TA-E devices also generate on-chip digital signatures dynamically through Edge TruST25 services to prove the origin of the product in ownership detection and associated data. They also embed custom certificates for enrollment verification.

The Augmented NDEF feature is an automatic contextual NDEF message service that allows tags to react to dynamic content without user interaction.

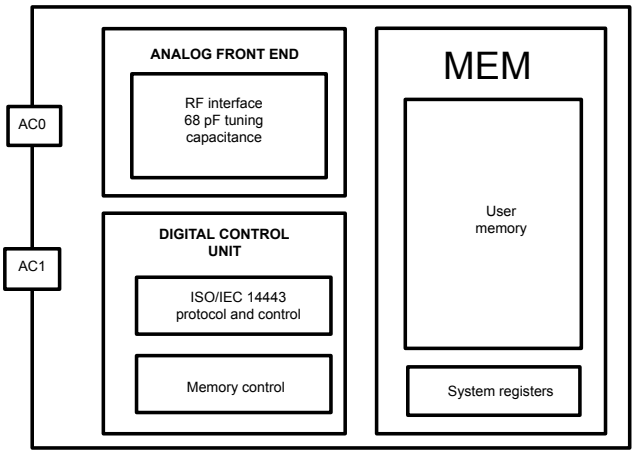
The ST25TA-E devices have a configurable flash memory with 25 years of data retention and work with a 13.56 MHz short range RFID reader or an NFC phone.

The contactless interface is compliant with the ISO/IEC 14443 standard and NFC Forum Type 4 tag specification.

1.1 Block diagram

The ST25TA-E devices are depicted in the following block diagram:

Figure 1. ST25TA-E block diagram



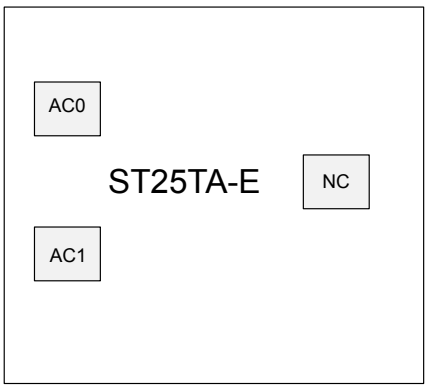
1.2 Package connections

The ST25TA-E devices are provided in one delivery form: sawn and bumped wafer.

Table 1. ST25TA-E signal names

Signal name	Function	Direction
AC0	Antenna coils	in-out
AC1	Antenna coils	in-out

Figure 2. **ST25TA-E die connection for sawn and bumped wafer**



DT73964V1

2 Signal descriptions

2.1 Antenna coil (AC0, AC1)

These inputs are used to connect the ST25TA-E device to an external coil exclusively. It is advised not to connect any other DC or AC path to neither AC0 nor AC1.

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

3 Memory management

The ST25TA-E devices are organized as a file system, and they support the NDEF tag application as defined in the NFC Forum Type 4 tag specification. The ST25TA-E devices are composed of several files:

- CC (capability container) file
- NDEF file
- ANDEF file: an ST proprietary file.

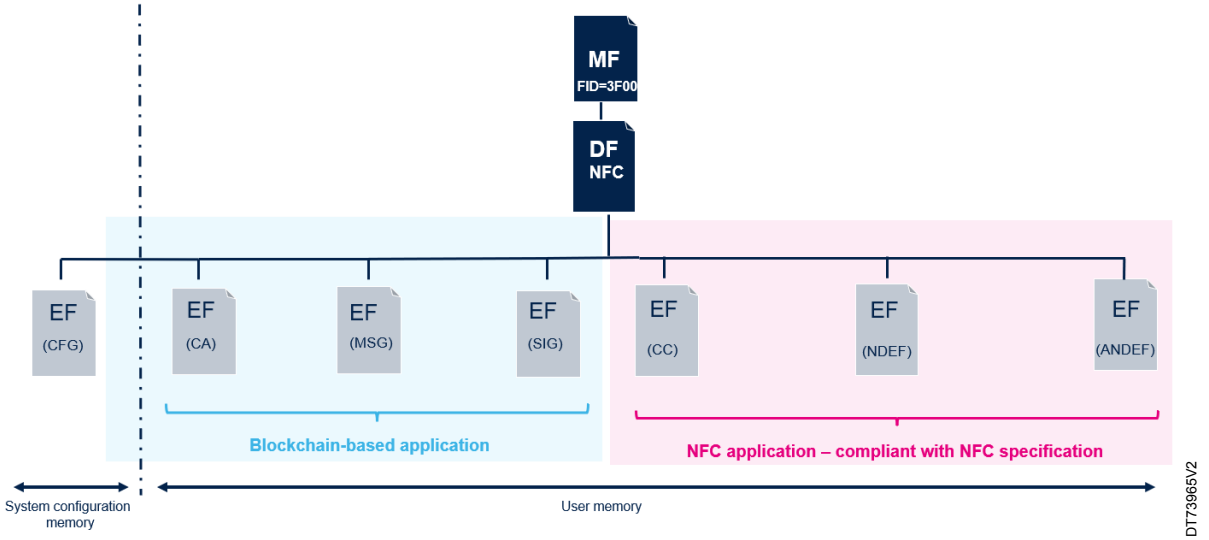
The CC, NDEF, and ANDEF files are dedicated to the NDEF tag application.

Other elementary files that are not included into the CC file are defined as ST proprietary files, and are dedicated to the TruST25 and Edge-TruST25 services and ST25TA-E programmable services:

- MSG file
- SIG file
- CA file
- CFG file

A configuration file provides some information for handling the main features. The CFG file is located into the system configuration memory. The NDEF tag application and the TruST25 and Edge-TruST25 services or configuration files reside under the NFC application DF file. The MF master file is the root of the file system.

Figure 3. ST25TA-E file system organization



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

Table 2. File identifier

File identifier	Meaning
0xE101	CFG file
0xE103	CC file
0xE104	NDEF file
0xE105	ANDEF file
Other identifiers	Contact your STMicroelectronics sales officer for more information.

Selecting the NDEF tag application with a specific AID (application identifier) handles most of the commands, which are authorized in the SELECTED APP state. Refer to Section 5.2: State machine.

Selecting the MF file handles a few commands, authorized in the PROTOCOL state. Refer to Section 5.2: State machine.

Note: In PROTOCOL and SELECTED APP states, the ST25TA-E behaves in accordance with the ISO/IEC 14443-4 part. The ST25TA-E devices exit from PROTOCOL state and enter SELECTED APP state when a valid `SelectApplication` *command is successfully received.*

The table below lists the elementary files located in the user memory and the CFG file located in the system configurartion memory. They are accessed with the `UpdateBinary` and `ReadBinary` commands.

Table 3. List of user files

File name	Access rights
CFG file	read/write
CC file	read only
NDEF file	read/write
ANDEF file	read/write
CA file	Contact your STMicroelectronics sales officer for more information.
MSG file	
SIG file	

On factory delivery, the file system is not protected. Passwords can be setup to protect read and/or write access to elementary file, except for the CC file that is always readable. Most of the elementary files can have individual read and/or write access permissions. Refer to Section 4.1: File protection.

3.1 CC (capacity container) file layout

The CC file gives some information about the ST25TA-E and the NDEF or ANDEF files. This file is a read-only file for the RF host and cannot be modified by issuing an `UPDATE_BINARY` command.

Table 4. CC file layout

File offset	Meaning	Value	Comments
0x0000	Length CC file	0x0017	-
0x0002	Mapping version	0x20	Version 2.0
0x0003	MIe: Maximum number of bytes that can be read	0x00FF	-
0x0005	MIc: Maximum number of bytes that can be written	0x0075	-
0x0007	NDEF file control TLV	0x04	T Field
0x0008		0x06	L Field
0x0009		0xE104	File ID
0x000B		0x0100	FLEN: Maximum NDEF file size in bytes
0x000D		0x00	Read access permission
0x000E		0x00	Write access permission
0x000F	ANDEF file control TLV	0x05	T Field
0x0010		0x06	L Field
0x0011		0xE105	File ID
0x0013		0x002C	FLEN: Maximum ANDEF file size in bytes
0x0015		0x00	Read access permission
0x0016		0x00	Write access permission

3.2 NDEF file layout

The NDEF file provides the NDEF message that contains user data. The RF host can read and write data. The first two bytes, named *NDEF message length*, define the size of the NDEF message.

Table 5. NDEF file layout

File offset	Field	Meaning
0x0000	NLEN	NDEF message length
0x0002	User data	NDEF message
…		
…		
…		
0x00FF		

Note: The NLEN gives the size of the NDEF message (up to 0x00FE).

3.3 ANDEF file layout

The ANDEF file provides the ANDEF custom message that contains user data for Augmented NDEF support. The RF host can read and write data. The first two bytes, named *ANDEF message length*, define the size of the ANDEF message.

Table 6. ANDEF file layout

File offset	Field	Meaning
0x0000	ANLEN	ANDEF message length
0x0002	User data	ANDEF message
…		
…		
…		
…		
0x002B		

Note: ASCII valid values should be used into the ANDEF message.

Note: The ANLEN gives the size of the message (0x002A).

3.4 CA file layout

The CA file is used by the Edge-TruST25 services. For further information, contact your STMicroelectronics sales officer.

3.5 MSG file layout

The MSG file is used by the TruST25 and Edge-TruST25 services. For further information, contact your STMicroelectronics sales officer.

3.6 SIG file layout

The SIG file is used by the TruST25 and Edge-TruST25 services. For further information, contact your STMicroelectronics sales officer.

3.7 CFG file layout

The CFG file specifies the configuration of the ST25TA-E devices. The RF host can read and may write configuration register fields: configuration fields can either be RFU, read-only, or read and write. The first two bytes, named *CFG message length*, define the size of the CFG configuration fields.

Table 7. CFG file layout

File offset	Field	Meaning
0x0000	CFGLEN	CFG message length
0x0002	RFU	00h…00h
….		...
0x0007		00h…00h
0x0008	System data	Configuration register field
…		
…		
….		

In addition to the user memory including all previous EF files, the system configuration memory includes the CFG EF file, where a set of registers are located. Registers are read during the boot sequence and define the basic ST25TA-E behavior.

The table below lists the configuration registers of the ST25TA-E device. They are accessed with the `UpdateBinary` and `ReadBinary` commands.

Depending on the configuration register, when its content is updated during an RF session, the effect of the new value is activated either immediately or at the start of the next RF session.

Register information stored in the CFG EF file is structured as follows (MSB first):

Table 8. List of configuration registers

Name	Offset	Bytes	Access type	Activation time(1)	Section
CFG_UID	0008h	7	Read only	-	Refer to Section 6.1: Product identifier: Unique identifier (UID)
CFG_MEM_SIZE	000Fh	2	Read only	-	Refer to Section 6.3: Product information
CFG_IC_REF	0011h	1	Read only	-	
CFG_PRIV_NUID	0012h	3	Read write	B	Refer to Section 4.7.2: Anonymous mode description
CFG_PRIV	0015h	1	Read write	B	
CFG_GP_CNT_LIMIT	0016h	3	Read write	I	Refer to Section 4.6.1: Remote monitoring
CFG_GP_CNT_CFG	0019h	1	Read only, write (once)	I	
CFG_GP_CNT_OFFSET_ADD	001Ah	2	Read write	I	
CFG_GP_CNT_EN	001Ch	3	Read write	B for CFG_GP_CNT EN[23] I for CFG_GP_CNT_EN[22:0]	
CFG_ANDEF_BYTE_OFFSET	001Fh	1	Read write	B	Refer to Section 4.3: Augmented NDEF feature (ANDEF)
CFG_ANDEF_CFG	0020h	1	Read write	I	
CFG_ANDEF_SEP	0021h	1	Read write	I	
CFG_ANDEF_DIAG_CFG	0022h	1	Read write	I	
CFG_ANDEF_EN	0024h	1	Read write	B	
CFG_PWD_LOCK	002Dh	3	Read only, write (once)	I	Refer to Section 4.2.2: Permanent password lock

1. *'I' means Immediate, 'B' means on the next RF boot.*

Note: The `UpdateBinary` command may execute burst write access only if all registers to be written are tagged as "writable-ready". If one register in the burst is tagged as RO or RFU (refer to Table 7, address range [0x0002:0x0007]), no update is performed and the whole burst write operation is aborted. Registers tagged "write once" or "write (once)" may be included into a burst since they are masked automatically by the ST25TA-E device. Note that the tag "write once" is applied on all the bits of a field into a register whereas the tag "write (once)" is applied on some bits of the field into a register.

Note: Authorization and value validity are checked during the update operation for each register. If the verification failed, the whole burst write is aborted.

4 Specific features

4.1 File protection

Each elementary file can have individual read and/or write access permissions to prevent unauthorized reading from or writing to a file.

The ST25TA-E devices support a lock feature that provides read and write protection of each elementary file in user and/or system configuration memory; the lock feature can be permanent or reversible.

- The permanent lock file mechanism that permanently changes the memory content to be readable or writable and makes it impossible to read or change the content after it has been written. This is achieved by changing the file permissions. The effect of a permanent lock file operation cannot be reverted.
- The reversible lock file protection mechanism is based on password-based authentication. This mechanism can restrict use of some ST25TA-E features/commands and prevent read and/ or write access to data stored in each elementary file of user or system configuration memory.

4.1.1 Permanent lock file protection

Each EF file, except the CC file, can be individually locked in read or write access from each other with the `EnablePermanentRequirement` command. Thus, data in the locked EF file cannot be accessed (permanent state):

- A write-protect lock command prevents the content of a file from being altered.
- A read-protect lock command prevents any user from reading or accessing the data in the file.

Table 9. Lis of permanent read/write lock protection

File name	Permanent read lock	Permanent write lock
CFG file	yes	yes
CC file	n/a	n/a
NDEF file	yes	yes
ANDEF file	yes	yes
MSG file	For further information, contact your STMicroelectronics sales officer.	
SIG file		
CA file		

The effect of a permanent lock file operation cannot be reverted.

Note: Open or close a security session is still possible even if permanent lock protection is enabled for a file.

Note: The permanent write CFG lock protection prevents the access to the configuration registers of the CFG file. It also prevents disabling the reversible lock of any file.

4.1.2 Reversible lock file protection

The ST25TA-E devices provide reversible protection using the password protection for user and system configuration elementary files.

Table 10. List of read/write password protection

File name	Reversible read lock	Reversible write lock
CFG file	yes	yes
CC file	n/a	n/a
NDEF file	yes	yes
ANDEF file	yes	yes
MSG file	For further information, contact your STMicroelectronics sales officer.	
SIG file		
CA file		

Each EF file can be individually locked (respectively unlocked) from each other with the `Enable VerificationRequirement` command (respectively `DisableVerficationRequirement` command) in read and/or write access.

Once enabled, access to data into a file is controlled by a security session based on passwords. On successful (respectively failed) presentation of a password, a security session is open (respectively not open or closed) and grants (respectively denies) access to the protected files.

Table 11. Security session type

Security session	Open by presenting	Rights granted when the session is open
CFG file	PWD_CFG_WR	Write access to configuration registers of CFG file. Enable/disable reversible lock of any file. Enable permanent lock of any file. Revert GP counter. Check CFG write lock status. Update PWD_CFG_WR value.
	PWD_CFG_RD	Read access to configuration registers of CFG file. Check CFG lock status. Update PWD_CFG_RD value.
NDEF file	PWD_NDEF_WR	Write access to NDEF file. Check NDEF write lock status. Update PWD_NDEF_WR value.
	PWR_NDEF_RD	Read access to NDEF file. Check NDEF read lock status. Update PWD_NDEF_RD value.
ANDEF file	PWD_ANDEF_WR	Write access to ANDEF file. Check ANDEF write lock status. Update PWD_ANDEF_WR value.
	PWD_ANDEF_RD	Read access to ANDEF file. Check ANDEF read lock status. Update PWD_ANDEF_RD value.

Once enabled, the status of the protection can be retrieved by issuing a `Verify` command and by decoding sw1-sw2 status, as mentioned in the previous section.

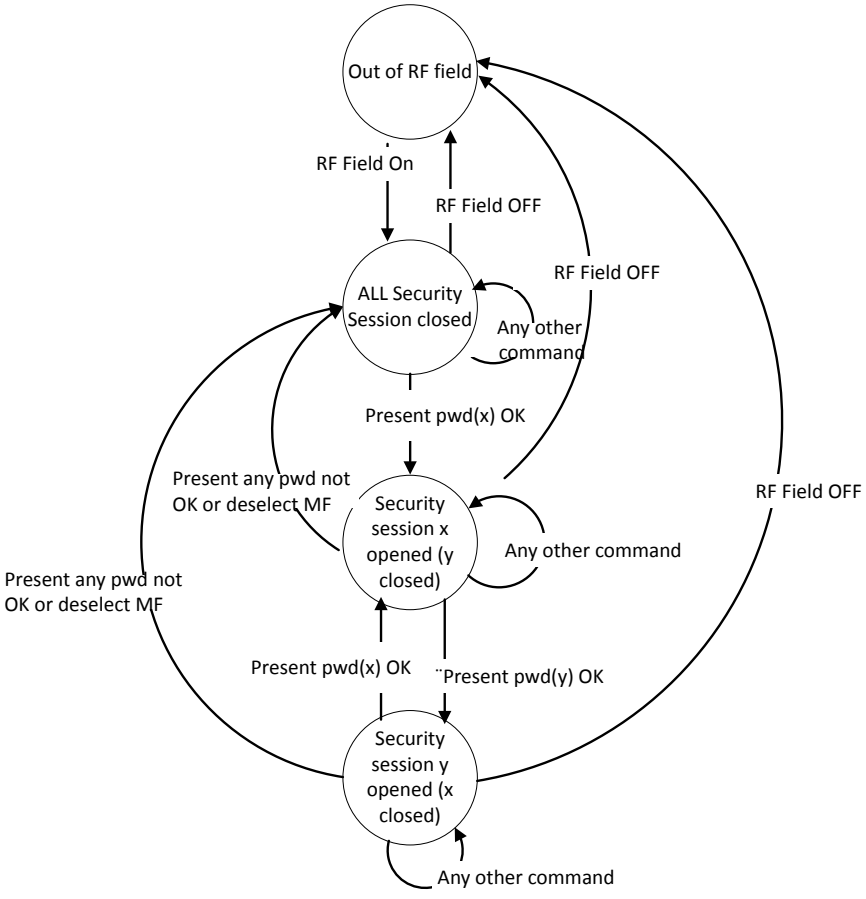
Data access to a protected file is performed by issuing a `Verify` command with adequate security attributes and with an adequate obfuscated password presentation (refer to Section 4.2.1: Cover coding), followed by the `ReadBinary` or `UpdateBinary` commands.

The obfuscated password presentation with the `Verify` command opens a security session on an EF file with the corresponding password identifier and valid encrypted password. To close the security session corresponding to a password identifier, the user can choose one of the following options:

- Remove the tag from the RF field.
- `DeSelect` the tag.
- Use the `Verify` command with the same password identifier, and an invalid password value.
- Open a security session corresponding to a different password identifier. Opening a new security session automatically closes the previously opened one (even if the open operation fails).
- Select the MF master file.

The following figure describes the mechanism to open/close the security sessions.

Figure 4. ST25TA-E security session management



4.1.3 Permission status and permission interaction

Once enabled, the permission status can be retrieved by issuing a `Verify` command and by decoding SW1 and SW2 status, as follows:

Table 12. List of read protection status

Status	Verify (P2 [b0]= 1) R-APDU	Description
RD authorized	9000h	Read access w/o any security (delivery state)
RD protected	6300h	Read access is protected by a password
RD forbidden	6984h	Read access forbidden (persistent state)

Table 13. List of write protection status

Status	Verify (P2 [b1]= 1) R-APDU	Description
WR authorized	9000h	Write access w/o any security (delivery state)
WR protected	6300h	Write access protected by password
WR forbidden	6984h	Write access forbidden (persistent state)

When the read (respectively write) permanent lock is enabled and applied to an authorized access, the permanent lock operation is successfully enabled. Data in the locked EF file cannot be accessed: any read (respectively write) access in a read (respectively write) locked file is ignored. Once successfully enabled, the permission status returns the read (respectively write) forbidden status.

When the read (respectively write) permanent lock is enabled and applied to a read (respectively write) protected access, the permanent lock operation is successfully enabled. Data in the locked EF file cannot be accessed and any password-based read (respectively write) access in a read (respectively write) locked file is ignored, even if the security session is or can be opened or closed. Once successfully enabled, the permission status returns the read (respectively write) forbidden status.

When password-protected read (respectively write) reversible lock is enabled and applied to an authorized access, the reversible lock operation is successfully enabled. Access to data in a protected file is controlled by a security session based on passwords: any read (respectively write) access is protected by the read (respectively write) password presentation. Once successfully enabled, the permission status returns a read (respectively write) protected status.

When password-protected read (respectively write) reversible lock is enabled and applied to a read (respectively write) locked access, the reversible lock operation is successfully ignored and an error is returned during the activation of the reversible lock operation for all EF files except for the write CFG locked file. Refer to the note into the Section 4.1.1: Permanent lock file protection. Data in the locked EF file cannot be accessed: Any read (respectively write) access in a read (respectively write) locked file is ignored. Any read (respectively write) protected access in a read (respectively write) locked file is ignored too. Once successfully enabled, the permission status returns read (respectively write) protected status. In other cases (ignored), the permission status returns read (respectively write) forbidden status.

4.2 Password management

The password management addresses all stages of the password, including generation, conveyance, and storage or cyclic upgrade and offers several password protection mechanisms.

The ST25TA-E devices can support several passwords for different purposes:

- Security session mechanism
- Command or feature protection

Note: The ST25TA-E devices do not permit password-protected commands to be executed unless they are accompanied by the correct password.

By 'accompanied', it is understood that:

- *the password is present into the payload of the command, or*
- *the password is presented by issuing the verify command (security session) prior the command execution.*

Each of the ST25TA-E passwords is 64-bit long and the default factory password value is 0000000000000000h.

Table 14. List of file passwords

Passwords	Size	Passwords index	Factory activation	Applied to
PWD_CFG_WR	8-byte	00h	no	CFG file
PWD_CFG_RD		01h		
PWD_NDEF_WR		02h		NDEF file
PWD_NDEF_RD		03h		
PWD_ANDEF_WR		04h		ANDEF file
PWD_ANDEF_RD		05h		

Table 15. List of feature passwords

Password	Size	Password index	Factory activation	Applied to
PWD_PRIV	8-byte	0Ch	yes	Privacy feature

Note: In addition to the file-related passwords, the PWD_PRIV password (with 0Ch password index) is used with the `ManageBasicLogicalChannel` command for privacy modes.

4.2.1 Cover coding

The ST25TA-E device applies an obfuscation mechanism, also called cover coding mechanism. This scheme is used to transmit obfuscated password values in the password-referenced data field of the following command frames:

Table 16. List of password-related command frames

Command	Meaning
`Verify`	Present password
`ChangeReferenceData`	Update the password value
`ManageBasicLogicalChannel`	Change the tag state (normal state against privacy state)
`EnableVerificationRequirement`	Enable password lock mechanism
`DisableVerificationRequirement`	Disable password lock mechanism

Note: The password-referenced data field in a request frame shall be computed as follows: `password verification data = XOR(CHALLENGE_8B, PASSWORD_8B)`

The requester produces the cipher text by applying an exclusive-or (XOR) operation of the 8-byte password and an 8-byte random value and sends the cipher text defined as the password-referenced data field of the password-related commands, to the ST25TA-E device. The ST25TA-E device applies the XOR operation to recover the plain text and the password and check if it matches with the internal reference value. The ST25TA-E devices initiate the generation of an 8-byte random number and retain this number for use in a subsequent password-related command.

This mechanism requires that a call to the `GetChallenge` command has been issued since the latest boot of the ST25TA-E device, otherwise the password-related commands fail. Additionally, if the latest call to a password-related command failed because of an invalid value of the password-referenced data field, it is required that a call to the `GetChallenge` command is issued before attempting a new call to either of these commands.

4.2.2 Permanent password lock

4.2.2.1 Password Lock description

The ST25TA-E devices provide password lock processing, which allows a user to lock each password individually or globally: a locked password can no longer be modified with the `ChangeDataReference` command. The effect of a password lock operation cannot be reverted.

4.2.2.2 Password lock registers

CFG_PWD_LOCK

23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Reserved										PRIV		ANDEF RD		ANDEF WR		CFG RD		CFG WR		NDEF RD		NDEF WR	
RWO																							

Note: RWO: Read and write once. The RWO access attribute helps the password value not to be reverted.

Address: 002Dh for register range [23:16], 002Eh for register range [15:8], 002Fh for register range [7:0]

Reset: 555 555h

Description: Lock password value

[23:14]	Reserved
[13:12]	**PRIV:**Lock privacy password • 01b: privacy password value is unlocked. • 10b: privacy password value is locked.
[11:10]	**ANDEF RD:** Lock ANDEF read password • 01b: ANDEF read password value is unlocked. • 10b: ANDEF read password value is locked.
[9:8]	**ANDEF WR:** Lock ANDEF write password • 01b: ANDEF write password value is unlocked. • 10b: ANDEF write password value is locked.
[7:6]	**CFG RD:** Lock CFG read password • 01b: CFG read password value is unlocked. • 10b: CFG read password value is locked.
[5:4]	**CFG WR:** Lock CFG write password • 01b: CFG write password value is unlocked. • 10b: CFG write password value is locked.
[3:2]	**NDEF RD:** Lock NDEF read password • 01b: NDEF read password value is unlocked. • 10b: NDEF read password value is locked.
[1:0]	**NDEF WR:** Lock NDEF write password • 01b: NDEF write password value is unlocked. • 10b: NDEF write password value is locked.

4.3 Augmented NDEF feature (ANDEF)

4.3.1 ANDEF description

The Augmented NDEF (ANDEF) feature is a contextual automatic NDEF message service, allowing the tag to provide dynamic content without an explicit update of the NVM memory by the end user.

The ANDEF feature is enabled or disabled by issuing an `UpdateBinary` command, applied on the CFG EF file with the adequate security attributes.

The feature is enabled (respectively disabled) when the value of register CFG_ANDEF_EN is 1b (respectively 0b) during the latest RF boot sequence. When the feature is enabled, user memory data at byte addresses ranging from ANDEF_START to ANDEF_END is replaced by the content of a virtual memory ANDEF_MEM in the response to `ReadBinary` requests in the NDEF file. Byte addresses ANDEF_START and ANDEF_END depend on the ANDEF_BYTE_OFFSET field configuration during the last RF session.

Figure 5. NDEF read data response when the ANDEF feature is disabled/enabled

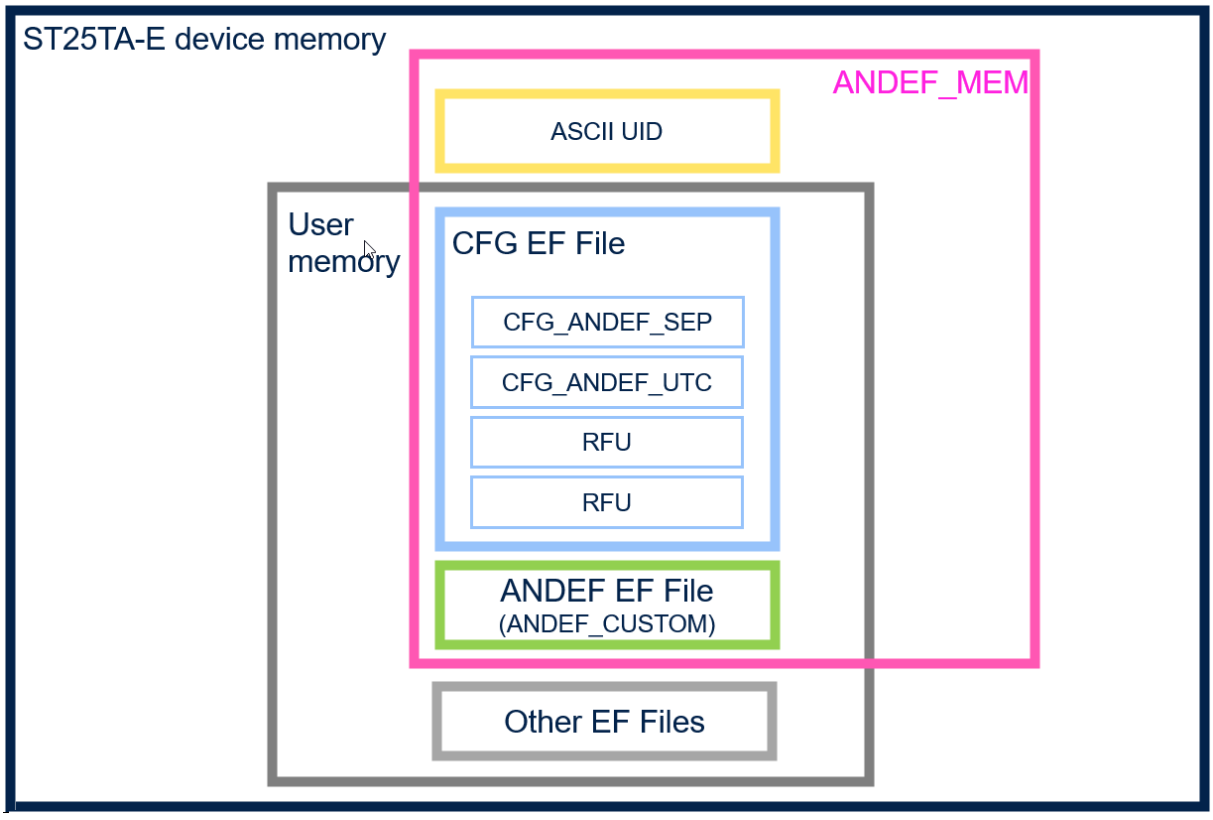
Note: ANDEF_START is defined by the CFG_ANDEF_BYTE_OFFSET value.

ANDEF_END is the minimum value between END_NDEF_FILE and (ANDEF_START + ANDEF_LEN -1) with END_NDEF_FILE, is the last address available in the NDEF file, and NDEF_LEN is the number of bytes available in the virtual ANDEF_MEM dedicated to the ANDEF feature.

Once enabled, the ANDEF feature has no effect on the `UpdateBinary` requests in this address range [ANDEF_START: ANDEF_END]. The incoming data, to be written, is directly written to the user NDEF file at the requested offset addresses but cannot be read by issuing a `ReadBinary` command when the ANDEF feature is enabled.

The content of a virtual ANDEF_MEM memory depends on the selected ANDEF contextual fields, enabled by the CFG_ANDEF_CFG register . The content of ANDEF_MEM is the result of the concatenation of ANDEF fields.

Figure 6. ANDEF_MEM content



Each field corresponds to a configuration register and may be enabled individually. A separator tag, defined by the CFG_ANDEF_SEP register, is inserted between each ANDEF field when conditions are met. The order of appearance, the content, and condition of presence of each field are listed in the below table.

The ANDEF elementary file is one of the ANDEF field, called ANDEF_CUSTOM field in the below table.

Table 17. Concatenated ANDEF fields in the ANDEF MEM

Order	Content(1)	Byte length	Condition of presence
1	ANDEF_UID	14 (2)	When CFG_ANDEF_UID_EN =1b
2	ANDEF_SEP	1	When CFG_ANDEF_SEP_EN =1b and CFG_ANDEF_UTC_EN = 1b
3	ANDEF_UTC	4	When CFG_ANDEF_UTC_EN = 1b
4	ANDEF_SEP	1	When CFG_ANDEF_SEP_EN =1b and any ANDEF_DIAG bits = 1b
5	ANDEF_DIAG	For further information, contact your STMicroelectronics sales officer.	-
6	ANDEF_SEP	1	When ANDEF_SEP_EN =1b and CFG_ANDEF_CUSTOM_EN =1b
7	ANDEF_CUSTOM(3)	42	When ANDEF_CUSTOM_EN =1b

1. *When a register value is coded on several bytes, it is copied in LSB to MSB bytes order in the ANDEF MEM memory.*
2. *UID field is 14-byte long when CFG_ANDEF_UID_EN is only set to 1b.*
3. *ANDEF_CUSTOM field is the representation of the payload of the ANDEF file. The two first ANLEN bytes of the ANDEF file are not included into the ANDEF_MEM.*

On factory delivery, the CFG_ANDEF_EN register is disabled and the CFG_ANDEF_CFG register is set to 10h.

4.3.2 ANDEF registers

CFG_ANDEF_BYTE_OFFSET

7	6	5	4	3	2	1	0
ANDEF_BYTE_OFFSET							
RW							

Address: 001Fh

Reset: 00h

Description: ANDEF message start into an elementary file

[7:0]	**ANDEF_BYTE_OFFSET:** Offset the value into an elementary file to compute the start address of the ANDEF

CFG_ANDEF_CFG

7	6	5	4	3	2	1	0
Unused			ANDEF_SEP_EN	ANDEF_CUSTOM_EN	ANDEF_DIAG_EN	ANDEF_UTC_EN	ANDEF_UID_EN
R			RW	RW	RW	RW	RW

Address: 0020h

Reset: 10h

Description: ANDEF display configuration

[7: 5]	**Unused:** Reading this field returns 0.
[4]	**ANDEF_SEP_EN:** Activation of the SEP field in the ANDEF message display. • 0b: field is disabled. • 1b: field is enabled.
[3]	**ANDEF_CUSTOM_EN:** Activation of the CUSTOM field in the ANDEF message display. • 0b: Field is disabled. • 1b: Field is enabled.
[2]	**ANDEF_DIAG_EN:** Activation of the DIAG field in the ANDEF message display. • 0b: Field is disabled. • 1b: Field is enabled.
[1]	**ANDEF_UTC_EN:** Activation of the UTC field in the ANDEF message display. • 0b: Field is disabled. • 1b: Field is enabled
[0]	**ANDEF_UID_EN:** Activation of the UID field in the ANDEF message display. • 0b: Field is disabled. • 1b: Field is enabled.

CFG_ANDEF_SEP

7	6	5	4	3	2	1	0
ANDEF_SEP							
RW							

Address: 0021h

Reset: 78h

Description: ANDEF separator field value

[7:0]	**ANDEF_SEP:** Separator value into the ANDEF message, in ASCII format.

CFG_ANDEF_EN

7	6	5	4	3	2	1	0
Unused							ANDEF_EN
R							RW

Address: 0024h

Reset: 00h

Description: Activation of ANDEF feature.

[7:1]	**Unused**: Reading this field returns 0.
[0]	**ANDEF_EN:** Activation of ANDEF feature. • 0b: feature is disabled. • 1b: feature is enabled.

4.4 Smart authentication

To successfully ensure the protection of all key elements of a IoT solution, the TruST25 services deliver one smart service, which ensures that the UID of the NFC/RFID devices is genuine and can contribute to attest a smart authentication of the chip if the TruST25 services is coupled with other security mechanisms at system level and through the ANDEF feature.

The TruST25 solution encompasses the secure industrialization process and the tools deployed by STMicroelectronics to generate, store, and check the signature in the ST25TA-E device.

For further information, contact your STMicroelectronics sales officer.

4.5 Strong authentication

To ensure a successful protection of all the key elements of an IoT solution, the Edge-TruST25 services deliver one safe service, which ensures that the NFC/RFID tag devices are genuine and if bond with the physical asset is unique and tamper proof, can prove physical asset authenticity.

The Edge-TruST25 solution encompasses secure industrialization processes and tools deployed by STMicroelectronics to generate, store, and check the sensitive assets in the device.

For further information, contact your STMicroelectronics sales officer.

4.6 Monitoring and diagnosis

Monitoring may be enabled in the ST25TA-E devices for operation tracking. ST25TA-E GP counter defines the main component for remote monitoring.

4.6.1 Remote monitoring

4.6.1.1 General purpose counter description

Remote monitoring by applicative counter in the ST25TA-E devices can help for tracking operation.

The general purpose (GP) counter is identified as a key feature for the monitoring process. This is a 24-bit counter that can track up to 2^{24} read/write events on one of the EF files. It benefits from an antitearing mechanism that ensures consistency of the counter, even if there is an electrical problem during its increment.

The general purpose counter can be configured, activated, and read or reverted to its initial value or decremented by one, with the adequate security attributes. Once activated, a reset to factory operation on this counter is possible with a PWD_CFG_WR password presentation prior to the `RevertGPcounter` command.

The GP counter is activated by issuing an `UpdateBinary` command in the CFG_GP_CNT_EN register of the CFG EF file with the adequate security attributes and is effective on the next RF session.

All fields of the CFG_GP_CNT registers, except the GP_CNT_DEC_DIS field, are locked as soon as the counter is activated.

Note: No increment is performed if the CFG_GP_CNT_EN register is updated with an invalid file index. Only the index among the authorized seven file indexes is valid.

The GP_CNT_INC_CALL field of the CFG_GP_CNT_CFG register can be programmed to restrict the increment only to the read access (or only write access) in any address of the selected user file.

The GP_CNT_INC_RANGE field can be programmed to restrict the increment to access only into a specific address of the user file. This specific address is configured by the CFG_GP_CNT_OFFSET_ADD register. The GP_CNT_INC_CALL, GP_CNT_INC_RANGE configurations can be combined.

If the GP_CNT_INC_CALL field and the GP_CNT_INC_RANGE field are set to 0 into the CFG_GP_CNT_CFG register, the increment is performed by any successful read or write access into any address of the user file.

Once activated, the GP counter is automatically incremented by a successful access into the address range of the user file. If the GP counter reached the GP_CNT_LIMIT value, the GP counter is blocked at the maximum value. On factory delivery. The CFG_GP_CNT_LIMIT register is set to the FFFFFFh value.

Note: If the CFG_GP_CNT_LIMIT register needs to be updated to a lower value, it shall be set before the GP counter activation.

The GP counter value can be read by issuing the `GetGPcounter` command at any time after the protocol activation. The GP counter value can be reverted to its preceding values by issuing a `RevertGPcounter` command only if the decrement operation is enabled.

Note: The GP counter decrement is disabled by issuing an `UpdateBinary` command into the CFG_GP_CNT_EN register of the CFG EF file and is effective immediately. The GP counter decrement/revert deactivation is permanent.

The GP counter is always incremented by one whereas the decrement of the GP counter is decremented by one or is programmed to its reset value '000000h' (roll-over to initial value). The programmable dec value (decrement by -1 or return initial value) for the decrement is programmed with the P1/P2 parameter of the `RevertGPcounter` command.

4.6.1.2 *GP_CNT registers*

CFG_GP_CNT_LIMIT

23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
GP_CNT_LIMIT																							
RW																							

Address: 0016h

Reset: FFFFFFh

Description: Limit the value of the general-purpose counter.

[23:0]	**GP_CNT_LIMIT:** Authorized limit value of the GP counter.

CFG_GP_CNT_CFG

7	6	5	4	3	2	1	0
Unused				GP_CNT_INC_RANGE	GP_CNT_INC_CALL		GP_CNT_DEC_DIS
R				RW	RW		RWO

Note: RWO: read and write once

Address: 0019h

Reset: 00h

Description: General-purpose counter configuration.

[7:4]	**Unused**: Reading this field returns 0.
[3]	**GP_CNT_INC_RANGE:** Range format where the increment is applied • 0b: any access in the elementary file selected by the CFG_GP_CNT_EN register. • 1b: any access at the address offset specified in the CFG_GP_CNT_OFFSET_ADD register.
[2:1]	**GP_CNT_INC_CALL**: The event by which the increment is issued • 00b: first access (read or write) of the current RF field, increments the GP counter. • 01b: first read access of the current RF field, increments the GP counter. • 10b: first write access of the current RF field, increments the GP counter.
[0]	**GP_CNT_DEC_DIS**: Deactivation of the decrement/revert feature of the GP counter • 0b : deactivation of the decrement/revert feature is disabled • 1b: deactivation of the decrement/revert feature is enabled

CFG_GP_CNT_OFFSET_ADD

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
GP_CNT_OFFSET_ADD															
RW															

Address: 001Ah

Reset: 0000h

Description: Address offset value for general-purpose counter range configuration

[15:0]	**GP_CNT_OFFSET_ADD:** Address the offset value used by the CFG_GP_CNT_CFG register.

CFG_GP_CNT_EN

23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
GP_CNT_EN	Unused															GP_CNT_FILE_IDX							
RW	R															RW							

Address: 001Ch for register range [23:16]
001Dh for register range [15:8]
001Eh for register range [7:0]

Reset: 000001h

Description: Address and configuratin on the general-purpose counter

[23]	**GP_CNT_EN:** Activation of the GP_CNT counter. • **0b**: GP counter is disabled. • **1b**: GP counter is enabled.
[22:8]	**Unused**: Reading this field returns 0.
[7:0]	**GP_CNT_FILE_IDX**: File index of the selected elementary file where the GP counter is applied. Authorized file index: • 00h: cfg file • 01h: ndef file • 02h: andef file • 08h: cc file

4.7 Privacy

The two privacy modes, called *kill* and *anonymous*, offer consumer privacy capabilities, which are required by the GDPR European regulation.

4.7.1 Kill mode description

Kill mode is the entry-level privacy mode. When the ST25TA-E device is in KILLED state, all incoming RF requests are ignored during the current RF session and on the further RF sessions. The users can configure, intentionally the ST25TA-E device in KILLED state in two manners:

- On a successful `ManageBasicLogicalChannel` command with P1=10h and P2= 5Ah. In this case, the privacy password is used (user usage, immediate action).
- By issuing an `UpdateBinary` command into the CFG EF file, setting the CFG_PRIV register at the 5Ah value. In this case, the control CFG write-password is used (admin usage, no immediate action).

Once the ST25TA-E device has entered the KILLED state, it can only switch between the power-off and killed state.

The kill commands are enabled/disabled when the DIS_KILL attribute has respectively, 00h/FFh value during the latest boot sequence. The update of the DIS_KILL attribute is effective on the next RF boot sequence. On factory delivery, the DIS_KILL attribute is set to 00h. If the DIS_KILL attribute is active (FFh), the two kill commands, `ManageBasicLogicalChannel` and `UpdateBinary` return respectively the error code 6985h and 6A80h as the SW1SW2 code response.

STMicroelectronics fully controls the DIS_KILL attribute configuration during the EWS operation. For selection of an active DIS_KILL attribute, contact your STMicroelectronics sales office.

4.7.2 Anonymous mode description

Anonymous mode is the second privacy mode. When the ST25TA-E device is in UNTRACEABLE state, all incoming RF requests and features are handled except the following:

- The ANDEF feature is forbidden. The ANDEF enable control configuration is ignored and the ANDEF message is not appended to the NDEF file during the NDEF read.
- The ANDEF custom file is forbidden.
- The `GetSystemInformation` command returns an error code (6985h).

Note: Forbidden files (ANDEF file) are considered as invalid file (when issuing the `SelectFile` command) and the `SelectFile` command should return 6985h as SW1SW2 error code.

Note: All invalid files already selected before entering in anonymous (with their security sessions already opened), close their security session as soon as the anonymous mode is successfully configured, and the NFC application DF file is selected.

The ST25TA-E device enters the UNTRACEABLE state in two manners:

- On a successful `ManageBasicLogicalChannel` command with P1=80h and leaves the UNTRACEABLE state on a successful `ManageBasicLogicalChannel` command with P1=20h. In this case, the privacy password is used (user usage, immediate action).
- By issuing an `UpdateBinary` command into the CFG EF file, setting the CFG_PRIV register at F0h value and leaves the UNTRACEABLE state, with 00 value of the CFG_PRIV register. In this case, the control CFG write-password is used (admin usage, no immediate action).

Once the ST25TA-E device has entered the UNTRACEABLE state, it can switch between the power-off, KILLED state, PROTOCOL state, and UNTRACEABLE state. The action is immediate.

Note: In the UNTRACEABLE state, the UID used in request and response frames is a random or fixed value. In this case, the ISO/IEC 14443-3 standard allows only a single 4-byte UID: In case of nonunique fixed value, the first byte of UID (UID0) is '5Fh' and in case of random value, the first byte of UID (UID0) is '08h'. In an UNTRACEABLE state, the UID size is updated in the ATQA parameter and SAK1 parameter when the random UID is used

Note: The 4-byte UID mode (nonunique fixed number or random) is selected by PRIV_UID attribute. ST fully controls the PRIV_UID attribute configuration during EWS operation. For selection of nonunique fixed UID, contact your STMicroelectronics sales office.

Note: The 3 LSB bytes of the nonunique fixed UID number can be updated by users. This is done with the 3-byte CFG_PRIV_NUID register, by issuing an `UpdateBinary` command into the CFG EF file.

4.7.3 Privacy registers

CFG_PRIV_NUID register

23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
PRIV_NUID																							
RW																							

Address: 0012h for register range [23:16]
0013h for register range [15:8]
0014h for register range [7:0]

Reset: 029A00h

Description: 3-byte value of the 4-byte nonunique UID, used in anonymous mode (privacy mode).

[23:0]	**PRIV_NUID**: LSB value of the nonunique UID.

CFG_PRIV register

7	6	5	4	3	2	1	0
				PRIV_DFLT			
RW							

Address: 0015h

Reset: 00h

Description: Privacy configuration by default at the beginning of each RF session when enabled once.

[7:0] **PRIV_DFLT**: The device boots in privacy or normal mode according to the field value

- 00h: in/out mode. The device boots in PROTOCOL state when the device left the previous RF session in PROTOCOL state. The device boots in UNTRACEABLE state when the device letf the previous RF session in UNTRACEABLE state.
- F0h: anonymous by default mode. The device boots always in UNTRACEABLE state at the beginning of each RF session when enabled once.
- 5Ah: kill by default–the device is in KILLED state in further RF sessions.

4.8 Security

In order to prevent an unauthorized use of the device or a fraudulent access to data, the ST25TA-E devices implement a set of hardware security mechanisms, including a dedicated protection for counter monotonicity and for sensitive assets. Security requirements at applicative level, are also available in the *ST25TA-E Security Guidance and operational manual document*, and must be applied in some conditions.

4.8.1 Antitearing

The ST25TA-E devices benefit from an antitearing mechanism that ensures the consistency of each counter even if there has been an electrical problem during its increment. In the case of tearing, data is recovered.

Antitearing on counters

The antitearing mechanism is applied on the following counters:

- GP counter

Data is recovered with new data. New data is equal or higher than the preceding value.

This antitearing mechanism is also applied on the password values during password update. Data is recovered with preceding data before tearing.

4.8.2 Physical protection: Active shield and laser detection

The ST25TA-E devices are protected by active shields and laser detections.

4.8.3 Nonvolatile memory protection

The ST25TA-E devices protect nonvolatile memory from erase/write operations with data integrity mechanisms.

5 RF operations

5.1 RF communications

This section describes the principle of communication between an RF host and the ST25TA-E devices.

ST25TA-E devices are NFC Type 4 tags. The communication principle of this type of tag is based on the NFC-A technology specification. The RF host generates the RF field and the RF commands.

Responses and commands are transmitted using respectively OOK modulation and ASK 100% modulation of a 13.56 MHz carrier wave transmitted by the PCD reader. Responses are transmitted using backscattering of the same carrier wave.

Both commands and responses are transmitted at 106 kbps.

ST25TA-E devices follow an activation, anticollision and selection process allowing one-to-one communication in the presence of several tags.

5.2 State machine

The state diagram specifies all possible state transitions in NFC-A and ISO DEP.

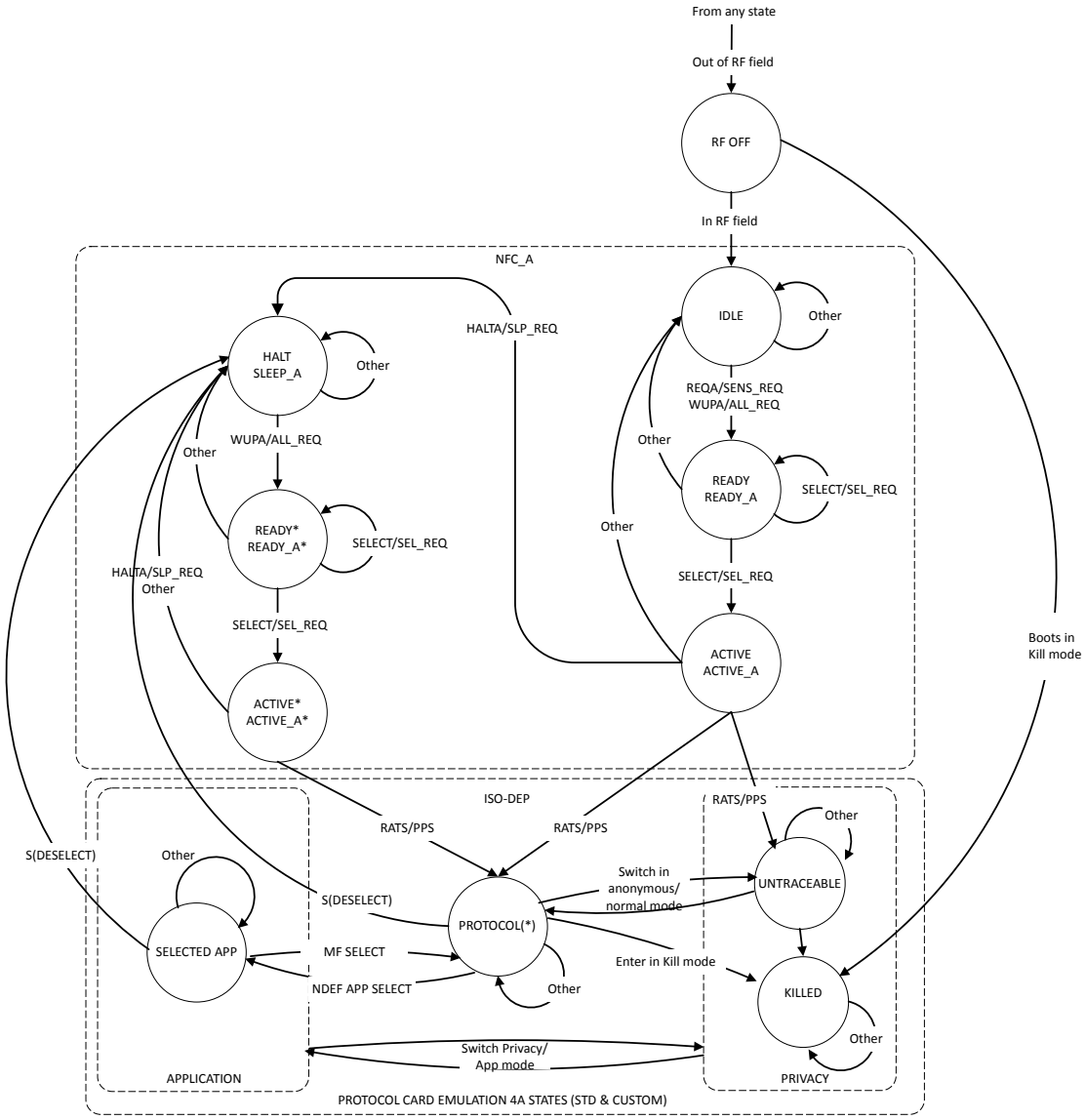
In addition to the standardized states specified in the NFC-A and the ISO DEP, the ST25TA-E devices support three custom states:

- SELECTED APP
- UNTRACEABLE
- KILLED

Transitions with these states are specified in the figure below.

In PROTOCOL state, the ST25TA-E devices behave in accordance with ISO DEP.

Figure 7. **ST25TA-E RF FSM**



Protocol state

In PROTOCOL state, the ST25TA-E shall must respond only to the following commands:

- `SelectApplication`
- `GetChallenge`
- `ManageBasicLogicalChannel`
- `GetSystemInformation`
- `GetGPCounter`

In PROTOCOL state, the ST25TA-E devices enter the SELECTED APP state after it has received a valid `SelectApplication` command.

In PROTOCOL state, the ST25TA-E devices enter HALT/Sleep A state after it has received a valid `DeSelect` command.

In PROTOCOL state, the ST25TA-E devices enter KILLED state or in UNTRACEABLE state after it has received a valid `ManageBasicLogicalChannel` command with enabling, respectively, the kill mode or anonymous mode option.

Selected App state

In SELECTED APP state, the ST25TA-E must respond to all commands described in Section 5.4: RF command set and to the `DeSelect` command.

In SELECTED APP state, the ST25TA-E enter PROTOCOL state after it received a valid MF master file selection by issuing a `SelectFile` command.

In SELECTED APP state, the ST25TA-E devices enter HALT/Sleep A state after it has received a valid `DeSelect` command.

In SELECTED APP state, the ST25TA-E devices enter KILLED state or in UNTRACEABLE state after it has received a valid `ManageBasicLogicalChannel` command with enabling, respectively, the kill mode or anonymous mode option.

Untraceable state

In UNTRACEABLE state, the ST25TA-E device must respond to all commands described in Section 4.7.2: Anonymous mode description .

In UNTRACEABLE state, the ST25TA-E devices enter PROTOCOL state after it received a valid `ManageBasicLogicalChannel` command with disabling the anonymous mode option and if the MF master file is selected during the UNTRACEABLE state or before the UNTRACEABLE state.

In UNTRACEABLE state, the ST25TA-E devices enter SELECTED APP state after it received a valid `ManageBasicLogicalChannel` command with disabling the anonymous mode option and if the DF or an authorized file is selected during the UNTRACEABLE state or if an invalid file is selected before the UNTRACEABLE state.

Note: When an invalid file is already selected before entering in UNTRACEABLE state, the NFC application DF file is automatically selected.

In UNTRACEABLE state, the ST25TA-E devices enter HALT/Sleep A state after it has received a valid `DeSelect` command.

Killed state

In KILLED state, the ST25TA-E must behave as described in Section 4.7.1: Kill mode description and ignore all incoming commands.

5.3 RF protocol

The transmission protocol (or simply named ‘the protocol’) defines the mechanism used to exchange instructions and data between the PCD (proximity coupling device) and the PICC (proximity integrated circuit card) in both directions. It is based on the concept of ‘PCD first talk’. The ST25TA-E device acts as a PICC.

This means that a ST25TA-E does not start transmitting unless it has received and properly decodes an instruction sent by the PCD. The protocol is based on exchange of commands, which consists of in request/response transactions between the PCD and the ST25TA-E device:

- A request is sent from the PCD to the ST25TA-E
- A response to this request is sent from the ST25TA-E to the PCD.

There are four command families:

- The NFC-A activation, anticollision, and selection process command set
- The NFC Forum Type 4 tag command set
- The ISO/IEC 7816-4 command set
- The ST-proprietary command set

The following table lists the request command sets with a brief description of each of the commands.

Table 18. RF command sets

Family command set	Command name	Brief description
NFC-A activation, anticollision	ALL_REQs,SENS_REQs, SDD_REQ, SEL_REQ,SLP_REQ	Anticollision command set
	RATS	TA4 Tag activation
	PPS	Protocol and parameter selection
	DeSelect	Tag desactivation
NFC Forum T4T	SelectApplication	NDEF tag application select
	SelectFile	EF file select
	ReadBinary	Read data from file
	UpdateBinary	Write or erase data to an EF file
ISO/IEC 7816-4	GetChallenge	Retrieve a challenge generated by the device
	Verify	Check the right access or present a password
	ChangeReferenceData	Changes a read or write password value
	EnableVerificationRequirement	Activates a reversible file protection
	DisableVerificationRequirement	Disable a reversible file protection
ST-proprietary	EnablePermanentRequirement	Activate a permanent file protection
	ManageBasicLogicalChannel	Activate or disable privacy mode
	GetSystemInformation	Retrieve system information
	GetGPcounter	Retrieve GP counter value
	RevertGPcounter	Revert or initialize the GP counter.

The different command families use different kinds of data formats, the most frequently based on what are 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

The following subsections describe the structure of I-block, R-block, and S-block.

5.3.1 I-block format

The NFC Forum Type 4 tag command-set and the ISO/IEC 7816-4 command-set use the I-Block format. The I-block is used to exchange data between the PCD and the ST25TA-E devices. It is composed of three fields as detailed in the table below.

Table 19. I-block format

Name	StartofData		Payload	EndOfData
	PCB	CID		CRC
Length	**1 byte**	**1 byte**	**1 to 251 bytes**	**2 bytes**
PCB field				
CID field				
RF host to tag C-APDU or tag R-APDU				
2 CRC bytes				

Table 20. PCB field of the I-Block format

	b7-b6	b5	b4	b3	b2	b1	b0
	0b00	0b	0b	X	0b	1b	X
I-block							
RFU							
Must be set to 0b							
CID field is present if this bit is set to 1b							
Must be set to 0b							
Must be set to 1b							
Block number							

Note: Block numbering notes:

PCD rules

- *The PCD device block number shall be initialized to 0.*
- *When an I-block or an R(ACK) block with a block number equal to the current block number is received, the PCD device shall toggle the current block number before optionally sending a block to the ST25TA-E.*

ST25TA-E rules

- *The ST25TA-E block number shall be initialized to 1 at activation.*
- *When an I-block is received, the ST25TA-E must toggle its block number before sending a block.*

Note: TheST25TA-E may check if the received block number is not in compliance with PCD rules to decide neither to toggle its internal block number or to send a response block

- *When an R(ACK) block with a block number not equal to the current ST25TA-E block number is received, the ST25TA-E must toggle its block number before sending a block.*

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

When the PCD device sends a command to the ST25TA-E, the format of the payload is the C-APDU.

When the ST25TA-E device sends a command to the RF host, the format of the payload is the R-APDU.

C-APDU: payload format of a command

The C-APDU format is used by the RF host to send a command to the ST25TA-E. The table below describes its format.

Table 21. C-APDU format

Name	Payload field						
	CLA	INS	P1	P2	Lc	Data	Le
Length	1 byte	1 byte	1 byte	1 byte	1 byte	Lc bytes	1 byte
Class byte: 0x00: standard command 0xA2: ST command							
Instruction byte							
Parameter byte 1							
Parameter byte 2							
Number of bytes of the data field							
Data bytes							
Number of bytes to be read in ST25TA-E memory							

R-APDU: payload format of a command

The ST25TA-E devices use the I-Block format to reply to a command that has used the I-Block format. The table below describes its format.

Table 22. R-APDU format

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

5.3.2 R-block format

The R-Block is used to convey positive or negative acknowledgment between the PCD and the ST25TA-E devices. The table below describes its format.

Table 23. R-block format

Name	StartofData		Payload	EndOfData
	PCB	CID		CRC
Length	1 byte	1 byte	0 byte	2 bytes
R(ACK) without CID field: 0xA2 or 0xA3 R(ACK) with CID field: 0xAA or 0xAB R(NAK) without CID field: 0xB2 or 0xB3 R(NAK) with CID field: 0xBA or 0xBB				
CID field (optional)				
2 CRC bytes				

There are two kinds of R-Blocks:

- R(ACK): the acknowledgment block sent by the PCD or by the ST25TA-E device.
- R(NAK): the non-acknowledgment block sent by the PCD device.

Table 24. PCB field of the R-Block format

	b7-b6	b5	b4	b3	b2	b1	b0
	0b00	0b	0b	X	0b	1b	X
R-block							
Must be set to 1b							
• 0b: ACK • 1b: NACK							
CID field is present if this bit is set to 1b							
Must be set to 0b							
Must be set to 1b							
Block number							

5.3.3 S-block format

The S-Block is used to exchange control information between a PCD and the ST25TA-E device.

Table 25. S-block format

Name	StartofData		Payload	EndOfData
	PCB	CID		CRC
Length	1 byte	1 byte	1 byte	2 bytes
S(DES) without CID field: 0xC2 S(DES) with CID field: 0xCA S(WTX) without CID field: 0xF2 S(WTX) with CID field: 0xFA				
CID field (optional)				
WTX field (optional)(1)				
2 CRC bytes				

1. *This field is present when b5-b4 bits are set to b11 (S-block is a WTX). See Table 26. PCB field of the S-Block format.*

There are two requests using the S-Block format:

- S(DES): the `DeSelect` command.
- S(WTX): the `waiting frame eXtension` command or response.

*Note: A waiting time eXtension request occurs in RF when the operating time needed by the ST25TA-E is greater than 65.536 ms. The WTX field indicates the increase time factor to be used in this command execution (FDTtemp = WTX * 65.536 ms). WTX depends on FWI.*

Table 26. PCB field of the S-Block format

	b7-b6	b5-b4	b3	b2	b1	b0
	0b00	X	X	0b	1b	0b
S-block • 0b00: Deselect • 0b11: WTX						
CID field is present if this bit is set to 1b						
Must be set to 0b						
Must be set to 1b						
Must be set to 1b						

5.3.4 CRC of an RF frame

The two CRC bytes check the data transmission between the PCD and the ST25TA-E devices.

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.

5.3.5 Return code list

A command is acknowledged by SW1 and SW2, giving the status of the command execution.

The table below lists the SW1-SW2 codes into the ST25TA-E devices.

Table 27. **SW1-SW2 codes into the ST25TA-E devices**

SW1-SW2		Execution and error status	Description
90	00	Processing completed – no error	Normal processing – fully executed
63	00	Warning processing	Password is required
65	81	Processing aborted- execution error	Memory failure: unsuccessful update
66	00	Processing aborted- execution error	Security-related issues
67	00	Processing aborted- checking error	Wrong frame length
69	81	Processing aborted- checking error	Incompatible command with the file structure
69	82	Processing aborted- checking error	Security status not satisfied
69	84	Processing aborted- checking error	Forbidden file access
69	85	Processing aborted- checking error	Condition not satisfied
6A	80	Processing aborted- checking error	Incorrect payload parameters
6A	82	Processing aborted- checking error	EF or DF not found
6A	86	Processing aborted- checking error	Incorrect P1 or P2 parameters
6A	88	Processing aborted- checking error	Referenced data not found
6D	00	Processing aborted- checking error	Instruction code not supported or invalid
6E	00	Processing aborted- checking error	Class not supported

5.4 RF command set

The ST25TA-E device supports the following RF command set:

Table 28. **RF command sets**

Class	opcode	Command name	Brief description
0x00	A4h	SelectApplication	Refer to Section 5.4.1: NFC T4T command-set
	A4h	SelectFile	
	B0h	ReadBinary	
	D6h	UpdateBinary	
	84h	GetChallenge	Refer to Section 5.4.2: ISO/IEC 7816-4 command-set
	20h	Verify	
	24h	ChangeReferenceData	
	28h	EnableVerificationRequirement	
	26h	DisableVerificationRequirement	
0xA2	28h	EnablePermanentRequirement	Refer to Section 5.4.3: ST proprietary command set
	70h	ManageBasicLogicalChannel	
	B6h	GetSystemInformation	
	C4h	GetGPcounter	
	D4h	RevertGPcounter	

Commands are described in the following sections.

5.4.1 NFC T4T command-set

The ST25TA-E command set is built to easily support the NFC Forum Type 4 tag protocol.

5.4.1.1 *SelectApplication command*

When receiving the NDEF tag application select request, the ST25TA-E devices switch to SELECTED APP state by selecting the NDEF tag application identifier, defined in the NFC Forum digital protocol.

Syntax: 00 A4 04 00 07 *Data-in*

Type: IN

Instruction inputs: provide 7-byte *Data-In* value matching with NFC application ID

(NFC AID = D2 76 00 00 85 01 01h)

Instruction outputs: Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: The Le field is optional and may be absent from this C-APDU.

Table 29. With C-APDU format

SelectApp	Payload field						
	CLA	INS	P1	P2	Lc	Data	Le
Length	1 byte	1 byte	1 byte	1 byte	1 byte	Lc bytes	1 byte/-
00h		A4h	A4h	00h	07h	D2 76 00 00 85 01 01h	00h/-

Table 30. With R-APDU format

SelectApp	Payload field		
	Data	SW1	SW2
Length	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.1.2 *SelectFile command*

When receiving the `SelectFile` request, the ST25TA-E devices switch to the selected file. Before sending a `SelectFile` command, the ST25TA-E devices should be in SELECTED APP state.

Syntax: 00 A4 00 0C 02 *Data-in*

Type: IN

Instruction inputs: provide 2-byte *Data-In* value matching with one of the following FID (file identifier) values:

- (NFC CC FID = E1 03h)
- (NFC NDEF FID = E1 04h)
- (NFC ANDEF FID = E1 05h)
- (EF CFG FID = E1 01h)
- (MF FID = 3F 00h)

Instruction outputs: Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Table 31. With C-APDU format

SelectFile	Payload field						
	CLA	INS	P1	P2	Lc	Data	Le
Length	1 byte	1 byte	1 byte	1 byte	1 byte	Lc bytes	0 byte
00h		A4h	00h	0Ch	02h	FID	-

Table 32. With R-APDU format

SelectFile	Payload field		
	Data	SW1	SW2
Length	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.1.3 *ReadBinary command*

When receiving the `ReadBinary` request, the ST25TA-E devices read the requested memory field in a selected EF file and send back its value in the R-APDU response. Before sending a `ReadBinary` command, the ST25TA-E devices should be in SELECTED APP state and a file should be selected by using the EF file identifier.

Syntax: 00 B0 *Offset-in Le-in*

Type: OUT

Instruction inputs:

- Provide a 2 byte *Offset-in* value in the file selected matching with the start address of the requested memory field.
- Provide a 1-byte *Le-in* value matching with the number of bytes to read, between (0x00 <= Le <= max (selected file length, 0xFF)

Instruction outputs:

- Retrieve Le-byte data matching with the requested memory field in a selected file.
- Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: If the Le field contains only bytes set to '00', then all the bytes until the end of the file should be read within the limit of 256 for a short Le field.

The response of the `ReadBinary` command is successful when the data to be read is within the selected file; in other words, when the sum of Offset-in and Le-in fields is equal to or lower than the selected file length. When (Offset+Le) overflows the size of the file, the exact number of available data bytes is returned and the SW1 SW2 '9000' with the truncated data

If the file RD authentication is enabled, the RD password of this EF file shall be presented prior to reading the requested file.

Table 33. With C-APDU format

ReadBinary	Payload field						
	CLA	INS	P1	P2	Lc	Data	Le
Length	1 byte	1 byte	1 byte	1 byte	0 byte	0 byte	1 byte
00h		B0h	Offset-in[15:8]	Offset-in[7:0]	-	-	Nb of bytes

Table 34. With R-APDU format

ReadBinary	Payload field		
	Data	SW1	SW2
	Le bytes	1 byte	1 byte
Memory file content		Status byte 1	Status byte 2

5.4.1.4 *UpdateBinary command*

When receiving the `UpdateBinary` request, the ST25TA-E devices update the requested memory field in a selected EF file and returns the R-APDU response. Before sending an `UpdateBinary` command, the ST25TA-E devices should be in SELECTED APP state and a file should be selected by using an EF file identifier.

Syntax: 00 D6 *Offset-in Lc-in Data-in*

Type: IN

Instruction inputs:

- Provide a 2 byte *Offset-in* value in the file selected matching with the start address of the requested memory field.
- Provide a 1-byte *Lc-in* value matching with the number of bytes to be written, between (0x00 <= Lc <= max (selected File Length, Mlc for NDEF file).
- Provide an Lc-byte *Data-in* matching with the requested memory field to be written in a selected file.

Instruction outputs: Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: If the file WR authentication is enabled, the WR password of this EF file must be presented prior to updating the requested file.

Table 35. With C-APDU format

UpdateBinary	Payload field						
	CLA	INS	P1	P2	Lc	Data	Le
Length	1 byte	1 byte	1 byte	1 byte	1 byte	Lc bytes	0 byte
00h		D6h	Offset-in [15:8]	Offset-in [7:0]	Nb of bytes	Data to be written	-

Table 36. With R-APDU format

UpdateBinary	Payload field		
	Data	SW1	SW2
	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.2 ISO/IEC 7816-4 command-set

The ST25TA-E command supports the applicative command set, such as the ISO7816-4 command set once the RF session is open.

5.4.2.1 GetChallenge command

When receiving the `GetChallenge` request, the ST25TA-E devices generate and return an 8-byte random value. Before sending a `GetChallenge` command, the ST25TA-E devices can be in PROTOCOL state or in SELECTED APP state.

Syntax: 00 84 00 00 08

Type: OUT

Instruction inputs: -

Instruction outputs:

- Retrieve 8-byte Data-out value matching with a new random value used by the cover coding process and in subsequent password related commands.
- Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Table 37. With C-APDU format

GC	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	0 byte	0 byte	1 byte
00h		84h	00h	00h	-	-	08h

Table 38. **With R-APDU format**

GC	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	0 byte	0 byte	1 byte
00h		84h	00h	00h	-	-	08h

5.4.2.2 *Verify command*

When receiving the `Verify` request, the ST25TA-E devices check if a password is required to access the EF file (no L_C field) or present a password and check that the password embedded in the `Verify` command allows the access to the memory (the L_c field = 8h). Before sending a `Verify` command, the ST25TA-E devices should be in SELECTED APP state.

Syntax: 00 20 00 *Id-in* or 00 20 00 *Id-in* 08 *Data-in*

Type: IN

Instruction inputs:

- Provide a 1 byte *id-in* identification value matching with the requested password identification to be presented or checked.
  - (CFG WR ID 00h)
  - (CFG RD ID 01h)
  - (NDEF WR ID 02h)
  - (NDEF RD ID 03h)
  - (ANDEF WR ID 04h)
  - (ANDEF RD ID 05h)
  - (PRIV ID 0Ch)
- Provide 8-byte *Data-in* Xored password value matching with the requested password value to be presented.

Instruction outputs: Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: The DF file must be selected prior to verifying the PRIV password (status check). The EF file must be selected prior to verifying the CFG/NDEF/ANDEF passwords.

The 8-byte data-in must follow the cover coding rules (obfuscation mechanism with Xor algorithm and an 8-byte challenge). Refer to Section 4.2.1: Cover coding. If required, the command `GetChallenge` must be requested prior to presenting the password.

Table 39. **With C-APDU format**

Verify	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	0 byte/ 1 byte	0 byte/Lc bytes	0 byte
00h		20h	00h	Id-in	-/8h	-/8h byte Data in	-

Table 40. **With R-APDU format**

Verify	Payload field		
	Data-out	SW1	SW2
Length	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.2.3 *ChangeReferenceData command*

When receiving the `ChangeReferenceData` request, the ST25TA-E devices replace the current embedded password value with a new data-in value. Before sending a `ChangeReferenceData` command, the ST25TA-E devices should be in the SELECTED APP state.

Syntax: 00 24 01 *Id-In* 08 *Data-in*

Type: IN

Instruction inputs:

- Provide a 1 byte *Id-in* identification value matching with the requested password to be changed.
  - (CFG WR ID 00h)
  - (CFG RD ID 01h)
  - (NDEF WR ID 02h)
  - (NDEF RD ID 03h)
  - (ANDEF WR ID 04h)
  - (ANDEF RD ID 05h)
  - (PRIV ID 0Ch)
- Provide 8-byte *Data-in* Xored password value matching with the requested password value to be presented.

Instruction outputs: Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: The 8-byte data-in must follow the cover coding rules (obfuscation mechanism with Xor algorithm and an 8-byte challenge). Refer to Section 4.2.1: Cover coding. If required, the `GetChallenge` command must be requested prior to changing the password value.

`Password` must be presented prior to changing the password.

The requested file must be selected prior to changing the password associated to the requested EF file.

The DF file must be selected prior to verifying the PRIV password.

The EF file must be selected prior to verifying the CFG/NDEF/ANDEF passwords.

Table 41. With C-APDU format

CRD	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	1 byte	Lc bytes	0 byte
00h		24h	01h	ID-in	08h	Data-In	-

Table 42. With R-APDU format

CRD	Payload field		
	Data-out	SW1	SW2
Length	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.2.4 *EnableVerificationRequirement command*

When receiving the `EnableVerificationRequirement` request, the ST25TA-E devices activate the password authentication on an EF file. Before sending an `EnableVerificationRequirement` command, the ST25TA-E devices should be in the SELECTED APP state.

Syntax: 00 28 *01 id-in* 08 *Data-in* or 00 28 *00 id-in*

Type: IN

Instruction inputs:

- Provide a 1 byte *Id-in* identification value matching with the requested password to be activated.
  - (CFG WR ID 00h)
  - (CFG RD ID 01h)
  - (NDEF WR ID 02h)
  - (NDEF RD ID 03h)
  - (ANDEF WR ID 04h)
  - (ANDEF RD ID 05h)
  - (PRIV ID 0Ch)
- Provide 8-byte *Data-in* Xored password value matching with the requested password value to be checked and then activated.

Instruction outputs: Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: The 8-byte Data-in shall follow the cover-coding rules (obfuscation mechanism with Xor algorithm and an 8-byte challenge). Refer to Section 4.2.1: Cover coding. If required, the command `GetChallenge` shall be requested prior to activating the password authentication.

If CFG WR authentication is enabled, the CFG WR password shall be presented prior to activating any password authentication.

The CFG file shall be selected prior to activating any password authentication.

Authentication with (PRIV ID=0Ch) password ID is enabled by default and cannot be deactivated with this command.

Other values of P1/P2 parameters are RFU and the error code should be returned.

Table 43. With C-APDU format

EVR	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	0 byte/1 byte	0 byte/Lc bytes	0 byte
00h		28h	00/01h	ID-in	-/8h	-/8-byte Data-Invalue	-

Table 44. With R-APDU format

EVR	Payload field		
	Data-out	SW1	SW2
Length	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.2.5 *DisableVerificationRequirement command*

When receiving the `DisableVerificationRequirement` request, the ST25TA-E devices deactivate the password authentication on an EF file. Before sending a `DisableVerificationRequirement` command, the ST25TA-E devices should be in the SELECTED APP state.

Syntax: 00 26 01 *id-in* 08 *Data-in* or 00 26 00 *id-in*

Type: IN

Instruction inputs:

- Provide a 1 byte *Id-in* identification value matching with the requested password to be activated.
  - (CFG WR ID 00h)
  - (CFG RD ID 01h)
  - (NDEF WR ID 02h)
  - (NDEF RD ID 03h)
  - (ANDEF WR ID 04h)
  - (ANDEF RD ID 05h)
- Provide 8-byte *Data-in* Xored password value matching with the requested password value to be checked and then activated.

Instruction outputs: Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: The 8-byte Data-in shall follow the cover coding rules (obfuscation mechanism with Xor algorithm and an 8-byte challenge). Refer to Section 4.2.1: Cover coding. If required, the command `GetChallenge` shall be requested prior to deactivating the password authentication.

If CFG WR authentication is enabled, the CFG WR password shall be presented prior to deactivating any password authentication.

The CFG file shall be selected prior to deactivating any password authentication.

Authentication with (PRIV ID 0Ch) password ID is enabled by default and cannot be deactivated with this command.

Other values of P1/P2 parameters are RFU and the error code should be returned.

Table 45. With C-APDU format

DVR	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	0 byte/1 byte	0 byte/Lc bytes	0 byte
00h		26h	00/01h	ID-in	-/8h	-/8-byte data-in value	-

Table 46. With R-APDU format

DVR	Payload field		
	Data-out	SW1	SW2
Length	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.3 ST proprietary command set

The ST25TA-E command supports the specific command set once the RF session is open.

5.4.3.1 *EnablePermanentRequirement command*

When receiving the `EnablePremanentRequirement` request, the ST25TA-E devices lock any EF file permanently. Before sending an `EnablePremanentRequirement` command, the ST25TA-E devices should be in the SELECTED APP state.

Syntax: A2 28 01 *Id-in*

Type: IN

Instruction inputs: Provide 1 byte *Id-in* value matching with EF file index with read or write access rights types.

- (CFG WR ID 00h)
- (CFG RD ID 01h)
- (NDEF WR ID 02h)
- (NDEF RD ID 03h)
- (ANDEF WR ID 04h)
- (ANDEF RD ID 05h)

Instruction outputs: Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: If the CFG WR authentication is enabled, the CFG WR password must be presented prior to forbidding (CFG/ NDEF/ANDEF/ RD/WR) access. The CFG file must be selected prior to locking these EF files.

Table 47. With C-APDU format

EPR	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	0 byte	0 byte	0 byte
A2h		28h	01h	Id-in	-	-	-

Table 48. With R-APDU format

EPR	Payload field		
	Data	SW1	SW2
Length	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.3.2 *ManageBasicLogicalChannel command*

When receiving the `ManageBasicLogicalChannel` request, the ST25TA-E devices switch on and off privacy modes. Before sending a `ManageBasicLogicalChannel` command, the ST25TA-E devices can be in PROTOCOL state or in SELECTED APP state.

Syntax: A2 70 *mode-in access-in* 08 *Data-in*

Type: IN

Instruction Inputs:

- Provide 1-byte *mode-in* operation value matching with the requested operation to be activated/disabled.
  - (ENABLE PRIV-ANONYMOUS 80h)
  - (DISABLE PRIV-ANONYMOUS 20h)
  - (ENABLE PRIV-KILL 10h) (warning: permanent kill operation)
- Provide 1-byte *access-in* value matching with the requested operation to be authorized.
  - Authorize PRIV-KILL mode 5Ah
  - Authorize PRIV--ANONYMOUS 00h
- Provide 8-byte *Data-in* Xored value matching with PRIV password.

Instruction outputs: Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: The 8-byte Data-in must follow the cover coding rules (obfuscation mechanism with Xor algorithm and an 8-byte challenge). Refer to Section 4.2.1: Cover coding. If required, the command `GetChallenge` must be requested prior to activating the password authentication.

Table 49. With C-APDU format

MBC	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	1 byte	Lc bytes	1 byte
A2h		70h	Mode-in	Access-in	08h	Data-in	-

Table 50. With R-APDU format

MBC	Payload field		
	Data-out	SW1	SW2
Length	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.3.3 *GetSystemInformation command*

When receiving the `GetSystemInformation` request, the ST25TA-E devices send back system information in the response. Before sending a `GetSystemInformation` command, the ST25TA-E devices can be in SELECTED APP state or in PROTOCOL state.

Syntax: A2 B6 P-*Id 00* Lc *Data-in* Le

Type: IN/OUT

Instruction inputs:

- Provide 1 byte *P-id* value matching with the number of requested groups.
  - (01h: one group)
  - (02h: two groups)
- Provide Lc value matching with the requested byte-data length. Each requested group needs 2 bytes (group ID index byte followed by the byte of the mask value in this group).
- Provide Lc-byte Data-in value matching with data Information per requested group ID:
  First byte with:
  - (01h system public information)
  - (02h extended public information)

  Second byte= Mask data byte of selected data into the group.

The different public group IDs are defined as follows:

Table 51. System information group

Bit	System information	Length (bytes)
b0	0: UID not requested 1: UID requested	7
b1	0: IC Ref not requested 1: IC Ref requested	1
b2	0: Usr Memory size not requested 1: Usr Memory size requested	2
b3	Reserved	1
b4	Reserved	1
b5	0: Fixed UID not requested 1: Fixed UID requested	4
b6	Reserved	1

Table 52. Extended system information group

Bit	Extended system information	Length (bytes)
b0	0: Product code not requested 1: Product code requested	2
b1	0: Revision not requested 1: Revision requested	1
b2	0: Dedicated revision not requested 1: Dedicated revision requested	2
b3	0: Full revision (or SoC revision) 1: Full revision requested	4

Instruction Outputs:

- Retrieve Le-byte Data-out value matching with system information response or extended system information response.
- Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: The response of the get system information command is successful when the data to be read is within the well-known group ID; in other words when the second or next group ID is not valid, the exact number of available data bytes are returned and the SW1 SW2 '9000' with the truncated data.

If the Le field contains only bytes set to '00', then all the bytes of the selected data information should be read.

Table 53. With C-APDU format

GSI	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	1 byte	Lc bytes	1 byte
A2h		B6h	P-ID	00h	(P1+P2)*2	Data information per group ID	Data length

Table 54. With R-APDU format

GSI	Payload field		
	Data-out	SW1	SW2
Length	Le bytes	1 byte	1 byte
System information		Status byte 1	Status byte 2

5.4.3.4 *GetGPCounter command (Get general purpose counter)*

When receiving the `GetGPCounter` request, the ST25TA-E devices send back GP counter value. Before sending a `GetGPCounter` command, the ST25TA-E devices can be in SELECTED APP state or PROTOCOL state.

Syntax: A2 C4 00 00 03

Type: OUT

Instruction inputs:-

Instruction outputs:

- Retrieve 3-byte data-out value matching with general purpose counter value.
- Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Table 55. With C-APDU format

GGC	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	0 byte	0 byte	1 byte
A2h		C4h	00h	00h	-	-	03h

Table 56. With R-APDU format

GGC	Payload field		
	Data-out	SW1	SW2
Length	Le bytes	1 byte	1 byte
GP counter		Status byte 1	Status byte 2

5.4.3.5 *RevertGPCounter command (Revert general purpose counter)*

When receiving the `RevertGPCounter` request, the ST25TA-E devices revert to the expected General Purpose counter value. Before sending a `RevertGPCounter` request, the ST25TA-E devices should be in the SELECTED APP state.

Syntax: A2 D4 *Op-In* 00

Type: IN

Instruction inputs:

Provide 1 byte *Op-in* value matching with the revert operation to be executed:

- (00h: decrement by one)
- (01h: reset to initial value)

Instruction outputs:

Instruction fully executed or error status. Refer to Table 27. SW1-SW2 codes into the ST25TA-E devices.

Note: If the CFG WR authentication is enabled, the CFG WR password must be presented prior to reverting to the expected GP counter value.

Note: The CFG file must be selected prior to reverting to the expected GP counter value.

Table 57. With C-APDU format

RGC	Payload field						
	CLA	INS	P1	P2	Lc	Data-in	Le
Length	1 byte	1 byte	1 byte	1 byte	0 byte	0 byte	0 byte
A2h		D4h	Op-In	00h	-	-	-

Table 58. With R-APDU format

RGC	Payload field		
	Data-out	SW1	SW2
Length	Le bytes	1 byte	1 byte
-		Status byte 1	Status byte 2

5.4.4 ISO14443-4 / NFC-A command- set

The ST25TA-E command supports the specific command set, once the RF session is open.

5.4.4.1 *Anticollision command set*

The table below lists the commands that can be issued only by the RF host. The format of these commands is described in the NFC Forum Digital Protocol specification.

Table 59. Commands issued by the PCD

Family command-set	Command name	Instruction
NFC-A technology	ALL_REQs	52h
	SENS_REQs	26h
	SDD_REQ	93h or 95h
	SEL_REQ	9370h or 9570h
	SLP_REQ	50h

The parameter values for ISO/IEC 14443 activation and selection, used by the ST25TA-E device can be summarized by as follows:

Table 60. Anticollision and activation parameters

Family command-set			Command name	Instruction
ATQA	SENS_REQ or ALL-REQ	52h or 26h	0042h or 0002h(*)	(*): Random UID
SAK1	SEL_REQ	93h	04h or 20h(*)	(*): Random UID
SAK2	SEL_REQ	95h	20h	-

ATQA value is 0042h, which denotes a double size (7 byte) UID. However, ST25TA-E offers a configuration of random ID, which is single size (4 byte). If the random ID feature is enabled, then the ATQA is changed to 0002h.

According to ISO/IEC 14443-3, the ATQA bytes are transmitted as LSB first. The value of SAK1, for double size UID, in cascade level 1 is 04h, indicating that the UID is not complete. SAK2 in cascade level 2 is 20h, indicating UID complete and supporting ISO/IEC 14443-4.

For single size UID, which is used in the random ID case, the value of SAK is 20h, indicating UID complete and supporting ISO/IEC 14443-4.

5.4.4.2 *RATS command and ATS response*

RATS command and ATS response are used for NFC Forum Type 4A Tag Platform Device Activation (as defined in the NFC Forum Digital Protocol specification).

The table below details the RATS command. This command shall be sent after the anticollision process and expects an ATS response from the ST25TA-E device.

Table 61. RATS command

Name	INS	Payload		CRC
Byte field	**0x0E**	**1 byte**		**2 bytes**
Bit field	**-**	**b7-b4**	**b3-b0**	**2 bytes**
Instruction code				
FSDI				
DID (0<=DID <=14)				
2 CRC bytes				

The FSDI field codes the FSD that defines the maximum size that the PCD is able to receive. The table below gives the conversion from FSDI to FSD.

Table 62. Conversion from FDSI to FSD

FDSI	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9-0xE	0xF
FSD	16	24	32	40	48	64	96	128	256	RFU	256

The DID (Dynamic ID, optionally affected to the ST25TA-E by the host to address ST25TA-E in all commands) field defines the value of the addressed ST25TA-E.

If DID is not '0', the ST25TA-E ignore the command if it contains a DID different from the one affected to ST25TA-E during RATS.

Table 63. ATS response

Name	TL	T0	TA(1)	TB(1)		TC(1)	CRC
Byte field	0x05	0x77	0x80	0x81		0x2	2 bytes
Bitfield	-	-	-	b7-b4	b3-b0	-	-
Length of the ATS response							
FSCI=7, FSC= 128 bytes							
The maximum ascending data rate is 106 kbps. The maximum descending data rate is 106 kbps							
FWI field (FWI= 8 -> FWT = 77.3 ms)							
SFGI field (SFGI = 1 -> SFGT = 604 us)							
The DID is supported							
2 CRC bytes							

5.4.4.3 *PPS command and response*

PPS (protocol and parameter selection) command and response are defined in ISO/IEC 14443-4, in the protocol activation of PICC Type A.

The PPS command allows the user to change the ascending (PCD to ST25TA-E device) and descending (ST25TA-E to PCD) data rates. Usage of this command is optional, as the ST25TA-E devices only support 106 Kbit/s in both directions.

Table 64. PPS command

Name	INS (PPSs)		PPS0	PPS1			CRC
Byte field	0xDx		0x11	1 byte			2 bytes
Bitfield	b7-b4, b3-b0			b7-b4	b3-b2	b1-b0	-
Description	Instruction code	DID	PPS1 is present	RFU	Descending data rate (106 kbps) = 0b00	Ascending data rate (106 kbps) =0b00	CRC

The ascending and descending data rates shall be coded as described in the table below.

Table 65. Ascending and descending data rate coding

Value	0b00	0b01	0b10	0b11
Data rate	106 kbps	RFU	RFU	RFU

When the ST25TA-E devices receive a PPS request as described in Table 64. PPS command, they return the following response. The data rate of this response is 106 kbps. The table below provides the details of the PPS response.

Table 66. **PPS response**

Name	Response (PPSs)		CRC
Byte field	0xDx	-	2 bytes
Bitfield	b7-b4	B3-b0	-
Description	Response code	DID field	CRC

5.4.4.4 *DeSelect command*

The `DeSelect` command and response are defined in ISO/IEC 14443-4, in the protocol deactivation of PICC Type A. This command makes it possible to put the tag in standby power mode (this state can also be reached by a shutdown of the RF field.) It consists of an S(DES) request block (see Section 5.3.3: S-block format) sent by the RF host and an S(DES) response sent as acknowledge by the tag.

6 Product identification and user information

6.1 Product identifier: Unique identifier (UID)

Each ST25TA-E device is uniquely identified by a 7-byte unique identifier (UID). The UID is compliant with ISO/IEC 14443-A and ISO/IEC 7816-6. The UID is a read-only code and comprises:

- The 1-byte IC manufacturer code (0x02 for STMicroelectronics).
- A device number which is an 6-byte unique device value.

The table below describes the UID format.

Table 67. UID format

UID0	UID1:UID6
b55-b48	b47-b0
0x02	6 bytes
IC manufacturer	
Unique device number	

6.2 Product identifier: Untraceable UID and nonunique ID (NUID)

The support of random ID feature is implemented according to ISO/IEC14443-3 standard, it allows only single 4-byte UID to be a nonunique fixed number or a random UID with respectively, UID0= xFh and UID0= 08h.

Note: In anonymous mode, the UID size is updated in the ATQA parameter and SAK1 parameter when the nonunique UID is used.

Table 68. Random UID information

UID0	UID1:UID3
b31-b24	b23-b0
0x08	3 bytes
Single-NUID	
Device number	

Table 69. NUID information

UID0	UID1:UID3
b31-b24	b23-b0
0x5F	3 bytes
Single-NUID	
Device number	

Note: The usage of the NUID and random UID are detailed in Section 4.7.2: Anonymous mode description .

The CFG_UID register contents the 7-byte UID (refer to Table 67. UID format) except when the ST25TA-E devices meet either of the following conditions:

- The current RF session started in UNTRACEABLE state.
- The current state is UNTRACEABLE state.

Then the content of the CFG_UID register (refer to Section 3.7: CFG file layout) is overwritten immediately with null value. When the ST25TA-E devices exit from the UNTRACEABLE state, the content of the register is reverted immediately to the 7-byte UID value.

Note: Product identifier UID cannot be retrieved by issuing `GetSystemInformation` command or by issuing a `ReadBinary` command in the selected CFG file in UNTRACEABLE state whereas the product identifier UID can be retrieved with the two manners when the device exit from privacy mode.

When the ST25TA-E devices meet the following conditions:

- The current RF session started in PROTOCOL state and switch in UNTRACEABLE state.
- A power-off is issued prior to a select command.

Then the 4-byte random or fixed UID is delivered in the next RF session.

When the ST25TA-E devices meet the following conditions:

- The current RF session started in PROTOCOL state and switch in UNTRACEABLE state.
- A `DeSelect` command is issued prior to a select.

Then the 7-byte unique UID is delivered in the current RF session even if the ST25TA-E devices are in UNRTACEABLE state.

6.3 Product information

The IC product code if the ST25TA-E device is identified by the 1-byte unique identifier (IC ref).

Table 70. IC REF information

User information	Value
IC ref	0x9A

The Mem Size of the ST25TA-E device is identified by the 2-byte field and defined the user memory size of the 2 Kbits NDEF file.

Table 71. Memsize information

User information	Value
Mem size	0x00FF

Note: Both product information can be retrieved by issuing `GetSystemInformation` command or by issuing a `ReadBinary` command in the selected CFG file.

7 Device parameters

This section summarizes the operating and measurement conditions, and the DC and AC characteristics of the devices in RF mode.

The parameters in the DC and AC characteristics tables that follow are derived from tests performed under the measurement conditions summarized in the relevant tables.

Designers should check that the operating conditions in their circuit match the measurement conditions when relying on the quoted parameters.

7.1 Absolute maximum ratings

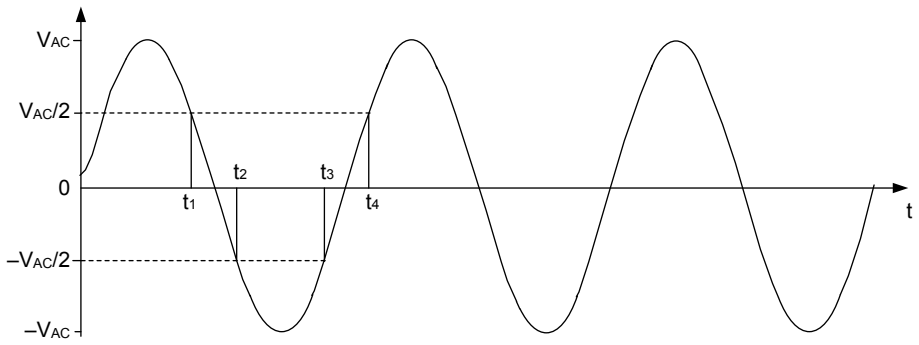
Stressing the device above the ratings listed in Table 72. Absolute maximum ratings. Absolute maximum ratings may permanently damage it. These are stress ratings only and operation of the device, at these or any other conditions above those indicated in the operating sections of this specification, is not implied. Exposure to absolute maximum rating conditions for extended periods may affect the device reliability. Refer also to the STMicroelectronics SURE program and other relevant quality documents.

Table 72. Absolute maximum ratings

Symbol	Description	Min	Max	Unit
T_A	Ambient operating temperature	-25	+85	°C
T_{STG}	Storage temperature	-40	+125	°C
t STG	Storage duration	-	9(1)	months
V_{esd} AC0, AC1	Electrostatic discharge voltage product according to JESD22-A114(human body model)	-	4000	V
V max carrier	Maximum input voltage (pins AC0, and AC1)	-	+/- 5.7	V
S_{max}(2)	Carrier signal maximum rising and falling slope	-	+/- 1.59	V/ns

1. *Counted from ST production date*
2. *Refer to figure below Smax failing slope = Vac/(t2-t1)Smax rising slope= Vac/(t4-t3)*

Figure 8. Carrier signal waveform



8 Package information

In order to meet environmental requirements, ST offers these devices in different grades of ECOPACK packages, depending on their level of environmental compliance. ECOPACK specifications, grade definitions and product status are available at: www.st.com. ECOPACK is an ST trademark.

8.1 Sawn and bumped wafer

Contact your STMicroelectronics sales office to get the die description document.

9 Ordering information

Example: **ST25 T** **A** **E** **xxx** **-** **A** **I** **Y** **6**

Device type

ST25 T: Tags

Protocol type

A: NFC Forum T4A

Crypto type

E: ECC crypto

Customer code

xxx = customer code

Hardware interface

A: no interface

Features

I: internal provisioning

Package

E: 140 µm ± 10 µm bumped and sawn wafer

F: 75 µm ± 10 µm bumped and sawn wafer

Capacitor value

6: 68 pF

Note: For a list of available options (speed, package, etc.) or for further information on any aspect of this device, contact your nearest STMicroelectronics sales office.

Revision history

Table 73. **Document revision history**

Date	Revision	Changes
01-Dec-2023	1	Initial release.
19-Mar-2024	2	Updated the following: • Section Features • Section 1: Description
02-Apr-2024	3	Document scope change.
19-Jun-2024	4	General data brief update.
26-Jul-2024	5	Minor editorial changes. First public version.
31-Jan-2025	6	Updated the following: • Section 3.1: CC (capacity container) file layout • Section 3.3: ANDEF file layout • Section 3.7: CFG file layout • Section 4.3.1: ANDEF description • CFG_GP_CNT_OFFSET_ADD • CFG_PRIV_NUID register • Section 5.2: State machine • Section 5.4.3.2: ManageBasicLogicalChannel command • Section 5.4.4.2: RATS command and ATS response • Section 6.2: Product identifier: Untraceable UID and nonunique ID (NUID) • Section 4.7.1: Kill mode description • Section 4.7.2: Anonymous mode description • Section 9: Ordering information

Glossary

Native operation Operation running on the operating system of the reader device, communicating with the tag, without any external software layers such as mobile custom application. Only the NFC T4T command-set is used in this native operation.

Tap action Action that allows to detect NFC devices, exchange NFC messages or digital content, and connect electronic devices, such as smartphone, with a touch. NFC exchanges are short range (from a touch to a few centimeters) and require the devices to be in close proximity.

Contents

List of tables

List of figures