AN5614

Application note

Migrating from ST25TVxxx to ST25TVxxxC

Introduction

The ST25TVxxx and ST25TVxxxC are EEPROM memory devices, with an ISO/IEC ISO15693 RF interface and an optional tamper detection interface.

The ST25TVxxxC is an update of the ST25TVxxx, including an additional Augmented NDEF feature.

The purpose of this document is to explain how to migrate from the ST25TVxxx tag to the ST25TVxxxC tag.

The new Augmented NDEF feature is not discussed in this document.

Table 1. **Applicable products**

Type	Part numbers	
	ST25TVxxx	ST25TVxxxC
RF interface EEPROM	ST25TV512	ST25TV512C
	ST25TV02K	ST25TV02KC

1 Acronyms and notational conventions

1.1 Acronyms

Table 2. List of acronyms

Acronym	Definition
AFI	Application family identifier
AN	Application note
CC	Capability container file as defined by the NFC Forum T5T specification
CRC	Cyclic redundancy check
DSFID	Data storage format identifier
DS	Datasheet
EAS	Electronic article surveillance
EEPROM	Electrically erasable programmable read-only memory
EOF	End of frame
FID	Feature identifier
IC	Integrated circuit
IC Ref	Integrated circuit reference
IEC	International electrotechnical commission
ISO	International organization for standardization
NA	Not applicable
NDEF	NFC data exchange format defined by the NFC Forum
NFC	Near field communication
PID	Parameter identifier
RF	Radio frequency
SOF	Start of frame
TD	Tamper detection
UID	Unique identifier
UFDFPN	Ultra-thin fine pitch dual flat package No-lead
VCD	Vicinity coupling device
VICC	Vicinity integrated circuit card

1.2 Conventions

The following conventions and notations apply in this document unless otherwise stated.

1.2.1 Product family denomination

Product families are abbreviated as follows:

- ST25TVxxx refers to the ST25TV02K product family which includes ST25TV512 and ST25TV02K
- ST25TVxxxC refers to the ST25TV02KC product family which includes ST25TV512C and ST25TV02KC

1.2.2 Binary number representation

Binary numbers are represented by strings of 0 and 1 digits, with the most significant bit (MSB) on the left, the least significant bit (LSB) on the right, and a ‘b’ suffix added at the end.

Example: 11110101b

1.2.3 Hexadecimal number representation

Hexadecimal numbers are represented by strings of numbers from 0 to 9 and letters from A to F, and an ‘h’ suffix added at the end. The most significant byte (MSB) is shown on the left and the least significant byte (LSB) on the right.

Example: F5h

1.2.4 Decimal number representation

Decimal numbers are represented without any trailing character.

Example: 245

2 ST25TVxxx and ST25TVxxxC product feature comparison

Table 3 lists the features of ST25TVxxx and ST25TVxxxC products. For full details, please refer to the ST25TVxxx [1] and ST25TVxxxC [2] product datasheets.

Table 3. Feature comparison summary

<table>
<tr><th>Feature</th><th>ST25TVxxx</th><th>ST25TVxxxC</th></tr>
<tr><td>Pinout</td><td colspan="2">Same pinout</td></tr>
<tr><td rowspan="4">Package</td><td colspan="2">Sawn and bumped wafer, 120 +/- 10 µm</td></tr>
<tr><td colspan="2">Sawn and bumped wafer, 75 +/- 10 µm</td></tr>
<tr><td colspan="2">UFDFPN5 (with tamper detection interface only)</td></tr>
<tr><td>Unsawn wafer, 725 +/- 20 µm</td><td>NA</td></tr>
<tr><td rowspan="2">Tuning capacitance</td><td colspan="2">23 pF</td></tr>
<tr><td colspan="2">99.7 pF</td></tr>
<tr><td rowspan="3">Contactless interface</td><td>ISO/IEC 15693 compliant</td><td>ISO/IEC 15693 compliant[1]</td></tr>
<tr><td colspan="2">NFC Forum Type 5 Tag, certified by the NFC Forum</td></tr>
<tr><td>Max Rx datarate: 53 kbit/s</td><td>Max Rx datarate: 26 kbit/s</td></tr>
<tr><td rowspan="8">Memory</td><td colspan="2">Block size: 4 bytes</td></tr>
<tr><td colspan="2">ST25TV512, ST25TV512C: 16 blocks</td></tr>
<tr><td>ST25TV02K: 64 blocks</td><td>ST25TV02KC: 80 blocks</td></tr>
<tr><td colspan="2">Single block write access, single and multiple block read access</td></tr>
<tr><td colspan="2">Data retention: 60 years at 55°C</td></tr>
<tr><td colspan="2">Minimum endurance: 100k write cycles</td></tr>
<tr><td>16-bit write event counter</td><td>24-bit unique tap code[1]</td></tr>
<tr><td>NA</td><td>Augmented NDEF</td></tr>
<tr><td rowspan="7">Password management</td><td colspan="2">4 x 32-bit passwords registers, cover coding (C)</td></tr>
<tr><td colspan="2">PresentPassword (C: yes), 32 or 64 bits (single area password)</td></tr>
<tr><td>WritePassword (C: no), 32 bits only</td><td>WritePassword (C: yes), 32 | 64 bits</td></tr>
<tr><td>Kill (C: no), LockKillPassword</td><td>Kill (C: yes)</td></tr>
<tr><td>EnableUntraceableMode (C: yes)</td><td>ToggleDiscreetSilent (C: yes)</td></tr>
<tr><td>NA</td><td>Tearproof update procedure</td></tr>
<tr><td>NA</td><td>Failed attempt counters</td></tr>
<tr><td rowspan="3">System configuration</td><td>1-byte parameter identifier (P)</td><td>2-byte parameter identifier (F,P)</td></tr>
<tr><td>Immediate activation time</td><td>Delayed activation time</td></tr>
<tr><td>Global lock of registers</td><td>Family-wise (F) lock of registers</td></tr>
<tr><td rowspan="5">Data protection</td><td colspan="2">Single area mode: access to AREA1 protectable by 1x 64-bit password
Dual area mode: access to AREA1/2 protectable by 2x 32-bit passwords</td></tr>
<tr><td>Dual area: fixed boundary</td><td>Dual area: configurable boundary</td></tr>
<tr><td colspan="2">System configuration: access protected by a 32-bit password</td></tr>
<tr><td colspan="2">Permanent write lock of specific user area blocks</td></tr>
<tr><td colspan="2">Temporary write lock at user area level</td></tr>
<tr><td rowspan="2">Product identification and protection</td><td colspan="2">Tamper detection: open/short status of tamper loop detected during boot</td></tr>
<tr><td>NA</td><td>Memorization of tamper events[1]</td></tr>
</table>

<table>
<tr><th>Feature</th><th>ST25TVxxx</th><th>ST25TVxxxC</th></tr>
<tr><td rowspan="5">Product identification and protection</td><td>NA</td><td>Identification of input capacitance</td></tr>
<tr><td colspan="2">InventoryInitiated commands for custom anticollision procedure</td></tr>
<tr><td>InventoryRead command</td><td>NA</td></tr>
<tr><td colspan="2">TruST25 digital signature</td></tr>
<tr><td>Electronic article surveillance</td><td>AFI protection</td></tr>
<tr><td rowspan="4">Privacy</td><td>Kill command always enabled</td><td>Kill command can be disabled</td></tr>
<tr><td>Untraceable mode (smartphone interoperability disabled) activated by command</td><td>Silent mode (smartphone interoperability disabled) activated by command</td></tr>
<tr><td>NA</td><td>Discreet mode (smartphone interoperability enabled) activated by command</td></tr>
<tr><td>NA</td><td>Silent/Discreet modes activated by default, or by tamper status</td></tr>
</table>

1. *The boot time of the ST25TVxxxC may exceed the guard time specified in [3] when the ‘unique tap code’ feature or the ‘tamper event memorization’ feature is active.*

3 Hardware considerations

ST25TVxxx and ST25TVxxxC products are available in 120 µm and 75 µm thick wafers (sawn and bumped).

Only ST25TV02K and ST25TV02KC products are available in UFDFPN5 packages, for the version providing a tamper detection interface.

Only ST25TV02K products are available in 725 µm thick wafers (unsawn).

ST25TVxxx and ST25TVxxxC products are pin-to-pin compatible when using the same package.

Table 4. ST25TVxxx and ST25TVxxxC product package availability

Product	Package			
	Wafer 75µm	Wafer 120µm	UFDFPN5	Wafer 725µm
ST25TV512	X	X	-	-
ST25TV512C	X	X	-	-
ST25TV02K	X	X	X[1]	X
ST25TV02KC	X	X	X[1]	-

1. Only for the tamper detection version of the product.

Migrating from a ST25TVxxx product to a ST25TVxxxC product with identical input capacitance (23pf or 99.7pF) does not require a modification of the antenna design.

4 RF operations

ST25TVxxx and ST25TVxxxC products are based on the ISO/IEC 15693 standard and are certified by the NFC Forum as Type 5 tags.

ST25TVxxx and ST25TVxxxC products both address RF blocks of 4 bytes.

ST25TVxxx and ST25TVxxxC products are similar in their RF operations (protocol, modulations, and timings) and support of standard ISO15693 commands, but they differ in their custom commands.

4.1 RF command list

Table 5 shows the differences in standard commands supported by ST25TVxxx and ST25TVxxxC:

- the support of the ExtendedGetSystemInfo command has been added to the ST25TVxxxC. This command can be used to retrieve the list of optional commands supported by the ST25TVxxxC.
- the WriteAFI and LockAFI commands may be protected by password on the ST25TVxxxC (see Section 11.8: AFI protection).

Table 5. **ISO/IEC 15693 mandatory and optional commands supported in ST25TVxxx and ST25TVxxxC products**

Command code	ST25TVxxx	ST25TVxxxC	Comment
01h	Inventory		Same behaviors
02h	StayQuiet		
20h	ReadSingleBlock		
21h	WriteSingleBlock		
22h	LockBlock		
23h	ReadMultipleBlocks		
25h	Select		
26h	ResetToReady		
27h	WriteAFI		Protectable on ST25TVxxxC
28h	LockAFI		
29h	WriteDSFID		Same behaviors
2Ah	LockDSFID		
2Bh	GetSystemInfo		
2Ch	GetMultipleBlockSecurityStatus		
3Bh	-	ExtendedGetSystemInfo	ST25TVxxxC only

Table 6 shows the differences in custom commands supported by ST25TVxxx and ST25TVxxxC products:

- the command set related to the EAS feature is not supported on the ST25TVxxxC.
- the commands allowing a response data rate of 53 kbit/s are not supported on the ST25TVxxxC.
- the InventoryRead feature is not supported on the ST25TVxxxC.
- some differences in the format or the behavior of ReadConfig, WriteConfig, Kill, WritePassword and PresentPassword commands, detailed in following sections.

Table 6. **ISO/IEC 15693 custom commands supported in ST25TVxxx and ST25TVxxxC products**

Command code	ST25TVxxx	ST25TVxxxC	Comment
A0h	ReadConfig[1]		Section 6.1: Configuration commands
A1h	WriteConfig[1]		
A2h	SetEAS	-	ST25TVxxx only
A3h	ResetEAS	-	
A4h	LockEAS	-	
A5h	EnableEAS	-	
A6h	Kill[1]		Section 12.2: Behavior on erroneous commands in non-addressed mode and Section 10.1: Kill mode
A7h	WriteEASId	-	ST25TVxxx only
A8h	WriteEASConfig	-	
B1h	WritePassword[1]		Section 12.2: Behavior on erroneous commands in non-addressed mode
B2h	LockKill	-	ST25TVxxx only
B3h	PresentPassword[1]		Section 12.2: Behavior on erroneous commands in non-addressed mode
B4h	GetRandomNumber		Same behaviors
BAh	EnableUntraceableMode	ToggleDiscreetSilent	Section 12.2: Behavior on erroneous commands in non-addressed mode and Section 10.2: Untraceable and Silent modes
C0h	FastReadSingleBlock	-	ST25TVxxx only
C1h	FastInventoryInitiated	-	
C2h	FastInitiate	-	
C3h	FastReadMultipleBlocks	-	
D1h	InventoryInitiated		Same behaviors
D2h	Initiate		
D3h	InventoryRead	-	ST25TVxxx only
D4h	FastInventoryRead	-	

[1] *Different behaviors on ST25TVxxx and ST25TVxxxC products*

4.2 RF boot time

The boot time of ST25TVxxx devices is always lower than 1 ms:

- it is compliant with the 1 ms guard time specified in the ISO15693 ([3]) specification.
- it is compliant with the 5 ms guard time specified in the T5T ([5]) specification.

When the unique tap counter (see Section 8.2: Unique tap code) and tamper event memorization (see Section 9.2: Tamper event memorization) features of a ST25TVxxxC device are inactive, the boot time is lower than 1 ms:

- it is compliant with the 1 ms guard time specified in the ISO15693 ([3]) specification.
- it is compliant with the 5 ms guard time specified in the T5T ([5]) specification.

When either of the unique tap counter or tamper event memorization features of a ST25TVxxxC device is active, the boot time is lower than 5 ms and may be greater than 1 ms:

- it is not compliant with the 1 ms guard time specified in the ISO15693 ([3]) specification.
- it is compliant with the 5 ms guard time specified in the T5T ([5]) specification.

5 Password management

5.1 Password identifiers

Table 7 shows the differences in the usage of password identifiers on ST25TVxxx and ST25TVxxxC products.

Table 7. Usage of password identifiers on ST25TVxxx and ST25TVxxxC products

Id	ST25TVxxx	ST25TVxxxC	Comment
00h	PWD_KILL	PWD_CFG	ST25TVxxx: Untraceable and Kill modes. ST25TVxxxC: CONFIG session and Kill mode.
01h	PWD_A1		Similar usage on ST25TVxxx and ST25TVxxxC products. ST25TVxxxC: 01h usable for AFI protection.
02h	PWD_A2		Similar usage on ST25TVxxx and ST25TVxxxC products. Difference on usage of 02h in single area mode.
03h	PWD_CFG	PWD_PRIV	ST25TVxxx: CONFIG session. ST25TVxxxC: PRIV session and Silent/Discreet modes.

Password identifiers 01h and 02h have a similar usage on ST25TVxxx and ST25TVxxxC products:

- They are respectively used to open a security session protecting the access to blocks from AREA1 and AREA2 in user memory (see Section 7.2: User areas).
- In dual area mode (AREA1 and AREA2 available):
  - the access to blocks from AREA1 and AREA2 is respectively protected by the 32-bit PWD_A1 and PWD_A2 passwords.
  - both password identifiers can be used with the PresentPassword and WritePassword commands.
- In single area mode (AREA1 only), PWD_A1 and PWD_A2 passwords are handled by the PresentPassword command as a single 64-bit password identified with value 01h, and usage of password identifier 02h is:
  - forbidden with the PresentPassword command on both products
  - granted with the WritePassword command on the ST25TVxxx (see Section 5.5.2: Update of AREA1 password in single area mode)
  - forbidden with the WritePassword command on the ST25TVxxxC (see Section 5.5.2: Update of AREA1 password in single area mode)

Password identified by value 01h may be used to protect the write access to the AFI parameter on the ST25TVxxxC only (see Section 11.8: AFI protection).

The password used to manage the CONFIG security session is identified by 03h and 00h on ST25TVxxx and ST25TVxxxC products respectively.

The password used to manage the Kill mode is identified by 00h on both products.

The password used to manage the Untraceable mode is identified by 00h on the ST25TVxxx product.

The password used to manage the PRIV security session and the Silent and Discreet modes is identified by 03h on the ST25TVxxxC product.

5.2 Password encryption

An encryption mechanism - known as cover coding - is used to transmit coded password values in the Password_data field of some command frames on both products:

Table 8. **Usage of cover coding on ST25TVxxx and ST25TVxxxC products**

Command	ST25TVxxx	ST25TVxxxC	Comment
PresentPassword	Yes		Used on both products
WritePassword	No	Yes	Plain value on ST25TVxxx
Kill	No	Yes	Plain value on ST25TVxxx
EnableUntraceableMode	Yes	-	ST25TVxxx-only command
ToggleDiscreetSilent	-	Yes	ST25TVxxxC-only command

This mechanism requires that a call to the GetRandomNumber command has been issued since the latest boot of a device, the responded random number is used to encrypt a plain password by application of a binary XOR operation.

See “Password encryption“ section of the ST25TVxxxC product datasheet [2] for further details on this encryption mechanism.

5.2.1 Behavior on invalid password presentation

Let RN1 be the latest value responded by the GetRandomNumber command since the boot of a device.

On both products, a command using cover coding fails if an invalid value of Password_data – that is, an invalid plain password value encrypted with RN1 – is presented (this does not apply to the WritePassword command).

However, the products behave differently for the subsequent presentation of an encrypted password in the same RF session (that is, without reset of the RF field since the invalid password presentation):

- On ST25TVxxx, the same random number RN1 may be reused for the generation of the next value of Password_data. If this next value corresponds to the correct plain password value encrypted with RN1, it is handled as the valid password value and the cover coding command succeeds.
- On ST25TVxxxC, the same random number RN1 cannot be reused for the generation of the next value of Password_data. If this next value corresponds to the correct plain password value encrypted with RN1, it is still handled as an invalid password value and the cover coding command fails.
- On ST25TVxxxC, it is mandatory to issue a new call to the GetRandomNumber command – responding a new value RN2 – for the generation of subsequent Password_data value. If the next value corresponds to the correct plain password value encrypted with RN2, it is handled as the valid password value and the cover coding command succeeds.

Note: *On ST25TVxxx and ST25TVxxxC products, the RN1 value may be kept during a RF session for generation of encrypted Password_data values as long as the password presentations succeed.*

5.3 Failed attempt counters

The ST25TVxxxC devices offer the capability to protect a password against brute-force attacks, thanks to a limiter mechanism on failed password attempts with the PresentPassword, Kill and ToggleDiscreetSilent commands.

Refer to AN5577 ([7]), for more details on how to use it. Contact your STMicroelectronics sales office to get this document.

5.4 PresentPassword command

The format of the PresentPassword command - depicted in the following table - is identical on ST25TVxxx and ST25TVxxxC products.

Table 9. **PresentPassword request format**

SOF	Request_flags	Opcode	IC Mfg code	UID [1]	Password_id	Password_data[2]	CRC_B	EOF
-	00xx00xxb	B3h	02h	64 bits	8 bits	32 or 64 bits	16 bits	-

1. *UID field present when Request_flags=001000xxb.*
2. *The unique case of 64 bits password is for Password_id=01h in single area mode.*

On both products, the unique valid Password_data value is obtained from the encryption of the plain password value (see Section 5.2: Password encryption).

The response time of the PresentPassword command is identical on both products in case of success: its value is t_1 = 320.9 µs.

The products differ on the response time of the PresentPassword command in case of invalid Password_data value:

- On ST25TVxxx, the response time is W_t=5.2 ms.
- On ST25TVxxxC, the response time is t1 when select_flag = 1 (in SELECTED state) or address_flag = 1, otherwise no response is sent (see Section 12.2: Behavior on erroneous commands in non-addressed mode).

The behaviors of the products are different after the presentation of an invalid value of Password_data with the PresentPassword command (see Section 12.1: Behavior on invalid settings of Request_flags):

- On ST25TVxxx, a call to GetRandomNumber command is not needed before attempting a new call to a command using cover coding in the same RF session.
- On ST25TVxxxC, a call to GetRandomNumber command is mandatory before attempting a new call to a command using cover coding in the same RF session.

The following subsections describe behavioral differences of the products for this command.

5.4.1 Presentation of password with identifier value 00h

Table 10 shows the differences in the usage of password identifier 00h with the PresentPassword command on ST25TVxxx and ST25TVxxxC products.

Table 10. **Usage of password identifier 00h with PresentPassword**

State	ST25TVxxx	ST25TVxxxC	Comment
READY SELECTED QUIT	-	PWD_CFG	ST25TVxxx: identifier 00h forbidden with PresentPassword while in ISO15693 standard state
UNTRACEABLE	PWD_KILL	-	ST25TVxxx : PresentPassword with identifier 00h used to switch from UNTRACEABLE to READY state
DISCREET	-	-	ST25TVxxxC: PresentPassword command not supported in DISCREET
SILENT	-	-	ST25TVxxxC: PresentPassword command not supported in SILENT
KILLED	-	-	No command supported in KILLED state

On the ST25TVxxxC product, the value 00h of Password_id is used with the PresentPassword command while in an ISO15693 state (READY, SELECTED or QUIET) to open the CONFIG security session: protected access to system configuration registers is granted (if not locked) when the valid password is presented.

On the ST25TVxxx product:

- the value 00h of Password_id is used with the PresentPassword command while in UNTRACEABLE state to return to the READY state (see Section 10.2: Untraceable and Silent modes).
- the value 00h of Password_id is forbidden with the PresentPassword command while in READY, SELECTED or QUIET state, the write access to the PWD_KILL password does not depend from a security session opened with the PresentPassword command (see Section 5.5.3: Update of password with identifier value 00h).

5.5 WritePassword command

The format of the WritePassword command - depicted in the following table - is similar on ST25TVxxx and ST25TVxxxC products, but they are behavioral differences (see following subsections).

Table 11. **WritePassword request format**

SOF	Request_flags	Opcode	IC Mfg code	UID[1]	Password_id	Password_data	CRC_B	EOF
-	0xxx00xxb	B1h	02h	64 bits	8 bits	32 bits or 64 bits[2]	16 bits	-

1. *UID field present when Request_flags=0x1000xxb.*
2. *64-bits password is used only by ST25TVxxxC in single area mode with Password_id=01h.*

5.5.1 Value of Password_data field

On the ST25TVxxx product, the Password_data field contains a **plain** password value.

On the ST25TVxxxC product, the Password_data field contains an **encrypted** password value (see Section 5.2: Password encryption).

Danger: *On the ST25TVxxxC product, if a plain value is mistakenly used in the Password_data field of the WritePassword command:*

- *the presentation of its encrypted value with the PresentPassword command will fail.*
- *the actual plain password value updated on the device will remain unknown if the random number value used before the call to WritePassword was not saved jointly with the transmitted Password_data value.*

Note: On the ST25TVxxxC product, the random number used in password encryption of the preceding PresentPassword command may be reused in password encryption of the WritePassword command.

5.5.2 Update of AREA1 password in single area mode

In single area mode, both products use a concatenation of 32-bit passwords PWD_A1 and PWD_A2 to protect the access to blocks from AREA1 with a 64-bit password identified by value 01h. This password is presented with a 64-bit Password_data field in the PresentPassword command.

However, the products differ in the procedure used to update the 64-bit password while in single area mode:

- On a ST25TVxxx, the following procedure is used:
  1. GetRandomNumber request if needed.
  2. PresentPassword command requested with Password_id=01h and valid 64-bit encrypted Password_data value.
  3. WritePassword command requested with Password_id=01h and valid 32-bit plain Password_data value. This updates the PWD_A1 register with the plain Password_data value.
  4. WritePassword command requested with Password_id=02h and valid 32-bit plain Password_data value. This updates the PWD_A2 register with the plain Password_data value.

- On a ST25TVxxxC, the following procedure is used:

1. GetRandomNumber request if needed.
2. PresentPassword command requested with Password_id=01h and valid 64-bit encrypted Password_data value.
3. WritePassword command requested with Password_id=01h and valid 64-bit encrypted Password_data value. This updates the PWD_A1 and PWD_A2 registers with the plain values decrypted from the Password_data value.

5.5.3 Update of password with identifier value 00h

For Password_id values 01h, 02h and 03h, both products require that a security session is opened using the PresentPassword command, before issuing a call to WritePassword with the corresponding Password_id value.

On the ST25TVxxx product, the password PWD_KILL identified with value 00h is updated by a direct call to the WritePassword command (see 'Write Kill Password' section of DS12074 [1]) requested with Password_id=00h and a plain Password_data value. A preceding call to the PresentPassword command with Password_id=00h is forbidden (see Section 5.4.1: Presentation of password with identifier value 00h). It is recommended to program the PWD_KILL register at delivery of a ST25TVxxx, then lock it using the LockKill command (see Section 5.6: LockKill command).

On the ST25TVxxxC product, the password PWD_CFG identified with value 00h is updated as a regular 32-bit password using the following procedure:

1. GetRandomNumber request if needed.
2. PresentPassword command requested with Password_id=00h and valid 32-bit encrypted Password_data value.
3. WritePassword command requested with Password_id=00h and valid 32-bit encrypted Password_data value. This updates the PWD_CFG register with the plain value decrypted from the Password_data value.

5.5.4 Tearproof password update procedure

The ST25TVxxxC devices provide a password recovery feature, which allows the user to reprogram a password corrupted by a RF field failure during a WritePassword command.

Refer to application note AN5577 [7], for more details on how to use it. Contact your STMicroelectronics sales office to get this document.

5.6 LockKill command

The LockKill command is used to permanently lock the write access to the PWD_KILL password on a ST25TVxxx device (see 'Lock Kill' section of DS12074 [1]).

This command is not available on a ST25TVxxxC device.

5.7 Kill command

The format of the Kill command - depicted in the following table - is similar on ST25TVxxx and ST25TVxxxC products.

Table 12. **Kill request format**

SOF	Request_flags	Opcode	IC Mfg code	UID	Password_id	Password_data	CRC_B	EOF
-	0x1000xxb	A6h	02h	64 bits	00h	32 bits	16 bits	-

On the ST25TVxxx product:

- the Password_data field contains a **plain** password value.
- the Kill command is always enabled.
- Password_id value 00h is also used to toggle the Untraceable mode (see Section 10.2: Untraceable and Silent modes).

On the ST25TVxxxC product:

- the Password_data field contains an **encrypted** password value, a preceding call to the GetRandomNumber command may be required before calling the Kill command (see Section 5.2: Password encryption).
- after the presentation of an invalid value of Password_data, a call to GetRandomNumber command is mandatory before attempting a new call to PresentPassword, Kill or ToggleDiscreetSilent in the same RF session (see Section 5.2.1: Behavior on invalid password presentation).
- the Kill command may be enabled or disabled by configuration (see Section 10.1: Kill mode).
- Password_id value 00h is also used to open a CONFIG security session.

5.8 EnableUntraceableMode and ToggleDiscreetSilent commands

The formats of the EnableUntraceableMode (ST25TVxxx only) and ToggleDiscreetSilent commands (ST25TVxxxC only) – depicted in the following table – are similar.

Table 13. **EnableUntraceableMode / ToggleDiscreetSilent request format**

SOF	Request_flags	Opcode	IC Mfg code	UID[1]	Password_id	Password_data	CRC_B	EOF
-	0xx000xxb	BAh	02h	64 bits	00h (ST25TVxxx) 03h (ST25TVxxxC)	32 bits	16 bits	-

1. UID field present when Request_flags=0x1000xxb.

On both products:

- the Password_data field contains an encrypted Password_data value.
- the device is switched from READY, SELECTED or QUIET state to the UNTRACEABLE state by requesting the command with Address_flag=1 (Request_flags=0x1000xxb).

On the ST25TVxxx product:

- the value of the Password_id field is 00h.
- the device is switched from READY, SELECTED or QUIET state to the UNTRACEABLE state by requesting the EnableUntraceableMode command with Address_flag=1 (Request_flags=0x1000xxb).
- the EnableUntraceableMode command is not available while in UNTRACEABLE state, the PresentPassword command requested with Password_id=00h is used to switch the device from UNTRACEABLE state to READY state (see Section 10.2: Untraceable and Silent modes).
- after the presentation of an invalid value of Password_data, a call to GetRandomNumber command is not needed before attempting a new call to EnableUntraceableMode in the same RF session.

On the ST25TVxxxC product:

- the value of the Password_id field is 03h.
- the device is switched from READY, SELECTED or QUIET state to the DISCREET or SILENT state by requesting the ToggleDiscreetSilent command with Address_flag=1 (Request_flags=0x1000xxb).
- the ToggleDiscreetSilent command is requested with Address_flag=0 (Request_flags=0x0000xxb) to switch the device from DISCREET or SILENT state to READY state, the PresentPassword command is not available while in DISCREET or SILENT state (see Section 10.2: Untraceable and Silent modes).
- after the presentation of an invalid value of Password_data, a call to GetRandomNumber command is mandatory before attempting a new call to ToggleDiscreetSilent, Kill, or PresentPassword in the same RF session.

6 System configuration

6.1 Configuration commands

Table 14, Table 15 and Table 16 show the format of the ReadConfiguration and WriteConfiguration commands available on both ST25TVxxx and ST25TVxxxC products.

Table 14. **ReadConfiguration request format**

SOF	Request_flags	Opcode	IC Mfg code	UID[1]	FID[2]	PID	CRC_B	EOF
-	00xx00xxb	A0h	02h	64 bits	8 bits	8 bits	16 bits	-

1. *UID field present when Request_flags=001000xxb.*
2. *FID field present on ST25TVxxxC product only.*

Table 15. **ReadConfiguration response format when Error_flag equals 0**

SOF	Response_flags	Data[1]	CRC_B	EOF
-	00h	8 to 64 bits	16 bits	-

1. *Size of data responded depends on the requested PID value for the ST25TVxxx product, and on the requested FID and PID values for the ST25TVxxxC product.*

Table 16. **WriteConfiguration request format**

SOF	Request_flags	Opcode	IC Mfg code	UID[1]	FID[2]	PID	Data[3]	CRC_B	EOF
-	0xx000xxb	A1h	02h	64 bits	8 bits	8 bits	8-32 bits	16 bits	-

1. *UID field present when Request_flags = 0x1000xxb.*
2. *FID field present on ST25TVxxxC product only.*
3. *Size of Data field is only 8 bits on ST25TVxxx product.*

On the ST25TVxxx product:

- the configuration registers are identified with a single 8-bit PID parameter – PID – in the ReadConfiguration and WriteConfiguration requests.
- the size of the Data parameter is 8 bits or 16 bits (for PID=04h only) in a ReadConfiguration response.
- the size of the Data parameter is 8 bits only in a WriteConfiguration request.
- the CONFIG security session is opened by a successful PresentPassword command requested with Password_id value 03h.

On the ST25TVxxxC product:

- the configuration registers are identified with two 8-bit parameters – FID and PID – in the ReadConfiguration and WriteConfiguration requests.
- the size of the Data parameter is 8, 16, 24, 32 or 64 bits in a ReadConfiguration response (see ‘System configuration registers’ of [2] for more details).
- the size of the Data parameter is 8, 16 or 32 bits only in a WriteConfiguration request.
- the CONFIG security session is opened by a successful PresentPassword command requested with Password_id value 00h.

6.2 Configuration registers

Table 17 shows a comparison of the configuration registers available on the ST25TVxxx and ST25TVxxxC products.

Table 17. Comparison of configuration registers on ST25TVxxx and ST25TVxxxC products

ST25TVxxx		ST25TVxxxC					Comment
PID	Register name		FID	PID	RST[1]	RD[2]	
00h	RW_PROTECTION_A1[3]		00h	00h	Y	Y	See Section 7.2: User areas
	MEM_ORG[3]	END_A1		01h	Y	Y	
01h	RW_PROTECTION_A2		01h	00h	Y	Y	
02h	W_PROTECTION_EAS	-	-	-	-	-	See Section 11.7: Electronic article surveillance
03h	CNT_EN	UTC_EN	02h	00h	Y	Y	See Section 8: Counter
	CNT_CLR	-		-	-	-	
04h	CNT_VAL	UTC		01h	-	Y	
-	-	TD_EVENT_UPDATE_EN	03h	00h	Y	Y	See Section 9.2: Tamper event memorization
-	-	TD_SEAL_MSG		01h	N	P	
-	-	TD_UNSEAL_MSG		02h	N	P	
-	-	TD_RESEAL_MSG		03h	N	P	
-	-	TD_SHORT_MSG		04h	N	P	See Section 9.1: Tamper loop status
-	-	TD_OPEN_MSG		05h	N	P	
05h	TAMPER_DETECT	TD_STATUS		06h	-	Y	
-	-	ANDEF_EN	04h	00h	Y	Y	See Section 7.3: Augmented NDEF
-	-	ANDEF_CFG		01h	Y	Y	
-	-	ANDEF_SEP		02h	N	P	
-	-	ANDEF_CUSTOM_LSB		03h	N	P	
-	-	ANDEF_CUSTOM_MSB		04h	N	P	
-	-	PRIVACY	05h	00h	Y	Y	See Section 10: Privacy
-	-	AFI_PROT	08h	00h	Y	Y	See Section 11.8: AFI protection
-	-	REV	FEh	00h	-	Y	See Section 11.5: IC revision
-	-	UID		01h	-	Y	
06h	LOCK_CFG	LCK_CONFIG	FFh	00h	N	Y	See Section 6.2.2: Access rights

1. *Reset of the ST25TVxxxC needed (Y) or not (N) after a WriteConfiguration command.*
2. *Read access of ST25TVxxxC register is protected (P) or always granted (Y).*
3. *On ST25TVxxx, RW_PROTECTION_A1 and MEM_ORG are stored on the same byte*

6.2.1 Activation time

On the ST25TVxxx product, the new value of a configuration register updated with a WriteConfiguration command is **immediately effective**.

On the ST25TVxxxC product, the effect expected from the new value of a configuration register updated with a WriteConfiguration command may be immediate or **delayed to the next boot of the device** (respectively ‘N’ or ‘Y’ value in the ‘RST’ column of Table 17. Comparison of configuration registers on ST25TVxxx and ST25TVxxxC products).

Danger: *On the ST25TVxxxC product, the new value of a configuration register updated with a WriteConfiguration command is immediately readable with a ReadConfiguration command, regardless of the activation time of the effect.*

After the update of a register with a delayed activation time:

- *the new value is immediately readable with the ReadConfiguration command.*
- *the* ***old*** *value is effective until the RF session is terminated (RF field shutdown).*
- *the new value is effective at the start of the next RF session (RF field restored).*

6.2.2 Access rights

On the ST25TVxxx product:

- the write access to all configuration registers can be permanently locked by writing the value 1b to the LOCK_CFG register.
- the read access to any configuration register is always granted, regardless of the status of the CONFIG security session.
- the write access to a writable configuration register (CNT_VAL and TAMPER_DETECT are read-only registers) is granted if LOCK_CFG=0b and the CONFIG security session is open, otherwise it is denied.

On the ST25TVxxxC product:

- the access to a group of configuration registers – identified by a value of the FID parameter – can be permanently locked by setting the corresponding bit of the LCK_CONFIG register to 1b.
- the read access to a configuration register may be (see ‘RD’ column of Table 17. Comparison of configuration registers on ST25TVxxx and ST25TVxxxC products):
  - always granted.
  - granted if bit FID of LCK_CONFIG is set to 0b and the CONFIG security session is open, otherwise it is denied.
- the write access to a writable configuration register is granted if bit FID of LCK_CONFIG is set to 0b and the CONFIG security session is open, otherwise it is denied.

7 User memory

7.1 Generalities

On ST25TVxxx and ST25TVxxxC products:

- The user memory is accessed by blocks of 4 bytes.
- The number of blocks of the user memory is retrieved with the GetSystemInfo command (or with ExtendedGetSystemInfo on ST25TVxxxC only).
- Block 00h is always readable and is used to store the CC file in a T5T application.
- Individual blocks can be read with the ReadSingleBlock command.
- Range of blocks can be read with the ReadMultipleBlocks command. If some blocks of the requested range are not readable (address out of bound, or read access denied), the responded range is truncated before the first non-readable block.
- Blocks can be written only individually with the WriteSingleBlock command.
- The write access to a block can be permanently locked with the LockBlock command.
- The Block Security Status (BSS) of a block signals whether its write access is granted or not. BSS is read with a GetMultipleBlockSecurityStatus command, or with a ReadSingleBlock/ReadMultipleBlocks command requested with Option_flag=1b.

On ST25TV512 and ST25TV512C devices, the user memory contains 16 blocks.

On ST25TV02K devices, the user memory contains 64 blocks.

On ST25TV02KC devices, the user memory contains 80 blocks.

On ST25TVxxx product only, blocks with addresses ranging from F8h to FFh are used by the EAS feature (see Section 11.7: Electronic article surveillance).

7.2 User areas

The user memory of both ST25TVxxx and ST25TVxxxC products can be configured in single or dual area mode:

- In dual area mode, the user memory includes two contiguous groups of blocks AREA1 and AREA2, which can be read- or readwrite-protected by a dedicated 32-bit password (respectively PWD_A1 and PWD_A2 for protection of AREA1 and AREA2)
- In single area mode, the AREA2 partition is disabled and its corresponding blocks are included in the AREA1 partition. In that case, the blocks of AREA1 can be read- or readwrite-protected by a 64-bit password identified by value 01h (it consists in the concatenation of the PWD_A1 and PWD_A2 32-bit passwords)

On the ST25TVxxx product:

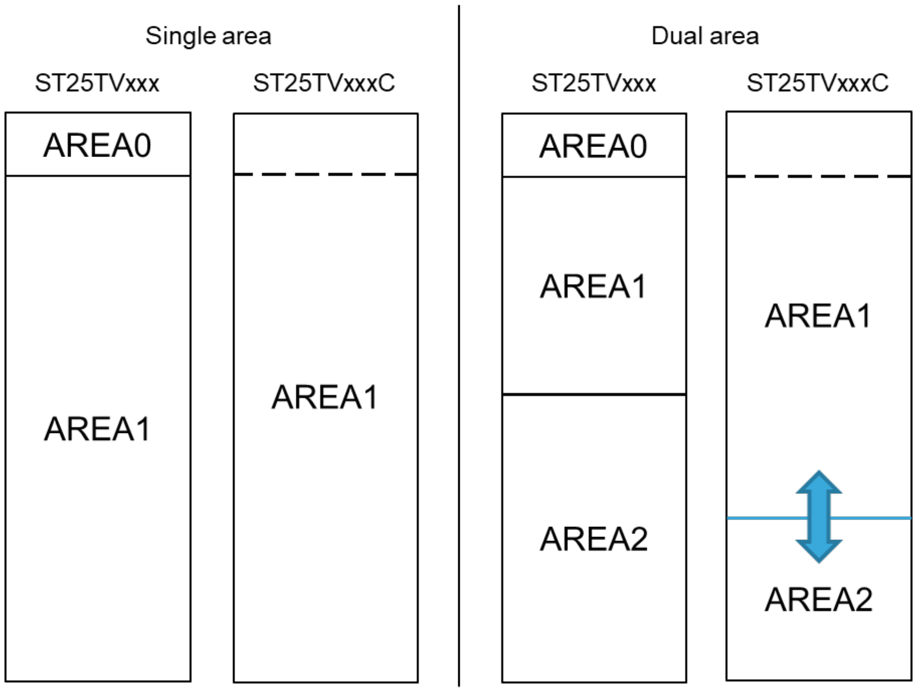
- AREA0 is an area containing only block at address 00h.
- AREA1 starts at block address 01h.
- In dual area mode, AREA2 starts at half of the user memory (block address 08h and 20h on ST25TV512 and ST25TV02K devices respectively).
- The partitioning of the user memory is configured with register MEM_ORG (see Section 6.2: Configuration registers):
  - When MEM_ORG=0b, the user memory is partitioned in three areas AREA0, AREA1 and AREA2 (dual area mode).
  - When MEM_ORG=1b, the user memory is partitioned in two areas AREA0 and AREA1 (single area mode).

On the ST25TVxxxC product:

- AREA1 starts at block address 00h (AREA0 is not defined).
- In dual area mode, AREA2 starts at block address END_A1+1, where END_A1 is configurable (see Section 6.2: Configuration registers).
- Let END_MEM be the address of the last user block (0Fh and 4Fh on ST25TV512C and ST25TV02KC respectively).

- The partitioning of the user memory is configured with register END_A1 (see Section 6.2: Configuration registers):
  - When END_A1<END_MEM, the user memory is partitioned in two areas AREA1 and AREA2 (dual area mode).
  - When END_A1=END_MEM, the user memory is partitioned in one area AREA1 (single area mode).

Figure 1. **Comparison of single and dual area modes on ST25TVxxx and ST25TVxxxC products**



On both ST25TVxxx and ST25TVxxxC products, the access to blocks of AREA1 (respectively AREA2) can be protected by the corresponding password depending on the value of register RW_PROTECTION_A1 (respectively RW_PROTECTION_A2) as described in Table 18 and Table 19.

Table 18. **Access rights depending on RW_PROTECTION_A1 value**

Value	Block 00h		Other blocks from AREA1
	ST25TVxxx	ST25TVxxxC	
00b	Read always granted Write always granted	Read always granted Write always granted	
01b		Read always granted Write protected by PWD_A1	
10b		Read always granted Write protected by PWD_A1	Read protected by PWD_A1 Write protected by PWD_A1
11b		Read always granted Write always forbidden	Read protected by PWD_A1 Write always forbidden

Note: *The read access to block 00h is always granted on both products.*

The write access to block 00h:

- *does not depend on RW_PROTECTION_A1 on the ST25TVxxx product.*
- *depends on RW_PROTECTION_A1 on the ST25TVxxxC product.*

Table 19. Access rights depending on RW_PROTECTION_A2 value

Value	Blocks from AREA2
00b	Read always granted Write always granted
01b	Read always granted Write protected by PWD_A2
10b	Read protected by PWD_A2 Write protected by PWD_A2
11b	Read protected by PWD_A2 Write always forbidden

7.3 Augmented NDEF

On the ST25TVxxxC product only, the user memory data returned by ReadSingleBlock and ReadMultipleBlocks commands may be shadowed by content from system configuration memory when the Augmented NDEF feature is enabled. See the datasheet of the ST25TVxxxC product [2] for more details.

8 Counter

8.1 Write counter

On the ST25TVxxx product only, a 16-bits counter can be enabled to track write events on the user memory. The value of the counter is:

- Stored in the CNT_VAL register (see Section 6.2: Configuration registers).
- Reset by setting the CNT_CLR register to 1b.
- Incremented on the first successful WriteSingleBlock command in a RF session when the CNT_EN register is set to 1b.

See the ST25TVxxx product datasheet [1] for more details.

8.2 Unique tap code

The write counter of the ST25TVxxx product is not available on the ST25TVxxxC.

Instead, a Unique Tap Code feature (UTC) can be enabled on the ST25TVxxxC to uniquely identify each RF session with a 24-bit identifier. The value of the UTC is:

- Stored in the UTC register.
- Updated at the start of each RF session when the UTC_EN register is set to 1b.

See the ST25TVxxxC product datasheet [2] and AN5580 [9] for more details.

Warning: *When the UTC_EN register is set to 1b, the update of the UTC register involves a programmation of the EEPROM during the boot sequence, consequently its duration tBoot_RF is:*

- *Compliant with the 5ms guard-time value defined by the NFC Forum [4].*
- *Not compliant with the 1ms guard-time value defined in ISO15693 [3].*

Note: When the ‘Unique tap code’ and ‘Tamper event memorization’ (see Section 9.2: Tamper event memorization) features of a ST25TVxxxC device are disabled, its boot time is guaranteed to be compliant with the ISO15693 specification [3].

9 Tamper detection

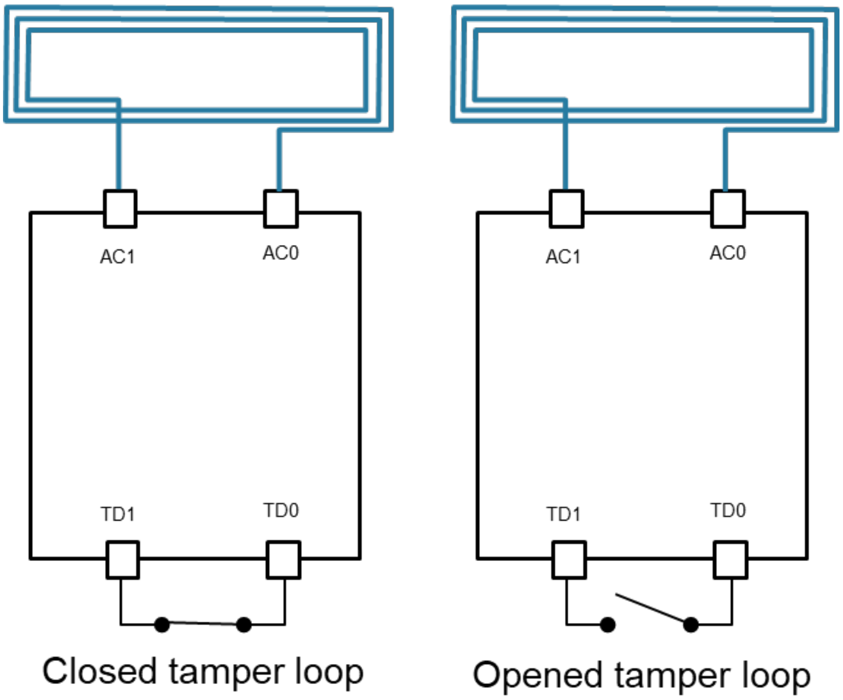
9.1 Tamper loop status

On both ST25TVxxx and ST25TVxxxC products, a tamper detection feature allows to check whether the TD0 and TD1 pins were disconnected or connected by a tamper loop during the latest boot of the device. The status of the tamper loop is:

‘opened’ when the TD0 and TD1 pins were disconnected

‘closed’ when the TD0 and TD1 pins were connected

Figure 2. **Tamper loop status**



On the ST25TVxxx product, the ‘opened’ and ‘closed’ tamper loop status are coded respectively by values 0b and 1b of the TAMPER_DETECT register (see section 6.2).

On the ST25TVxxxC product:

The tamper loop status is stored in the TD_LOOP field of the TD_STATUS register.

The values taken by the TD_LOOP field in case of ‘opened’ and ‘closed’ tamper loop are configured respectively by the TD_OPEN_MSG and TD_SHORT_MSG registers.

Table 20. **Fields of the TD_STATUS register (ST25TVxxxC only)**

Bit	Name	Value
b15-b0	TD_EVENT	TD_SEAL_MSG, TD_UNSEAL_MSG or TD_RESEAL_MSG according to the tamper event status
b23-b16	TD_LOOP	TD_SHORT_MSG or TD_OPEN_MSG according to the tamper loop status

Note: *As other multiple-byte fields, the TD_STATUS register is transmitted in LSB to MSB byte order in the response of ReadConfiguration command.*

Caution: *On both products, the tamper loop status retrieved in a ReadConfiguration response reflects the connection status of the TD0 and TD1 pins captured during the latest boot of the device, the capture of TD0/TD1 connection status is not triggered by a ReadConfiguration request.*

9.2 Tamper event memorization

On the ST25TVxxxC product only, the TD_EVENT field of the TD_STATUS register (see Table 24) is used to monitor the first occurrences of TD_UNSEAL and TD_RESEAL tamper events defined as follows:

TD_UNSEAL: TD_EVENT_UPDATE_EN register was set to 1b, and TD0 and TD1 were not connected at capture time.

TD_RESEAL: TD_EVENT_UPDATE_EN register was set to 1b, TD_UNSEAL event already occured, and TD0 and TD1 were connected at capture time.

The values taken by the TD_EVENT field are:

TD_SEAL_MSG before the first TD_UNSEAL event.

TD_UNSEAL_MSG after the first TD_UNSEAL event.

TD_RESEAL_MSG after the first TD_RESEAL event

The values of the TD_SEAL_MSG, TD_UNSEAL_MSG and TD_RESEAL_MSG registers can be configured (see section 6.2).

When the TD_EVENT_UPDATE_EN register is set to 0b, the memorization of tamper events is disabled and the value of TD_EVENT field is not updated whatever the connection status of the TD0 and TD1 pins during the boot sequence of the ST25TVxxxC device.

See the ST25TVxxxC product datasheet [2] for more details.

Note: *Warning:When the TD_EVENT_UPDATE_EN register is set to 1b, the TD_EVENT field may be updated. If the later happens, a programming of the EEPROM occurs during the boot sequence and its duration tBoot_RF is:- compliant with the 5ms guard-time value defined by the NFC Forum [4]- not compliant with the 1ms guard-time value defined in ISO15693 [3]*

Note: *Note: When the ‘Unique Tap Code’ (see section 8.2) and ‘Tamper event memorization’ features of a ST25TVxxxC device are disabled, its boot time is guaranteed to be compliant with the ISO15693 specification [3].*

10 Privacy

10.1 Kill mode

On both ST25TVxxx and ST25TVxxxC products, the Kill mode feature enables to permanently deactivate a device. When this mode is activated, all incoming RF requests are ignored by the tag. This mode is permanent once activated: it cannot be undone by any mean.

On the ST25TVxxx product:

The Kill mode is activated by a successful presentation of the PWD_KILL password using a plain value in the Kill command (see section 5.6).

The Kill command is always enabled.

The update of the PWD_KILL password is handled by a specific usage of the WritePassword (see section 5.4.3) and LockKill (see section 5.5) commands.

On the ST25TVxxxC product:

The Kill mode is activated by a successful presentation of the PWD_CFG password using an encrypted value in the Kill command (see section 5.6).

The Kill command is enabled (respectively disabled) when the value of the DIS_KILL field of the PRIVACY register is 0b (respectively 1b).

The update of the PWD_CFG password is handled with the same procedure as other 32-bit passwords (see section 5.4.3).

Table 21. **Fields of the PRIVACY register (ST25TVxxxC only)**

Bit	Name	Function	Factory value
b2-b0	DS_MODE	000: device boots in DISCREET state when DS_STS=1b 001: device boots in DISCREET state regardless of DS_STS value 010: device boots in DISCREET state when DS_STS=1b or tamper loop is closed[(1)] 011: device boots in DISCREET state when DS_STS=1b or tamper loop is open[(1)] 100: device boots in SILENT state when DS_STS=1b 101: device boots in SILENT state regardless of DS_STS value 110: device boots in SILENT state when DS_STS=1b or tamper loop is closed[(1)] 111: device boots in SILENT state when DS_STS=1b or tamper loop is open[(1)]	00b
b3	DIS_KILL	0: Kill command is enabled 1: Kill command is disabled	0b
b7-b4	RFU	-	0000b

1. *Effective on ST25TV02KC-T devices only. On ST25TVxxxC-A devices, x10b and x11b values of DS_MODE parameter are interpreted as value x00b.*

10.2 Untraceable and Silent modes

On the ST25TVxxx product, the Untraceable mode enables to set the device in a low-responsivity UNTRACEABLE state. When this mode is activated, the content of the user memory cannot be accessed and the IC is not interoperable with smartphones: all incoming RF requests are ignored by the tag, except some authentication requests used to switch the tag back to the READY state where it is fully responsive.

On the ST25TVxxxC product, the Silent mode enables to set the device in a low-responsitivity SILENT state, which is equivalent to the UNTRACEABLE state of the ST25TVxxx product.

On the ST25TVxxx product:

- The tag switches from READY, SELECTED, or QUIET state to UNTRACEABLE state with a successful presentation of the **PWD_KILL** password using an encrypted value in the EnableUntraceableMode command (see Section 5.8: EnableUntraceableMode and ToggleDiscreetSilent commands) issued with Address_flag=1b.
- The tag switches from UNTRACEABLE state to READY state with a successful presentation of the **PWD_KILL** password using an encrypted value in the PresentPassword command (see Section 5.4.1: Presentation of password with identifier value 00h).
- The value **00h** of the Password_id field is used in the EnableUntraceableMode and PresentPassword commands for presentation of the **PWD_KILL** password.
- While the ST25TVxxx is in UNTRACEABLE state, all incoming commands are ignored except the GetRandomNumber and PresentPassword commands.
- When the RF field is powered off while the ST25TVxxx is in UNTRACEABLE, the tag boots in UNTRACEABLE state at the start of the next RF session.

On the ST25TVxxxC product, when the DS_MODE field of the PRIVACY register is set to 1xxxb:

- The tag switches from READY, SELECTED, or QUIET state to SILENT state with a successful presentation of the **PWD_PRIV** password using an encrypted value in the ToggleDiscreetSilent command (see Section 5.8: EnableUntraceableMode and ToggleDiscreetSilent commands) issued with Address_flag=1b. On this transition, the value of the DS_STS register is set to 1b.
- The tag switches from SILENT state to READY state with a successful presentation of the **PWD_PRIV** password using an encrypted value in the ToggleDiscreetSilent command (see Section 5.4.1: Presentation of password with identifier value 00h) issued in non-addressed mode (Address_flag=Select_flag=0b). On this transition, the value of the DS_STS register is set to 0b.
- The value **03h** of the Password_id field is used in the ToggleDiscreetSilent command for presentation of the **PWD_PRIV** password.
- While the ST25TVxxxC is in SILENT state:
  - The GetRandomNumber command in non-addressed mode is supported.
  - The ToggleDiscreetSilent command in non-addressed mode is supported.
  - All other incoming commands are ignored.
- Depending on the value of the DS_MODE field of the PRIVACY register (see Table 21. Fields of the PRIVACY register (ST25TVxxxC only)) and the status of the tamper loop, the tag may boot automatically in SILENT state without an explicit activation of the Silent mode (that is, without calling the ToggleDiscreetSilent command with Address_flag=1).

Note: *A ST25TVxxx device in UNTRACEABLE state is not interoperable with smartphones operating Android™ and iOS® systems. The DS_MODE=0xxb/1xxb setting of the ST25TVxxxC respectively allows/forbids the interoperability of the IC with smartphones while it is in DISCREET/SILENT state.*

10.3 Discreet mode

On the ST25TVxxxC product, the Discreet mode enables to set the device in a low-responsitivity DISCREET state. When this mode is activated, the content of the user memory cannot be accessed, while the IC remains interoperable with a smartphone: all incoming RF requests are ignored by the tag, except some authentication requests (to switch the tag back to READY state) and some NFC Forum T5T commands (for interoperability).

When the DS_MODE field of the PRIVACY register is set to 0xxb:

- The tag switches from READY, SELECTED, or QUIET state to DISCREET state with a successful presentation of the PWD_PRIV password using an encrypted value in the ToggleDiscreetSilent command (see section 5.8) issued with Address_flag=1b. On this transition, the value of the DS_STS register is set to 1b.
- The tag switches from DISCREET state to READY state with a successful presentation of the PWD_PRIV password using an encrypted value in the ToggleDiscreetSilent command (see section 5.8) issued with Address_flag=Select_flag=0b. On this transition, the value of the DS_STS register is set to 0b.
- While the ST25TVxxxC is in DISCREET state:
  - The GetRandomNumber command in non-addressed mode is supported
  - The ToggleDiscreetSilent command in non-addressed mode is supported
  - The Inventory command, which behaves with AFI, DSFID and UID values respectively set to 00h, 00h, and content from Table 22.
  - The ReadSingleBlock command issued on block 00h with Address_flag=1 and the UID field set to the value of Table 22
  - Depending on the value of the DS_MODE field of the PRIVACY register (see Table 21) and the status of the tamper loop, the tag may boot automatically in DISCREET state without an explicit activation of the Discreet mode (that is, without calling the ToggleDiscreetSilent command with Address_flag=1).

Table 22. UID value in DISCREET state (ST25TVxxxC only)

b63-b56	b55-b48	b47-b40	b39-b0
E0h	02h	00h	0000000000h

11 Product identification and protection

11.1 Product codes and IC reference codes

On ST25TVxxx and ST25TVxxxC devices, the product code is the third byte of the UID (see Table 27), and the IC reference code is read in the response to a GetSystemInfo command (see Table 28).

The product code value is identical to the IC reference code value on both products:

- 23h on ST25TVxxx products
- 08h on ST25TVxxxC products

Table 23. Product code field in UID

b63-b56	b55-b48	b47-b40	b39-b0
E0h	02h[1]	Product code	Unique identifier

[1] *IC manufacturer code 02h for STMicroelectronics*

Table 24. GetSystemInfo response format

SOF	Response_flags	Info_flags	UID	DSFID	AFI	Memory_size	IC_ref	CRC_B	EOF
-	00h	0Fh	64 bits	8 bits	8 bits	16 bits	8 bits	16 bits	-

11.2 Memory size

On ST25TVxxx and ST25TVxxxC devices, the memory size is read as the Memory_size field in a response to the GetSystemInfo command.

Table 25. Memory_size field in GetSystemInfo response

b15-b8	b7-b0
03h(1)	NB(2)

b15-b8	b7-b0
03h(1)	NB(2)

(1): Block size in bytes minus 1, value is 03h on both products.

(2): Memory size in blocks minus 1.

The value of the NB byte from the Memory_size field (see Table 29) is:

0Fh on ST25TV512 and ST25TV512C products

3Fh on ST25TV02K product

4Fh on ST25TV02KC product

11.3 Tamper detection

The availability of the tamper detection interface on a device is identified by a successful ReadConfiguration command for the following configuration registers (see Section 6.2: Configuration registers):

- TAMPER_DETECT (PID=05h) on the ST25TVxxx product
- TD_STATUS (FID=03h, PID=06h) on the ST25TVxxxC product

11.4 ExtendedGetSystemInfo

On the ST25TVxxxC product only, the following informations can be retrieved with the ExtendedGetSystemInfo command (see the ST25TVxxxC product datasheet [2]):

- IC reference code
- Memory size
- List of optional ISO15693 commands

11.5 IC revision

On the ST25TVxxxC product only, the revision number of the product is retrieved from the REV register (see Section 6.2: Configuration registers), and the UID can be retrieved as a configuration register.

The value of the REV register can be used to identify the input capacitance of a ST25TVxxxC product:

- value 12h identifies an input capacitance of 23pF (ST25TVxxxC-xxx3 order code)
- value 25h identifies an input capacitance of 99.7pF (ST25TVxxxC-xxx9 order code)

11.6 TruST25 digital signature

The ST25TVxxx and ST25TVxxxC products support the TruST25 digital signature feature, which allows the user to verify the authenticity of the device, based on a unique digital signature.

TruST25 solution encompasses secure industrialization processes and tools deployed by STMicroelectronics to generate, store and check the signature in the device.

Implementation details can be found in application notes AN5104 [6] and AN5578 [8]. Contact your STMicroelectronics sales office to get this documentation.

11.7 Electronic article surveillance

On the ST25TVxxx product only, the EAS (Electronic article surveillance) feature is used for library management, applications, requiring an anti-theft protection. Block addresses ranging from F8h to FFh in the user memory are used for storage of EAS telegram. See the ST25TVxxx product datasheet [1] for more details.

The EAS feature is not available on the ST25TVxxxC product. Block addresses ranging from F8h to FFh in the user memory are not used on the ST25TVxxxC.

11.8 AFI protection

On the ST25TVxxxC product only, the write access to the AFI register may be protected to meet security constraints from the ISO28560 specification [10] in library applications.

Depending on the value of the AFI_PROT register (see Section 6.2: Configuration registers), the enforcement of the write access to the AFI register by the AREA1 security session may be enabled or disabled as described in Table 30.

Table 26. **AFI_PROT register (ST25TVxxxC only)**

Bit	Name	Value
b0	AFI_PROT	0: WriteAFI and LockAFI commands do not depend on password identified by value 01h 1: WriteAFI and LockAFI commands fail when password identified by value 01h was not presented successfully
b7-b1	RFU	-

See the ST25TVxxxC product datasheet [2] for more details.

12 Behavior when erroneous commands are received

12.1 Behavior on invalid settings of Request_flags

This section shows the behavior of the products for the following cases of invalid Request_flags settings:

- Inventory_flag=0 for inventory commands (opcodes 01h, C1h, D1h, D3h or D4h)
- Inventory_flag=1 for non-inventory commands (other opcodes)
- Inventory_flag=0 and Address_flag=1 and Select_flag=1

Remember: *Inventory_flag, Address_flag and Select_flag respectively are bits 2, 4 and 5 of the Request_flags byte. Error_flag is bit 0 of the Response_flags byte.*

Table 27. **Generic ISO15693 request format with Address_flag=Select_flag=1**

SOF	Request_flags	Opcode	Parameters	Data	CRC_B	EOF
-	xx**11**x**0**xxb	8 bits	optional	optional	16 bits	-

Table 28. **GetSystemInfo request format with invalid value of Inventory_flag**

SOF	Request_flags	Opcode	Parameters	Data	CRC_B	EOF
-	00000**1**xxb	8 bits	optional	optional	16 bits	-

When processing a command requested with such invalid setting of Request_flags, a ST25TVxxx device may stay mute or reply a response frame with Error_flag=1.

Table 29. **ISO15693 response format when Error_flag=1**

SOF	Response_flags	Error_code	CRC_B	EOF
-	01h	8 bits	16 bits	-

When processing a command requested with such invalid setting of Request_flags, a ST25TVxxxC device always stays mute.

12.2 Behavior on erroneous commands in non-addressed mode

When an error occurs while processing a command requested in non-addressed mode (with Inventory_flag=0, Address_flag=0 and Select_flag=0), a ST25TVxxx device may stay mute or reply a response frame with Error_flag=1.

Table 30. **ISO15693 request format in non-addressed mode**

SOF	Request_flags	Opcode	Parameters	Data	CRC_B	EOF
-	xx00x0xxb	8 bits	optional	optional	16 bits	-

When an error occurs while processing a command requested in non-addressed mode, a ST25TVxxxC device always stays mute.

13 Reference documents

Table 31. **Reference documents**

Reference	Alternate name	Revision	Title
[1]	DS12074	Latest version	ST25TV02K ST25TV512 datasheet
[2]	DS13304		ST25TV02KC ST25TV512C datasheet
[3]	ISO15693		International standard ISO/IEC 15693-3: Identification cards – Contactless integrated circuit cards – Vicinity cards
[4]	DIGITAL		Digital Protocol Specification, NFC Forum
[5]	T5T		Type 5 Tag Specification, NFC Forum
[6]	AN5104		TruST25™ digital signature for ST25TV512 and ST25TV02K devices
[7]	AN5577		Password management for ST25TV512C and ST25TV02KC devices
[8]	AN5578		TruST25™ digital signature for ST25TV512C and ST25TV02KC devices
[9]	AN5580		Unique tap code for ST25TV512C and ST25TV02KC devices
[10]	ISO28560		International standard ISO/IEC 28560-2: Information and documentation – RFID in libraries – Part2: Encoding of RFID data elements based on rules from ISO/IEC 15962

Revision history

Table 32. **Document revision history**

Date	Revision	Changes
05-Mar-2021	1	Initial release.
6-Sep-2022	2	Updated: • Section 2: ST25TVxxx and ST25TVxxxC product feature comparison • Section 3: Hardware considerations • Section 11.5: IC revision
13-May-2025	3	Updated: • Section Introduction • Section 1.2.1: Product family denomination • Section 2: ST25TVxxx and ST25TVxxxC product feature comparison • Section 4.1: RF command list • Section 5.1: Password identifiers • Section 5.2: Password encryption • Section 5.3: Failed attempt counters • Section 5.7: Kill command • Section 5.4.1: Presentation of password with identifier value 00h • Section 5.7: Kill command • Section 5.8: EnableUntraceableMode and ToggleDiscreetSilent commands • Section 10.1: Kill mode • Section 10.2: Untraceable and Silent modes Added Section 10.3: Discreet mode

Contents

List of tables

List of figures