Application note

Password encryption for ST25TV512 and ST25TV02K devices

Introduction

The ST25TV512 and ST25TV02K (hereinafter referred to as ST25TV512/02K) devices are NFC/RFID tag ICs with a tamper-proof feature, and specific modes to protect tag access.

This document defines the available passwords, and explains how to encrypt the passwords to grant access rights to user areas, modify the file device configuration or change the ST25TV512 / 02K modes.

1 ST25TV512/02K passwords

1.1 User area passwords

ST25TV512/02K user memory can be split into either 2 or 3 areas (Area 0, Area 1, Area 2).

- **Area 0** includes the first 4 bytes block of user memory. It is always readable, and can be locked. Passwords are not applicable to Area 0.
- **Areas 1 and 2** can be protected in read and/or write access by passwords depending on the configuration written in the static registers A1SS and A2SS.

When Area 1 is protected by read (or respectively write) access, before the Area 1 itself can be read (or respectively written) by the reader device, the Area 1 password must be presented to ST25TV512/02K. The password must be properly encrypted by the tag reader device to grant the requested access right to the reader device.

Similarly for Area 2: the Area 2 password must be presented encrypted to ST25TV512/02K before Area 2 can be read (respectively written) by the reader device. The password encryption is explained in Section 2 Password encryption.

1.2 Kill password

In order to activate the kill mute mode, the kill password must be presented to ST25TV512/02K. The kill password must be sent as it is (non encrypted) by the reader device. This application note does not apply to the kill password

1.3 Untraceable password

In order to activate the untraceable mode of ST25TV512/02K, the untraceable password must be presented to ST25TV512/02K. The untraceable password must be properly encrypted by the reader device, as explained in Section 2 Password encryption.

1.4 Configuration password

When the ST25TV512/02K configuration is not locked, the configuration password must be presented to ST25TV512/02K for the reader device to be granted the right to modify the ST25TV512/02K configuration. The configuration password must be properly encrypted by the reader device, as explained in Section 2 Password encryption.

2 Password encryption

2.1 Overview

When ST25TV512/02K has been set up to protect access to configuration, and/or user areas, the access to the resource is protected by password. If the reader device wants to be granted access to the configuration, the configuration password that has been programmed into ST25TV512/02K must be presented to ST25TV512/02K once it has gone through the following encryption scheme.

Same applies to the user area, the password that has been programmed into ST25TV512/02K must be presented to ST25TV512/02K once it has gone through the following encryption scheme.

An encryption is also necessary when the ST25TV512/02K must enter in untraceable mode.

Usually, when a password has been programmed once into ST25TV512/02K (step 1 of Figure 1. Configuring passwords, and enable protected data modification), this password must be presented every time the protected data access is requested (step 2 of Figure 1. Configuring passwords, and enable protected data modification).

Figure 1. Configuring passwords, and enable protected data modification

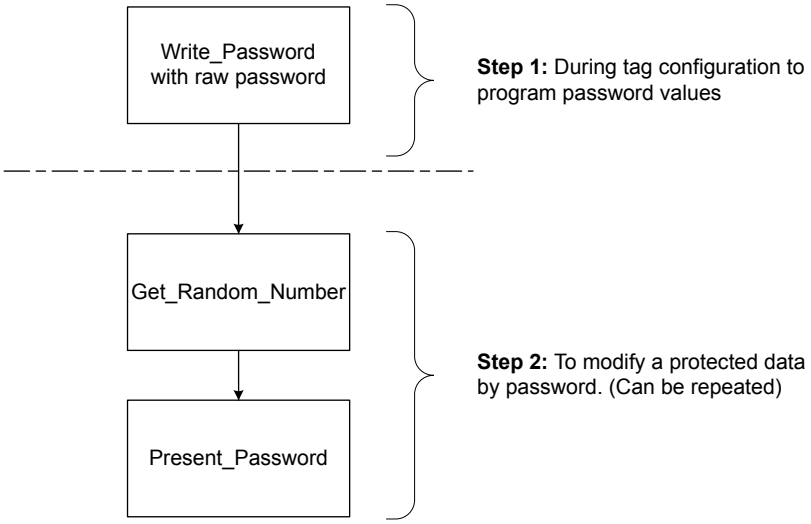


Table 1. Example of configuring passwords and enable protected data modification shows an example of configuring password and enable protected data modification.

Table 1. Example of configuring passwords and enable protected data modification

Step 1								
Request:	Write password PWD_A1 with value 0x12345678							
Request SOF	**Request_flags**	**Write password**	**IC Mfg code**	**UID** (1)	**Password number**	**Data**	**CRC16**	**EOF**
-	8 bits	B1h	02h	64 bits	01h	12345678h	16 bits	-
Response:	No error							
SOF	**Response_flags**	**CRC16**	**EOF**					
-	00h	16 bits						
Step 2								
Request:	Get Random Number. Response from ST25TV512/02K is 5F3Ch							
Request SOF	**Request_flags**	**Get random number**	**IC Mfg code**	**UID**(1)	**CRC16**	**EOF**		

-	8 bits	B4h	02h	64 bits	16 bits	-		
Response:	No error, with random value 5F3Ch returned							
SOF	**Response_flags**	**Random number**	**CRC16**	**EOF**				
-	00h	5F3Ch	16 bits	-				
Request:	Present password PWD_A1 with encrypted password value Encrypted password value is 12345678 bit-xor 5F3C5F3C i.e. 4D080944h							
Request SOF	**Request_flags**	**Present password**	**IC Mfg code**	**UID** (1)	**Password number**	**Data**	**CRC16**	**EOF**
-	8 bits	B3h	02h	64 bits	01h	4D080944h	16 bits	-
Response:	No error							
SOF	**Response_flags**	**CRC16**	**EOF**					
-	00h	16 bits	-					

1. ***The field is optional.***

2.2 Programming password into ST25TV512/02K

The command 'Write Password' is used for programming a password into ST25TV512/02K. On receiving the Write Password request, the ST25TV512/02K uses the data contained in the request to write the password and reports whether the operation was successful in the response.

Table 2 shows the Write Password request format:

Table 2. Write Password request format

Request SOF	Request_flags	Present Password	IC Mfg code	UID (1)	Password number	Password	CRC16	Request EOF
-	8 bits	B1h	02h	64 bits	8 bits	32 bits	16 bits	-

1. *This field is optional.*

The 32-bit field 'Password' contains the password value of the actual ST25TV512/02K password corresponding to the password number of the 8-bit field 'Password number' of the request.

Table 3. Password identifier

Password number	Password (32 bit)
00h	PWD_KILL or PWD_UNTRACEABLE
01h	PWD_A1 (covering Area 1)
02h	PWD_A2 (covering Area 1 for 2 areas, or Area 2 for 3 areas)
03h	PWD_CFG

PWD_A1 and PWD_A2 can be concatenated into a 64-bit password PWD_A1_64 covering Area 1 in case ST25TV512/02K is programmed with 2 user areas (instead of 3).

PWD_CFG has to be presented with its current password value before issuing the Write Password command with Password number 03h and the new password value

When MEM_ORG=0b, PWD_A1 or PWD_A2 has to be presented with its current password value before issuing the Write Password command with Password number 01h or 02h respectively and the new password value

When MEM_ORG=1b, PWD_A1_64 has to be presented with its current 64-bit value before issuing the Write Password command with Password numbers 01h and 02h, and passwords PWD_A1 and PWD_A2 (the WritePassword command only support 32-bit password values, and not 64-bit values).

The values of the 32-bit or 64-bit passwords used as arguments of Write Password request are referred in the next section as the Raw 32-bit password or Raw 64-bit password.

2.3 Password presentation to ST25TV512/02K for granting access rights

When the reader device wants to modify the mode of ST25TV512/02K or change the user data protected by password, it must present the encrypted password to ST25TV512/02K. The encrypted passwords are calculated from the Raw 32-bit or Raw 64-bit password using the following scheme.

2.3.1 Password encryption

Before sending a present password command, it is necessary to obtain a valid random number through the command 'Get_Random_Number' (see Section 2.3.3 Get Random Number).

The passwords must be presented encrypted in the following way:

- Case of 32-bit password:

```
{raw 32-bit password}

    Bit wise XOR

{last Get_Random_Number 16 bit value, last Get_Random_Number 16 bit value}
```

- Case of 64-bit password:

```
{raw 64-bit password}

    Bit wise XOR

{last Get_Random_Number 16 bit value, last Get_Random_Number 16 bit value,

    last Get_Random_Number 16 bit value, last Get_Random_Number 16 bit value}
```

2.3.2 Present Password

On receiving the Present Password command, the ST25TV02K/512 compares the requested password with the data contained in the request and reports if the operation has been successful in the response. After a successful command, the security session associated to the password is open.

Table 4. Present Password request format

Request SOF	Request_flags	Present Password	IC Mfg code	UID (1)	Password number	Password	CRC16	Request EOF
-	8 bits	B3h	02h	64 bits	8 bits	32 or 64 bits	16 bits	-

1. *This field is optional.*

Request parameter:

- Request flags
- UID (optional)
- Password number (00h = PWD_UNTRACEABLE, 0x01 = PWD_A1 or PWD_A1_64, 0x02 = PWD_A2, 0x03 = PWD_CFG, other = Error)
- Password is 32-bit wide for all passwords, except for Area 1 if MEM_ORG = 1b1 (ST25TV02K/512 configured in two areas), when the password is 64-bit wide, where a 64-bit wide password is used (PWD_A1_64). This password must be encrypted according to Section 2.3.1 Password encryption.

Table 5. Present Password response format when Error_flag is NOT set

Response SOF	Response_flags	CRC16	Response EOF
-	8 bits	16 bits	-

Response parameter:

- No parameter. The response is sent back after the write cycle.

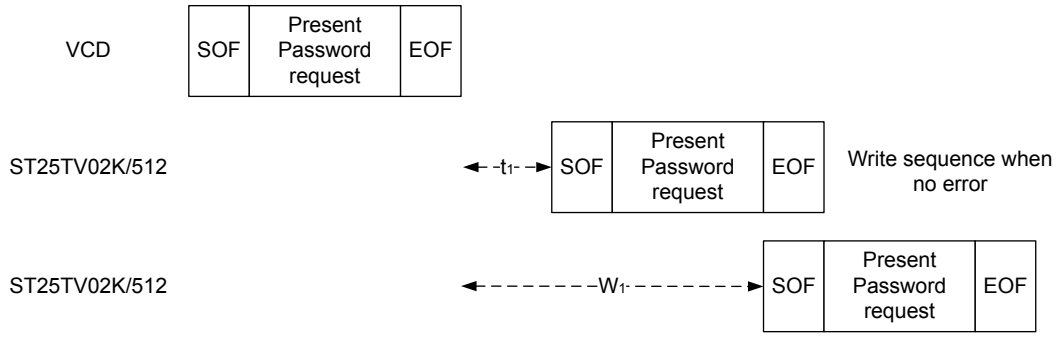
Table 6. Present Password response format when Error_flag is set

Response SOF	Response_flags	Error code	CRC16	Response EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set:
  - 02h: command not recognized
  - 03h: command option not supported
  - 0Fh: the present password is incorrect
  - 10h: the password number is incorrect

Figure 2. Present Password frame exchange between VCD and ST25TV02K/512



2.3.3 Get Random Number

When ST25TV02K/512 receive the Get Random Number command, ST25TV02K/512 returns a 16 bit random number.

Table 7. Get Random Number request format

Request SOF	Request_flags	Get random number	IC Mfg code	UID (1)	CRC16 request	EOF
-	8 bits	B4h	02h	64 bits	16 bits	-

1. *This field is optional.*

Request parameters:

- Request flags
- UID (optional)

Table 8. Get Random Number response format when Error_flag is NOT set

Request SOF	Response_flags	Random number	CRC16 request	EOF
-	8 bits	16 bits	16 bits	-

Response parameter:

- Random number

Table 9. Get Random Number response format when Error_flag is set

Request SOF	Response_flags	Error code	CRC16 request	EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code as Error_flag is set
  - 03h: command option is not supported

2.3.4 Enable Untraceable mode

With the Enable Untraceable mode command the ST25TV512/02K will not respond to any command except Present Password and Get Random Number.

The Enable_Untraceable command requires the password number for the untraceable access code (fixed value) and the crypted untraceable mode password to be presented for the command to be executed properly

Table 10. Enable Untraceable mode request format

Response SOF	Request_flags	Enable untraceable mode	IC Mfg code	UID	Password number	Crypted password	CRC16 request	EOF
-	8 bits	BAh	02h	64 bits	00h	32 bits	16 bits	-

Request parameters:

- Request flags
- UID
- Password Number = 00h
- Crypted Password

Table 11. Enable Untraceable mode response format when Error_flag is NOT set

Request SOF	Response_flags	CRC16 request	EOF
-	8 bits	16 bits	-

Response parameter:

None

Table 12. Enable Untraceable mode response format when Error_flag is set

Request SOF	Response_flags	Error code	CRC16 request	EOF
-	8 bits	8 bits	16 bits	-

Response parameter:

- Error code when Error_flag is set
  - 03h: command option is not supported
  - 0Fh: error with no information given
  - 10h: password number is not 00h
  - 13h: the EAS configuration was not successfully programmed

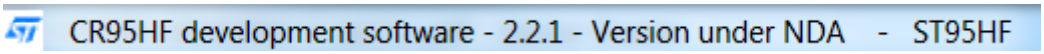
2.3.5 Examples

1. **Entering Untraceable mode**

To put the ST25TV512/02K in Untraceable mode, it is necessary to know the tag UID and send the 'Enable Untraceable Mode' command in the addressed mode.

Figure 3. CR95HF development software shows the CR95HF development software version used in this example.

Figure 3. CR95HF development software



The following steps can be followed for setting up Untraceable mode:

INVENTORY

```
>>> CR95HFDLL_SENDRECEIVE, 260100
      <<< 800D0000F0C8D601042302E064A300
```

The UID of the tag is E002230401D6C8F0. In the code it is written in the little endian order (LSB transmitted first) and is highlighted in bold.

WRITE PASSWORD

The password must be programmed into ST25TV512/02K. For example the following password: 0x78563412 is programmed using the following code:

```
>>> CR95HFDLL_SENDRECEIVE, 02B10200 12345678
           <<< 80040078F000
```

Note: The password is written in the little endian order and is highlighted in bold.

WRITE PASSWORD

To enter Untraceable mode, a random value must be requested from the ST25TV512/02K.

```
>>> CR95HFDLL_SENDRECEIVE, 02B402
           <<< 800600916B9C1B00
```

The ST25TV512/02K returns: 0x6B91 as the random value.

ENABLE UNTRACEABLE MODE

Untraceable mode can be entered with the 'Enable Untraceable Mode' command. After the encryption, the encrypted password must be passed to the ST25TV512/02K as written below:

Encrypted Password

```
= UnEncrypted Password XOR {16 bi12345678t Random Value, 16 bit Random Value}
= 0x78563412 XOR 0x6B916B91
= 0x13C75F83
```

The below code sets the Addressed mode of the command (bit 5 of the Request Flag is 1).

```
 >>> CR95HFDLL_SENDRECEIVE, 22BA02F0C8D601042302E000835FC713
<<< 80040078F000
```

2. **Expected behaviour when in Untraceable mode**

   Untraceable mode only allows execution of the Get Random Number and Present Password command.

   The examples below explain the behaviour in Untraceable mode:

   Response to Get Random Number

```
>>> CR95HFDLL_SENDRECEIVE, 22B402F0C8D601042302E0
<<< 800600F06B116700
```

   The ST25TV512/02K returns **0x6BF0** as the random value.

   Response to other commands in addition to Get Random Number and Present Password command

   No response is given by the ST25TV512/02K to command other than Get Random Number and Present Password.

   For example: **INVENTORY command**

```
>>> CR95HFDLL_SENDRECEIVE, 260100
<<< 8700 : Frame wait time out OR no tag
```

   The ST25TV512/02K device does not respond to the INVENTORY command.

3. **Exiting Untraceable Mode**

   To exit from Untraceable mode, must be presented the *Untraceable Mode password* afterwards the encryption with the last random number obtained.

   Considering 0x6BF0 that is the last random number received, and 0x78563412 that is the last password written into, the corresponding encrypted password is: **0x13A65FE2**. It is obtained as below:

```
0x78563412 XOR 0x6BF06BF0 = 0x13A65FE2
```

   This password is presented to ST25TV512/02K with the LSB first:

   PRESENT PASSWORD

```
>>> CR95HFDLL_SENDRECEIVE, 22B302F0C8D601042302E000E25FA613
<<< 80040078F000
```

   The ST25TV512/02K is now out of Untraceable mode and answers all commands.

   For example:

   INVENTORY

```
>>> CR95HFDLL_SENDRECEIVE, 260100
<<< 800D0000F0C8D601042302E064A300
```

   The UID returned here is: E0 02 23 04 01 D6 C8 F0.

Revision history

Table 13. **Document revision history**

Date	Revision	Changes
27-Nov-2017	1	Initial release.
05-Jul-2018	2	Updated: • Table 10. Enable Untraceable mode request format Added: • Section 2.3.5 Examples
02-Feb-2021	3	Changed the document classification from ST Restricted to Public. Updated: • Section Introduction

Contents

List of tables

List of figures