NT4H console example user manual

Version 1.3

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

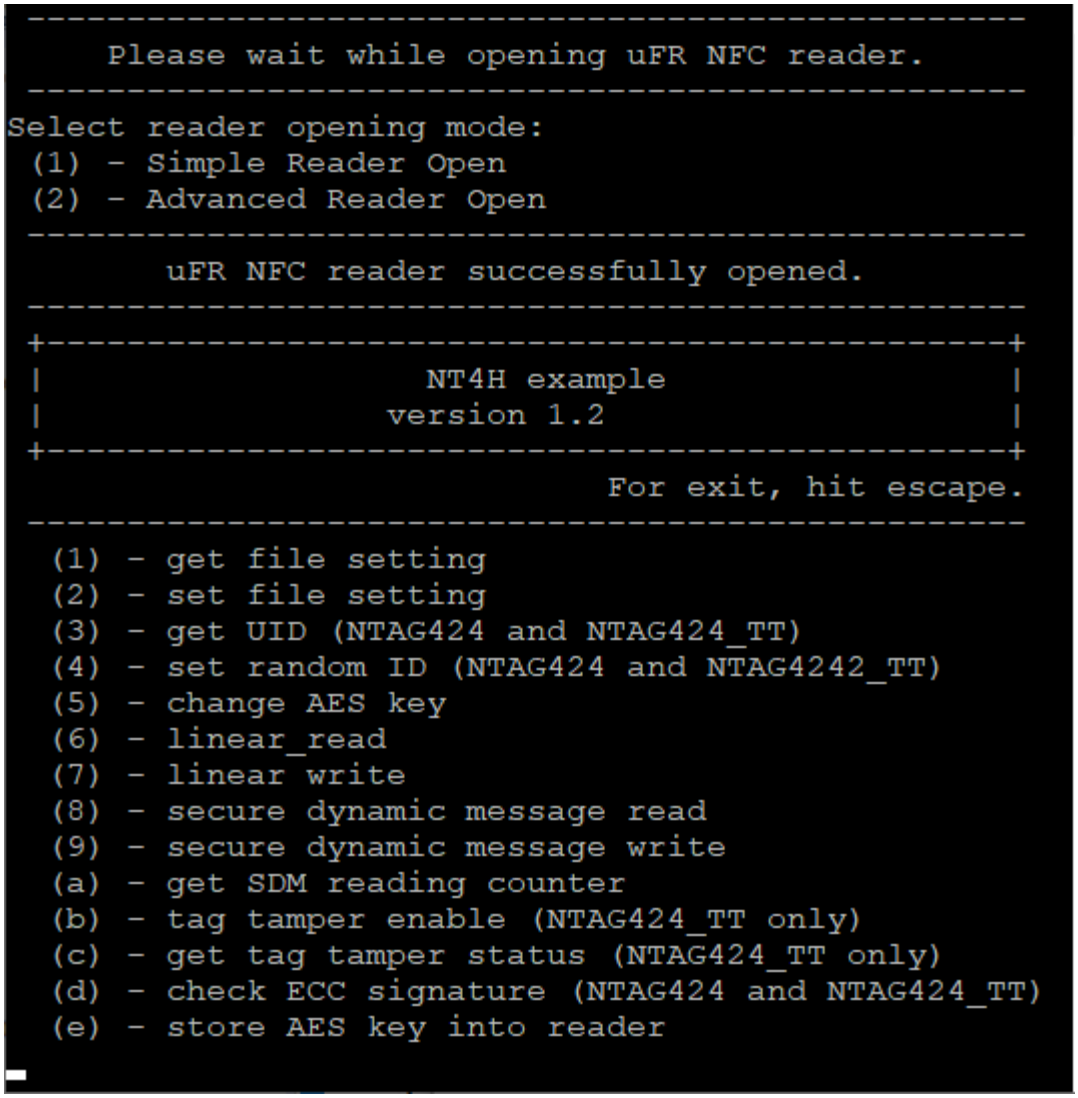
Table of contents

1. Introduction

The NT4H is a new series of NXP NTAG® cards.
There is NTAG413 DNA, NTAG424 DNA, and NTAG424 TT DNA.
NTAG 424 DNA is fully compliant with the NFC Forum Type 4 Tag IC.
They come with AES-128 cryptographic operation and a new Secure Unique NFC (SUN) Message.

2. Application overview

Link: https://git.d-logic.net/nfc-rfid-reader-sdk/ufr-examples-c-nt4h
In the picture is the layout of the application where simple reader opening mode is used.



2.1 Get file setting (1)

The NTAG413 has two standard data files:

- File number 1 is Capability Container file (32 bytes)
- File number 2 is NDEF file (128 bytes)

The NTAG424 has three standard data files:

- File number 1 is Capability Container file (32 bytes)
- File number 2 is NDEF file (256 bytes)
- File number 3 is proprietary file (128 bytes)

Number of returned parameters is variable.

If current file is standard data file with AES secure messaging, then the following information is obtained:

- File type
- Communication mode
- File access rights
- File size

Example:

File number = 3 (NTAG424 proprietary file)

Communication mode is enciphered (0x03)

Secure dynamic messaging is disabled

Key number for read is 2,

key number for write is 3,

Key number for read/write is 3,

Key number for change file settings is 0,

File size is 128 bytes.

```
------------------------------------------------------------------
                        Get file setting
------------------------------------------------------------------

Enter file number (1 - 2 for NTAG413) (1 - 3 for NTAG424)
3

Get file setting successful
File type: Standard data file
Communication mode: enciphered
Secure dynamic messaging: disabled
File access rights (0x0E - free access, 0x0F - no access)
Read key: 0x02
Write key: 0x03
ReadWrite key: 0x03
Change key: 0x00
File size: 128
```

If the current file is a standard data file with secure dynamic messaging, then there is more information.
Example:
File number is 2 (NDEF file).
Secure dynamic messaging is enabled.
Free access for reading and writing operations (key 0x0E)
File size is 256 bytes.
UID mirroring is enabled.
SDM reading counter is enabled.
SDM reading counter limit is disabled.
Encrypted part of file data used.
Key number for SDM meta read is 2 (UID, SDM reading counter, PICC data, MAC)
Key number for the encrypted part of file data is 2.
SDM reading counter can read without authentication.
PICC data offset (encrypted UID and SDM reading counter) is 49.
MAC input offset is 86.
Encrypted part of the file data offset is 86.
Encrypted part of the file data length is 32.
MAC offset is 124.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

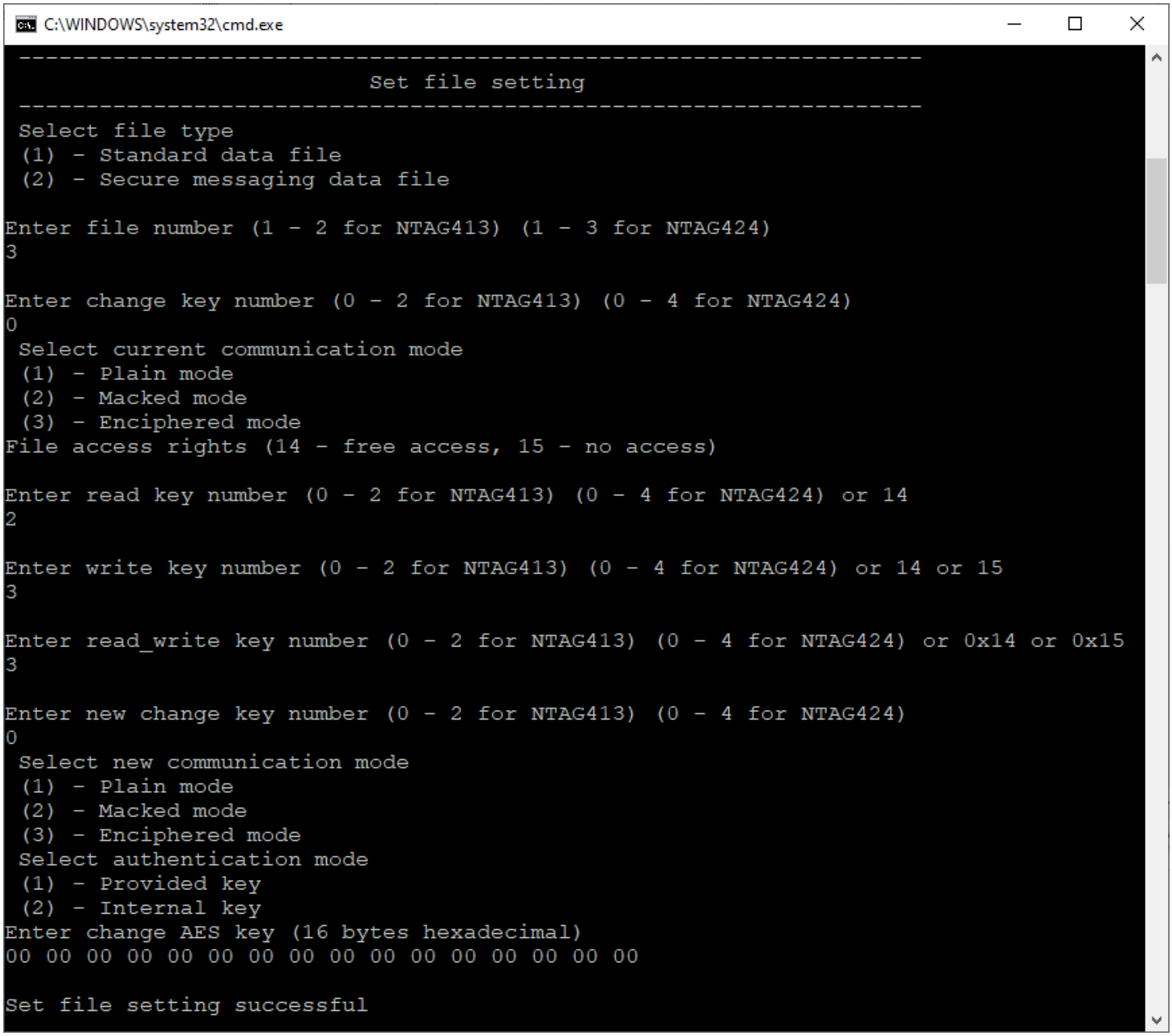
```
 ---------------------------------------------------------------
                          Get file setting
 ---------------------------------------------------------------

Enter file number (1 - 2 for NTAG413) (1 - 3 for NTAG424)
2

Get file setting successful
File type: Standard data file
Communication mode: plain
Secure dynamic messaging: enabled
File access rights (0x0E - free access, 0x0F - no access)
Read key: 0x0E
Write key: 0x0E
ReadWrite key: 0x0E
Change key: 0x00
File size: 256
Secure dynamic message options
UID mirroring: enabled
Read counter: enabled
Read counter limit: disabled
Encrypted part of file data: enabled
SDM access rights (0x0E free/plain, 0x0F no access/no data
SDM meta read: 0x02
SDM file key: 0x02
SDM reading counter read key: 0x0E
PICC data offset: 49
MAC input data offset: 86
Encrypted data offset: 86
Encrypted data length: 32
MAC offset: 124
```

2.2 Set file setting (2)

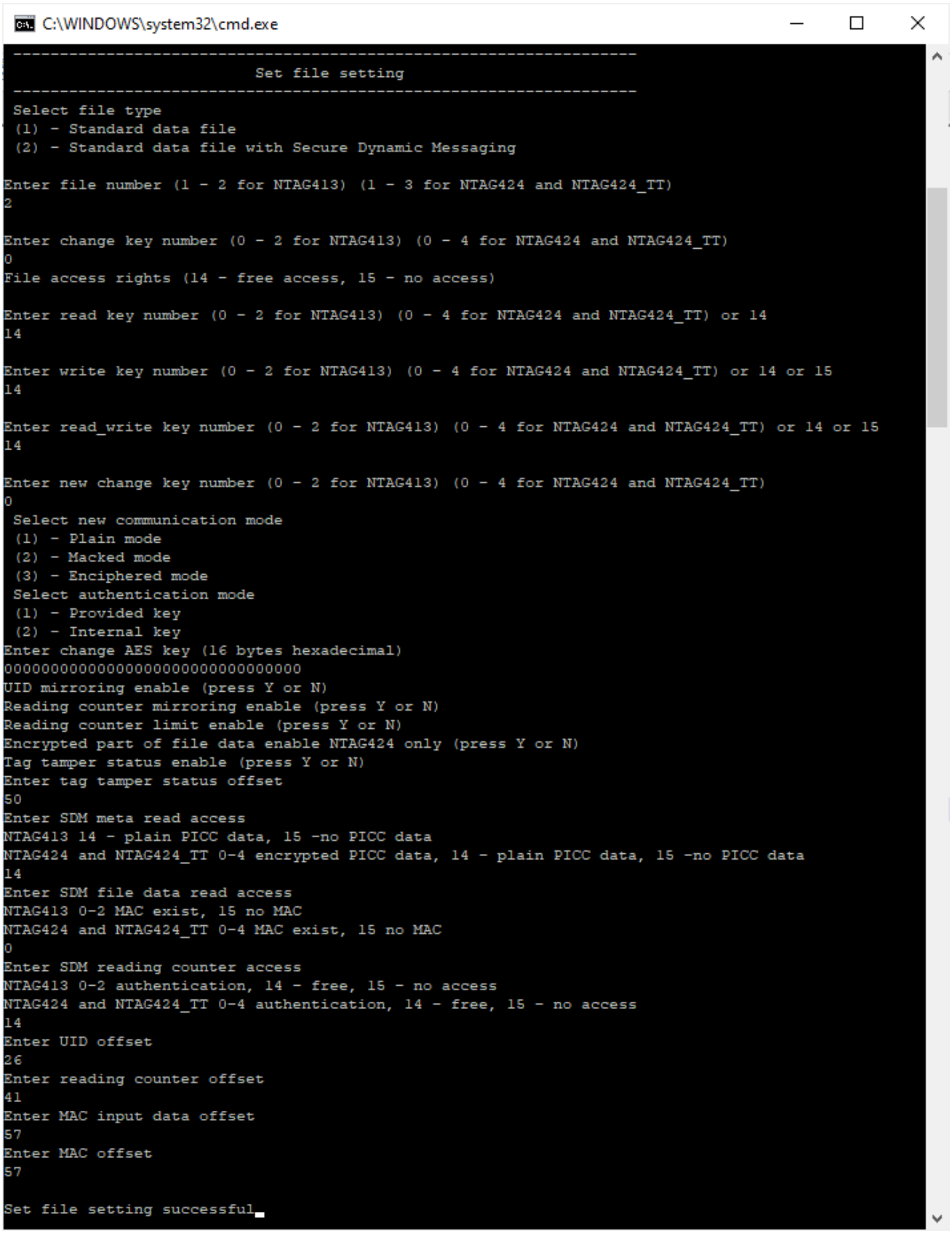
Due to the large number of parameters, there are two functions for setting file parameters.
Example:
Standard data file.
File number 3 (Proprietary file), current communication mode is enciphered, and change key number is 0.
New settings is: plain communication mode, read key 2, write key 3, read/write key 3, change key 0, authentication mode provided key



Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Example 2:
Standard data file with secure dynamic messaging. NTAG 424 TT.
File number 2.
Communication mode plain, SDM enabled, Read key 14 (free access), Write key 14, Read/Write key 14, Change key 0.
SDM options:
UID mirroring: enabled
Read counter: enabled
Read counter limit: disabled
Encrypted part of file data: disabled
Tag Tamper status: enabled
SDM access rights (0x0E free/plain, 0x0F no access/no data
SDM meta read: 0x0E
SDM file key: 0x00
SDM reading counter read key: 0x0E
UID offset: 26
Read counter offset: 41
Tag Tamper status offset: 50
MAC input data offset: 57
MAC offset: 57

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com



Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

2.3. Get UID (3)

NTAG424 DNA only.
Function returns 7 bytes long card UID. This is useful if the Random ID options activated.
Valid authentication with any card key is required.

```
 ------------------------------------------------------------------
                            Get UID
                          NTAG424 only
 ------------------------------------------------------------------
Enter key number (0 - 4)0
 Select authentication mode
 (1) - Provided key
 (2) - Internal key
Enter AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Get UID successful
UID = 04:5B:A8:92:76:63:80
```

2.4. Set Random ID (4)

NTAG424 DNA only.
The card returns 4 bytes random ID instead 7 bytes unique ID.
Warning: this operation is irreversible.
Authentication with application master key (number 0) is required.

```
 ------------------------------------------------------------------
                          Set random ID
                          NTAG424 only
 ------------------------------------------------------------------
 Select authentication mode
 (1) - Provided key
 (2) - Internal key
Enter AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Set random ID successful
```


Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

2.5 Change AES key (5)

Authentication with application master key (number 0) is required.
If the key which will changed is not master key, then old key value is required.
Example:
Key number 4.
Application master key value 0x00000000000000000000000000000000
Old key 4 value 0x00000000000000000000000000000000
New key 4 value 0x11111111111111111111111111111111

```
------------------------------------------------------------------------
                          Change AES key
------------------------------------------------------------------------
Enter key number (0 - 4)
4
 Select authentication mode
 (1) - Provided key
 (2) - Internal key
Enter master AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Enter new AES key (16 hexadecimal bytes)
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11
Enter old AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Change key successful
```

2.6. Linear read (6)

Function read data from file.
Required parameters are:

- File number
- Key number for read, or read/write access
- Communication mode
- Authentication mode (if read key is 14 then no authentication select)
- Start address (0 - max address)
- Length of data

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

```
 ------------------------------------------------------------------
                         Linear read
 ------------------------------------------------------------------
Enter file number (NTAG413 1-2 NTAG424 1-3)
3
Enter key number (NTAG413 0-2 NTAG424 0-4
2
 Select communication mode
 (1) - Plain mode
 (2) - Macked mode
 (3) - Enciphered mode
Enter linear address
0
Enter length
128
 Select authentication mode
 (1) - Provided key
 (2) - Internal key
 (3) - No authentication
Enter AES key
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Liear read successful
Hexadecimal:
54:68:69:73:20:69:73:20:74:68:65:20:74:65:73:74:20:66:6F:72:20:6C:69:
6E:65:61:72:20:64:61:74:61:20:77:72:69:74:65:20:69:6E:74:6F:20:66:69:
6C:65:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
ASCI:
This is the test for linear data write into file
```

2.7. Linear write (7)

Function write data to file.
Required parameters are:

- File number
- Key number for write, or read/write access
- Communication mode
- Authentication mode (if read key is 14 then no authentication select)
- Start address (0 - max address)
- Data in ASCII or hexadecimal format

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

```
 ------------------------------------------------------------------
                          Linear write
 ------------------------------------------------------------------
Enter file number (NTAG413 1-2 NTAG424 1-3)
3
Enter key number (NTAG413 0-2 NTAG424 0-4
3
 Select communication mode
 (1) - Plain mode
 (2) - Macked mode
 (3) - Enciphered mode
Enter linear address
0
Enter data
 (1) - ASCI
 (2) - HEX
Enter ASCI text
This is the test for linear data write into file
 Select authentication mode
 (1) - Provided key
 (2) - Internal key
 (3) - No authentication
Enter AES key
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Liear write successful
```

2.8. Secure dynamic message read (8)

File must be in Secure dynamic message mode, and read access must be free (key no 14, no authentication required).

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

```
-----------------------------------------------------------------
                Secure dynamic message read
   File number = 2, free read access, plain communication mode
-----------------------------------------------------------------
Raw hexadecimal data:
00:74:D1:01:70:55:00:68:74:74:70:3A:2F:2F:77:77:77:2E:74:65:73:74:2E:63:6F:6D:2F:6E:74:34:68:
3F:70:3D:38:44:43:31:44:37:35:34:42:37:42:38:39:32:30:38:36:37:32:35:43:33:38:37:41:43:35:42:
39:33:45:38:65:3D:30:32:46:42:41:32:38:35:42:45:35:33:31:45:43:30:36:42:36:44:46:31:43:34:34:
45:36:44:31:41:44:30:6D:3D:35:41:45:37:37:46:31:43:45:41:41:45:34:32:46:35:26:43:6D:61:63:3D:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00
NDEF file context: http://www.test.com/nt4h?p=8DC1D754B7B892086725C387AC5B93E8e=02FBA285BE531
EC06B6DF1C44E6D1AD0m=5AE77F1CEAAE42F5&Cmac=

PICC encrypted data: 8DC1D754B7B892086725C387AC5B93E8
Enter meta data AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PICC data decrypted successful
UID = 04:5B:A8:92:76:63:80
Reading counter = 97

Encrypted part of file data: 02FBA285BE531EC06B6DF1C44E6D1AD0
Enter file data read AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Part of file data decrypted successful
Part of file data = test data

ASCI MAC data: 5AE77F1CEAAE42F5
ASCI MAC input data: 02FBA285BE531EC06B6DF1C44E6D1AD0m=
MAC is correct
```

Example for NTAG424 TT, where the tag tamper status is within the encrypted part of file data.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

```
 ----------------------------------------------------------------
                Secure dynamic message read
   File number = 2, free read access, plain communication mode
 ----------------------------------------------------------------
Raw hexadecimal data:
00:94:D1:01:90:55:00:68:74:74:70:3A:2F:2F:77:77:77:2E:74:65:73:74:2E:63:6F:6D:2F:6E:74:34:68:3F:70:
3D:45:42:35:42:35:31:31:44:41:39:35:36:44:37:34:41:46:45:42:34:33:43:42:31:44:45:45:46:41:46:33:30:
65:3D:35:43:35:33:38:32:34:34:32:33:37:37:44:30:46:32:36:39:32:38:35:44:43:35:43:42:31:45:38:39:43:
35:36:33:32:41:45:45:32:35:36:41:34:45:39:37:30:34:41:42:39:45:34:33:46:38:44:35:42:44:37:33:46:38:
6D:3D:46:42:31:44:38:41:33:30:32:38:32:45:33:44:36:39:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
NDEF file context: http://www.test.com/nt4h?p=EB5B511DA956D74AFEB43CB1DEEFAF30e=5C5382442377D0F2692
85DC5CB1E89C5632AEE256A4E9704AB9E43F8D5BD73F8m=FB1D8A30282E3D69

PICC encrypted data: EB5B511DA956D74AFEB43CB1DEEFAF30
Enter meta data AES key (16 hexadecimal bytes)
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11
PICC data decrypted successful
UID = 04:5B:A8:92:76:63:80
Reading counter = 15

Encrypted part of file data: 5C5382442377D0F269285DC5CB1E89C5632AEE256A4E9704AB9E43F8D5BD73F8
Enter file data read AES key (16 hexadecimal bytes)
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11
Part of file data decrypted successful
Part of file data = SDM tag tamper testt=CC

Tag tamper permanent status: C
Tag tamper current status: C

ASCI MAC data: FB1D8A30282E3D69
ASCI MAC input data: 5C5382442377D0F269285DC5CB1E89C5632AEE256A4E9704AB9E43F8D5BD73F8m=
MAC is correct
```

2.9. Secure dynamic message write (9)

File must be in Secure dynamic message mode, and read access must be free (key no 14, no authentication required).

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

```
 ---------------------------------------------------------------
                Secure dynamic message write
   File number = 2, free read access, plain communication mode
 ---------------------------------------------------------------

Enter change key number (0 - 2 for NTAG413) (0 - 4 for NTAG424)
0

Enter write key number (0 - 2 for NTAG413) (0 - 4 for NTAG424) or 14 or 15
14

Enter read_write key number (0 - 2 for NTAG413) (0 - 4 for NTAG424) or 0x14 or 0x15
14

Enter new change key number (0 - 2 for NTAG413) (0 - 4 for NTAG424)
0
Does PICC data (UID, SDM reading counter) exist? (press Y or N)
NTAG424 only
Does PICC data encrypted? (press Y or N)
Enter SDM meta read access
NTAG424 0-4 encrypted PICC data
2
UID mirroring enable (press Y or N)
Reading counter mirroring enable (press Y or N)
Encrypted part of file data enable NTAG424 only (press Y or N)
Does MAC exist? (press Y or N)
Enter SDM file data read access
NTAG413 0-2 MAC exist
NTAG424 0-4 MAC exist
2
SDM reading counter limit enable (press Y or N)
Enter SDM reading counter access
NTAG413 0-2 authentication, 14 - free, 15 - no access
NTAG424 0-4 authentication, 14 - free, 15 - no access
2
Enter URL (for example http://www.test.com/nt4h)
Enter ASCI text
http://www.test.com/nt4h
Enter additional number of characters for MAC calculation
counted to left from MAC position (default 0 no additional data)
0
Enter data for encryption
Enter ASCI text
test data
Hexadecimal file data with NDEF header
00:74:D1:01:70:55:00:68:74:74:70:3A:2F:2F:77:77:77:2E:74:65:73:74:2E:63:6F:6D:2F:6E:74:34:68:
3F:70:3D:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:
30:30:30:30:65:3D:74:65:73:74:20:64:61:74:61:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:6D:3D:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
NDEF message
http://www.test.com/nt4h?p=00000000000000000000000000000000e=test data

 Change setting of file number 2
 File change AES key
 Select authentication mode
 (1) - Provided key
 (2) - Internal key
Enter change AES key (16 bytes hexadecimal)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 Write NDEF into file number 2
Secure dynamic message write successful
```


Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Example for NTAG424 TT, where the tag tamper status is within the encrypted part of file data.

```
 ---------------------------------------------------------------
                Secure dynamic message write
   File number = 2, free read access, plain communication mode
 ---------------------------------------------------------------

Enter change key number (0 - 2 for NTAG413) (0 - 4 for NTAG424 and NTAG424_TT)
0

Enter write key number (0 - 2 for NTAG413) (0 - 4 for NTAG424 and NTAG424_TT) or 14 or 15
14

Enter read_write key number (0 - 2 for NTAG413) (0 - 4 for NTAG424 and NTAG424_TT) or 0x14 or 0x15
14

Enter new change key number (0 - 2 for NTAG413) (0 - 4 for NTAG424 and NTAG424_TT)
0
Does PICC data (UID, SDM reading counter) exist? (press Y or N)
NTAG424 and NTAG424_TT
Does PICC data encrypted? (press Y or N)
Enter SDM meta read key number (0 - 4)
2
UID mirroring enable (press Y or N)
Reading counter mirroring enable (press Y or N)
Encrypted part of file data enable NTAG424 and NTAG424_TT (press Y or N)
Does MAC exist? (press Y or N)
Enter SDM file data read key number
NTAG413 0-2 MAC exist
NTAG424 and NTAG424_TT 0-4 MAC exist
2
SDM reading counter limit enable (press Y or N)
Enter SDM reading counter access
NTAG413 0-2 authentication, 14 - free, 15 - no access
NTAG424 and NTAG424_TT 0-4 authentication, 14 - free, 15 - no access
14
Enter URL (for example http://www.test.com/nt4h)
Enter ASCI text
http://www.test.com/nt4h

TT status mirroring enable (press Y or N)
Does TT status within encrypted part of file data? (press Y or N)

Enter additional number of characters for MAC calculation
counted to left from MAC position (default 0 no additional data)
0
Enter data for encryption
Enter ASCI text
SDM tag tamper test
Hexadecimal file data with NDEF header
00:94:D1:01:90:55:00:68:74:74:70:3A:2F:2F:77:77:77:2E:74:65:73:74:2E:63:6F:6D:2F:6E:74:34:68:3F:70:
3D:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:30:
65:3D:53:44:4D:20:74:61:67:20:74:61:6D:70:65:72:20:74:65:73:74:74:3D:00:00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
6D:3D:00:00:00:00:00:00:00:00:00:00:00:00:00:00
NDEF message
http://www.test.com/nt4h?p=00000000000000000000000000000000e=SDM tag tamper testt=

 Change setting of file number 2
 File change AES key
 Select authentication mode
 (1) - Provided key
 (2) - Internal key
Enter change AES key (16 bytes hexadecimal)
00000000000000000000000000000000

 Write NDEF into file number 2
Secure dynamic message write successful
```


Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

2.10. Get SDM reading counter (a)

The Secure dynamic message reading counter exists only if in file settings enabled SDM.
Depends of setting of SDM reading counter access, authentication required or not.

```
 ------------------------------------------------------------------
                    Get SDM reading counter
 ------------------------------------------------------------------
Enter file number (NTAG413 2 NTAG424 2-3)
2
 Select authentication mode
 (1) - Provided key
 (2) - Internal key
 (3) - No authentication
Enter key number (NTAG413 0-2 NTAG424 0-4
2
Enter AES key (16 hexadecimal bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

SDM reading counter = 84
```

2.11. Tag tamper enable (b)

NTAG424 TT DNA only.
Enabling the Tag Tamper feature.
Warning: this operation is irreversible.
Authentication with application master key (number 0) is required.

Example for free tag tamper status read.

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

```
------------------------------------------------------------------
                    Tag tamper status enable
------------------------------------------------------------------

Enter TT status access
key ordinal number (0 - 4), free access - 14, no access - 15
14
Select authentication mode
 (1) - Provided key
 (2) - Internal key
Enter AES key
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Tag tamper enabled successful
```

2.12 Get tag tamper status (c)

NTAG424 TT DNA only.
Example when the seal is still closed.

```
------------------------------------------------------------------
                    Get tag tamper status
------------------------------------------------------------------
Select authentication mode
 (1) - Provided key
 (2) - Internal key
 (3) - NoAuthentication

Tag tamper status read successful
Permanent status is: C
Current status is: C
```

Example when the seal was opened.

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

```
------------------------------------------------------------------------
                        Get tag tamper status
------------------------------------------------------------------------
Select authentication mode
 (1) - Provided key
 (2) - Internal key
 (3) - NoAuthentication

key ordinal number (0 - 4)
0
Enter AES key
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Tag tamper status read successful
Permanent status is: O
Current status is: O
```

2.13. Check ECC signature (d)

Example for cards with UID. Authentication isn't required.

```
------------------------------------------------------------------
Card type: DL_NTAG_424_DNA_TT, sak = 0x20, uid[7] = 04:75:7C:AA:5C:5E:80
------------------------------------------------------------------
------------------------------------------------------------------
                    ECC signature validation
------------------------------------------------------------------

ECC signature read successful
ECC signature: 02:D9:33:90:43:1C:8B:37:1F:6C:15:67:0F:7F:52:97:26:D6:E3:C5:EC:D5:81:30:6F:61:89:73:
48:F2:0D:BC:69:3D:4B:1C:16:E3:A3:88:77:C5:AC:82:A2:DA:15:B7:26:D0:5E:2D:1E:B3:48:39

ECC signature validation
TAG IS NXP GENUINE
```

Example for cards with Random ID. Authentication with valid key required.

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

```
------------------------------------------------------------------
Card type: DL_NTAG_424_DNA_TT, sak = 0x20, uid[4] = 08:40:B1:05
------------------------------------------------------------------
------------------------------------------------------------------
                    ECC signature validation
------------------------------------------------------------------

Random ID detected, authentication required
Select authentication mode
 (1) - Provided key
 (2) - Internal key

key ordinal number (0 - 4)
0
Enter AES key
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

ECC signature read successful
ECC signature: 67:01:6D:2C:C2:0C:5B:21:0C:22:AE:F0:57:2E:4B:35:F8:68:84:8E:EA:E4:D3:25:4E:72:DB:04:
66:96:A5:DF:70:B4:E4:C0:45:6E:4B:4F:D2:07:DD:E5:5C:42:51:C1:08:C9:4D:96:64:3E:20:BA

ECC signature validation
TAG IS NXP GENUINE
```

2.14. Store AES key into reader (e)

The reader may store 16 AES keys. Key number 0 - 15.
Example:
Store key 0x00000000000000000000000000000000 into reader in address 1.

```
------------------------------------------------------------------
                    Store AES key into reader
------------------------------------------------------------------
 (1) - AES keys
 (2) - Unlock reader
 (3) - Lock reader

Enter AES key
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Enter key index (0 - 15)
1

Key written into reader
```

You can lock the key into the reader with an 8 bytes password. By default keys are unlocked, and you can enter any password for locking.
Example:
Password is "12345678"

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

```
 ------------------------------------------------------------------
                    Store AES key into reader
 ------------------------------------------------------------------
 (1) - AES keys
 (2) - Unlock reader
 (3) - Lock reader

Enter password of 8 bytes
 (1) - ASCI
 (2) - HEX
Enter ASCI text
12345678

Reader keys are locked
```

If keys are locked, you must unlock them first with an 8 bytes long password.
Example:
Password is "12345678"

```
 ------------------------------------------------------------------
                    Store AES key into reader
 ------------------------------------------------------------------
 (1) - AES keys
 (2) - Unlock reader
 (3) - Lock reader

Enter password of 8 bytes
 (1) - ASCI
 (2) - HEX
Enter ASCI text
12345678

Reader keys are unlocked
```


Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Revision history

Date	Version	Comment
2021-09-10	1.3	Term Secure Dynamic Messaging file replaced with Standard Data File with SDM
2020-10-07	1.2	Tag Tamper and Originality checking added
2020-01-30	1.0	Base document

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com