AN12998

NTAG 22x DNA (StatusDetect) - Features and hints

Rev. 1.1 — 17 February 2022

Application note
COMPANY PUBLIC

Document information

Information	Content
Keywords	NTAG 22x DNA (StatusDetect), features, hints, configuration, personalization
Abstract	Guidelines for integration, configuring and verification side computations for NTAG 22x DNA (StatusDetect)

Revision history

Rev	Date	Description
v 1.1	20220217	Security status changed to "Company public"
v 1.0	20220127	Initial version

1 Abbreviations

Table 1. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
C-APDU	Command APDU
CTT	Capacitive Tag Tamper, counter measure to detect product manipulations by capacitive means
CMAC	MAC according to NIST Special Publication 800-38B
CRC	Cyclic Redundancy Check
IC	Integrated Circuit
KDF	Key Derivation Function
LSB	Lowest Significant Byte
LSb	Lowest Significant Bit
MAC	Message Authentication Code
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
R-APDU	Response APDU (received from PICC)
TT	Tag Tamper
UID	Unique IDentifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

2 About this document

This document addresses developers who are developing applications based on NTAG 22x DNA (StatusDetect) products.

This application note is a supplementary document for implementations using the mentioned products. It shall be used in addition to NTAG 22x DNA (StatusDetect) data sheets [2], [3], [4] and [5]. The best use of this application note is achieved by reading the mentioned data sheets in advance.

Note: This application note does not replace data sheets, or design guides.

2.1 Byte order in this document

All values within this document are in HEX values, if not noted otherwise. For example, 010203 means 010203h (0x010203).

2.1.1 LSB representation

Represented least significant byte (LSB) first are:

- plain command parameters consisting of multiple bytes
- ISO/IEC 14443 parameters during the activation
- UID mirror

2.1.2 MSB representation

Represented as most significant byte (MSB) first are:

- cryptographic parameters
- keys
- random numbers exchanged during authentication
- computed MACs - CMAC mirror
- NFC Counter mirror for SUN-CMAC calculation

3 Target applications

NTAG 22x DNA (StatusDetect) is attractive for many applications. To name few in the list below:

- **Anti-counterfeiting**
  Verify authenticity of physical goods and identify sales outside authorized markets.
- **Tamper protection**
  Digital guarantee of the seal protection.
- **Secured exclusive user experiences**
  Reward customers with truly exclusive and personalized content, offers, and privileges.
- **Document authentication**
  Authenticate originality and track provenance of documents that bear credentials.
- **Protected monetary offers**
  Confer trust to proximity transactions such as coupons, promotions, or loyalty points.
- **Secure authentication and configuration of closed loop devices**
  Authenticate consumables and parts and enable automated transfer of device settings.
- **Verified physical visitor presence**
  Enable secure visitor authentication, with proof of live presence and service records.
- **Secure log-in credentials**
  Protect web services using two-factor authentication logons to sensitive content sites.

4 Standards compliancy and certifications

4.1 ISO 14443

NTAG 22x DNA (StatusDetect) is fully compliant to layers 1, 2, 3 of ISO/IEC 14443 [1].

4.2 NFC Forum compliancy

NFC tag is a contactless tag capable of storing NDEF data, which interoperates with ISO 14443 infrastructure and NFC devices as defined by the NFC Forum specifications. NFC Forum defines logical data structure for storing NDEF message into Tag's EEPROM.

Structure of EEPROM memory complies with NFC Forum Type 2 Tag [7].

4.3 NFC Forum certification

NTAG 22x DNA (StatusDetect) is NFC Forum certified product.

4.4 Security certification

NTAG 22x DNA (StatusDetect) is CC EAL +3, AVA_VAN.2 certified product.

5 NFC Forum NDEF features

5.1 NFC counter

NFC counter provides to verification side (e.g. server) information about how many unique NDEF reads were done on particular tag with it's specific UID. NFC Counter also serves for randomness as one of inputs in SUN-CMAC calculation Section 5.3.2. Therefore when SUN-CMAC is used the NFC counter increment shall not be disabled (NFC_CNT_INCR_EN = 0b at delivery). If NFC Counter is disabled, the SUN-CMAC value remains a constant for every tap, so not unique. This would diminish the CMAC's intention and strength.

NFC counter value is stored in a special part of memory. It is 3 Bytes in size and irreversibly increased on a first valid READ (or FAST_READ) command after NTAG ISO activation. This counter size offers 32 years of incrementing if tag is tapped every minute.

NFC Counter value can be retrieved (Read out from the tag) by:

- READ_CNT command (39h 02h), which returns NFC Counter hexadecimal value
- READ or FAST_READ command of the NDEF message, where NFC counter is mirrored automatically to User Memory location (e.g. to the Type2Tag Area's NDEF message) as depicted in Section 5.2.2.

5.2 ASCII mirroring

This functionality enables NTAG 22x DNA (StatusDetect) to virtually mirror:

- 7 byte UID
- 3 byte NFC counter value
- 5 byte Tag Tamper information
- 8 byte SUNCMAC

over the physical memory of the IC in ASCII code. These mirrors can be (is intended to) part of NDEF Message Record as shown below. On the READ or FAST READ command to the involved user memory pages, NTAG 22x DNA (StatusDetect) responds with the virtual memory content of the UID, NFC counter value and Tag Tamper message in ASCII code.

Note: If ASCII mirroring is enabled (MIRROR_EN = 1b), then all three (3) parts are always mirrored together with "x" as separator character: UID, NFCCounter, SUNCMAC. Means that e.g. NFCCounter mirror cannot be disabled, keeping other two enabled.

Note: Every nibble of a mirrored byte requires one byte of ASCII code. It means that the length of mirrored element gets doubled. For example 7 bytes of UID will be mirrored to 14 bytes of ASCII codes.

Block [hex]	Byte 0	Byte 1	Byte 3	Byte 4	ASCII
00	04	AA	2B	0D	(UID)
01	D2	33	57	80	(UID)
02	36	48	00	00	(BCC1)
03	E1	10	12	00	(CC)
04	01	03	A0	0C	….
05	34	03	3E	D1	4.>.
06	01	3A	55	04	.
07	6E	74	61	67	ntag
08	2E	6E	78	70	.nxp
09	2E	63	6F	6D	.com
0A	2F	32	32	78	/22x
0B	3F	6D	3D	30	?m=0
0C	31	30	32	30	1020
0D	33	30	34	30	3040
0E	35	39	36	30	5060
0F	37	78	36	35	7x65
10	34	33	32	31	4321
11	78	30	31	30	x010
12	32	30	33	30	2030
13	34	30	35	30	4050
14	36	30	37	30	6070
15	38	FE	00	00	8
.	00	00	00	00	

Figure 1. Physically programmed EEPROM memory

Block [hex]	Byte 0	Byte 1	Byte 3	Byte 4	ASCII
00	04	AA	2B	0D	(UID)
01	D2	33	57	80	(UID)
02	36	48	00	00	(BCC1)
03	E1	10	12	00	(CC)
04	01	03	A0	0C	….
05	34	03	3E	D1	4.>.
06	01	3A	55	04	.
07	6E	74	61	67	ntag
08	2E	6E	78	70	.nxp
09	2E	63	6F	6D	.com
0A	2F	32	32	78	/22x
0B	3F	6D	3D	30	?m=0
0C	34	41	41	32	4AA2
0D	42	44	32	33	BD23
0E	33	35	37	38	3578
0F	30	78	30	30	0x00
10	30	30	30	31	0001
11	78	42	31	38	xB18
12	38	41	43	36	8AC6
13	46	36	39	31	F691
14	34	30	42	39	40B9
15	32	FE	00	00	2
.	00	00	00	00	

Figure 2. Virtual content overlay

NDEF Message - Record 1. URI Records of:

- Physically programmed EEPROM: https://ntag.nxp.com/22x?m=01020304050607x654321x0102030405060708
- Virtual overlaid content: https://ntag.nxp.com/22x?m=04AA2BD2335780x000001xB188AC6F69140B92

5.2.1 UID ASCII mirror function

With MIRROR_EN set to 1b, ISO14443 7-Byte UID is mirrored into User EEPROM memory. Values are HEX values of ASCII characters mirrored when NFC interface reader does first READ (or FAST_READ) command during RF ON session. Location of mirror start can be configured by setting MIRROR_PAGE and MIRROR_BYTE.

NFC Forum compatible interface reads NDEF message from the tag and converts it from HEX to ASCII characters automatically.

Block [hex]	Byte 0	Byte 1	Byte 3	Byte 4	ASCII
00	04	AA	2B	0D	(UID)
01	D2	33	57	80	(UID)
02	36	48	00	00	(BCC1)
03	E1	10	12	00	(CC)
04	01	03	A0	0C	….
05	34	03	3E	D1	4.>.
06	01	3A	55	04	.
07	6E	74	61	67	ntag
08	2E	6E	78	70	.nxp
09	2E	63	6F	6D	.com
0A	2F	32	32	78	/22x
0B	3F	6D	3D	30	?m=0
0C	34	41	41	32	4AA2
0D	42	44	32	33	BD23
0E	33	35	37	38	3578
0F	30	.	.	.	0...
.	.	.	.	.	.

Figure 3. UID ASCII mirror

NFC Forum reader parses read NDEF URI Record content to OS as:

https://ntag.nxp.com/22x?m=04AA2BD2335780... (rest)

5.2.2 NFC counter ASCII mirror function

The 24-bit NFC Counter is located in dedicated memory location, which can be accessed by READ_CNT command. Value of NFC Counter can be mirrored (if MIRROR_EN is set to 1b) over User memory EEPROM in MSB order as HEX value of ASCII code.

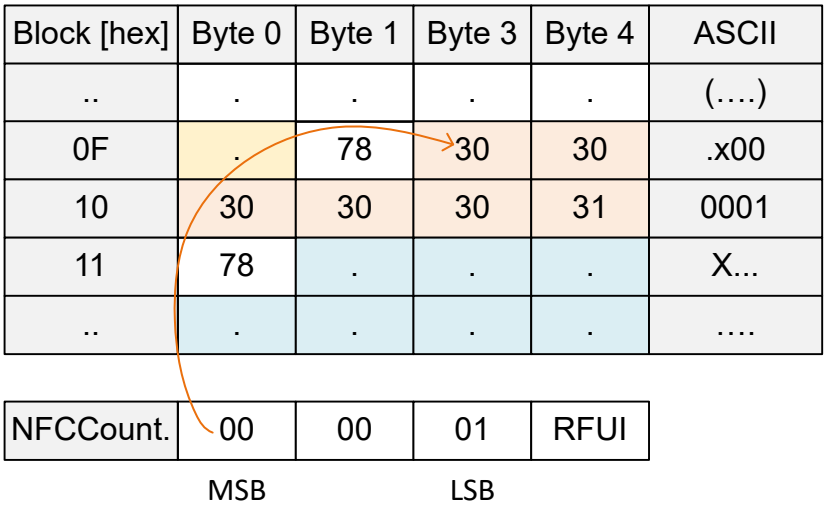


Figure 4. NFC Counter ASCII mirror

NFC Forum reader parses read NDEF URI Record content to reader's operating system as URI schemed data:

https://ntag.nxp.com/22x?m=……..x000001x...

5.2.3 SUN-CMAC mirror function

The SUNCMAC is calculated over the UID, NFC counter and for NTAG 22x DNA StatusDetect also Tag Tamper information. This function enables NTAG 22x DNA (StatusDetect) to virtually mirror the 8 byte SUNCMAC in ASCII code into the physical memory of the IC.

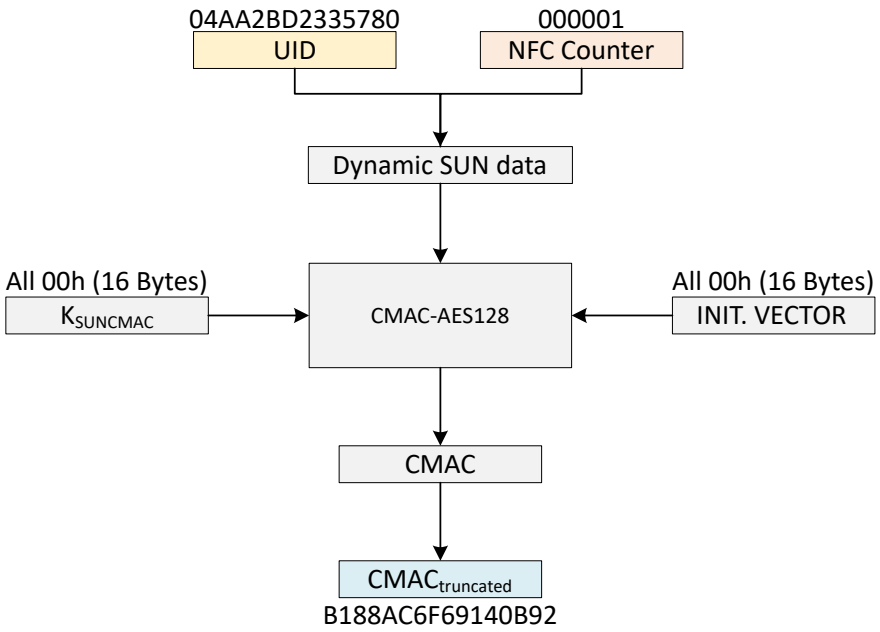


Figure 5. SUN-CMAC calculation diagram with example data

Block [hex]	Byte 0	Byte 1	Byte 3	Byte 4	ASCII
..	.	.	.	.	
11	78	42	31	38	xB18
12	38	41	43	36	8AC6
13	46	36	39	31	F691
14	34	30	42	39	40B9
15	32	FE	00	00	2
..	.	.	.	.	

Figure 6. SUN-CMAC ASCII Mirror

SUN-CMAC computation (can be used for verification as well) is described in [Section 5.3.2]

NFC Forum reader parses read NDEF URI Record content to OS as:

https://ntag.nxp.com/22x?m=04AA2BD2335780x000001xB188AC6F69140B92

5.2.4 Tag Tamper mirror function

This functionality is present on NTAG 22x DNA StatusDetect product only. For more information on Capacitive Tag Tamper (StatusDetect), refer to [6].

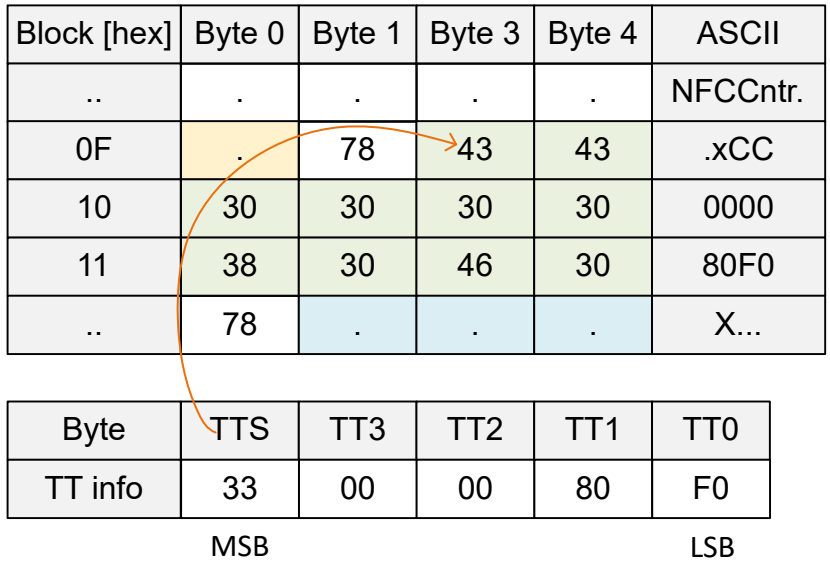
5.2.4.1 Resistive TT ASCII mirror

NTAG 22x DNA StatusDetect with enabled resistive TT measurement detects, during the start-up, open/close status of an external TT wire/conductor connected between DP pad and GND pad.

- tbd (image here) -

5.2.4.2 Capacitive TT ASCII mirror

NTAG 22x DNA StatusDetect with enabled capacitive TT measurement detects, during the start-up, open/close status of an external TT wire/conductor connected between DP pad and GND pad.



Block [hex]	Byte 0	Byte 1	Byte 3	Byte 4	ASCII
..	.	.	.	.	NFCCntr.
0F	.	78	43	43	.xCC
10	30	30	30	30	0000
11	38	30	46	30	80F0
..	78	.	.	.	X...

Byte	TTS	TT3	TT2	TT1	TT0
TT info	33	00	00	80	F0
	MSB				LSB

Figure 7. Capacitive TT ASCII mirror

5.3 Secure unique NDEF (SUN)

5.3.1 DynamicSUNData

SUNCMAC is computed using the underlying CMAC AES block cipher.

SUNCMAC is calculated over input data in following order:

1. UID [0:6]
2. NFC counter [2:0]
3. NIST padding bytes

excluding separation bytes ("x" or 78h)!

If Tag Tamper feature is enabled, SUNCMAC is calculated over input data in following order:

1. UID [0:6]
2. NFC counter [0:2]
3. TagTamperStatus [6:0]
4. TagTamperInfo [3:0]
5. NIST padding bytes

excluding separation bytes ("x" or 78h)!

Note: NFC Counter serves for randomness. Therefore, NFC counter increment shall not be disabled (bit NFC_CNT_INCR_EN). If it is disabled, the SUNCMAC value remains a constant for every tap, not unique, which significantly reduces security.

5.3.2 SUNCMAC computation

CMAC is calculated by the NTAG 22x DNA (StatusDetect) automatically. This computation shall serve for verification side, to be able to compute, compare and verify the CMAC for given input data (K_{SUNMAC_KEY} and DynamicSUNData). Verification side gets SUN to verify upon usually via NDEF URL. It is read out by NFC interface automatically (e.g. NFC mobile) and submitted to verification server via mobile's browser.

Prerequisites:	• CMAC algorithm with AES-128 cipher core • Knowledge of DynamicSUNData
Key used:	AES Key1 = SUNCMAC_KEY
Key Length [bytes]:	16
Algorithm:	SUN-CMAC = AES-CMAC($K_{SUNCMAC\_KEY}$; DynamicSUNData)

Output:

1. SUN-CMAC

Table 2. SUN-CMAC calculation

Step	Command		Data
1	UID	=	04C767F2066180
2	NFCCounter	=	000003 (MSB first as per [Section 2.1])
3	$K_{SUNCMAC\_KEY}$	=	00000000000000000000000000000000
4	DynamicSUNData	=	04AA2BD2335780000003
	Subkey Generation Algorithm		As recommended in [NIST-CMAC]
5	Step 1. L = AES-128(K, const_ Zero)	=	66E94BD4EF8A2C3B884CFA59CA342B2E
6	Step 2. if MSB(L) is equal to 0 then **K1 := L << 1**; else K1 := (L << 1) XOR const_Rb	=	CDD297A9DF1458771099F4B39468565C

Table 2. SUN-CMAC calculation*...continued*

Step	Command		Data
7	Step 3. if MSB(K1) is equal to 0 then K2 := K1 << 1; else **K2 := (K1 << 1) XOR const_Rb**	=	9BA52F53BE28B0EE2133E96728D0AC3F
	CMAC computation		As recommended in [NIST-CMAC]
8	Step 1.	=	K1, K2 generated
9	Step 2.	=	Mlen = 0, n = 1
10	M1*||10^j	=	04C767F20661800000003800000000000
11	Step 4. If Mn is a complete block: then M1 = K1 ⊕ M1* else **M1 = K2 ⊕ (M1*||10^j)**	=	9F6248A1B84930EE2130696728D0AC3F
12	Step 6. AES-128($K_{SUNCMAC\_KEY}$; M1)	=	4837F3791479D73D09FE865947213988
13	Step 7. Truncate CMAC	=	3779793DFE592188

6 Key management

6.1 Key handling

NTAG 22x DNA (StatusDetect) comes with 2 keys:

1. AES_KEY (only on NTAG 224 DNA (StatusDetect))
2. SUNCMAC_KEY

Table 3. Keys

Key name	Key type, size	Description	Shall be die individual?[1]
AES_KEY	AES-128 (16 Bytes)	Is used to access elements in the protected memory areas, after successful authentication Section 7.2	Yes
SUNCMAC_KEY	AES-128 (16 Bytes)	Is used to calculate SUN-CMAC response Section 5.3.2	Yes

1 - Key shall be UID diversified. More info on key diversification can be found in [9]

2 - In order to change applicable key, upfront successful mutual authentication is needed with AES_KEY.

Values of the keys can be permanently (irreversibly) locked against changes by setting LOCK_ SUNCMAC_KEY bit or LOCK_AES_KEY bit.

BLOCK_LOCK_ KEY permanently (irreversibly) locks status of LOCK_ SUNCMAC_KEY and LOCK_AES_KEY bits.

Note: EEPROM Memory pages holding the AES_KEY and SUNCMAC key can never be read (READ or FAST_READ command), independent of the configuration. Reading would return values masked with zeroes.

6.2 Key programming

Keys (AES_KEY, SUNCMAC_KEY) can be written during personalization or at any later stage using the WRITE command, with condition that keys are not already locked against writing.

Note: Over the RF interface data is always sent in plain between PCD and a tag (NTAG 22x DNA (StatusDetect)). Therefore personalization environment needs to be secured or for convenience NXP's Trust Provisioning service can be used.

7 Authentication

7.1 Password authentication

ISO14443-3 Activation is needed upfront.

Table 4. Command PWD_AUTH

Step	Command		Data Message
1	Password	=	00000000
2	Command: PWD_AUTH	=	1B
3	Arg	=	00
4	PWD_AUTH with password	>	1B00000000
5	R-APDU PACK[1]	<	0000

1 - PACK response is configurable/programmable

7.2 Mutual authentication

ISO14443-3 Activation is needed upfront.

Table 5. Command Authenticate (part1, part2) using AES_KEY

Step	Command		Data Message
1	K_{AES_KEY}	=	00000000000000000000000000000000
2	Command: Authenticate - part 1	=	1A
3	Arg	=	00
4	IV	=	00000000000000000000000000000000
5	Authenticate - part 1	>	1A00
6	R-APDU AF || E(K_{AES_KEY}, RndB)	<	AF50930CE80347F2883EF65AB675E2B60A
7	E(K_{AES_KEY}, RndB)	=	50930CE80347F2883EF65AB675E2B60A
8	D(K_{AES_KEY}, RndB)	=	629FB1507560F896DA308E90E1C16894
9	PCD prepares RndB' (rotate left by 1 byte)	=	9FB1507560F896DA308E90E1C1689462
10	PCD generates RndA	=	06B56B43FF20100549D4BB8609B1FAE7
11	PCD prepares RndA || RndB'	=	06B56B43FF20100549D4BB8609B1FAE79FB150 7560F896DA308E90E1C1689462
12	E(K_0, RndA || RndB')	=	E9DD8325737BDE109BE76D41A98C20858430D FDC1A4A09F2EA46796F57833FA0
13	Authenticate - part 2	>	AFE9DD8325737BDE109BE76D41A98C2085843 0DFDC1A4A09F2EA46796F57833FA0
14	R-APDU 00 || E(K_{AES_KEY}, RndA')	<	00C7EC1ECF388FA44D520FB20CC2FF74E8
15	E(K_{AES_KEY}, RndA')	=	C7EC1ECF388FA44D520FB20CC2FF74E8

Table 5. Command Authenticate (part1, part2) using AES_KEY*...continued*

Step	Command		Data Message
16	D(K_{AES_KEY} , RndA´)	=	B56B43FF20100549D4BB8609B1FAE706
17	RndA´ (16 byte)	=	C5DB8A5930439FC3DEF9A4C675360F13
18	PDcap2 (6 byte)	=	000000000000
19	PCDcap2 (6 byte)	=	000000000000
20	RndA (rotate right for 1 byte)	=	06B56B43FF20100549D4BB8609B1FAE7
21	PCD compares sent RndA (from step 10.) and received RndA (from step 20)	=	06B56B43FF20100549D4BB8609B1FAE7 == 06B56B43FF20100549D4BB8609B1FAE7
22	SV 2 = [0x5A][0xA5][0x00][0x01] [0x00][0x80][RndA[15:14] || [(RndA[13:8] ⊕ RndB[15:10])] || [RndB[9:0] || RndA[7:0]	=	5AA50001008006B509DC4E706565F896DA308E 90E1C1689449D4BB8609B1FAE7
23	CMAC Session Key ($K_{SesAuthMAC}$) = CMAC(K_0, SV2)	=	ED03090FB065B64E512F50AB9B4DD317

7.3 Failed Authentication Counter

As card-only side-channel attacks are a common risk for NTAG 22x DNA (StatusDetect), a failed authentications limit is present. It can be activated by setting corresponding configuration element to a value between 001h and 3FFh. The failed authentication counter is by default disabled (set to value 000h).

Note: It is recommended to reset this limit to a value of 100 (064h) or below.

The negative authentication counter will count each unsuccessful attempt of authentication. Each successful authentication reduces the counter by 10h. Once the negative authentication counter reaches its limit, the access to protected memory cannot be further authenticated even if the used key is correct. Any further authentication attempt will result in a failure.

8 Special functionalities

8.1 Originality Signature Verification

8.1.1 Asymmetric check

Each NTAG 22x DNA (StatusDetect) contains the pre-programmed NXP Originality Signature.

- It is computed according to Elliptic Curve DSA (ECDSA) based on the UID
- Key pair created in NXP Fab's HSM. Private key is stored in a high secure HSM in NXP premises, Public Key is provided in this document.
- Signature is 48 bytes long and calculated according to SEC standard **secp192r1** curve

Asymmetric check procedure consists of:

- retrieve Originality Signature (48 bytes) from the tag with READ_SIG command
- knowledge of Public key - available for public below
- ECDSA signature verifying operation needs to be applied - procedure and sample code (C#, Java, C) can be found in [10]

NTAG public key: **0485 D5 B9 35 3B 4F AA 77 58 1B A2 AE 96 63 0C 58 76 D6 E8 60 33 08 AB E9 A8 1A 0B 50 6F 52 D0 2D 04 FE E6 F2 D3 65 B3 DE E7 B9 FA D9 13 3E 29 76**

04 = IETF protocols use the *[SEC1]* representation of a point on an elliptic curve, which is a sequence of the following fields:

SEC1 point representation	
Field	**Description**
B0	{02, 03, 04}, where 02 or 03 represent a compressed point (x only), while 04 represents a complete point (x,y)
X	x coordinate of a point
Y	y coordinate of a point, optional (present only for B0=04)

Table 6. Asymmetric Originality Signature verification

Step	Command		Data
1	Cmd	=	3C
2	Cmd header (Address)	=	00
3	C-APDU	>	3C00
4	R-APDU (56 bytes of ECDSA)	<	6A5D5E034F4FC823CACAB56C1A77A409B8DB345F89BD3FD59ED1F9C0093518609BE62D0A20764D2011E47EFA187F29AA
5	**ECDSA verification**		
6	Elliptic curve name	=	secp192r1

Table 6. Asymmetric Originality Signature verification*...continued*

Step	Command		Data
7	Input data (UID)	=	043302218D3D00
8	Public key point coordinate **xD** (24 bytes)	=	85D5B9353B4FAA77581BA2AE96630C5876D6E8603308ABE9
9	Public key point coordinate **yD** (24 bytes)	=	A81A0B506F52D02D04FEE6F2D365B3DEE7B9FAD9133E2976
10	Signature part 1 **r**	=	6A5D5E034F4FC823CACAB56C1A77A409B8DB345F89BD3FD5
11	Signature part 2 **s**	=	9ED1F9C0093518609BE62D0A20764D2011E47EFA187F29AA
12	Use ECDSA Verify tools (e.g. free online tools)	=	Signature valid

8.2 Capacitive Tag Tamper operation

For more information on Capacitive Tag Tamper (StatusDetect), refer to [4], [5] and application note [6].

NTAG 22x DNA (StatusDetect) with enabled capacitive TT measurement mode detects during the start-up the change of an external TT capacitor value in the range from 2 pF to 5 pF with accuracy of 0.25 pF of external capacitor connected between DP and GND pad. TT status is interpreted as ”closed”, if measured capacitance is within the low and high limits stored (by customer after calibration) in the IC user configuration area. Otherwise the TT status is interpreted as ”open”.

The analog part of the Capacitive Tag Tamper (CTT) block works by comparing the charging time of 2 capacitors (one IC internal, one external) until given threshold is reached. A fixed internal capacitor will determine a reference slope, while a trimming routine from PCD is used to adjust the slope for the external capacitor to get as close as possible to the internal capacitor charge time slope.

9 References

[1] ISO/IEC 14443 - Cards and security devices for personal identification — Contactless proximity objects. Part 1, 2 and 3, ISO/IEC 14443-x:2018(E)

[2] NTAG 223 DNA (NT2H2331G0) - NFC T2T compliant IC, doc.no. 5989xx[1]

[3] NTAG 224 DNA (NT2H2421G0) - NFC T2T compliant IC, doc.no. 5991xx

[4] NTAG 223 DNA StatusDetect (NT2H2331S0) - NFC T2T compliant IC with StatusDetect feature, doc.no. 5988xx

[5] NTAG 224 DNA StatusDetect (NT2H2421S0) - NFC T2T compliant IC with StatusDetect feature, doc.no. 5990xx

[6] AN12999 - NTAG 22x DNA StatusDetect - Capacitive loop sensing guidelines, doc.no. 7093xx

[7] NFC Type 2 Tag Technical Specification, Version 1.1, 2019-12-12 [T2T] NFC Forum™

[8] NIST Special Publication 800-38B, National Institute of Standards and Technology (NIST). Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf

[9] AN10922 - Symmetric key diversifications

[10] AN11350 - NTAG Originality Signature Validation Rev. 1.2 — 22 August 2017, doc. no. 2604xx

1 xx … document version number

10 Legal information

10.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

10.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

10.3 Licenses

Purchase of NXP ICs with NFC technology — Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

10.4 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

NTAG — is a trademark of NXP B.V.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 17 February 2022
Document identifier: AN12998