NTP5210

NTAG 5 switch - NFC Forum-compliant PWM and GPIO bridge

Rev. 3.3 — 3 July 2020
544633

Product data sheet
COMPANY PUBLIC

1 General description

Designed as an MCU replacement in various gaming and lighting applications, this NFC tag adds connectivity and increases flexibility while saving energy and lowering the bill of materials.

NXP's NTAG 5 switch lets designers eliminate the MCU in selected gaming and lighting applications and other cost sensitive designs, for added functionality, connectivity, and efficiency at a lower cost. Operating at 13.56 MHz, it is an NFC Forum-compliant (customer development board is NFC Forum certified - Certification ID: 58626) contactless tag that can be read by any NFC-enabled device at close range and by an ISO/IEC 15693-enabled industrial reader over a longer range. Easy configuration supports a range of control functions, and the integrated originality check lets the user verify an end product's authenticity.

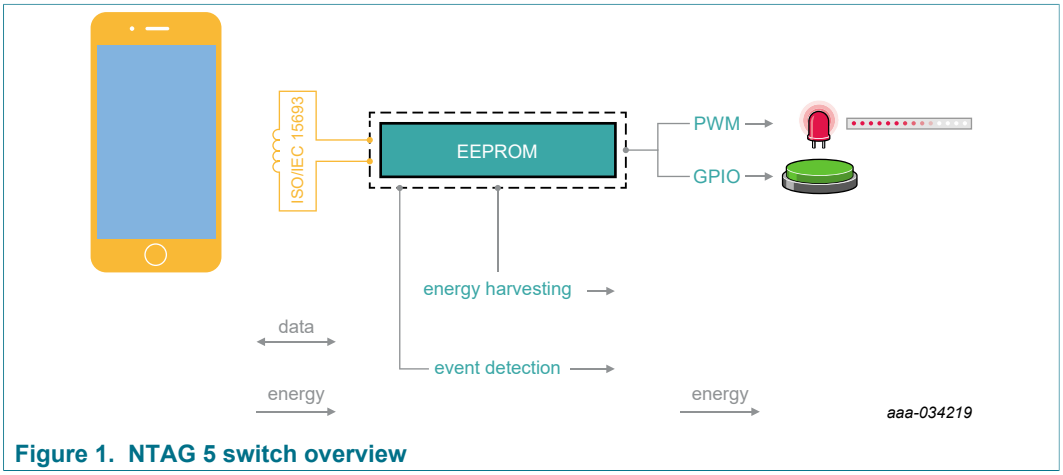


Figure 1. NTAG 5 switch overview

In some lighting and gaming applications, NTAG 5 switch enables simple and cost-effective designs without a microcontroller. It implements multiplexed pins, offering general-purpose I/O (GPIO) and pulse width modulation (PWM) as well as NFC field detection. The characteristics of the PWM or GPIO signal can be configured through the NFC interface. These features can be used to switch on/off and control motor speed or LED brightness.

Support for ISO/IEC 15693 lets the NTAG 5 switch communicate securely in two ways — with powerful industrial readers, at a range of up to 60 cm and with NFC-enabled devices within proximity range. This duality makes it possible for the device to be calibrated and parameterized automatically while in the factory and then, when put to use in the field, safely communicate with contactless devices such as NFCenabled smartphones.

The tag's 512 bytes of memory can be divided into three areas, and each area can use a different protection level, varying from no protection to 32-/64-bit, password-protected read/write access. Different parties in the value chain can have their own dedicated memory areas for storing access data.

The NTAG 5 switch comes with pre-programmed proof-of-origin functionality to verify authenticity. The elliptic curve cryptography (ECC) based originality signature can be locked or reprogrammed by the customer.

The NTAG 5 is a powerhouse, harvesting the energy from an NFC Reader, it can operate without a battery. Better yet, with its configurable output voltage, it can power a circuit, a sensor network and even charge a super capacitor wireless.

2 Features and benefits

- Reading distance with long-range reader > 60 cm (> 25 inches)
- Flexible operation with PWM/GPIO interface
- Flexible split between three open and/or protected memory areas
- Ensured authenticity of product through value chain
- Interoperable data exchange according to NFC Forum standards
- Energy-efficient design with reduced bill of material
- Interoperable and high performance NFC interface
  - ISO/IEC 15693 and NFC Forum Type 5 Tag compliant
  - 64-bit Unique IDentifier
- Reliable and robust memory
  - 512 bytes (4096 bits) user EEPROM on top of configuration memory
  - 40 years data retention
  - Write endurance of 1 000 000 cycles
- Configurable contact interface
  - One configurable event detection pin
  - Two GPIOs
  - Two Pulse Width Modulation (PWM) channels as multiplexed GPIOs and/or ED pin
  - 1.62 V to 5.5 V supply voltage
- Scalable security for access and data protection
  - Disable NFC interface temporarily
  - NFC PRIVACY mode
  - Read-only protection as defined in NFC Forum Type 5 Tag Specification
  - Full, read-only, or no memory access based on 32-bit password
  - Optional 64-bit password protection
  - ECC-based reprogrammable originality signature
- Low-power budget application support
  - Energy harvesting with configurable output voltage up to 30 mW
  - Low-power standby current typically <6 µA
  - Hard power down current typically <0.25 µA
- Very robust architecture
  - -40 °C to 105 °C for EEPROM read and register access
  - -40 °C to 85 °C for EEPROM write access
- Extensive product support package
  - Feature specific application notes
  - Development board including software and source code
  - Hands-on training

3 Applications

- Use cases
  - Calibration
  - Trimming
  - Authenticity check and data protection
  - Late "in the box" configuration
  - LED driver configuration
  - NFC charging
- Applications
  - Lighting
  - Smart home
  - Hearable and Wearable
  - Consumer
  - Industrial
  - Gaming

4 Ordering information

Table 1. Ordering information

Orderable part number	Package		
	Name	Description	Version
NTP52101G0JHKZ	XQFN16	NTAG 5 switch with GPIOs, PWM and 512 bytes user EEPROM plastic, extremely thin quad flat package; no leads; 16 terminals	SOT1161-2
NTP52101G0JTTZ	TSSOP16	NTAG 5 switch with GPIOs, PWM and 512 bytes user EEPROM plastic, thin shrink small outline package; 16 leads; 0.65 mm pitch; 5 mm x 4.4 mm x 1.1 mm body	SOT403-1
NTP52101G0JTZ	SO8	NTAG 5 switch with GPIOs, PWM and 512 bytes user EEPROM plastic, small outline package; 8 leads; 1.27 mm pitch; 4.9 mm x 3.9 mm x 1.75 mm body	SOT96-1
NTP52101G0FUAV	Wafer	NTAG 5 switch; 8 inch wafer, 150 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format)	-

REMARK: Wafer specification addendum is available after exchange of a non-disclosure agreement (NDA)

5 Marking

Table 2. Marking codes

Type number	Marking code			
	Line A	Line B	Line C	Line D
NTP52101G0JHK	G11	DBSN|ASID	DYWW	-
NTP52101G0JTT	NP52101	DBID|ASID	ZnDYY	WW
NTP52101G0JT	NP52101	DBSN|ASID	nDYWW	-

Used abbreviations:

ASID: Assembly Sequence ID

D: RHF-2006 indicator

DBID: Diffusion Batch ID

DBSN: Diffusion Batch Sequence Number

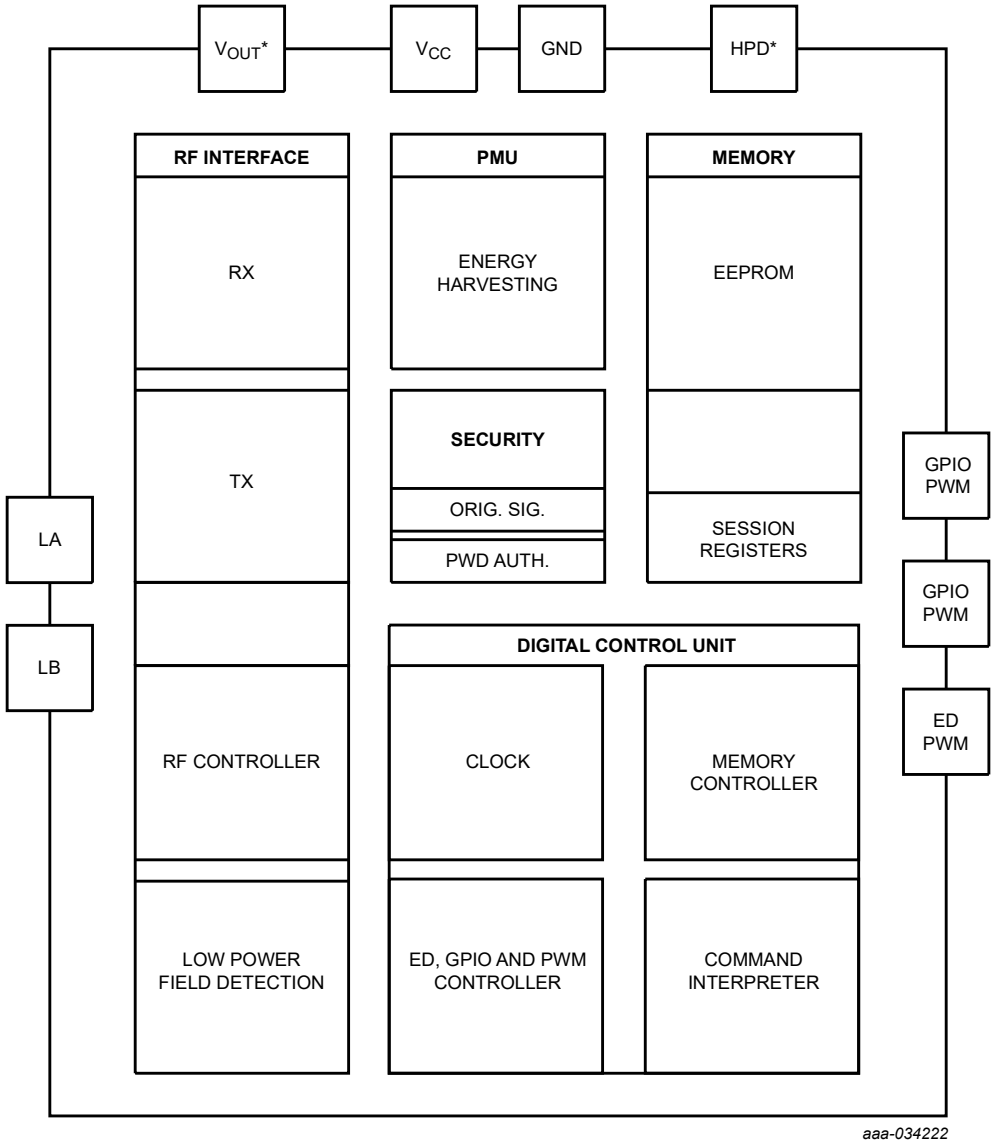
n: Assembly Centre Code

WW: week

Y or YY: year

Z: Diffusion Centre Code

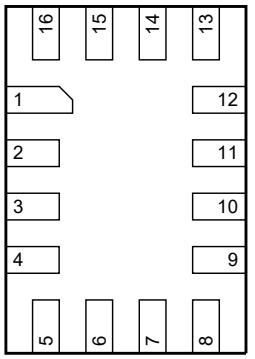
6 Block diagram



* HPD and V_{OUT} are not available for SO8 package

Figure 2. Block diagram NTAG 5 switch

7 Pinning information



Transparent top view

Figure 3. Pin configuration for XQFN16 package

Table 3. Pin description for XQFN16

Pin	Symbol	Description	When unused
1	GND	Ground	connect to GND
2	GND	Ground	connect to GND
3	N.C.	not connected	keep floating
4	N.C.	not connected	keep floating
5	N.C.	not connected	keep floating
6	GPIO1/PWM1	Multiplexed GPIO1 and PWM1	keep floating
7	GPIO0/PWM0	Multiplexed GPIO0 and PWM0	keep floating
8	ED/PWM0	Multiplexed event detection and PWM0	keep floating
9	V_{CC}	External power supply	keep floating
10	HPD	Hard power down	keep floating
11	GND	Ground	connect to GND
12	V_{OUT}	Energy harvesting voltage output	keep floating
13	N.C.	not connected	keep floating
14	LB	Antenna connection	keep floating
15	LA	Antenna connection	keep floating
16	N.C.	not connected	keep floating

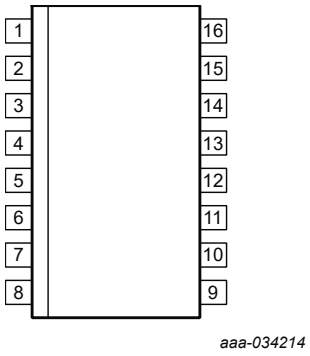


Figure 4. Pin configuration for TSSOP16 package

Table 4. Pin description for TSSOP16

Pin	Symbol	Description	When unused
1	LA	Antenna connection	keep floating
2	N.C.	not connected	keep floating
3	GND	Ground	connect to GND
4	GND	Ground	connect to GND
5	N.C.	not connected	keep floating
6	N.C.	not connected	keep floating
7	N.C.	not connected	keep floating
8	GPIO1/PWM1	Multiplexed GPIO1 and PWM1	keep floating
9	GPIO0/PWM0	Multiplexed GPIO0 and PWM0	keep floating
10	ED/PWM0	Multiplexed event detection and PWM0	keep floating
11	V_{CC}	External power supply	keep floating
12	HPD	Hard power down	keep floating
13	GND	Ground	connect to GND
14	V_{OUT}	Energy harvesting voltage output	keep floating
15	N.C.	not connected	keep floating
16	LB	Antenna connection	keep floating

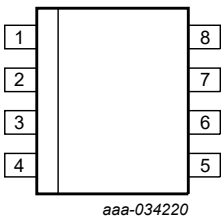


Figure 5. Pin configuration for SO8 package

Table 5. Pin description for SO8

Pin	Symbol	Description	When unused
1	GND	Ground	connect to GND
2	LA	Antenna connection	keep floating
3	LB	Antenna connection	keep floating
4	GND	Ground	connect to GND
5	GPIO1/PWM1	Multiplexed GPIO1 and PWM1	keep floating
6	GPIO0/PWM0	Multiplexed GPIO0 and PWM0	keep floating
7	ED/PWM0	Multiplexed event detection and PWM0	keep floating
8	V_{CC}	External power supply	keep floating

8 Functional description

8.1 Memory Organization

8.1.1 General

The entire memory is divided into three different parts:

- User memory
  - This part of the memory is intended to be used to store user data. It is organized in blocks of 4 bytes each (see Section 8.1.2).
  - According to NFC Forum Type 5 Tag Specification, EEPROM block 0 contains the Capability Container directly followed by the NDEF Message TLV. If NTAG 5 switch is used in a proprietary way, any user data may be stored in the user memory. Direct read/write access with the standard READ BLOCK and WRITE BLOCK commands (see Section 8.2.3.4) to this part of the memory is possible depending on the related security and write protection conditions.
  - 16-bit counter
    The last block of the EEPROM memory contains the 16-bit counter and the counter protection flag (see Section 8.1.2.1).
- Configuration area
  - Within this part of the memory all configuration options are stored (see Section 8.1.3). This memory area can only be accessed with the READ CONFIG (see Section 8.2.3.2.1) or WRITE CONFIG (see Section 8.2.3.2.2) commands.
  - The configuration area contains required security-related information, such as access passwords with related privileges, headers, customer ID (CID), originality signature and many more which will be loaded at power-on reset.
  - Access to configuration blocks may be blocked at all or password protected with related configuration bits.
  - All session registers are accessible in the configuration area as long as not locked by LOCK_SESSION_REG. These configuration items can be changed on the fly and have immediate effect, but get lost after power-on reset.

WARNING: The content of bytes and bits defined as RFU SHALL NOT be changed.

8.1.2 User memory

According to NFC Forum Type 5 Tag Specification, the user accessible EEPROM memory is divided into blocks. A block is the smallest access unit. For NTAG 5 switch, each block consists of 4 bytes (1 block = 32 bits). Bit 0 in each byte represents the least significant bit (lsb) and bit 7 the most significant bit (msb), respectively.

The last block contains the 16-bit counter (see Section 8.1.2.1).

NTAG 5 switch offers 512 bytes (4096 bits) of user memory.

Table 6. User memory organization

Block Address		Byte 0 (LSB)	Byte 1	Byte 2	Byte 3 (MSB)	Description
NFC						
00h		Capability Container				or user memory
01h		User Memory				

Block Address		Byte 0 (LSB)	Byte 1	Byte 2	Byte 3 (MSB)	Description
NFC						
:						
7Eh						
7Fh		C0	C1	00h	PROT	Counter

User data at delivery contains an NFC Forum-compliant capability container and an NDEF message containing the URL www.nxp.com/nfc. First 6 blocks are initialized as illustrated in below table. The counter block is initialized with all 00h. Content of the rest of the user memory is undefined and contains random (rnd) data at delivery.

Table 7. Memory content at delivery

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
00h		E1h	40h	20h	09h
01h		03h	10h	D1h	01h
02h		0Ch	55h	01h	6Eh
03h		78h	70h	2Eh	63h
04h		6Fh	6Dh	2Fh	6Eh
05h		66h	63h	FEh	00h
06h		rnd	rnd	rnd	rnd
...		rnd	rnd	rnd	rnd
7Fh		00h	00h	00h	00h

8.1.2.1 16-bit counter

Last Block of the user memory contains the 16-bit counter. The block can be accessed with the standard read and write commands but special data format is required.

The standard protection conditions for the user memory are not valid for the counter block.

Counter block can only be accessed from NFC perspective.

The 16-bit counter can be

- preset to initial start value protected with the write password
- read
- increased by one, optionally protected with the read password

The counter can be read with an (EXTENDED) READ SINGLE BLOCK to the last block or (EXTENDED) READ MULTIPLE BLOCK command including the last block. The 4 byte data of the counter block provide the following information in Table 8.

Table 8. COUNTER BLOCK data structure

Byte	Name	Value	Description
0	C0 (LSB)	00h - FFh	Counter value
1	C1 (MSB)	00h - FFh	

Byte	Name	Value	Description
2	-	00h	RFU
3	PROT	00h	Incrementing of the counter value is not protected
		01h	Incrementing of the counter value is protected with the read password

The counter can be preset to a start value with an (EXTENDED) WRITE SINGLE BLOCK command to counter block. The counter can only be preset to a start value after a SET PASSWORD command with the write password.

The PROT byte (data byte 3) value defines if the protection to increment the counter is enabled or disabled. If the protection is enabled, the read password is required to increment the counter value.

The data for the (EXTENDED) WRITE SINGLE BLOCK command to preset the counter is defined in Table 9.

Remark: *A Preset counter value of 0x0001 is not possible, a (EXTENDED) WRITE SINGLE BLOCK command with that value will only increment the counter.*

Table 9. Preset counter data structure

Byte	Name	Value	Description
0	C0	00h, 02h - FFh (LSB)	Counter value
1	C1	00h - FFh (MSB)	
2	-	00h	RFU
3	PROT	00h	Disable the protection to increment the counter
		01h	Enable the protection to increment the counter with read password

To increment the counter by one with a (EXTENDED) WRITE SINGLE BLOCK command to counter block. If the protection to increment the counter is enabled, a SET PASSWORD command with the read password is required before.

The data for the (EXTENDED) WRITE SINGLE BLOCK command to increment the counter is defined in Table 10.

Remark: *The counter can only be incremented with the C0 and C1 values defined in Table 10. Other values than that preset the counter if a SET PASSWORD command with the write password or leads to an error message.*

Table 10. Increment counter data structure

Byte	Name	Value	Description
0	C0	01h (LSB)	Value to increment the counter
1	C1	00h (MSB)	
2	-	00h	RFU
3	-	00h	RFU

8.1.3 Configuration memory

The configuration memory contains the security and configuration information. Access to this memory area is only possible with WRITE CONFIG (see Section 8.2.3.2.2) and READ CONFIG (see Section 8.2.3.2.1) commands depending on the initialization status.

Writing to blocks with only RFU bytes is not possible and results in error code 0Fh. Reading complete RFU blocks results in receiving all bytes 00h.

Changing RFU bytes and bits is not allowed and may result in unintended behavior.

Different features can be configured with CONFIG bits. Similar to all other configuration options, the effect does not take place in the current session. The effect takes place after POR. If immediate change is expected, related session register bytes or bits need to be used (see Section 8.1.4).

To which section each block belongs is defined in first column (Sec.). Sections might be locked by setting related bit to 1b (see Section 8.1.3.21).

Table 11. Configuration Memory organization

Sec.	Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
	NFC						
0	00h		ORIGINALITY_SIGNATURE				32 byte Originality Signature (see Section 8.1.3.1)
0	...						
0	07h						
0	08h		CH	RFU			Configuration Header (see Section 8.1.3.2)
0	09h		CID		RFU		Customer ID (see Section 8.1.3.3)
N/A	0Ah		RFU				
N/A	0Bh		RFU				
0	0Ch		RFU	NFC_GCH	RFU		NFC Global Crypto Header (see Section 8.1.3.4)
0	0Dh		RFU	NFC_CCH	RFU		NFC Crypto Configuration Header (see Section 8.1.3.5)
0	0Eh		NFC_AUTH_LIMIT		RFU		NFC Authentication Limit Counter (see Section 8.1.3.6)
N/A	0Fh		RFU				
N/A	...						
N/A	1Fh						
0	20h		NFC_PWD_0				Read Password (see Section 8.1.3.7)
0	21h		NFC_PWD_1				Write Password (see Section 8.1.3.7)

Sec.	Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
	NFC						
0	22h		NFC_PWD_2				Privacy Password (see Section 8.1.3.7)
0	23h		NFC_PWD_3				Destroy Password (see Section 8.1.3.7)
0	24h		NFC_PWD_4				EAS/AFI Password (see Section 8.1.3.7)
0	25h		NFC_PWD_5				Restricted AREA_1 Read Password (see Section 8.1.3.7)
0	26h		NFC_PWD_6				Restricted AREA_1 Write Password (see Section 8.1.3.7)
N/A	27h		RFU				
N/A	...						
N/A	36h						
2	37h		CONFIG				Feature Configuration (see Section 8.1.3.8)
N/A	38h		RFU				
3	39h		PWM_GPIO_CONFIG		RFU		PWM and GPIO Configuration (see Section 8.1.3.9)
3	3Ah		PWM0_ON_OFF				PWM1 Configuration (see Section 8.1.3.10)
3	3Bh		PWM1_ON_OFF				PWM1 Configuration (see Section 8.1.3.10)
N/A	3Ch		RFU				
3	3Dh		EH_CONF	RFU	ED_CONF	RFU	Energy Harvesting (see Section 8.1.3.11) and Event Detection Pin (see Section 8.1.3.12) Configuration
N/A	3Eh		RFU				
3	3Fh		RFU	CONF_ PROT	PP_AREA_1		Configuration Protection (see Section 8.1.3.13) AREA_1 Protection Pointer (see Section 8.1.3.14)
N/A	40h		RFU				

Sec.	Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
	NFC						
N/A	...						
N/A	54h						
4	55h		AFI	RFU			Application Family Identifier (see Section 8.2.3.6.1)
4	56h		DSFID	RFU			DSFID (see Section 8.1.3.16)
4	57h		EAS_ID		RFU		EAS ID (see Section 8.1.3.17)
4	58h		PP_AREA_0H	NFC_PPC	RFU		NFC Protection Pointer (see Section 8.1.3.18) and NFC Protection Pointer Conditions (see Section 8.1.3.19)
N/A	59h		RFU				
N/A	...						
N/A	69h						
5	6Ah		NFC_LOCK_BLOCK		RFU		NFC Lock block configuration (see Section 8.5.1)
5	...						
5	71h						
N/A	72h		RFU				
N/A	...						
N/A	91h						
8	92h		NFC_ SECTION_ LOCK	RFU			NFC section lock bytes (see Table 53)
8	93h						
N/A	94h		RFU				
N/A	...						
N/A	9Fh						

8.1.3.1 Originality Signature

The Originality signature (see Section 8.7) is stored in first 8 blocks (block 00h to block 07h) of configuration memory and may be verified by the NFC device using the corresponding ECC public key. As the NXP originality signature is on default not locked, it may be re-programmed by the customer. If the originality check is not needed, it may even be used as additional 32 byte user EEPROM.

Table 12. 32 Byte Originality Signature

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
00h		SIG0 (LSB)	SIG1	SIG2	SIG3
01h		SIG4	SIG5	SIG6	SIG7
02h		SIG8	SIG9	SIG10	SIG11
03h		SIG12	SIG13	SIG14	SIG15
04h		SIG16	SIG17	SIG18	SIG19
05h		SIG20	SIG21	SIG22	SIG23
06h		SIG24	SIG25	SIG26	SIG27
07h		SIG28	SIG29	SIG30	SIG31 (MSB)

8.1.3.2 Configuration Header

The Configuration Header (CH) byte defines the access conditions of both, Customer ID and Originality Signature.

Table 13. Configuration Header (CH) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
08h		CH	RFU		

Configuration Header byte can be read with READ CONFIG command (see Section 8.2.3.2.1) and written with WRITE CONFIG command (see Section 8.2.3.2.2). Once locked (set to E7h), CH byte cannot be updated anymore and Originality Signature and Customer ID gets locked permanently.

Table 14. Configuration Header Codes

Value	Mode	Write Access
81h	Writeable (default)	Yes
E7h	Locked	No
All others	Invalid	No

8.1.3.3 Customer ID (CID)

The Customer ID at delivery is C000h and can be reprogrammed and locked. It might be used to identify the product.

The two most significant bits (b7 and b6 of CID (MSB)) are always equal to 11b. Only CID[13-0] may be written by customer. Note, that other values of the two most significant bits are RFU.

When the CID is written with WRITE CONFIG command, the 2 most significant bits are always set to 11b. The input CID in WRITE CONFIG command (see Section 8.2.3.2.2) is bit wise ORed with C000h.

Example: When setting CID to 10AAh, resulting customer-specific CID is D0AAh.

Table 15. Customer ID (CID) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
09h		CID (LSB)	CID (MSB)	RFU	

The CID can be permanently locked by setting the Configuration Header to Locked state (see Table 14) using WRITE CONFIG command. Note, that Originality Signature gets locked, too.

8.1.3.4 NFC Global Crypto Header

The NFC Global Crypto Header (NFC_GCH) defines the status and access of the

- NFC passwords

As long as not locked by the RF section lock, the NFC Global Crypto Header can be written with WRITE CONFIG command (see Section 8.2.3.2.2). The programming of NFC Global Crypto Header can be done in only one direction from lower state to higher and it is irreversible.

Once locked (as per table below), GCH cannot be updated anymore.

Table 16. NFC Global Crypto Header (GCH) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
0Ch		RFU	NFC_GCH	RFU	

Table 17. Global Crypto Header Configuration

Value	Status	Description
81h	Writable (default)	The NFC passwords can be read and written with the READ CONFIG and WRITE CONFIG commands.
E7h	Locked	The NFC passwords cannot be read and written with the READ CONFIG and WRITE CONFIG commands.
all others	Invalid	

NOTE: LOCK PASSWORD command is needed to lock NFC passwords permanently (see Section 8.2.3.3.4).

8.1.3.5 NFC Crypto Configuration Header

The value of the NFC Crypto Configuration Header (NFC_CCH) locks the NFC Authentication Limit to the defined value and can only be changed after authentication. NFC_CCH can be written by using the WRITE CONFIGURATION command (see Section 8.2.3.2.2).

Table 18. Crypto Configuration Header (CCH) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
0Dh		RFU	NFC_CCH	RFU	

Table 19. Crypto Configuration Header Values

Value	Mode	Write Access
81h	Unlocked (default)	Authentication limit can be modified.
E7h	Locked	Authentication limit is locked and can only be modified after authenticating with the write password. In 64-bit password mode both, the read and write password are required, depending on the used security level.
All others	Invalid	

8.1.3.6 NFC Authentication Limit Counter

NTAG 5 switch implements the NFC Authentication Limit in counting negative Password Authentication attempts with the SET PASSWORD command, except for the Privacy password. The counter will be reset automatically to zero after a successful authentication.

Table 20. NFC Authentication Limit Counter (NFC_AUTH_LIMIT) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
0Eh		NFC_AUTH_ LIMIT (LSB)	NFC_AUTH_ LIMIT (MSB)	RFU	

Byte 0 of Block 0Eh is LSB and Byte 1 is MSB of the NFC Authentication Limit counter value.

The Authentication limit is enabled with the most significant bit of Byte 1 is set to 1b. The remaining 15 bits of NFC_AUTH_LIMIT are defining the preset value.

T Counter can be written with a WRITE CONFIG command (see Section 8.2.3.2.2) if

- the Crypto Config Header is not set to "Locked" and NFC Global Crypto Header is not set to "Locked", or
- a valid SET_PASSWORD command with the write password has been executed before. In 64-bit password mode, both read and write passwords are required.

Examples:

- 8000h enables and presets the authentication limit to 0, which means the maximum number of authentications (32767) before a preset is required again
- F000h enables and presets the authentication limit to 28672

If the NFC authentication limit counter reaches FFFFh, then SET_PASSWORD command is permanently locked. No further authentication is possible.

Remark: *The absolute maximum authentication limit value is FFFEh before a is required, otherwise the authentication is irreversibly locked (no longer available).*

8.1.3.7 Passwords

The passwords are stored in the configuration memory.

Default password bytes of Privacy and Destroy password are all 0Fh, Read, Write and EAS/AFI password bytes have a default value of all 00h.

The usage of passwords, read and write access to passwords depends upon NFC Global Crypto Header settings.

Table 21. Plain Password location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
NFC						
20h		NFC_PWD0_0 (LSB)	NFC_PWD0_1	NFC_PWD0_2	NFC_PWD0_3 (MSB)	Read Password
21h		NFC_PWD1_0 (LSB)	NFC_PWD1_1	NFC_PWD1_2	NFC_PWD1_3 (MSB)	Write Password
22h		NFC_PWD2_0 (LSB)	NFC_PWD2_1	NFC_PWD2_2	NFC_PWD2_3 (MSB)	Privacy Password
23h		NFC_PWD3_0 (LSB)	NFC_PWD3_1	NFC_PWD3_2	NFC_PWD3_3 (MSB)	Destroy Password
24h		NFC_PWD4_0 (LSB)	NFC_PWD4_1	NFC_PWD4_2	NFC_PWD4_3 (MSB)	EAS/AFI Password
25h		NFC_PWD5_0 (LSB)	NFC_PWD5_1	NFC_PWD5_2	NFC_PWD5_3 (MSB)	AREA_1 Read Password
26h		NFC_PWD6_0 (LSB)	NFC_PWD6_1	NFC_PWD6_2	NFC_PWD6_3 (MSB)	AREA_1 Write Password

8.1.3.8 Configuration

Different features can be configured with CONFIG bits. The effect does not take place in the current session. The effect takes place after POR. All config bits can be read and written.

Table 22. Configuration Bytes Location (CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
37h		CONFIG_0	CONFIG_1	CONFIG_2	RFU

On POR, all CONFIG bits are copied to CONFIG_REG (see Section 8.1.4.2).

Table 23. Configuration Definition (CONFIG_0)

Bit	Name	Value	Description
7	RFU	0b	
6 to 4	RFU	0b	
3	EH_MODE	00b	RFU
		01b	
2		10b	Energy harvesting optimized for low field strength (default)
		11b	Energy harvesting optimized for high field strength
1	LOCK_SESSION_REG	0b	NFC Write access to all session register (default)
		1b	No NFC write access to session registers A3h to A7h
0	AUTO_STANDBY_MODE_EN	0b	Normal Operation Mode (Default)
		1b	IC enters standby mode after boot if there is no RF field present automatically.

Table 24. Configuration Definition (CONFIG_1)

Bit	Name	Value	Description
7	RFU	0b	
6	RFU	0b	
5	HOST_IF	00b	RFU
		01b	RFU
4		10b	GPIO/PWM (default)
		11b	All host interface functionality disabled and pads are in 3-state mode
3 to 0	RFU	0000b	

Table 25. Configuration Definition (CONFIG_2)

Bit	Name	Value	Description
7	GPIO1_IN	00b	Receiver disabled
		01b	Plain input with weak pull-up
6		10b	Plain input
		11b	Plain input with weak pull-down (Default)
5	GPIO0_IN	00b	Receiver disabled (Default)
		01b	Plain input with weak pull-up
4		10b	Plain input
		11b	Plain input with weak pull-down (Default)
3	EXTENDED_COMMANDS_ SUPPORTED	0b	Extended commands are disabled (Default)
		1b	Extended commands are supported
2	LOCK_BLOCK_ COMMAND_SUPPORTED	0b	Lock block commands are disabled
		1b	Lock block commands are supported (Default)
1	GPIO1_SLEW_RATE	0b	Low Speed GPIO
		1b	High Speed GPIO (Default)
0	GPIO0_SLEW_RATE	0b	Low Speed GPIO
		1b	High Speed GPIO (Default)

8.1.3.9 Pulse Width Modulation and GPIO configuration

These configuration bytes define the various configuration bits for GPIO/PWM use case (see Section 8.1.3.8). All features can be configured from NFC perspective. For details refer to Section 8.3.2 and Section 8.3.3.

Table 26. PWM and GPIO Configuration Location (PWM_GPIO_CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
39h		PWM_GPIO_ CONFIG_0	PWM_GPIO_ CONFIG_1	RFU	

Table 27. PWM and GPIO Configuration Definition (PWM_GPIO_CONFIG_0)

Bit	Name	Value	Description
7	GPIO1_OUT_STATUS	0b	Output status on pad is LOW (default)
		1b	Output status on pad is HIGH
6	GPIO0_OUT_STATUS	0b	Output status on pad is LOW (default)
		1b	Output status on pad is HIGH
5 to 4	RFU	00b	
3	GPIO1	0b	Output (Default)
		1b	Input
2	GPIO0	0b	Output (Default)
		1b	Input
1	GPIO1_PWM1	0b	GPIO (Default)
		1b	PWM
0	GPIO0_PWM0	0b	GPIO (Default)
		1b	PWM

Table 28. PWM and GPIO Configuration Definition (PWM_GPIO_CONFIG_1 and PWM_GPIO_CONFIG_1_REG)

Bit	Name	Value	Description
7	PWM1_PRESCALE	00b	Pre-scalar configuration for PWM1 channel (default 00b)
6			
5	PWM0_PRESCALE	00b	Pre-scalar configuration for PWM0 channel (default 00b)
4			
3	PWM1_RESOLUTION_CONF	00b	6-bit resolution (default)
		01b	8-bit resolution
2		10b	10-bit resolution
		11b	12-bit resolution
1	PWM0_RESOLUTION_CONF	00b	6-bit resolution (default)
		01b	8-bit resolution
0		10b	10-bit resolution
		11b	12-bit resolution

8.1.3.10 Pulse Width Modulation duty cycle settings

Details can be found in PWM Mode section (see Section 8.3.3).

Table 29. Pulse Width Modulation Duty Cycle Configuration Location (PWMx_ON and PWMx_OFF)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
3Ah		PWM0_ON (LSB)	PWM0_ON (MSB)	PWM0_OFF (LSB)	PWM0_OFF (MSB)
3Bh		PWM1_ON (LSB)	PWM1_ON (MSB)	PWM1_OFF (LSB)	PWM1_OFF (MSB)

Table 30. Pulse Width Modulation Duty Cycle Session Register Location (PWMx_ON and PWMx_OFF)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
A4h		PWM0_ON_ REG (LSB)	PWM0_ON_ REG (MSB)	PWM0_OFF_REG (LSB)	PWM0_OFF_ REG (MSB)
A5h		PWM1_ON_ REG (LSB)	PWM1_ON_ REG (MSB)	PWM1_OFF_REG (LSB)	PWM1_OFF_ REG (MSB)

Table 31. Pulse Width Modulatin ON time Configuration Definition (PWMx_ON and PWMx_ON_REG)

Bit	Name	Default Value	Description
7 to 4	RFU	all 0b	
3 to 0	PWMx_ON (MSB)	all 0b	coded time PWM channel x output will be asserted HIGH
7 to 0	PWMx_ON (LSB)	all 0b	

Table 32. Pulse Width Modulation OFF time Configuration Definition (PWMx_OFF and PWMx_OFF_REG)

Bit	Name	Default Value	Description
7 to 4	RFU	all 0b	
3 to 0	PWMx_OFF (MSB)	all 0b	coded time PWM channel x output will be asserted LOW
7 to 0	PWMx_OFF (LSB)	all 0b	

PWM on and off times are coded by using maximum 12 bits. To code for example, PWM0_ON as 0123h, PWM0_ON (LSB) is set to 23h, and PWM0_ON (MSB) is set to 01h.

8.1.3.11 Energy harvesting settings

Energy harvesting configuration controls the behavior of the energy harvesting output pin. If DISABLE_POWER_CHECK is 0b and energy harvesting is enabled with EH_ENABLE is 1b, only when the applied field strength is sufficient to generate configured minimum output load current (EH_IOUT_SEL) and voltage (EH_VOUT_SEL), the energy harvesting output is enabled.

If energy harvesting will be enabled during the session with register bits, EH_IOUT_SEL and EH_VOUT_SEL define the needed output power. However, DISABLE_POWER_CHECK and EH_ENABLE bits need to be set to 0b in this case.

Details can be found in energy harvesting section (see Section 8.4).

Table 33. Energy harvesting Configuration Location (EH_CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
3Dh		EH_CONFIG	RFU	ED_CONFIG	RFU

Table 34. Energy harvesting Configuration Value Definition (EH_CONFIG)

Bit	Name	Value	Description
7	RFU		
6	EH_VOUT_I_SEL	000b	>0.4 mA (Default)
		001b	>0.6 mA
		010b	>1.4 mA
5		011b	>2.7 mA
		100b	>4.0 mA
		101b	>6.5 mA
4		110b	>9.0 mA
		111b	>12.5 mA
3	DISABLE_ POWER_CHECK	0b	Only if sufficient power can be harvested, VOUT will be enabled (default)
		1b	Power level will not be checked, VOUT will be enabled immediately after startup
2	EH_VOUT_V_SEL	00b	1.8 V (Default)
		01b	2.4 V
1		10b	3 V
		11b	RFU
0	EH_ENABLE	0b	Energy harvesting disabled (default)
		1b	Energy harvesting enabled

8.1.3.12 Event detection pin configuration settings

Event detection and field detection functionality define the behavior of the active low ED pin depending on various events. As this pin is an open-drain active low implementation, ED pin state ON means that signal is LOW and OFF means that signal is HIGH. More details can be found in ED section (see Section 8.3.1).

Table 35. Event Detection Configuration Location (ED_CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
3Dh		EH_CONFIG	RFU	ED_CONFIG	RFU

Table 36. Event Detection Configuration Register Location (ED_CONFIG_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
A8h		ED_COFIG_REG	RFU		

Table 37. Event Detection Definition (ED_CONFIG and ED_CONFIG_REG)

Bit	Name	Value	ED pin state	Description
7 to 4	RFU	0000b	N/A	
3 to 0	Disable ED	0000b	OFF	Event detection pin disabled (default)
	NFC Field detect	0001b	ON	NFC field present
			OFF	NFC field absent
	PWM	0010b	ON	Pulse width modulation signal during OFF period
			OFF	Pulse width modulation signal during On period
	RFU	0011b	ON	
			OFF	
	RFU	0100b	ON	
			OFF	
	RFU	0101b	ON	
			OFF	
	NDEF Message TLV Length	0110b	ON	Length byte(block 1, byte 1) is not ZERO
			OFF	Length byte (block 1, byte1) is ZERO
	Stand-by mode	0111b	ON	IC is NOT in standby mode
			OFF	IC is in standby mode
	WRITE command indication	1000b	ON	Start of programming cycle during WRITE command
			OFF	Start of response to WRITE command or NFC off
	READ command indication	1001b	ON	Start of read cycle during READ command
			OFF	• End of read access, or • NFC off
	Start of command indication	1010b	ON	Start of (any) command
			OFF	• End of response to command, or • NFC off
	RFU	1011b	ON	
			OFF	
	RFU	1100b	ON	
			OFF	
	Software Interrupt	1101b	ON	1101b written to ED_CONFIG
			OFF	Event needs to be cleared by setting b0 of ED_RESET_REG to 1b

Bit	Name	Value	ED pin state	Description
	RFU	1110b	N/A	
	RFU	1111b	N/A	

Table 38. Event Detection Clear Register Location (ED_INTR_CLEAR_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
ABh		ED_INTR_CLEAR_REG	RFU		

Table 39. Event Detection Clear Register (ED_INTR_CLEAR_REG)

Bit	Name	Value	Description
7 to 1	RFU	all 0b	
0	ED_INTR_CLEAR	1b	write 1b to release ED pin

ED pin is cleared i.e. released when writing 01h to the ED clear register. The bit gets automatically cleared after clearing the ED pin.

8.1.3.13 configuration protection

Access to blocks 37h to 54h of configuration area can be restricted with CONFIG_PROT byte.

Table 40. Configuration Byte location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
3Fh		RFU	CONF_PROT	PP_AREA_1 (LSB)	PP_AREA_1 (MSB)

Table 41. Configuration Protection (CONF_PROT)

Bit	Name	Value	Description
7 to 2	RFU	all 0b	
1	NFC_CONFIG_W	0b	Configuration area is not write protected (Default)
		1b	Configuration area is write protected
0	NFC_CONFIG_R	0b	Configuration area is not read protected (Default)
		1b	Configuration area is read protected

8.1.3.14 Restricted AREA_1 pointer

The AREA_1 Pointer (PP_AREA_1) can be configured by directly writing PP_AREA_1 byte to configuration memory using WRITE CONFIG command (see Section 8.2.3.2.2). The default value is FFFFh.

Table 42. Restricted AREA_1 Pointer location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
3Fh		RFU	CONF_PROT	PP_AREA_1 (LSB)	PP_AREA_1 (MSB)

In below example, NFC protection pointer (PP_AREA_0H) is set to 50h and PP_AREA_1 is set to 0060h, e.g. PP_AREA_1 (LSB) is 60h and PP_AREA_1 (MSB) is 00h.

Table 43. Memory organization example

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
0000h					AREA_0-L
0001h					
0002h					
...	...	...	...	...	
004Fh					
0050h					AREA_0-H
0051h					
...	...	...	...	...	
005Fh					
0060h					AREA_1
0061h					
...	...	...	...	...	
007Eh					
007Fh	C0	C1	00h	PROT	Counter

8.1.3.15 Application Family Identifier

The Application Family Identifier (AFI) represents the type of application targeted by the device and is used to extract from all the ICs present only the ICs meeting the required application criteria.

AFI can be configured using WRITE AFI command (see Section 8.2.3.6.1) or directly writing AFI byte to configuration memory using WRITE CONFIG command (see Section 8.2.3.2.2).

Default value of AFI is 00h.

Table 44. Application Family Identifier (AFI) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
55h		AFI	RFU		

8.1.3.16 Data Storage Format Identifier

The Data Storage Format Identifier may indicate how the data is structured in the VICC memory. If not used, this byte shall be set to 00h, which is the default value.

The Data Storage Format Identifier (DSFID) can be configured using WRITE DSFID command (see Section 8.2.3.6.3) or directly writing DSFID byte to configuration memory using WRITE CONFIG command (see Section 8.2.3.2.2).

Table 45. Data Storage Format Identifier (DSFID) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
56h		DSFID	RFU		

8.1.3.17 Electronic Article Surveillance ID

The Electronic Article Surveillance ID (EAS ID) can be configured using WRITE EAS ID (see Section 8.2.3.6.10) command or directly writing EAS_ID byte to configuration memory using WRITE CONFIG command (see Section 8.2.3.2.2).

Default value of EAS_ID is 0000h.

Table 46. Electronic Article Surveillance ID (EASID) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
57h		EAS_ID (LSB)	EAS_ID (MSB)	RFU	

8.1.3.18 NFC protection pointer

The NFC protection pointer (PP_AREA_0H) can be configured using PROTECT PAGE command (see Section 8.2.3.3.6) or directly writing PP_AREA_0H byte to configuration memory using WRITE CONFIG command (see Section 8.2.3.2.2).

Default value is FFh.

Table 47. NFC Protection Pointer (NFC PP) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
58h		PP_AREA_0H	NFC_PPC	RFU	RFU

In below example, NFC protection pointer is set to 50h. PP_AREA_1 is out side of the EEPROM area in this example.

Table 48. Memory organization example

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
0000h					AREA_0-L
0001h					
0002h					
...	...	...	...	...	
004Fh					
0050h					AREA_0-H
0051h					
...	...	...	...	...	

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
007Eh					
007Fh	C0	C1	00h	PROT	Counter

8.1.3.19 NFC Protection Pointer Conditions

The NFC Protection Pointer Conditions (NFC PPC) can be configured using PROTECT PAGE command (see Section 8.2.3.3.6) or directly writing NFC_PPC byte to configuration memory using WRITE CONFIG command (see Section 8.2.3.2.2) as defined in table below.

Table 49. NFC Protection Pointer Conditions (NFC_PPC) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
58h		PP_AREA_0H	NFC_PPC	RFU	RFU

Table 50. NFC Protection Pointer Configuration (NFC_PPC)

Bit	Name	Value	Description
7	RFU	0b	
6	RFU	0b	
5	Write AREA_0_H	0b	AREA_0-H is not write protected (Default)
		1b	AREA_0-H is write protected
4	Read AREA_0_H	0b	AREA_0-H is not read protected (Default)
		1b	AREA_0-H is read protected
3	RFU	0b	
2	RFU	0b	
1	Write AREA_0_L	0b	AREA_0-L is not write protected (Default)
		1b	AREA_0-L is write protected
0	Read AREA_0_L	0b	AREA_0-L is not read protected (Default)
		1b	AREA_0-L is read protected

8.1.3.20 NFC lock bytes

User blocks can be blocked from writing by the NFC interface. These bits are one time programmable. Once written to 1b, they cannot be changed back to 0b. Each bit locks one block of user memory area (e.g., bit 0 of byte 0 locks block 0).These bytes can be written by NFC. The access to these bytes for the particular interface can be restricted by configuring the device SECTION_LOCK (see Table 52).

Table 51. NFC Lock Block Configuration location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
6Ah		NFC_LOCK_BL00	NFC_LOCK_BL01	RFU	RFU
...		...	...	RFU	RFU

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
71h		NFC_LOCK_BL14	NFC_LOCK_BL15	RFU	RFU

8.1.3.21 Device configuration section lock bytes

Lock bits are provided to lock different sections of the configuration area. 16 bits are provided to define access conditions for different sections of the configuration area.

First column in the configuration memory table (see Table 11) defines the affiliated blocks of each section.

Table 52. Device configuration section lock bytes location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
92h		NFC_LOCK_0	RFU		
93h		NFC_LOCK_1	RFU		

These section lock configurations are provided to allow customer to initialize NTAG 5 switch during customer configuration from NFC interface. After the configuration is done, it is recommended to write the appropriate lock conditions and lock the device configuration bytes.

These lock bytes take the highest priority above all locks. Different section access conditions have to be chosen appropriately, so that the other interface does not change and corrupt the other interface security configuration.

If NFC_LOCK_0 bits are set to 1b, then the lock bytes cannot be updated and gets locked permanently.

Table 53. NFC configuration section lock byte 0 definition (NFC_SECTION_LOCK_0)

Bit	Name	Value	Description
7	Section 7	0b	Section 7 is writable
		1b	Section 7 is not writable
6	Section 6	0b	Section 6 is writable
		1b	Section 6 is not writable
5	Section 5	0b	Section 5 is writable
		1b	Section 5 is not writable
4	Section 4	0b	Section 4 is writable
		1b	Section 4 is not writable
3	Section 3	0b	Section 3 is writable
		1b	Section 3 is not writable
2	Section 2	0b	Section 2 is writable
		1b	Section 2 is not writable
1	Section 1	0b	Section 1 is writable
		1b	Section 1 is not writable
0	Section 0	0b	Section 0 is writable

Bit	Name	Value	Description
		1b	Section 0 is not writable

Table 54. NFC configuration section lock Byte 1 definition (NFC_SECTION_LOCK_1)

Bit	Name	Value	Description
7	Section 8	0b	Section 8 is writable
		1b	Section 8 is not writeable
6	Section 6	0b	Section 6 is readable
		1b	Section 6 is not readable
5	Section 5	0b	Section 5 is readable
		1b	Section 5 is not readable
4	Section 4	0b	Section 4 is readable
		1b	Section 4 is not readable
3	Section 3	0b	Section 3 is readable
		1b	Section 3 is not readable
2	Section 2	0b	Section 2 is readable
		1b	Section 2 is not readable
1	Section 1	0b	Section 1 is readable
		1b	Section 1 is not readable
0	Section 0	0b	Section 0 is readable
		1b	Section 0 is not readable

Note: Section 8 (Device configuration lock bytes) is always readable.

In case of not readable and/or not writeable, IC responds with an error from NFC perspective, when trying to access locked sections.

8.1.4 Session registers

After POR, the content of the configuration settings (see Section 8.1.3) is loaded into the session register. The values of session registers can be changed during a session. Change to session registers take effect immediately, but only for the current communication session. After POR, the session registers values will again contain the configuration register values as before.

To change the default behavior, changes to the related configuration bytes are needed, but the related effect will only be visible after the next POR.

Session registers starting from block A3h until the end may be write protected with LOCK_REGISTER bit.

Most of the parameters are defined in the configuration memory section.

Table 55. Session Register Location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Remark
NFC						
A0h		STATUS_REG		RFU		Status Register (see Section 8.1.4.1)
A1h		CONFIG_REG				Configuration (see Section 8.1.4.2)
A2h		RFU				
A3h		PWM_GPIO_CONFIG_REG		RFU		PWM and GPIO Configuration(see Section 8.1.4.3)
A4h		PWM0_ON_OFF_REG				PWM1 Configuration (see Section 8.1.4.4)
A5h		PWM1_ON_OFF_REG				PWM1 Configuration (see Section 8.1.4.4)
A6h		RFU				
A7h		EH_CONFIG_REG	RFU			Energy Harvesting Configuration (see Section 8.1.4.5)
A8h		ED_CONFIG_REG	RFU			Event detection functionality (see Section 8.1.4.6)
A9h		RFU				
AAh		RESET_ GEN_REG	RFU			Reset Register (see Section 8.1.4.7)
ABh		ED_INTR_ CLEAR_REG	RFU			Clear Event Detection (see Section 8.1.4.8)
ACh		RFU				
ADh		RFU				
AEh		RFU				
AFh		RFU				

8.1.4.1 Status register

Different status of NTAG 5 switch can be known by reading status register. The status register can be read by READ_CONFG.

Some of the registers may be cleared. Setting status bits to 1b is not possible at all.

Table 56. Status Register Location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
A0h		STATUS0_REG	STATUS1_REG	RFU	

Table 57. Status 0 Register

Bit	Name	Access		Value	Description
		NFC			
7	EEPROM_WR_BUSY	R		0b	EEPROM is not busy
				1b	EEPROM is busy (programming cycle ongoing)
6	EEPROM_WR_ERROR	R/W		0b	all data written successfully
				1b	EEPROM write error happened. This bit needs to be cleared.
5 to 2	RFU	R		0000b	
1	VCC_SUPPLY_OK	R		0b	VCC supply not present
				1b	VCC supply available
0	NFC_FIELD_OK	R		0b	No NFC field present
				1b	NFC field present

Table 58. Status 1 Register

Bit	Name	Access		Value	Description
		NFC			
7	VCC_BOOT_OK	R		0b	VCC boot not done
				1b	VCC boot done
6	NFC_BOOT_OK	R		0b	NFC boot not done
				1b	NFC boot done
5	RFU	R		0b	
				1b	
4	GPIO1_IN_STATUS	R		0b	GPIO_1 input is LOW
				1b	GPIO_1 input is HIGH
3	GPIO0_IN_STATUS	R		0b	GPIO_0 input is LOW
				1b	GPIO_0 input is HIGH
2 to 0	RFU	R		000b	

8.1.4.2 Configuration register

On POR all CONFIG bits (see Section 8.1.3.8) are copied to CONFIG_REG. Some of these features may be changed with CONFIG_REG bits during a session. These features are valid at once. Most of them are just read only from NFC.

Table 59. Configuration Register Location (CONFIG_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
A1h		CONFIG_0_REG	RFU	CONFIG_2_REG	RFU

Table 60. Configuration Definition (CONFIG_0_REG)

Bit	Name	Access		Value	Description
		NFC			
7	RFU	R		0b	
6	RFU	R		0b	
5	RFU	R		0b	
4	RFU	R		0b	
3	RFU	R		0b	
2	RFU	R		0b	
1	RFU	R		0b	
0	AUTO_STANDBY_MODE_EN	R		0b	Normal Operation Mode
				1b	IC enters standby mode after boot if there is no RF field present automatically.

Table 61. Configuration Definition (CONFIG_2_REG)

Bit	Name	Access		Value	Description
		NFC acc.			
7	GPIO1_IN	R		00b	Receiver disabled
				01b	Plain input with weak pull-up
6				10b	Plain input
				11b	Plain input with weak pull-down
5	GPIO0_IN	R		00b	Receiver disabled
				01b	Plain input with weak pull-up
4				10b	Plain input
				11b	Plain input with weak pull-down
3	EXTENDED_COMMANDS_SUPPORTED	R		0b	Extended commands are disabled
				1b	Extended commands are supported
2	LOCK_BLOCK_COMMAND_SUPPORTED	R		0b	Lock block commands are disabled
				1b	Lock block commands are supported
1	GPIO1_SLEW_RATE	R		0b	Low-Speed GPIO
				1b	High-Speed GPIO
0	GPIO0_SLEW_RATE	R		0b	Low-Speed GPIO
				1b	High-Speed GPIO

8.1.4.3 Pulse Width Modulation and GPIO configuration register

These session register bytes define the various configurations for GPIO/PWM use case (see Section 8.1.3.8). IN_STATUS bits are read only, all others maybe changed during a session. For details refer to Section 8.3.2 and Section 8.3.3.

Table 62. PWM and GPIO Configuration Register Location (PWM_GPIO_CONFIG_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
A3h		PWM_GPIO_CONFIG_0_REG	PWM_CONFIG_1_REG	RFU	

Table 63. PWM and GPIO Configuration Register Definition (PWM_GPIO_CONFIG_0_REG)

Bit	Name	Access		Value	Description
		NFC acc.			
7	GPIO1_OUT_STATUS	R/W		0b	Output status on pad is LOW
				1b	Output status on pad is HIGH
6	GPIO0_OUT_STATUS	R/W		0b	Output status on pad is LOW
				1b	Output status on pad is HIGH
5	GPIO1_IN_STATUS	R		0b	Input status
				1b	
4	GPIO0_IN_STATUS	R		0b	Input status
				1b	
3	GPIO1	R/W		0b	Output
				1b	Input
2	GPIO0	R/W		0b	Output
				1b	Input
1	GPIO1_PWM1	R/W		0b	GPIO
				1b	PWM
0	GPIO0_PWM0	R/W		0b	GPIO
				1b	PWM

Table 64. PWM and GPIO Configuration Register Definition (PWM_GPIO_CONFIG_1_REG)

Bit	Name	Access		Value	Description
		NFC Acc.			
7	PWM1_PRESCALE	R/W		00b	Pre-scalar configuration for PWM1 channel
6					
5	PWM0_PRESCALE	R/W		00b	Pre-scalar configuration for PWM0 channel

Bit	Name	Access		Value	Description
		NFC Acc.			
4					
3	PWM1_RESOLUTION_CONF	R/W		00b	6-bit resolution
				01b	8-bit resolution
2				10b	10-bit resolution
				11b	12-bit resolution
1	PWM0_RESOLUTION_CONF	R/W		00b	6-bit resolution
				01b	8-bit resolution
0				10b	10-bit resolution
				11b	12-bit resolution

8.1.4.4 Pulse Width Modulation duty cycle register

The PWM duty cycle maybe changed during one session from NFC perspective (see Section 8.1.3.10).

8.1.4.5 Energy harvesting register

Energy harvesting registers may be used to enable energy harvesting during one NFC session. In this case, EH_ENABLE bit of EH_CONFIG byte in block 3Dh is set to 0b. Required EH_VOUT_I_SEL and EH_VOUT_V_SEL need to be set in that EH_CONFIG byte. Desired energy harvesting mode (EH_MODE) needs to be configured in CONFIG_0 byte of block 37h. In case of energy harvesting is enabled already during boot (EH_ENABLE bit of EH_CONFIG is 1b), or energy harvesting is not used at all, this register byte gives no information.

Setting EH_TRIGGER to 1b is needed to trigger power detection.

Polling for bit EH_LOAD_OK should be used to check, if sufficient energy is available. Only if EH_LOAD_OK = 1b, energy harvesting may be enabled via session registers by writing 09h to this byte.

Details can be found in energy harvesting section (see Section 8.4).

Table 65. Energy Harvesting Configuration Register Location (EH_CONFIG_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
A7h		EH_COFIG_REG	RFU		

Table 66. Energy Harvesting Register Value Definition EH_CONFIG_REG)

Bit	Name	Access		Value	Description
		NFC Acc.			
7	EH_LOAD_OK	R		0b	Field is not sufficient to provied configured power on V_{OUT}. Do not enable energy harvesting.
				1b	Minimum desired energy available. V_{OUT} may be enabled. As soon as EH_ENABLE is set to 1b, this bit gets cleared automatically.
6 to 4	RFU	R			
3	EH_TRIGGER	R/W		0b	When reading, this byte this bit is RFU and the value is undefined and may be 0b or 1b.
				1b	When writing to this byte, this bit needs to be set to 1b always
2 to 1	RFU	R			
0	EH_ENABLE	R/W		0b	Energy Harvesting disabled (default)
				1b	Energy Harvesting enabled

8.1.4.6 Event detection register

Event detection and field detection functionality define the behavior of the ED pin depending on various events. Indicated event may be changed during one session. More details can be found in ED section (see Section 8.3.1).

8.1.4.7 System reset generation

System reset can be generated by writing to RESET_GEN_REG register using WRITE CONFIG command (see Section 8.2.3.2.2). Writing E7h will trigger the system reset. This byte gets automatically reset after the system reset.

Table 67. RESET_GEN_REG location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
AAh		RESET_GEN_REG	RFU		

8.1.4.8 Clear event detection register

Event detection pin is cleared i.e. released when writing 01h to the Clear Event Detection Register. The bit gets cleared after releasing the ED pin automatically. Other values are RFU.

Table 68. ED_INTR_CLEAR_REG location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
ABh		ED_INTR_ CLEAR_REG	RFU		

8.2 NFC interface

The definition of the NFC interface is according to the ISO/IEC 15693 and NFC Forum Type 5 Tag. The details of passive communication mode are described in Section 8.2.1.

8.2.1 Passive communication mode

Main uses cases for passive communication mode are Smart Metering, Home automation and in the box configuration. With antenna sizes of Class 4 or bigger, energy harvesting on the one side and long-distance read/write access to the EEPROM is possible in a very efficient way.

8.2.2 State diagram and state transitions

The state diagram illustrates the different states and state transitions of NTAG 5 switch.

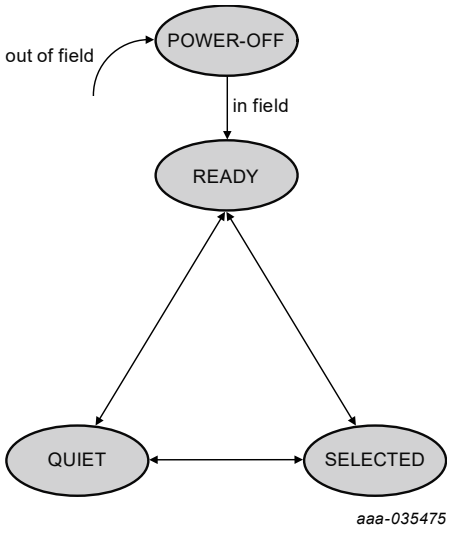


Figure 6. State Machine and State Transitions

8.2.2.1 POWER-OFF state

8.2.2.1.1 State transitions from and to POWER-OFF state

If NFC field is switched off or below, H_{MIN} NTAG 5 switch goes to POWER-OFF state.

POWER-OFF state will be left to READY state no later than 1 ms after NTAG 5 switch is powered by an NFC field greater than H_{MIN}.

NOTE: When loading default data to mirrored SRAM, start-up time, dependent on the pre-loaded bytes, might be greater than 1 ms.

8.2.2.2 READY state

8.2.2.2.1 Transitions between READY and SELECTED state

Transition from READY to SELECTED state is done when

- receiving a SELECT command with a matching UID

8.2.2.2.2 Transitions between READY and QUIET state

Transition from READY to QUIET state is done when

- receiving a STAY QUIET command with a matching UID
- receiving a (FAST) INVENTORY READ command (extended mode) with Quiet_Flag set

8.2.2.2.3 Commands which stay in READY state

NTAG 5 switch stays in READY state when

- receiving any other command where Select_Flag is not set

8.2.2.3 SELECTED state

8.2.2.3.1 Transitions between SELECTED and READY state

Transition from SELECTED to READY state is done by

- receiving a RESET TO READY command where Select_Flag is set
- receiving a SELECT command with a different UID

8.2.2.3.2 Transitions between SELECTED and QUIET state

Transition from SELECTED to QUIET state is done when

- receiving a STAY QUIET command with a matching UID

8.2.2.3.3 Commands which stay in SELECTED state

NTAG 5 switch stays in SELECTED state when

- receiving any other command where Select_Flag is set

8.2.2.4 QUIET state

8.2.2.4.1 Transitions between QUIET and READY state

Transition from QUIET to READY state is done by

- receiving a RESET_TO_READY command

8.2.2.4.2 Transitions between QUIET and SELECTED state

Transition from QUIET to SELECTED state is done by

- receiving a SELECT command with a matching UID

8.2.2.4.3 Commands which stay in QUIET state

NTAG 5 switch stays in QUIET state when

- receiving any other command where Addressed_Flag is set AND Inventory_Flag is not set

8.2.3 Command set

ISO/IEC 15693 mandatory commands are

- INVENTORY
- STAY QUIET

NFC Forum Type 5 Tag mandatory commands are

- READ SINGLE BLOCK
- WRITE SINGLE BLOCK
- LOCK SINGLE BLOCK

On top of those, all optional commands of ISO/IEC 15693 are implemented. Several customer-specific commands are implemented to, e.g., improve overall transaction time. These custom commands all use NXP manufacturer code 04h.

A complete list of all supported commands is given in below table.

Table 69. NFC command set supported by NTAG 5 switch

Code	ISO/IEC 15693	NFC Forum T5T	Command name
01h	Mandatory	Mandatory	INVENTORY (see ISO/IEC 15693 and Digital Protocol)
02h	Mandatory	Mandatory	STAY QUIET (see ISO/IEC 15693) and Type 5 Tag - SLPV_REQ)
20h	Optional	Mandatory	READ SINGLE BLOCK (see ISO/IEC 15693 and Type 5 Tag - READ_SINGLE_BLOCK_REQ)
21h	Optional	Mandatory in READ/WRITE state	WRITE SINGLE BLOCK (see ISO/IEC 15693 and Type 5 Tag - WRITE_SINGLE_BLOCK_REQ)
22h	Optional	Optional	LOCK BLOCK (see ISO/IEC 15693 and Type 5 Tag - LOCK_SINGLE_BLOCK_REQ)
23h	Optional	Optional	READ MULTIPLE BLOCKS (ISO/IEC 15693 and Type 5 Tag - READ_MULTIPLE_BLOCK_REQ)
25h	Optional	Optional	SELECT (see ISO/IEC 15693 and Type 5 Tag - SELECT_REQ)
26h	Optional	Not defined	RESET TO READY (see ISO/IEC 15693)
27h	Optional	Not defined	WRITE AFI (see ISO/IEC 15693)
28h	Optional	Not defined	LOCK AFI (see ISO/IEC 15693)
29h	Optional	Not defined	WRITE DSFID (see ISO/IEC 15693)
2Ah	Optional	Not defined	LOCK DSFID (see ISO/IEC 15693)
2Bh	Optional	Not defined	GET SYSTEM INFORMATION (see ISO/IEC 15693)
2Ch	Optional	Not defined	GET MULTIPLE BLOCK SECURITY STATUS (see ISO/IEC 15693)
2Dh	Optional	Not defined	FAST READ MULTIPLE BLOCKS (see ISO/IEC 15693)
3Bh	Optional	Not defined	EXTENDED GET SYSTEM INFORMATION (see ISO/IEC 15693)
3Ch	Optional	Not defined	EXTENDED GET MULTIPLE BLOCK SECURITY STATUS (see ISO/IEC 15693)
3Dh	Optional	Not defined	FAST EXTENDED READ MULTIPLE BLOCKS (see ISO/IEC 15693)
A0h	Custom	Not defined	INVENTORY READ (see Section 8.2.3.4.1)
A1h	Custom	Not defined	FAST INVENTORY READ (see Section 8.2.3.4.2)
A2h	Custom	Not defined	SET EAS (see Section 8.2.3.6.5)

Code	ISO/IEC 15693	NFC Forum T5T	Command name
A3h	Custom	Not defined	RESET EAS (see Section 8.2.3.6.6)
A4h	Custom	Not defined	LOCK EAS (see Section 8.2.3.6.7)
A5h	Custom	Not defined	EAS ALARM (see Section 8.2.3.6.8)
A6h	Custom	Not defined	PROTECT EAS/AFI (see Section 8.2.3.6.9)
A7h	Custom	Not defined	WRITE EAS ID (see Section 8.2.3.6.10)
ABh	Custom	Not defined	GET NXP SYSTEM INFORMATION (see Section 8.2.3.6.14)
B2h	Custom	Not defined	GET RANDOM NUMBER (see Section 8.2.3.3.1)
B3h	Custom	Not defined	SET PASSWORD (see Section 8.2.3.3.2)
B3h	Custom	Not defined	DISABLE NFC PRIVACY (see Section 8.2.3.3.10)
B4h	Custom	Not defined	WRITE PASSWORD (see Section 8.2.3.3.3)
B5h	Custom	Not defined	LOCK PASSWORD (see Section 8.2.3.3.4)
B6h	Custom	Not defined	PROTECT PAGE (see Section 8.2.3.3.6)
B7h	Custom	Not defined	LOCK PAGE PROTECTION CONDITION (see Section 8.2.3.3.7)
B9h	Custom	Not defined	DESTROY (see Section 8.2.3.3.8)
BAh	Custom	Not defined	ENABLE NFC PRIVACY (see Section 8.2.3.3.9)
BBh	Custom	Not defined	64 BIT PASSWORD PROTECTION (see Section 8.2.3.3.5)
BDh	Custom	Not defined	READ SIGNATURE (see Section 8.2.3.5.1)
C0h	Custom	Not defined	READ CONFIGURATION (see Section 8.2.3.2.1)
C1h	Custom	Not defined	WRITE CONFIGURATION (see Section 8.2.3.2.2)

All command/responses are sent/received in the request/response format as defined in ISO/IEC 15693 and NFC Forum Type 5 Tag specification.

8.2.3.1 Commands for state transitions

Following commands are implemented for all possible state transitions according to ISO/IEC 15693.

- INVENTORY
- STAY QUIET
- SELECT
- RESET TO READY

On top of these commands, NTAG 5 switch offers

- INVENTORY READ in extended mode (see Section 8.2.3.4.1)
- FAST INVENTORY READ in extended mode (see Section 8.2.3.4.2)

8.2.3.2 Configuration operations

8.2.3.2.1 READ CONFIGURATION

Command code = C0h

The READ CONFIG command returns configuration memory content starting with the first block defined by the Block Address and reads Number of Blocks + 1 configuration blocks.

Access to the configuration blocks depends on the status and definition of the related block within the configuration memory (see Section 8.1.3).

If one of the requested configuration blocks is not accessible due to the actual status, NTAG 5 switch will respond with Error_flag set.

A READ CONFIG command can read one or multiple blocks of the following areas of the configuration memory within one command execution:

- Block 00h to block 17h
- rest of configuration memory

Only Option_flag = 0b is supported.

Table 70. READ CONFIG request format

Flags	READ CONFIG	Manuf. code	UID	Block Address	Number of Blocks	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits	8 bits	16 bits

Table 71. READ CONFIG response format when Error_flag is NOT set

Flags	Data	CRC16
8 bits	(Number of blocks + 1) times 32 bits	16 bits

Table 72. READ CONFIGURATION response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.2.2 WRITE CONFIGURATION

Command code = C1h

The WRITE CONFIG command writes the 4 byte data to the requested block address of the configuration memory.

Access to the configuration blocks depends on the status and definition of the related block within the configuration memory (see Section 8.1.3).

If the requested configuration block is not write accessible due to the actual status, NTAG 5 switch will respond with Error_flag set.

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 73. WRITE CONFIG request format

Flags	WRITE CONFIG	Manuf. code	UID	Block Address	Data	CRC16
8 bits	8 bits	8 bits	64 (optional)	8 bits	32 bits	16 bits

Table 74. WRITE CONFIG response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 75. WRITE CONFIG response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.3 PWD Authentication

NTAG 5 switch can be configured to be used for plain password authentication.

8.2.3.3.1 GET RANDOM NUMBER

Command code = B2h

The GET RANDOM NUMBER command is required to receive a 16-bit random number. The passwords that will be transmitted with the SET PASSWORD, ENABLE/DISABLE NFC PRIVACY and DESTROY commands have to be calculated with the password and the random number (see Section 8.2.3.3.2).

Table 76. GET RANDOM NUMBER request format

Flags	GET RANDOM NUMBER	Manuf. code	UID	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits

Table 77. GET RANDOM NUMBER response format when Error_flag is NOT set

Flags	Random_Number	CRC16
8 bits	16 bits	16 bits

Table 78. GET RANDOM NUMBER response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.3.2 SET PASSWORD

Command code = B3h

The SET PASSWORD command enables the different passwords to be transmitted to the IC to access the different protected functionalities of the following commands. The

SET PASSWORD command has to be executed just once for the related password if the IC is powered.

Remark: *The SET PASSWORD command can only be executed in addressed or selected mode and the timing of the SET PASSWORD command is write alike.*

The XOR password has to be calculated with the password and two times the received random number from the last GET RANDOM NUMBER command:

XOR_Password[31:0] = Password[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}.

The different passwords are addressed with the password identifier.

Only Option_flag = 0b is supported.

Table 79. SET PASSWORD request format

Flags	SET PASSWORD	Manuf. code	UID	Password identifier	XOR password	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits	32 bits	16 bits

Table 80. Password Identifier

Password Identifier	Password
01h	Read
02h	Write
04h	see Section 8.2.3.3.10
08h	Destroy
10h	EAS/AFI
40h	Read from AREA_1
80h	Write to AREA_1

Table 81. SET PASSWORD response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 82. SET PASSWORD response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

Remark: *If the IC receives an invalid password, it will not execute any following command until a Power-On Reset (POR) (NFC reset) is executed.*

8.2.3.3.3 WRITE PASSWORD

Command code = B4h

The WRITE PASSWORD command enables a new password to be written into the related memory if the related old password has already been transmitted with a SET PASSWORD command and the addressed password is not locked (see Section 8.2.3.3.4).

Remark: *The WRITE PASSWORD command can only be executed in addressed or SELECTED mode. The new password takes effect immediately which means that the new password has to be transmitted with the SET PASSWORD command to access protected blocks/pages.*

The different passwords are addressed with the password identifier as defined in Table 80.

The timing of the command is write-alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 83. WRITE PASSWORD request format

Flags	WRITE PASSWORD	Manuf. code	UID	Password identifier	Password	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits	32 bits	16 bits

Table 84. WRITE PASSWORD response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 85. WRITE PASSWORD response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.3.4 LOCK PASSWORD

Command code = B5h

The LOCK PASSWORD command enables the addressed password to be locked if the related password has already been transmitted with a SET PASSWORD command. A locked password cannot be changed.

The different passwords are addressed with the password identifier (see Table 80).

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 86. LOCK PASSWORD request format

Flags	LOCK PASSWORD	Manuf. code	UID	Password identifier	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits	16 bits

Table 87. LOCK PASSWORD response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 88. LOCK PASSWORD response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.3.5 64 BIT PASSWORD PROTECTION

Command code = BBh

The 64-bit PASSWORD PROTECTION command enables NTAG 5 switch to be instructed that both, Read and Write passwords are required to get access to password protected blocks. This mode can be enabled if the Read and Write passwords have been transmitted first with a SET PASSWORD command.

If the 64-bit password protection is enabled, both passwords are required for read & write access to protected blocks.

Once the 64-bit password protection is enabled, a change back to 32-bit password protection (read and write password) is not possible.

Remark: *A retransmission of the passwords is not required after the execution of the 64-bit PASSWORD PROTECTION command.*

Remark: *The 64-bit PASSWORD PROTECTION does not include the 16-bit counter block.*

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 89. 64 BIT PASSWORD PROTECTION request format

Flags	64 BIT PASSWORD PROTECTION	Manuf. code	UID	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits

Table 90. 64 BIT PASSWORD PROTECTION response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 91. 64 BIT PASSWORD PROTECTION response format when Error_flag is NOT set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.3.6 PROTECT PAGE

Command code = B6h

The PROTECT PAGE command defines the protection pointer address of the user memory to divide the user memory into two arbitrarily sized pages and defines the access conditions for the two pages.

The protection pointer address defines the base address of the higher user memory segment Page 0-H. All block addresses smaller than the protection pointer address are in the user memory segment Page 0-L.

Table below shows an example of the user memory segmentation with the protection pointer address PP_AREA_0H 14h.

Remark: *In the example below PP_AREA_1 is pointing outside the user memory.*

Table 92. Memory organization

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
00h					Page 0-L
01h					
02h					
:	:	:	:	:	
12h					
13h					
14h					Page 0-H
15h					
:	:	:	:	:	
7Fh	C0	C1	00	Protection	Counter

Remark: *If the protection pointer address is set to block 0, the entire user memory is defined as Page 0-H.*

The access conditions and the protection pointer address can be changed under the following circumstances for plain password mode:

- The related passwords (Read and Write password) have been transmitted first with the SET PASSWORD command.
- The page protection condition is not locked (see Section 8.2.3.3.7)

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 93. PROTECT PAGE request format

Flags	PROTECT PAGE	Manuf. code	UID	Protection pointer address	Extended protection status	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits	8 bits	16 bits

Remark: *The IC only accepts protection pointer address values from 00h to 7Eh. The block containing the 16-bit counter is excluded from the standard user memory protection scheme.*

Table 94. Extended Protection status byte

Bit	Name	Value	Description
7	RFU	0b	
6	RFU	0b	
5	WH	0b	Page 0-H is not write protected
		1b	Page 0-H is write protected
4	RH	0b	Page 0-H is not read protected
		1b	Page 0-H is read protected
3	RFU	0b	
2	RFU	0b	
1	WL	0b	Page 0-L is not write protected
		1b	Page 0-L is write protected
0	RL	0b	Page 0-L is not read protected
		1b	Page 0-L is read protected

Table 95. Protection status bits definition

WH/WL	RH/RL	32-bit Protection	64-bit Protection
0b	0b	Public	Public
0b	1b	Read and Write protected by the Read password	Read and Write protected by the Read plus Write password
1b	0b	Write protected by the Write password	Write protected by the Read plus Write password
1b	1b	Read protected by the Read password and Write protected by the Read and Write password	Read and Write protected by the Read plus Write password

Table 96. PROTECT PAGE response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 97. PROTECT PAGE response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

The information about the stored settings of the protection pointer address and access conditions can be read with the GET NXP SYSTEM INFORMATION command (see Section 8.2.3.6.14).

8.2.3.3.7 LOCK PAGE PROTECTION CONDITION

Command code = B7h

The LOCK PAGE PROTECTION CONDITON command locks the protection pointer address and the status of the page protection conditions.

The LOCK PAGE PROTECTION CONDITON command can be successfully executed under the following circumstances:

- The Read and Write passwords have been transmitted with the SET PASSWORD command.

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 98. LOCK PAGE PROTECTION CONDITION request format

Flags	LOCK PAGE PROTECTION CONDITION	Manuf. code	UID	Protection pointer address	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits	16 bits

Table 99. LOCK PAGE PROTECTION CONDITION response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 100. LOCK PAGE PROTECTION CONDITION response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

Remark: *If the transmitted protection pointer address does not match with the stored address the IC will respond according to the error handling.*

8.2.3.3.8 DESTROY

Command code = B9h

T DESTROY command disables NTAG 5 switch if the destroy password is correct. This command is irreversible and NTAG 5 switch will never respond to any command again.

The DESTROY command can only be executed in addressed or SELECTED mode.

The XOR password has to be calculated with the password and two times the received random number from the last GET RANDOM NUMBER command:

XOR_Password[31:0] = Password[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}.

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 101. DESTROY request format

Flags	DESTROY	Manuf. code	UID	XOR password	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits	16 bits

Table 102. DESTROY response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 103. DESTROY response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.3.9 ENABLE NFC PRIVACY

Command code = BAh

The ENABLE NFC PRIVACY command enables NFC PRIVACY mode (see Section 8.6) for NTAG 5 switch if the Privacy password is correct.

The XOR password has to be calculated with the password and two times the received random number from the last GET RANDOM NUMBER command:

XOR_Password[31:0] = Password[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}.

To get out of the NFC PRIVACY mode, the valid Privacy password has to be transmitted to the IC with the DISABLE NFC PRIVACY command.

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 104. ENABLE NFC PRIVACY request format

Flags	SET PASSWORD	IC Mfg code	UID	XOR password	CRC16
8 bits	8 bits	8 bits	64 bits optional	32 bits	16 bits

Table 105. ENABLE NFC PRIVACY response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 106. ENABLE NFC PRIVACY response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.3.10 DISABLE NFC PRIVACY

Command code = B3h

The DISABLE NFC PRIVACY command moves the NTAG 5 switch out of the NFC PRIVACY mode.

Remark: *The timing of the DISABLE PRIVACY command is write alike.*

The XOR password has to be calculated with the password and two times the received random number from the last GET RANDOM NUMBER command:

XOR_Password[31:0] = Password[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}.

The Privacy identifier is 04h.

Option_flag = 1b and Option_flag = 0b are supported.

Table 107. DISABLE NFC PRIVACY request format

Flags	SET PASSWORD	Manuf. code	UID	Privacy identifier	XOR password	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits	32 bits	16 bits

Table 108. DISABLE NFC PRIVACY response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 109. DISABLE NFC PRIVACY response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

Remark: *If the IC receives an invalid password, it will not execute any following command until a Power-On Reset (POR) (NFC reset) is executed.*

8.2.3.4 Memory operations

Following commands are implemented for accessing user memory according to ISO/IEC 15693.

- READ SINGLE BLOCK
- WRITE SINGLE BLOCK
- LOCK BLOCK
- READ MULTIPLE BLOCKS up to 3Fh blocks

On top of these commands, NTAG 5 switch offers INVENTORY READ and FAST INVENTORY READ

8.2.3.4.1 INVENTORY READ

Command code = A0h

When receiving the INVENTORY READ request, NTAG 5 switch performs the same as the anti-collision sequence, with the difference that instead of the UID and the DSFID, the requested response is defined by additional options.

The INVENTORY READ command provides two modes which are defined by the most significant bit of the mask length byte as follows:

- Standard mode (most significant bit of mask length byte equal 0b) (see Section 8.2.3.4.1.1)
- Extended mode (most significant bit of mask length byte equal 1b) The extended mode offers additional features to optimize the inventory procedure for different requirements (see Section 8.2.3.4.1.2)

The INVENTORY READ command may also be transmitted in addressed or SELECTED mode. Then the command behaves similar to a READ or READ MULTIPLE BLOCK (see Section 8.2.3.4.1.3).

8.2.3.4.1.1 Standard mode

If most significant bit of mask length byte is equal 0b the INVENTORY READ command is used in the standard mode.

If the Inventory_flag is set to 1b and an error is detected, NTAG 5 switch remains silent.

If the Option flag is set to 0b, n blocks of data are transmitted. If the Option flag is set to 1b, n blocks of data and the part of the UID which is not part of the mask are transmitted.

The request contains:

- Flags
- INVENTORY READ command code
- IC manufacturer code
- AFI (if AFI_flag is set to 1b)
- Mask length (most significant bit equal 0b)
- Mask value (if mask length > 00h)
- First block number to be read
- Number of blocks to be read
- CRC 16

Table 110. INVENTORY READ request format

Flags	INVENTORY READ	Manuf. code	AFI	Mask length	Mask value	First block number	Number of blocks	CRC16
8 bits	8 bits	8 bits	8 bits (optional)	8 bits	0 to 8 bytes	8 bits	8 bits	16 bits

If the Inventory_flag is set to 1b, only NTAG 5 switch in the READY or SELECTED (SECURE) state will respond (same behavior as in the INVENTORY command). The meaning of Flags bits 7 to 4 is as defined in ISO/IEC 15693.

The INVENTORY READ command can also be transmitted in the addressed or SELECTED mode (see Section 8.2.3.4.1.3).

The number of blocks in the request is one less than the number of blocks that NTAG 5 switch returns in its response.

If the Option_flag in the request is set to logic 0b the response contains:

Table 111. INVENTORY READ response format: Option flag logic 0b

Flags	Data	CRC16
8 bits	Number of blocks times 32 bits	16 bits

NTAG 5 switch reads the requested block(s) and sends back their value in the response. The mechanism and timing of the INVENTORY READ command performs the same as the INVENTORY command which is defined in ISO/IEC 15693.

If the Option_flag in the request is set to logic 1b, the response contains:

Table 112. INVENTORY READ response format: Option flag logic 1b

Flags	Rest of UID which is not part of the mask and slot number	Data	CRC16
8 bits	0 to 64 bit, always a multiple of 8 bits	Number of blocks times 32 bits	16 bits

NTAG 5 switch reads the requested block(s) and sends back their value in the response. Additionally the bytes of the UID, which are not parts of the mask and the slot number in case of 16 slots, are returned. Instead of padding with zeros up to the next byte boundary, the corresponding bits of the UID are returned. The mechanism and timing of the INVENTORY READ command perform the same as the INVENTORY command which is defined in ISO/IEC 15693.

Remark: *The number of bits of the retransmitted UID can be calculated as follows:*

- 16 slots: 60 bits (bit 64 to bit 4) - mask length rounded up to the next byte boundary
- 1 slot: 64 bits - mask length rounded up to the next byte boundary

Remark: *If the sum of first block number and number of blocks exceeds the total available number of user blocks, the number of transmitted blocks is less than the requested number of blocks. This means that the last returned block is the highest available user block, followed by the 16-bit CRC and the EOF.*

Example: mask length = 30 bits

Returned: bit 64 to bit 4 (30 bits) = 30 gives 4 bytes

Table 113. Example: mask length = 30

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	UID
mask value including padding with zeros				-				transmitted by interrogator
				returned value				transmitted by NTAG 5 switch

8.2.3.4.1.2 Extended Mode

If the most significant bit of the Mask Length byte is equal 1b the response format is defined by the extended option byte.

The request contains:

- Flags
- Inventory Read command code
- IC Manufacturer code
- AFI (if the AFI flag is set to 1b)

- Mask length (most significant bit equal 1b)
- Extended Options
- Mask value (if mask length > 0)
- First Block Number to be read, if specified in extended options byte
- Number of Blocks to be read, if specified in extended options byte
- CRC 16

Table 114. Inventory Read (extended mode) request format

Flags	INVENTORY READ	Manuf. code	AFI	Mask Length	ext.Options	Mask Value	First block number	Number of blocks	CRC 16
8 bits	8 bits	8 bits	8 bits (optional)	8 bits	8 bits	0 to 64 bits	8 bits (optional)	8 bits (optional)	16 bits

If the Inventory_flag is set to 1b, only NTAG 5 switch in the READY or SELECTED (SECURE) state will respond (same behavior as in the INVENTORY command). The meaning of flags 5 to 8 is in accordance with table 5 in ISO/IEC 15693.

The INVENTORY READ command can also be transmitted in the addressed or SELECTED mode (see Section 8.2.3.4.1.3).

Table 115. Extended options

Bit	Name	Value	Feature
7	RFU	0	
6	RFU	0	
5	QUIET	0	remain in current state
		1	go to QUIET state after response
4	SKIP_DATA	0	NTAG 5 switch will add the user memory blocks in the response as requested with first block number byte and number of blocks byte in the command
		1	No user memory data is requested, first block number byte and number of blocks byte shall not be transmitted in the command
3	CID_RESPONSE	0	Custom ID (CID) will be NOT transmitted in the response
		1	Custom ID (CID) will be transmitted in the response
2	CID_COMPARE	0	No CID is transmitted in the command
		1	16-bit CID will be transmitted in the command and only NTAG 5 switch with the same CID will respond
1	UID_MODE	0	UID will be transmitted as in regular mode (truncated reply depending on least significant 7 bits value of mask length and the mask value)
		1	Complete UID will be transmitted (independent from mask length)
0	EAS_MODE	0	NTAG 5 switch responds independent from the EAS status
		1	Respond only, when EAS is enabled

If the Option_flag in the request is set to 1b the response contains the truncated or complete UID depending on the extended option UID_MODE bit.

If the Option_flag in the request is set to 0b the UID is not part of the response.

Table 116. Inventory Read (extended mode) response format: Option_flag 1b

Flags	Optional truncated UID OR complete UID	Optional data	CRC16
8 bits	0 to 64 bits	Block length	16 bits
	Multiple of 8 bits	Repeated as needed	

The mechanism and timing of the INVENTORY READ command performs the same as at the INVENTORY command which is defined in ISO/IEC 15693.

If the UID is requested in the truncated format the retransmitted UID can be calculated as follows:

16 slots: 64 - 4 - mask length rounded up to the next byte boundary

1 slot: 64 - mask length rounded up to the next byte boundary

Example: mask length = 30 Returned: 64 - 4 - 30 = 30 gives 4 bytes

Table 117. Example

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	UID
mask value incl. padding with zeros								transmitted by Interrogator
				returned value				transmitted by NTAG 5 switch

8.2.3.4.1.3 Addressed and SELECTED mode

The INVENTORY READ command can also be transmitted in the addressed or SELECTED mode. In this case, the Inventory_flag is set to 0 and the meaning of flags 7 to 4 is in accordance with ISO/IEC 15693.

In the addressed or selected mode, the INVENTORY READ command behaves similar to a READ or READ MULTIPLE BLOCK command.

In the addressed mode, it is recommended to address the IC with a mask length of 64 and to transmit the complete UID in the mask value field.

In the selected mode (IC has been selected with a valid SELECT command before), it is recommended to address the IC with a mask length of 0 (and do not transmit the mask value field).

Remark: *If the INVENTORY READ command is used in the addressed or selected mode, the AFI shall not be transmitted and the IC will only respond in the first-time slot.*

8.2.3.4.2 FAST INVENTORY READ

Command code = A1h

When receiving the FAST INVENTORY READ command, NTAG 5 switch behaves the same as the INVENTORY READ command with the following exceptions:

The data rate in the direction NTAG 5 switch to the reader is twice as defined in ISO/IEC 15693 depending on the Datarate_flag 53 kbit (high data rate) or 13 kbit (low data rate).

The data rate from the reader to NTAG 5 switch and the time between the rising edge of the EOF from the reader to NTAG 5 switch remains unchanged (stays the same as defined in ISO/IEC 15693).

Only the single subcarrier mode is supported for the response to the FAST INVENTORY READ command.

8.2.3.5 Originality Signature

8.2.3.5.1 READ SIGNATURE

Command code = BDh

The READ SIGNATURE command returns an IC-specific, 32 byte ECC signature. How to change and / or lock the originality signature is described in Section 8.7.

Only Option_flag = 0b is supported.

Table 118. READ SIGNATURE request format

Flags	READ SIGNATURE	Manuf. code	UID	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits

Table 119. READ SIGNATURE response format when Error_flag is NOT set

Flags	Originality Signature	CRC16
8 bits	256 bits	16 bits

Table 120. READ SIGNATURE response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

Details on how to validate the signature is provided in AN11350.

8.2.3.6 Other

8.2.3.6.1 WRITE AFI

As defined in ISO/IEC 15693.

8.2.3.6.2 LOCK AFI

As defined in ISO/IEC 15693.

8.2.3.6.3 WRITE DSFID

As defined in ISO/IEC 15693.

8.2.3.6.4 LOCK DSFID

As defined in ISO/IEC 15693.

8.2.3.6.5 SET EAS

Command code = A2h

The SET EAS command enables the EAS mode if the EAS mode is not locked.

If the EAS mode is password protected the EAS password has to be first transmitted with the SET PASSWORD command.

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 121. SET EAS request format

Flags	SET EAS	Manuf. code	UID	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits

Table 122. SET EAS response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 123. SET EAS response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.6.6 RESET EAS

Command code = A3h

The RESET EAS command disables the EAS mode if the EAS mode is not locked.

If the EAS mode is password protected the EAS password has to be first transmitted with the SET PASSWORD command.

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 124. RESET EAS request format

Flags	RESET EAS	Manuf. code	UID	CRC16
8 bits	8 bits	8 bits	64 bits optional	16 bits

Table 125. RESET EAS response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 126. RESET EAS response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.6.7 LOCK EAS

Command code = A4h

The LOCK EAS command locks the current state of the EAS mode and the EAS ID.

If the EAS mode is password protected the EAS password has to be first transmitted with the SET PASSWORD command.

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 127. LOCK EAS request format

Flags	LOCK EAS	Manuf. code	UID	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits

Table 128. LOCK EAS response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 129. LOCK EAS response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.6.8 EAS ALARM

Command code = A5h

The EAS ALARM command can be used in the following configurations:

- Option_flag is set to 0b:
  EAS ID mask length and EAS ID value shall not be transmitted.
  If the EAS mode is enabled, the EAS response is returned from the IC.
- Option_flag is set to 1b:
  Within the command, the EAS ID mask length has to be transmitted to identify how many bits of the following EAS ID value are valid (multiple of 8-bits). Only those ICs will respond with the EAS sequence which have stored the corresponding data in the EAS ID configuration (selective EAS) and if the EAS Mode is set.
  If the EAS ID mask length is set to 00h, the IC will answer with its EAS ID.

Table 130. EAS ALARM Request format

Flags	EAS ALARM	Manuf. code	UID	EAS ID mask length	EAS ID value	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits (optional)	0, 8 or 16 bits (optional)	16 bits

If an error is detected the IC remains silent.

Option_flag is set to 0b or Option_flag is set to logic 1b and the EAS ID mask length is not equal to 00h:

Table 131. EAS ALARM Response format (Option flag logic 0)

Flags	EAS sequence	CRC16
8 bits	256 bits	16 bits

EAS sequence (starting with the least significant bit, which is transmitted first; read from left to right):

11110100 11001101 01000110 00001110 10101011 11100101 00001001 11111110 00010111 10001101 00000001 00011100 01001011 10000001 10010010 01101110 01000001 01011011 01011001 01100001 11110110 11110101 11010001 00001101 10001111 00111001 10001011 01001000 10100101 01001110 11101100 11110111

Option_flag is set to 1b and the EAS ID mask length is equal to 00h:

Table 132. EAS ALARM Response format(Option flag logic 1)

Flags	EAS ID value	CRC16
8 bits	16 bits	16 bits

Table 133. EAS ALAMR response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

If the EAS mode is disabled, the IC remains silent.

Remark: *NTAG 5 switch in the QUIET state will not respond to an EAS ALARM command except the addressed flag is set.*

8.2.3.6.9 PROTECT EAS/AFI

Command code = A6h

The PROTECT EAS/AFI command enables the password protection for EAS and/or AFI if the EAS/AFI password is first transmitted with the SET PASSWORD command.

Option_flag set to 0b: EAS will be protected.

Option_flag set to 1b: AFI will be protected.

Both protections (AFI and EAS) can be enabled separately.

Once the EAS/AFI protection is enabled, it is not possible to change back to unprotected EAS and/or AFI.

The timing of the command is write-alike as of write commands with Option_flag set to 0b.

Note: *Option_flag is only related to the parameter to be locked, and NOT to the response behavior.*

Table 134. PROTECT EAS/AFI request format

Flags	PROTECT EAS/AFI	Manuf. code	UID	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits

Table 135. PROTECT EAS/AFI response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 136. PROTECT EAS/AFI response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.6.10 WRITE EAS ID

Command code = A7h

The command WRITE EAS ID enables a new EAS Identifier to be stored in the corresponding configuration memory.

If EAS is password protected (for Set and Reset EAS) the EAS password has to be first transmitted with the SET PASSWORD command.

The timing of the command is write alike.

Option_flag = 0b and Option_flag = 1b is supported and is in accordance with ISO/IEC 15693 write-alike commands.

Table 137. WRITE EAS ID request format

Flags	WRITE EAS ID	Manuf. code	UID	EAS ID value	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits	16 bits

Table 138. WRITE EAS ID response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 139. WRITE EAS ID response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.6.11 GET MULTIPLE BLOCK SECURITY STATUS

As defined in ISO/IEC 15693.

8.2.3.6.12 GET SYSTEM INFORMATION

As defined in ISO/IEC 15693.

The TAG type of NTAG 5 switch is "01h".

8.2.3.6.13 EXTENDED GET SYSTEM INFORMATION

As defined in ISO/IEC 15693 and ISO/IEC 29167-10.

Command code = 3Bh

8.2.3.6.14 GET NXP SYSTEM INFORMATION

Command code = ABh

The GET NXP SYSTEM INFORMATION command provides information about the IC access conditions and supported features.

Table 140. GET NXP SYSTEM INFORMATION request format

Flags	Get NXP System Info	Manuf. code	UID	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits

Table 141. GET NXP SYSTEM INFORMATION response format when Error_flag is NOT set

Flags	PP pointer	PP condition	Lock bits	Feature flag	CRC16
8 bits	8 bits	8 bits	8 bits	32 bits	16 bits

On a valid received command the IC responds with detailed information:

PP pointer byte contains the block address of the protection pointer.

PP condition byte contains information about the access condition to Page H and Page L.

Table 142. Protection Pointer condition byte

Bit	Name	Value	Description
7	RFU	0b	
6	RFU	0b	
5	WH	0b	Page 0-H is not write protected
		1b	Page 0-H is write protected
4	RH	0b	Page 0-H is not read protected
		1b	Page 0-H is read protected
3	RFU	0b	
2	RFU	0b	
1	WL	0b	Page 0-L is not write protected
		1b	Page 0-L is write protected
0	RL	0b	Page 0-L is not read protected
		1b	Page 0-L is read protected

Lock bits byte contains information about permanently locked features.

Table 143. Lock bits byte

Bit	Name	Value	Description
7 to 4	RFU	0b	
3	PP_AREA_0H and NFC_PPC	0b	PP_AREA_0H and NFC_PPC is NOT locked
		1b	PP_AREA_0H and NFC_PPC is locked
2	DSFID	0b	DSFID is NOT locked

Bit	Name	Value	Description
		1b	DSFID is locked
1	EAS	0b	EAS is NOT locked
		1b	EAS is locked
0	AFI	0b	AFI is NOT locked
		1b	AFI is locked

Feature flag byte contains information about supported features (related bit is 1b) of NTAG 5 switch. With this response, it is possible to distinguish the different NTAG 5 family members.

Table 144. Feature flags byte 0

Bit	Name	Description	NTAG 5
7	CID	Customer ID supported (see Section 8.1.3.3)	1b
6	EAS IR	EAS selection supported by extended mode in INVENTORY READ command (see Section 8.2.3.4.1)	1b
5	INVENTORY READ EXT	Extended mode supported by INVENTORY READ command (see Section 8.2.3.4.1)	1b
4	AFI PROT	AFI protection supported (see Section 8.2.3.6.9)	1b
3	EAS PROT	EAS protection supported (see Section 8.2.3.6.9)	1b
2	EAS ID	EAS ID supported by EAS ALARM command (see Section 8.2.3.6.10)	1b
1	COUNTER	NFC Counter supported (see Section 8.1.2.1)	1b
0	UM PROT	User memory protection supported (see Section 8.2.3.3.6)	1b

Table 145. Feature flags byte 1

Bit	Name	Description	NTAG 5	
			NTP5210	NTP5312 NTP5332 NTA5332
7	HIGH BITRATES	high bitrates supported	0b	1b
6	WRITE CID	Write and Lock CID enabled (see Section 8.1.3.3)	1b	
5	DESTROY	DESTROY feature supported (see Section 8.2.3.3.8)	1b	
4	NFC PRIVACY	NFC Privacy mode supported (see Section 8.2.3.3.9)	1b	
3	RFU		0b	
2	PERS QUIET	PERSISTENT QUIET feature supported	0b	
1	RFU		0b	
0	ORIG SIG	Originality signature supported (see Section 8.1.3.1)	1b	

Table 146. Feature flags byte 2

Bit	Name	Description	NTAG 5	
			NTP5210 NTP5312	NTP5332 NTA5332
7 to 3	RFU		all 0b	
2	KEY PRIV	Key privileges supported	0b	1b
1	MUTUAL AUTH	Mutual Authentication feature supported	0b	1b
0	TAG AUTH	Tag Authentication feature supported	0b	1b

Table 147. Feature flags byte 3

Bit	Name	Description	NTAG 5		
			NTP5210	NTP5312	NPT5332 NTA5332
7	EXT FLAG	Additional 32 bits feature flags are transmitted	0b		
6-5	Interface	00b only NFC interface available	01b	11b	
		01b GPIO/ED host interface			
		10b RFU			
		11b GPIO and I^2C host interface			
4	RFU		0b		
3 to 0	NUM KEYS	Number of Keys	0h		4h

Table 148. GET NXP SYSTEM INFORMATION response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.4 Data integrity

Following mechanisms are implemented in the contactless communication link between reader and NTAG 5 switch to ensure very reliable data transmission:

- 16-bit CRC per block
- Bit count checking
- Bit coding to distinguish between logic 1, logic 0, and no information
- Channel monitoring (protocol sequence and bit stream analysis)

8.2.5 Error Handling

8.2.5.1 Transmission Errors

According to ISO/IEC 15693 NTAG 5 switch will not respond if a transmission error (CRC, bit coding, bit count, wrong framing) is detected and will silently wait for the next correct received command.

8.2.5.2 Not supported commands or options

If the received command or option is not supported, the behavior depends on the addressing mechanism.

- Non-Addressed Mode
  NTAG 5 switch remains silent
- Addressed or selected Mode
  NTAG 5 switch responds with error code 0Fh (no information given, or error code not supported).
  If the Inventory flag or the Protocol Extension flag is set, the IC will not respond if the command or option is not supported.
- Parameter out of range
  - Read alike commands
    If the sum of the first block number and the number of blocks exceeds the total available number of user blocks, the number of transmitted blocks is less than the requested number of blocks. This means that the last returned block is the highest available user block, followed by the 16-bit CRC and the EOF.
  - Write alike commands
    If the address of a block to be written does not exist or a block to be written is locked, the behavior of the IC depends on the addressing mechanism.
    - Non-Addressed Mode
      NTAG 5 switch remains silent.
    - Addressed or SELECTED Mode
      NTAG 5 switch responds with error code 0Fh (no information given, or error code not supported).

8.3 Wired Interface

NTAG 5 switch has not only an NFC interface, but also a wired interface. Details are described in following clauses.

8.3.1 Event detection

The event detection feature provides the capability to trigger an external device (e.g., µController) or switch on the connected circuitry by an external power management unit depending on activities on the NFC interface. On top this active low pin can be used as one of the two possible PWM channels.

As the event detection pin functionality is operated via NFC field power, V_{CC} supply for the IC itself is only required when ED pin is used as PWM channel.

NOTE: In some cases V_{OUT} pin might be used as field detection trigger.

The configurable events indicated at event detection pin are:

- The presence/absence of the NFC field
- NDEF Message TLV length field is ZERO/non-ZERO
- IC is/is not in standby mode
- Dedicated config bit is ZERO
- Write/Read command ongoing

Event detection pin is an active LOW signal. Due to open-drain implementation an external pull-up resistor shall be used on this pin.

How to use the event detection pin in applications is described in AN11203.

8.3.2 GPIO

At POR, the GPIO are set to high-impedance state. When configuration is read, the pins are controlled to behave as per the configuration.

GPIOs can be configured to be either input or output (see Section 8.1.3.9). In input mode, the status of the pad will be available in one of the session register bits. In output mode status depends on the session register/config bits content.

How to use the GPIO pins in applications is described in AN11203.

8.3.3 PWM

GPIO pins and ED pin are multiplexed and can be used as a pulse width modulation output. GPIO pins have push-pull architecture, ED pin is an open-drain implementation, which means the PWM signal gets inverted.

PWM resolution, pre-scalar factor (see Section 8.1.3.9) as well as duty cycle can be configured using configuration bytes (see Section 8.1.3.10).

The pulse width modulation resolution (PWMx_RESOLUTION_CONF) defines the maximum number of pulses that are available in the given PWM period. PWM resolution can be set independently for both outputs to either 6, 8, 10 or 12 bits.

The 2-bit PWMx_PRESCALE value divides the PWM input frequency (1695 kHz) by a factor of 1, 2, 4 or 8.

Table 149. Pulse Width Modulation Frequency

Resolution	Pre-scalar			
	00b	01b	10b	11b
12 bit	413 Hz	206 Hz	103 Hz	52 Hz
10 bit	1.7 kHz	825.0 Hz	412.6 Hz	206.2 Hz
8 bit	6.6 kHz	3.3 kHz	1.7 kHz	825.0 Hz
6 bit	26.4 kHz	13.2 kHz	6.6 kHz	3.3 kHz

PWMx_ON and PWMx_OFF defines the starting point and end point of the PWMx output is asserted to HIGH.

To calculate proper PWMx_ON (start of HIGH level) and PWMx_OFF (end of HIGH level) values, PWMx_RESOLUTION_CONF value and PWM_PRESCALE values need to be set to achieve desired PWM frequency. As an example 12-bit resolution is chosen. Duty cycle shall be set to 20 % and start time shall be 10 % offset.

Start Time 10 %: 2^{12} * 10/100= 4096 * 10/100 = ~410 -> PWMx_ON = 19Ah

PWM Duty Cycle 20 %: 2^{12} * 20/100= 4096 * 20/100 = ~819 -> PWMx_OFF = 410 + 819 = 1229 = 4CDh

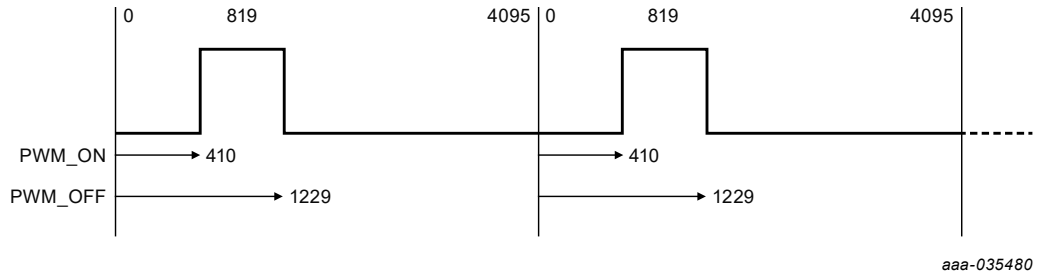


Figure 7. Pulse Width Modulation Example

How to use PWM in applications is described in AN11203.

8.3.4 Standby mode

To minimize overall current consumption, when the IC is supplied via V_{CC} NTAG 5 switch can be set to standby mode by writing related session bit form NFC perspective. The IC will leave standby mode when NFC field is detected, automatically, or HPD pin gets pulled to HIGH for at least 20 µs and released again. In standby mode the current is typically less than 6 µA.

Worst case standby current consumption values can be found in Section 10.1 table.

In case GPIO/PWM pins are not used the pins can be left floating. However, to ensure lowest standby current, following settings are needed:

CONFIG bytes USE_CASE_CONF shall be set in any case to GPIO/PWM, both pins SDA_GPIO1 and SCL_GPIO0 shall be set as input using weak pull-up (GPIOx_IN in).

Block 37h: CONFIG_1, USE_CASE_CONF shall be set to GPIO/PWM (10b) and CONFIG, GPIOx_IN, both shall be set to plain input with weak pullup (01b).

Block 39h: PWM_GPIO_CONFIG_0, SDA_GPIO1 and SCL_GPIO0 shall both be set to 1b to define them as general-purpose input.

8.3.5 Hard power-down mode

In hard power-down mode NTAG 5 switch is switched off using hard power down pin. When pulled to HIGH, the hard power down current is typically less than 0.25 µA. This mode can only be left by connecting HPD pin to ground.

There is no hard power-down mode, when using SO8 packaged version of NTAG 5 switch.

Worst case hard power down current consumption values can be found in Section 10.1 table.

8.4 Energy harvesting

NTAG 5 switch provides the capability to supply external low-power devices with energy harvested from the NFC field of an NFC device.

When DISABLE_POWER_CHECK bit is set to 0b, minimum provided output power can be configured by setting desired voltage and minimum required output current in the related configuration bytes (see Section 8.1.3.11).

WARNING: Sufficient RF field is required when DISABLE_ POWER_CHECK is set to 0b to have access to EEPROM. As long as NTAG 5 switch detects too less

energy to be harvested from the field only INVENTORY command and READ/WRITE CONFIGURATION to access session registers will be handled. This feature ensures a stable system, as the host will only be supplied if there is sufficient energy available. However, during design phase we recommend disabling this power check.

The provided output power in general of course depends on many parameters like the strength of the NFC field, the antenna size, or the distance from the NFC device. The design ensures with the right settings, that V_{OUT} is only enabled, when sufficient energy can be harvested from the NFC field.

1.8 V, 2.4 V or 3 V output voltage can be selected by coding EH_VOUT_V_SEL accordingly.

Minimum required load current can be coded in EH_VOUT_I_SEL configuration field.

VOUT and VCC need to be connected as soon as energy harvesting is used. Otherwise there is no EEPROM access possible from NFC perspective and status registers may contain invalid information.

Appropriate capacitor dependent on load needs to be placed between V_{OUT} and ground to close energy gaps during miller pauses. An example circuit is illustrated in the figure below.

V_{OUT} pin shall be kept floating (not connected) in case energy harvesting feature is not used. If energy harvesting is disabled, pin will be connected to GND internally.

With EH_ENABLE configuration bit st to 1b, energy harvesting will be enabled after boot, automatically and all energy harvesting-related session register bits are meaningless.

When enabling energy harvesting via session registers, EH_MODE, EH_VOUT_SEL and EH_IOUT_SEL needs to be configured properly in the related configuration bytes. EH_ENABLE configuration bit need to be 0b in this case.

After boot, session registers can be used to first trigger current detection by setting EH_TRIGGER to 1b, then poll for EH_LOAD_OK that gets 1b and finally set EH_TRIGGER and EH_ENABLE to 1b, or directly enable energy harvesting by setting EH_TRIGGER and EH_ENABLE bit to 1b (see Table 66).

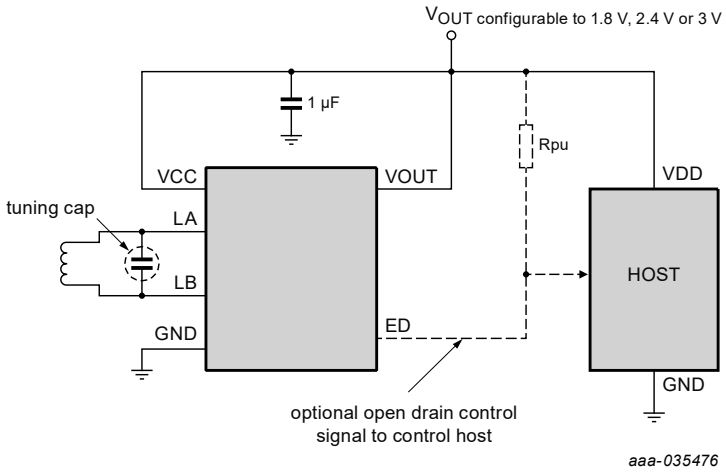


Figure 8. Energy harvesting example circuit

How to use energy harvesting in applications is described in AN12365.

8.5 Security

NTAG 5 switch implements different levels to protect data. The easiest, but efficient method is to lock EEPROM to read only.

With the plain password authentication scheme, the memory can be split in three different parts with different access conditions.

Configuration area can be protected as well.

Further implementation details can be found in AN12366.

8.5.1 Locking EEPROM to read only

Independent on the split of the memory, the user memory may be locked to read-only. If the user EEPROM shall stay in read/write state, the LOCK BLOCK command can be disabled (see Table 25) and lock block sections can be locked (see Table 52). With these features, it can be ensured, NTAG 5 switch stays in read/write state.

Locking the complete EEPROM to read-only as defined in NFC Forum Type 5 Tag specification is quite time consuming. Every single block needs to be addressed by a LOCK BLOCK command (see Section 8.2.3.4). To accelerate this locking, NTAG 5 switch stores the information in the configuration area. With this feature, locking the EEPROM can be accelerated by a factor of 16. Note, that these bits are one time programmable (see Section 8.1.3.20) and blocks are indicated as locked in the Get Multiple Block Security Status response.

Table 150. NFC Lock Block Configuration location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
6Ah		NFC_LOCK_BL0	NFC_LOCK_BL1	RFU	RFU
...		...	...		
71h		NFC_LOCK_BL14	NFC_LOCK_BL15		

8.5.2 Memory Areas

The memory may be split into three different configurable areas with different access conditions.

Highest priority has the 16-bit Protection Pointer PP_AREA_1. It splits the memory into an AREA_0 and an AREA_1 at the address configured with the PP_AREA_1.

Restricted area AREA_1, starting from block address PP_AREA_1 is automatically protected by the AREA_1 read and AREA_1 write password in plain password mode.

The area below this address can be split into two more areas with the 8-bit PP_AREA_0-H (see Section 8.1.3.18) .

AREA_0-L, usually used to store NDEF messages, starts from block 0. AREA_0-H, usually used as password protected area to store private data, starts from block address configured by the 8-bit PP_AREA_0H and ends just before the block addressed with the PP_AREA_1 configuration byte. If PP_AREA_1 points outside the addressable memory space, only AREA_0-L and AREA_0-H are available.

The concept is illustrated in the Figure below and further details can be found in AN12366.

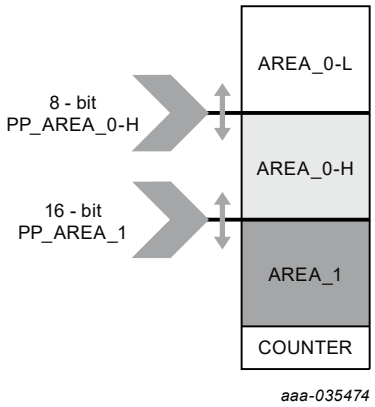


Figure 9. Concept of memory areas

8.5.3 Plain password authentication

NTAG 5 switch implements plain password authentication scheme from NFC perspective.

In summary, seven 32-bit passwords are available from NFC perspective.

- Read
- Write
- Restricted AREA_1 Read
- Restricted AREA_1 Write
- Destroy
- NFC Privacy password (is used to come out of NFC PRIVACY mode)
- EAS/AFI protection

64-bit password protection can be enabled for read and write operations.

A 32-bit password is used to authenticate, before doing memory operations. The mechanism is easy to use. After setting and locking the password, and setting right access conditions in initialization phase, the NFC Device needs to fetch a random number from the ICs. XORing the plain password and this random number results in used password to authenticate.

To resist brute force attacks, a negative authentication counter can be enabled.

How to use plain password authentication in applications is described in AN12366.

8.6 NFC privacy mode

In the privacy mode, the NTAG 5 switch is not traceable by its UID neither by data stored in the user memory. All NTAG 5 switch in the NFC PRIVACY mode will respond to an Inventory command with the UID E0 04 00 00 00 00 00 00, consequently also the user memory is NOT accessible.

NTOE: An anti-collision procedure is not possible.

ENABLE NFC PRIVACY Mode command (see Section 8.2.3.3.9) with a valid privacy password is used to set NTAG 5 switch to this mode and DISABLE NFC PRIVACY (see Section 8.2.3.3.10) is used to disable it again.

NTAG 5 switch in NFC PRIVACY mode only support following commands:

- INVENTORY
- SELECT
- STAY QUIET
- RESET TO READY
- GET RANDOM NUMBER
- DISABLE NFC PRIVACY

8.7 Programmable Originality signature

NTAG 5 switch original signature is based on standard Elliptic Curve Cryptography (curve name secp128r1), according to the ECDSA algorithm. The use of a standard algorithm and curve ensures easy software integration of the originality check procedure in NFC devices without specific hardware requirements.

The UID is signed with an NXP private key and the resulting 32 byte signature is stored in the configuration memory during IC production.

The originality signature is stored in the configuration memory block 00h to block 07h.

Table 151. 32 Byte Originality Signature

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC					
00h		SIG0 (LSB)	SIG1	SIG2	SIG3
01h		SIG4	SIG5	SIG6	SIG7
02h		SIG8	SIG9	SIG10	SIG11
03h		SIG12	SIG13	SIG14	SIG15
04h		SIG16	SIG17	SIG18	SIG19
05h		SIG20	SIG21	SIG22	SIG23
06h		SIG24	SIG25	SIG26	SIG27
07h		SIG28	SIG29	SIG30	SIG31 (MSB)

This signature can be retrieved using the READ_SIGNATURE command or with the READ CONFIG command and can be verified in the NFC device by using the corresponding ECC public key provided by NXP. In case the NXP public key is stored in the reader device, the complete signature verification procedure can be performed offline.

To verify the signature (for example with the use of the public domain crypto library OpenSSL) the tool domain parameters shall be set to secp128r1, defined within the standards for elliptic curve cryptography SEC.

NTAG 5 switch provides the possibility to customize the originality signature to personalize the IC individually for specific application. At delivery, the NTAG 5 switch is pre-programmed with the NXP originality signature described above. This signature is unlocked in the dedicated memory. If needed, the signature can be reprogrammed with a custom-specific signature using the WRITE CONFIG command during the personalization process by the customer. The signature can be permanently locked afterwards by setting the Config Header to “locked” with the WRITE CONFIG command to avoid further modifications.

In any case, it is recommended to permanently lock the originality signature during the initialization process by setting the Config Header to lock with the WRITE CONFIG command.

How to use and verify Originality Signature in applications is described in AN11350.

How to generate Originality Signature is described in AN11859.

9 Limiting values

Table 152. Limiting values In accordance with the Absolute Maximum Rating System (IEC 60134).

Symbol	Parameter	Conditions	Min	Max	Unit
T_{stg}	storage temperature	all packages	-65	+150	°C
T_j	junction temperature	EEPROM write operation	-	+95	°C
T_j	junction temperature	EEPROM read, SRAM and register operation	-	+115	°C
V_{ESD}	electrostatic discharge voltage	charged device model (CDM)[1]	-2	2	kV
		human body model (HBM)[2]	-2	2	kV
V_{CC}	supply voltage	on pin V_{CC}	-0.5	7.15	V
V_i	input voltage	on pin ED, HPD	-0.5	7.15	V
$V_{I\ (RF)}$	RF input voltage	on pin LA/LB	-0.5	5.2	Vp
V_i	input voltage	on pin LA; LB is 0 V; sine wave of 13.56 MHz	-0.5	5.2	Vp
		on pin LB; LA is 0 V; sine wave of 13.56 MHz	-0.5	5.2	Vp
$I_{i(max)}$	maximum input current	La/Lb; peak	-168	168	mA

[1] According to ANSI/ESDA/JEDEC JS-002.
[2] According to ANSI/ESDA/JEDEC JS-001.

10 Characteristics

10.1 Static Characteristics

Table 153. Characteristics

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
General						
f_i	input frequency	ISO/IEC 15693	13.553	13.56	13.567	MHz
C_i	input capacitance	LA-LB, Pin capacitance, VLA-LB @ 1.8Vp, Network Analyzer (13.56 MHz) @Room temp	-	15	-	pF
R_i	Impedance from LA to LB	V_{LALB}=1.8Vpp	30	-	-	kΩ
Operating conditions						
T_{amb}	ambient temperature	$T_j<T_{j\_max}$; for EEPROM write operation	-40	25	85	°C
T_{amb}	ambient temperature	$T_j<T_{j\_max}$; for EEPROM read, SRAM and register operation	-40	25	105	°C
R_{TH_JA}	thermal resistance	JEDEC 2s2p board and SO8 package	-	82	-	K/W
R_{TH_JA}	thermal resistance	JEDEC 2s2p board and TSSOP16 package	-	126	-	K/W
R_{TH_JA}	thermal resistance	JEDEC 2s2p board and XQFN16 package	-	75	-	K/W
V_{CC}	supply voltage	on pin V_{CC}	1.62	-	5.5	V
I_i	input current	La/Lb; 12 A/m; RMS	-	-	43.75	mA
		La/Lb; 12 A/m; peak	-	-	61.87	mA
Current consumption						
I_{VCC}	V_{CC} supply current	V_{CC} = 5.5 V; NFC passive communication no host activity	-	120	150	µA
I_{VCC}	V_{CC} supply current	V_{CC} = 5.5 V, IDLE Mode. No NFC or Host activity	-	-	120	µA
I_{VCC}	V_{CC} supply current	V_{CC} = 5.5 V, PWM/GPIO use case	-	128	175	µA
$I_{hrd\_pwr\_dwn\ Vcc}$	hard power down current	V_{CC} = 1.8 V; XQFN16 package only	-	0.23	2.3	µA
$I_{hrd\_pwr\_dwn\ Vcc}$	hard power down current	V_{CC} = 3.3 V; XQFN16 package only	-	0.25	3.44	µA
$I_{hrd\_pwr\_dwn\ Vcc}$	hard power down current	V_{CC} = 5.5 V; XQFN16 package only	-	0.31	5.72	µA
Energy harvesting VOUT pad						

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{out}	output voltage	configured to 1.8 V; load current <= configured output current	1.62	-	1.98	V
		configured to 2.4 V; load current <= configured output current	2.16	-	2.64	V
		configured to 3.0 V; load current <= configured output current	2.7	-	3.3	V
I_{out}	min. output current	at different regulated output voltages when current detection is enabled and dependent on selected output current value	0.4	-	12.5	mA
ED pin characteristics						
V_{OL}	LOW-level output voltage	IOL = 3 mA	-	-	0.4	V
I_{IED}	leakage current	V_{IN} = 0 V to 5.5 V	10	-	1000	nA
HPD pin characteristics for XQFN16 package						
V_{IL}	LOW-level input voltage		0	-	$0.3*V_{CC}$	V
V_{IH}	HIGH-level input voltage		$0.7*V_{CC}$	-	V_{CC}	V
I_{IL}	LOW-level input current	V_{IN} = 0 V	-1	-	-	µA
I_{IH}	HIGH-level input current	V_{IN} = 5.5 V	-	-	1	µA
C_i	input capacitance		-	-	1.2	pF
V_{IH}	HIGH-level input voltage		$0.7*V_{CC}$	-	-	V
V_{IL}	LOW-level input voltage		-	-	$0.3*V_{CC}$	V
I_{OL}	static output low current	at V_{OL} = 0.4 V	4	-	-	µA
I_{OH}	static output high current	at V_{OH} = V_{CC} - 0.4 V	4	-	1	µA
I_{IL}	LOW-level input current		-1	-	-	µA
I_{OH}	HIGH-level output current		-	-	1	µA
C_i	input capacitance		-	-	3.5	pF
C_L	load capacitance		-	400	-	pF

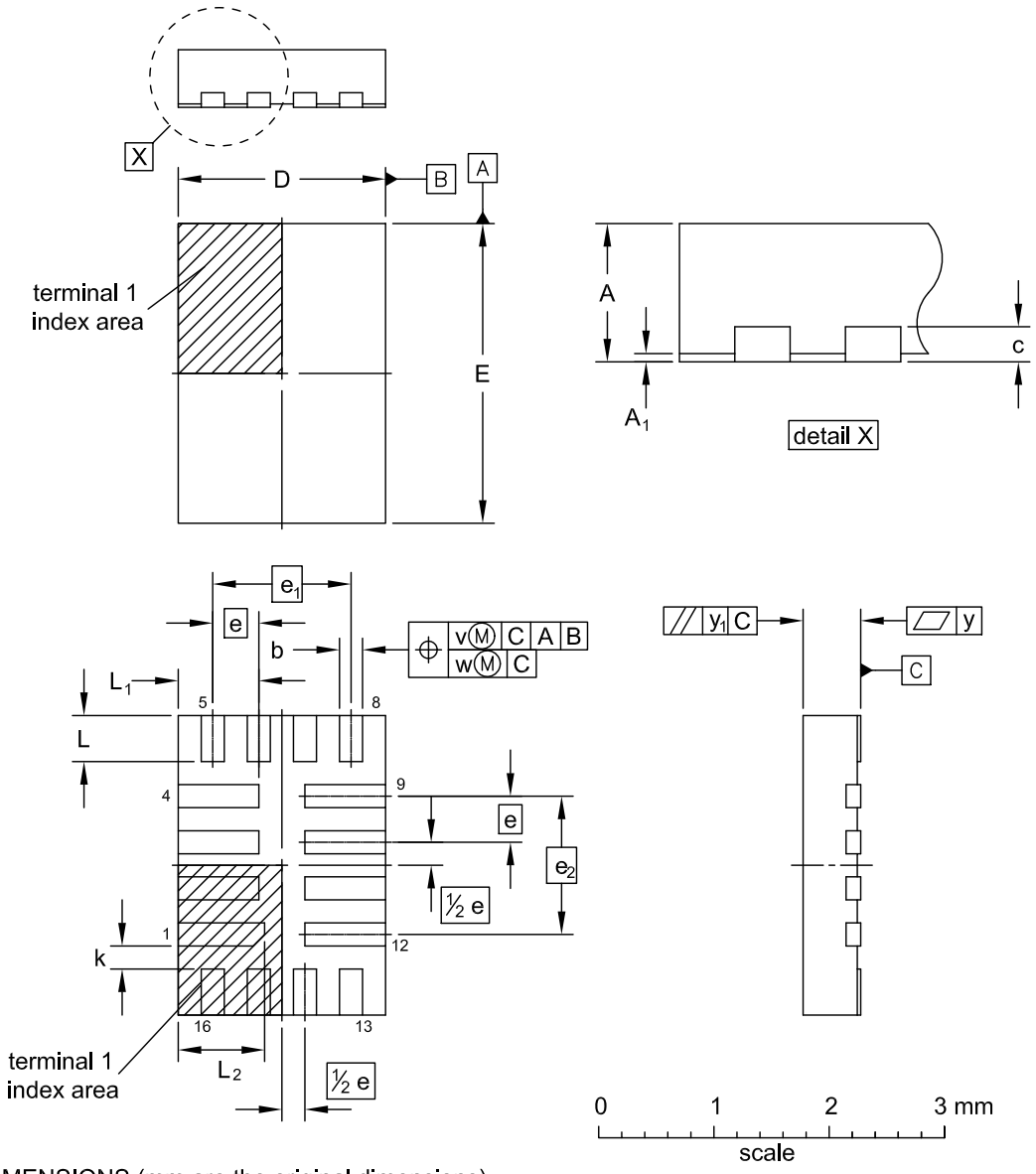
10.2 Dynamic characteristics

Table 154.

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
PWM AC timings						
PWM_{freq}	PWM output frequency		414	-	26400	Hz
Pulse Width	PWM signal pulse width		0.6	-	-	µs
PWM_{freq_tol}	PWM output frequency tolerance		-	-	10	%

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
PWM_{V_tol}	PWM output voltage tolerance	I_{OH} = 4 mA	V_{CC} - 0.4	-	V_{CC}	V
GPIO pin characteristics						
tr	rise time	CL = 20 pF; V_{CC} = 1.8 V	-	-	20.9	ns
		CL = 20 pF; V_{CC} = 3.3 V	-	-	10.92	ns
		CL = 20 pF; V_{CC} = 5.5 V	-	-	8.22	ns
tf	fall time	CL = 20 pF; V_{CC} = 1.8 V	-	-	129	ns
		CL = 20 pF; V_{CC} = 3.3 V	-	-	77.9	ns
		CL = 20 pF; V_{CC} = 5.5 V	-	-	66.9	ns
Start Up time						
t_{Start_RF}	Startup time from NFC from Power OFF state. After this time, the IC is able to receive the command from NFC interface.		-	-	1	ms
EEPROM characteristics						
t_{ret}	retention time	Ta < 85 °C	40	-	-	year
$N_{endu(W)}$	write endurance	Ta <85 °C	1000000	-	-	cycle

11 Package outline



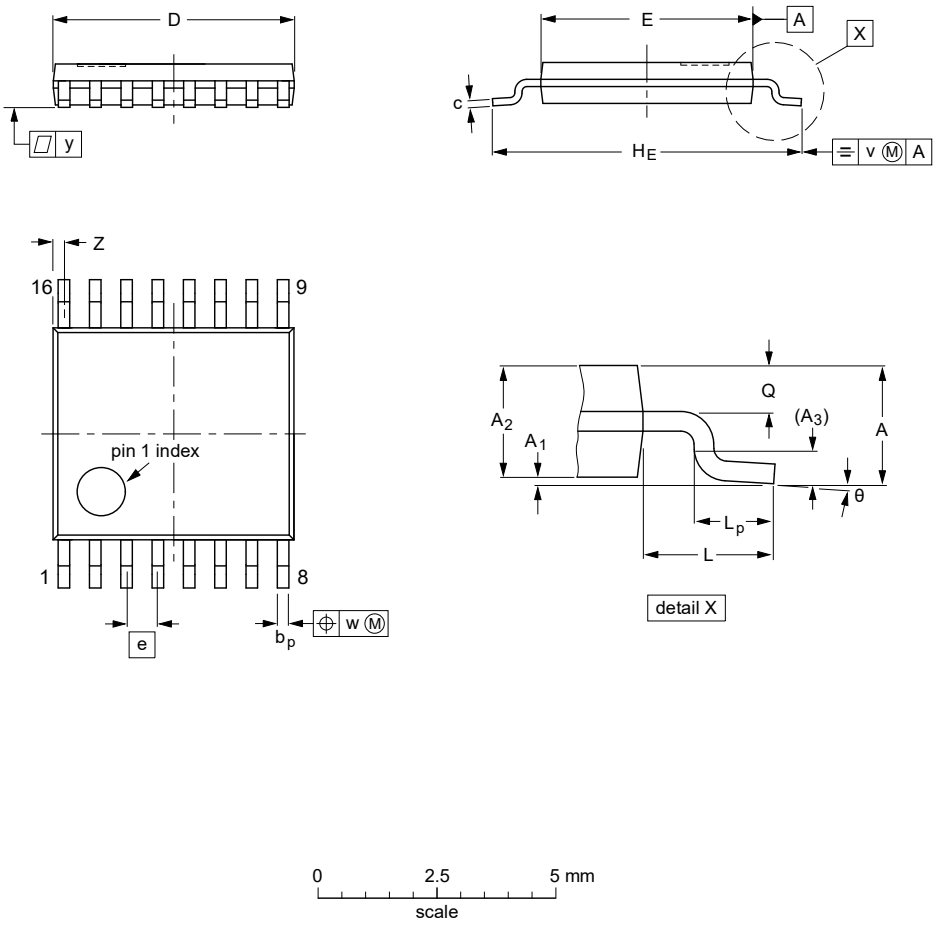
DIMENSIONS (mm are the original dimensions)

UNIT		$A^{(1)}$	A_1	b	c	$D^{(1)}$	$E^{(1)}$	e	e_1	e_2	k	L	L_1	L_2	v	w	y	y_1
mm	MAX	0.50	0.05	0.25		1.90	2.70					0.45	0.75	0.80				
	NOM			0.20	0.127	1.80	2.60	0.40	1.20	1.20	0.2	0.40	0.70	0.75	0.1	0.05	0.05	0.1
	MIN		0.00	0.15		1.70	2.50					0.35	0.65	0.70				

Notes
1. Plastic or metal protrusions of 0.075 maximum per side are not included.

Figure 10. Package outline XQFN16

TSSOP16: plastic thin shrink small outline package; 16 leads; body width 4.4 mm **SOT403-1**



DIMENSIONS (mm are the original dimensions)

UNIT	A max.	A_1	A_2	A_3	b_p	c	D (1)	E (2)	e	H_E	L	L_p	Q	v	w	y	Z (1)	θ
mm	1.1	0.15 0.05	0.95 0.80	0.25	0.30 0.19	0.2 0.1	5.1 4.9	4.5 4.3	0.65	6.6 6.2	1	0.75 0.50	0.4 0.3	0.2	0.13	0.1	0.40 0.06	8° 0°

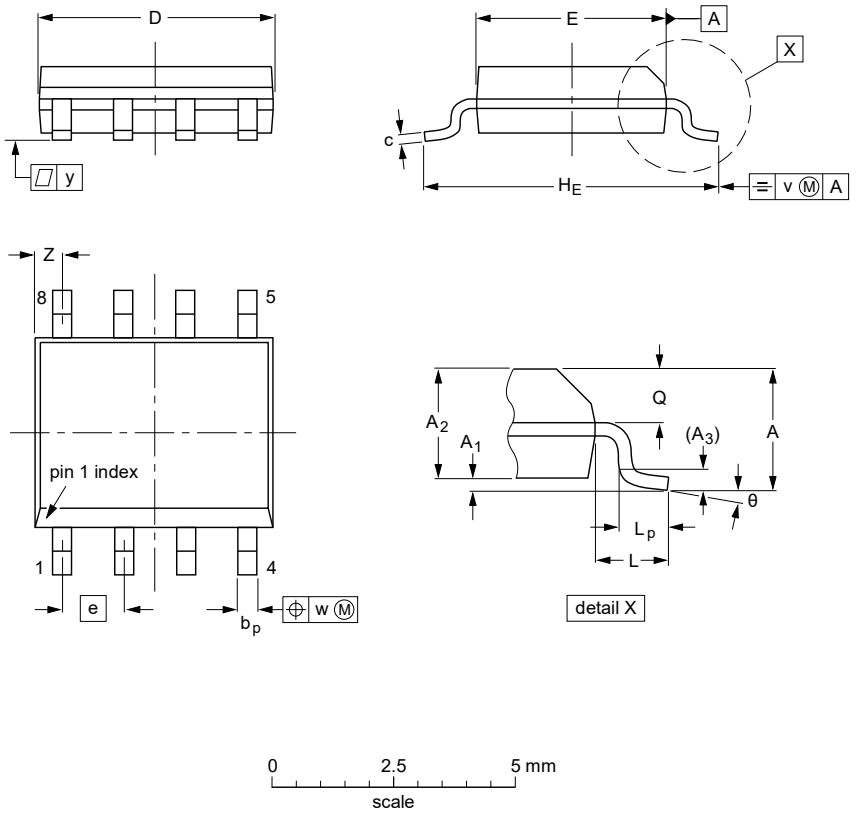
Notes

1. Plastic or metal protrusions of 0.15 mm maximum per side are not included.
2. Plastic interlead protrusions of 0.25 mm maximum per side are not included.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT403-1		MO-153				~~99-12-27~~ 03-02-18

Figure 11. Package outline TSSOP16

SO8: plastic small outline package; 8 leads; body width 3.9 mm **SOT96-1**



DIMENSIONS (inch dimensions are derived from the original mm dimensions)

UNIT	A max.	A_1	A_2	A_3	b_p	c	$D^{(1)}$	$E^{(2)}$	e	H_E	L	L_p	Q	v	w	y	$Z^{(1)}$	θ
mm	1.75	0.25 0.10	1.45 1.25	0.25	0.49 0.36	0.25 0.19	5.0 4.8	4.0 3.8	1.27	6.2 5.8	1.05	1.0 0.4	0.7 0.6	0.25	0.25	0.1	0.7 0.3	8^o 0^o
inches	0.069	0.010 0.004	0.057 0.049	0.01	0.019 0.014	0.0100 0.0075	0.20 0.19	0.16 0.15	0.05	0.244 0.228	0.041	0.039 0.016	0.028 0.024	0.01	0.01	0.004	0.028 0.012	

Notes

1. Plastic or metal protrusions of 0.15 mm (0.006 inch) maximum per side are not included.
2. Plastic or metal protrusions of 0.25 mm (0.01 inch) maximum per side are not included.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT96-1	076E03	MS-012				~~99-12-27~~ 03-02-18

Figure 12. Package outline SO8

12 Handling information

CAUTION

This device is sensitive to ElectroStatic Discharge (ESD). Observe precautions for handling electrostatic sensitive devices.

Such precautions are described in the *ANSI/ESD S20.20, IEC/ST 61340-5, JESD625-A* or equivalent standards.

13 Abbreviations

Table 155. Abbreviations

Acronym	Description
BoM	Bill of Material
CCH	Crypto Configuration Header
CH	Configuration Header
CID	Customer ID
ECC	Elliptic Curve Cryptography
EEPROM	Electrically Erasable Programmable Read-only Memory
GPIO	General Purpose Input Output
IC	Integrated Circuit
lsb	least significant bit
LSB	Least Significant Byte
Manuf. Code	IC Manufacturing Code of NXP is 04h.
msb	most significant bit
MSB	Most Significant Byte
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
POR	Power On Reset
PWM	Pulse Width Modulation
RFU	Reserved for Future Use
TNEP	Tag NDEF Exchange Protocol
SRAM	Static Random-Access Memory

14 References

[1] NFC Forum specification, Digital Protocol - Technical Specification Version 2.1 2019-04-03 [T5T] NFC Forum™
https://nfc-forum.org/product-category/specification/

[2] NFC Forum specification, Type 5 Tag - Technical Specification Version 1.0 2018-04-27 [T5T] NFC Forum™
https://nfc-forum.org/product-category/specification/

[3] ISO/IEC 15693
https://www.iso.org/ics/35.240.15/x/

[4] AN11203 - NTAG 5 Use of PWM, GPIO and Event detection, doc.no. 5302xx
https://www.nxp.com/docs/en/application-note/AN11203.pdf

[5] AN11201 - NTAG 5 How to use energy harvesting, doc.no. 5304xx
https://www.nxp.com/docs/en/application-note/AN12365.pdf

[6] AN12366 - NTAG 5 Memory Configuration and Scalable Security, doc.no. 5305xx
https://www.nxp.com/docs/en/application-note/AN12366.pdf

[7] AN11859 - MIFARE Ultralight and NTAG Generating Originality Signature
https://www.docstore.nxp.com/products

[8] AN11350 - NTAG Originality Signature Validation
https://www.nxp.com/confidential/AN11350

15 Revision history

Table 156. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
NTP5210 v. 3.3	20200703	Product data sheet	-	NTP5210 v. 3.2
Modifications:	• Ambient temperature added for non write operations (see Table 153) • PICK RANDOM UID is not supported by NTAG 5 switch • Information about privacy mode was missing (see Section 8.6) • Password identifier for access to restricted area added (see Table 80) • Editorial updates			
NTP5210 v. 3.2	20200427	Product data sheet	-	NTP5210 v. 3.1
NTP5210 v. 3.1	20200324	Product data sheet	-	NTP5210 v. 3.0
NTP5210 v. 3.0	20200116	Product data sheet	-	NTP5210 v. 2.0
NTP5210 v. 2.0	20191002	Preliminary data sheet	-	NTP5210 v. 1.0
NTP5210 v. 1.0	20190528	Objective data sheet		-

16 Legal information

16.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.
[2] The term 'short data sheet' is explained in section "Definitions".
[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

16.2 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.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

16.3 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.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

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.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

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.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

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.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

16.4 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.

16.5 Trademarks

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

NTAG — is a trademark of NXP B.V.

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

Tables

Figures