NTP53x2

NTAG 5 link - NFC Forum-compliant I²C bridge

Rev. 3.3 — 3 July 2020
544533

Product data sheet
COMPANY PUBLIC

1 General description

Optimized for sensor-driven applications, this highly integrated NFC IC creates a secure, standard-based link from the device to the cloud, in a future proof way to address and even power sensors.

NTAG 5 link is available in two different variants (see Section 4). NTP5332 supports all features of NTP5312, and on top of these, it offers also I²C master features, as well as AES mutual authentication.

NXP's NTAG 5 link lets designers of sensor-equipped systems add an NFC interface with a wired host interface that's configurable as an I²C master/slave, a pulse width modulator (PWM), or a general-purpose I/O (GPIO). Operating at 13.56 MHz, it is an NFC Forum-compliant Type 5 Tag (customer development board is NFC Forum certified - Certification ID: 58626) that can be read and written by an NFC-enabled device at close range and by an ISO/IEC 15693-enabled industrial reader over a longer range.

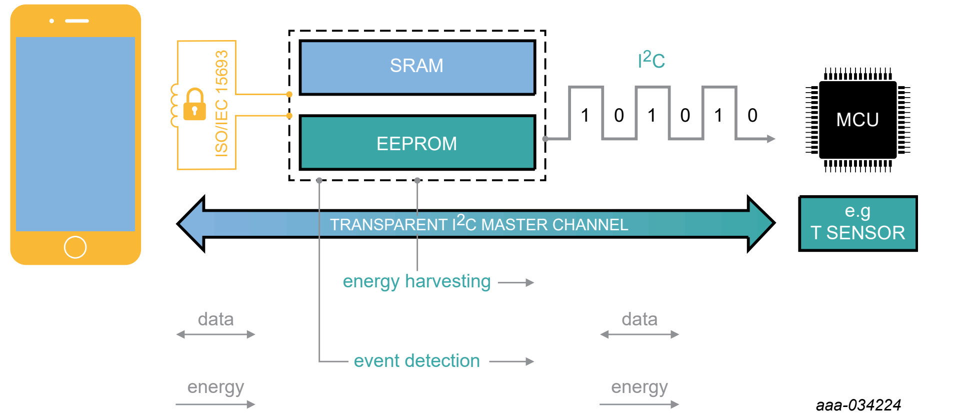


Figure 1. NTAG 5 link overview

The NTAG 5 link can act as a direct bridge between an NFC-enabled device and any I²C slave, such as a sensor or external memory. This is especially useful in environments that require zero-power, single-shot measurements.

With NTAG 5 link, the device can connect to the cloud with a single tap. The connection uses an NFC Forum-compliant data exchange mechanism involving SRAM to ensure highly interoperable data transfers.

Support for ISO/IEC 15693 lets the NTAG 5 link communicate securely in two ways: with powerful industrial readers, at a range of up to 60 cm and with NFC-enabled devices in 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 be used in the field, safely communicate with contactless devices such as mobile phones.

NTAG 5 link offers 2048 bytes (16384 bits) bytes of memory which 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 or up to 128-bit-AES mutual authentication protected read/write access.

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

The NTAG 5 link can operate without a battery by drawing power from the NFC reader instead. It supports energy harvesting, which means it can be used to supply power to other components in the system. When sufficient energy is available, NTAG 5 link can supply a fixed, configurable voltage level to ensure a stable overall system.

2 Features and benefits

- Reading distance with long-range reader > 60 cm (> 25 inches)
- Zero-power readout of an I²C sensor
- Adjustable security levels up to mutual AES authentication (NTP5332 only)
- 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
  - 2048 bytes (16384 bits) user EEPROM on top of configuration memory
  - 256 bytes (2048 bits) SRAM for frequently changing data and pass-through mode
  - 40 years data retention
  - Write endurance of 1 000 000 cycles
- Configurable contact interface
  - I²C slave standard (100 kHz) and fast (400 kHz) mode
  - NTP5332 offers a Transparent I²C master channel (for example, read sensors without an MCU)
  - One configurable event detection pin
  - Two GPIOs as multiplexed I²C lines
  - 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
  - Disable I²C 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 from both interfaces
  - Optional 64-bit password protection from NFC perspective
  - 128-bit AES authentication as defined in ISO/IEC 15693 for NTP5332
  - ECC-based reprogrammable originality signature
- Multiple fast data transfer mode
  - Pass-through mode with 256 byte SRAM buffer
  - Standardized data transfer mode (PHDC, TNEP)
- 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, SRAM 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
  - Simple dynamic secure pairing
  - Commissioning
  - Parameterization
  - Diagnosis
  - Firmware download
  - Low BoM and low-power data acquisition for sensors
  - 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
  - Smart sensor
  - Smart metering

4 Ordering information

Table 1. Ordering information

Orderable part number	Package		
	Name	Description	Version
NTP53121G0JHKZ	XQFN16	NTAG 5 link; with I^{2}C interface and 2048 bytes user EEPROM plastic, extremely thin quad flat package; no leads; 16 terminals	SOT1161-2
NTP53121G0JTTZ	TSSOP16	NTAG 5 link; with I^{2}C interface and 2048 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
NTP53121G0JTZ	SO8	NTAG 5 link; with I^{2}C interface and 2048 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
NTP53121G0FUAV	Wafer	NTAG 5 link; 8 inch wafer, 150 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format)	-
NTP53321G0JHKZ	XQFN16	NTAG 5 link with I^{2}C master/slave interface, AES authentication and 2048 bytes user EEPROM plastic, extremely thin quad flat package; no leads; 16 terminals	SOT1161-2
NTP53321G0JTTZ	TSSOP16	NTAG 5 link with I^{2}C master/slave interface, AES authentication and 2048 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
NTP53321G0JTZ	SO8	NTAG 5 link with I^{2}C master/slave interface, AES authentication and 2048 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
NTP53321G0FUAV	Wafer	NTAG 5 link; 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
NTP53121G0JHK	I21	DBSN|ASID	DYWW	-
NTP53121G0JTT	NP53121	DBID|ASID	ZnDYY	WW
NTP53121G0JT	NP53121	DBSN|ASID	nDYWW	-
NTP53321G0JHK	D21	DBSN|ASID	DYWW	-
NTP53321G0JTT	NP53321	DBID|ASID	ZnDYY	WW
NTP53321G0JT	NP53321	DBSN|ASID	nDYWW	-

Used abbreviations:

ASID: Assembly Sequence ID

D: RHF-2006 indicator

DBID: Diffusion Batch ID

DBSN: Diffusion Batch Sequence Number

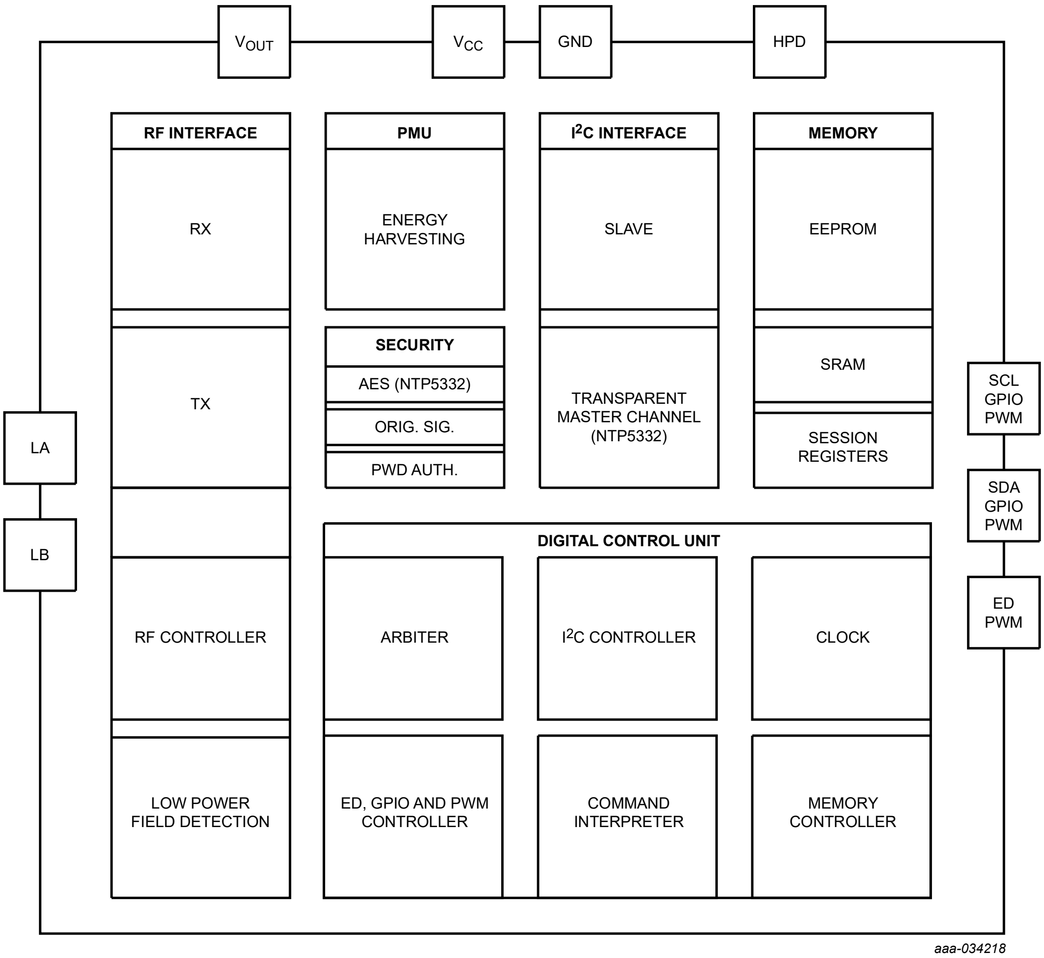
n: Assembly Centre Code

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 link

7 Pinning information

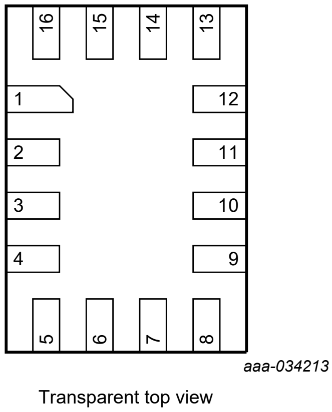


Figure 3. Pin configuration for XQFN16 package

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	SDA/GPIO1/PWM1	Multiplexed serial data I^2C, GPIO1 and PWM1	keep floating
7	SCL/GPIO0/PWM0	Multiplexed serial clock I^2C, 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

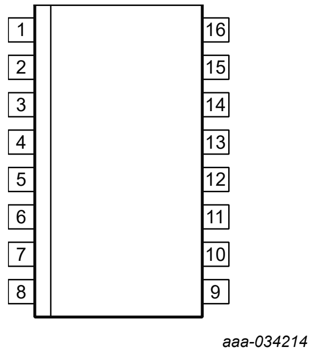


Figure 4. Pin configuration for TSSOP16 package

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	SDA/GPIO1/PWM1	Multiplexed serial data I^2C, GPIO1 and PWM1	keep floating
9	SCL/GPIO0/PWM0	Multiplexed serial clock I^2C, 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

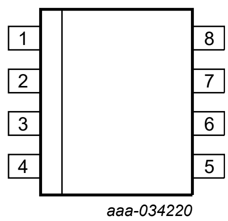


Figure 5. Pin configuration for SO8 package

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	SDA/GPIO1/PWM1	Multiplexed GPIO1 and PWM1	keep floating
6	SCL/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 link 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 8.2.3.5) 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 from NFC perspective contains the 16-bit counter and the counter protection flag (see Section 8.1.2.1). This counter is not accessible from I^2C perspective.
- 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 from NFC perspective. From I^2C perspective, normal READ and WRITE commands are used.
  - The configuration area contains required security-related information, such as access keys 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.
- SRAM
  - SRAM is accessible when NTAG 5 link is V_{CC} supplied and SRAM_ENABLE is set to 1b.
  - Volatile SRAM can be used for fast and frequent data transfer (see Section 8.1.5). With WRITE SRAM (see Section 8.2.3.6.2) and READ SRAM (see Section 8.2.3.6.1), the content is written or read.
  - When the SRAM gets mapped to user memory (the start address is always block 0 from both interfaces), then standard READ BLOCK and WRITE BLOCK commands can be used. This mechanism is used, e.g., for PHDC or dynamic pairing.
  - From I^2C perspective, SRAM is always located from address 2000h to 203Fh.

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 link, 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.

User EEPROM map looks totally the same from NFC and I²C perspective.

The last block contains the 16-bit counter (see Section 8.1.2.1). It is only accessible from NFC perspective.

NTAG 5 link offers 2048 bytes (16384 bits) of user memory.

Table 6. User memory organization

Block Address		Byte 0 (LSB)	Byte 1	Byte 2	Byte 3 (MSB)	Description
NFC	I²C					
00h	0000h	Capability Container				or user memory
01h	0001h	User Memory				
:	:					
1FEh	01FEh					
1FFh	-	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	I²C				
00h	0000h	E1h	40h	80h	09h
01h	0001h	03h	10h	D1h	01h
02h	0002h	0Ch	55h	01h	6Eh
03h	0003h	78h	70h	2Eh	63h
04h	0004h	6Fh	6Dh	2Fh	6Eh
05h	0005h	66h	63h	FEh	00h
06h	0006h	rnd	rnd	rnd	rnd
...	...	rnd	rnd	rnd	rnd
1FFh	-	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 or by mutual authentication with a key with the Write privilege

- read
- increased by one, optionally protected with the read password or by mutual authentication with a key with the Read privilege

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	
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 or by mutual authentication depending on the used security level

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 or a valid mutual authentication with a key with the Write privilege, depending on the used security level.

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 or a valid mutual authentication with a key with the Read privilege is required to increment the counter value, again depending on the used security level.

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 or mutual authentication

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 or a valid mutual authentication with a key with the Read privilege 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 a valid mutual authentication with a key with the Write privilege has been executed before 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 from NFC perspective and NAK from I²C perspective. Reading complete RFU blocks results in receiving all bytes 00h.

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

From I²C perspective, the configuration can be accessed using READ MEMORY and WRITE MEMORY command. Block address of configuration area from I²C perspective starts from 1000h.

In Table 11 all NFC_KHs, NFC_KPs and AES_KEYs (all marked with an asterisk) are only available in AES mode. NFC_KHs and NFC_KPs are not available at all and set to RFU in plain password mode. In the area of KEY_0 and KEY_1, the plain passwords are stored (see Section 8.1.3.9). The rest of the KEY area is RFU in plain password mode.

NOTE: AES mode is only available for NTP5332.

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 8.1.3.32).

Table 11. Configuration Memory organization

Sec.	Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
	NFC	I²C					
0	00h	1000h	ORIGINALITY_SIGNATURE				32 byte Originality Signature (see Section 8.1.3.1)
0	...	...					
0	07h	1007h					
0	08h	1008h	CH	RFU			Configuration Header (see Section 8.1.3.2)

Sec.	Block Address NFC	Block Address I²C	Byte 0	Byte 1	Byte 2	Byte 3	Description
0	09h	1009h	CID		RFU		Customer ID (see Section 8.1.3.3)
N/A	0Ah	100Ah	RFU				
N/A	0Bh	100Bh	RFU				
0	0Ch	100Ch	RFU	NFC_GCH	RFU		NFC Global Crypto Header (see Section 8.1.3.4)
0	0Dh	100Dh	RFU	NFC_CCH	RFU		NFC Crypto Configuration Header (see Section 8.1.3.5)
0	0Eh	100Eh	NFC_AUTH_LIMIT		RFU		NFC Authentication Limit Counter (see Section 8.1.3.6)
N/A	0Fh	100Fh	RFU				
0	10h	1010h	RFU	NFC_KH0*	RFU		NFC Key Header 0 (see Section 8.1.3.7)
0	11h	1011h	NFC_KP0*	RFU			NFC Key Privileges 0 (see Section 8.1.3.8)
0	12h	1012h	RFU	NFC_KH1*	RFU		NFC Key Header 1 (see Section 8.1.3.7)
0	13h	1013h	NFC_KP1*	RFU			NFC Key Privileges 1 (see Section 8.1.3.8)
0	14h	1014h	RFU	NFC_KH2*	RFU		NFC Key Header 2 (see Section 8.1.3.7)
0	15h	1015h	NFC_KP2*	RFU			NFC Key Privileges 2 (see Section 8.1.3.8)
0	16h	1016h	RFU	NFC_KH3*	RFU		NFC Key Header 3 (see Section 8.1.3.7)
0	17h	1017h	NFC_KP3*	RFU			NFC Key Privileges 3 (see Section 8.1.3.8)
N/A	18h	1018h	RFU				
N/A	...	...					
N/A	1Fh	101Fh					
0	20h	1020h	KEY_0*				AES key 0 or NFC_PWD_0 to NFC_PWD_3 (see Section 8.1.3.9)
0	21h	1021h					
0	22h	1022h					
0	23h	1023h					

Sec.	Block Address NFC	Block Address I²C	Byte 0	Byte 1	Byte 2	Byte 3	Description
0	24h	1024h	KEY_1*				AES key 1 or NFC_PWD_4 to NFC_PWD_6 (see Section 8.1.3.9)
0	25h	1025h					
0	26h	1026h					
0	27h	1027h					
0	28h	1028h	KEY_2*				AES key 2 or RFU (see Section 8.1.3.9)
0	29h	1029h					
0	2Ah	102Ah					
0	2Bh	102Bh					
0	2Ch	102Ch	KEY_3*				AES key 3 or RFU (see Section 8.1.3.9)
0	2Dh	102Dh					
0	2Eh	102Eh					
0	2Fh	102Fh					
1	30h	1030h	I2C_KH	RFU			I²C Key Header (see Section 8.1.3.10)
1	31h	1031h	I2C_PP	I2C_PPC	RFU		I²C Protection Pointer and Config (see Section 8.1.3.11)
1	32h	1032h	I2C_AUTH_LIMIT		RFU		Authentication Limit Counter (see Section 8.1.3.12)
1	33h	1033h	I2C_PWD_0				I²C read password (see Section 8.1.3.9)
1	34h	1034h	I2C_PWD_1				I²C write password (see Section 8.1.3.9)
1	35h	1035h	I2C_PWD_2				Restricted AREA_1 I²C read password (see Section 8.1.3.9)
1	36h	1036h	I2C_PWD_3				Restricted AREA_1 I²C write password (see Section 8.1.3.9)
2	37h	1037h	CONFIG				Feature Configuration (see Section 8.1.3.13)
3	38h	1038h	SYNC_DATA_BLOCK		RFU		Block may be used for data transfer synchronization (see Section 8.1.3.14)

Sec.	Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
	NFC	I²C					
3	39h	1039h	PWM_GPIO_CONFIG		RFU		PWM and GPIO Configuration (see Section 8.1.3.15)
3	3Ah	103Ah	PWM0_ON_OFF				PWM1 Configuration (see Section 8.1.3.16)
3	3Bh	103Bh	PWM1_ON_OFF				PWM1 Configuration (see Section 8.1.3.16)
3	3Ch	103Ch	WDT_CONFIG			SRAM_ COPY_ BYTES	Watch Dog Timer Configuration (see Section 8.1.3.17) and SRAM Copy Bytes (see Section 8.1.5)
3	3Dh	103Dh	EH_CONF	RFU	ED_CONF	RFU	Energy Harvesting (see Section 8.1.3.18) and Event Detection Pin (see Section 8.1.3.19) Configuration
3	3Eh	103Eh	I2C_SLAVE_CONFIG		I2C_MASTER_CONFIG (NTP5332)		I²C Configuration (see Section 8.1.3.20 and Section 8.1.3.21)
3	3Fh	103Fh	SEC_CONF	SRAM_ CONF_PROT	PP_AREA_1		Device Security Configuration (see Section 8.1.3.22) SRAM and Configuration Protection (see Section 8.1.3.23) AREA_1 Protection Pointer (see Section 8.1.3.24)
N/A	40h	1040h	RFU				
N/A	...	...					
N/A	44h	1044h					
7	45h	1045	SRAM_DEFAULT				Default SRAM content (see Section 8.1.5)
7	...	...					
7	54h	1054					
4	55h	1055h	AFI	RFU			Application Family Identifier (see Section 8.2.3.9.1)
4	56h	1056h	DSFID	RFU			DSFID (see Section 8.1.3.26)

Sec.	Block Address NFC	Block Address I^2C	Byte 0	Byte 1	Byte 2	Byte 3	Description
4	57h	1057h	EAS_ID		RFU		EAS ID (see Section 8.1.3.27)
4	58h	1058h	NFC_ PP_AREA_0H	NFC_PPC	RFU		NFC Protection Pointer (see Section 8.1.3.28) and NFC Protection Pointer Conditions (see Section 8.1.3.29)
N/A	59h	1059h	RFU				
N/A	...	...					
N/A	69h	1069h					
5	6Ah	106Ah	NFC_LOCK_BLOCK		RFU		NFC Lock block configuration (see Section 8.6.1)
5	...	...					
5	89h	1089h					
6	8Ah	108Ah	I2C_LOCK_BLOCK		RFU		I^2C Lock block configuration (see Section 8.1.3.31)
6	...	...					
6	91h	1091h					
8	92h	1092h	NFC_ SECTION_ LOCK	RFU			NFC section lock bytes (see Table 81)
8	93h	1093h					
8	94h	1094h	I2C_ SECTION_ LOCK	RFU			I^2C section lock bytes (see Table 83)
8	95h	1095h					
N/A	96h	1096h	RFU from NFC perspective I2C_PWD_0_AUTH				I^2C read password authenticate(see Section 8.1.3.9)
N/A	97h	1097h	RFU from NFC perspective I2C_PWD_1_AUTH				I^2C write password authenticate (see Section 8.1.3.9)
N/A	98h	1098h	RFU from NFC perspective I2C_PWD_2_AUTH				Restricted AREA_1 I^2C read password authenticate (see Section 8.1.3.9)
N/A	99h	1099h	RFU from NFC perspective I2C_PWD_3_AUTH				Restricted AREA_1 I^2C write password authenticate (see Section 8.1.3.9)
N/A	9Ah	109Ah	RFU				
N/A	...	...					

Sec.	Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
	NFC	I²C					
N/A	9Fh	109Fh					

8.1.3.1 Originality Signature

The Originality signature (see Section 8.8) 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	I²C				
00h	1000h	SIG0 (LSB)	SIG1	SIG2	SIG3
01h	1001h	SIG4	SIG5	SIG6	SIG7
02h	1002h	SIG8	SIG9	SIG10	SIG11
03h	1003h	SIG12	SIG13	SIG14	SIG15
04h	1004h	SIG16	SIG17	SIG18	SIG19
05h	1005h	SIG20	SIG21	SIG22	SIG23
06h	1006h	SIG24	SIG25	SIG26	SIG27
07h	1007h	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	I²C				
08h	1008h	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 from NFC perspective.

From I²C perspective this block can be read and written if not locked by the I²C section lock. Once locked, CH byte cannot be updated anymore and Originality Signature and CID gets locked permanently from I²C perspective.

Table 14. Configuration Header Codes

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

Value	Mode	Write Access
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.

As long as not locked by the I²C section lock, CID maybe updated from I²C perspective with the same logic as from NFC perspective.

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	I²C				
09h	1009h	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 in plain password mode and all other NFC features listed below
- NFC Keys
- NFC Protection Pointer
- NFC Protection Pointer Conditions
- NFC Key Headers
- NFC Key Privileges
- NFC Crypto Configuration Header
- EAS and AFI protection

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 independently from the interface and it is irreversible.

Same rules apply from I²C perspective, as long as not locked by the I²C section lock.

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	I²C				
0Ch	100Ch	RFU	NFC_GCH	RFU	

Table 17. Global Crypto Header Configuration in plain password mode

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).

Table 18. Global Crypto Header Configuration Value in AES mode

Value	Status	Description
81h	Deactivated (default)	The settings of the NFC Protection Pointer and the NFC Protection Pointer Condition are not activated. Read and write access to the user memory is possible independent of the settings without a previous mutual authentication. The Protection Pointer Address and the NFC Protection Pointer Condition byte can be modified with a PROTECT PAGE command without a previous mutual authentication except of the LOCK PAGE PROTECTION CONDITION command has been successfully executed before. The Keys and Key Privileges can be read and written with the READ CONFIG and WRITE CONFIG commands according to the status of the related Key Header. The settings for the EAS/AFI protection are not activated. Access with the related commands to EAS and AFI is possible without a previous mutual authentication.
87h	Deactivated & privileges locked	The status is the same as for 81h with the exception that the Key Privileges are locked and cannot longer be modified. The settings for the EAS/AFI protection are not activated. Access with the related commands to EAS and AFI is possible without a previous mutual authentication.
C1h	Access right activated	The settings of the Protection Pointer address and the Protection Pointer Condition are enabled. Read and write access protection is enabled according to the initialized values. The Keys and Key Privileges can be read and written with the READ CONFIG and WRITE CONFIG commands according to the status of the related Key Header. The settings for the EAS/AFI protection are enabled. Access with the related commands to EAS and AFI is only possible according to the EAS/AFI protection conditions.

Value	Status	Description
C7h	Access right activated &privileges locked	The status is the same as for C1h with the exception that the Key Privileges are locked and cannot longer be modified. The settings for the EAS/AFI protection are enabled. Access with the related commands to EAS and AFI is only possible according to the EAS/AFI protection conditions.
E7h	Activated	The settings of the NFC Protection Pointer and the NFC Protection Pointer Condition are enabled. Read and write access protection is enabled according to the initialized values. All Key Header Privileges and Keys are locked cannot be modified The settings for the EAS/AFI protection are enabled. Access with the related commands to EAS and AFI is only possible according to the EAS/AFI protection conditions.
all others	Invalid	

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).

From I²C perspective, NFC_CCH can be accessed with READ and WRITE command, as long as not locked by the I²C section lock.

Table 19. Crypto Configuration Header (CCH) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
0Dh	100Dh	RFU	NFC_CCH	RFU	

Table 20. 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 mutual authentication with a key with activated crypto configuration privilege or 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

The NFC Authentication Limit Counter is a feature to limit the number of authentications. When enabled, the counter is incremented for every CHALLENGE (see Section 8.2.3.4.5) or AUTHENTICATION (see Section 8.6.4) command. Both, positive and negative attempts get counted. On default. the counter is not enabled (NFC_AUTH_LIMIT = 0000h).

In plain password mode, NTAG 5 link 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 21. NFC Authentication Limit Counter (NFC_AUTH_LIMIT) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
0Eh	100Eh	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.

The start value for the Authentication Limit can be preset with a WRITE CONFIG command (see Section 8.2.3.2.2) if

- the Crypto Config Header is not set to "Locked" and the NFC Global Crypto Header is not set to "Activated" or
- a valid mutual authentication with a key with the Crypto Config privilege set has been executed before.

In plain password mode, the 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 is enabled, the authentication limit value is increased by one at each CHALLENGE or AUTHENTICATE command (first step only). As soon as the value of the Authentication limit reaches

- FF00h: only mutual authentication will be accepted to reset the authentication limit
- FFFFh: no further authentication is possible any longer. This status is irreversible.

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

From I²C perspective, this block can be read and written if not locked by the I²C section lock.

8.1.3.7 NFC Key Header

The NFC Key Header bytes (NFC_KH0, NFC_KH1, NFC_KH2, NFC_KH3) define the status for the related NFC key.

The programming of NFC Key Header can be done in only one direction from lower state to higher and it is irreversible from NFC perspective.

Same rules apply from I^2C perspective, as long as not locked by the I^2C section lock. Once locked (as per table below) cannot be updated anymore from I2C interface.

Table below shows the location of the NFC Key Headers in the configuration memory. When using password authentication, these bytes and blocks are all RFU.

NOTE: Key headers are only available for NTP5332 in AES mode.

Table 22. NFC Key Header (KHx) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I^2C				
10h	1010h	RFU	NFC_KH0*	RFU	
12h	1012h	RFU	NFC_KH1*	RFU	
14h	1014h	RFU	NFC_KH2*	RFU	
16h	1016h	RFU	NFC_KH3*	RFU	

If the Global Crypto Header is in the "Activate and locked" state, all crypto settings (Key Headers, Keys and Privileges) are locked and cannot longer be modified.

Table 23. NFC Key Header Values

Value	Status	Description
81h	Not active (default)	The related Key and the Key Privileges can be read and written with the READ CONFIG and WRITE CONFIG commands. The related key is not active and cannot be used. The Key Privileges of the related Key are not valid.
E7h	Active and locked	The related Key and its privileges are active and locked and cannot be modified any longer. The related Key cannot be read or written with the READ CONFIG and WRITE CONFIG commands. The related Key Header and Key Privileges can only be read with the READ CONFIG command.
FFh	Disabled	Related Key is disabled and cannot be used

Remark: *It is recommended to set the key header for not required keys to disabled (FFh).*

8.1.3.8 NFC Key Privileges

The NFC Key Privileges bytes define the privileges for the related key. Writing with WRITE CONFIG command to the related block depends on the status of the related NFC Key Header (see Table 23)

From I^2C perspective, this block can be read and written if not locked by the I^2C section lock.

Table shows the location of the Key Privileges in the configuration memory.

NOTE: Key privileges are only available for NTP5332.

Table 24. NFC Key Privileges (KPx) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
11h	1011h	NFC_KP0	RFU		
13h	1013h	NFC_KP1	RFU		
15h	1015h	NFC_KP2	RFU		
17h	1017h	NFC_KP3	RFU		

Table 25 shows the definition of the Key Privileges bytes KPx. The bits define the privileges for the related key used with mutual authentication. If the related bit is set to 1b, the access for the dependent area/feature is granted after mutual authentication with the related key.

Table 25. Definition of NFC Key Privileges bytes KPx

Bit	Privilege	Description
7	Restricted AREA_1 Write	Write access to restricted user memory AREA_1
6	Restricted AREA_1 Read	Read access to restricted user memory AREA_1
5	Crypto Config	Preset of Authentication Limit
4	EAS/AFI	Access for write alike command for EAS and AFI as following: PROTECT EAS/AFI SET EAS RESET EAS LOCK EAS WRITE EAS ID WRITE AFI LOCK AFI
3	Destroy	Access to the DESTROY functionality
2	Privacy	Enable/disable of the PRIVACY mode
1	Write	Write access to protected user memory area
0	Read	Read access to protected user memory area

8.1.3.9 Keys and passwords

The keys or passwords are stored in the configuration memory. The usage of the individual keys depends on the related Key Privileges.

The state of the keys (including read and write access with the READ CONFIG and WRITE CONFIG commands) depends on the status of the related Key Header and the status of the Global Crypto Header.

From I²C perspective, these blocks can be written if not locked by the I²C section lock.

Table below shows the location of the 128-bit AES Table 26 keys in the configuration memory.

NOTE: AES keys are only available for NTP5332 in AES mode.

Table 26. Key location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
20h	1020h	KEY0_0 (LSB)	KEY0_1	KEY0_2	KEY0_3
21h	1021h	KEY0_4	KEY0_5	KEY0_6	KEY0_7
22h	1022h	KEY0_8	KEY0_9	KEY0_10	KEY0_11
23h	1023h	KEY0_12	KEY0_13	KEY0_14	KEY0_15 (MSB)
24h	1024h	KEY1_0 (LSB)	KEY1_1	KEY1_2	KEY1_3
25h	1025h	KEY1_4	KEY1_5	KEY1_6	KEY1_7
26h	1026h	KEY1_8	KEY1_9	KEY1_10	KEY1_11
27h	1027h	KEY1_12	KEY1_13	KEY1_14	KEY1_15 (MSB)
28h	1028h	KEY2_0 (LSB)	KEY2_1	KEY2_2	KEY2_3
29h	1029h	KEY2_4	KEY2_5	KEY2_6	KEY2_7
2Ah	102Ah	KEY2_8	KEY2_9	KEY2_10	KEY2_11
2Bh	102Bh	KEY2_12	KEY2_13	KEY2_14	KEY2_15 (MSB)
2Ch	102Ch	KEY3_0 (LSB)	KEY3_1	KEY3_2	KEY3_3
2Dh	102Dh	KEY3_4	KEY3_5	KEY3_6	KEY3_7
2Eh	102Eh	KEY3_8	KEY3_9	KEY3_10	KEY3_11
2Fh	102Fh	KEY3_12	KEY3_13	KEY3_14	KEY3_15 (MSB)

If using NFC plain password mode, block addresses 20h to 26h (from NFC perspective) and 1020h to 1026h (from I²C perspective) are used to store seven 32-bit passwords as shown in Table 27. Blocks from 27h up to and including 2Fh are not used in plain password mode and are set to RFU.

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 27. Plain Password location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
NFC	I²C					
20h	1020h	NFC_PWD0_ 0 (LSB)	NFC_PWD0_1	NFC_PWD0_2	NFC_PWD0_ 3 (MSB)	Read Password
21h	1021h	NFC_PWD1_ 0 (LSB)	NFC_PWD1_1	NFC_PWD1_2	NFC_PWD1_ 3 (MSB)	Write Password
22h	1022h	NFC_PWD2_ 0 (LSB)	NFC_PWD2_1	NFC_PWD2_2	NFC_PWD2_ 3 (MSB)	Privacy Password
23h	1023h	NFC_PWD3_ 0 (LSB)	NFC_PWD3_1	NFC_PWD3_2	NFC_PWD3_ 3 (MSB)	Destroy Password
24h	1024h	NFC_PWD4_ 0 (LSB)	NFC_PWD4_1	NFC_PWD4_2	NFC_PWD4_ 3 (MSB)	EAS/AFI Password

Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
NFC	I²C					
25h	1025h	NFC_PWD5_0 (LSB)	NFC_PWD5_1	NFC_PWD5_2	NFC_PWD5_3 (MSB)	AREA_1 Read Password
26h	1026h	NFC_PWD6_0 (LSB)	NFC_PWD6_1	NFC_PWD6_2	NFC_PWD6_3 (MSB)	AREA_1 Write Password

For I²C password authentication, there are four 32-bit I²C passwords (default value of all password bytes is 00h) which can be read or written by the host depending on the I²C Key Header configuration.

Table 28. I²C Password location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
NFC	I²C					
33h	1033h	I2C_PWD0_0 (LSB)	I2C_PWD0_1	I2C_PWD0_2	I2C_PWD0_3 (MSB)	Read Password
34h	1034h	I2C_PWD1_0 (LSB)	I2C_PWD1_1	I2C_PWD1_2	I2C_PWD1_3 (MSB)	Write Password
35h	1035h	I2C_ PWD2_0 (LSB)	I2C_PWD2_1	I2C_PWD2_2	I2C_PWD2_3 (MSB)	AREA_1 Read Password
36h	1036h	I2C_ PWD3_0 (LSB)	I2C_PWD3_1	I2C_PWD3_2	I2C_PWD3_3 (MSB)	AREA_1 Write Password

Password authentication from I²C perspective is done by using I²C write command with the password to the I²C Key authenticate location. This will make the I²C logic to enter the Authenticated state if the key matches with the respective key.

Table 29. I²C Key Authenticate Password location

Block Address	Byte 0	Byte 1	Byte 2	Byte 3	
1096h	I2C_PWD0_0_AUTH (LSB)	I2C_PWD0_1_AUTH	I2C_PWD0_2_AUTH	I2C_PWD0_3_AUTH (MSB)	Read Authenticate
1097h	I2C_PWD1_0_AUTH (LSB)	I2C_PWD1_1_AUTH	I2C_PWD1_2_AUTH	I2C_PWD1_3_AUTH (MSB)	Write Authenticate
1098h	I2C_PWD2_0_AUTH (LSB)	I2C_PWD2_1_AUTH	I2C_PWD2_2_AUTH	I2C_PWD2_3_AUTH (MSB)	AREA_1 Read Authenticate
1099h	I2C_PWD3_0_AUTH (LSB)	I2C_PWD3_1_AUTH	I2C_PWD3_2_AUTH	I2C_PWD3_3_AUTH (MSB)	AREA_1Write Authenticate

8.1.3.10 I²C Key Header

The Host interface can access the user memory with I²C READ and I²C WRITE commands. The memory access may be protected by plain password depending on the access conditions.

The programming of I²C Key Header can be done in only one direction from lower state to higher state and it is irreversible.

The NFC interface can access this block with READ CONFIG and WRITE CONFIG commands if not locked by NFC section lock. Once locked as per table below, I2C_KH cannot be updated from the NFC interface anymore.

Table below shows the location of the I²C Key Header Configuration in the configuration memory:

Table 30. I²C Key Header (I2C_KH) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
30h	1030h	I2C_KH	RFU		

Table 31. I²C Key Header Values

Value	Status	Description
81h	Not active (default)	The related I²C passwords, I²C Protection Pointer and I²C Protection Pointer Condition can be read and written with the I²C READ and I²C WRITE commands. The related password is not active and cannot be used.
C3h	Active	The I²C passwords are active. After authentication with write key the I2C_PP, I2C_PPC and Key header can be written and I2C Keys can be read or written.
E7h	Active and locked	The I²C key is active and locked and cannot be modified any longer. The related key cannot be read or written with the I²C READ or I²C WRITE command. The I2C_PP and I2C_PPC can be read with the READ command, but writing with the WRITE command is not possible any longer.
all other	Disabled	Key is disabled and cannot be used

8.1.3.11 I²C Protection Pointer and Condition

The I²C Protection pointer (I2C_PP) defines the address of the user memory where the user memory below PP_AREA_1 is divided into AREA_0-L and AREA_0-H, two arbitrarily sized sections with independent access conditions, which are defined by condition byte (I2C_PPC).

The NFC interface can access this configuration block with READ CONFIG and WRITE CONFIG commands if not locked by NFC section lock.

Table 32. I²C Protection Pointer and Configuration location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
31h	1031h	I2C_PP	I2C_PPC	RFU	RFU

The protection pointer address (I2C_PP) defines the base address where the user memory below PP_ARA_1 is divided into higher and lower sections.

- The memory address below protection pointer address is called I²C AREA_0-L.
- The memory address above and including protection pointer address is called I²C AREA_0-H
- I²C AREA_0-H ends, where AREA_1 starts. Note it is the same position (PP_AREA_1) as from NFC perspective (see Section 8.1.3.24).

Below is an example where the memory is divided into to areas with I2C_PP address set to 0050h. In this example PP_AREA_1 is pointing outside the user EEPROM, which means I²C AREA_0-H ends at the end of the user memory.

Default value of I2C_PP is FFh.

Table 33. I^{2}C Memory organization example

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
0000h					AREA_0-L
0001h					
0002h					
...	...	...	...	...	
004Eh					
004Fh					
0050h					AREA_0-H
0051h					
:	:	:	:	:	
01FEh					
01FFh	RFU				Note: Counter page from NFC perspective

If the protection pointer address is set to block 0, then the entire user memory is defined as AREA_0-H.

The protection pointer address and protection pointer configuration can be only changed under following conditions:

- I^{2}C Key Header Configuration status is "Not Active"
- I^{2}C Key Header Configuration status is "Active and read/write after authentication" with read and write privilege key I^{2}C authentication has been executed before successfully.

The protection pointer address and protection pointer configuration cannot be changed when I^{2}C configuration status is "Active and Locked". This status is irreversible.

Configuration area and SRAM access can be protected by I^{2}C authentication when related bits in SRAM_CONF_PROT are set to 1b.

The default value of I2C_PPC is 00h. Which means full access to AREA_0-L and AREA_0-H.

Table 34. I^{2}C Protection Pointer Configuration (I2C_PPC)

Bit	Name	Value	Description
7	RFU	0b	
6	RFU	0b	
5	WRITE_AREA_H	0b	AREA_0-H is not write protected
		1b	AREA_0-H is write protected
4	REA_AREA_H	0b	AREA_0-H is not read protected
		1b	AREA_0-H is read protected
3	RFU	0b	
2	RFU	0b	
1	WRITE_AREA_L	0b	AREA_0-L is not write protected
		1b	AREA_0-L is write protected

Bit	Name	Value	Description
0	READ_AREA_L	0b	AREA_0-L is not read protected
		1b	AREA_0-L is read protected

8.1.3.12 I²C Authentication Limit Counter

The I²C Authentication Limit Counter is a feature to limit the maximum number of failed authentications from I²C perspective. The counter is incremented for failed password write to block 1096h to 1099h. The counter resets on positive authentication.

The NFC interface can access this block with READ CONFIG and WRITE CONFIG commands if not locked by NFC section lock.

Table 35. I²C Authentication Limit Counter (I2C_AUTH_LIMIT) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
32h	1032h	I2C_AUTH_ LIMIT (LSB)	I2C_AUTH_ LIMT (MSB)	RFU	

Byte 0 of Block 32h is LSB and Byte 1 is MSB of the I²C Authentication Limit counter value. Default value of I2C_AUTH_LIMIT is 00h.

The start value for the Authentication Limit can be preset with an I²C WRITE command if

- I2C Key header is not locked or Not active
- I2C Key header is Active then after valid authentication with a write key.

The Authentication limit is enabled with the most significant bit of Byte 1 is set to 1b. The remaining 15 bit of I2C_AUTH_LIMIT are defining the preset value.

Example:

- 8000h enables and presets the authentication limit to 0, which means the maximum number of failed authentications before a successful is required again is 32767.

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

As soon as the value of the Authentication limit reaches

- FFFFh: no further authentication possible any longer. This status is irreversible.

8.1.3.13 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 from both interfaces.

Table 36. Configuration Bytes Location (CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
37h	1037h	CONFIG_0	CONFIG_1	CONFIG_2	RFU

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

Table 37. Configuration Definition (CONFIG_0)

Bit	Name	Value	Description
7	SRAM_COPY_EN	0b	SRAM copy on POR disabled (default)
		1b	SRAM copy on POR enabled
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 38. Configuration Definition (CONFIG_1)

Bit	Name	Value	Description
7	EH_ARBITER_MODE_EN	0b	In energy harvesting use case, ARBITER_MODE needs to be set with session registers after startup (default)
		1b	ARBITER_MODE is set automatically in any case after startup
6	RFU	0b	
5	USE_CASE_CONF	00b	I²C slave (default)
		01b	I²C master only for NTP5332
4		10b	GPIO/PWM
		11b	All host interface functionality disabled and pads are in 3-state mode
3	ARBITER_MODE	00b	Normal Mode (default)
		01b	SRAM mirror mode
2		10b	SRAM passes through mode
		11b	SRAM PHDC mode
1	SRAM_ENABLE	0b	SRAM is not accessible (default)
		1b	SRAM is available (when VCC supplied)
0	PT_TRANSFER_DIR	0b	Data transfer direction is I²C to NFC (default)
		1b	Data transfer direction is NFC to I²C

Table 39. 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
		1b	Extended commands are supported (Default)
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)

8.1.3.14 Synchronization Block

These bytes define the block address of the user memory being a terminator block. Whenever there is read or written to the block address as specified in SYNCH_DATA_BLOCK from the NFC interface the respective status bit is set. And also ED pin is set accordingly if configured to detect SYNCH_DATA_BLOCK access.

Table 40. Synchronization Block Bytes Location (SYNCH_DATA_BLOCK)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
38h	1038h	SYNCH_DATA_ BLOCK (LSB)	SYNCH_DATA_ BLOCK (MSB)	RFU	

Table 41. Synchronization Block Register Bytes Location (SYNCH_DATA_BLOCK_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
A2h	10A2h	SYNCH_DATA_ BLOCK_REG (LSB)	SYNCH_DATA_ BLOCK_REG (MSB)	RFU	

8.1.3.15 Pulse Width Modulation and GPIO configuration

These configuration bytes define the various configuration bits for GPIO/PWM use case (see Section 8.1.3.13). All features can be configured from NFC and I²C perspective as long NTAG 5 link is configured for slave mode. For details refer to Section 8.3.3 and Section 8.3.4.

Table 42. PWM and GPIO Configuration Location (PWM_GPIO_CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
39h	1039h	PWM_GPIO_CONFIG_0	PWM_GPIO_CONFIG_1	RFU	

Table 43. PWM and GPIO Configuration Definition (PWM_GPIO_CONFIG_0)

Bit	Name	Value	Description
7	SDA_GPIO1_OUT_STATUS	0b	Output status on pad is LOW (default)
		1b	Output status on pad is HIGH
6	SCL_GPIO0_OUT_STATUS	0b	Output status on pad is LOW (default)
		1b	Output status on pad is HIGH
5 to 4	RFU	00b	
3	SDA_GPIO1	0b	Output (Default)
		1b	Input
2	SCL_GPIO0	0b	Output (Default)
		1b	Input
1	SDA_GPIO1_PWM1	0b	GPIO (Default)
		1b	PWM
0	SCL_GPIO0_PWM0	0b	GPIO (Default)
		1b	PWM

Table 44. 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

8.1.3.16 Pulse Width Modulation duty cycle settings

Details can be found in PWM Mode section (see Section 8.3.4).

Table 45. Pulse Width Modulation Duty Cycle Configuration Location (PWMx_ON and PWMx_OFF)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
3Ah	103Ah	PWM0_ON (LSB)	PWM0_ON (MSB)	PWM0_OFF (LSB)	PWM0_OFF (MSB)
3Bh	103Bh	PWM1_ON (LSB)	PWM1_ON (MSB)	PWM1_OFF (LSB)	PWM1_OFF (MSB)

Table 46. Pulse Width Modulation Duty Cycle Session Register Location (PWMx_ON and PWMx_OFF)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
A4h	10A4h	PWM0_ON_REG (LSB)	PWM0_ON_REG (MSB)	PWM0_OFF_REG (LSB)	PWM0_OFF_REG (MSB)
A5h	10A5h	PWM1_ON_REG (LSB)	PWM1_ON_REG (MSB)	PWM1_OFF_REG (LSB)	PWM1_OFF_REG (MSB)

Table 47. 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 48. 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.

8.1.3.17 Watch Dog Timer settings

I²C Watch Dog Timer settings can be adjusted and enabled via configuration bytes from both interfaces. Related session registers are read only. Watch Dog Timer 16-bit default value is 0848h. Details can be found in WDT section (see Section 8.3.1.3).

Table 49. Watch Dog Timer Configuration Location (WDT_CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
3Ch	103Ch	WDT_CONFIG (LSB)	WDT_CONFIG (MSB)	WDT_ENABLE	SRAM_COPY_BYTES

Table 50. Watch Dog Timer Configuration Register Location (WDT_CONFIG_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
A6h	10A6h	WDT_CONFIG_ REG (LSB)	WDT_CONFIG_ REG (MSB)	WDT_EN_REG	RFU

Table 51. Watch Dog Timer Enable Definition (WDT_ENABLE and WDT_EN_REG)

Bit	Name	Default Value	Description
7 to 1	RFU	all 0b	
0	WDT_ENABLE	0b	Watch Dog Timer disabled
		1b	Watch Dog Timer enabled (default)

8.1.3.18 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 8.5).

Table 52. Energy harvesting Configuration Location (EH_CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
3Dh	103Dh	EH_CONFIG	RFU	ED_CONFIG	RFU

Table 53. 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

Bit	Name	Value	Description
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

8.1.3.19 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 8.3.2).

Table 54. Event Detection Configuration Location (ED_CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
3Dh	103Dh	EH_CONFIG	RFU	ED_CONFIG	RFU

Table 55. Event Detection Configuration Register Location (ED_CONFIG_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
A8h	10A8h	ED_COFIG_REG	RFU		

Table 56. 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

Bit	Name	Value	ED pin state	Description
	PWM	0010b	ON	Pulse width modulation signal during OFF period
			OFF	Pulse width modulation signal during On period
	I²C to NFC pass-through	0011b	ON	Last byte of SRAM data has been read via NFC; host can access SRAM again
			OFF	• Last byte written by I²C, or • NFC off, or • V_{CC} is off
	NFC to I²C pass-through	0100b	ON	Last byte written by NFC; host can read data from SRAM
			OFF	• Last byte has been read from I²C, or • NFC off, or • V_{CC} off
	Arbiter lock	0101b	ON	Arbiter locked access to NFC interface
			OFF	Lock to NFC interface released
	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
	READ from SYNCH_BLOCK	1011b	ON	Data read from SYNCH_BLOCK
			OFF	Event needs to be cleared by setting b0 of ED_RESET_REG to 1b or NFC off
	WRITE to SYNCH_BLOCK	1100b	ON	Data written to SYNCH_BLOCK
			OFF	Event needs to be cleared by setting b0 of ED_RESET_REG to 1b or NFC 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
	RFU	1110b	N/A	
	RFU	1111b	N/A	

Table 57. Event Detection Clear Register Location (ED_INTR_CLEAR_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
ABh	10ABh	ED_INTR_ CLEAR_REG	RFU		

Table 58. 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.

8.1.3.20 I²C slave configuration settings

I²C slave functionality can be configured with the following configuration registers from both interfaces.

Table 59. I²C Slave Configuration Location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
3Eh	103Eh	I2C_SLAVE_ADDR	I2C_SLAVE_CONFIG	I2C_MASTER_ SCL_LOW	I2C_MASTER_ SCL_HIGH

Table 60. I²C Slave Configuration Definition (I2C_SLAVE_ADDR)

Bit	Name	Value	Description
7	RFU	0b	
6 to 0	I2C_SLAVE_ADDR	54h	I²C slave address used in slave configuration

Table 61. I²C Slave Configuration Definition (I2C_SLAVE_CONFIG)

Bit	Name	Value	Description
7 to 3	RFU	00000b	
2	I2C_S_REPEATED_START	0b	Slave does not reset if repeated start is received (Default)
		1b	I²C slave resets internal state machine on repeated start
1	RFU	0b	
0	RFU	0b	

8.1.3.21 I²C master clock configuration settings

I²C Master baud rate and SCL high and low can be configured by the related configuration values.

Details about the formula can be found in I²C master section.

NOTE: I²C master is only available for NTP5332.

Table 62. I²C Master Clock Settings Configuration Location (I2C_MASTER_CONFIG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
3Eh	103Eh	I2C_SLAVE_ADDR	I2C_SLAVE_CONFIG	I2C_MASTER_ SCL_LOW	I2C_MASTER_ SCL_HIGH

Table 63. I²C Master Clock Configuration Definition (I2C_MASTER_SCL_LOW)

Bit	Name	Default Value	Description
7	RFU		
6 to 0	I2C_MASTER_SCL_LOW	09h	I²C master configuration SCL low period. Default: 400 kHz, 41%duty cycle.

Table 64. I²C Master Clock Configuration Definition (I2C_MASTER_SCL_HIGH)

Bit	Name	Default Value	Description
7	RFU		
6 to 0	I2C_MASTER_SCL_HIGH	02h	I²C master configuration SCL HIGH period. Default: 400 kHz, 41%duty cycle.

8.1.3.22 Device security configuration bytes

NTAG 5 link features scale-able security. The level of security can be selected with DEV_SEC_CONFIG byte.

SRAM_CONF_PROT is described in Section 8.1.3.23.

PP_AREA_1 is described in Section 8.1.3.24.

Table 65. Device Security Configuration Byte location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
3Fh	103Fh	DEV_SEC_CONFIG	SRAM_CONF_PROT	PP_AREA_1 (LSB)	PP_AREA_1 (MSB)

The IC security features can be enabled or disabled or can choose different security options available from NFC perspective:

- AES authentication scheme
- Plain password feature

Table 66. Device Security Byte Definition (DEV_SEC_CONFIG)

Bit	Name	Value	Description
7 to 5	Security Lock	010b	block 3Fh with device security configuration bytes is locked
		101b	block 3Fh is writeable (default)
		other	RFU

Bit	Name	Value	Description
4	RFU	00b	
3			
2	NFC Security	other	RFU
1		010b	AES (only applicable for NTP5332 - do NOT use for NTP5312)
0		101b	plain password (default)

8.1.3.23 SRAM and Configuration protection

Access to complete SRAM and blocks 37h to 54h of configuration area can be restricted with SRAM_CONFIG_PROT byte.

Table 67. SRAM and Configuration Byte location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
3Fh	103Fh	DEV_SEC_CONFIG	SRAM_CONF_PROT	PP_AREA_1 (LSB)	PP_AREA_1 (MSB)

Table 68. SRAM and Configuration Protection (SRAM_CONF_PROT)

Bit	Name	Value	Description
7 to 6	RFU	00b	
5	I2C_CONFIG_W	0b	Configuration area is not write protected from I²C perspective (default)
		1b	Configuration area is write protected from I²C perspective
4	I2C_CONFIG_R	0b	Configuration area is not read protected from I²C perspective (Default)
		1b	Configuration area is read protected from I²C perspective
3	NFC_SRAM_W	0b	SRAM is not write protected from NFC perspective (Default)
		1b	SRAM is write protected from NFC perspective
2	NFC_SRAM_R	0b	SRAM is not read protected from NFC perspective (Default)
		1b	SRAM is read protected from NFC perspective
1	NFC_CONFIG_W	0b	Configuration area is not write protected from NFC perspective (Default)
		1b	Configuration area is write protected from NFC perspective
0	NFC_CONFIG_R	0b	Configuration area is not read protected from NFC perspective (Default)
		1b	Configuration area is read protected from NFC perspective

8.1.3.24 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). This 16-bit block address is the same for NFC and I²C perspective. The default value is FFFFh.

Table 69. Restricted AREA_1 Pointer location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
3Fh	103Fh	DEV_SEC_CONFIG	SRAM_CONF_PROT	PP_AREA_1 (LSB)	PP_AREA_1 (MSB)

In below example, NFC protection pointer (NFC_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. This example illustrates the view from NFC perspective.

From I²C perspective Area 1 will be the same, however Area 0-L and Area 0-H may look different depending on I²C protection pointer.

Table 70. Memory organization example from NFC perspective

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					
...	...	...	...	...	
01FEh					
01FFh	C0	C1	00h	PROT	Counter

8.1.3.25 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 8.2.3.9.1) 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.

From I²C perspective, this byte can be accessed with normal READ and WRITE commands as long as not locked by I²C section locks.

Table 71. Application Family Identifier (AFI) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
55h	1055h	AFI	RFU		

8.1.3.26 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 8.2.3.9.3) or directly writing DSFID byte to configuration memory using WRITE CONFIG command (see Section 8.2.3.2.2).

From I²C perspective, this byte can be accessed with normal READ and WRITE commands as long as not locked by I²C section locks.

Table 72. Data Storage Format Identifier (DSFID) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
56h	1056h	DSFID	RFU		

8.1.3.27 Electronic Article Surveillance ID

The Electronic Article Surveillance ID (EAS ID) can be configured using WRITE EAS ID (see Section 8.2.3.9.10) 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.

From I²C perspective, this byte can be accessed with normal READ and WRITE commands as long as not locked by I²C section locks.

Table 73. Electronic Article Surveillance ID (EASID) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
57h	1057h	EAS_ID (LSB)	EAS_ID (MSB)	RFU	

8.1.3.28 NFC protection pointer

The NFC protection pointer (NFC_PP_AREA_0H) can be configured using PROTECT PAGE command (see Section 8.2.3.3.6) or directly writing NFC_PP_AREA_0H byte to configuration memory using WRITE CONFIG command (see Section 8.2.3.2.2).

Default value is FFh.

Table 74. NFC Protection Pointer (NFC PP) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
58h	1058h	NFC_ 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. This example illustrates the view from NFC perspective.

Table 75. Memory organization example

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
0000h					AREA_0-L

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
0001h					
0002h					
...	...	...	...	...	
004Fh					
0050h					AREA_0-H
0051h					
...	...	...	...	...	
01FEh					
01FFh	C0	C1	00h	PROT	Counter

8.1.3.29 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 76. NFC Protection Pointer Conditions (NFC_PPC) location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
58h	1058h	NFC_PP_AREA_0H	NFC_PPC	RFU	RFU

Table 77. 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

8.1.3.30 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 and I²C. The access to these bytes for the particular interface can be restricted by configuring the device SECTION_LOCK (see Table 80).

Table 78. NFC Lock Block Configuration location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
6Ah	106Ah	NFC_LOCK_BL00	NFC_LOCK_BL01	RFU	RFU
...	...	...	...	RFU	RFU
89h	1089h	NFC_LOCK_BL62	NFC_LOCK_BL63	RFU	RFU

8.1.3.31 I²C lock bytes

User blocks can be blocked from writing by the I²C interface. These bits are one time programmable. Once written 1b, they cannot be changed back to 0b. Each bit locks 4 blocks of user memory area (e.g., bit 0 of byte 0 locks blocks 0, 1, 2 and 3).These bytes can be written by NFC and I²C. The access to these bytes for the particular interface can be restricted by configuring the device configuration section locks bytes (see Table 80). I2C_LOCK_BL00 – bit 0 – will lock user blocks 0,1,2,3 from I²C perspective.

Table 79. I²C Lock Block Configuration location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
8Ah	108Ah	I2C_LOCK_BL00	I2C_LOCK_BL01	RFU	RFU
...	...	...	...	RFU	RFU
91h	1091h	I2C_LOCK_BL14	I2C_LOCK_BL15	RFU	RFU

8.1.3.32 Device configuration section lock bytes

Lock bits are provided to lock different sections of the configuration area. 16 bits for each interface 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 80. Device configuration section lock bytes location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
92h	1092h	NFC_LOCK_0	RFU		
93h	1093h	NFC_LOCK_1	RFU		
94h	1094h	I2C_LOCK_0	RFU		
95h	1095h	I2C_LOCK_1	RFU		

These section lock configurations are provided to allow customer to initialize NTAG 5 link during customer configuration from either I²C or 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 I2C_LOCK_0 and NFC_LOCK_0 bits are set to 1b, then the lock bytes cannot be updated and gets locked permanently. If any interface is not locked i.e. any one of the I2C_LOCK_0 and NFC_LOCK_0 bits are 0b, then the particular interface can unlock the other.

Table 81. NFC configuration section lock byte 0 definition (NFC_SECTION_LOCK_0)

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

Table 82. NFC configuration section lock Byte 1 definition (NFC_SECTION_LOCK_1)

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

Bit	Name	Value	Description
		1b	Section 2 is not readable by NFC
1	Section 1	0b	Section 1 is readable by NFC
		1b	Section 1 is not readable by NFC
0	Section 0	0b	Section 0 is readable by NFC
		1b	Section 0 is not readable by NFC

Table 83. I²C configuration section lock byte 0 definition (I2C_SECTION_LOCK_0)

Bit	Name	Value	Description
7	Section 7	0b	Section 7 is writable by I²C
		1b	Section 7 is not writable by I²C
6	Section 6	0b	Section 6 is writable by I²C
		1b	Section 6 is not writable by I²C
5	Section 5	0b	Section 5is writable by I²C
		1b	Section 5 is not writable by I²C
4	Section 4	0b	Section 4 is writable by I²C
		1b	Section 4 is not writable by I²C
3	Section 3	0b	Section 3 is writable by I²C
		1b	Section 3 is not writable by I²C
2	Section 2	0b	Section 2 is writable by I²C
		1b	Section 2 is not writable by I²C
1	Section 1	0b	Section 1 is writable by I²C
		1b	Section 1 is not writable by I²C
0	Section 0	0b	Section 0 is writable by I²C
		1b	Section 0 is not writable by I²C

Table 84. I²C configuration section lock byte 1 definition (I2C_SECTION_LOCK_1)

Bit	Name	Value	Description
7	Section 8	0b	Section 8 writable by I²C
		1b	Section 8 is not writeable by I²C
6	Section 6	0b	Section 6 is readable by I²C
		1b	Section 6 is not readable by I²C
5	Section 5	0b	Section 5is readable by I²C
		1b	Section 5 is not readable by I²C
4	Section 4	0b	Section 4 is readable by I²C
		1b	Section 4 is not readable by I²C
3	Section 3	0b	Section 3 is readable by I²C

Bit	Name	Value	Description
		1b	Section 3 is not readable by I²C
2	Section 2	0b	Section 2 is readable by I²C
		1b	Section 2 is not readable by I²C
1	Section 1	0b	Section 1 is readable by I²C
		1b	Section 1 is not readable by I²C
0	Section 0	0b	Section 0 is readable by I²C
		1b	Section 0 is not readable by I²C

Note: Section 7 (default SRAM content) and Section 8 (Device configuration lock bytes) are always readable.

In case of not readable and/or not writeable, IC responds with an NACK from I²C perspective and 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.

Reading and writing the session registers via I²C can only be done with READ REGISTER and WRITE REGISTER commands.

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

Table 85. Session Register Location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Remark
NFC	I²C					
A0h	10A0h	STATUS_REG		RFU		Status Register (see Section 8.1.4.1)
A1h	10A1h	CONFIG_REG				Configuration (see Section 8.1.4.2)
A2h	10A2h	SYNC_DATA_BLOCK_REG		RFU		Block Address (see Section 8.1.4.3)
A3h	10A3h	PWM_GPIO_CONFIG_REG		RFU		PWM and GPIO Configuration(see Section 8.1.4.4)

Block Address NFC	Block Address I²C	Byte 0	Byte 1	Byte 2	Byte 3	Remark
A4h	10A4h	PWM0_ON_OFF_REG				PWM1 Configuration (see Section 8.1.4.5)
A5h	10A5h	PWM1_ON_OFF_REG				PWM1 Configuration (see Section 8.1.4.5)
A6h	10A6h	WDT_CONFIG_REG			RFU	Watch Dog Timer Configuration (see Section 8.1.4.6)
A7h	10A7h	EH_CONFIG_REG	RFU			Energy Harvesting Configuration (see Section 8.1.4.7)
A8h	10A8h	ED_CONFIG_REG	RFU			Event detection functionality (see Section 8.1.4.8)
A9h	10A9h	I2C_SLAVE_CONFIG_REG		RFU		I²C Slave Configuration (see Section 8.1.4.9)
AAh	10AAh	RESET_GEN_REG	RFU			Reset Register (see Section 8.1.4.10)
ABh	10ABh	ED_INTR_CLEAR_REG	RFU			Clear Event Detection (see Section 8.1.4.11)
ACh	10ACh	I2C_M_S_ADD_REG	I2C_M_LEN_REG	RFU	RFU	I²C Master Configuration (see Section 8.1.4.12)
ADh	10ADh	I2C_M_STATUS_REG	RFU			I²C Master Configuration (see Section 8.1.4.12)
AEh	10AEh	RFU				
AFh	10AFh	RFU				

8.1.4.1 Status register

Different status of NTAG 5 link 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 86. Status Register Location

Block Address NFC	Block Address I²C	Byte 0	Byte 1	Byte 2	Byte 3
A0h	10A0h	STATUS0_REG	STATUS1_REG	RFU	

Table 87. Status 0 Register

Bit	Name	Access		Value	Description
		NFC	I²C		
7	EEPROM_WR_BUSY	R	R	0b	EEPROM is not busy
				1b	EEPROM is busy (programming cycle ongoing)
6	EEPROM_WR_ERROR	R/W	R/W	0b	all data written successfully
				1b	EEPROM write error happened. This bit needs to be cleared.
5	SRAM_DATA_READY	R	R	0b	data not yet ready used in pass-through mode
				1b	data ready, used in pass-through mode
4	SYNCH_BLOCK_WRITE	R	R/W	0b	data has NOT been written to SYNCH_BLOCK
				1b	data had been written to SYNCH_BLOCK
3	SYNCH_BLOCK_READ	R	R/W	0b	data has NOT been read from SYNCH_BLOCK
				1b	data had been read from SYNCH_BLOCK
2	PT_TRANSFER_DIR	R	R	0b	I²C to NFC pass-through direction
				1b	NFC to I²C pass-through direction
1	VCC_SUPPLY_OK	R	R	0b	VCC supply not present
				1b	VCC supply available
0	NFC_FIELD_OK	R	R	0b	No NFC field present
				1b	NFC field present

Table 88. Status 1 Register

Bit	Name	Access		Value	Description
		NFC	I²C		
7	VCC_BOOT_OK	R	R	0b	VCC boot not done
				1b	VCC boot done
6	NFC_BOOT_OK	R	R	0b	NFC boot not done
				1b	NFC boot done
5	RFU	R	R	0b	
				1b	
4	GPIO1_IN_STATUS	R	R	0b	GPIO_1 input is LOW
				1b	GPIO_1 input is HIGH
3	GPIO0_IN_STATUS	R	R	0b	GPIO_0 input is LOW

Bit	Name	Access		Value	Description
		NFC	I²C		
				1b	GPIO_0 input is HIGH
2	RFU	R	R	0b	
				1b	
1	I2C_IF_LOCKED	R	R/W	0b	I²C Interface not locked by arbiter
				1b	Arbiter locked to I²C
0	NFC_IF_LOCKED	R	R	0b	NFC interface not locked by arbiter
				1b	Arbiter locked to NFC

8.1.4.2 Configuration register

On POR all CONFIG bits (see Section 8.1.3.13) 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 and/or I²C perspective.

Table 89. Configuration Register Location (CONFIG_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
A1h	10A1h	CONFIG_0_REG	CONFIG_1_REG	CONFIG_2_REG	RFU

Table 90. Configuration Definition (CONFIG_0_REG)

Bit	Name	Access		Value	Description
		NFC	I²C		
7	SRAM_COPY_EN	R	R	0b	SRAM copy on POR disabled
				1b	SRAM copy on POR enabled
6	RFU	R	R	0b	
5	DISABLE_NFC	R	R/W	0b	NFC interface enabled
				1b	NFC interface disabled, no response to NFC commands
4	RFU	R	R	0b	
3	RFU	R	R	0b	
2	RFU	R	R	0b	
1	RFU	R	R	0b	
0	AUTO_STANDBY_MODE_EN	R	R/W	0b	Normal Operation Mode
				1b	IC enters standby mode after boot if there is no RF field present automatically.

Table 91. Configuration Definition (CONFIG_1_REG)

Bit	Name	Access		Value	Description
		NFC acc.	I²C acc.		
7	RFU	R	R	0b	
6	RFU	R	R	0b	
5	USE_CASE_CONF	R	R	00b	I²C slave
				01b	I²C master
4				10b	GPIO/PWM
				11b	All host interface functionality disabled and pads are in 3-state mode
3	ARBITER_MODE	R	R/W	00b	Normal Mode
				01b	SRAM mirror mode
2				10b	SRAM passes through mode
				11b	SRAM PHDC mode
1	SRAM_ENABLED	R	R	0b	SRAM is not accessible
				1b	SRAM is accessible
0	PT_TRANSFER_DIR	R	R/W	0b	Data transfer direction is I²C to NFC
				1b	Data transfer direction is NFC to I²C

Table 92. Configuration Definition (CONFIG_2_REG)

Bit	Name	Access		Value	Description
		NFC acc.	I²C acc.		
7	GPIO1_IN	R	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	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	R	0b	Extended commands are disabled
				1b	Extended commands are supported
2	LOCK_BLOCK_COMMAND_ SUPPORTED	R	R	0b	Lock block commands are disabled
				1b	Lock block commands are supported
1	GPIO1_SLEW_RATE	R	R	0b	Low-Speed GPIO
				1b	High-Speed GPIO
0	GPIO0_SLEW_RATE	R	R	0b	Low-Speed GPIO
				1b	High-Speed GPIO

8.1.4.3 Synchronization block register

The terminator block maybe changed during one session from both interfaces (see Section 8.1.3.14). Both interfaces do have read and write access.

8.1.4.4 Pulse Width Modulation and GPIO configuration register

These session register bytes define the various configurations for GPIO/PWM use case (see Section 8.1.3.13). From NFC perspective IN_STATUS bits are read only, all others maybe changed during a session. From I²C perspective, all bits are read only. For details refer to Section 8.3.3 and Section 8.3.4.

Table 93. PWM and GPIO Configuration Register Location (PWM_GPIO_CONFIG_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
A3h	10A3h	PWM_GPIO_CONFIG_0_REG	PWM_CONFIG_1_REG	RFU	

Table 94. PWM and GPIO Configuration Register Definition (PWM_GPIO_CONFIG_0_REG)

Bit	Name	Access		Value	Description
		NFC acc.	I²C acc.		
7	SDA_GPIO1_OUT_STATUS	R/W	R	0b	Output status on pad is LOW
				1b	Output status on pad is HIGH
6	SCL_GPIO0_OUT_STATUS	R/W	R	0b	Output status on pad is LOW
				1b	Output status on pad is HIGH
5	SDA_GPIO1_SDA_IN_STATUS	R	R	0b	Input status
				1b	
4	SCL_GPIO0_IN_STATUS	R	R	0b	Input status
				1b	
3	SDA_GPIO1	R/W	R	0b	Output
				1b	Input
2	SCL_GPIO0	R/W	R	0b	Output
				1b	Input
1	SDA_GPIO1_PWM1	R/W	R	0b	GPIO
				1b	PWM
0	SCL_GPIO0_PWM0	R/W	R	0b	GPIO
				1b	PWM

Table 95. PWM and GPIO Configuration Register Definition (PWM_GPIO_CONFIG_1_REG)

Bit	Name	Access		Value	Description
		NFC Acc.	I^2C Acc.		
7	PWM1_PRESCALE	R/W	R	00b	Pre-scalar configuration for PWM1 channel
6					
5	PWM0_PRESCALE	R/W	R	00b	Pre-scalar configuration for PWM0 channel
4					
3	PWM1_RESOLUTION_CONF	R/W	R	00b	6-bit resolution
				01b	8-bit resolution
2				10b	10-bit resolution
				11b	12-bit resolution
1	PWM0_RESOLUTION_CONF	R/W	R	00b	6-bit resolution
				01b	8-bit resolution
0				10b	10-bit resolution
				11b	12-bit resolution

8.1.4.5 Pulse Width Modulation duty cycle register

The PWM duty cycle maybe changed during one session from NFC perspective (see Section 8.1.3.16).

As long as the I^2C slave use case is enabled, these settings can also be done from I^2C perspective.

8.1.4.6 Watch Dog Timer register

Watch Dog Timer register settings are read only (see Section 8.1.3.17).

8.1.4.7 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.

There is only read only access from I^2C perspective.

Details can be found in energy harvesting section (see Section 8.5).

Table 96. Energy Harvesting Configuration Register Location (EH_CONFIG_REG)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I^2C				
A7h	10A7h	EH_COFIG_REG	RFU		

Table 97. Energy Harvesting Register Value Definition EH_CONFIG_REG)

Bit	Name	Access		Value	Description
		NFC Acc.	I^2C Acc.		
7	EH_LOAD_OK	R	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	R		
3	EH_TRIGGER	R/W	R	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	R		
0	EH_ENABLE	R/W	R	0b	Energy Harvesting disabled (default)
				1b	Energy Harvesting enabled

8.1.4.8 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 from both interfaces. More details can be found in ED section (see Section 8.3.2).

8.1.4.9 I^2C slave register settings

I^2C slave settings can be read out from both interfaces.

I^2C interface can be disabled via NFC interface only. Repeated start functionality can be enabled via I^2C interface only.

Table 98. I^2C Slave Configuration Register Location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I^2C				
A9h	10A9h	I2C_SLAVE_ ADDR_REG	I2C_SLAVE_ CONFIG_REG	RFU	

Table 99. I²C Slave Configuration Definition (I2C_SLAVE_ADDR_REG)

Bit	Name	Access		Value	Description
		NFC	I²C		
7	RFU	R	R	0b	
6 to 0	I²2_SLAVE_ADDR	R	R	54h	I²C slave address used in slave configuration

Table 100. I²C Slave Configuration Definition (I2C_SLAVE_CONFIG_REG)

Bit	Name	Access		Value	Description
		NFC	I²C		
7 to 5	RFU	R	R	000b	
4	I2C_WDT_EXPIRED	R	R	0b	WDTdid not expire in previous transaction
				1b	Previous transaction was not successful. WDT expired. This bit gets cleared automatically, when new transaction is triggered.
3	I2C_SOFT_RESET	R/W	R/W	0b	Setting this bit to 1b, resets the I²C state machine and relases th SCL/ SDA lines. This bit gets cleared automatically.
2	I2C_S_REPEATED_ START	R	R/W	0b	Slave does not reset if repeated start is received (Default)
				1b	I²C slave resets internal state machine on repeated start
1	RFU	R	R	0b	
0	DISABLE_I²C (see Section 8.3.1.1.6)	R/W	R	0b	I²C interface enabled (default)
				1b	I²C interface disabled

8.1.4.10 System reset generation

System reset can be generated by both the interfaces 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 101. RESET_GEN_REG location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
AAh	10AAh	RESET_GEN_REG		RFU	

8.1.4.11 Clear event detection register

Event detection pin is cleared i.e. released when writing 01h to the Clear Event Detection Register from NFC or I²C interface. The bit gets cleared after releasing the ED pin automatically. Other values are RFU.

Table 102. ED_INTR_CLEAR_REG location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
ABh	10ABh	ED_INTR_ CLEAR_REG	RFU		

8.1.4.12 I²C master status registers

I²C master status can be checked by reading I²C master session register bits from NFC perspective. There is no write access to these registers. Details can be found in I²C master section.

NOTE: In I²C master mode there is no access to the registers from I²C perspective.

NOTE: I²C master is only available for NTP5332.

Table 103. I²C Master Configuration Register Location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
ACh	10ACh	I2C_M_S_ADD_REG	I2C_M_LEN_REG	RFU	RFU
ADh	10ADh	I2C_M_STATUS_REG	RFU		

Table 104. I²C Slave Address used in I²C master transaction (I2C_M_S_ADD_REG)

Bit	Name	Access		Value	Description
		NFC	I²C		
7	I2C_M_RS_EN	R	R	0b	STOP condition generated at the end of transaction
				1b	no STOP condition generated
6 to 0	I2C_M_S_ADD	R	R	00h	I²C slave of last addressed slave

Table 105. I²C Master Data Length Definition (I2C_M_LEN_REG)

Bit	Name	Value	Description
7 to 0	I2C_M_LEN_REG	all 0b	Codes the data length written to or read from I²C slave during last I²C transaction. Data length in bytes is I2C_M_LEN_REG plus 1.

Table 106. I²C Master Status Definition (I2C_M_STATUS_REG)

		Access			
Bit	Name	NFC	I²C	Value	Description
7 to 4	RFU	R	R	0000b	
3	I2C_M_WDT_EXPIRED	R	R	0b	WDT did not expire in last transaction
				1b	WDT expired in last transaction. This bit resets automatically, when new transaction is triggered.

		Access			
Bit	Name	NFC	I²C	Value	Description
2 to 1	I2C_M_TRANS_STATUS	R	R	00b	Reset value, automatically when new transaction starts
				01b	Address NAK
				10b	Data NAK
				11b	Transaction successful
0	I2C_M_BUSY	R	R	0b	I²C Master interface ready. No transaction ongoing
				1b	I²C Master interface busy. Transaction ongoing

8.1.5 SRAM

For frequently changing data, a volatile memory of 256 bytes with unlimited write endurance is built in. The 256 bytes are mapped in a similar way as done in the EEPROM, i.e., 256 bytes are seen as 64 pages of 4 bytes.

SRAM is only available when supplied by V_{CC} and SRAM_ENABLE bit is set to 1b.

The SRAM can be mirrored in the User Memory from block 00h to 3Fh for access from both interfaces as illustrated in the table below. This allows using NFC Forum read and write commands to access the SRAM.

The lock block condition (e.g. user EEPROM blocks are set to read-only) is not valid for the mirrored SRAM.

The access conditions (e.g. first blocks of user EEPROM are password protected) are valid for the mirrored SRAM, too, for both interfaces.

The access conditions for READ SRAM and WRITE SRAM commands can be restricted with SRAM_CONF_PROT security bits.

From I²C perspective, SRAM is located in blocks 2000h to 203Fh and can be accessed at any time without any protection.

NOTE: SRAM values are not initialized during boot and may have arbitrary data.

Table 107. SRAM mirroring

Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
NFC	I²C					
00h	0000h	SRAM				When SRAM is mirrored to user memory, READ and WRITE commands address SRAM
01h	0001h	:	:	:	:	
02h	0002h					
03h	0003h					
:	:					
3Fh	003Fh	SRAM				
40h	0040h	EEPROM				From block 40h onwards, READ and WRITE commands always address EEPROM
:	:	:	:	:	:	
1FEh	01FEh	EEPROM				

Block Address		Byte 0	Byte 1	Byte 2	Byte 3	Description
NFC	I^{2}C					
1FFh	N/A	C0	C1	00h	PROT	Counter

In the pass-through mode, READ and WRITE SRAM commands should be used to transfer data between the two interfaces.

After POR the SRAM can be pre-loaded with default data (e.g. NDEF message) depending on SRAM_COPY_ENABLE bit in CONFIG register. If SRAM_COPY_ENABLE bit and SRAM_ENABLE both are set to 1b, then the copy feature will be triggered after POR. The startup time depends upon the number of bytes (maximum 64) to be copied.

In the table below, an example is illustrated where 48 bytes are copied to the SRAM on POR.

Table 108. SRAM mirroring with default content

Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
0	SRAM_DEF00	SRAM_DEF01	SRAM_DEF02	SRAM_DEF03	When SRAM is mirrored and SRAM_COPY_BYTES is equal to 30h, 48 bytes will be copied to SRAM after POR automatically
:	...SRAM_DEF...				
11	SRAM_DEF44	SRAM_DEF45	SRAM_DEF46	SRAM_DEF47	
12	SRAM				Rest of mirrored SRAM will be random data
:	:	:	:	:	
63	SRAM				
64	EEPROM				From block 64 onwards again EEPROM will be addressed
:	:	:	:	:	
510	EEPROM				
511	C0	C1	00h	PROT	Counter

Table 109. SRAM COPY BYTES (SRAM_COPY_BYTES)

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I^{2}C				
3Ch	103Ch	WDT_CONFIG		WDT_ENABLE	SRAM_COPY_BYTES

Table 110. SRAM_COPY_BYTES Definition

Bit	Name	Description
7 to 6	RFU	RFU
5 to 0	SRAM_COPY_BYTES	6-bit length field. Defines the number of bytes (SRAM_COPY_BYTES + 1) to be copied from CONFIG memory to SRAM at startup. Maximum is 3Fh. Higher values are RFU. Default all bits are 0b.

Table 111. SRAM Default Content location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I^2C				
45h	1045h	SRAM_DEF00	SRAM_DEF01	SRAM_DEF02	SRAM_DEF03
...	...	...SRAM_DEF...			
54h	1054h	SRAM_DEF60	SRAM_DEF61	SRAM_DEF62	SRAM_DEF63

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.

Supported bitrates for different modes and communication directions are listed in tables below.

Table 112. Bit rates from reader to tag

Mode	Condition	1.66 kbps	26 kbps
passive	NFC only	yes	yes
passive	V_{CC} supplied	yes	yes

Table 113. Bit rates from tag to reader

Mode	Condition	6 kbps	26 kbps	53 kbps
passive	single subcarrier	yes	yes	yes
passive	dual subcarrier	yes	yes	no

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 link.

The SELECTED SECURE state is only available for NTP5332, when AES security is enabled.

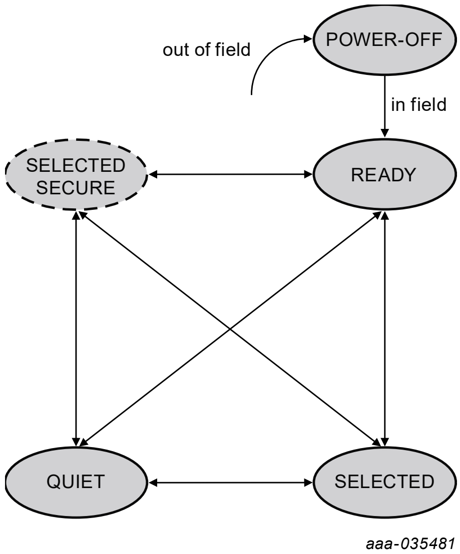


Figure 6. State Machine and State Transitions

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 link goes to POWER-OFF state.

POWER-OFF state will be left to READY state no later than 1 ms after NTAG 5 link 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 Transitions between READY and SELECTED SECURE state

Transition from READY to SELECTED SECURE state is done when

- mutual authentication with AUTHENTICATE command with a matching UID was successful

8.2.2.2.4 Commands which stay in READY state

NTAG 5 link 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 Transitions between SELECTED and SELECTED SECURE state

Transition from SELECTED to SELECTED SECURE state is done by

- mutual authentication with AUTHENTICATE command with Select_Flag set was successful

8.2.2.3.4 Transitions between SELECTED and NFC PRIVACY mode

Transition from SELECTED to NFC PRIVACY mode is done by

- receiving an ENABLE NFC PRIVACY command

8.2.2.3.5 Commands which stay in SELECTED state

NTAG 5 link stays in SELECTED state when

- receiving any other command where Select_Flag is set

8.2.2.4 SELECTED SECURE state

8.2.2.4.1 Transitions between SELECTED SECURE and READY state

Transition from SELECTED SECURE 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
- receiving a CHALLENGE command
- receiving a new AUTHENTICATE command

8.2.2.4.2 Transitions between SELECTED SECURE and QUIET state

Transition from SELECTED to QUIET state is done when

- receiving a STAY QUIET command with a matching UID

8.2.2.4.3 Transitions between SELECTED SECURE and SELECTED state

Transition from SELECTED to SELECTED SECURE state is done by

- receiving a SELECT command with a matching UID

8.2.2.4.4 Commands which stay in SELECTED SECURE state

NTAG 5 link stays in SELECTED SECURE state when

- receiving READBUFFER command
- receiving any other command where Select_Flag is set

8.2.2.5 QUIET state

8.2.2.5.1 Transitions between QUIET and READY state

Transition from QUIET to READY state is done by

- receiving a RESET_TO_READY command

8.2.2.5.2 Transitions between QUIET and SELECTED state

Transition from QUIET to SELECTED state is done by

- receiving a SELECT command with a matching UID

8.2.2.5.3 Transitions between QUIET and SELECTED SECURE state

Transition from QUIET to SELECTED SECURE state is done when

- mutual authentication with AUTHENTICATE command with a matching UID was successful

8.2.2.5.4 Commands which stay in QUIET state

NTAG 5 link 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 114. NFC command set supported by NTAG 5 link

Code	ISO/IEC 15693	NFC Forum T5T	Command name
01h	Mandatory	Mandatory	INVENTORY (see ISO/IEC 15693 and Digital Protocol)

Code	ISO/IEC 15693	NFC Forum T5T	Command name
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)
30h	Optional	Mandatory when supporting 2 byte addressing	EXTENDED READ SINGLE BLOCK (see ISO/IEC 15693 and Type 5 Tag - EXTENDED_READ_SINGLE_BLOCK_REQ)
31h	Optional	Mandatory when supporting 2 byte addressing in READ/ WRITE state	EXTENDED WRITE SINGLE BLOCK (see ISO/IEC 15693 and Type 5 Tag - EXTENDED_WRITE_SINGLE_BLOCK_REQ)
32h	Optional	Optional	EXTENDED LOCK BLOCK (see ISO/IEC 15693 and Type 5 Tag - EXTENDED_LOCK_SINGLE_BLOCK_REQ)
33h	Optional	Optional	EXTENDED READ MULTIPLE BLOCK (ISO/IEC 15693 and Type 5 Tag - EXTENDED_READ_MULTIPLE_BLOCK_REQ)
35h	Optional	Not defined	AUTHENTICATE (see ISO/IEC 15693) is only available in AES mode
39h	Optional	Not defined	CHALLENGE (see ISO/IEC 15693) is only available in AES mode
3Ah	Optional	Not defined	READBUFFER (see ISO/IEC 15693) is only available in AES mode
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 8.2.3.5.1)
A1h	Custom	Not defined	FAST INVENTORY READ (see Section 8.2.3.5.2)

Code	ISO/IEC 15693	NFC Forum T5T	Command name
A2h	Custom	Not defined	SET EAS (see Section 8.2.3.9.5)
A3h	Custom	Not defined	RESET EAS (see Section 8.2.3.9.6)
A4h	Custom	Not defined	LOCK EAS (see Section 8.2.3.9.7)
A5h	Custom	Not defined	EAS ALARM (see Section 8.2.3.9.8)
A6h	Custom	Not defined	PROTECT EAS/AFI (see Section 8.2.3.9.9)
A7h	Custom	Not defined	WRITE EAS ID (see Section 8.2.3.9.10)
ABh	Custom	Not defined	GET NXP SYSTEM INFORMATION (see Section 8.2.3.9.14)
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 8.2.3.7.1)
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)
C2h	Custom	Not defined	PICK RANDOM UID (see Section 8.2.3.9.15)
D2h	Custom	Not defined	READ SRAM (see Section 8.2.3.6.1)
D3h	Custom	Not defined	WRITE SRAM (see Section 8.2.3.6.2)
D4h	Custom	Not defined	WRITE I2C (see Section 8.2.3.8.1)
D5h	Custom	Not defined	READ I2C (see Section 8.2.3.8.2)

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 link offers

- INVENTORY READ in extended mode (see Section 8.2.3.5.1)

- FAST INVENTORY READ in extended mode (see Section 8.2.3.5.2)
- AUTHENTICATE to move to SELECTED SECURE state (see Section 8.2.3.4.4)

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 link 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
- Keys can only be read separately if "NOT active" or after a mutual authentication with a key with the Crypto Config privilege set in "active" state
  Key0: block 20h-23h
  Key1: block 24h-27h
  Key2: block 28h-2Bh
  Key3: block 2Ch-2Fh
- rest of configuration memory

Only Option_flag = 0b is supported.

Table 115. 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 116. 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 117. 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 link 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 118. 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 119. WRITE CONFIG response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 120. 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 link 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 121. 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 122. GET RANDOM NUMBER response format when Error_flag is NOT set

Flags	Random_Number	CRC16
8 bits	16 bits	16 bits

Table 123. 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 124. 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 125. 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 126. SET PASSWORD response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 127. 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 125.

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 128. 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 129. WRITE PASSWORD response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 130. 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 125).

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 131. 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 132. LOCK PASSWORD response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 133. 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 link 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 134. 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 135. 64 BIT PASSWORD PROTECTION response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 136. 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 NFC_PP_AREA_0H 14h.

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

Table 137. 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					
:	:	:	:	:	
1FFh	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 access conditions and the protection pointer address can be changed under the following circumstances for AES mode:

- The Global Crypto Header is set to "Deactivated" or
- if the Global Crypto Header is not set to "Deactivated" and a valid mutual authentication with a key with read and write privileges has been executed before and 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 138. 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 FFh. The block containing the 16-bit counter is excluded from the standard user memory protection scheme.*

Table 139. 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 140. Protection status bits definition in plain password mode

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 141. Protection status bits definition in AES mode

WH/WL	RH/RL	Protection
0b	0b	Public
0b	1b	Read and Write protected: Mutual authentication with a key with read privilege is required
1b	0b	Write protected: Mutual authentication with a key with write privilege is required
1b	1b	Read and Write protected: Mutual authentication with a key with read and write privileges is required

Table 142. PROTECT PAGE response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 143. 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 8.2.3.9.14).

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 Global Crypto Header is set to "Deactivated".
- If the Global Crypto Header is not set to "Deactivated" and a valid mutual authentication with a key with read and write privileges has been executed before.

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 144. 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 145. LOCK PAGE PROTECTION CONDITION response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 146. 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

In plain password mode the DESTROY command disables NTAG 5 link if the destroy password is correct. This command is irreversible and NTAG 5 link will never respond to any command neither NFC nor I^2C 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.

NOTE: In AES mode, Mutual Authentication with Purpose_MAM2 = 1011b needs to be executed to destroy NTAG 5 link.

Table 147. 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 148. DESTROY response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 149. 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 in plain password mode enables NFC PRIVACY mode (see Section 8.7) for NTAG 5 link 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.

NOTE: In AES mode, Mutual Authentication with Purpose_MAM2 = 1001b needs to be executed to enable the NFC PRIVACY mode for NTAG 5 link.

Table 150. 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 151. ENABLE NFC PRIVACY response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 152. 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 link 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 153. 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 154. DISABLE NFC PRIVACY response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 155. 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 AES Authentication

8.2.3.4.1 Introduction

NXP implements a scalable security approach. This means, during lifetime the security level may be changed. In production, NXP configures the IC, that plain password mode is enabled. With the DEV_SEC_CONFIG byte (see Table 66) AES mutual authentication may be activated. Only in case NFC Security is set to AES mode following commands and AES mutual authentication is enabled. To lock the security level, the Security Lock bits need to be set to 010b (see Table 66).

NOTE: AES authentication mode and this flexibility is only available for NTP5332.

8.2.3.4.2 PROTECT PAGE

See Section 8.2.3.3.6

8.2.3.4.3 LOCK PAGE PROTECTION CONDITION

See Section 8.2.3.3.7

8.2.3.4.4 AUTHENTICATE

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

Command code = 35h

CSI code= 00h (AES Crypto Suite)

The AUTHENTICATE command allows the interrogator to perform the following authentication procedures as defined in ISO/IEC 15693:

- Tag Authentication (TAM1)

- Mutual Authentication (MAM1, MAM2)

After receiving a valid AUTHENTICATE command, NTAG 5 link calculates the response and as soon as the calculation is finalized, the response with the result of the crypto calculation (b3 flag is set) is sent. Only for tag authentication the calculation result is additionally stored in the response buffer (b2 flag is set).

NTAG 5 link supports the Crypto Suite AES128 as defined in ISO/IEC 29167-10.

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

Table 156. AUTHENTICATE request format

Flags	AUTHENTICATE	UID	CSI	Message	CRC16
8 bits	8 bits	64 bits (optional)	8 bits	Depending on TAM1 (96 bit), MAM1 (96 bit) or MAM2 (136 bit)	16 bits

Table 157 defines the response of NTAG 5 link to an AUTHENTICATE command.

For more detailed information, refer to ISO/IEC 29167-10.

Table 157. AUTHENTICATE response format when Error_flag is NOT set(in process reply)

Flags	Barker Code	TResponse	CRC16
8 bits (b2 and b3 is set)	8 bits (Done flag is set)	Depending on TAM1 (128 bit), MAM1(176 bit) or MAM2 (0 bit)	16 bits

Table 158. AUTHENTICATE response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

Tag Authentication (TAM1)

Table 159 defines the message within the AUTHENTICATE command for tag authentication (TAM1).

For more detailed information, refer to ISO/IEC 29167-10.

Table 159. Message format for TAM1

	AuthMethode	CustomData	TAM1_RFU	KeyID	IChallenge_TAM1
# of bits	2	1	5	8	80
Description	00b	0b	00000b	[7:0]	random interrogator challenge

Table 160 defines the response of NTAG 5 link to an AUTHENTICATE command.

For more detailed information, refer to ISO/IEC 29167-10.

Table 160. TResponse for TAM1

TResponse TAM1 (128 bit)
AES-ECB-ENC(Key[KeyID].ENC_key,C_TAM1[15:0] || TRnd_TAM1[31:0] || IChallenge_TAM1[79:0])

Mutual Authentication (MAM1, MAM2)

The mutual authentication is a two-pass authentication procedure. The first AUTHENTICATE command (MAM1) is executing the tag authentication and gets the challenge from NTAG 5 link. The second AUTHENTICATE command (MAM2) is executing the interrogator authentication.

Table 161 defines the message within the AUTHENTICATE command for mutual authentication (MAM1).

For more detailed information, refer to ISO/IEC 29167-10.

Table 161. Message format for MAM1

	AuthMethode	Step	MAM1_RFU	KeyID	IChallenge_MAM1
# of bits	2	2	4	8	80
Description	10b	00b	0000b	[7:0]	random interrogator challenge

Table 162 defines the response of NTAG 5 link to an AUTHENTICATE command for MAM1.

For more detailed information, refer to ISO/IEC 29167-10.

Table 162. TReseponse for MAM1

TResponse MAM1 (176 bit)
AES-ECB-ENC(Key[KeyID].ENC_key,C_TAM1[15:0] || TChallenge_MAM1[31:0] || IChallenge_TAM1[79:0]) || TChallenge_MAM1[79:32]

Table 163 defines the message within the AUTHENTICATE command for mutual authentication (MAM2).

For more detailed information, refer to ISO/IEC 29167-10.

Table 163. Message format for MAM2

	AuthMethode	Step	MAM2_RFU	IResponse
# of bits	2	2	4	128
Description	10b	01b	0000b	AES-DEC(, Key[KeyID].ENC_key,C_MAM2[11:0] || Purpose_MAM2[3:0] || IChallenge_MAM1[31:0] || TChallenge_MAM1[79:0])

Table 164 defines valid values for Purpose_MAM2 for NTAG 5 link.

Table 164. Definition of Purpose_MAM2

	Purpose_MAM2	Description
Standard	0000b	Mutual Authentication
	all other 0xxxb	RFU
NXP specific	1000b	Disable NFC Privacy Mode until NFC field reset
	1001b	Enable NFC Privacy Mode
	1010b	Disable NFC Privacy Mode
	1011b	Destroy NTAG 5 link
	all other 1xxxb	RFU

Table 165 defines the response of NTAG 5 link to an AUTHENTICATE command for MAM2.

For more detailed information, refer to ISO/IEC 29167-10.

Table 165. TReseponse for MAM2

TResponse MAM2 (0 bit)
Empty message (no data)

8.2.3.4.5 CHALLENGE

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

Command code = 39h

CSI code= 00h (AES Crypto Suite)

The CHALLENGE command transmits the message (challenge) to NTAG 5 link to authenticate as defined in ISO/IEC 15693.

The CHALLENGE command can only be executed in the READY state and in not addressed mode.

After receiving a valid CHALLENGE command, NTAG 5 link starts with the crypto calculation.

If the calculation is finalized, NTAG 5 link will respond to a valid READBUFFER command with the result of the crypto calculation based on the previous CHALLENGE command message.

NTAG 5 link supports the Crypto Suite AES128 as defined in ISO/IEC 29167-10.

Only Option_flag = 0b is supported.

Table 166. CHALLENGE request format

Flags	CHALLENGE	UID	CSI	Message	CRC16
8 bits	8 bits	64 bits (optional)	8 bits	96 bits	16 bits

Table 167 defines the message within the CHALLENGE command.

For more detailed information, refer to ISO/IEC 29167-10.

Table 167. Message format

	AuthMethode	CustomData	TAM1_RFU	KeyID	IChallenge_TAM1
# of bits	2	1	5	8	80
Description	00b	0b	00000b	[7:0]	random interrogator challenge

No response is sent on a CHALLENGE command.

For more detailed information, refer to ISO/IEC 29167-10.

8.2.3.4.6 READBUFFER

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

Command code = 3Ah

The READBUFFER command allows the interrogator to request the crypto calculation result based on a valid previous CHALLENGE command from NTAG 5 link.

NTAG 5 link supports the Crypto Suite AES128 as defined in ISO/IEC 29167-10.

Only Option_flag = 0b is supported.

Table 168. READBUFFER request format

Flags	READBUFFER	UID	CRC16
8 bits	8 bits	64 bits (optional)	16 bits

For more detailed information, refer to ISO/IEC 29167-10.

Table 169 and Table 170 defines the response of NTAG 5 link to a READBUFFER command.

For more detailed information, refer to ISO/IEC 29167-10.

Table 169. READBUFFER response format when Error_flag is NOT set

Flags	TResponse	CRC16
8 bits	128 bits (see Table 122)	16 bits

Table 170. TResponse

TResponse
AES-ECB-ENC(Key[KeyID].ENC_key,C_TAM1[15:0] || TRnd_TAM1[31:0] || IChallenge_TAM1[79:0])

Table 171. READBUFFER response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.5 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
- EXTENDED READ SINGLE BLOCK
- EXTENDED WRITE SINGLE BLOCK
- EXTENDED LOCK BLOCK
- EXTENDED READ MULTIPEL BLOCKS up to 3Fh blocks

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

8.2.3.5.1 INVENTORY READ

Command code = A0h

When receiving the INVENTORY READ request, NTAG 5 link 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 8.2.3.5.1.1)
- 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 8.2.3.5.1.2)

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 8.2.3.5.1.3).

8.2.3.5.1.1 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 link 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 172. 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 link 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 8.2.3.5.1.3).

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

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

Table 173. INVENTORY READ response format: Option flag logic 0b

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

NTAG 5 link 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 174. 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 link 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 175. 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 link

8.2.3.5.1.2 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 176. Inventory Read (extended mode) request format

Flags	INVENTOR READ	Manuf. code	AFI	Mask Length	ext.Optio ns	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 link 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 8.2.3.5.1.3).

Table 177. 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 link 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 link 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 link 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 178. 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 179. 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 link

8.2.3.5.1.3 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.*

8.2.3.5.2 FAST INVENTORY READ

Command code = A1h

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

The data rate in the direction NTAG 5 link 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 link and the time between the rising edge of the EOF from the reader to NTAG 5 link 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.

8.2.3.6 SRAM operations

When SRAM is mirrored to user EEPROM address space, standard READ BLOCK and WRITE BLOCK commands can be used. To have a more efficient way to access the 256 bytes SRAM, READ SRAM and WRITE SRAM are implemented

8.2.3.6.1 READ SRAM

Command code = D2h

This command can only be used, when NTAG 5 link is powered via V_{CC} end SRAM_ENABLE bit (see Table 38) is set to 1b.

When receiving READ SRAM desired SRAM blocks will be returned.

NTAG 5 link returns only the requested blocks. The blocks are numbered from 00h to 3Fh. The number of blocks in the request is one less than the number of blocks that NTAG 5 link returns in its response. EXAMPLE: A value of 06h in the "Number of Blocks" field requests to read 7 blocks. A value of 00h requests to read a single block from SRAM.

If SRAM is read or write protected a valid authentication needs to be proceeded.

It is recommended to use this command in pass-through mode.

Only Option_flag = 0b is supported.

Table 180. READ SRAM request format

Flags	READ SRAM	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 181. READ SRAM response format when Error_flag is NOT set

Flags	Block Security Status (optional) + Data	CRC16
8 bits	(Number of Blocks+1) x 32 bits Data	16 bits

Block Security Status and Data bytes repeat as a duple.

Table 182. READ SRAM response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.6.2 Write SRAM

Command code = D3h

This command can only be used, when NTAG 5 link is powered via V_{CC} end SRAM_ENABLE bit (see Table 38) is set to 1b.

When receiving WRITE SRAM desired SRAM blocks will be written to the SRAM. It is recommended to use this command in pass-through mode because of performance reasons.

If SRAM is write protected a valid authentication needs to be preceded.

The blocks are numbered from 00h to 3Fh. The number of blocks in the request is one less than the number of blocks that the VICC shall write. E.g., to write one block to SRAM Number of Blocks is coded as 00h.

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

Table 183. WRITE SRAM request format

Flags	WRITE SRAM	IC Mfg code	UID	Block Address	Number of blocks	Data	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits	8 bits	(Number of blocks + 1) times 32 bits	16 bits

Table 184. WRITE SRAM response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 185. WRITE SRAM response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.7 Originality Signature

8.2.3.7.1 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 8.8.

Only Option_flag = 0b is supported.

Table 186. READ SIGNATURE request format

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

Table 187. READ SIGNATURE response format when Error_flag is NOT set

Flags	Originality Signature	CRC16
8 bits	256 bits	16 bits

Table 188. 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.

8.2.3.8 I²C Transparent Channel

NTAG 5 link offers an NFC to I²C bridge. With this mode, different I²C slaves (e.g., sensors) can be connected without a microcontroller. There shall be no other active I²C master on the same bus. The needed power for the sensors may be provided with NTAG 5 link energy harvesting capability.

I²C master communication can do maximum 256 bytes to read from, and write to the connected slave.

I²C master clock speed needs to be configured with I2C_MASTER_SCL_LOW and I2C_MASTER_SCL_HIGH (see Table 62). I²C slave address will be selected directly within WRITE I²C and READ I²C command.

SRAM needs to be enabled by setting SRAM_ENABLE bit (see Table 38) to 1b.

Basic principle for triggering an I²C write to the connected slave is illustrated in the figure below. NFC reader will get the response immediately, and then polls for the status of the I²C transaction (see Table 106).

Details of the NFC command WRITE I²C can be found in Section 8.2.3.8.1.

NOTE: This feature is only available for NTP5332.

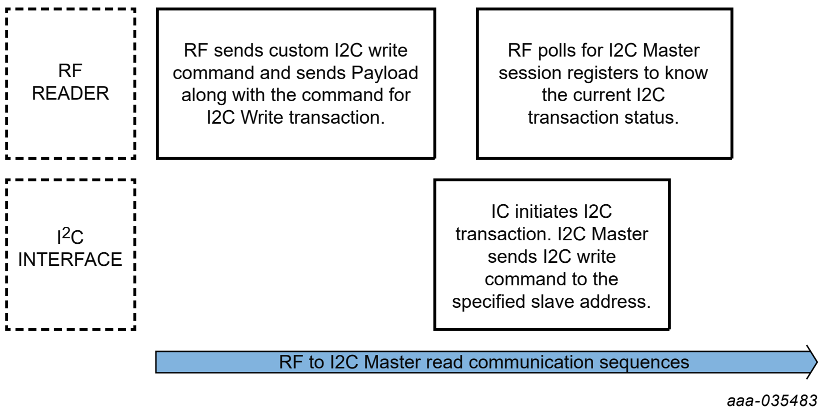


Figure 7. I²C Master write principle

Basic principle for triggering an I²C read and getting the response of the connected slave is illustrated in the figure below. Again the NFC reader will get a response immediately, and then polls for the status of the I²C transaction (see Table 106). Finally the result can be read from SRAM.

Details of the NFC command READ I²C can be found in Section 8.2.3.8.2

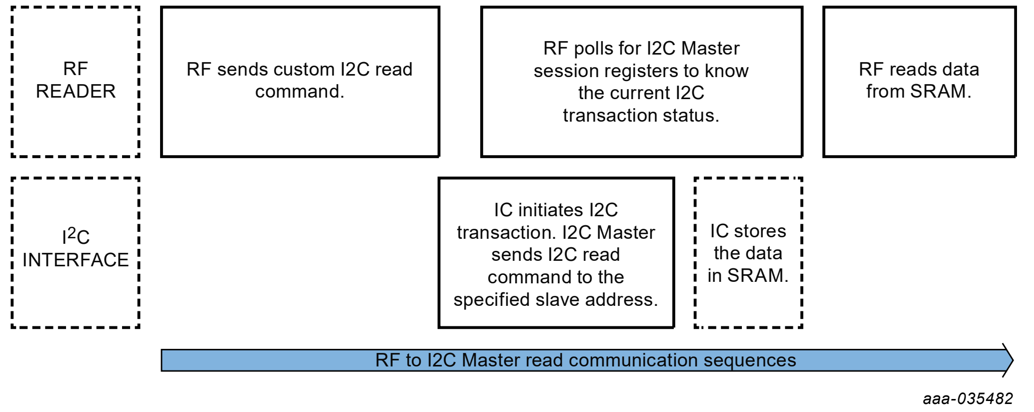


Figure 8. I²C Master read principle

8.2.3.8.1 WRITE I²C

Command code = D4h

WRITE I²C command is used to trigger an I²C master write command (R/W̄ bit is 0b) on the I²C bus.

Command parameters:

- I²C param contains I²C slave address and STOP condition option.
- Data length N byte codes the length of bytes to be sent to the slave. N+1 bytes need to be put in the Data field and will be sent to the slave. E.g., to send one byte, 00h needs to be coded.
- Data field contains the data to be sent to the I²C slave. Minimum number of bytes is 1 byte, maximum is 256 bytes.

If SRAM is read or write protected a valid authentication needs to be preceded.

Response to this command will follow immediately.

To check the status and result of the WRITE I²C command, I²C Master Status Registers ADh should be checked (see Table 106).

Only Option_flag = 0b is supported.

Table 189. WRITE I²C request format

Flags	WRITE I²C	Manuf. code	UID	I²C param	Data length N	Data	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	8 bits	8 bits	(N+1) x 8 bits	16 bits

Table 190. I²C param byte

I²C param bit	Status	Value	Description
7	Disable STOP condition	0b	STOP condition will be generated at the end of transaction
		1b	STOP condition will be omitted at the end of transaction
6 to 0	I²C Address	xxh	7-bit I²C slave address of connected slave

Table 191. WRITE I^2C response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 192. WRITE I^2C response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.8.2 READ I^2C

Command code = D5h

READ I^2C command is used to trigger an I^2C master read command (R/$\overline{W}$ bit is 1b) on the I^2C bus.

Command parameters:

- I^2C param contains I^2C address and STOP condition option
- Data length N byte codes the length of bytes to be read from the slave. N+1 bytes will be read from the slave. E.g., to read one byte 00h needs to be coded. Maximum is FFh, which means 256 bytes will be read.

Response to this command will follow immediately.

The status register Table 106 indicates when the I^2C read command is completed.

To get the response of the addressed I^2C slave device, the READ SRAM (see Section 8.2.3.6.1) command is used.

Only Option_flag = 0b is supported.

Table 193. READ I^2C request format

Flags	READ I^2C	IC Mfg code	UID	I^2C param	Data length	CRC16
8 bits	8 bits	8 bits	64 bits optional	8 bits	8 bits	16 bits

Table 194. I^2C param byte

Bit	Status	Value	Description
7	Disable STOP condition	0b	STOP condition will be generated at the end of transaction
		1b	STOP condition will be omitted at the end of transaction
6 to 0	I^2C Address	xxh	7-bit I^2C slave address of connected slave

Table 195. READ I^2C response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 196. READ I²C response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.9 Other

8.2.3.9.1 WRITE AFI

As defined in ISO/IEC 15693.

8.2.3.9.2 LOCK AFI

As defined in ISO/IEC 15693.

8.2.3.9.3 WRITE DSFID

As defined in ISO/IEC 15693.

8.2.3.9.4 LOCK DSFID

As defined in ISO/IEC 15693.

8.2.3.9.5 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.

If AES authentication scheme is enabled and EAS mode is protected, a valid mutual authentication with a key with the EAS/AFI privilege set has to executed before.

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 197. SET EAS request format

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

Table 198. SET EAS response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 199. SET EAS response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.9.6 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.

If AES authentication scheme is enabled and EAS mode is protected a valid mutual authentication with a key with the EAS/AFI privilege set has to executed before.

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 200. RESET EAS request format

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

Table 201. RESET EAS response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 202. RESET EAS response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.9.7 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.

If AES authentication scheme is enabled and EAS mode is protected a valid mutual authentication with a key with the EAS/AFI privilege set has to executed before.

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 203. LOCK EAS request format

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

Table 204. LOCK EAS response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 205. LOCK EAS response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.9.8 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 206. 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 207. 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 208. EAS ALARM Response format(Option flag logic 1)

Flags	EAS ID value	CRC16
8 bits	16 bits	16 bits

Table 209. 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 link in the QUIET state will not respond to an EAS ALARM command except the addressed flag is set.*

8.2.3.9.9 PROTECT EAS/AFI

Command code = A6h

In plain password mode 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.

In AES mode, the PROTECT EAS/AFI command enables the protection for EAS and/or AFI if a valid mutual authentication with the EAS/AFI privilege has been executed before.

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 210. 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 211. PROTECT EAS/AFI response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 212. PROTECT EAS/AFI response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.9.10 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.

If AES mode is enabled and the EAS is protected a valid mutual authentication with a key with the EAS/AFI privilege set has to executed before.

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 213. 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 214. WRITE EAS ID response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 215. WRITE EAS ID response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.9.11 GET MULTIPLE BLOCK SECURITY STATUS

As defined in ISO/IEC 15693.

8.2.3.9.12 GET SYSTEM INFORMATION

As defined in ISO/IEC 15693.

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

8.2.3.9.13 EXTENDED GET SYSTEM INFORMATION

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

Command code = 3Bh

8.2.3.9.14 GET NXP SYSTEM INFORMATION

Command code = ABh

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

Table 216. 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 217. 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 218. 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 219. Lock bits byte

Bit	Name	Value	Description
7 to 4	RFU	0b	
3	NFC_PP_AREA_0H and NFC_PPC	0b	NFC_PP_AREA_0H and NFC_PPC is NOT locked
		1b	NFC_PP_AREA_0H and NFC_PPC is locked
2	DSFID	0b	DSFID is NOT locked
		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 link. With this response, it is possible to distinguish the different NTAG 5 family members.

Table 220. 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 8.2.3.5.1)	1b
5	INVENTORY READ EXT	Extended mode supported by INVENTORY READ command (see Section 8.2.3.5.1)	1b
4	AFI PROT	AFI protection supported (see Section 8.2.3.9.9)	1b
3	EAS PROT	EAS protection supported (see Section 8.2.3.9.9)	1b
2	EAS ID	EAS ID supported by EAS ALARM command (see Section 8.2.3.9.10)	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 221. Feature flags byte 1

Bit	Name	Description	NTAG 5	
			NTP5210	NTP5312 NTP5332 NTA5332
7	HIGH BITRATES	high bitrates supported (see Section 8.2)	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 222. 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 (see Section 8.1.3.8)	0b	1b
1	MUTUAL AUTH	Mutual Authentication feature supported (see Section 8.6.4)	0b	1b

Bit	Name	Description	NTAG 5	
			NTP5210 NTP5312	NTP5332 NTA5332
0	TAG AUTH	Tag Authentication feature supported (see Section 8.6.4)	0b	1b

Table 223. 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 GPIO/ED host interface 10b RFU 11b GPIO and I²C host interface	01b	11b	
4	RFU		0b		
3 to 0	NUM KEYS	Number of Keys	0h		4h

Table 224. GET NXP SYSTEM INFORMATION response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

8.2.3.9.15 PICK RANDOM ID

Command code = C2h

In AES mode the PICK RANDOM ID commandinstructs NTAG 5 link in NFC PRIVACY Mode to generate a random ID. After a valid PICK RANDOM ID command, the IC will respond with that random ID on following INVENTORY commands or GET SYSTEM INFORMATION command until an RF reset to allow an anti-collision procedure.The random ID will include the CID to identify the group-password or group-key to disable the privacy mode.

Only Option_flag = 0b is supported.

Table 225. PICK RANDOM ID request format

Flags	Pick Random ID	Manuf. code	UID	CRC16
8 bits	8 bits	8 bits	64 bits (optional)	16 bits

Table 226. PICK RANDOM ID response format when Error_flag is NOT set

Flags	CRC16
8 bits	16 bits

Table 227. PICK RANDOM ID response format when Error_flag is set

Flags	Error Code	CRC16
8 bits	8 bits	16 bits

After a successful PICK_RANDOM_ID the NTAG 5 link will respond on an INVENTORY command with a random ID as defined in the table below.

Table 228. Random ID

MSB						LSB
63:56	55:48	47:40	39:32	31:24	23:16	15:0
E0h	04h	00h	00h	CID_1	CID_0	16-bit random ID

8.2.4 Data integrity

Following mechanisms are implemented in the contactless communication link between reader and NTAG 5 link 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 link 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 link remains silent
- Addressed or selected Mode
  NTAG 5 link 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 link remains silent.
– Addressed or SELECTED Mode
  NTAG 5 link responds with error code 0Fh (no information given, or error code not supported).

8.3 Wired Interface

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

8.3.1 I²C interface

The definition of the I²C interface is according to the UM10204. The details of slave and master mode are described in Section 8.3.1.1 and Section 8.3.1.2.

NOTE: I²C master mode is only available for NTP5332.

8.3.1.1 Slave mode

For details about I²C interface, refer to UM10204.

The I²C slave interface supports both standard (up to 100 kHz) and fast mode (up to 400 kHz) communication speeds for both read and write. Implementation will be a so-called asynchronous interface which uses the SCL clock for the I²C protocol handling after which the data is synchronized to the system clock for memory access. NTAG 5 link can be used in multi-master/multi-slave applications.

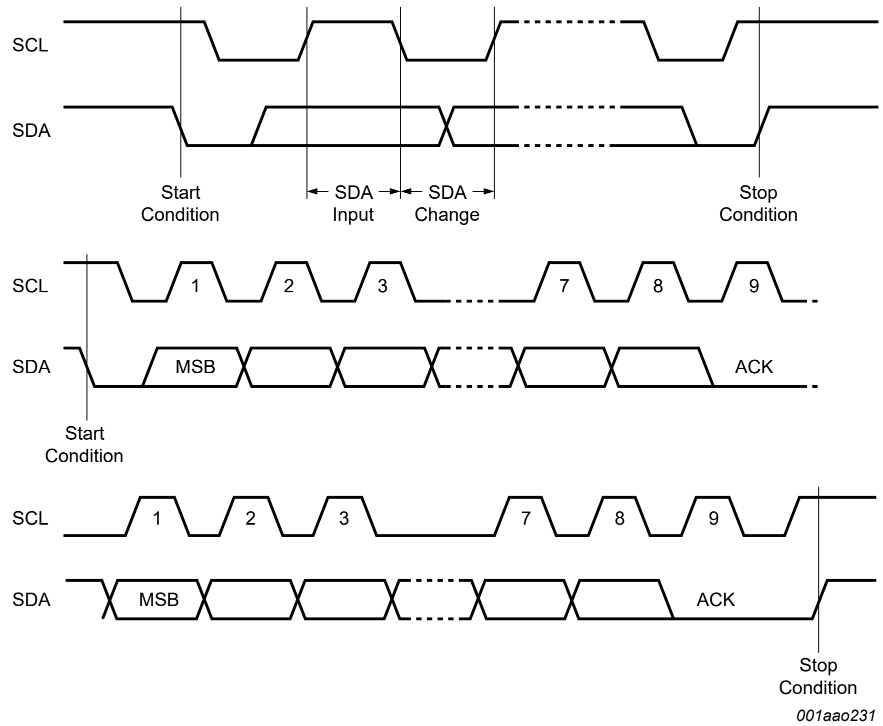


Figure 9. I²C bus protocol

NTAG 5 link supports the I²C protocol defined in UM10204. Any device that sends data onto the bus is defined as a transmitter, and any device that reads the data from the bus is defined as a receiver. The device that controls the data transfer is known as the "bus master", and the other as the "slave" device. A data transfer can only be initiated by the bus master, which will also provide the serial clock for synchronization.

8.3.1.1.1 Start condition

Start is identified by a falling edge of Serial Data (SDA), while Serial Clock (SCL) is stable in the high state. A Start condition must precede any data transfer command. NTAG 5 link continuously monitors SDA (except during a Write cycle) and SCL for a Start condition, and will not respond unless one is given.

8.3.1.1.2 Stop condition

Stop is identified by a rising edge of SDA while SCL is stable and driven high. A Stop condition terminates communication between NTAG 5 link and the bus master. A Stop condition at the end of a Write command triggers the internal write cycle.

8.3.1.1.3 Acknowledge bit (ACK)

The acknowledge bit is used to indicate a successful byte transfer. The bus transmitter, whether it is the bus master or slave device, releases Serial Data (SDA) after sending 8 bits of data. During the ninth clock pulse period, the receiver pulls Serial Data (SDA) low to acknowledge the receipt of the 9th data bits.

8.3.1.1.4 Data input

During data input, the IC samples SDA on the rising edge of SCL. For correct device operation, SDA must be stable during the rising edge of SCL, and the SDA signal must change only when SCL is driven low.

8.3.1.1.5 Addressing

To start communication between a bus master and NTAG 5 link, the bus master must initiate a Start condition. Following this initiation, the bus master sends the device address. The IC address from I²C consists of a 7-bit device identifier (see Table 229 for default value).

As long as I²C address is 7 bit long, the 8th bit (least significant bit) is used as the Read/ Write bit (R/$\overline{W}$). This bit is set to 1b for Read and 0b for Write operations.

If a match occurs on the device address, the IC gives an acknowledgment on SDA during the 9th bit time. If the IC does not match the device select code, it deselects itself from the bus and clears the register I2C_IF_LOCKED (see Table 88).

Table 229. Default NTAG 5 I²C address from I²C

	Device address						
	b6	b5	b4	b3	b2	b1	b0
Value	1 [1]	0 [1]	1 [1]	0 [1]	1 [1]	0 [1]	0 [1]

[1] Initial values - can be changed.

The I²C address of NTAG 5 link (Configuration Byte) can be modified by the NFC and I²C interface.

8.3.1.1.6 Disable I²C Interface

NTAG 5 link offers the option to disable the I²C interface temporarily using the session register bit DISABLE_I²C (see Table 100). With this feature, the NFC Device can easily get exclusive access to EEPROM.

This feature can be enabled via the NFC interface during the session by setting related session bit.

8.3.1.2 Master mode of NTP5332

NTAG 5 link can be configured in I²C master mode. Using I²C Master interface, I²C slave device like sensors or memories can be connected to NTAG 5 link without an external microcontroller. Using energy harvesting capability, I²C device can be powered by NTAG 5 link .

When using I²C master mode, it must be ensured, that there is no other active I²C master on the same bus. The USE_CASE_CONF needs to be set to I²C master (01b) and SRAM needs to be enabled in CONFIG_1 byte (see Table 38).

The used clock speed can be configured by setting I2C_MASTER_SCL_LOW and I2C_MASTER_SCL_HIGH (see Section 8.1.3.21).

To communicate with the connected I²C slave device two custom commands are implemented.

- WRITE I2C (see Section 8.2.3.8.1)
- READ I2C (see Section 8.2.3.8.2)

The response from the READ I²C command will be stored in the SRAM and can be read (see Section 8.2.3.6.1) afterwards from NFC perspective. Due to the 256 byte SRAM, only 256 bytes can be written / read at once to / from the I²C interface.

Of course, all other NFC commands are working in master mode and the user memory as well as configuration memory is accessible from NFC perspective.

WARNING: When enabling I²C master mode and disabling NFC interface in parallel, NTAG 5 link gets disabled for current session.

Implementation details can be found in AN12368.

8.3.1.3 Watch Dog Timer

A programmable watchdog timer is implemented to unlock the I²C host from NTAG 5 link latest after a defined maximum time period. The host itself will not be notified of this event directly but the NFC status register is updated accordingly.

On default Watch Dog Timer is enabled with a value of 0848h (~20 ms) but the watchdog timer can be freely set with WDT_CONFIG from 0000h (9.434 μs) up to (FFFFh+1) * 9.434 μs (~618 ms). It is recommended to keep this time as short as possible, by setting the value above, but close to the maximum needed I²C transaction time.

The timer is only active, when WDT_ENABLE is set to 1b and the IC is V_{CC} powered. The timer starts ticking when the I²C communication starts. The Watch Dog Timer ensures, that I²C interface gets released after the configured time period in any case.

In the case where the I²C communication has completed before the end of the timer and the status register I2C_IF_LOCKED was not cleared by the host, it will be cleared when defined watchdog time elapses.

NOTE: If WDT_CONFIG configured time elapses before ongoing I²C communication is finished, WDT will release SDA line in between of ongoing I²C communication.

The timer is reset automatically, when I2C_IF_LOCKED gets cleared, or the IC is not V_{CC} powered.

In I²C master use case, watchdog timer is always enabled independently of WDT_ENABLE. It is important to set WDT_CONFIG in accordance with maximum execution time.

8.3.1.4 Command Set

NTAG 5 link offers an easy to use I²C command set.

- WRITE MEMORY and READ MEMORY to access user and configuration memory
- WRITE MEMORY to present the related password, when password authentication from I²C perspective is enabled
- WRITE REGISTER and READ REGISTER to access session registers

In Figure 10 the access to EEPROM with READ MEMORY and WRITE MEMORY is illustrated and following symbols are used:

- START: I²C Start condition as defined in Section 8.3.1.1.1.
- SL_AD: 7-bit slave address (msb aligned) plus (lsb) R/W bit as defined in Section 8.3.1.1.5
- BL_AD1 (MSB) / BL_AD0 (LSB): 16-bit block address
- A/N: Acknowledge / NAK as defined in Section 8.3.1.1.3
- DATA 0, DATA 1, … , DATA N: Data bytes to be read or written.
  N shall be 3 for writing to EEPROM
  N shall be multiple of 4 reduced by 1; maximum 255 for writing to SRAM
  N is any number for reading data. NTAG 5 link will respond until host's NACK.
- Stop: Stop condition as defined in Section 8.3.1.1.2

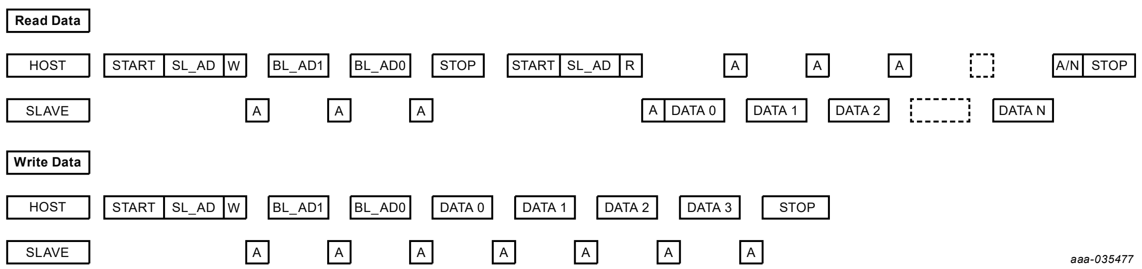


Figure 10. READ MEMORY and WRITE MEMORY command

In Figure 11 the access to Registers with READ REGISTER and WRITE REGISTER is illustrated and following symbols are used:

- START: I²C Start conditions as defined in Section 8.3.1.1.1.
- SL_AD: 7-bit slave address (msb aligned) plus (lsb) R/W bit as defined in Section 8.3.1.1.5
- BL_AD1 (MSB) | BL_AD0 (LSB): 16-bit register block address
- REGA: 8-bit register address
- MASK: 8-bit control register bit mask. Only if corresponding control bit is set to 1b, the register bit will be overwritten.
- A/N: Acknowledge / Not Acknowledge as defined in Section 8.3.1.1.3

- REGDAT: 8-bit register data to read/write
- STOP: Stop condition as defined in Section 8.3.1.1.2

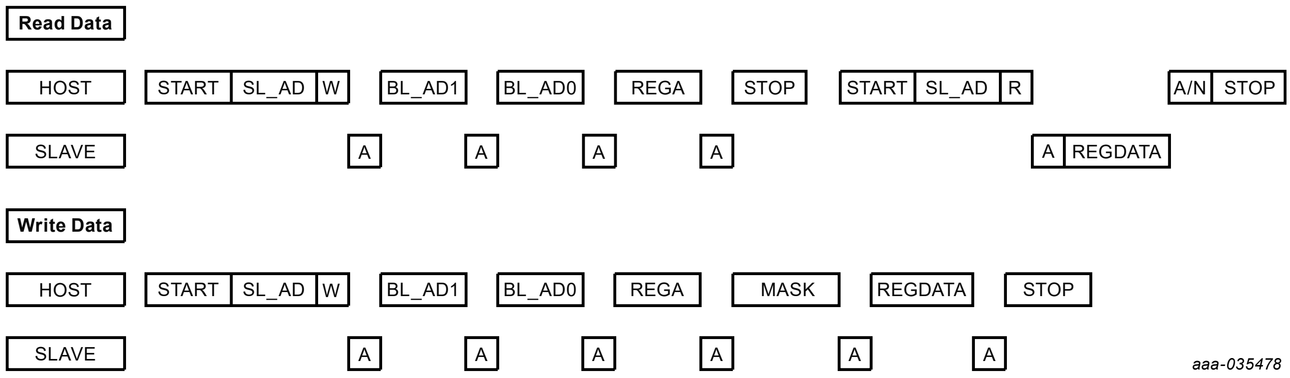


Figure 11. READ REGISTER and WRITE REGISTER command

8.3.1.5 Error Handling

In case of any detected error, NTAG 5 link in slave mode responds with a NACK:

- Memory Write
  - EEPROM
    generated on the fourth data byte if the block is not writable
  - SRAM
    generated on the first byte if the block is not writable
  - Arbiter locked to NFC interface, or
  - EEP cycle ongoing, or
  - I^2C interface disabled
    generate on block address BL_AD0
- Memory Read
  - EEPROM/SRAM
    returned data will be FFh if the access is to restricted region
  - Arbiter locked to NFC interface, or
  - EEP cycle ongoing, or
  - I^2C interface disabled
    generate on block address BL_AD0
- Register Access
  Registers are always accessible. NACK will only be generated:
  - DATA NACK due to register write command to trigger system reset
  - NACK for register read/write command on BL_AD0 if I^2C interface is disabled

8.3.2 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 to offer I^2C and PWM functionality.

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
- Data read/written in pass-through mode
- Arbiter locked/unlocked EEPROM to NFC interface
- 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.

8.3.3 GPIO

I^2C pins (SCL/SDA) are multiplexed and can be used as general-purpose input/output pins linked to configuration/session bits. When configured as GPIO pins, I^2C communication is not possible anymore.

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 8.1.3.15). 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.

8.3.4 PWM

I^2C pins (SDA/SCL) and ED pin are multiplexed and can be used as a pulse width modulation output. I^2C 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 8.1.3.15) as well as duty cycle can be configured using configuration bytes (see Section 8.1.3.16).

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 230. 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

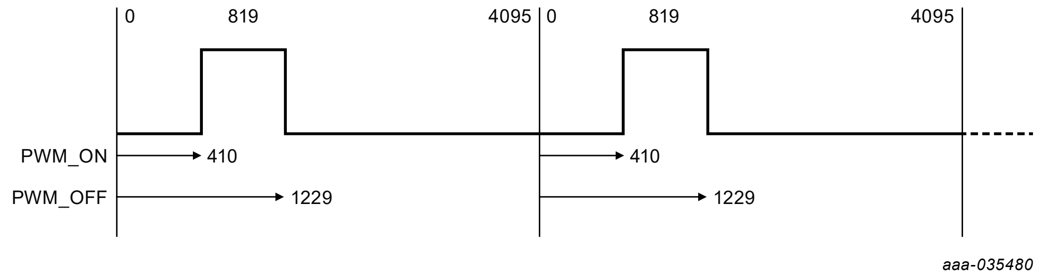


Figure 12. Pulse Width Modulation Example

How to use PWM in applications is described in AN11203.

8.3.5 Standby mode

To minimize overall current consumption, when the IC is supplied via V_{CC} NTAG 5 link can be set to standby mode by writing related session bit form NFC or I^2C perspective. The IC will leave standby mode according to configuration 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 SDA/SCLGPIO/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.

8.3.6 Hard power-down mode

In hard power-down mode NTAG 5 link 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 link.

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

8.4 Arbitration between NFC and I²C interface

There are different modes implement to ensure access to the EEPROM and described in detail hereafter. Two status bits (I2C_IF_LOCKED and NFC_IF_LOCKED) are provided to show the status of arbiter.

Details about the different arbitrations modes can be found in AN12364.

8.4.1 NFC Mode

If NTAG 5 link is only powered by NFC, arbiter needs only to lock to the NFC interface if the IC receives a valid NFC command. After completion of the NFC command, NFC_IF_LOCKED will be cleared automatically.

8.4.2 I²C Mode

If NTAG 5 link is only powered by V_{CC}, arbiter needs only to lock to the I²C interface if the IC is correctly addressed for the memory access. The host needs to clear I2C_IF_LOCKED. Otherwise, the bit will be cleared automatically if the watchdog timer expires.

In I²C mode, availability of the SRAM as part of the memory depends on SRAM_ENABLE bit.

8.4.3 Normal Mode

If NTAG 5 link is powered by NFC and VCC, arbiter locks interface on a first come first serve principle.

When receiving a valid NFC command and access is not locked to I²C, then the arbiter locks to the NFC interface. After completion of the NFC command, the lock will be released automatically. The host can access the registers at any time. Only access to EEPROM is locked.

When NTAG 5 link is correctly addressed by its I²C address for the memory access and access is not locked to NFC, then the arbiter locks to the I²C interface. The host needs to clear the lock actively. If not, the lock will be released automatically as soon as the watchdog timer expires. NFC reader can access the registers at any time. Only access to EEPROM is locked.

In this mode, availability of the SRAM depends on SRAM_ENABLE bit.

How to exchange data based on NDEF messages is defined in NFC Forum Tag NDEF Exchange Protocol (TNEP) Specification.

8.4.4 SRAM Mirror Mode

In this mode arbiter works like in normal mode with the exception, that SRAM is used instead of EEPROM.

8.4.5 SRAM Pass-Through Mode

In this mode, the NTAG 5 link transfers data from NFC to I²C and vice versa using the SRAM. The arbiter switches automatically between the two interfaces when accessing the terminator block (last block of SRAM).

Details can be found in AN12364.

8.4.6 SRAM PHDC Mode

This mode is similar to SRAM mirror mode. This mode needs to be enabled, when PHDC communication scheme as defined in NFC Forum PHDC specification shall be used. NFC will always get a response when accessing SRAM.

8.5 Energy harvesting

NTAG 5 link 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 8.1.3.18).

WARNING: Sufficient RF field is required when DISABLE_ POWER_CHECK is set to 0b to have access to EEPROM. As long as NTAG 5 link 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 97).

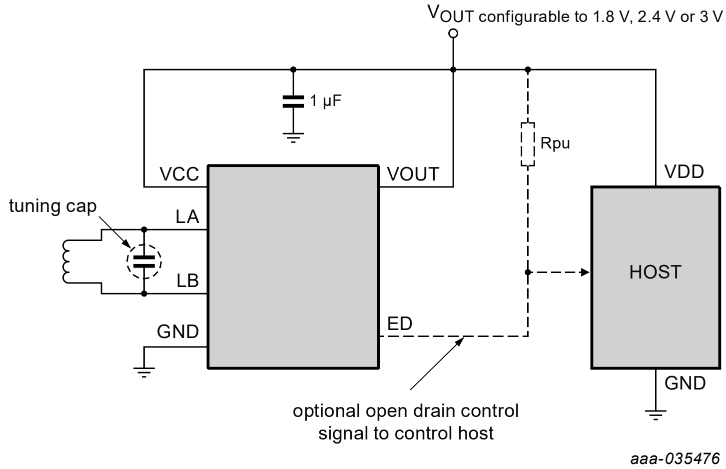


Figure 13. Energy harvesting example circuit

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

8.6 Security

NTAG 5 link 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.

With NTP5332's mutual AES authentication the memory is split in three different parts again, but with the advantage, that the password will never be transmitted in plain text.

Configuration area and SRAM can be protected from both interfaces as well.

Further implementation details can be found in AN12366.

8.6.1 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 39) and lock block sections can be locked (see Table 80). With these features, it can be ensured, NTAG 5 link 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 8.2.3.5). To accelerate this locking, NTAG 5 link 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 8.1.3.30) and blocks are indicated as locked in the Get Multiple Block Security Status response.

As long as I^{2}C Lock Block Configuration bytes are not set to 1b, the user EEPROM may still be modified from I^{2}C perspective.

Table 231. NFC Lock Block Configuration location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
6Ah	106Ah	NFC_LOCK_BL0	NFC_LOCK_BL1	RFU	RFU
...	...	...	...		
89h	1089h	NFC_LOCK_BL62	NFC_LOCK_BL63		

Table 232. I²C Lock Block Configuration location

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I²C				
8Ah	108Ah	I2C_LOCK_BL0	I2C_LOCK_BL1	RFU	RFU
8Bh	108Bh	I2C_LOCK_BL2	I2C_LOCK_BL3	RFU	RFU

8.6.2 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.

In AES mode, a key with read and write privilege is needed to be able to access the restricted area.

To enable password protection to AREA_1 from I²C perspective, I²C passwords need to be enabled by setting I²C key header (I2C_KH) to active. In that case AREA_1 read and write passwords need to be presented to NTAG 5 link.

The split configured with the 16-bit Protection Pointer is the same for both, NFC and I²C perspective.

The area below this address can be split into two more areas with the 8-bit NFC_PP_AREA_0-H (see Section 8.1.3.28) and the 8-bit I2C_PP_AREA_0-H (see Section 8.1.3.11), independently of the NFC and I²C perspective.

NFC AREA_0-L, usually used to store NDEF messages, starts from block 0. NFC AREA_0-H, usually used as password protected area to store private data, starts from block address configured by the 8-bit NFC_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.

I²C AREA_0-L starts from block 0. I²C AREA_0-H, starts from the block address configured by the 8-bit I2C_PP_AREA_0H.

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

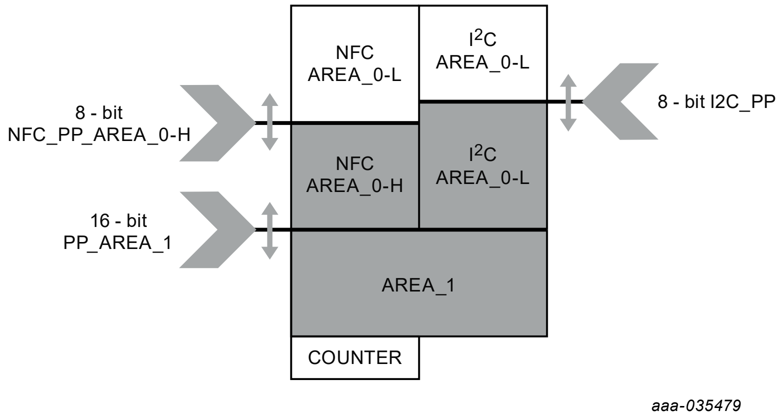


Figure 14. Concept of memory areas

8.6.3 Plain password authentication

NTAG 5 link 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.

From I²C perspective, plain password authentication can be enabled with two 32-bit passwords for the restricted AREA_1 and two for the rest of user EEPROM.

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

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

8.6.4 AES authentication

NTP5332 version of NTAG 5 link implements AES authentication from NFC perspective.

Highest security level of NTAG 5 link is AES mutual authentication based on the Crypto Suite AES128 as defined in ISO/IEC 29167-10. A 128-bit password is used to (mutual) authenticate, before doing memory operations.

From I²C perspective, only plain password authentication can be enabled.

How to use AES authentication in applications is described in AN12366.

8.7 NFC privacy mode

In the privacy mode, the NTAG 5 link is not traceable by its UID neither by data stored in the user memory. All NTAG 5 link 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 in plain password mode.

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

In AES mode, a valid mutual authentication (see Section 8.2.3.4.4) with the vendor-specific Purpose_MAM2[3:0] (see Table 164) and a key with the privacy privilege set to 1b is needed to enable using Purpose_MAM2 = 1001b and disable the NFC PRIVACY mode using Purpose_MAM2 = 1000b until next NFC field reset or 1010b permanently.

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

- INVENTORY
- SELECT
- STAY QUIET
- RESET TO READY
- PICK RANDOM ID (in AES mode to allow an anti-collision procedure)
- GET RANDOM NUMBER
- DISABLE NFC PRIVACY in plain password mode
- AUTHENTICATE

8.8 Programmable Originality signature

NTAG 5 link 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 233. 32 Byte Originality Signature

Block Address		Byte 0	Byte 1	Byte 2	Byte 3
NFC	I^2C				
00h	1000h	SIG0 (LSB)	SIG1	SIG2	SIG3
01h	1001h	SIG4	SIG5	SIG6	SIG7
02h	1002h	SIG8	SIG9	SIG10	SIG11
03h	1003h	SIG12	SIG13	SIG14	SIG15
04h	1004h	SIG16	SIG17	SIG18	SIG19
05h	1005h	SIG20	SIG21	SIG22	SIG23
06h	1006h	SIG24	SIG25	SIG26	SIG27
07h	1007h	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 link provides the possibility to customize the originality signature to personalize the IC individually for specific application. At delivery, the NTAG 5 link 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 234. 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 SDA, SCL,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 235. 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_{VCC}	V_{CC} supply current	V_{CC} = 1.8 V, 400 kHz, I^2C read/write operation	-	115	163	μA
I_{VCC}	V_{CC} supply current	V_{CC} = 3.3 V, 400 kHz, I^2C read/write operation	-	115	163	μA
I_{VCC}	V_{CC} supply current	V_{CC} = 5.5 V, 400 kHz, I^2C read/write operation.	-	138	168	μA
$I_{standby\ Vcc}$	standby current	V_{CC} = 1.8 V wake-up via I^2C	-	5.5	16	μA

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
$I_{standby\ Vcc}$	standby current	V_{CC} = 3.3 V wake-up via I^2C	-	5.9	18	μA
$I_{standby\ Vcc}$	standby current	V_{CC} = 5.5 V wake-up via I^2C	-	6.9	21	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						
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
GPIO pad pin characteristics in I^2C mode						
V_{IH}	HIGH-level input voltage		0.7*V_{CC}	-	-	V
V_{IL}	LOW-level input voltage		-	-	0.3*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
V_{OH}	HIGH-level output voltage	I_{OH} < 3 mA	0.7*V_{CC}	-	V_{CC}	V
V_{OL}	LOW-level output voltage	I_{OL} < 3 mA	0	-	0.4	V
C_i	input capacitance		-	-	3.5	pF

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
C_L	load capacitance		-	400	-	pF
GPIO pad pin characteristics in GPIO mode						
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

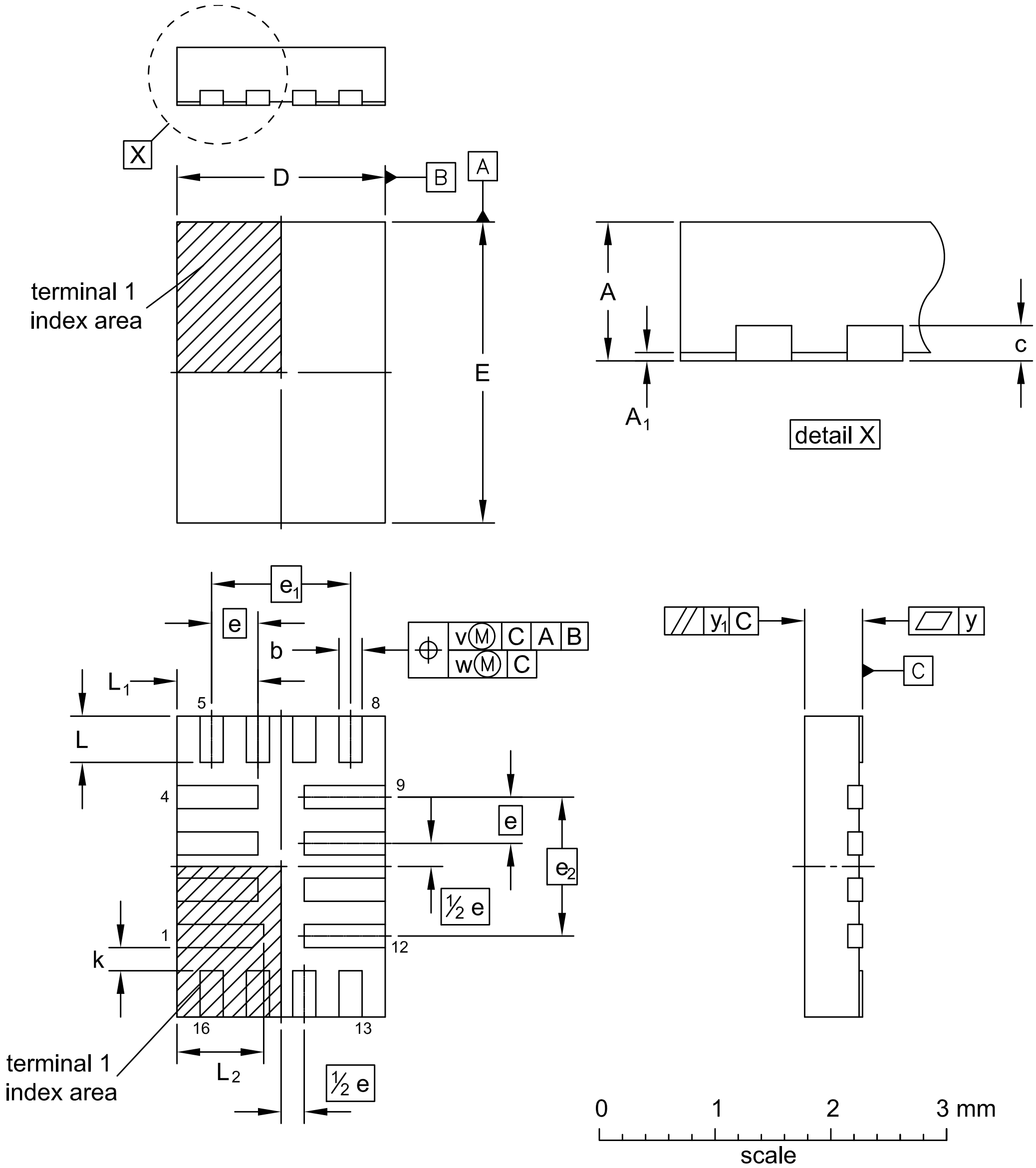
10.2 Dynamic characteristics

Table 236.

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
I^{2}C master SCL/SDA pin characteristics						
f_{SCL}	SCL clock frequency	fast mode; C_b < 400 pF	-	-	400	kHz
$t_{SU;STA}$	set-up time for a (repeated) START condition	fast mode; Cb < 400 pF	600	-	-	ns
$t_{HD;STA}$	hold time (repeated) STARTcondition	fast mode; Cb < 400 pF	600	-	-	ns
t_{LOW}	low period of the SCL clock	fast mode; Cb < 400 pF	1.3	-	-	us
t_{HIGH}	high period of the SCL clock	fast mode; Cb < 400 pF	600	-	-	ns
$t_{SU;DAT}$	data set-up time	fast mode; Cb < 400 pF	100	-	-	ns
$t_{HD;DAT}$	data hold time	fast mode; Cb < 400 pF	0	-	900	ns
tr_{SDA}	SDA rise time	CL = 100 pF, Rpull-up = 2 K, Standard and fast mode	30	-	250	ns
tf_{SDA}	SDA fall time	CL = 100 pF, Rpull-up = 2 K, Standard and fast mode	30	-	250	ns
Vhys	hysteresis of Schmitt trigger inputs	fast mode; Cb < 400 pF	0.05 *V_{CC}	-	-	V
I^{2}C slave SDA/SCL pin characteristics						
tr	rise time	CL = 100 pF, Rpull-up = 2 K,standard and fast mode	30	-	250	ns
tf	fall time	CL = 100 pF, Rpull-up = 2 K,standard and fast mode	30	-	250	ns
PWM AC timings						
PWM_{freq}	PWM output frequency		414	-	26400	Hz

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
Pulse Width	PWM signal pulse width		0.6	-	-	μs
PWM_{freq_tol}	PWM output frequency tolerance		-	-	10	%
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_VCC}	V_{CC} startup time from power OFF state. After this time, the IC is able to receive the command from I^2C interface.		-	-	3	ms
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)

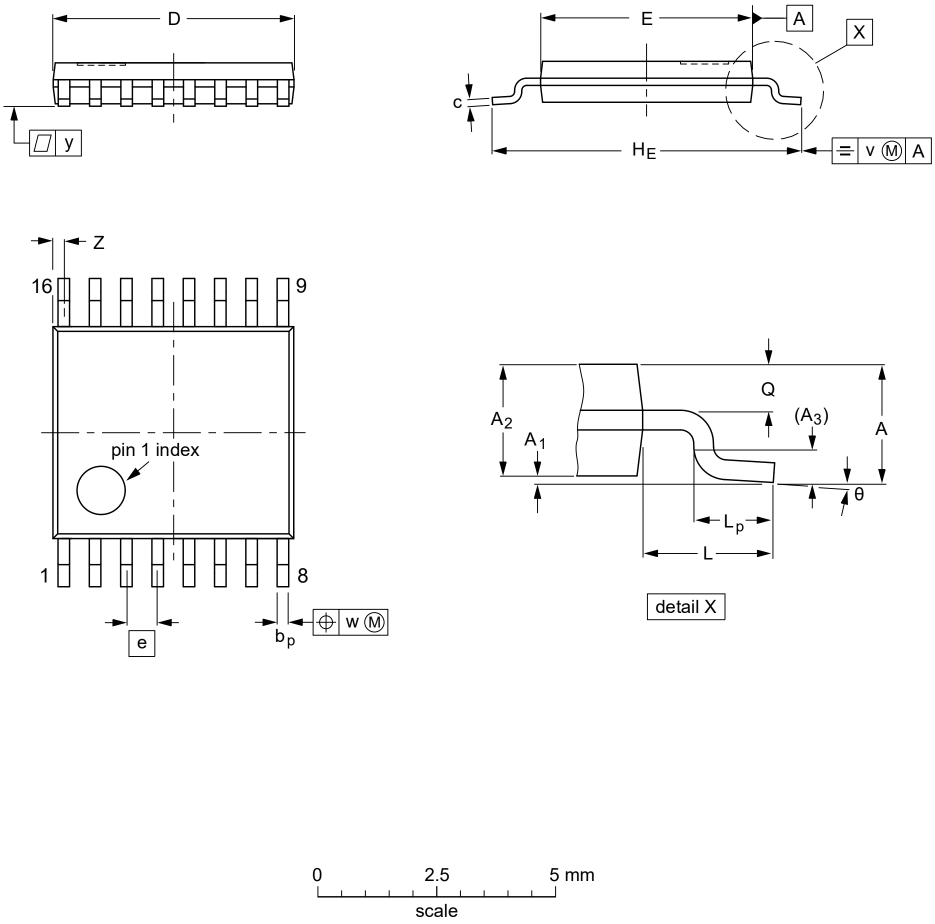
UNIT		A(1)	A_1	b	c	D(1)	E(1)	e	e_1	e_2	k	L	L_1	L_2	v	w	y	y_1
mm	MAX	0.50	0.05	0.25		1.90	2.70					0.45	0.75	0.80				
	NOM			0.20	0.127	1.80	2.60	0.40	1.20	1.20	0.2	0.40	0.70	0.75	0.1	0.05	0.05	0.1
	MIN		0.00	0.15		1.70	2.50					0.35	0.65	0.70				

Notes

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

Figure 15. 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.

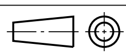
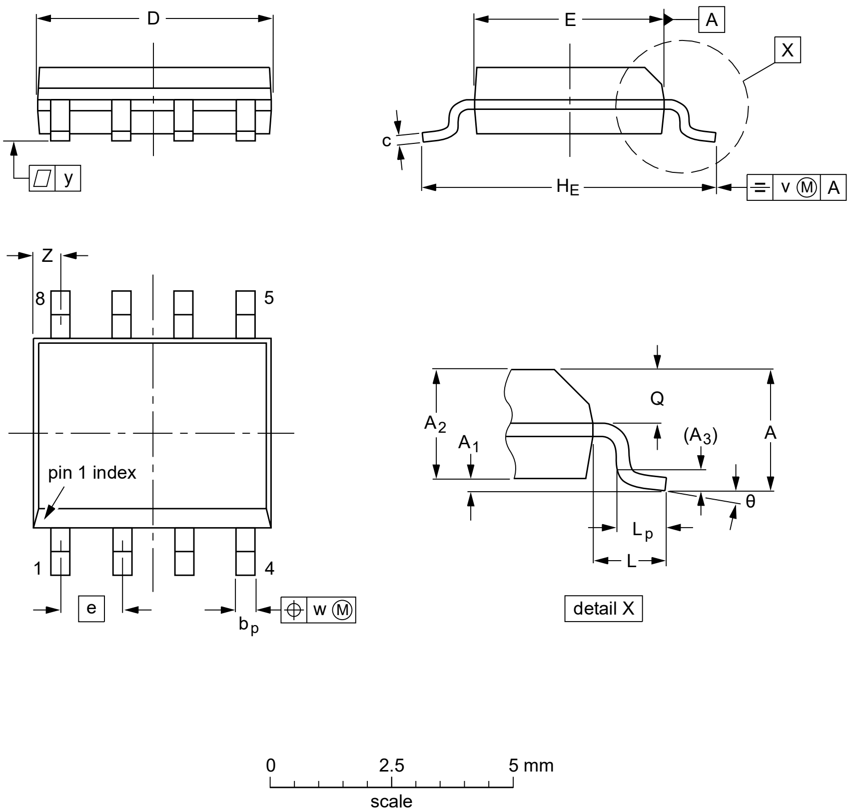
OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT403-1		MO-153				~~99-12-27~~ 03-02-18

Figure 16. 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° 0°
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 17. 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 237. 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] NFC Forum specification, Tag NDEF Exchange Protocol - Technical Specification Version 1.0 2019-04-24 [TNEP] NFC Forum™
https://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-candidate-technical-specifications/

[4] NFC Forum Personal Health Care Devices (PHDC) specification
https://nfc-forum.org/product-category/specification/

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

[6] ISO/IEC 29167-10
https://www.iso.org/ics/35.240.15/x/

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

[8] AN12364 - NTAG 5 Bidirectional data exchange, doc.no. 5303xx
https://www.nxp.com/docs/en/application-note/AN12364.pdf

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

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

[11] AN12368 - NTAG 5 Link I^{2}C Master mode, doc.no. 5306xx
https://www.nxp.com/docs/en/application-note/AN12368.pdf

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

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

[14] UM10204 - I2C-bus specification and user manual
https://www.nxp.com/docs/en/user-guide/UM10204.pdf

15 Revision history

Table 238. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
NTP53x2 v. 3.3	20200703	Product data sheet	.	NTP53x2 v. 3.2
Modifications:	• Clarified, that I²C master registers are only accessible from NFC perspective • Clarified, that PICK RANDOM ID is only supported in AES mode • Clarified that SRAM_CONFIG_PROT restricts access to blocks 37h to 54h (see Section 8.1.3.23) • Password identifier for access to restricted area added (see Table 125) • Editorial updates			
NTP53x2 v. 3.2	20200427	Product data sheet	.	NTP53x2 v. 3.1
NTP53x2 v. 3.1	20200324	Product data sheet	.	NTP53x2 v. 3.0
NTP53x2 v. 3.0	20200116	Product data sheet	.	NTP53x2 v. 2.0
NTP53x2 v. 2.0	20191002	Preliminary data sheet	-	-
NTP53x2 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.

I²C-bus — logo is a trademark of NXP B.V.

NTAG — is a trademark of NXP B.V.

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

Tables

Tab. 1. Ordering information 6
Tab. 2. Marking codes 7
Tab. 3. Pin description for XQFN16 9
Tab. 4. Pin description for TSSOP16 10
Tab. 5. Pin description for SO8 11
Tab. 6. User memory organization 13
Tab. 7. Memory content at delivery 13
Tab. 8. COUNTER BLOCK data structure 14
Tab. 9. Preset counter data structure 14
Tab. 10. Increment counter data structure 15
Tab. 11. Configuration Memory organization 15
Tab. 12. 32 Byte Originality Signature 20
Tab. 13. Configuration Header (CH) location 20
Tab. 14. Configuration Header Codes 20
Tab. 15. Customer ID (CID) location 21
Tab. 16. NFC Global Crypto Header (GCH) location 22
Tab. 17. Global Crypto Header Configuration in plain password mode 22
Tab. 18. Global Crypto Header Configuration Value in AES mode 22
Tab. 19. Crypto Configuration Header (CCH) location ...23
Tab. 20. Crypto Configuration Header Values 23
Tab. 21. NFC Authentication Limit Counter (NFC_AUTH_LIMIT) location 24
Tab. 22. NFC Key Header (KHx) location 25
Tab. 23. NFC Key Header Values 25
Tab. 24. NFC Key Privileges (KPx) location 26
Tab. 25. Definition of NFC Key Privileges bytes KPx 26
Tab. 26. Key location 27
Tab. 27. Plain Password location 27
Tab. 28. I2C Password location 28
Tab. 29. I2C Key Authenticate Password location 28
Tab. 30. I2C Key Header (I2C_KH) location 29
Tab. 31. I2C Key Header Values 29
Tab. 32. I2C Protection Pointer and Configuration location 29
Tab. 33. I2C Memory organization example 30
Tab. 34. I2C Protection Pointer Configuration (I2C_PPC) 30
Tab. 35. I2C Authentication Limit Counter (I2C_AUTH_LIMIT) location 31
Tab. 36. Configuration Bytes Location (CONFIG) 31
Tab. 37. Configuration Definition (CONFIG_0) 32
Tab. 38. Configuration Definition (CONFIG_1) 32
Tab. 39. Configuration Definition (CONFIG_2) 33
Tab. 40. Synchronization Block Bytes Location (SYNCH_DATA_BLOCK) 33
Tab. 41. Synchronization Block Register Bytes Location (SYNCH_DATA_BLOCK_REG) 33
Tab. 42. PWM and GPIO Configuration Location (PWM_GPIO_CONFIG) 34
Tab. 43. PWM and GPIO Configuration Definition (PWM_GPIO_CONFIG_0) 34
Tab. 44. PWM and GPIO Configuration Definition (PWM_GPIO_CONFIG_1 and PWM_GPIO_CONFIG_1_REG) 34
Tab. 45. Pulse Width Modulation Duty Cycle Configuration Location (PWMx_ON and PWMx_OFF) 35
Tab. 46. Pulse Width Modulation Duty Cycle Session Register Location (PWMx_ON and PWMx_OFF) 35
Tab. 47. Pulse Width Modulatin ON time Configuration Definition (PWMx_ON and PWMx_ON_REG) 35
Tab. 48. Pulse Width Modulation OFF time Configuration Definition (PWMx_OFF and PWMx_OFF_REG) 35
Tab. 49. Watch Dog Timer Configuration Location (WDT_CONFIG) 36
Tab. 50. Watch Dog Timer Configuration Register Location (WDT_CONFIG_REG) 36
Tab. 51. Watch Dog Timer Enable Definition (WDT_ENABLE and WDT_EN_REG) 36
Tab. 52. Energy harvesting Configuration Location (EH_CONFIG) 36
Tab. 53. Energy harvesting Configuration Value Definition (EH_CONFIG) 36
Tab. 54. Event Detection Configuration Location (ED_CONFIG) 37
Tab. 55. Event Detection Configuration Register Location (ED_CONFIG_REG) 37
Tab. 56. Event Detection Definition (ED_CONFIG and ED_CONFIG_REG) 37
Tab. 57. Event Detection Clear Register Location (ED_INTR_CLEAR_REG) 39
Tab. 58. Event Detection Clear Register (ED_INTR_CLEAR_REG) 39
Tab. 59. I2C Slave Configuration Location 39
Tab. 60. I2C Slave Configuration Definition (I2C_SLAVE_ADDR) 39
Tab. 61. I2C Slave Configuration Definition (I2C_SLAVE_CONFIG) 39
Tab. 62. I2C Master Clock Settings Configuration Location (I2C_MASTER_CONFIG) 40
Tab. 63. I2C Master Clock Configuration Definition (I2C_MASTER_SCL_LOW) 40
Tab. 64. I2C Master Clock Configuration Definition (I2C_MASTER_SCL_HIGH) 40
Tab. 65. Device Security Configuration Byte location 40
Tab. 66. Device Security Byte Definition (DEV_SEC_CONFIG) 40
Tab. 67. SRAM and Configuration Byte location 41
Tab. 68. SRAM and Configuration Protection (SRAM_CONF_PROT) 41
Tab. 69. Restricted AREA_1 Pointer location 42
Tab. 70. Memory organization example from NFC perspective 42
Tab. 71. Application Family Identifier (AFI) location 42
Tab. 72. Data Storage Format Identifier (DSFID) location 43

Tab. 73. Electronic Article Surveillance ID (EASID) location ... 43
Tab. 74. NFC Protection Pointer (NFC PP) location ... 43
Tab. 75. Memory organization example ... 43
Tab. 76. NFC Protection Pointer Conditions (NFC_PPC) location ... 44
Tab. 77. NFC Protection Pointer Configuration (NFC_PPC) ... 44
Tab. 78. NFC Lock Block Configuration location ... 45
Tab. 79. I2C Lock Block Configuration location ... 45
Tab. 80. Device configuration section lock bytes location ... 45
Tab. 81. NFC configuration section lock byte 0 definition (NFC_SECTION_LOCK_0) ... 46
Tab. 82. NFC configuration section lock Byte 1 definition (NFC_SECTION_LOCK_1) ... 46
Tab. 83. I2C configuration section lock byte 0 definition (I2C_SECTION_LOCK_0) ... 47
Tab. 84. I2C configuration section lock byte 1 definition (I2C_SECTION_LOCK_1) ... 47
Tab. 85. Session Register Location ... 48
Tab. 86. Status Register Location ... 49
Tab. 87. Status 0 Register ... 50
Tab. 88. Status 1 Register ... 50
Tab. 89. Configuration Register Location (CONFIG_REG) ... 51
Tab. 90. Configuration Definition (CONFIG_0_REG) ... 51
Tab. 91. Configuration Definition (CONFIG_1_REG) ... 52
Tab. 92. Configuration Definition (CONFIG_2_REG) ... 52
Tab. 93. PWM and GPIO Configuration Register Location (PWM_GPIO_CONFIG_REG) ... 53
Tab. 94. PWM and GPIO Configuration Register Definition (PWM_GPIO_CONFIG_0_REG) ... 53
Tab. 95. PWM and GPIO Configuration Register Definition (PWM_GPIO_CONFIG_1_REG) ... 54
Tab. 96. Energy Harvesting Configuration Register Location (EH_CONFIG_REG) ... 55
Tab. 97. Energy Harvesting Register Value Definition EH_CONFIG_REG) ... 55
Tab. 98. I2C Slave Configuration Register Location ... 55
Tab. 99. I2C Slave Configuration Definition (I2C_SLAVE_ADDR_REG) ... 56
Tab. 100. I2C Slave Configuration Definition (I2C_SLAVE_CONFIG_REG) ... 56
Tab. 101. RESET_GEN_REG location ... 56
Tab. 102. ED_INTR_CLEAR_REG location ... 57
Tab. 103. I2C Master Configuration Register Location ... 57
Tab. 104. I2C Slave Address used in I2C master transaction (I2C_M_S_ADD_REG) ... 57
Tab. 105. I2C Master Data Length Definition (I2C_M_LEN_REG) ... 57
Tab. 106. I2C Master Status Definition (I2C_M_STATUS_REG) ... 57
Tab. 107. SRAM mirroring ... 58
Tab. 108. SRAM mirroring with default content ... 59
Tab. 109. SRAM COPY BYTES (SRAM_COPY_BYTES) ... 59
Tab. 110. SRAM_COPY_BYTES Definition ... 59
Tab. 111. SRAM Default Content location ... 60
Tab. 112. Bit rates from reader to tag ... 60
Tab. 113. Bit rates from tag to reader ... 60
Tab. 114. NFC command set supported by NTAG 5 link ... 63
Tab. 115. READ CONFIG request format ... 66
Tab. 116. READ CONFIG response format when Error_flag is NOT set ... 66
Tab. 117. READ CONFIGURATION response format when Error_flag is set ... 66
Tab. 118. WRITE CONFIG request format ... 67
Tab. 119. WRITE CONFIG response format when Error_flag is NOT set ... 67
Tab. 120. WRITE CONFIG response format when Error_flag is set ... 67
Tab. 121. GET RANDOM NUMBER request format ... 67
Tab. 122. GET RANDOM NUMBER response format when Error_flag is NOT set ... 67
Tab. 123. GET RANDOM NUMBER response format when Error_flag is set ... 68
Tab. 124. SET PASSWORD request format ... 68
Tab. 125. Password Identifier ... 68
Tab. 126. SET PASSWORD response format when Error_flag is NOT set ... 68
Tab. 127. SET PASSWORD response format when Error_flag is set ... 69
Tab. 128. WRITE PASSWORD request format ... 69
Tab. 129. WRITE PASSWORD response format when Error_flag is NOT set ... 69
Tab. 130. WRITE PASSWORD response format when Error_flag is set ... 69
Tab. 131. LOCK PASSWORD request format ... 70
Tab. 132. LOCK PASSWORD response format when Error_flag is NOT set ... 70
Tab. 133. LOCK PASSWORD response format when Error_flag is set ... 70
Tab. 134. 64 BIT PASSWORD PROTECTION request format ... 70
Tab. 135. 64 BIT PASSWORD PROTECTION response format when Error_flag is NOT set ... 71
Tab. 136. 64 BIT PASSWORD PROTECTION response format when Error_flag is NOT set ... 71
Tab. 137. Memory organization ... 71
Tab. 138. PROTECT PAGE request format ... 72
Tab. 139. Extended Protection status byte ... 72
Tab. 140. Protection status bits definition in plain password mode ... 72
Tab. 141. Protection status bits definition in AES mode ... 73
Tab. 142. PROTECT PAGE response format when Error_flag is NOT set ... 73
Tab. 143. PROTECT PAGE response format when Error_flag is set ... 73
Tab. 144. LOCK PAGE PROTECTION CONDITION request format ... 73
Tab. 145. LOCK PAGE PROTECTION CONDITION response format when Error_flag is NOT set ... 74
Tab. 146. LOCK PAGE PROTECTION CONDITION response format when Error_flag is set ... 74
Tab. 147. DESTROY request format ... 74

Tab. 148. DESTROY response format when Error_flag is NOT set 74
Tab. 149. DESTROY response format when Error_flag is set 74
Tab. 150. ENABLE NFC PRIVACY request format 75
Tab. 151. ENABLE NFC PRIVACY response format when Error_flag is NOT set 75
Tab. 152. ENABLE NFC PRIVACY response format when Error_flag is set 75
Tab. 153. DISABLE NFC PRIVACY request format 76
Tab. 154. DISABLE NFC PRIVACY response format when Error_flag is NOT set 76
Tab. 155. DISABLE NFC PRIVACY response format when Error_flag is set 76
Tab. 156. AUTHENTICATE request format 77
Tab. 157. AUTHENTICATE response format when Error_flag is NOT set(in process reply) 77
Tab. 158. AUTHENTICATE response format when Error_flag is set 77
Tab. 159. Message format for TAM1 77
Tab. 160. TResponse for TAM1 77
Tab. 161. Message format for MAM1 78
Tab. 162. TReseponse for MAM1 78
Tab. 163. Message format for MAM2 78
Tab. 164. Definition of Purpose_MAM2 78
Tab. 165. TReseponse for MAM2 79
Tab. 166. CHALLENGE request format 79
Tab. 167. Message format 79
Tab. 168. READBUFFER request format 80
Tab. 169. READBUFFER response format when Error_flag is NOT set 80
Tab. 170. TResponse 80
Tab. 171. READBUFFER response format when Error_flag is set 80
Tab. 172. INVENTORY READ request format 81
Tab. 173. INVENTORY READ response format: Option flag logic 0b 82
Tab. 174. INVENTORY READ response format: Option flag logic 1b 82
Tab. 175. Example: mask length = 30 82
Tab. 176. Inventory Read (extended mode) request format 83
Tab. 177. Extended options 83
Tab. 178. Inventory Read (extended mode) response format: Option_flag 1b 84
Tab. 179. Example 84
Tab. 180. READ SRAM request format 85
Tab. 181. READ SRAM response format when Error_flag is NOT set 85
Tab. 182. READ SRAM response format when Error_flag is set 85
Tab. 183. WRITE SRAM request format 86
Tab. 184. WRITE SRAM response format when Error_flag is NOT set 86
Tab. 185. WRITE SRAM response format when Error_flag is set 86
Tab. 186. READ SIGNATURE request format 86
Tab. 187. READ SIGNATURE response format when Error_flag is NOT set 86
Tab. 188. READ SIGNATURE response format when Error_flag is set 87
Tab. 189. WRITE I2C request format 88
Tab. 190. I2C param byte 88
Tab. 191. WRITE I2C response format when Error_flag is NOT set 89
Tab. 192. WRITE I2C response format when Error_flag is set 89
Tab. 193. READ I2C request format 89
Tab. 194. I2C param byte 89
Tab. 195. READ I2C response format when Error_flag is NOT set 89
Tab. 196. READ I2C response format when Error_flag is set 90
Tab. 197. SET EAS request format 90
Tab. 198. SET EAS response format when Error_flag is NOT set 90
Tab. 199. SET EAS response format when Error_flag is set 90
Tab. 200. RESET EAS request format 91
Tab. 201. RESET EAS response format when Error_flag is NOT set 91
Tab. 202. RESET EAS response format when Error_flag is set 91
Tab. 203. LOCK EAS request format 91
Tab. 204. LOCK EAS response format when Error_flag is NOT set 92
Tab. 205. LOCK EAS response format when Error_flag is set 92
Tab. 206. EAS ALARM Request format 92
Tab. 207. EAS ALARM Response format (Option flag logic 0) 92
Tab. 208. EAS ALARM Response format(Option flag logic 1) 93
Tab. 209. EAS ALAMR response format when Error_flag is set 93
Tab. 210. PROTECT EAS/AFI request format 93
Tab. 211. PROTECT EAS/AFI response format when Error_flag is NOT set 93
Tab. 212. PROTECT EAS/AFI response format when Error_flag is set 93
Tab. 213. WRITE EAS ID request format 94
Tab. 214. WRITE EAS ID response format when Error_flag is NOT set 94
Tab. 215. WRITE EAS ID response format when Error_flag is set 94
Tab. 216. GET NXP SYSTEM INFORMATION request format 95
Tab. 217. GET NXP SYSTEM INFORMATION response format when Error_flag is NOT set 95
Tab. 218. Protection Pointer condition byte 95
Tab. 219. Lock bits byte 95
Tab. 220. Feature flags byte 0 96
Tab. 221. Feature flags byte 1 96
Tab. 222. Feature flags byte 2 96
Tab. 223. Feature flags byte 3 97
Tab. 224. GET NXP SYSTEM INFORMATION response format when Error_flag is set 97
Tab. 225. PICK RANDOM ID request format 97

Tab. 226. PICK RANDOM ID response format when Error_flag is NOT set 97
Tab. 227. PICK RANDOM ID response format when Error_flag is set 98
Tab. 228. Random ID 98
Tab. 229. Default NTAG 5 I2C address from I2C 100
Tab. 230. Pulse Width Modulation Frequency 104
Tab. 231. NFC Lock Block Configuration location 109
Tab. 232. I2C Lock Block Configuration location 109
Tab. 233. 32 Byte Originality Signature 111
Tab. 234. Limiting values In accordance with the Absolute Maximum Rating System (IEC 60134). 113
Tab. 235. Characteristics 114
Tab. 236. 116
Tab. 237. Abbreviations 122
Tab. 238. Revision history 124

Figures

Fig. 1. NTAG 5 link overview 1
Fig. 2. Block diagram NTAG 5 link 8
Fig. 3. Pin configuration for XQFN16 package 9
Fig. 4. Pin configuration for TSSOP16 package 10
Fig. 5. Pin configuration for SO8 package 10
Fig. 6. State Machine and State Transitions 61
Fig. 7. I2C Master write principle 87
Fig. 8. I2C Master read principle 88
Fig. 9. I2C bus protocol 99
Fig. 10. READ MEMORY and WRITE MEMORY command 102
Fig. 11. READ REGISTER and WRITE REGISTER command 103
Fig. 12. Pulse Width Modulation Example 105
Fig. 13. Energy harvesting example circuit 108
Fig. 14. Concept of memory areas 110
Fig. 15. Package outline XQFN16 118
Fig. 16. Package outline TSSOP16 119
Fig. 17. Package outline SO8 120

Contents

1 General description **1**
2 Features and benefits **3**
3 Applications **5**
4 Ordering information **6**
5 Marking **7**
6 Block diagram **8**
7 Pinning information **9**
8 Functional description **12**
8.1 Memory Organization 12
8.1.1 General 12
8.1.2 User memory 12
8.1.2.1 16-bit counter 13
8.1.3 Configuration memory 15
8.1.3.1 Originality Signature 20
8.1.3.2 Configuration Header 20
8.1.3.3 Customer ID (CID) 21
8.1.3.4 NFC Global Crypto Header 21
8.1.3.5 NFC Crypto Configuration Header 23
8.1.3.6 NFC Authentication Limit Counter 23
8.1.3.7 NFC Key Header 24
8.1.3.8 NFC Key Privileges 25
8.1.3.9 Keys and passwords 26
8.1.3.10 I2C Key Header 28
8.1.3.11 I2C Protection Pointer and Condition 29
8.1.3.12 I2C Authentication Limit Counter 31
8.1.3.13 Configuration 31
8.1.3.14 Synchronization Block 33
8.1.3.15 Pulse Width Modulation and GPIO configuration 33
8.1.3.16 Pulse Width Modulation duty cycle settings 35
8.1.3.17 Watch Dog Timer settings 35
8.1.3.18 Energy harvesting settings 36
8.1.3.19 Event detection pin configuration settings 37
8.1.3.20 I2C slave configuration settings 39
8.1.3.21 I2C master clock configuration settings 39
8.1.3.22 Device security configuration bytes 40
8.1.3.23 SRAM and Configuration protection 41
8.1.3.24 Restricted AREA_1 pointer 41
8.1.3.25 Application Family Identifier 42
8.1.3.26 Data Storage Format Identifier 43
8.1.3.27 Electronic Article Surveillance ID 43
8.1.3.28 NFC protection pointer 43
8.1.3.29 NFC Protection Pointer Conditions 44
8.1.3.30 NFC lock bytes 44
8.1.3.31 I2C lock bytes 45
8.1.3.32 Device configuration section lock bytes 45
8.1.4 Session registers 48
8.1.4.1 Status register 49
8.1.4.2 Configuration register 51
8.1.4.3 Synchronization block register 53
8.1.4.4 Pulse Width Modulation and GPIO configuration register 53
8.1.4.5 Pulse Width Modulation duty cycle register 54
8.1.4.6 Watch Dog Timer register 54
8.1.4.7 Energy harvesting register 54
8.1.4.8 Event detection register 55
8.1.4.9 I2C slave register settings 55
8.1.4.10 System reset generation 56
8.1.4.11 Clear event detection register 56
8.1.4.12 I2C master status registers 57
8.1.5 SRAM 58
8.2 NFC interface 60
8.2.1 Passive communication mode 60
8.2.2 State diagram and state transitions 60
8.2.2.1 POWER-OFF state 61
8.2.2.2 READY state 61
8.2.2.3 SELECTED state 62
8.2.2.4 SELECTED SECURE state 62
8.2.2.5 QUIET state 63
8.2.3 Command set 63
8.2.3.1 Commands for state transitions 65
8.2.3.2 Configuration operations 66
8.2.3.3 PWD Authentication 67
8.2.3.4 AES Authentication 76
8.2.3.5 Memory operations 80
8.2.3.6 SRAM operations 85
8.2.3.7 Originality Signature 86
8.2.3.8 I2C Transparent Channel 87
8.2.3.9 Other 90
8.2.4 Data integrity 98
8.2.5 Error Handling 98
8.2.5.1 Transmission Errors 98
8.2.5.2 Not supported commands or options 98
8.3 Wired Interface 99
8.3.1 I2C interface 99
8.3.1.1 Slave mode 99
8.3.1.2 Master mode of NTP5332 101
8.3.1.3 Watch Dog Timer 101
8.3.1.4 Command Set 102
8.3.1.5 Error Handling 103
8.3.2 Event detection 103
8.3.3 GPIO 104
8.3.4 PWM 104
8.3.5 Standby mode 105
8.3.6 Hard power-down mode 105
8.4 Arbitration between NFC and I2C interface 106
8.4.1 NFC Mode 106
8.4.2 I2C Mode 106
8.4.3 Normal Mode 106
8.4.4 SRAM Mirror Mode 106
8.4.5 SRAM Pass-Through Mode 106
8.4.6 SRAM PHDC Mode 107
8.5 Energy harvesting 107
8.6 Security 108
8.6.1 Locking EEPROM to read only 108
8.6.2 Memory Areas 109
8.6.3 Plain password authentication 110
8.6.4 AES authentication 110
8.7 NFC privacy mode 111
8.8 Programmable Originality signature 111
9 Limiting values **113**
10 Characteristics **114**

10.1 Static Characteristics 114
10.2 Dynamic characteristics 116
11 Package outline 118
12 Handling information 121
13 Abbreviations 122
14 References 123
15 Revision history 124
16 Legal information 125

Date of release: 3 July 2020
Document number: 544533