Chipsmall
深圳市津利帝科技有限公司
Geelead Technology Limited
Chipsmall
采购部

NT3H2111_2211

NTAG I^{2}C *plus*: NFC Forum T2T with I^{2}C interface, password protection and energy harvesting

Rev. 3.3 — 8 August 2018
359933

Product data sheet
COMPANY PUBLIC

1 General description

Designed to be the perfect enabler for NFC in home-automation and consumer applications, this feature-packed, second-generation connected NFC tag is the fastest, least expensive way to add tap-and-go connectivity to just about any electronic device.

NXP NTAG I^{2}C *plus* is a family of connected NFC tags that combine a passive NFC interface with a contact I^{2}C interface. As the second generation of NXP's industry leading connected-tag technology, these devices maintain full backward compatibility with first-generation NTAG I^{2}C products, while adding new, advanced features for password protection, full memory-access configuration from both interfaces, and an originality signature for protection against cloning.

The second-generation technology provides four times higher pass-through performance, along with energy harvesting capabilities, yet NTAG I^{2}C *plus* devices are optimized for use in entry-level NFC applications and offer the lowest BoM of any NFC solution.

I^{2}C and NFC communications are based on simple, standard command sets, and are augmented by the demo board OM5569/NT322E, which includes online reference source code. All that is required is a simple antenna design (see Ref. 5), with no or only limited extra components, and there are plenty of reference designs online for inspiration. NTAG I^{2}C *plus* development board is certified as NFC Forum Type 2 Tag (Certification ID: 58514).

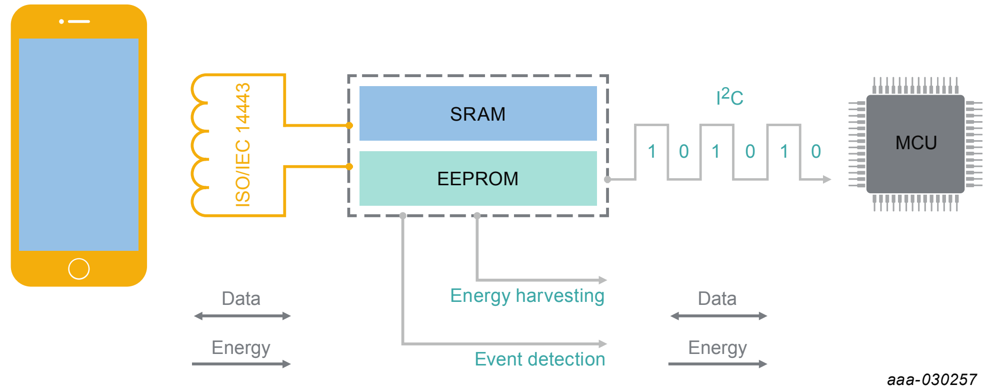


Figure 1. Contactless and contact system

2 Features and benefits

2.1 Key features

- Interoperability
  - ISO/IEC 14443 Part 2 and 3 compliant
  - NTAG I^{2}C *plus* development board is certified as NFC Forum Type 2 Tag (Certification ID: 58514)
  - Unique 7 byte UID
  - GET_VERSION command for easy identification of chip type and supported features
  - Input capacitance of 50 pF
- Host interface
  - I^{2}C slave
  - Configurable field detection pin based on open-drain implementation to signal NFC events or synchronize pass-through data transfer
- Memory
  - 2k bytes EEPROM
  - 64 bytes SRAM buffer for transfer of data between NFC and I^{2}C interfaces with memory mirror or pass-through mode
  - Clear arbitration between NFC and I^{2}C memory access
- Data transfer
  - Pass-through mode with 64 byte SRAM buffer
  - FAST_WRITE and FAST_READ NFC commands for higher data throughput
- Security and memory-access management
  - Full, read-only, or no memory access from NFC interface, based on 32-bit password
  - Full, read-only, or no memory access from I^{2}C interface
  - NFC silence feature to disable the NFC interface
  - Originality signature based on Elliptic Curve Cryptography (ECC) for simple, genuine authentication
- Power Management
  - Configurable field-detection output signal for data-transfer synchronization and device wake-up
  - Energy harvesting from NFC field, so as to power external devices (e.g. connected microcontroller)
- Industrial requirements
  - Temperature range from -40 °C up to 105 °C

2.2 NFC interface

- Contactless transmission of data at 106 kbps
- NTAG I^{2}C *plus* development board is certified as NFC Forum Type 2 Tag (Certification ID: 58514) (see Ref. 1)
- ISO/IEC 14443A compliant (see Ref. 2)
- Data transfer of 106 kbit/s
- 4 bytes (one page) written including all overhead in 4.8 ms via EEPROM or 0.8 ms via SRAM

- 64 bytes (whole SRAM) written including all overhead in 6.1 ms using FAST_WRITE command
- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- Operating distance of up to 100 mm (depending on various parameters, such as field strength and antenna geometry)
- True anticollision
- Unique 7-byte serial number (UID) according to ISO/IEC 14443-3 (see Ref. 2)

2.3 Memory

- 2k bytes EEPROM
- 64 bytes SRAM volatile memory without write endurance limitation
- Data retention time of minimum 20 years
- EEPROM write endurance minimum 500.000 cycles

2.4 I²C interface

- I²C slave interface supports frequencies up to 400 kHz (see Section 13.1)
- I²C slave supports 7-bit slave address.
- As the least significant R/$\overline{\text{W}}$ bit is used to indicate data transfer direction, default slave address 55h recalculates to an I²C write address AAh and an I²C read address ABh respectively.
- 16 bytes (one block) written in 4 ms (EEPROM) or 0.4 ms (SRAM)
- NTAG I²C *plus* can be used as standard I²C EEPROM and I²C SRAM

2.5 Security

- Manufacturer-programmed 7-byte UID for each device
- Capability container with one time programmable bits
- Field programmable read-only locking function per page for first 12 pages and per 16 (1k version) or 32 (2k version) pages for the extended memory section
- ECC-based originality signature
- 32-bit password protection to prevent unauthorized memory operations from NFC perspective may be enabled for parts of, or complete memory
- Access to password protected data area may be restricted from I²C perspective
- Pass-through and mirror mode operation may be password protected
- Protected data can be safeguarded against limited number of negative password authentication attempts

2.6 Key benefits

- Full interoperability with every NFC-enabled device
- Smooth end-user experience with super-fast data exchange (up to 40 kbit/s) via NFC and I²C interface
- Zero-power operation with non-volatile data storage
- Energy harvesting feature delivers up to 15 mW out of NFC field to power (parts of) host system
- Data protection to prevent unauthorized data manipulation

- Multi-application support, enabled by memory size and segmentation options
- Lowest bill of materials and smallest footprint for NFC solution in embedded electronics

3 Applications

NXP NTAG I^2C *plus* is a family of connected NFC tags that combine a passive NFC interface with a contact I^2C interface. As the second generation of NXP's industry-leading connected-tag technology, these devices maintain full backward compatibility with first-generation NTAG I^2C products, while adding new, advanced features for password protection, full memory-access configuration from both interfaces, and an originality signature for protection against cloning.

The second-generation technology provides four times higher pass-through performance, along with energy harvesting capabilities, yet NTAG I^2C *plus* devices are optimized for use in NFC applications like:

- IoT nodes (home automation, smart home, etc.)
- Pairing and configuration of consumer applications
- NFC accessories (headsets, speakers, etc.)
- Wearable infotainment
- Fitness equipment
- Consumer electronics
- Healthcare
- Smart printers
- Meters
- Electronic shelf labels

4 Ordering information

Table 1. Ordering information

Type number	Package		
	Name	Description	Version
NT3H2111W0FHK	XQFN8	Plastic, extremely thin quad flat package; no leads; 8 terminals; body 1.6 x 1.6 x 0.6 mm; 1k bytes memory, 50 pF input capacitance	SOT902-3
NT3H2211W0FHK	XQFN8	Plastic, extremely thin quad flat package; no leads; 8 terminals; body 1.6 x 1.6 x 0.6 mm; 2k bytes memory, 50 pF input capacitance	SOT902-3
NT3H2111W0FTT	TSSOP8	Plastic thin shrink small outline package; 8 leads; body width 3 mm; 1k bytes memory; 50 pF input capacitance	SOT505-1
NT3H2211W0FTT	TSSOP8	Plastic thin shrink small outline package; 8 leads; body width 3 mm; 2k bytes memory; 50 pF input capacitance	SOT505-1
NT3H2111W0FT1	SO8	Plastic small outline package; 8 leads; body width 3.9 mm, 1k bytes memory; 50 pF input capacitance	SOT96-1
NT3H2211W0FT1	SO8	Plastic small outline package; 8 leads; body width 3.9 mm, 2k bytes memory; 50 pF input capacitance	SOT96-1
NT3H2111W0FUG	FFC bumped	8 inch wafer, 150um thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 1k Bytes memory, 50 pF input capacitance	-
NT3H2211W0FUG	FFC bumped	8 inch wafer, 150um thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 2k Bytes memory, 50 pF input capacitance	-
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 1	Line 2	Line 3
NT3H2111W0FHK	211	-	-
NT3H2211W0FHK	221	-	-
NT3H2111W0FTT	32111	DBSN ASID	YWW
NT3H2211W0FTT	32211	DBSN ASID	YWW
NT3H2111W0FT1	NT32111	DBSN ASID	nDYWW
NT3H2211W0FT1	NT32211	DBSN ASID	nDYWW

Used abbreviations:

DBSN: Diffusion Batch Sequence Number

ASID: Assembly Sequence ID

n: Assembly Centre Code

D: RHF-2006 indicator

Y: year

WW: week

6 Block diagram

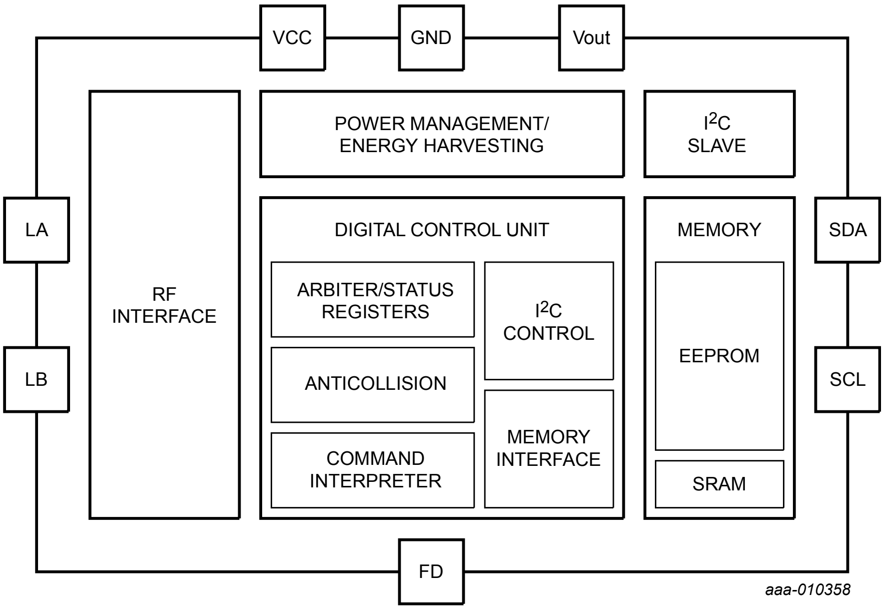
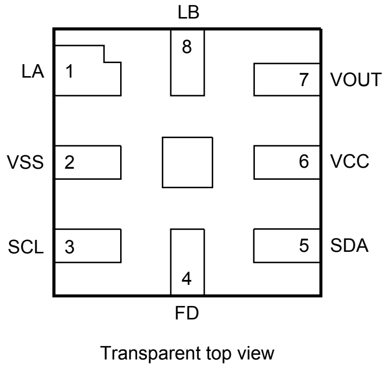


Figure 2. Block diagram

7 Pinning information

7.1 Pinning

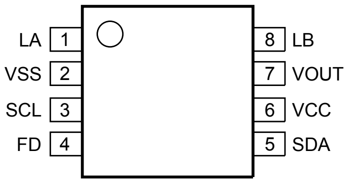
7.1.1 XQFN8



aaa-021647

Figure 3. Pin configuration for XQFN8

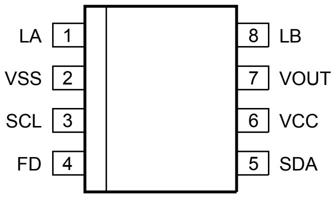
7.1.2 TSSOP8



aaa-021648

Figure 4. Pin configuration for TSSOP8

7.1.3 SO8



aaa-021649

Figure 5. Pin configuration for SO8

7.2 Pin description

Table 3. Pin description for XQFN8, TSSOP8 and SO8

Pin	Symbol	Description
1	LA	Antenna connection LA
2	VSS	GND
3	SCL	Serial clock I^{2}C
4	FD	Field detection
5	SDA	Serial data I^{2}C
6	VCC	VCC in connection (external power supply)
7	VOUT	Voltage out (energy harvesting)
8	LB	Antenna connection LB

8 Functional description

8.1 Block description

NTAG I^{2}C *plus* ICs consist of EEPROM, SRAM, NFC interface, Digital Control Unit (Command interpreter, Anticollision, Arbiter/Status registers, I^{2}C control and Memory Interface), Power Management and Energy Harvesting Unit and an I^{2}C slave interface. Energy and data are transferred via an antenna consisting of a coil with a few turns, which is directly connected to NTAG I^{2}C *plus* IC.

8.2 NFC interface

The passive NFC-interface is based on the ISO/IEC 14443-3 Type A standard.

It requires to be supplied by an NFC field (e.g. NFC enabled device) always to be able to receive appropriate commands and send the related responses.

As defined in ISO/IEC 14443-3 Type A for both directions of data communication, there is one start bit (start of communication) at the beginning of each frame. Each byte is transmitted with an odd parity bit at the end. The least significant bit of the byte 0 of the selected block is transmitted first.

For a multi-byte parameter, the least significant byte is always transmitted first. For example, when reading from the memory using the READ command, byte 0 from the addressed block is transmitted first, followed by bytes 1 to byte 3 out of this block. The same sequence continues for the next block and all subsequent blocks.

8.2.1 Data integrity

The following mechanisms are implemented in the contactless communication link between the NFC device and the NTAG I^{2}C *plus* IC to ensure very reliable data transmission:

- 16 bits CRC per block
- Parity bits for each byte
- Bit count checking
- Bit coding to distinguish between "1", "0" and "no information"
- Channel monitoring (protocol sequence and bit stream analysis)

The commands are initiated by the NFC device and controlled by the Digital Control Unit of the NTAG I^{2}C *plus* IC. The command response depends on the state of the IC, and for memory operations, the access conditions valid for the corresponding page.

8.2.2 NFC state machine

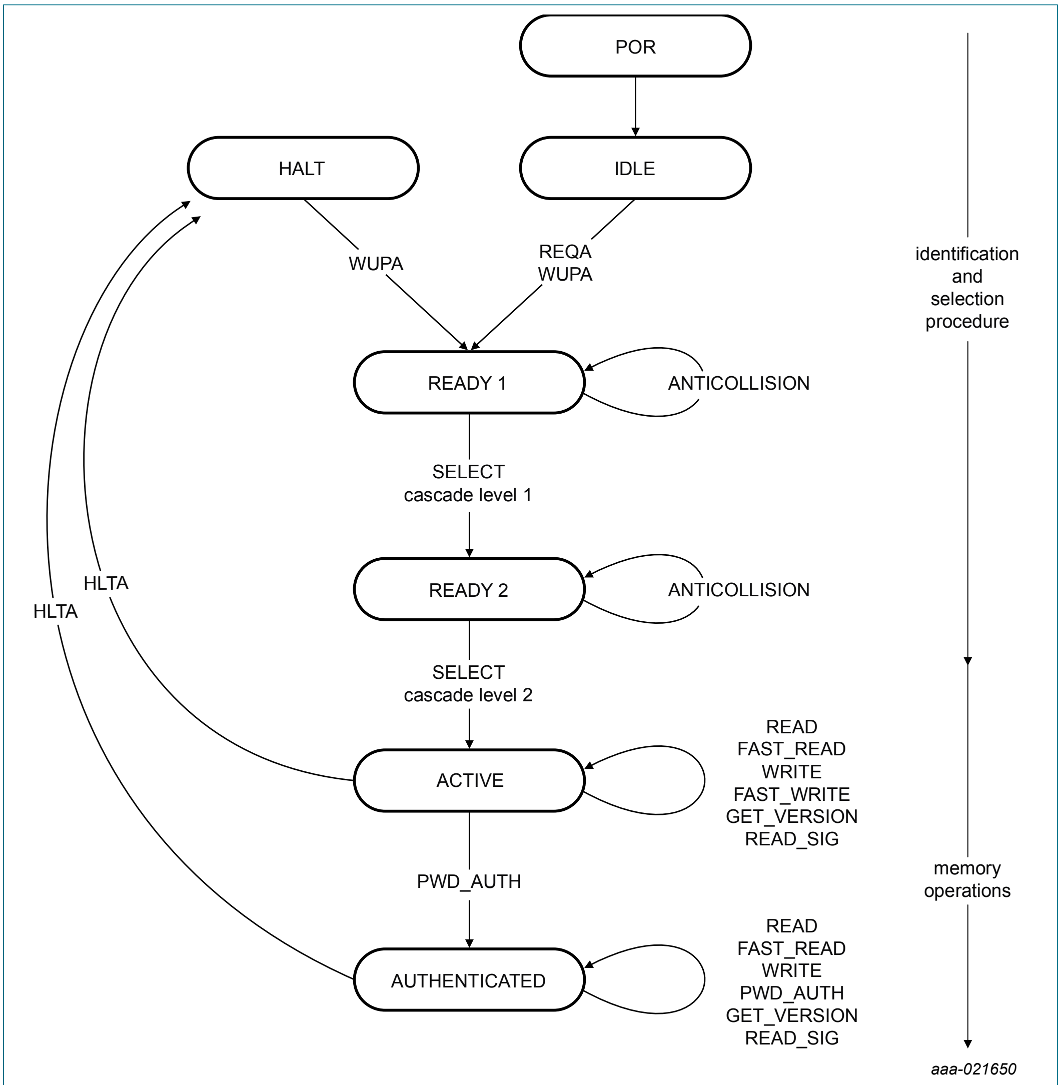


Figure 6. NFC state machine of NTAG I²C *plus*

The overall NFC state machine is summarized in Figure 6. When an error is detected or an unexpected command is received, in each state the tag returns to IDLE or HALT state as defined in ISO/IEC 14443-3 Type A.

8.2.2.1 IDLE state

After a Power-On Reset (POR), the NTAG I²C *plus* switches to the default waiting state, namely the IDLE state. It exits IDLE towards READY 1 state when a REQA or a WUPA command is received from the NFC device. Any other data received while in IDLE state is interpreted as an error, and the NTAG I²C *plus* remains in the IDLE state.

8.2.2.2 READY 1 state

In the READY 1 state, the NFC device resolves the first part of the UID (3 bytes) using the ANTICOLLISION or SELECT commands for cascade level 1. READY 1 state is correctly exited after.

- receiving SELECT command from cascade level 1 with the matching of complete first part of the UID. In this case, the NFC device switches the NTAG I^{2}C *plus* into READY 2 state where the second part of the UID gets resolved.

Remark: The response of the NTAG I^{2}C *plus* to the SELECT command is the Select AcKnowledge (SAK) byte with cascade bit set to 1b indicating that UID is not complete.

8.2.2.3 READY 2 state

In the READY 2 state, the NFC device resolves the second part of the UID (4 bytes) using the ANTICOLLISION or SELECT command for cascade level 2. READY2 state is correctly exited after.

- receiving SELECT command from cascade level 2 with the matching of complete second part of the UID. In this case, the NFC device switches the NTAG I^{2}C *plus* into ACTIVE state where all application-related commands can be executed.

Remark: The response of the NTAG I^{2}C *plus* to the SELECT command in READY 2 state is the Select AcKnowledge (SAK) byte with cascade bit cleared to indicate, that NTAG I^{2}C *plus* is now uniquely selected and only this device will communicate with the NFC device even when other contactless devices are present in the NFC device field.

8.2.2.4 ACTIVE state

All unprotected memory operations are operated in the ACTIVE and AUTHENTICATED states.

The ACTIVE state is exited with the PWD_AUTH command or with the HLTA command.

Upon reception of a correct password within PWD_AUTH command, the NTAG I^{2}C *plus* transits to AUTHENTICATED state after responding with PACK.

With the HLTA command, the NTAG I^{2}C *plus* transits to the HALT state.

Any other invalid command in ACTIVE state is interpreted as an error. Depending on its previous state, the NTAG I^{2}C *plus* returns to either to the IDLE or HALT state.

8.2.2.5 AUTHENTICATED state

Protected memory operations are only operated in the AUTHENTICATED state, however access to the unprotected memory is possible, too.

The AUTHENTICATED state is exited with the HLTA command and upon reception, the NTAG I^{2}C *plus* transits to the HALT state.

Any other invalid command in AUTHENTICATED state is interpreted as an error. Depending on its previous state, the NTAG I^{2}C *plus* returns to either to the IDLE or HALT state.

8.2.2.6 HALT state

HALT and IDLE states constitute the two waiting states implemented in the NTAG I^{2}C *plus*. An already processed NTAG I^{2}C *plus* in ACTIVE or AUTHENTICATED state can be set into the HALT state using the HLTA command. In the anticollision phase, this state helps the NFC device distinguish between processed tags and tags yet to be selected. The NTAG I^{2}C *plus* can only exit HALT state upon execution of the WUPA command. Any other data received when the device is in this state is interpreted as an error, and NTAG I^{2}C *plus* state remains unchanged.

8.3 Memory organization

The memory map is detailed in Table 4 (1k memory) and Table 5 (2k memory) from the NFC interface and in Table 6 (1k memory) and Table 7 (2k memory) from the I^{2}C interface. The SRAM memory is only available and accessible when powered via VCC. Please refer to Section 11 for examples of memory map from the NFC interface with SRAM mapping.

The structure of manufacturing data, static and dynamic lock bytes, capability container and user memory pages are compatible with other NTAG products.

Any memory access which starts at a valid address and extends into an invalid access region will return 00h value for the invalid region.

8.3.1 Memory map from NFC perspective

Memory access from the NFC perspective is organized in pages of 4 bytes each. If password protection is not used, complete user memory is unprotected.

Table 4. NTAG I^2C *plus* 1k memory organization from the NFC perspective

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
0	0	00h	Serial number (UID)				READ	
	1	01h	Serial number (UID)			Internal	READ	
	2	02h	Internal		Static lock bytes		READ/R&W	
	3	03h	Capability Container (CC)				READ&WRITE	
	4	04h	Unprotected user memory				READ&WRITE	
	...	...						
	AUTH0	AUTH0	Protected user memory				READ[1]	READ&WRITE
	...	...						
	225	E1h						
	226	E2h	Dynamic lock bytes			00h	R&W/READ	
	227	E3h	RFU	RFU	RFU	AUTH0	READ[1]	READ&WRITE
	228	E4h	ACCESS	RFU	RFU	RFU	READ[1]	READ&WRITE
	229	E5h	PWD[2]				READ[1]	READ&WRITE
	230	E6h	PACK[2]		RFU	RFU	READ[1]	READ&WRITE
	231	E7h	PT_I2C	RFU	RFU	RFU	READ[1]	READ&WRITE
	232	E8h	Configuration registers				see 8.3.12	
	233	E9h						
	234	EAh	Invalid access - returns NAK				n.a.	
	235	EBh						
	236	ECh	Session registers				see 8.3.12	
	237	EDh						
	238	EEh	Invalid access - returns NAK				n.a.	
	239	EFh						
	240	F0h	Invalid access - returns NAK				n.a.	
	...	...						
	255	FFh						
1	...	...	Invalid access - returns NAK				n.a.	
2	...	...	Invalid access - returns NAK				n.a.	
3	0	00h	Invalid access - returns NAK				n.a.	
	...	...						
	248	F8h	Mirrored session registers				see 8.3.12	
	249	F9h						

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
	...	...	Invalid access - returns NAK				n.a.	
	255	FFh						

[1] If NFC_PROT bit is set to 1b, NTAG I^{2}C *plus* returns NAK

[2] On reading PWD or PACK, NTAG I^{2}C *plus* always returns 00h for all bytes

Table 5. NTAG I^{2}C *plus* 2k memory organization from the NFC perspective

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
0	0	00h	Serial number (UID)				READ	
	1	01h	Serial number (UID)			Internal	READ	
	2	02h	Internal		Static lock bytes		READ/R&W	
	3	03h	Capability Container (CC)				READ&WRITE	
	4	04h	Unprotected user memory				READ&WRITE	
	...	...						
	AUTH0	AUTH0	Protected user memory				READ[1]	READ&WRITE
	...	...						
	225	E1h						
	226	E2h	Dynamic lock bytes			00h	R&W/READ	
	227	E3h	RFU	RFU	RFU	AUTH0	READ[1]	READ&WRITE
	228	E4h	ACCESS	RFU	RFU	RFU	READ[1]	READ&WRITE
	229	E5h	PWD[2]				READ[1]	READ&WRITE
	230	E6h	PACK[2]		RFU	RFU	READ[1]	READ&WRITE
	231	E7h	PT_I2C	RFU	RFU	RFU	READ[1]	READ&WRITE
	232	E8h	Configuration registers				see 8.3.12	
	233	E9h						
	234	EAh	Invalid access - returns NAK				n.a.	
	235	EBh						
	236	ECh	Session registers				see 8.3.12	
	237	EDh						
	238	EEh	Invalid access - returns NAK				n.a.	
	...	...						
	255	FFh						
1	0	00h	(Un-)protected user memory[3,4]				see protected user memory in Sector 0	
	...	...						
	255	FFh						
2	...	...	Invalid access - returns NAK				n.a.	
3	0	00h	Invalid access - returns NAK				n.a.	
	...	...						
	248	F8h	Mirrored session registers				see 8.3.12	
	249	F9h						

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
	...	...	Invalid access - returns NAK				n.a.	
	255	FFh						

[1] If NFC_PROT bit is set to 1b, NTAG I^2C *plus* returns NAK

[2] On reading PWD or PACK, NTAG I^2C *plus* always returns 00h for all bytes

[3] If 2K_PROT bit is set to 1b, complete Sector 1 of NTAG I^2C *plus* is password protected

[4] If NFC_DIS_SEC1 bit is set to 1b, complete Sector 1 of NTAG I^2C *plus* is not accessible from NFC perspective

8.3.2 Memory map from I^{2}C interface

The memory access of NTAG I^{2}C *plus* from the I^{2}C interface is organized in blocks of 16 bytes each.

I²C slave address is stored in most significant 7 bits of byte 0 in block 0. However, when reading block 0, NTAG I^{2}C *plus* always returns 04h for byte 0.

WARNING: When configuring Static lock bytes and Capability container, Address byte gets updated, too. Address byte consists of slave address (coded in most significant 7 bits) and least significant bit set to 0b.

REMARK: For convenience reasons it is recommended to configure Address byte (block 0, byte 0) to 04h.

Table 6. NTAG I^2C *plus* 1k memory organization from the I^2C perspective

I^2C block address		Byte number within a block				Access conditions		
		0	1	2	3	I^2C_PROT		
		4	5	6	7			
		8	9	10	11	00b	01b	1xb
Dec.	Hex.	12	13	14	15			
0	00h	Addr.[1]	Serial number (UID)			READ&WRITE		
		Serial number (UID)			Internal			
		Internal		Static lock bytes				
		Capability Container (CC)						
1	01h	Unprotected user memory				READ&WRITE		
...	...							
AUTH0	AUTH0	Protected user memory				READ&WRITE	READ	NAK
...	...							
55	37h							
56	38h	Protected user memory				READ&WRITE	READ	NAK
		Dynamic lock bytes			00h	READ&WRITE		
		RFU	RFU	RFU	AUTH0			
57	39h	ACCESS	RFU	RFU	RFU			
		PWD[2]						
		PACK[2]		RFU	RFU			
		PT_I2C	RFU	RFU	RFU			
58	3Ah	Configuration registers				see 8.3.12		
		00h	00h	00h	00h	READ		
		00h	00h	00h	00h			
59	3Bh	Invalid access - returns NAK				n.a.		
...	...							
247	F7h							
248	F8h	SRAM memory (64 bytes)				READ&WRITE		
...	...							
251	FBh							
...	...	Invalid access - returns NAK				n.a.		
254	FEh	Session registers				see 8.3.12		
		00h	00h	00h	00h	READ		

I^2C block address		Byte number within a block				Access conditions		
		0	1	2	3	I^2C_PROT		
		4	5	6	7			
		8	9	10	11	00b	01b	1xb
Dec.	Hex.	12	13	14	15			
		00h	00h	00h	00h			
255	FFh	Invalid access - returns NAK				n.a.		

[1] The byte 0 of block 0 is always read as 04h (UID0). Writing to block 0 updates the I^2C address.

[2] On reading PWD and PACK, NTAG I^2C *plus* always returns 00h for all bytes

Table 7. NTAG I^2C *plus* 2k memory organization from the I^2C perspective

I^2C block address		Byte number within a block				Access conditions		
		0	1	2	3	I^2C_PROT		
		4	5	6	7			
		8	9	10	11	00b	01b	1xb
Dec.	Hex.	12	13	14	15			
0	00h	Addr.[1]	Serial number (UID)			READ&WRITE		
		Serial number (UID)			Internal			
		Internal		Static lock bytes				
		Capability Container (CC)						
1	01h	Unprotected user memory				READ&WRITE		
...	...							
AUTH0	AUTH0	Protected user memory				READ&WRITE	READ	NAK
...	...							
56	38h	Protected user memory				READ&WRITE	READ	NAK
		Protected user memory						
		Dynamic lock bytes			00h	READ&WRITE		
		RFU	RFU	RFU	AUTH0			
57	39h	ACCESS	RFU	RFU	RFU			
		PWD[2]						
		PACK[2]		RFU	RFU			
		PT_I2C	RFU	RFU	RFU			
58	3Ah	Configuration registers				see 8.3.12		
		00h	00h	00h	00h	READ		
		00h	00h	00h	00h			
...	...	Invalid access - returns NAK				n.a.		
64	40h	(Un-)protected user memory				READ&WRITE	READ	NAK
...	...							
127	7Fh							
...	...	Invalid access - returns NAK				n.a.		
248	F8h	SRAM memory (64 bytes)				READ&WRITE		
...	...							
251	FBh							
...	...	Invalid access - returns NAK				n.a.		

I^{2}C block address		Byte number within a block				Access conditions		
		0	1	2	3	I^{2}C_PROT		
		4	5	6	7			
		8	9	10	11	00b	01b	1xb
Dec.	Hex.	12	13	14	15			
254	FEh	Session registers				see 8.3.12		
		00h	00h	00h	00h	READ		
		00h	00h	00h	00h			
255	FFh	Invalid access - returns NAK				n.a.		

[1] The byte 0 of block 0 is always read as 04h (UID0). Writing to block 0 updates the I^{2}C address.

[2] On reading PWD and PACK, NTAG I^{2}C *plus* always returns 00h for all bytes

8.3.3 EEPROM

The EEPROM is a non-volatile memory that stores the 7 byte UID, the memory lock conditions, IC configuration information and the user memory.

Sector 0 memory map looks totally the same for NTAG I^{2}C *plus* 1k and 2k version, the only difference is the dynamic lock bit granularity.

NXP introduced with NTAG I^{2}C *plus* the possibility to split the memory in an open and a password protected area see Section 8.3.11.

8.3.4 SRAM

For frequently changing data, a volatile memory of 64 bytes with unlimited endurance is built in. The 64 bytes are mapped in a similar way as done in the EEPROM, i.e., 64 bytes are seen as 16 pages of 4 bytes from NFC perspective.

The SRAM is only available when the tag is powered via the VCC pin.

The SRAM is located at the end of the memory space and it is always directly accessible by the I^{2}C host (addresses F8h to FBh). An NFC device cannot access the SRAM memory in normal mode (i.e., outside the pass-through mode). The SRAM is only accessible by the NFC device if the SRAM is mirrored onto the EEPROM memory space.

With SRAM mirror enabled (SRAM_MIRROR_ON_OFF = 1b - see Section 11.2), the SRAM can be mirrored in the User Memory from start page 01h to 74h for access from the NFC side.

The Memory mirror must be enabled once both interfaces are ON as this feature is disabled after each POR.

The register SRAM_MIRROR_BLOCK (see Table 14) indicates the address of the first page of the SRAM buffer. In the case where the SRAM mirror is enabled and the READ command is addressing blocks where the SRAM mirror is located, the SRAM byte values will be returned instead of the EEPROM byte values. Similarly, if the tag is not VCC powered, the SRAM mirror is disabled and reading out the bytes related to the SRAM mirror position would return the values from the EEPROM.

In the pass-through mode (PTHRU_ON_OFF = 1b - see Section 8.3.12), the SRAM is mirrored to the fixed address F0h - FFh for NFC access (see Section 11) in the first memory sector (Sector 0) of NTAG I^{2}C *plus*.

8.3.5 Serial number (UID)

The unique 7-byte serial number (UID) is programmed into the first 7 bytes of memory covering page addresses 00h and 01h - see Figure 7. These bytes are programmed and write protected during production.

UID0 is fixed to the value 04h - the manufacturer ID for NXP Semiconductors in accordance with ISO/IEC 14443-3.

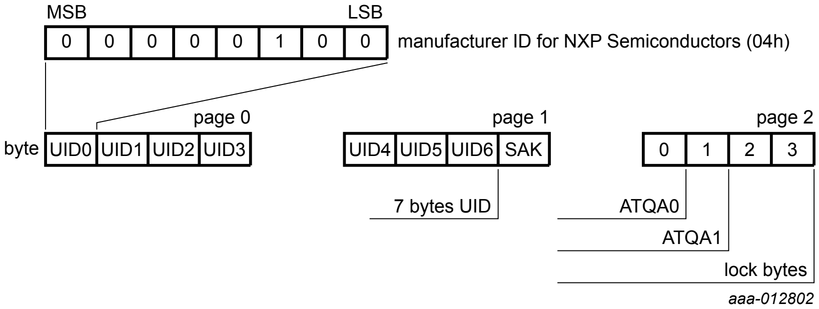


Figure 7. Serial number (UID)

8.3.6 Static Lock Bytes

According to NFC Forum Type 2 Tag specification, the bits of byte 2 and byte 3 of page 02h (via NFC) or byte 10 and 11 address 00h (via I^{2}C) represent the field programmable, read-only locking mechanism (see Figure 8). Each page from 03h (CC) to 0Fh can be individually locked by setting the corresponding locking bit to logic 1b to prevent further write access. After locking, the corresponding page becomes read-only memory.

In addition, NTAG I^{2}C *plus* uses the three least significant bits of lock byte 0 as the block-locking bits. Bit 2 controls pages 0Ah to 0Fh (via NFC), bit 1 controls pages 04h to 09h (via NFC) and bit 0 controls page 03h (CC). Once the block-locking bits are set, the locking configuration for the corresponding memory area is frozen, e.g. cannot be changed to read-only anymore.

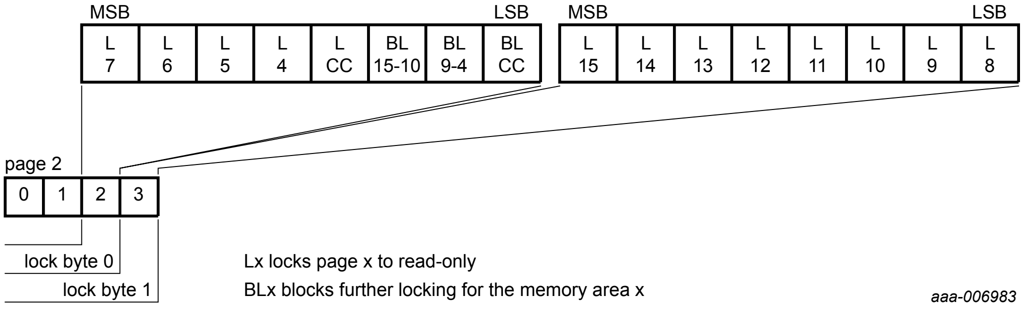


Figure 8. Static lock bytes 0 and 1

For example, if BL15-10 is set to logic 1b, then bits L15 to L10 (lock byte 1, bit[7:2]) can no longer be changed. The static locking and block-locking bits are set by the bytes 2 and 3 of the WRITE command to page 02h. The contents of the lock bytes are bit-wise OR'ed and the result then becomes the new content of the lock bytes. This process is irreversible from NFC perspective. If a bit is set to logic 1b, it cannot be changed back to logic 0b. From I²C perspective, the bits can be reset to 0b by writing bytes 10 and 11 of block 00h. As I²C address is coded in byte 0 of block 0, it may be changed unintentionally.

The contents of bytes 0 and 1 of page 02h (via NFC) are unaffected by the corresponding data bytes of the WRITE command.

The default value of the static lock bytes is 0000h.

8.3.7 Dynamic Lock Bytes

To lock the pages of NTAG I²C *plus* starting at page address 16 and onwards, the dynamic lock bytes are used. The dynamic lock bytes are located in Sector 0 at page E2h. The three lock bytes cover the memory area of 840 data bytes (NTAG I²C *plus* 1k) or 1864 data bytes (NTAG I²C *plus* 2k). The granularity is 16 pages for NTAG I²C *plus* 1k (see Figure 9) and 32 pages for NTAG I²C *plus* 2k (see Figure 10) compared to a single page for the first 48 bytes (see Figure 8).

NTAG I²C *plus* needs a Lock Control TLV as specified in NFC Forum Type 2 Tag specification to ensure NFC Forum Type 2 Tag compliancy.

When NFC Forum Type 2 Tag transition to READ ONLY state is intended, all bits marked as RFUI and dynamic lock bits related to the protected area shall be set to 0b when writing to the dynamic lock bytes.

The default value of the dynamic lock bytes is 000000h. The value of Byte 3 is always 00h when read.

Like for the static lock bytes, this process of modifying the dynamic lock bits is irreversible from NFC perspective. If a bit is set to logic 1b, it cannot be changed back to logic 0b. From I²C interface, these bits can be set to 0b again.