AN14513

NTAG X DNA - Dual Interface

Rev. 1.0 — 27 May 2025 Application note

Document information

Information	Content
Keywords	NTAG X DNA, Dual Interface, I²C, GPIO, NFC
Abstract	This document provides assistance in NFC system development and describes the main features of NTAG X DNA Dual Interface - I²C, NFC and GPIO coexistence.

1 Introduction

This document focuses on showing how to use NTAG X DNA Dual Interface feature.

This document addresses developers who are developing applications based on NTAG X DNA. This document shall be used in addition to the NTAG X DNA data sheet ref.[3]. The best use of this application note is achieved by reading the mentioned data sheet in advance.

Note: *This application note does not replace any of the relevant functional specifications, data sheets, or design guides.*

2 Target applications

NTAG X DNA offers a wide area of implementations due to its rich features and sophisticated as well as simple high security. Including, but not limited to, see the following examples:

Accessories

- Mobile phones
  - Cases/covers
  - Game controllers
  - Ear pods
  - Battery packs
  - Cables
  - Headsets
  - Camera attachments
  - more...
- Wall chargers
- USB-C protocol based
- Input devices (for example, tablet pens)

IoT security

- Smart speakers
- Access points
- Smart thermostats
- Security cameras
- Video doorbells
- Home door locks
- Smart appliances
- Energy storage
- eBikes
- Industrial controllers
- Smart meters

Medical

- Smart injectors
- Authentication of vials

Components

- Rechargeable Batteries

3 Types of applications

3.1 Contactless only

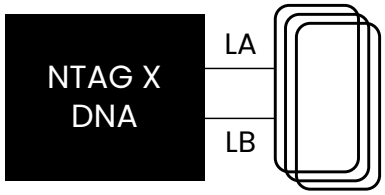

Figure 1. Block diagram - NFC interface only

- Interfaces: NFC
- Possible applications (not limited to):
  - Accessory authentication (Phone Case/Cover/etc.)
  - Consumables authentication
  - NFC Digital Product Passport (NDPP)
- Protocol: NFC (Type4Tag) + ECC Signature Secure Dynamic Messaging, ISO7816-4 incl. mutual auth

The contactless supply use case is the typical use case of a passive RFID card. The IC is supplied via a 13.56 MHz RF field and communicates via the ISO/IC14443 (Layer 4) interface over LA and LB. All other pins are not used for this use case. All other unused pins shall be either not connected or, for example, as in a flip-chip assembly - shorted/connected.

Example applications:

Below diagrams show typical NFC only NTAG X DNA applications:

- NFC mobile app-less (Android, iOS) cloud-based Secure-Dynamic-Messaging-based authentication and signature verification Figure 2

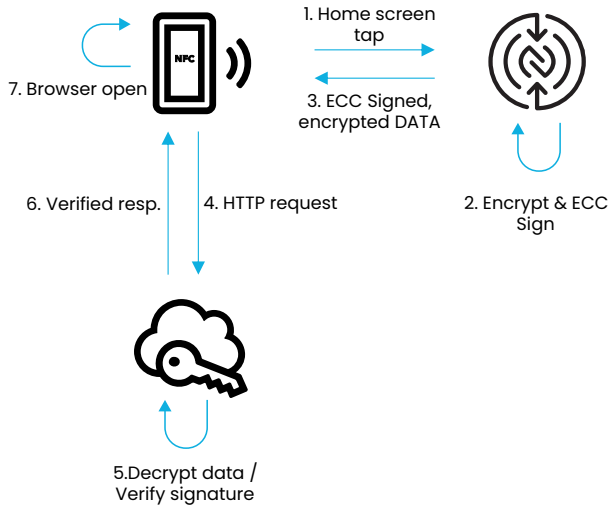

Figure 2. Example for NFC interface only: No NFC mobile application (Home screen NFC reading) - Cloud-based (automatic) system flow

- The diagram below shows a typical NFC-mobile-application-based system. In this case NFC mobile can trigger standard or custom commands to fetch (sensitive) data from NTAG X DNA Figure 3

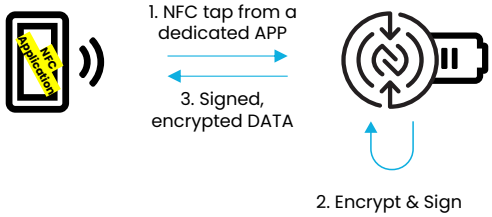

Figure 3. Example for NFC interface only: NFC-mobile-application-based NDPP example

In Figure 4 an example schematic of an NFC only tag is shown.

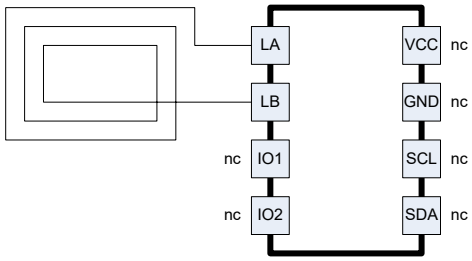

Figure 4. Example schematics - NFC interface only

3.2 Contact-based supply

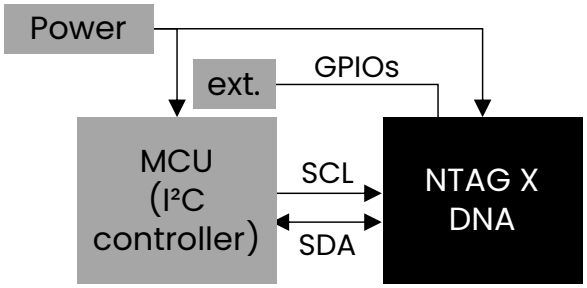

Figure 5. Example schematics - contact-based supply only

In contact-based supply operation the IC is powered via the VCC pin and only communicating via the I²C interface (SCL, SDA pins). The two general purpose IO pins GPIO1 and GPIO2 can be used for arbitrary input and output functionality (for example, sensing a digital input, putting signals as output etc.). Supply voltage range is either 1.1V typical (minimum 1.0V) or 1.8V typical (maximum 2.0V). I²C communication speed is up to Fast-mode Plus (1 Mbit/s). All pads are directly supplied via the VCC supply pin.

Typical applications are authentication of accessories, storing and using secret key material in a high-secure IC while the connected host (microcontroller) has only a functional application. Current consumption in contact-based application is up to 15 mA (from the VCC pin).

Deep Power-down mode can be entered with a command or timeout. There are configurable wake-up conditions (configurable SDA pulldown, correct I^2C follower address, existing RF field).

General design recommendations:

Power-on reset

- Host controller to control NTAGs V_{CC} (to perform a power-on reset).
- It is possible to supply A30 via the MCU/MPU GPIO. The GPIO shall be able to deliver current up to 15 mA.

NTAG X DNA can trigger a Reset via T=1‘ over I^2C protocol.

- Proprietary NXP S-Blocks SE chip reset request/response (ISO7816)

NTAG X DNA enables Deep Power Down via T=1‘ over I^2C protocol.

- Proprietary NXP S-Block Deep Power Down request/response

Example applications:

- Accessory authentication: for example, cables, adapters, headsets, docking stations, HID (game controller, keyboard, mouse), printer cartridges, etc.
- Cryptocoprocessor for the host

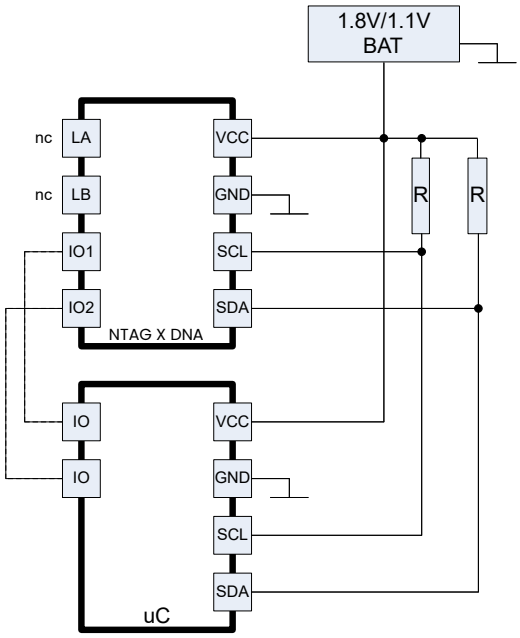

Figure 6. Example schematics - Contact-based supply

3.3 Dual-interface supply

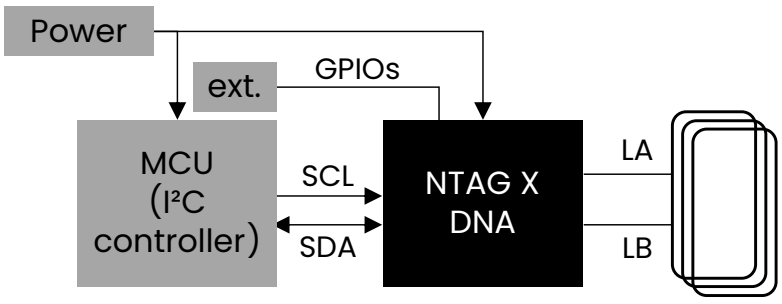

Figure 7. Block diagram: Accessory authentication - VDD powered

In the dual-interface supply mode the IC has a permanent direct connection of the supply from a permanent power supply (for example, battery) via the V_{CC} pin, within the given specification limit (1.0 V to 1.98 V). In this mode, the NTAG X DNA IC is connected on one side to an I²C controller (for example, a microcontroller) and on the contactless interface communicating with an NFC reader. NTAG X DNA provides mechanisms to control data flow either from MCU → NFC or vice versa. "NFC Pause" Section 4.1.5 is one of the unique features that NTAG X DNA supports, and only possible in NFC Forum T4T.

A state diagram of NTAG X DNA can be found in chapter Section 4.2.1.

The NTAG X DNA can be put into a deep Power-down mode (5 µA current consumption). The wake-up can happen either through I²C activity or from an ISO/IEC14443 field.

Dual Interface also covers NFC and NTAG X DNA's GPIO co-existence.

- Interfaces: NFC (antenna connected to LA, LB), I²C, and GPIO
- Possible applications (not limited to):
  - Monitoring/Checking Status (i.e. Smart metering)
  - Activating/Provisioning credentials (i.e. activate new function)
  - Secure MCU firmware update via NFC (instead of BLE)
- Protocol: Global Platform T=1 over I²C + NFC (Type4Tag) + ECC Signature

Example applications:

- IoT
- Medical wearable devices (for example, glucose meter)

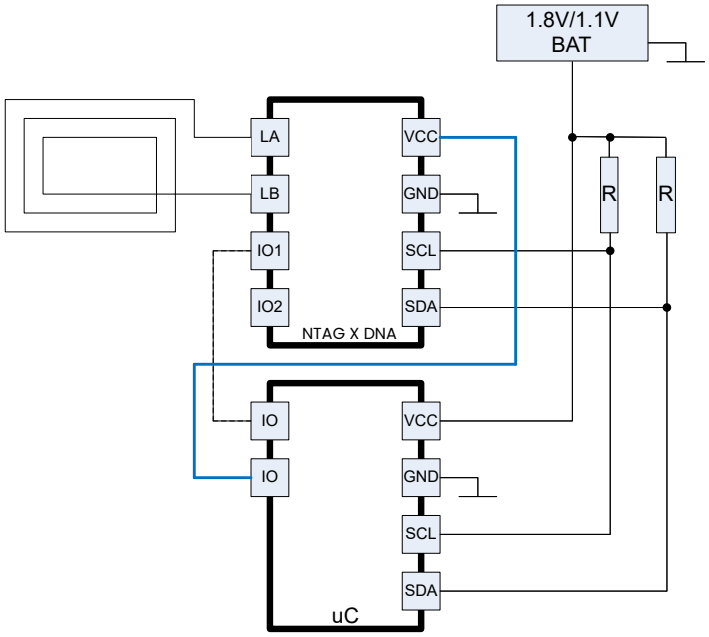

Figure 8. Example schematics - Dual-interface-based supply

3.4 Special use case: Energy harvesting

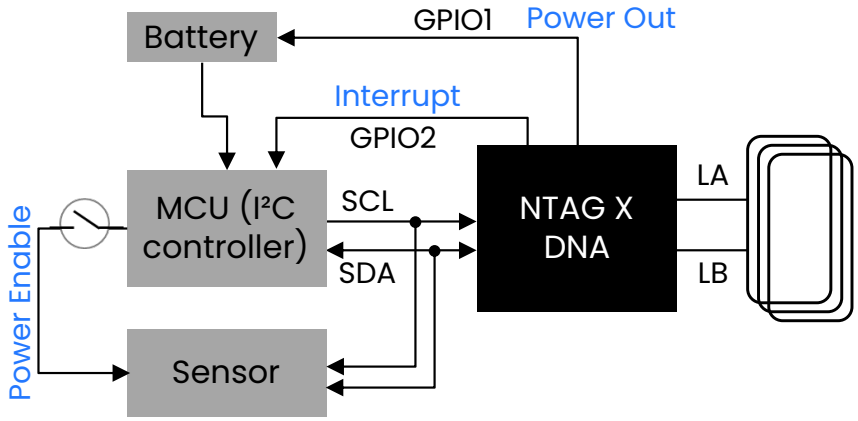

Figure 9. Block diagram: Energy harvesting

A circuit example is shown in the following figure Figure 10. RF field is coming via LA/LB interface, while the default state of the power harvesting feature is OFF at startup. After a dedicated command (Cmd.ManageGPIO, Operation byte Bit 1 - "MEASURE: execute measurement"), a potential energy yield can be measured. After that, the energy harvesting feature can be enabled, which puts out the regulated voltage on the GPIO1 pin. It can be assumed that an enough large capacitance is connected at the output of the GPIO1 pin to stabilize ISO14443 PCD → PICC Miller pauses.

In case there is no further activity on any of the I²C pins or back supply from VCC, the energy harvesting output is kept enabled until a command disables it or if the RF field gets disabled by the reader. This configuration is always done via software.

The principle of this use case is that a part of the power that is transmitted via the RF field and that is not needed for the internal operation of the NTAG X DNA can be output to a GPIO1 pin and can be used for supplying directly another device, charging a battery or capacitance.

The power output can reach ~10 mW, which at a maximum output voltage of 1.8 V (max. up to 2.0V) results in a current of ~5.5 mA. Note that the available field strength must be large enough (for example, if a Class 1 antenna is targeted, field strength shall be over 3.5 A/m).

For applications where more power is required, "alternative NFC field harvesting" is recommended through NXP wireless charging products or passive components with additional rectifier.

- Interfaces: NFC, I²C, and GPIO
- Possible applications (not limited to):
  - Medical wearables (smart diagnostics)
  - Monitoring/Checking Status (i.e. Smart metering)
  - Activating/Provisioning credential (i.e. activate new function)
  - Firmware update via NFC (instead of BLE)
- Protocol: NFC (Type4Tag) + ECC Signature Secure Dynamic Messaging, ISO7816-4 incl. mutual auth, GPIO Interrupts

Example applications:

- Mobile cases with LEDs (with MCU or without MCU)
- Charging peripheral system

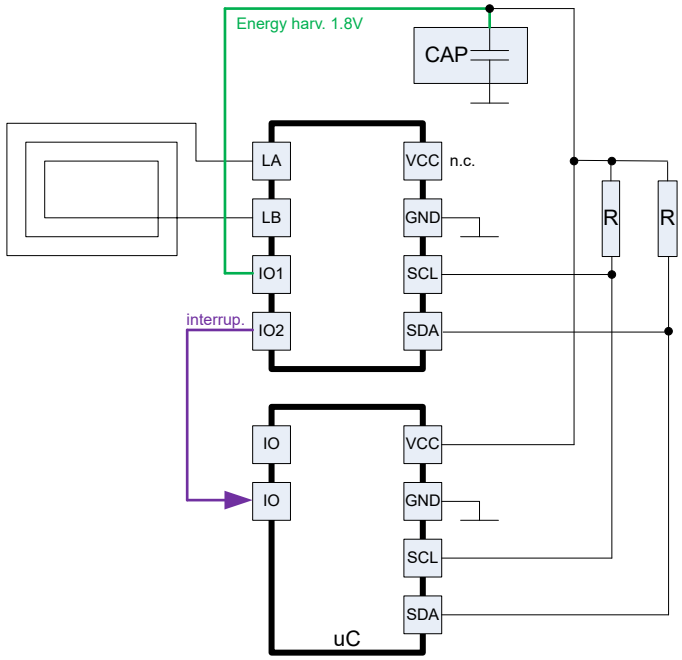

Figure 10. Example schematics - Energy harvesting

Note: *More detailed information can be found in ref.[5]*

3.5 Special use case: IO pin control from contactless operation

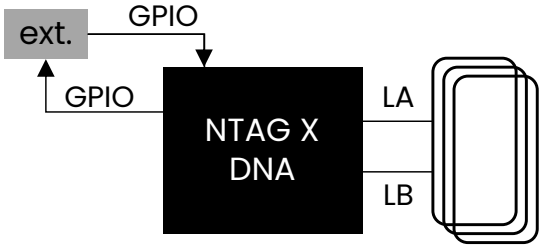

Figure 11. Block diagram: Block diagram: GPIO control from contactless

In this use case, the supply is only available via the contactless interface. The supply pins (VCC, GND) and the I2C pins (SCL, SDA) are not connected and not supplied internally. The two additional pins GPIO1 and GPIO2 can be used in this configuration as GPIOs.

An application where the IOs are used as output would be an LED that is placed at the output of the pin.

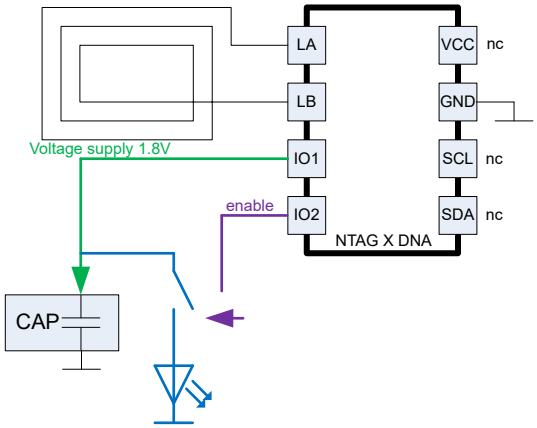

Figure 12. Example schematics - GPIO pin control from NFC, GPIO1 as energy source, GPIO2 as Output

Typical use cases are, where a pin is configured as input is for tag tamper detection or detection of pressing a button.

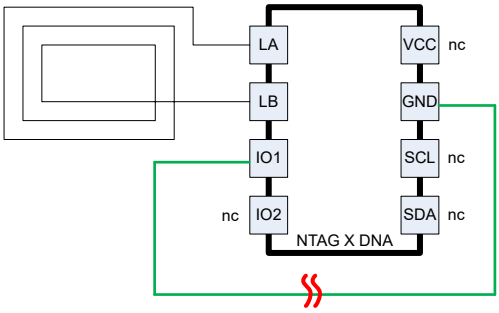

Figure 13. Example schematics - GPIO1 as Input, TagTamper detection

- Interfaces: NFC (LA/LB) + GPIO
- Possible applications (not limited to):
  - NTAG with status detection
  - NFC with action buttons
- Protocol: NFC (Type4Tag) + ECC Signature Secure Dynamic Messaging, ISO7816-4 incl. mutual auth

4 Design/features examples

4.1 Main features examples

4.1.1 ManageGPIO

GPIOs can be toggled (set, clear, toggle) by use of the the ManageGPIO command from either the I²C or NFC interface. The command may require an authentication and CommMode.FULL, depending on SetConfig settings.

If a GPIO is configured for output, after a power-on reset, the GPIO will be initialized with the state as configured by the GPIOXConfig from SetConfiguration Option 0x11 on the first command after activation. This is independent of the state from a previous activation. Immediately after the PoR, output GPIOs will be in high-impedance (High-Z) state.

The following example shows how only an Authentic NFC reader/writer device can toggle GPIO1. Authentic NFC reader/writer device must perform mutual authentication (SIGMA-I or AES-128/256) prior to sending the Cmd.ManageGPIO command, to create a secure NFC communication channel. Note that the CommMode of the Cmd.ManageGPIO command can be changed by Cmd.SetConfig, Option byte 0x11 (for example, can be set in a way that no authentication is required for toggling GPIOx).

Prerequisites:

1. *Successful mutual authentication. For the example below the following values are assumed:*
   - *$K_{SesAuthMAC}$ = 72 12 CB E0 03 2E FA 8F 7F B0 5F A1 B4 9E B6 E3 (session key generated during AES-128 mutual authentication ref.[4])*
   - *TI = 50 E2 8E 06*
   - *CmdCtr = 02 00*
2. ManageGPIOAccessCondition for Cmd.SetConfig, GPIO Management option is set to:
   - CommMode: 0x1 (communication channel will be integrity protected with MAC signatures)
   - AccessCondition: 0x0 (only Key0x00 has access rights for the Cmd.ManageGPIO command).

Table 1. Cmd.ManageGPIO

Step	Command		Data
1	Cmd (INS) of Cmd.ManageGPIO	=	42
2	CommMode	=	CommMode.MAC
3	$K_{SesAuthMAC}$	=	7D 97 4D 25 C6 07 81 88 92 EE 9E 7C 39 C9 07 16
4	GPIONo (GPIO0)		00
5	Operation (SET: set the GPIO State to HIGH (driven)		01
6	CmdHeader (Step 5 || Step 6)		00 01
7	CMD || CmdCtr || TI [|| CmdHeader] [|| CmdData]	=	42 02 00 50 E2 8E 06 00 01
8	MAC($K_{SesAuthMAC}$; CMD || CmdCtr || TI [|| CmdHeader] [|| CmdData])	=	28 D6 3C F6 81 65 B4 F2 19 88 EC 8D 16 56 83 5E
9	MACt	=	D6 F6 65 F2 88 8D 56 5E

Table 1. Cmd.ManageGPIO*...continued*

Step	Command		Data
10	APDU	>	90 42 00 00 0A 00 01 D6 F6 65 F2 88 8D 56 5E 00
11	R-APDU	<	21 D1 F0 DB C3 1F 16 FC 91 00
12	PICC's MAC	=	21 D1 F0 DB C3 1F 16 FC
13	SW1 SW2	=	91 00
14	Verify Response MAC RC (SW2) || CmdCtr++ || TI [|| RespData]	=	00 03 00 50 E2 8E 06
15	MAC($K_{SesAuthMAC}$; RC || CmdCtr || TI [|| RespData])	=	AE 21 3D D1 F2 F0 CD DB 99 C3 21 1F 96 16 9C FC
16	MACt	=	21 D1 F0 DB C3 1F 16 FC
17	Compare MACt-s (from step 10 and step 15)	=	21 D1 F0 DB C3 1F 16 FC == 21 D1 F0 DB C3 1F 16 FC

Figure 14 shows response on Cmd.ManageGPIO in non-authenticated and authenticated state. GPIO1 is configured (Cmd.SetConfig) as AccessCondition: 0x0 (only Key0x00 has access rights for the Cmd.ManageGPIO command).

- First Cmd.ManageGPIO does not succeed to toggle GPIO1, because the NFC reader did not perform mutual authentication first.
- Second Cmd.ManageGPIO is successful, because of successful mutual authentication upfront with Key 0x00 (because of AccessCondition: 0x0 for GPIO1).

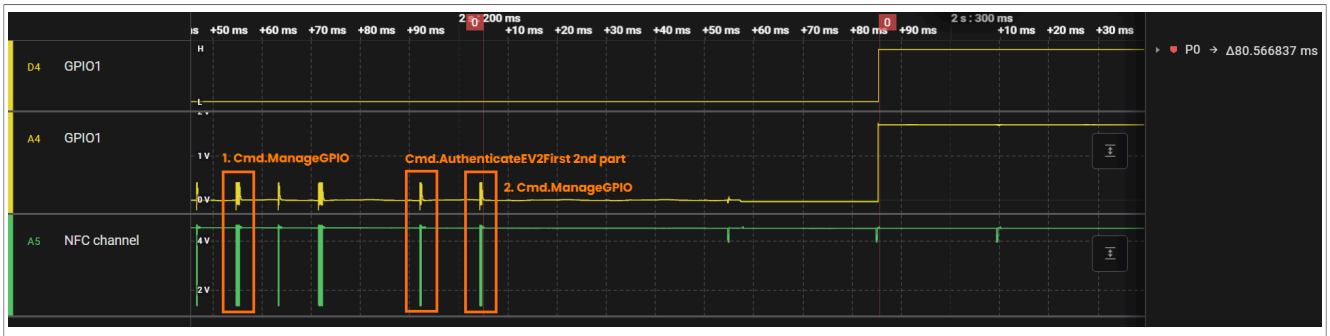

Figure 14. Cmd.ManageGPIO trace

Note: When executing a Cmd.ManageGPIO SET or MEASURE operation, or the combination of both, NTAG X DNA always returns a WTX over the NFC interface, before executing the operation. WTXes can be seen on Figure 14 as small ripples on the "NFC channel" until the GPIO1 toggle command is in process.

4.1.2 ReadGPIO

Cmd.ReadGPIO may be used to read the current status of the GPIOs. Status can be read of GPIOs configured either as an Output or Input.

Following example shows how an NFC reader/writer device can read the status of (all) GPIOs. Optionally, NFC reader/writer device can perform mutual authentication (SIGMA-I or AES-128/256) prior to sending the

Cmd.ReadGPIO command, to create a secure NFC communication channel. Note that the CommMode of the Cmd.ReadGPIO command can be changed by Cmd.SetConfig, Option byte 0x11 (for example, can be set in a way that no authentication is required for toggling GPIOx).

Prerequisites:

1. aGPIO1Conf, GPIO2Conf
2. ReadGPIOAccessCondition for Cmd.SetConfig, GPIO Management option is set to:
   - CommMode: 0x0 (communication channel is in PLAIN)
   - AccessCondition: 0xE ("free" access rights for Cmd.ReadGPIO command)

Table 2. Cmd.ReadGPIO

Step	Command		Data
1	Cmd (INS) of GetKeySettings	=	43
2	CommMode	=	CommMode.PLAIN
3	APDU	>	90 43 00 00 00
4	R-APDU	<	49 48 48 91 00
5	Response	=	49 48 48
6	GPIOByte0 (0x49 is N/A)	=	49
7	GPIOByte1 (0x48 is High)	=	48
8	GPIOByte2 (0x48 is High)	=	48

4.1.2.1 GPIO status mirroring in the NDEF message

The status of GPIOs can be automatically projected by NTAG X DNA itself. This feature makes it possible that any NFC Forum device (for example, mobile phone) - with simple tap from Home screen (no dedicated application running needed), gets values/statuses of GPIOs. The whole data payload is in the form of NDEF message (for example, URL). The mobile phone then makes a request to the verification server automatically, where data can be either decryptedor checked for authenticity and integrity. The feature is called SDM (Secure Dynamic Messaging). More details can be found in ref.[4].

Below is the example of NDEF message structure and how GPIO status can is mirrored into NDEF message automatically.

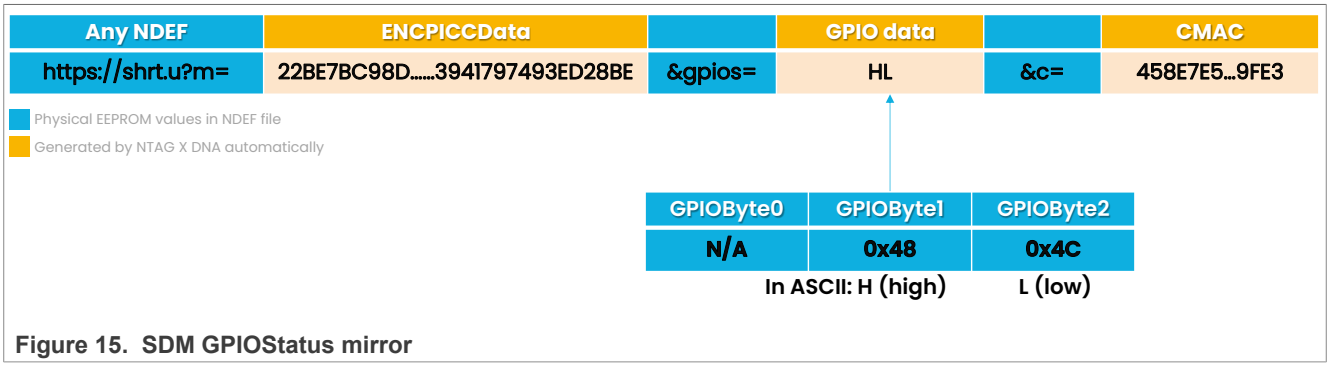

Figure 15. SDM GPIOStatus mirror

Note: *The GPIO status mirror can be encrypted on top, using the SDMENCFileData encryption option.*

4.1.3 Authentication notification

GPIOs can be toggled (set, clear) automatically by the IC, when successful mutual authentication is performed.

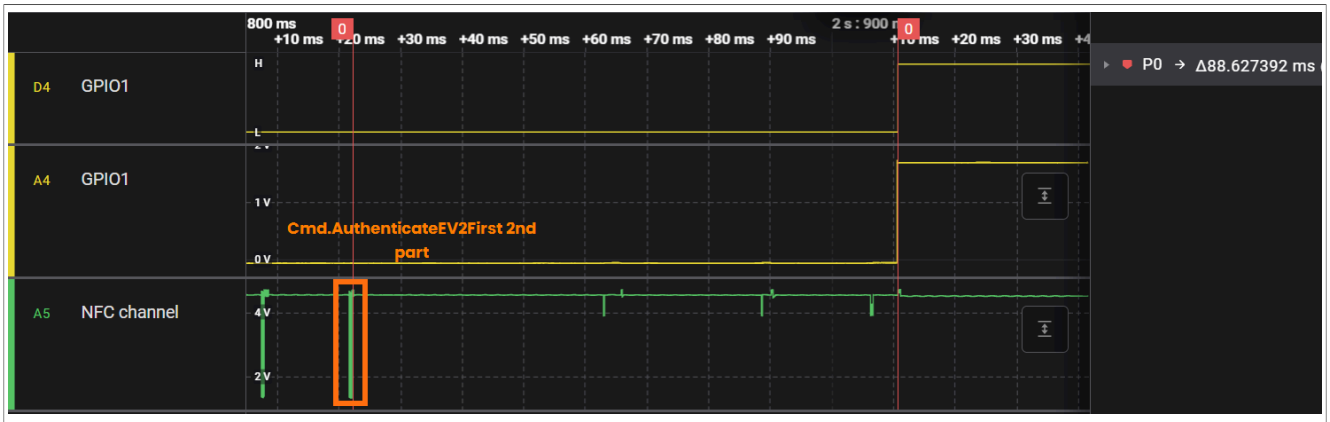

Figure 16. Successful Authentication notification

4.1.4 ISOSelectFile NDEF notification

GPIOs can be toggled (set, clear) automatically by IC, when the NFC host performs successful T4T NDEF Application selection (Cmd.ISOSelectFile of NDEF App - D2760000850101h). This is done by NFC Forum compatible device automatically.

In the following example NTAG X DNA is configured as follows:

- GPIO1:
  - GPIO1Mode: 0x02 (output)
  - GPIO1Config: 0x00 (Initial state after power-off cycle: LOW)
  - GPIO1Notif: 0x01 (enable authentication notification)
- GPIO2:
  - GPIO2Mode: 0x02 (output)
  - GPIO2Config: 0x00 (Initial state after power-off cycle: LOW)
  - GPIO2Notif: 0x02 (enable NFC field notification)

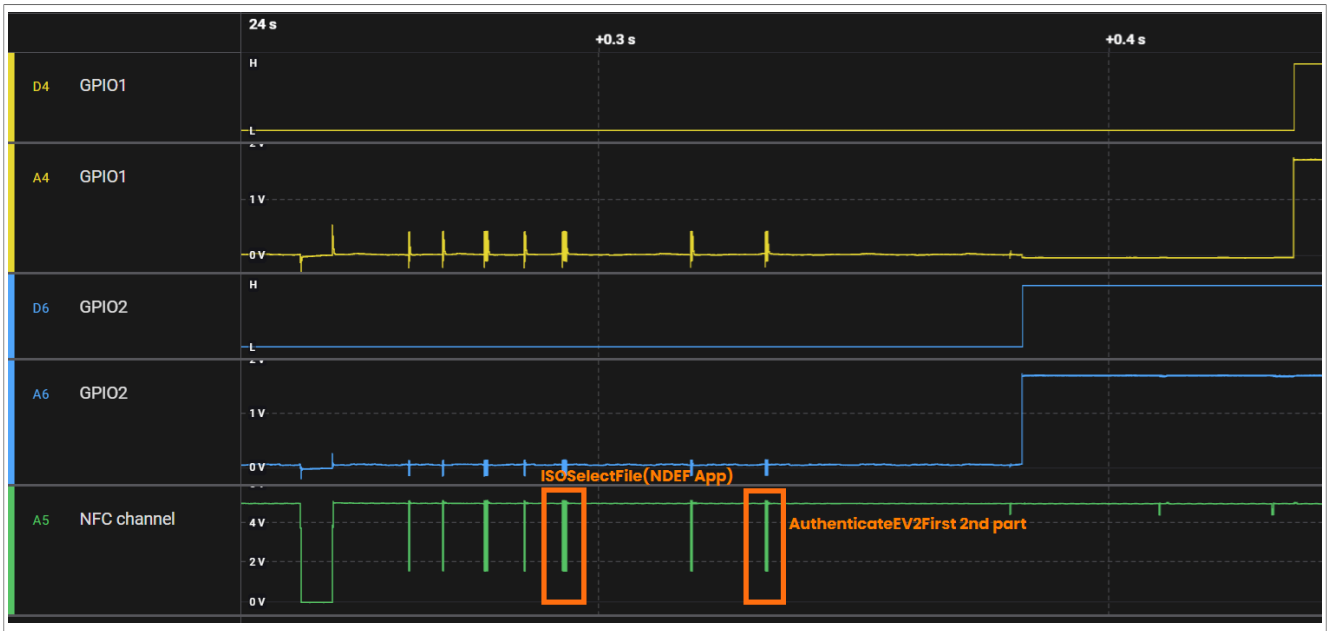

Figure 17. Cmd.ISOSelectFile and Cmd.AuthenticateEV2First notification

4.1.5 NFCPause example applications

An example of "NFCPause" communication can be seen in the following flow Figure 18.

The following steps are shown in the example flow:

1. RF field is switched ON by an NFC reader/writer device and NTAG X DNA boots
2. The NFC activation (as per ref.[1]) is done by an NFC reader/writer device
3. NTAG X DNA returns its UID and SAK
4. The NFC activation (as per ref.[2]) is done by an NFC reader/writer device
5. NTAG X DNA returns ATS and PPS. Additionally, NFC reader/writer device can perform the switch to HBR
6. NFC reader/writer device Selects NDEF Application (Additionally, NFC reader/writer device can select a CC file before and reads its contents)
7. NFC reader/writer device Selects NDEF File (within selected NDEF Application)
8. NFC reader/writer device writes to NDEF file
9. NFC reader/writer device triggers ManageGPIO command (Optionally GPIO can be toggled automatically by Cmd.ISOReadBinary, if configured)
10. NTAG X DNA sends WTX back to NFC reader/writer device
11. NTAG X DNA toggles its GPIO to notify MCU (through, for example, interrupt handler) that NFC reader/writer device is done accessing NTAG X DNA flash memory (NDEF file)
12. MCU reads NDEF file contents (note: no need to reselect NDEF Application by I²C controller / MCU)
13. NTAG X DNA returns data requested in step 12.
14. MCU triggers Cmd.ManageGPIO to toggle the GPIO back and provide additional custom NFCPauseResp data (up to 240 Bytes) to the NFC reader/writer device
15. NTAG X DNA stops/releases WTX automatically
16. NTAG X DNA responds with additional custom NFCPauseResp data to NFC reader/writer device
17. MCU acts upon received NDEF data contents

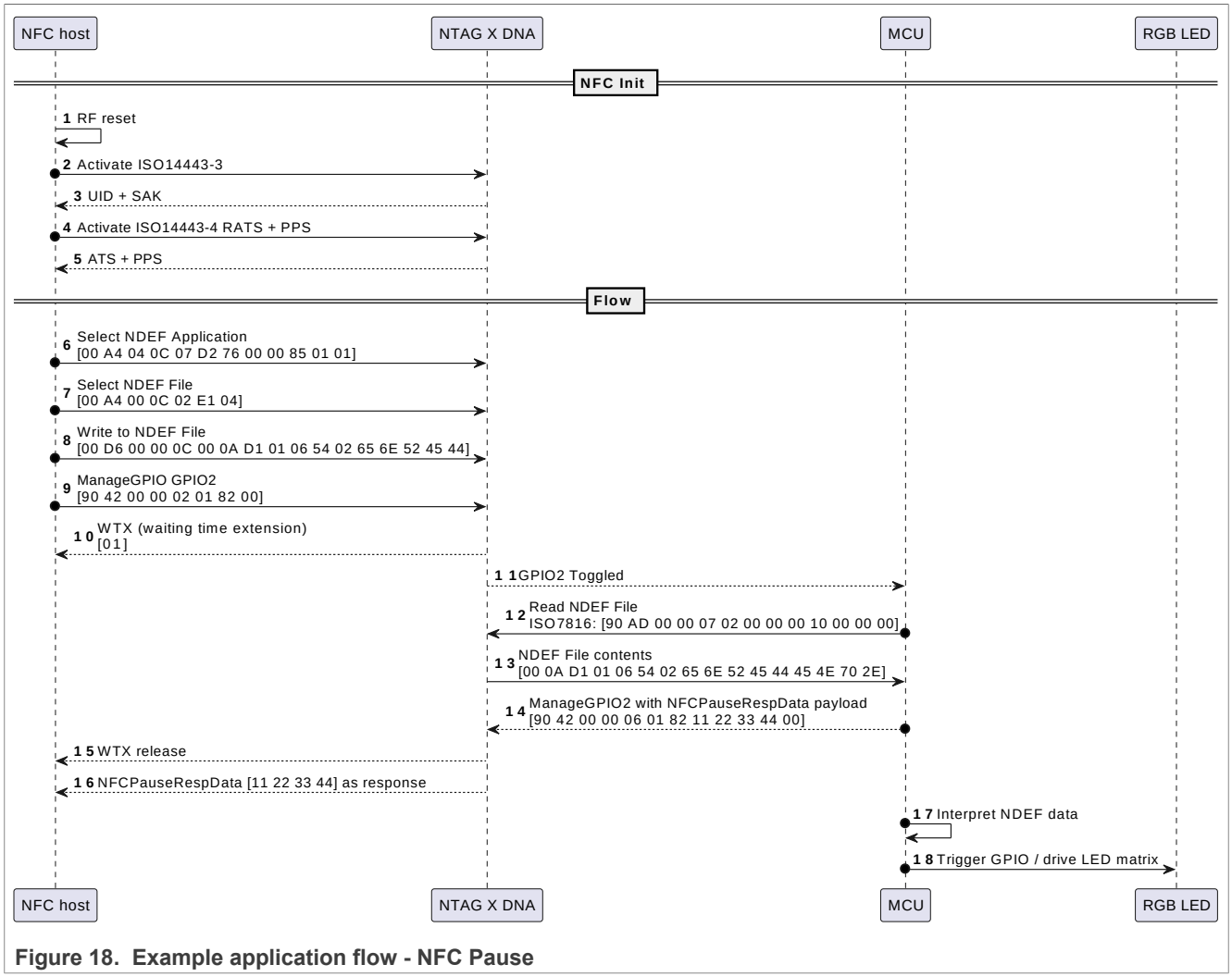

Figure 18. Example application flow - NFC Pause

Note: *Additionally Mutual authentication (SIGMA-I or AES) may be included before step 6 freely, so only the authentic NFC reader/writer is allowed to continue the flow.*

4.1.6 Read integrity protected, authentic, secure sensor data

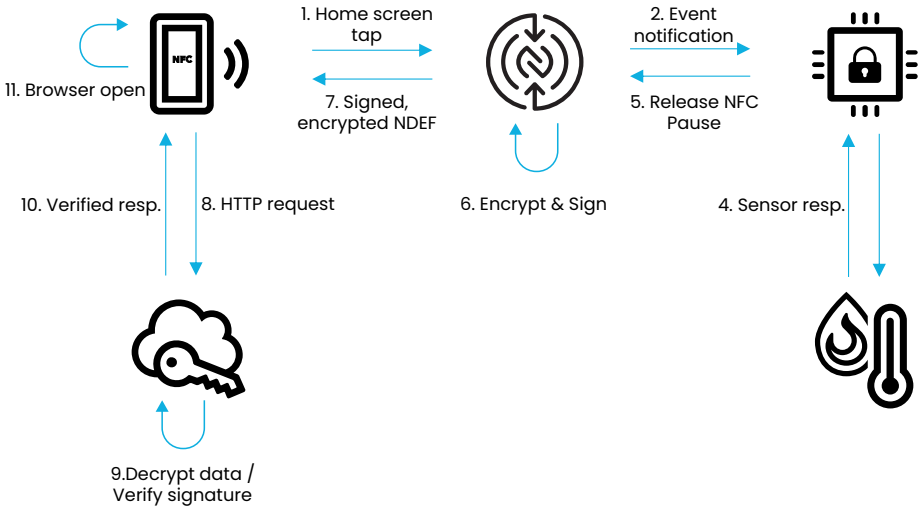

Figure 19. Sensor data read out - communication flow

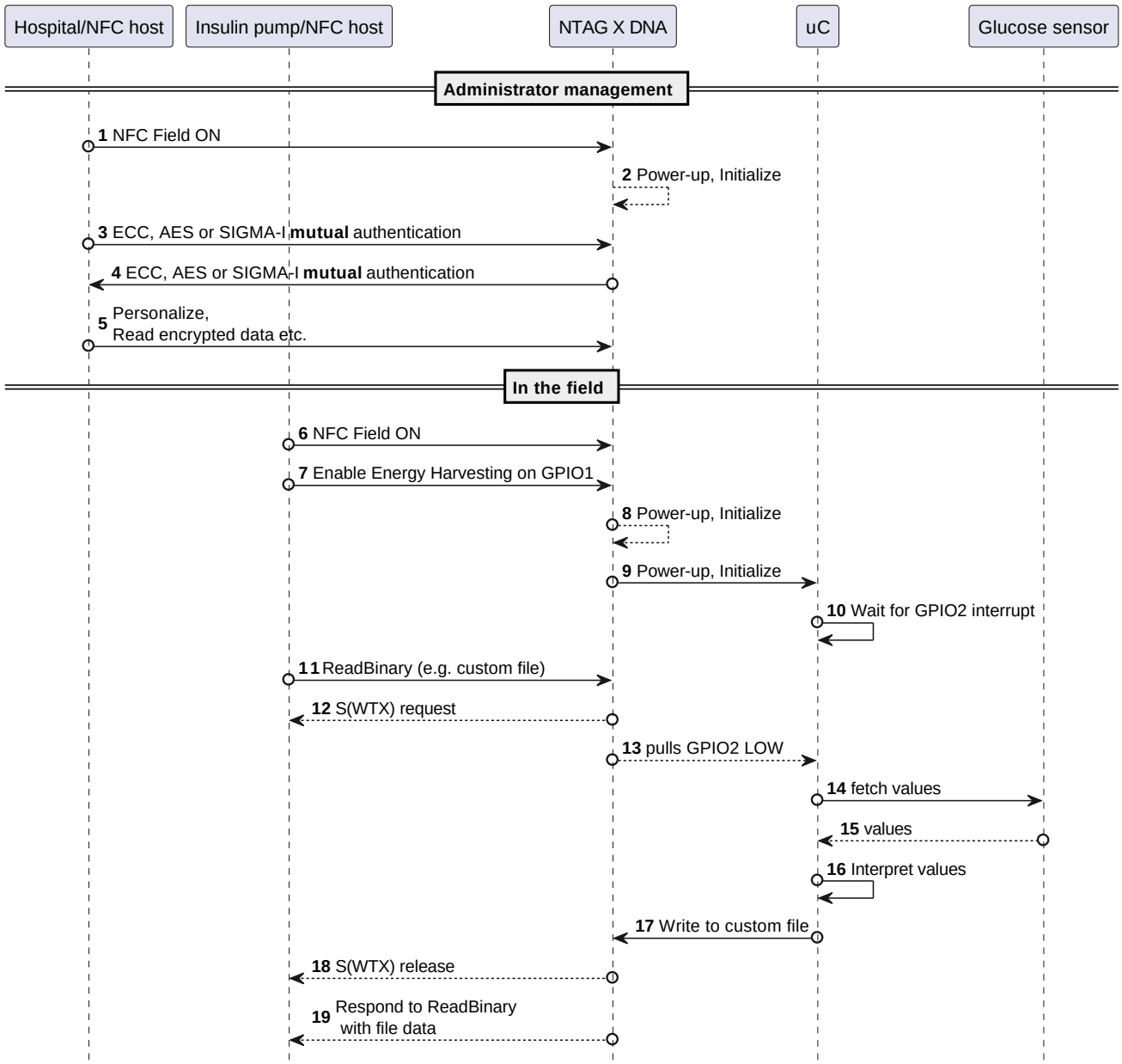

Figure 20. Body glucose meter and insulin doser appliance

4.2 Appendix - State diagrams

4.2.1 NTAG X DNA Dual Interface state diagram

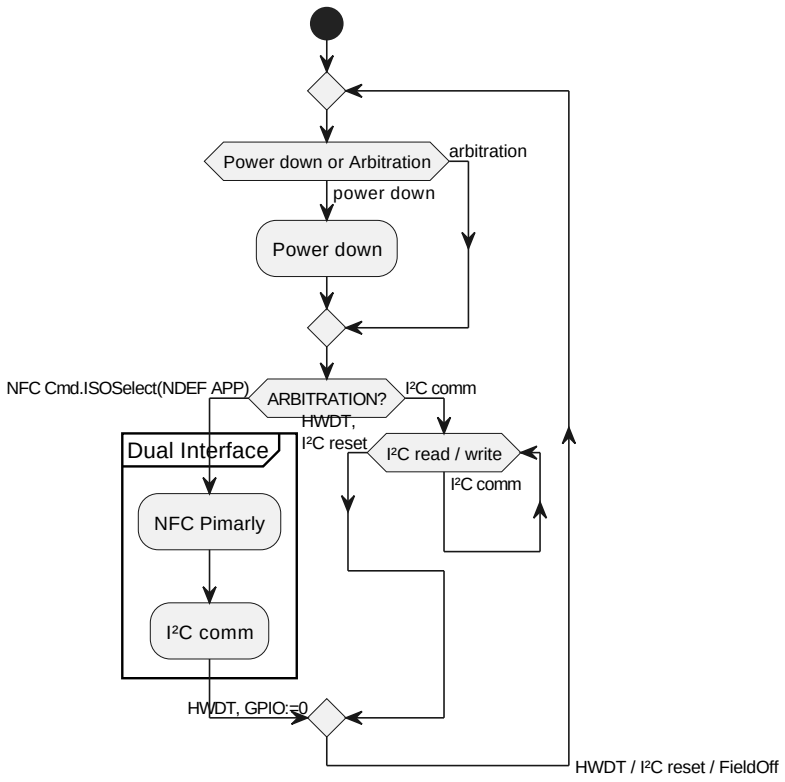

Figure 21. NTAG X DNA Dual Interface state diagram

4.2.2 Example of NFC reader application state diagram

The following figure shows an example of how the NFC reader SW can be designed for Section 4.1.5. Note that "WTX" ("NFC Pause") is standardized in ISO 14443-4 ref.[2].

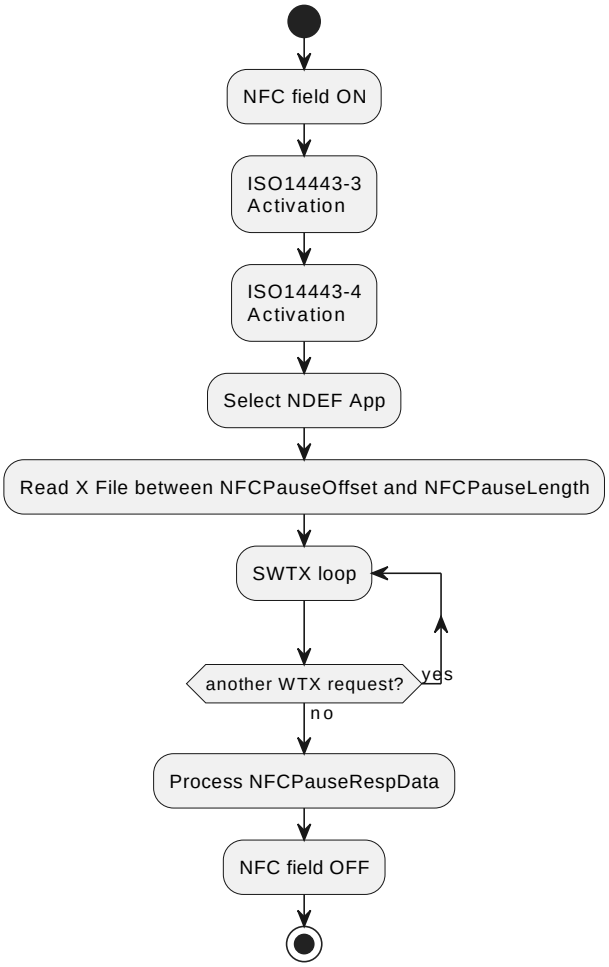

Figure 22. Example of NFC reader application state diagram

4.2.3 Example of MCU state diagram

The following figure shows an example of how the MCU SW can be designed for Section 4.1.5. The The idea is to use interrupt on one of the GPIOs of the MCU.

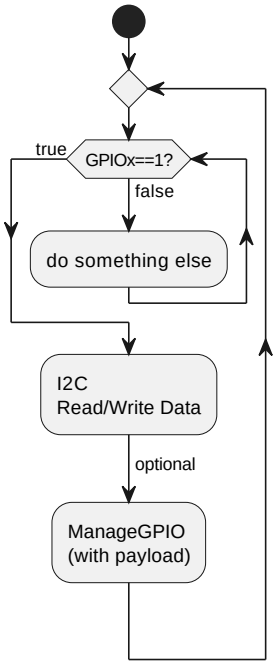

Figure 23. Example of MCU state diagram

5 NX Middleware examples

The following examples represent Dual Interface use cases:

Note: *There may be others which are a better fit for the final application. See https://github.com/NXP/nxmw.*

- dual_interfaces Example
- gpio Example
- gpio_notif Example
- hkdf Example
- nx_cli_tool
- nx_deep_pwr_down
- nx_release_req_cmd
- nx_tool_setconfig
- sdm Example
- setConfig Example
- symmetric symmetric Example
- tls_client Example
- usb_c Example
- nx_access_manager Example
- vcom Example
- host co-processor Example
- Qi authenticator Example

6 Abbreviations

Table 3. Abbreviations

Acronym	Description
EH	Energy harvesting (NFC Field)
AID	Application IDentifier
APDU	Application Protocol Data Unit
DF-Name	ISO7816 Dedicated filename
C-APDU	Command APDU
CMAC	MAC according to NIST Special Publication 800-38B
CRC	Cyclic Redundancy Check
ECC	Eliptic Curve Cryptography
IC	Integrated Circuit
KDF	Key derivation function
LSB	Lowest Significant Byte
LSb	Lowest Significant bit
MAC	Message Authentication Code
NDEF	NFC Data Exchange Format
NDPP	NFC Digital Product Passport
NFC	Near Field Communication
NVM	Non-volatile memory
PCD	Proximity Coupling Device
PICC	Proximity-Integrated Circuit Card
PRF	Pseudo Random Function
R-APDU	Response APDU (received from PICC)
SSM	Standard Secure Messaging
SUN	Secure Unique NFC Messaging
UID	Unique Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

7 References

[1] Specification - ISO/IEC 14443-3:2018 - Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anti-collision

[2] Specification - ISO/IEC 14443-4:2018 - Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol

[3] Data sheet - NTAG X DNA - Secure NFC Forum T4T compliant IC with PKI (Public Interface Structure) (link)

[4] Application note - AN14137 - NTAG X DNA - Features and hints (link)

[5] Application note - AN14362 - NTAG X DNA - Energy harvesting (link)

8 Revision history

Table 4. Revision history

Document ID	Release date	Description
AN14513 v.1.0	27 May 2025	• Initial version

Legal information

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.

Disclaimers

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

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

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

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

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

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

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

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

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

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

Suitability for use in non-automotive qualified products — Unless this document 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.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

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

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

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.

Trademarks

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

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

MIFARE — is a trademark of NXP B.V.

Tables

Figures

Contents