OPTIGA™ Authenticate NBT

Extended datasheet

The OPTIGA™ Authenticate NBT is a ready-to-use dual-interface bridge tag with a contactless passive NFC interface and an I2C target interface to the MCU. It supports high performance NFC-to-I2C communication, comes with an NFC Forum Type 4 Tag compliant 8 KB file system with file-based password protection, one-way authentication using ECDSA asymmetric cryptography and symmetric AES-128-CMAC based cryptography

Features

- NFC-to-I2C bridge device for synchronous high-speed communication from an NFC reader to an I2C-connected host MCU
- NFC Forum Type 4 Tag with 4 KB NDEF message plus 4 KB proprietary files storage for NFC tag application and asynchronous data transfer between the host MCU and NFC reader
  - Flexible file access policy
- ECDSA-based one-way authentication using NIST P-256 and public key infrastructure for offline authentication
- AES-128-CMAC-based cryptographic one-time token for online authentication

Potential applications

NFC bridge tag applications	NFC tag applications
Bluetooth or Wi-Fi pairing	Accessory authentication
Headless configuration	Brand protection with offline verification
Product activation	Brand protection with online verification
Key-less entry	

Product validation

Qualified for applications according to the test conditions in the relevant tests of JEDEC JESD22 and J-STD-020.

Description

The OPTIGA™ Authenticate NBT can be powered by an external NFC field, where the NFC reader connects to the NFC tag application via the contactless interface (L_A, L_B) and an externally connected antenna. In addition to the NFC interface, the device can also be supplied from an external power supply (V_{CC}, GND), including an integrated I2C interface and one IRQ for communication with external host systems.

The OPTIGA™ Authenticate NBT embedded software includes an NFC tag application that complies with the NFC Forum Tag Application Specification for Type 4 Tag (Listener) for NFC-A, and an NFC-to-I2C bridge functionality.

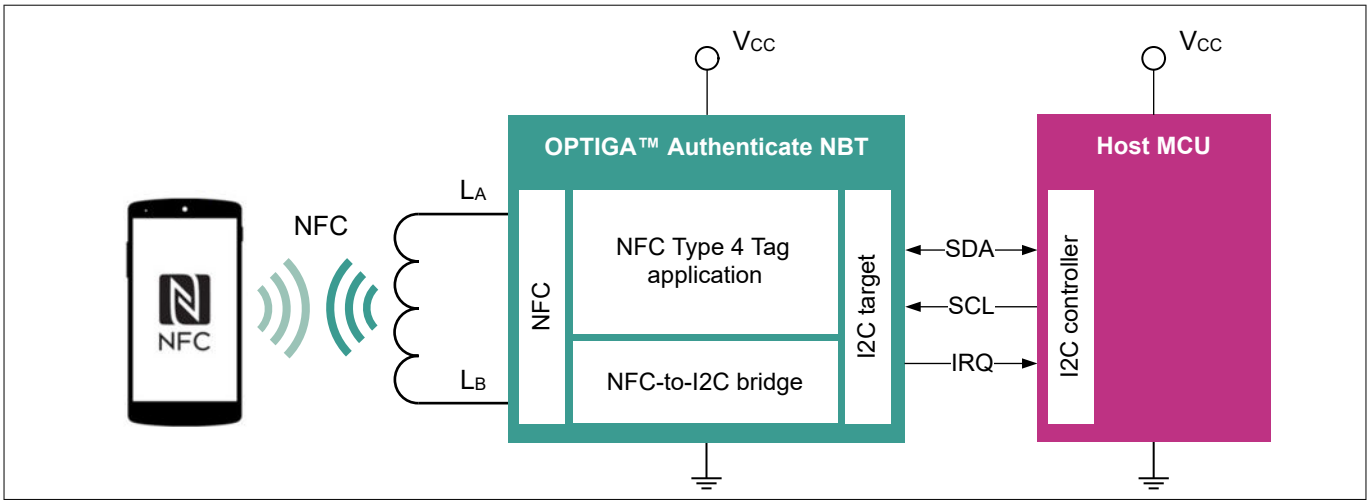


Figure 1 Block diagram - OPTIGA™ Authenticate NBT

Ordering information

Product name	Ordering code	Marking	Package
OPTIGA™ Authenticate NBT	NBT2000A8K0T4	NBT2	PG-USON-8-8

About this document

Scope and purpose

This document describes the features, functionality and operational characteristics of the OPTIGA™ Authenticate NBT.

Intended audience

This document is primarily intended for system and application developers.

Table of contents

Table of contents

Table of contents

Table of contents

List of tables

List of tables

List of figures

1 Introduction

The OPTIGA™ Authenticate NBT is a dynamic and secure turn-key solution for embedded NFC tag applications with varying levels of security and communication.

The OPTIGA™ Authenticate NBT communicates with the host MCU via I2C and with NFC-enabled mobile phones and NFC readers via NFC. The two interfaces can be operated in a mode known as "bridge mode". An IRQ can be used to signal the presence of an NFC field to the host system.

To meet the needs of demanding applications, the OPTIGA™ Authenticate NBT includes an NFC Forum Type 4 Tag compliant file system: Capability Container (EF.CC) file, NDEF file (4 KB), and four additional proprietary files (1 KB each). Using 32 bit passwords, a flexible password-based file access policy allows to restrict access on a per-file and per-interface basis.

The OPTIGA™ Authenticate NBT is equipped with state-of-the-art elliptic curve (EC) and AES-based features for cryptographic security needed in brand protection applications.

A pre-installed, chip-individual Infineon X.509 certificate provides the OEM with an EC-based originality check of the chip. The originality check is actively authenticated using a reader-supplied nonce, a protected chip-individual private key.

The OPTIGA™ Authenticate NBT can be easily personalized to customer public key infrastructures (PKIs) using customer-issued certificates and EC keys. For brand protection applications, even in offline scenarios, cutting-edge ECDSA with NIST P-256 one-way authentication offers protection.

Additionally, the OPTIGA™ Authenticate NBT enables dynamic computation of a NDEF-embedded cryptographic one-time token for server-side symmetric-key based authentication. Each time the Type 4 Tag application on the device is selected, the token is freshly computed using a secured AES-128-CMAC key. When the NDEF message is read, this token gets embedded into the response. The one-time token can be transferred to a server-side system as part of a URL to authenticate a tag without the use of specific mobile applications.

***Note**: For a collection of all available support material for the OPTIGA™ Authenticate NBT, refer to its product page [14].*

1.1 Target applications

The OPTIGA™ Authenticate NBT is suitable for a wide range of applications, including the following:

- Offline brand protection: I2C or NFC-based authentication of products or accessories when internet connectivity is not available
- Online brand protection: NFC-based authentication of products or accessories without requiring a dedicated application on the mobile phone
- Headless configuration/readout of consumer IoT devices or industrial equipment
- Wi-Fi/Bluetooth pairing
- Product activation
- Accessory authentication

1.2 Interface description

The OPTIGA™ Authenticate NBT provides an ISO/IEC 14443-4 [4] compliant interface that allows it to connect to any NFC-enabled mobile phone, tablets and other portable and stationary NFC reader devices. On top of the contactless interface, an NFC Forum compliant Type 4 Tag application is implemented.

The OPTIGA™ Authenticate NBT can be powered by the NFC field for NFC-only applications. Alternatively, the device can be supplied from the host system's V_{CC}.

Furthermore, the OPTIGA™ Authenticate NBT includes an I2C interface that uses the Global Platform standardized GP T=1' over I2C protocol for easy integration with a wide range of host systems. Polling and interrupt-based communication are both supported by the device.

Using both NFC and I2C interfaces in bridge mode, OPTIGA™ Authenticate NBT enables NFC-to-I2C (and reverse) communication. The bridge mode supports two pass-through modes:

- Asynchronous pass-through via the file system, where the chip can be power-cycled in-between
- Synchronous pass-through, where the APDUs are forwarded between NFC and I2C immediately

The OPTIGA™ Authenticate NBT can detect the presence of an NFC field and signal it to the host system via its IRQ, triggering host-side actions.

Depending on the configuration, the IRQ can be used for one or more of the following tasks:

- Signaling states of the NFC state machine (RF-IRQ)
- GP T=1' over I2C interruption to the host system (I2C-IRQ)
- Pass-through data availability interruption to the host system (PT-IRQ)

1.3 Conventions used

Throughout this document:

- Communication to and from the OPTIGA™ Authenticate NBT is accomplished logically through the use of Application Data Protocol Units (APDUs). Command-APDUs (C-APDUs) are APDUs transferred from the communication initiator (host system using I2C or NFC reader using NFC), while Response-APDUs (R-APDUs) are the responses of the device
- "Pass-through" will represent only "synchronous pass-through"
- All lengths are represented in bytes, unless otherwise specified

2 Solution overview

This section describes the intended use cases of the product, security guidance and compliance.

2.1 Use cases

This section describes the four primary product use cases. The OPTIGA™ Authenticate NBT enables a variety of applications. A customer can configure and personalize the device for one or more of these use cases, depending on the application needs.

2.1.1 Use case: Asynchronous data transfer (ADT)

Asynchronous data transfer (ADT) allows the transfer of arbitrary application-specific data from an NFC reader to the host system or from the host system to an NFC reader.

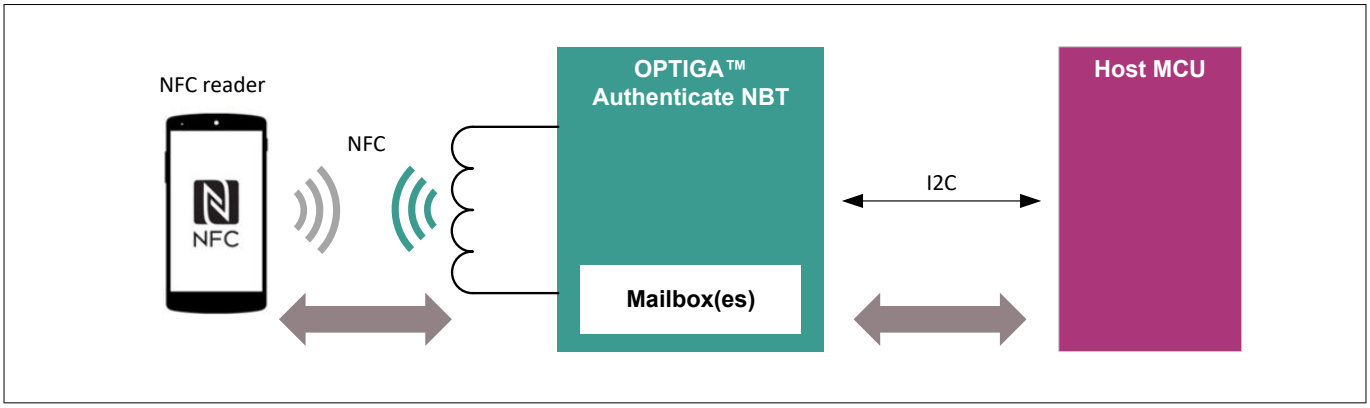


Figure 2 Asynchronous data transfer mode

The OPTIGA™ Authenticate NBT implements data exchange in asynchronous data transfer mode via "mailboxes". These mailbox files are part of the NFC Type 4 Tag application and can be accessed through the I2C and NFC interfaces. Depending on the needs of the application, the NFC reader or host system serves as the initiator. They can write data to or read data from the NDEF message or one (or more) of the proprietary files.

The data written to these files is stored in the non-volatile memory of the OPTIGA™ Authenticate NBT and persists across power cycles. Later, the "other party" obtains data from the mailboxes. As a result, using the file system in the Type 4 Tag application results in asynchronous data transfer. The device governs file access rights (read or write) and restricts file read or write access from the host-side, respectively the NFC reader-side, via its file access policy configuration (in EF.FAP). Interface multiplexing mediates parallel access from both interfaces to avoid race conditions.

The asynchronous data transfer mode can be used in the following scenarios.

Scenario 1: Device manufacturing

During device manufacturing, the OEM stores device initialization data on the OPTIGA™ Authenticate NBT using an NFC reader. These initialization data can be obtained from the device when the host system powers up in the field.

Scenario 2: Configuring an unpowered device

An end customer can send onboarding information to a light bulb before powering it. After the light bulb is screwed into the mains, the light bulb's host system when powered on, obtains the onboarding information to join the costumer's local network.

Scenario 3: Reporting diagnostic data

The host system periodically writes usage and diagnostic data to a file. In the event that the device host system fails, an NFC reader can power the OPTIGA™ Authenticate NBT and read the most recent data.

Scenario 4: Obtain Wi-Fi/Bluetooth pairing data

The host system sends a Connection Handover (CH) NDEF message to the OPTIGA™ Authenticate NBT with the most recent Wi-Fi/Bluetooth pairing information. If the host system needs to update this information, the NDEF message is replaced again (for example, if the Bluetooth speaker is reset; or the Wi-Fi router password

changed). By simply powering on the device and reading the NDEF message containing the CH record, the phone can read the most recent configuration at any time.

2.1.2 Use case: Synchronous pass-through (PT)

In synchronous pass-through mode (PT), the OPTIGA™ Authenticate NBT bridges data received from the NFC interface (from an Initiator) to the I2C interface connected to the host system (Responder). The device notifies the host system about the availability of data via its IRQ after receiving the NFC command data. The host system (as I2C controller) actively obtains the Initiators command, executes the operation, prepares a response, and sends the response back to the device returns the response data to the NFC reader without evaluating the content.

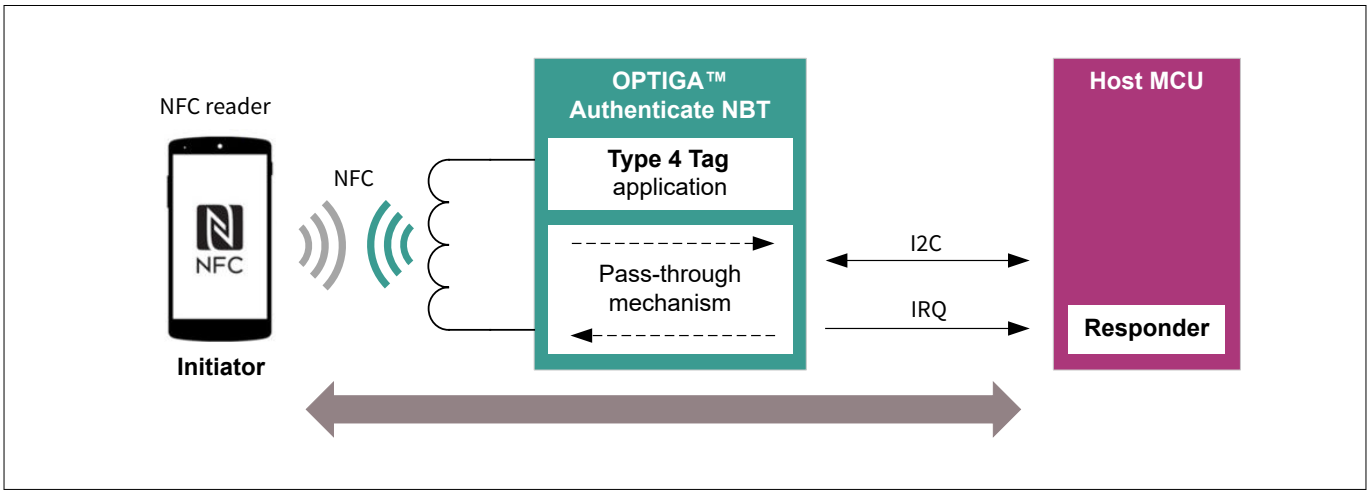


Figure 3 Synchronous pass-through mode

By selecting an unregistered application[1)] on the OPTIGA™ Authenticate NBT, the NFC reader can enable pass-through mode. This use case simplifies the implementation of "virtual" applications on the host system.

The synchronous pass-through is applicable in the following scenarios:

Scenario 1: Download firmware update to the host system

To update the firmware of a host system, the NFC reader transfers the firmware data in a series of command frames to the host system.

Scenario 2: Configure or control a host system ("headless")

The NFC device sends control or configuration data to the host system, which the host system immediately uses, for example, to establish a Wi-Fi connection from the host system to the local Wi-Fi network. The host system may return the most recent status information in its response.

2.1.3 Use case: Brand protection (online) using AES-128-CMAC-based cryptographic one-time token (COTT)

If configured, the OPTIGA™ Authenticate NBT generates a new cryptographic one-time token (COTT) value for each NDEF message access. The COTT is encoded in Base64url format and contains a 1-byte header, a 7-byte UID for the tag, an 8-byte random number, and an AES-128-CMAC signature computed over the header, UID, and random number. The device will insert this COTT value in the NDEF message at a brand owner-defined location, for example, in the parameters of a URL contained in an URI NDEF record.

An NFC Forum compliant mobile phone will automatically recognize and prompt the user to access the URL. Upon access, the COTT value is sent to the server as part of the URL. To determine whether the URL access was the result of a recent tag readout, the server can use cryptographic and heuristic measures.

1 The OPTIGA™ Authenticate NBT supports two registered applications: the NFC Type 4 Tag application and the CONFIGURATOR application. Other applications than these two are considered "unregistered." For more information, refer to Chapter 4.

The main advantage of this system is that no mobile phone application is required since all major phone operating systems support reading and opening URLs from NFC tags. Validation logic is implemented only on server side.

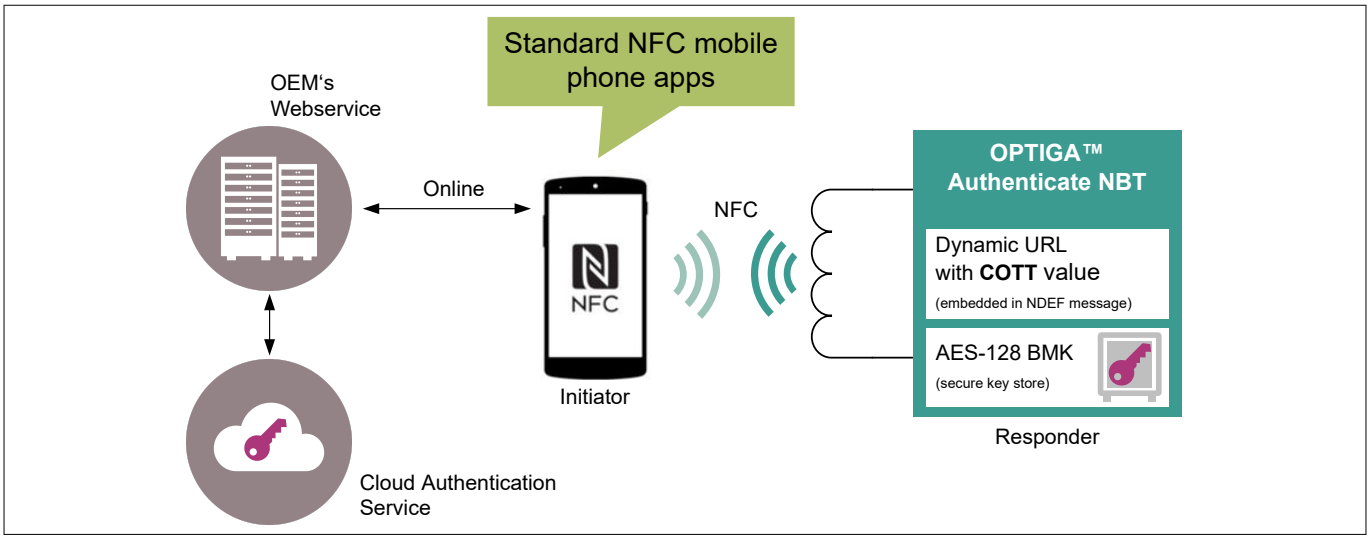


Figure 4 Online authentication using AES-128-CMAC-based COTT

Scenario 1: Validate authenticity of a product without using a mobile application

The customer taps the OPTIGA™ Authenticate NBT, which directs them to the vendor's website. The web server uses the COTT value in the URL to validate the product, and to display the validation result to the user as a web page.

Scenario 2: Validate/track smart poster usage

The customer taps a smart poster (as defined by the NFC Forum) and is directed to a web page advertised by the poster. The website uses the COTT value in the URL to validate and track access to a specific poster and user-tag interaction.

2.1.4 Use case: Brand protection (offline) using ECDSA one-way authentication

In this use case, the NFC reader/phone obtains a public-key certificate from the OPTIGA™ Authenticate NBT using active challenge-response. The use of public-key certificates and a vendor public key infrastructure allows the mobile application to validate without internet access or a web server. Furthermore, the certificate can include any preferred information about the device that needs to be authenticated, such as product details or manufacturing/expiry dates, etc.

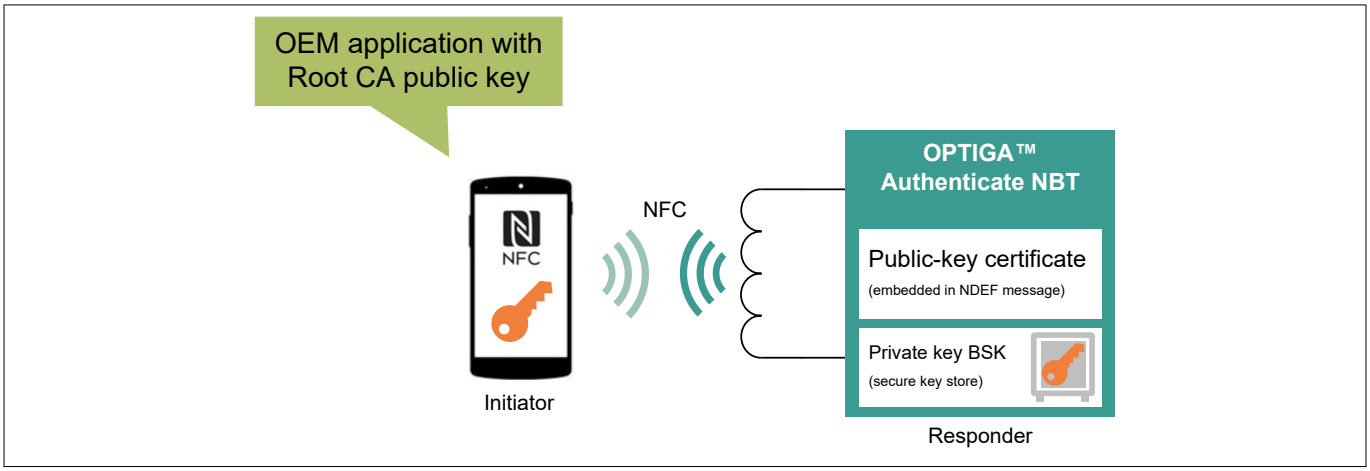


Figure 5 Offline authentication using ECDSA one-way authentication

Scenario 1: Main system validates disposable or accessory

The OPTIGA™ Authenticate NBT can be used to authenticate a disposable or accessory that connects to a main system. The main system uses one of the following communication channels to perform the challenge-response authentication:

- NFC reader, which is used to communicate to accessory's device
- Bluetooth, which is used to communicate with the host (MCU) system of the accessory. The host MCU delegates authentication to the device using I2C

2.2 Security guidance

This section provides information on how to configure and how to use the OPTIGA™ Authenticate NBT in an effective way in a customer solution.

Personalization environment

The personalization entity is responsible for:

- The generation and protection of to-be-personalized key and certificate data
- The initialization and protection of the personalization data generation infrastructure

Product delivery state and product personalization

- In the product's delivery condition, Infineon-generated keys are present
  - To validate the product's origin, the personalization entity should use the initial Infineon-generated certificate
  - When offline brand protection is used, then
    - It is recommended to personalize a customer-generated Brand Protection Signing Key (BSK) to replace the initial Infineon-generated BSK
    - The personalization entity must personalize a customer-specific certificate
  - When using COTT for online brand protection, the personalization entity must personalize a customer-specific Brand Protection MAC'ing Key (BMK). The initial BMK shall not be used for production
- The personalization entity must configure a file access policy based on the needs of the individual use case. If required by the respective use case needs, the personalization entity must protect the file access policy file (EF.FAP) by configuring respective access conditions
  - For example, an NDEF file with the write access condition "ALWAYS" can be modified in the field by any entity, erasing the certificate required for offline brand protection
- Before the product leaves the secured personalization environment, the personalization entity must change the product's life cycle state to OPERATIONAL, using the FINALIZE PERSONALIZATION command (PERSONALIZE DATA command with DGI $BF6300_H$)

2.3 Functional compliance

The OPTIGA™ Authenticate NBT, including its integrated Type 4 Tag application, complies with the following:

- NFC Forum Type 4 Tag Technical Specification [7]
- NFC Forum Analog Technical Specification [8]
- NFC Forum Digital Protocol Technical Specification [9]
- NFC Forum Activity Technical Specification [10]
- NFC Forum NDEF Technical Specification [11]

3 Delivery forms

This chapter provides information about available delivery forms and how the product's interfaces are assigned to the package pins. For further information on compliance of the packages with European Parliament Directives, see Chapter 3.2.

For details and recommendations on the assembly of packages on PCBs, please refer to [23].

3.1 SMD package

The following package is available:

- PG-USON-8-8

The figures in the sections below show the following aspects of the package:

- **Package outline:** It shows the package dimensions of the device in the individual packages
- **Package footprint:** It shows footprint recommendations
- Tape and reel packing
- **Sample marking pattern:** It describes the productive sample marking pattern on the package
- **Package layout:** It shows a simple layout with the pin numbers described in the pin-to-signal reference section

***Notes**:*

1. *The drawings are for information only and not drawn to scale. More detailed information about package characteristics and assembly instructions is available on request.*

2. *Unless specified otherwise, all figure dimensions are given in mm.*

3.1.1 PG-USON-8-8

Package outline

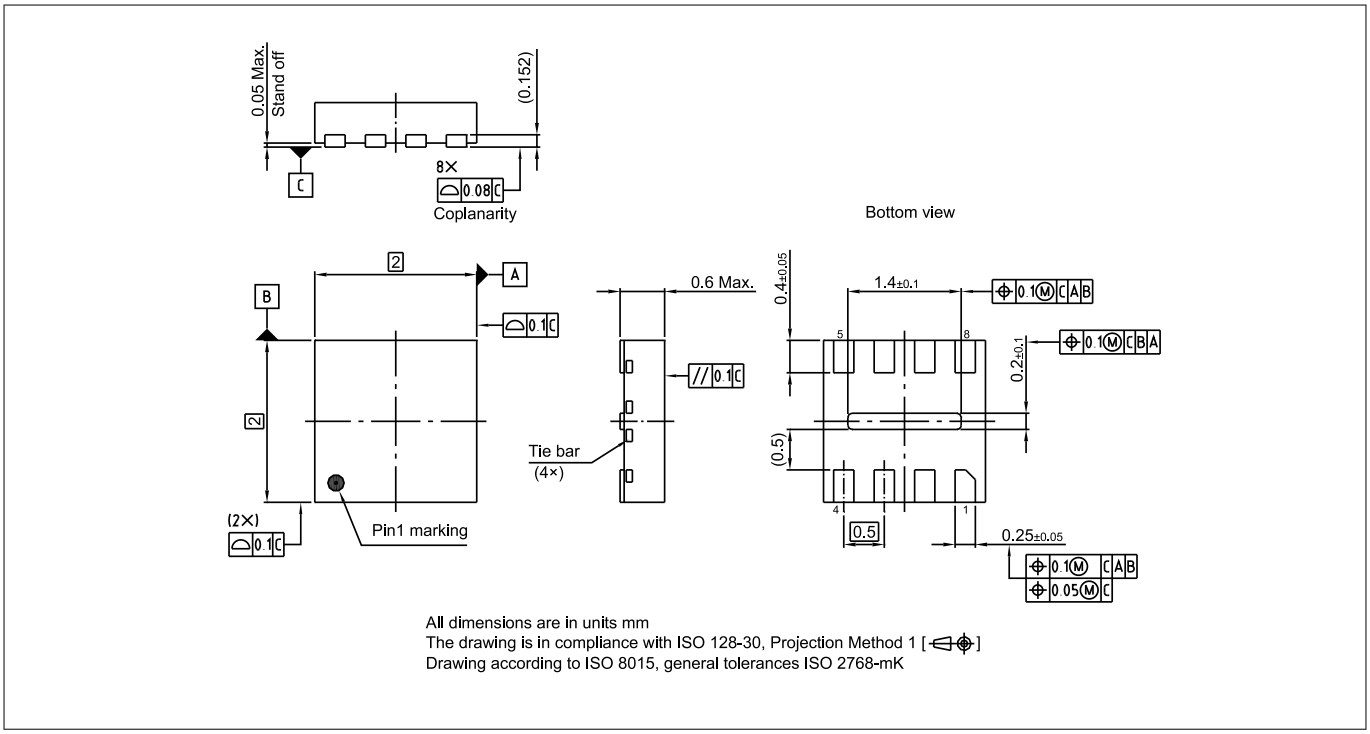


Figure 6 PG-USON-8-8 package outline

3 Delivery forms

Package footprint

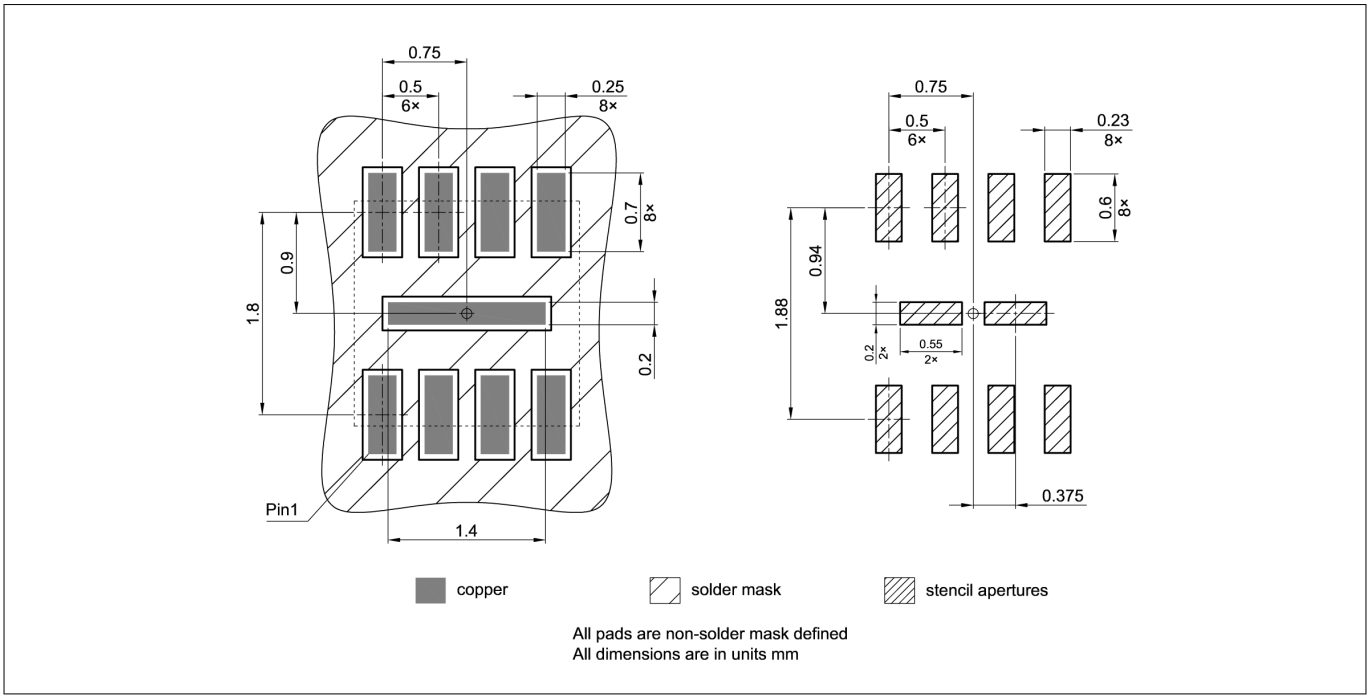


Figure 7 PG-USON-8-8 package footprint

Tape & reel packing

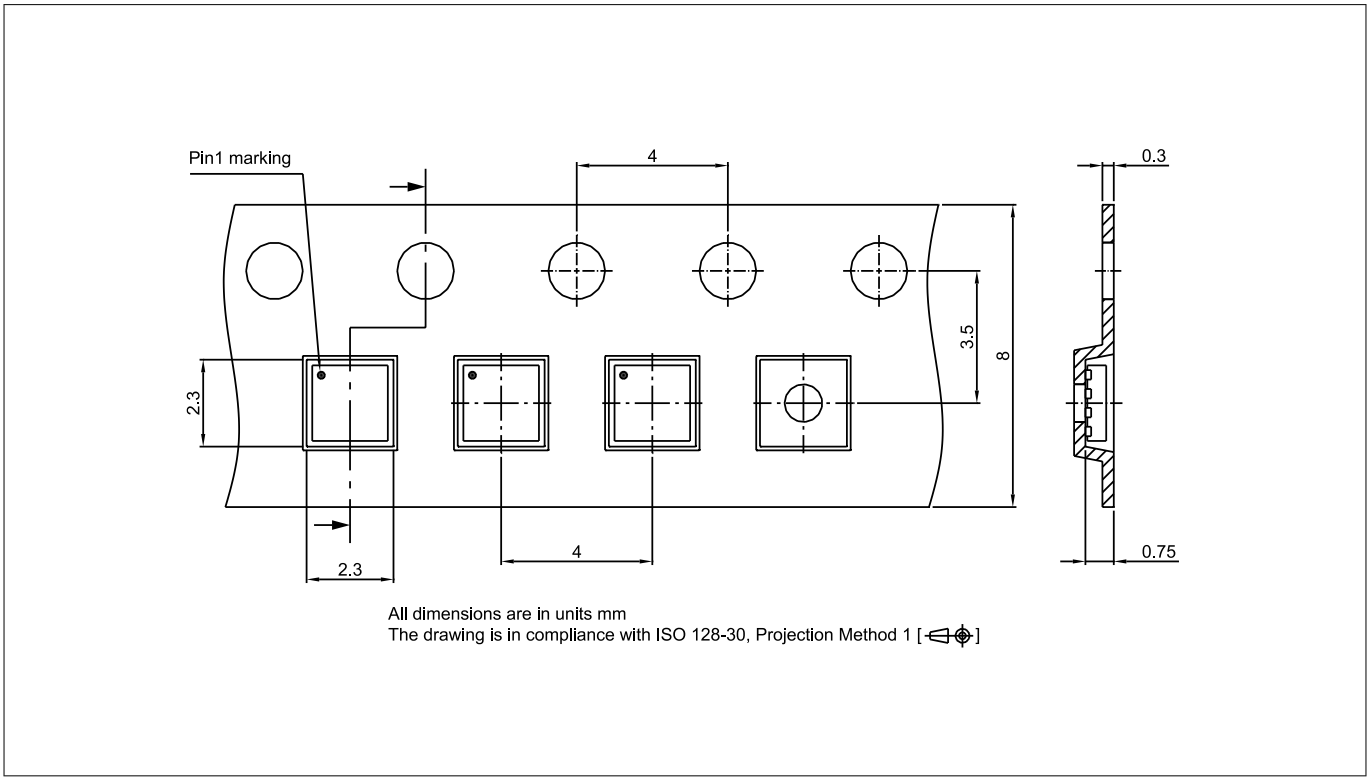


Figure 8 PG-USON-8-8 tape & reel packing

Production sample marking pattern

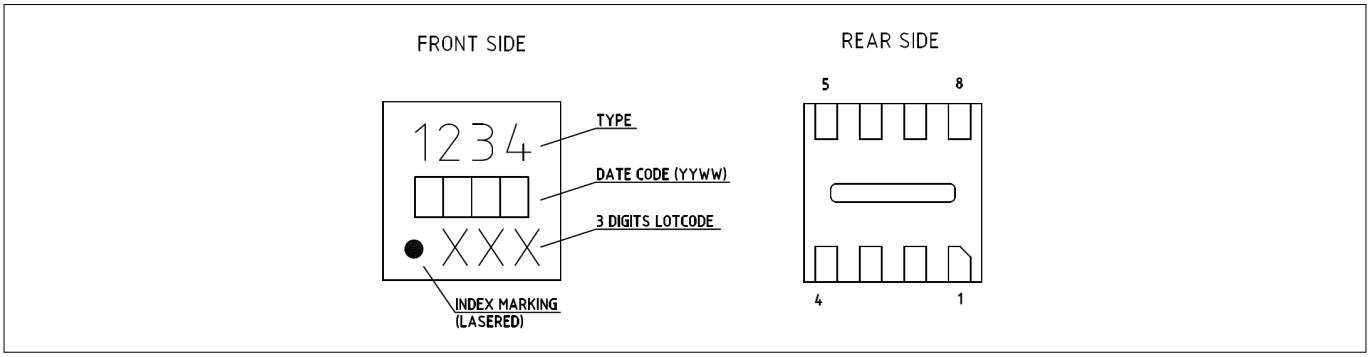


Figure 9 PG-USON-8-8 sample marking pattern

The dot indicates pin 1 for the chip. The following table describes the sample marking pattern:

Table 1 Marking table for PG-USON-8-8 packages

Indicator	Description
1234[1)]	**Type code** • OPTIGA™ Authenticate NBT: NBT2
□□□□	**Production date:** “<YYWW>”, two bytes, BCD coded • <YY>: Production year • <WW>: Production week It is inserted during fabrication
XXX	**Lot code** It is defined and inserted during fabrication, issued by the packaging site

1) "1234" in Figure 9 represents a wildcard.

Package layout

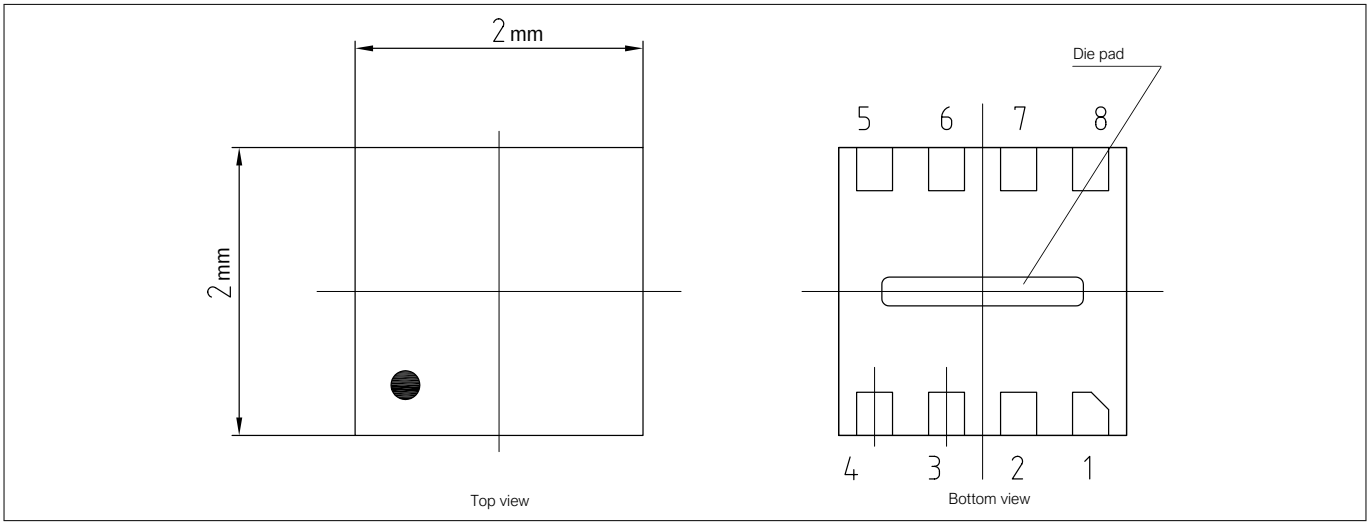


Figure 10 PG-USON-8-8 package layout

***Note**: It is recommended to connect the exposed die pad to the common ground reference (GND) for heat distribution.*

Pin-to-signal reference

Table 2 Pin-to-signal reference for PG-USON-8-8

Pin	Symbol	Pin configuration	Signal function/remarks
1	GND	GND	Power supply: Common ground reference
2	L_A	Contactless	Antenna connection: Contactless usage
3	SDA	I/O	I2C interface: Data line
4	NC	-	No internal connection
5	IRQ	Output	Interrupt: The respective output function can be configured
6	SCL	Input	I2C interface: Clock line
7	L_B	Contactless	Antenna connection: Contactless usage
8	V_{CC}	PWR	Power supply: Power and pad supply (V_{CC})

3.2 RoHS compliance

On January 27, 2003 the European Parliament and the council adopted the directives:

- 2002/95/EC on the Restriction of the use of certain Hazardous Substances in electrical and electronic equipment ("RoHS")
- 2002/96/EC on Waste Electrical and Electronic Equipment ("WEEE")

Some of these restricted (lead) or recycling-relevant (brominated flame retardants) substances are currently found in the terminations (e.g. lead finish, bumps, balls) and substrate materials or mold compounds.

The European Union has finalized the Directives. It is the member states' task to convert these Directives into national laws. Most national laws are available, some member states have extended timelines for implementation. The laws arising from these Directives have come into force in 2006 or 2007.

The electro and electronic industry has to eliminate lead and other hazardous materials from their products. In addition, discussions are on-going with regard to the separate recycling of certain materials, for example plastic containing brominated flame retardants.

Infineon is fully committed to giving its customers maximum support in their efforts to convert to lead-free and halogen-free[2)] products. For this reason, Infineon's "Green Products" are ROHS-compliant.

Since all hazardous substances have been removed, Infineon calls its lead-free and halogen-free semiconductor packages "green." Details on Infineon's definition and upper limits for the restricted materials can be found here.

The assembly process of our high-technology semiconductor chips is an integral part of our quality strategy. Accordingly, we will accurately evaluate and test alternative materials in order to replace lead and halogen so that we end up with the same or higher quality standards for our products.

The use of lead-free solders for board assembly results in higher process temperatures and increased requirements for the heat resistivity of semiconductor packages. This issue is addressed by Infineon by a new classification of the Moisture Sensitivity Level (MSL). In a first step the existing products have been classified according to the new requirements.

2 Any material used by Infineon is PBB and PBDE-free. Plastic containing brominated flame retardants, as mentioned in the WEEE directive, will be replaced if technically/economically beneficial.

3 Delivery forms

4 System architecture

This section describes the product architecture, including major internal components and interfaces to common customer system architectures.

4.1 Architecture diagram

The OPTIGA™ Authenticate NBT is delivered with the following selectable applications:

- CONFIGURATOR application: Used to modify the device's hardware-related settings or configuration such as interface settings, IRQ behavior, life cycle state, and additional settings
- Type 4 Tag application: Contains application data files that are the EF.CC (Capability Container file), the NDEF file, proprietary "mailbox" files, and the EF.FAP (File Access Policy file)
- Pass-through application: This "virtual" application allows to transfer bigger amount of data between an NFC reader device and a host. The device manages the NFC protocol in terms of framing, timing, and waiting time extensions during the exchange of application commands

In a protected secure key store, the OPTIGA™ Authenticate NBT hosts the BSK (Brand Protection Signing Key) and the BMK (Brand Protection MAC'ing Key). Furthermore, the passwords used to manage the access to the application files are saved in a secured memory area.

Figure 11 depicts the main components of the product architecture of the OPTIGA™ Authenticate NBT.

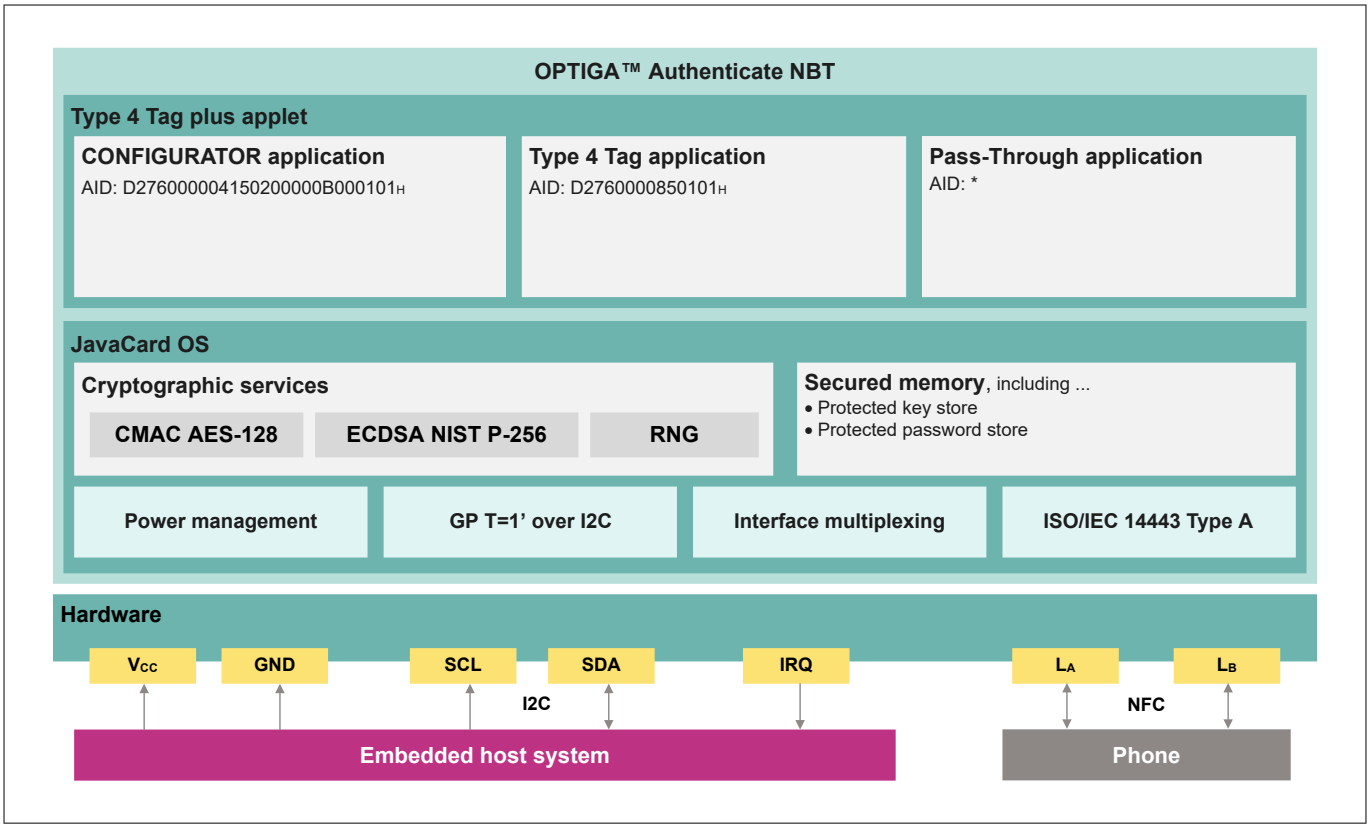


Figure 11 OPTIGA™ Authenticate NBT product architecture

The OPTIGA™ Authenticate NBT can be powered from the host system (V_{CC}, GND). The host system serves as an I2C controller, offering serial clock (SCL) and read/write serial data (SDA) to/from the device as an I2C target. The device uses the IRQ to signal RF field detection, I2C or pass-through events to the host system.

The OPTIGA™ Authenticate NBT can also be powered by NFC from a mobile phone (or any NFC Forum compliant reader device).

***Note**: While the OPTIGA™ Authenticate NBT is powered from the NFC reader field only, its IRQ and I2C interfaces are not functional given that they require V_{CC} supply to operate*

Interfaces are handled depending on the configured use case. The I2C and NFC interfaces can be operated simultaneously (refer to Chapter 5.2.3).

4.2 Component description

The OPTIGA™ Authenticate NBT hosts two applications, which are as follows:

- The **CONFIGURATOR application** (refer to Chapter 5.2.4.1) is used to adjust hardware-related configuration during the production of the host system, of which the device is an integral part
- The **Type 4 Tag application** provides the majority of personalization and operational features, including the file system and the authentication features. Refer to Chapter 5.3.2 for personalization, and refer to Chapter 5.2.5 for operational features

The **synchronous pass-through** application is a "virtual" application that can be activated by attempting to select an application with an AID, which is not used by the CONFIGURATOR or the Type 4 Tag application (refer to Chapter 5.2.6.2).

Table 3 Supported applications of the OPTIGA™ Authenticate NBT (real and virtual)

Application ID (AID)	Application	Functionality
D2 76 00 00 04 15 02 00 00 0B 00 01 01_H	CONFIGURATOR	Interface configurations
D2 76 00 00 85 01 01_H	Type 4 Tag	NFC Forum Type 4 Tag
Any other (length: 5 to 16 Bytes)	Pass-through	NFC to I2C Bridge Tag

5 Solution details

The following section provides comprehensive details about the OPTIGA™ Authenticate NBT solution, including information about the chip hardware's operational characteristics, embedded software, and implemented functionalities that enable different use cases. Additionally, the list of supported commands provides guidance on how to personalize and operate the device in the field.

5.1 Hardware details

The OPTIGA™ Authenticate NBT includes a contactless passive NFC interface and an I2C target interface for connecting to an I2C controller (host MCU). The interfaces are configurable and support following features.

I2C interface:

- Target interface, 7-bit address, initial value: 18_H
- Supported clock frequencies:
  - Standard mode (SM) 100 kHz
  - Fast mode (FM) 400 kHz
  - Fast mode plus (FM+) 1000 kHz
- Protocol: GlobalPlatform T=1' I2C [12] and [13]

NFC interface:

- 7-byte UID (fixed, programmed during manufacturing at Infineon)
- ISO/IEC 14443-4 Type A [4]
- Data rate: Up to 848 kbit/s
- Frame size: 255 bytes
- WTX handling enabled
- Chaining supported
- NFC Forum Type 4 Tag compliant (see Chapter 2.3)

IRQ line:

- Configurable behavior depending on the mode of operation
  - Wake-up signal for host system
  - Indicating NFC state machine state transitions
  - Signaling I2C Data transfer
  - Initiating pass-through mode

5.1.1 Technical data

This section provides a brief overview of the absolute maximum ratings and operational characteristics of the OPTIGA™ Authenticate NBT. These include electrical AC and DC characteristics, interface characteristics and package characteristics.

***Notes**:*

1. *T_A as given for the operating temperature range of the device unless otherwise stated*

2. *All currents flowing into the device are considered positive*

5.1.1.1 Absolute maximum ratings

This section defines the absolute maximum ratings. Stresses exceeding the values listed in Table 4 may permanently damage the device. This is only a stress rating; functional operation of the device under these or any other conditions with values greater than those specified in the operational characteristics sections of this

specification is not implied. Long-term exposure to absolute maximum rating conditions may have an impact on device reliability, including NVM data retention and programming endurance.

Table 4 Absolute maximum ratings

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Operating temperature, ambient	T_A	-25	-	+85	°C	T_J (max) must not be exceeded
Operating temperature, ambient, extended range, no NFC field available	$T_{A\_EXT\_NONFC}$	-40	-	+105	°C	T_J (max) must not be exceeded; maximum depends on PCB design and operating conditions
Operating temperature, ambient, extended range, NFC field available	$T_{A\_EXT\_NFC}$	-40	-	+85	°C	T_J (max) must not be exceeded
Junction temperature	T_J	-	-	+110	°C	T_J (max) must not be exceeded
Supply voltage	V_{CC}	-0.3	-	4.6	V	
Input voltage SDA, SCL, IRQ	$V_{IN\_I2C\_IRQ}$	-0.3	-	V_{CC} + 0.3 or 4.6	V	
Input voltage (L_A - L_B)	V_{IN_LALB}	-6.0	-	+6.0	V	Maximum peak-to-peak amplitude of the AC input voltage at conditions of the "Alternating magnetic field" as per ISO/IEC14443-1 [1]
Input current (L_A - L_B)	I_{IN_LALB}	-	-	+/-150	mA	Maximum peak-to-peak amplitude of the AC input voltage at conditions of the "Alternating magnetic field" as per ISO/IEC14443-1 [1]
ESD robustness SDA, SCL, IRQ	$V_{ESD\_I2C\_IRQ,HBM}$	4000	-	-	V	Human body model
ESD robustness SDA, SCL, IRQ	$V_{ESD\_I2C\_IRQ,CDM}$	750	-	-	V	Charge device model
ESD robustness L_A, L_B	$V_{ESD\_LALB,HBM}$	3000	-	-	V	Human body model
ESD robustness L_A, L_B	$V_{ESD\_LALB,CDM}$	750	-	-	V	Charge device model
ESD robustness L_A, L_B against SDA, SCL, IRQ	$V_{ESD\_LALB\_I2C\_IRQ,HBM}$	2000	-	-	V	Human body model
ESD robustness L_A, L_B against SDA, SCL, IRQ	$V_{ESD\_LALB\_I2C\_IRQ,CDM}$	750	-	-	V	Charge device model
NVM data retention		10	-	-	Years	T_A = 25°C
NVM cycle endurance		200.000	-	-	Cycles	per NVM block[1)]

(table continues...)

Table 4 (continued) Absolute maximum ratings

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Storage temperature	T_S	+5	-	+40	°C	Infineon-originally packed, 10..75% humidity, up to 36 months. Condensation and bedewing shall be avoided

1) NVM blocks are not individually addressable with APDUs

5.1.1.2 Operational characteristics

This section specifies the AC and DC characteristics of the OPTIGA™ Authenticate NBT, as well as details about the specific interfaces provided by the device.

5.1.1.2.1 AC electrical characteristics

This section describes the AC electrical characteristics of the device.

Table 5 AC electrical characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
V_{CC} ramp-up time	t_{VCCR}	2[1)]	-	-	µs	0 to 100% of V_{CC} target voltage ramp
Device start-up time V_{CC} powered	$t_{STARTUP\_VCC}$	-	1	-	ms	T_A = +25°C Defines the time from power-on (V_{CC} ≥ 1.62 V) to STANDBY mode
Device start-up time NFC field powered	$t_{STARTUP\_NFC}$	-	420	-	µs	T_A = +25°C Class-5 reference antenna, resonance frequency: 13.8 MHz
Contactless interface initialization time	t_{INIT_NFC}	-	150	-	µs	T_A = +25°C Device is V_{CC} powered, NFC interface initialization time until it is ready for communication

1) At a faster supply ramp-up time the device internal ESD elements cause temporarily a cross current between V_{CC} and GND

Power-up considerations

The ramp-up times in Table 5 are based on the assumption of a linear voltage rise from 0% to 100% of the target voltage level. However, due to the possibility of current spike effects, it is recommended to follow the voltage characteristics shown in the figure below.

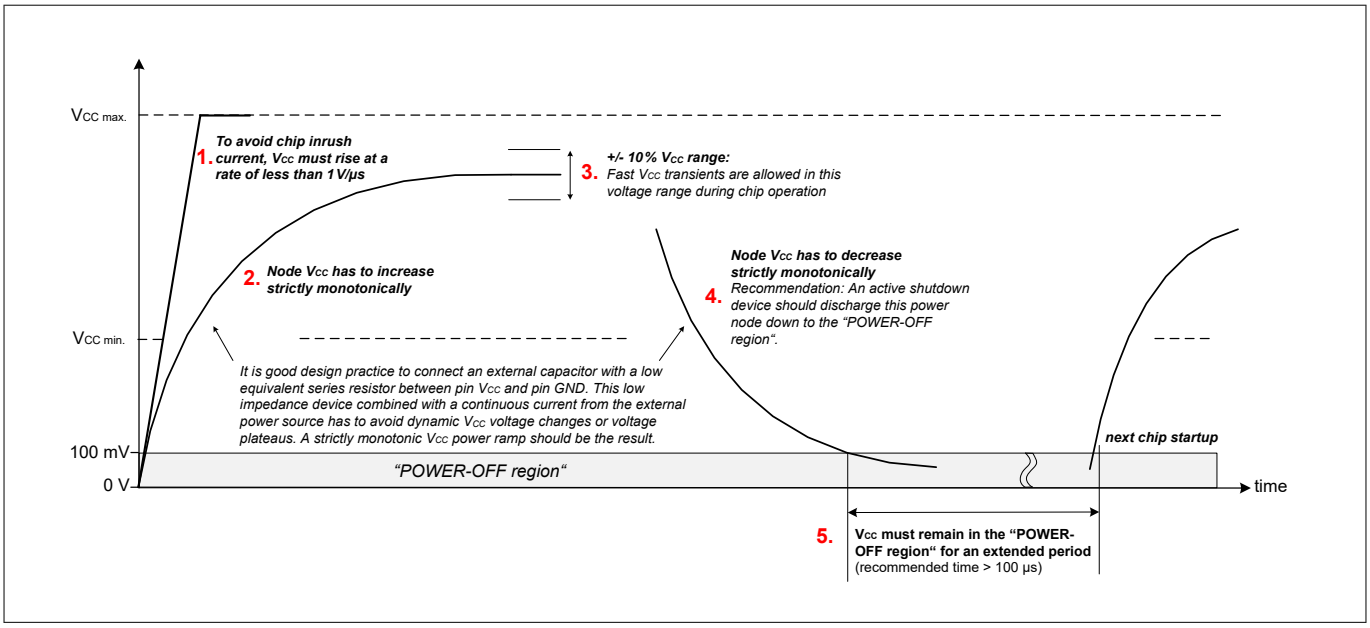


Figure 12 Recommended power-up behavior

Device start-up

After a power-on reset, the device starts by executing a boot initialization sequence before entering STANDBY mode. At the end of the start-up, the pins are re-configured for the use as I2C interface and IRQ.

Prior to re-configuration, the pins are in the hardware reset state:

- SCL and SDA: Input is enabled, output is disabled (SDA), and internal weak pull-up is enabled
- IRQ: Input is enabled, output is disabled[3)]

After the device start-up:

- SCL and SDA pins are reconfigured for I2C operation to open drain and the internal pull-up is disabled
- The IRQ pin is reconfigured to act as output (push-pull)

Figure 13 depicts the device start-up behavior and the corresponding basic timings and average currents.

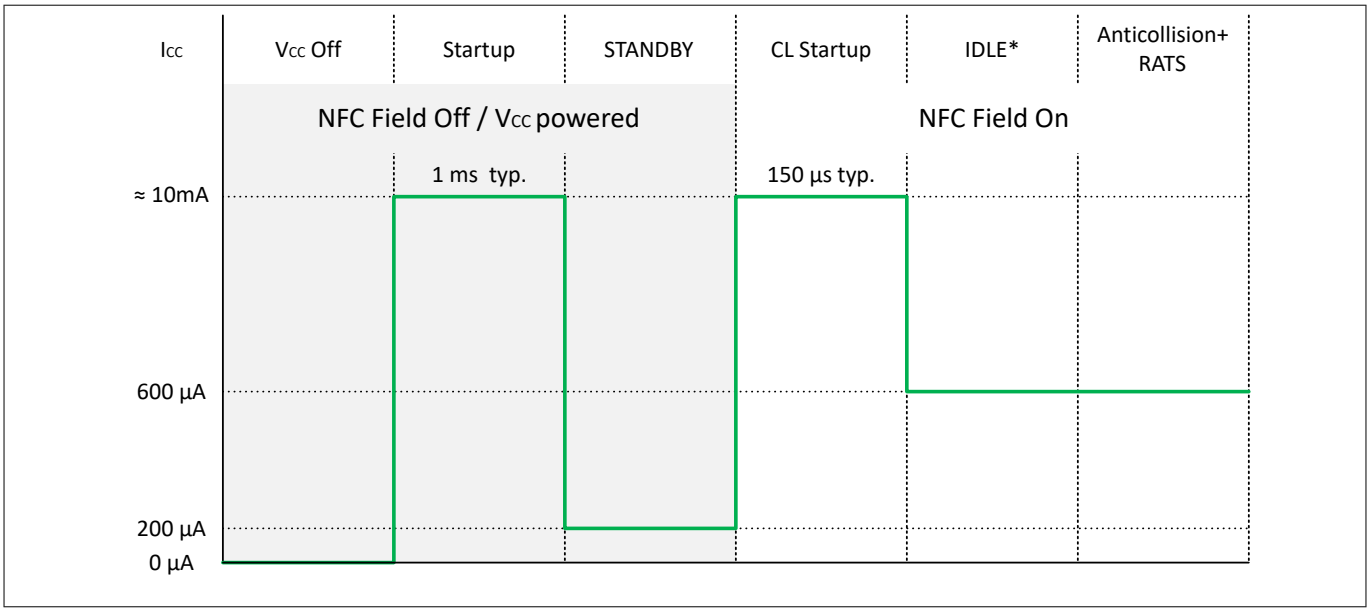


Figure 13 Device start-up behavior

3 The host system and/or external circuitry must keep the IRQ static (0 or 1) during $t_{STARTUP\_VCC}$

5.1.1.2.2 DC electrical characteristics

This section describes the DC electrical characteristics of the device.

Table 6 DC electrical characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Supply voltage	V_{CC}	1.62	-	3.63	V	Overall functional range
Supply voltage operational	V_{CC_OP}	V_{CC_NOM} *0.9	-	V_{CC_NOM} *1.1	V	During device operation (all states, including STANDBY) the supply voltage must stay within this range around the nominal supply voltage V_{CC_NOM} Maximum operating voltage must stay below V_{CC_max}
Supply current, ACTIVE mode	I_{CC_ACTIVE}	-	10.1	-	mA	V_{CC} = 3.3 V, T_A= 25°C
Supply current, no NFC field available	I_{CC1}	-	9.9	-	mA	V_{CC} = 1.98 V, T_A= 25°C
Supply current, no NFC field available	I_{CC2}	-	10.3	-	mA	V_{CC} = 1.98 V, T_A= 105°C
Supply current, no NFC field available	I_{CC3}	-	10.0	-	mA	V_{CC} = 3.63 V, T_A= 25°C
Supply current, no NFC field available	I_{CC4}	-	10.4	-	mA	V_{CC} = 3.3 V, T_A= 105°C
Supply current, no NFC field available, current limitation enabled	I_{CC1_CURLIM}	-	4.2	-	mA	V_{CC} = 1.98 V, T_A= 25°C Current limitation = ON (default value: 06_H)
Supply current, no NFC field available	I_{CC2_CURLIM}	-	4.4	-	mA	V_{CC} = 1.98 V, T_A= 105°C Current limitation = ON (default value: 06_H)
Supply current, no NFC field available	I_{CC3_CURLIM}	-	4.3	-	mA	V_{CC} = 3.63 V, T_A= 25°C Current limitation = ON (default value: 06_H)
Supply current, no NFC field available	I_{CC4_CURLIM}	-	4.6	-	mA	V_{CC} = 3.63 V, T_A= 105°C Current limitation = ON (default value: 06_H)
Supply current IDLE mode, NFC	$I_{CC\_IDLE\_NFC}$	-	600	-	µA	V_{CC} = 3.3 V, T_A= 25°C
Supply current IDLE mode, I2C	$I_{CC\_IDLE\_I2C}$	-	600	-	µA	V_{CC} = 3.3 V, T_A= 25°C
Supply current STANDBY mode	$I_{CC\_STANDBY}$	-	-	200	µA	V_{CC} = 3.3 V, T_A= 25°C

5.1.2 NFC interface characteristics

The interface pads to an antenna coil are L_A and L_B. The resonance frequency of the serial resonance circuit depends on the input capacitance between L_A and L_B and with the coil inductance.

The voltage obtained at the device contacts is primarily defined by the following factors:

- The RF field strength and, together with the coil geometry, the resulting induced voltage
- The resonance frequency and
- The quality factor (mainly defined by the current consumption of the OPTIGA™ Authenticate NBT)

Table 7 NFC interface characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Maximum input current at (L_A - L_B), L_B	$I_{IN\_LALB\_OP}$	-	-	+/-90	mA	Maximum peak input current
L_A/L_B input capacitance	C_P	-	75.6	-	pF	Tolerance +/- 10% see Note

***Notes**:*

1. *Measurement conditions for L_A/L_B input capacitance:*
Threshold point: 2.8 V_{PEAK}, 13.56 MHz, RFI in reception mode (system in STANDBY mode), device operating on contactless power; bare die only (package details available on request, please contact Infineon Technologies).

2. *The parameter L_A/L_B input capacitance is not tested during production. Value ranges are based on measurements during qualification of the product at different technology corners.*

3. *Hints and guidelines for antenna design are available in the Antenna Design Guide document [16].*

5.1.3 I2C interface characteristics

The electrical characteristics of the I2C interface are given below.

5.1.3.1 General I2C characteristics

Table 8 I2C operational supply and input voltages

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Supply voltage	V_{CC}	1.62	-	3.63	V	V_{CC} to 3.3 V +10%
SDA, SCL input voltage	V_{IN_I2C}	-0.3	-	V_{CC} + 0.5	V	V_{IN_I2C} is the internal voltage domain for the I2C interface, which is internally connected to the V_{CC} pad
	$V_{IN\_I2C\_SWITCHED\ OFF}$	-0.3	-	0.5	V	V_{CC} is switched off. See Note

***Note**:* *The power supply of the OPTIGA™ Authenticate NBT must not be switched off as the device may drain significant pad input current.*

5.1.3.2 I2C standard/fast mode interface characteristics

The electrical characteristics of the I2C interface are in accordance with the I2C bus specification [25] for "standard-mode" (f_{SCL} up to 100 kHz), "fast-mode" (f_{SCL} up to 400 kHz), and "fast-mode plus" (f_{SCL} up to 1 MHz), with the exceptions listed in the tables below.

Table 9 I2C standard mode interface characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	-	100	kHz	
Input low-level voltage	V_{IL}	-0.3	-	0.3*V_{CC}	V	
Input high-level voltage	V_{IH}	0.7*V_{CC}	-	V_{CC}+0.5	V	
Low-level output voltage	V_{OL1}	0	-	0.4	V	Sink current 3 mA; $V_{CC} \geq 2.7$ V Sink current 2 mA; $V_{CC} < 2.7$ V
Low-level output current	I_{OL}	3 2	-	-	mA	$V_{OL} = 0.4$ V; $V_{CC} \geq 2.7$ V $V_{OL} = 0.4$ V; $V_{CC} < 2.7$ V
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	-	-	250	ns	$C_b \leq 400$ pF; $V_{CC} \geq 2.7$ V $C_b \leq 200$ pF; $V_{CC} < 2.7$ V
Hold time for START (S, Sr) condition	$t_{HD;STA}$	4	-	-	µs	
SCL low period	t_{LOW}	4.7	-	-	µs	
SCL high period	t_{HIGH}	4.0	-	-	µs	
Setup time for repeated START (Sr) condition	$t_{SU;STA}$	4.7	-	-	µs	
SDA hold time	$t_{HD;DAT}$	0	-	-	ns	
SDA input setup time	$t_{SU;DAT}$	250	-	-	ns	
SDA/SCL rise time (bus line)	t_r	-	-	1000	ns	
SDA fall time (bus line, input)	t_{fSDA}	-	-	300	ns	
SCL fall time (bus line, input)	t_{fSCL}	-	-	300	ns	
Setup time for STOP (P) condition	$t_{SU;STO}$	4.0	-	-	µs	

(table continues...)

Table 9 (continued) I2C standard mode interface characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Bus free time between STOP (P) and START (S) condition	t_{BUF}	4.7	-	-	µs	
SDA output valid time	$t_{VD;DAT}$	-	-	3.45	µs	
Input capacitance (package pin)	C_I	-	9	15	pF	
Capacitance load for each bus line	C_b	-	-	400 200	pF	$V_{CC} \geq 2.7$ V $V_{CC} < 2.7$ V

Table 10 I2C fast mode interface characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	-	400	kHz	
Input low-level voltage	V_{IL}	-0.3	-	$0.3*V_{CC}$	V	
Input high-level voltage	V_{IH}	$0.7*V_{CC}$	-	$V_{CC}+0.5$	V	
Low-level output voltage	V_{OL1}	0	-	0.4	V	Sink current 3 mA; $V_{CC} \geq 2.7$ V Sink current 2 mA; $V_{CC} < 2.7$ V
Low-level output voltage	V_{OL2}	0	-	$0.2*V_{CC}$	V	Sink current 2 mA; $V_{CC} \leq 2$ V
Low-level output current	$I_{OL(0.4)}$	3 2	-	-	mA	$V_{OL} = 0.4$ V; $V_{CC} \geq 2.7$ V $V_{OL} = 0.4$ V; $V_{CC} < 2.7$ V
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	-	-	250	ns	$C_b \leq 400$ pF; $V_{CC} \geq 2.7$ V $C_b \leq 200$ pF; $V_{CC} < 2.7$ V
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	$20*V_{CC}/5.5$ V	-	250	ns	$C_b = 400$ pF
Spikes suppressed by input filters	t_{SP}	-	-	50	ns	
Hold time for START (S, Sr) condition	$t_{HD;STA}$	0.6	-	-	µs	
SCL low period	t_{LOW}	1.3	-	-	µs	

(table continues...)

Table 10 (continued) I2C fast mode interface characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCL high period	t_{HIGH}	0.6	-	-	µs	
Setup time for repeated START (Sr) condition	$t_{SU;STA}$	0.6	-	-	µs	
SDA hold time	$t_{HD;DAT}$	0	-	-	ns	
SDA input setup time	$t_{SU;DAT}$	100	-	-	ns	
SDA/SCL rise time (bus line)	t_r	20	-	300	ns	
SDA fall time (bus line, input)	t_{fSDA}	-	-	300	ns	
SCL fall time (bus line, input)	t_{fSCL}	-	-	300	ns	
Setup time for STOP (P) condition	$t_{SU;STO}$	0.6	-	-	µs	
Bus free time between STOP (P) and START (S) condition	t_{BUF}	1.3	-	-	µs	
SDA output valid time	$t_{VD;DAT}$	-	-	0.9	µs	
Input capacitance (package pin)	C_I	-	9	15	pF	
Capacitance load for each bus line	C_b	-	-	400 200	pF	$V_{CC} \geq 2.7$ V $V_{CC} < 2.7$ V

5.1.3.3 I2C fast mode plus interface characteristics

The electrical characteristics of the I2C interface are in accordance with the I2C bus specification [25] for "fast mode plus" (f_{SCL} up to 1 MHz), with a few exceptions listed in the table below.

Table 11 I2C fast mode interface characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	-	1	MHz	
Input low-level voltage	V_{IL}	-0.3	-	$0.3*V_{CC}$	V	
Input high-level voltage	V_{IH}	$0.7*V_{CC}$	-	$V_{CC}+0.5$	V	

(table continues...)

Table 11 (continued) I2C fast mode interface characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Low-level output voltage	V_{OL1}	0	-	0.4	V	Sink current 3 mA; $V_{CC} \geq 2.7$ V Sink current 2 mA; $V_{CC} < 2.7$ V
Low-level output current	I_{OL}	3 2	-	-	mA	$V_{OL} = 0.4$ V; $V_{CC} \geq 2.7$ V $V_{OL} = 0.4$ V; $V_{CC} < 2.7$ V
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	-	-	120	ns	$C_b \leq 150$ pF
Spikes suppressed by input filters	t_{SP}	-	-	50	ns	
Hold time for START (S, Sr) condition	$t_{HD;STA}$	260	-	-	ns	
SCL low period	t_{LOW}	500	-	-	ns	
SCL high period	t_{HIGH}	260	-	-	ns	
Setup time for repeated START (Sr) condition	$t_{SU;STA}$	260	-	-	ns	
SDA hold time	$t_{HD;DAT}$	0	-	-	ns	
SDA input setup time	$t_{SU;DAT}$	50	-	-	ns	
SDA/SCL rise time (bus line)	t_r	-	-	120	ns	
SDA fall time (bus line, input)	t_{fSDA}	-	-	120	ns	
SCL fall time (bus line, input)	t_{fSCL}	-	-	120	ns	
Setup time for STOP (P) condition	$t_{SU;STO}$	260	-	-	ns	
Bus free time between STOP (P) and START (S) condition	t_{BUF}	500	-	-	ns	
SDA output valid time	$t_{VD;DAT}$	-	-	450	ns	
Input capacitance (package pin)	C_I	-	9	15	pF	
Capacitance load for each bus line	C_b	-	-	150	pF	

5.1.4 IRQ interface characteristics

The electrical characteristics of the OPTIGA™ Authenticate NBT's IRQ pin, including restrictions on maximum sink / source currents, are listed below.

Table 12 DC electrical characteristics of the IRQ

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Output low voltage	V_{OL}	-	-	0.3	V	I_{OL} = 1 mA
Output low voltage	V_{OL}	-	-	0.4	V	I_{OL} = 4 mA $V_{CC} \geq 2.7$ V
Output low current	I_{OL}	1	-	-	mA	V_{OL} = 0.3 V
Output low current	I_{OL}	4	-	-	mA	V_{OL} = 0.4 V $V_{CC} \geq 2.7$ V
Output high voltage	V_{OH}	V_{CC} – 0.3	-	-	V	I_{OL} = -1 mA
Output high voltage	V_{OH}	V_{CC} – 0.4	-	-	V	I_{OL} = -4 mA $V_{CC} \geq 2.7$ V
Output high current	I_{OH}	-1	-	-	mA	$V_{OH} = V_{CC}$ – 0.3 V
Output high current	I_{OH}	-4	-	-	mA	$V_{OH} = V_{CC}$ – 0.4 V $V_{CC} \geq 2.7$ V
Input capacitance	C_{IN_IRQ}	-	9	15	pF	Pad capacitance is subject to process variation and depending on supply voltage (increasing capacitance at lower supply)

***Note**: The power supply of the OPTIGA™ Authenticate NBT must not be switched off as the device may drain significant pad input current.*

Table 13 AC electrical characteristics of the IRQ

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Output signal rise time	t_r	-	4.5	15	ns	10% V_{CC} to 90% V_{CC} C_{LOAD} = 15 pF pull-up/pull-down: off no DC load
Output signal fall time	t_f	-	4.5	15	ns	90% V_{CC} to 10% V_{CC} C_{LOAD} = 15 pF pull-up/pull-down: off no DC load

5.1.5 Package characteristics

The overall thermal performance of a package in a system is generally characterized by junction-to-ambient thermal resistance chains. Typically, the application of the device defines the thermal requirements of the

system while the package type and outline defines the boundary conditions for implementing the thermal management on the PCB assembly.

Table 14 PG-USON-8-8 package characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Thermal resistance	$R_{th\text{-}ja}$	-	58.1	-	K/W	JEDEC 2s2p board and PG-USON-8-8 package; exposed die pad of package connected to common ground (GND) for heat distribution with two vias
Thermal resistance case to top of package	$R_{th\text{-}jCtop}$	-	96.4	-	K/W	Exposed die pad of PG-USON-8-8 package connected to common ground (GND) for heat distribution with two vias. See Figure 14
Thermal resistance pins and case to bottom of package	$R_{th\text{-}jpins\_Cbot}$	-	6.44	-	K/W	Exposed die pad of PG-USON-8-8 package connected to common ground (GND) for heat distribution with two vias. See Figure 14

Figure 14 shows the thermal equivalent circuit of the packaged device.

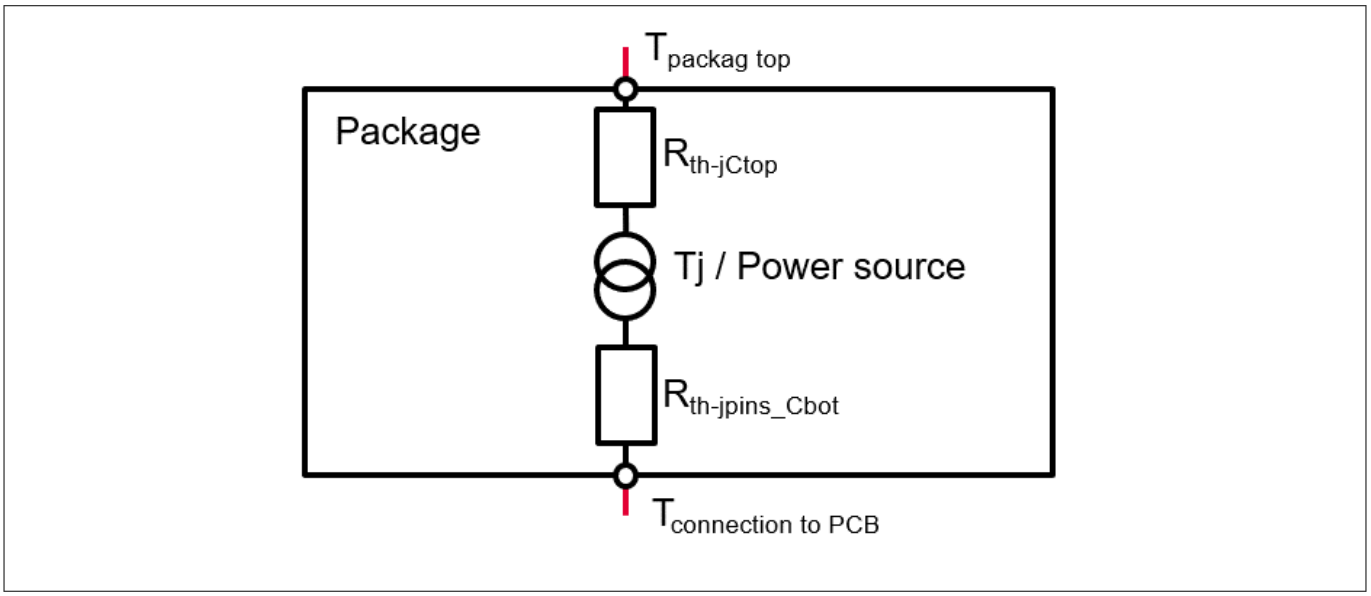


Figure 14 Package characteristics

5.1.6 Hardware integration diagram

This section list some key principles for the integration of the OPTIGA™ Authenticate NBT in various application use cases. The device can operate as a standalone device without requiring any connection to a host. The device must be connected to an NFC antenna through its L_A and L_B pins to obtain energy from the electromagnetic field the NFC reader. Figure 15 illustrates the NFC-only tag configuration.

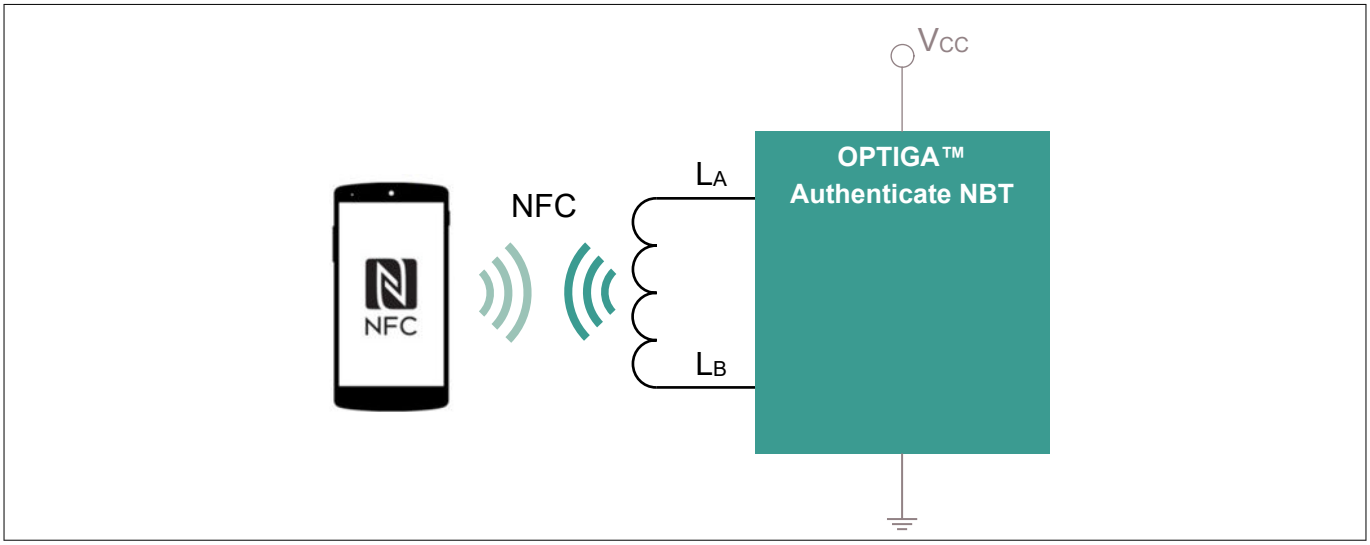


Figure 15 NFC-only tag

The tag may also be connected to an external supply via its power pins (V_{CC}, GND). In this scenario, the OPTIGA™ Authenticate NBT is powered from this external supply and may communicate with the NFC reader in the range of its NFC antenna.

In NFC-to-I2C bridge use cases, the OPTIGA™ Authenticate NBT is embedded into a system that includes a host MCU and an NFC antenna. The device is externally supplied from the host system through its power pins V_{CC} and GND and is connected to the host MCU via its I2C target interface (see Figure 16).

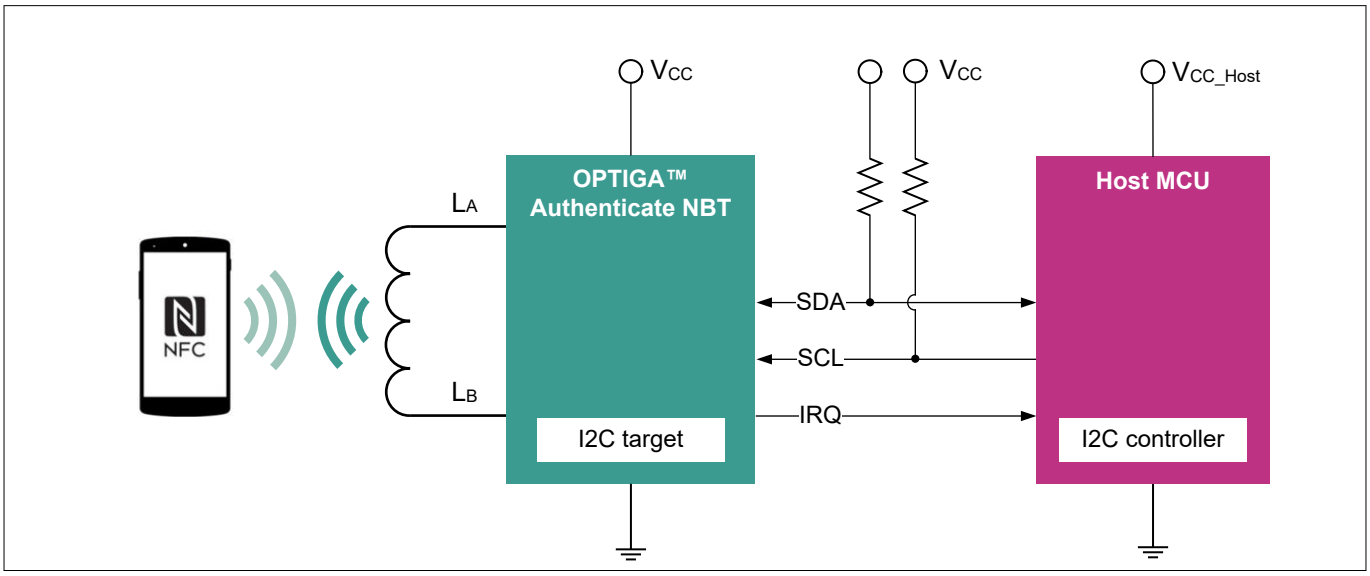


Figure 16 Bridge tag

While the host MCU and the OPTIGA™ Authenticate NBT may be powered with different voltages (V_{CC_Host} and V_{CC}), a single voltage domain is preferred to avoid the usage of level shifters. V_{CC} must not exceed the allowed input voltage levels of the I2C controller device.

For more information on hardware integration, refer to [17].

5.2 Embedded software

The embedded software primarily aims to manage the following tasks:

- Communication interfaces and protocols
- Power states and communication modes
- Product administration
- Product life cycle states and transitions
- Use cases operation

5.2.1 Communication interfaces

The product supports two communication interfaces:

- I2C protocol implementation, according to [13]
- NFC protocol implementation, according to ISO/IEC 14443 standard, Type A [3][4]

In the delivery configuration, both interfaces are active after the startup of the OPTIGA™ Authenticate NBT, however the interfaces can only be used in a mutually exclusive manner.

In case an NFC reader is selecting the Type 4 Tag application on the OPTIGA™ Authenticate NBT, then the device is locked into the NFC communication mode for the duration while the NFC field is present. During an active NFC session, I2C requests will not be acknowledged.

In case I2C communication is initiated, the device will remain in the I2C communication mode for the duration while the host is active and the preset I2C idle timeout is not yet expired. During an active I2C session, NFC communication will not be acknowledged.

The OPTIGA™ Authenticate NBT handles both interfaces without the need for a power cycle. Furthermore, it supports two modes of operation and employs different communication models:

- Asynchronous data transfer
- Synchronous pass-through communication

These are the conditions that need to be met to switch the communication interface:

- From I2C to NFC is only possible when the device is in STANDBY state (preset I2C idle timeout expired)
- From NFC to I2C is only possible when the NFC field is removed

Refer to Chapter 5.2.3 for more details.

Figure 17 illustrates interface handling and emphasizes on the mutual exclusive usage of communication interfaces.

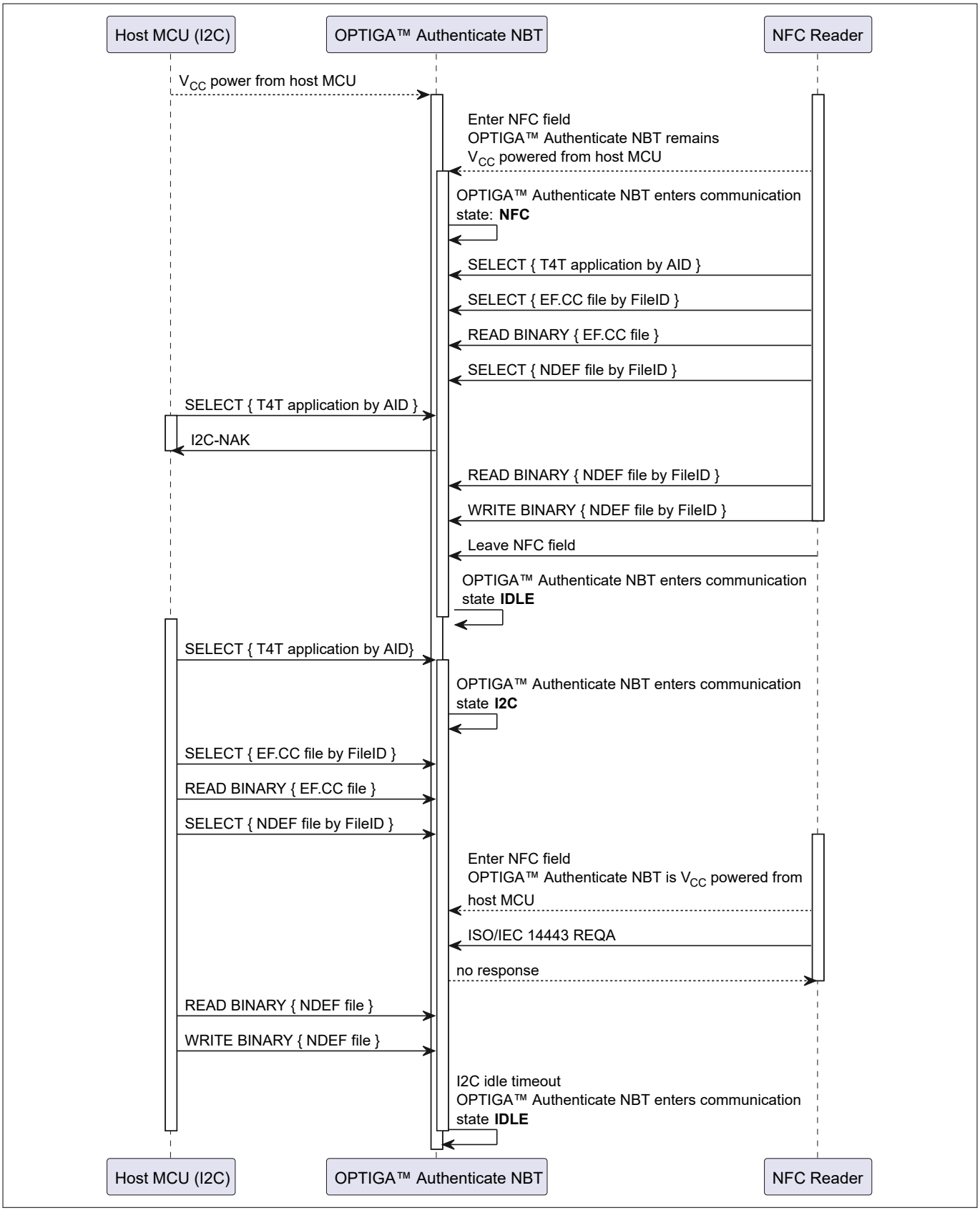


Figure 17 Communication interface handling

Depending on the targeted use case, the customer may also choose to disable one of the communication interfaces (NFC or I2C). For setting up the communication interface, refer to Table 15.

IRQ pin usage

The IRQ line of the OPTIGA™ Authenticate NBT can be configured for one of the following functions:

- signaling NFC state machine state transitions
- I2C data ready interrupt, see Chapter 5.2.1.1
- NFC-to-I2C pass through data available signaling, see Chapter 5.2.6.2

NFC event types

If the IRQ line is configured to signal transitions of the NFC state machine it can be used to trigger an event or wake up the host system.

The signaling of NFC events can be configured for one of the following events:

- NFC field presence
- activation of ISO/IEC 14443 Layer 4 (application layer)
- APDU processing stage

***Note**: The SET CONFIGURATION command is used to configure the OPTIGA™ Authenticate NBT. Refer to the Chapter 5.2.4.1 for configuration instructions.*

5.2.1.1 I2C protocol

The I2C communication protocol is implemented according to [13].

The I2C communication interface supports the following features:

- Target interface, 7-bit address, initial device address: 18_H
- Supported clock frequencies
  - Standard mode (SM) 100 kHz
  - Fast mode (FM) 400 kHz
  - Fast mode plus (FM+) 1000 kHz
- Clock stretching is not supported
- The OPTIGA™ Authenticate NBT implements a proprietary power saving method:
  - Enters IDLE power state immediately after sending a response
  - Enters STANDBY power state when the I2C idle timeout expires
- Two modes are supported to detect if the device is ready to send data:
  - Polling mechanism
  - Data ready interrupt mechanism over the IRQ (I2C-IRQ), according to the GP T=1' protocol specification

For available configuration options, refer to Table 15.

5.2.1.2 NFC protocol

The NFC communication protocol is according to [9].

The NFC communication interface supports following features:

- 7-byte UID (fixed, programmed during manufacturing at Infineon)
- ISO/IEC 14443-4 Type A
- Data rate: Up to 848 kbit/s
- Frame size: 255 bytes
- WTX handling enabled
- Chaining supported
- NFC Forum Type 4 Tag compliant

5.2.2 Product life cycle states

The OPTIGA™ Authenticate NBT supports two life cycle states:

- PERSONALIZATION state: The device will be in the PERSONALIZATION state at the time of delivery. In this life cycle state, application developers can unconditionally modify the specific settings to prepare the device for the targeted use case. This covers:
  - Interface configurations
  - File access conditions and passwords
  - Cryptographic keys
  - File content

When the product configuration and the data personalization steps are finished, the OPTIGA™ Authenticate NBT can be switched to the OPERATIONAL life cycle state.

- OPERATIONAL state: In this state, the device is ready to be used in the target application scenario. Product configuration functions are disabled. Configured file access policies prevent unverified operations on the file (based on the use case configuration). When the product is in OPERATIONAL state, the life cycle cannot be restored to PERSONALIZATION state and the configuration is locked

***Note**: Prior to distribution to the end customers, the application developer must ensure that the product is in OPERATIONAL state to prevent unintended modification of the chip configurations and application data.*

***Note**: The SET CONFIGURATION command or the PERSONALIZE DATA command can be used to trigger this life cycle state transition.*

5.2.3 Power and communication states

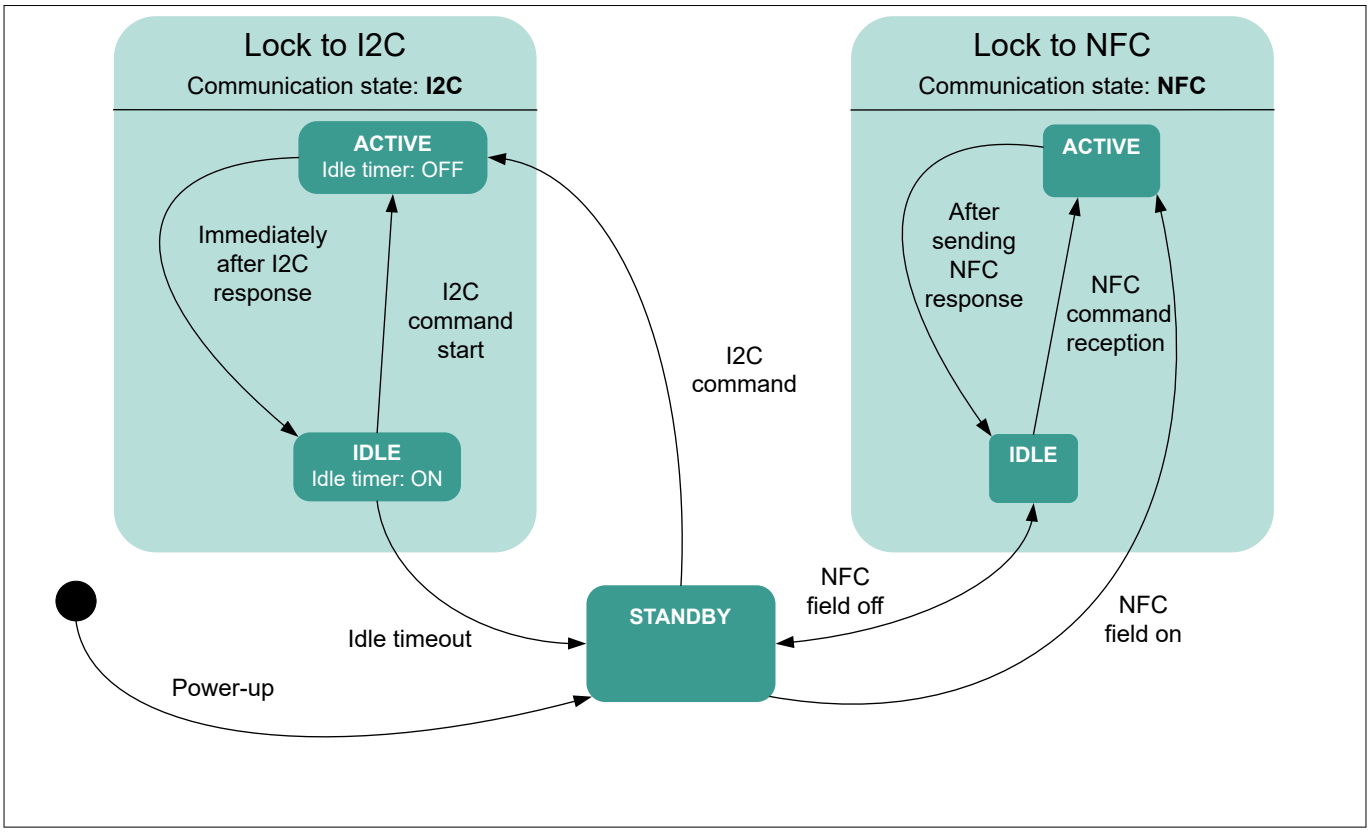


Figure 18 Power and communication states

The OPTIGA™ Authenticate NBT can either be powered from the RF field of an NFC reader or from an external supply via its power pins (V_{CC}, GND). In case the device is powered from the NFC field, communication over I2C/IRQ is not possible.

After a power-on reset, the device starts by executing a boot initialization sequence before entering STANDBY mode (see Power-up considerations).

If the I2C communication is active, the OPTIGA™ Authenticate NBT is locked into I2C operation. The device will enter the IDLE state immediately after processing and sending the response to an I2C command. It will return to STANDBY state once the preset I2C idle timeout expires (see Table 15 and Chapter 5.3).

The OPTIGA™ Authenticate NBT power reset may be achieved in the following ways:

- While powered by the NFC field only, remove the device from the field
- While in V_{CC} powered mode (V_{CC}, GND) either by:
  - Power cycle, or
  - I2C software reset (SWR)

5.2.4 Product administration

The OPTIGA™ Authenticate NBT provides a set of administrative parameters to configure the device for the targeted use case. The following chip settings can be modified to prepare the device accordingly:

- Configuration of the hardware, communication interface and IRQ settings
- File access rights to user data files can be specified based on application requirements
- Update/exchange of the symmetric AES-128 key (BMK)
- Update/exchange of the asymmetric ECC key (BSK) to match the customer-specific certificate

Specific parameter values can either be read from (GET CONFIGURATION) or written to (SET CONFIGURATION) the OPTIGA™ Authenticate NBT after selecting the CONFIGURATOR applet.

5.2.4.1 Hardware configuration

Here are the features and functionalities that can be configured on the OPTIGA™ Authenticate NBT:

- Interface activation/deactivation
- Behavior of the IRQ line: Function, assert level, output type
- NFC IRQ event type: RF field detection, Layer-4 entry
- I2C interface configuration: Target address, idle time out, I2C data rate
- NFC interface configuration: UID type, ATS response, WTX mode
- Life cycle state transition
- Current limitation: Activation and adjustment

Table 15 provides a list of parameters and possible values.

In order to enable administrative operations the CONFIGURATOR applet must be successfully selected. The configuration changes will be activated only after a device restart by either a power cycle or a software reset (SWR) triggered through the I2C interface.

Table 15 Configuration reference table

Tag	Length [bytes]	Value	GET CONFIGURATION	SET CONFIGURATION[1)]	Description
$C020_H$	10_H		✓		*Product short name*
$C021_H$	02_H		✓	✓	Product life cycle states (see Chapter 5.2.2)
		$5AA5_H$			PERSONALIZATION state
		$C33C_H$			OPERATIONAL state

(table continues...)

Table 15 (continued) Configuration reference table

Tag	Length [bytes]	Value	GET CONFIGURATION	SET CONFIGURATION[1)]	Description
$C022_H$	08_H		✓		*Software version information*
$C028_H$	04_H		✓		Manufacturer specific data
$C029_H$	04_H		✓		Manufacturer specific data
$C030_H$	01_H		✓	✓	*IRQ function*
		01_H			Disabled
		02_H			NFC-IRQ: NFC IRQ output, see Chapter 5.2.1
		03_H			I2C-IRQ: I2C data ready IRQ output, see Chapter 5.2.1.1
		04_H			PT-IRQ: NFC-I2C pass-through IRQ output, see Chapter 5.2.6.2
$C031_H$	01_H		✓	✓	*IRQ assert level*
		01_H			Low level active
		02_H			High level active
$C032_H$	01_H		✓	✓	*IRQ output type*
		01_H			Push-pull
		02_H			Open-drain
$C033_H$	01_H		✓	✓	*IRQ pull type*
		01_H			No pull
		02_H			Pull up
		03_H			Pull down
$C034_H$	01_H		✓	✓	*NFC IRQ event type*
		01_H			RF field presence
		02_H			Layer 4 entry
		03_H			APDU processing stage
$C040_H$	04_H		✓	✓	*I2C idle timeout*
		$XXXXXXXX_H$			I2C idle timeout defined in milliseconds[2)], see Chapter 5.2.3
$C041_H$	01_H		✓	✓	*I2C drive strength*
		01_H			Weak
		02_H			Strong
$C042_H$	01_H		✓	✓	*I2C speed[3)] [4)]*
		00_H			100 kHz
		01_H			400 kHz
		02_H			1000 kHz
$C043_H$	01_H		✓	✓	*I2C target address*

(table continues...)

Table 15 (continued) Configuration reference table

Tag	Length [bytes]	Value	GET CONFIGURATION	SET CONFIGURATION[1)]	Description
		XX_H			I2C target address according to I2C bus specification
$C050_H$	$0E_H$		✓	✓	*NFC ATS configuration*[5)]
					ATS according to ISO/IEC 14443 Type A[6) 7)]
$C051_H$	01_H		✓	✓	*NFC WTX mode*[8)]
		00_H			Manual WTX sending
		$01_H..3B_H$			Automatic WTX sending with this value as WTXM multiplier
$C052_H$	$FF0138_H$		✓	✓	*NFC RF hardware configuration*[9)]
					Use only Infineon provided calibration values[10)]
$C053_H$	01_H		✓	✓	*NFC UID type for anti-collision*
		00_H			Unique device specific 7-byte NFC UID
		01_H			Random 4-byte NFC UID
$C060_H$	01_H		✓	✓	*Communication interface enable*
		01_H			NFC disabled | I2C enabled
		10_H			NFC enabled | I2C disabled
		11_H			NFC enabled | I2C enabled
$C061_H$	01_H		✓	✓	*Current limitation*
		01_H			No current limitation
		02_H			Current limitation enabled[11)]
$C062_H$	01_H		✓	✓	*Current limitation configuration*
		$02_H..1F_H$			Use only Infineon provided calibration values

1) Limited to PERSONALIZATION life cycle state
2) Low values will have a negative effect on communication performance. The minimal accepted value is 2 x polling time, however, it is not smaller than 10 ms
3) Lower communication speeds can always be initiated by the host
4) Lowering the speed allows for higher I2C line capacitance
5) Incorrect settings will result in NFC communication issues
6) The first byte of the ATS string must contain the total length of the ATS string
7) Incorrect settings will result in NFC communication issues
8) Incorrect settings will result in NFC communication issues
9) The configuration is limited to PERSONALIZATION life cycle state
10) Attention: Incorrect settings will render the NFC interface unusable
11) See table Table 6 for typical current consumption

***Note**: Changes of interface configurations are restricted to the PERSONALIZATION life cycle state (refer to Chapter 5.2.2).*

***Note**: Default product configuration is summarized in Table 24.*

5.2.4.2 File access policy

The EF.FAP file contains file access policy settings for any file within the application (EF.CC, EF.NDEF, the four proprietary EFs, and EF.FAP). The FAP is used to manage operations on a per-file and per-interface basis.

For more information on the EF.FAP file, refer to Chapter 5.2.5.4.

5.2.4.3 Key loading

During the personalization phase, both the symmetric AES-128 key for the online brand protection scheme and the asymmetric ECC key for the offline brand protection procedure can be updated to customer-specific values. These data elements must be encoded in dedicated DGIs (Data Group Identifiers) and transferred to the OPTIGA™ Authenticate NBT (refer to Chapter 5.4.2).

5.2.4.4 Certificate loading

The NFC Type 4 Tag application comes with a certificate loaded already (by default, within the NDEF message).

***Note**: The applet makes no sanity or cryptographic checks on the loaded certificate. As a consequence, the verifier's responsibility is to parse and validate the certificate off-chip.*

5.2.5 NFC tag

An NFC tag in the context of this product, is an NFC-enabled tag or IoT device that implements the NFC Forum Type 4 Tag Technical Specification [7] for hosting NDEF messages. It can be accessed by a reader device that implements the operational part of the Type 4 Tag Technical Specification. The ISO/IEC 14443 Type A transmission protocol is implemented by Type 4 Tags in particular. The NFC Data Exchange Format (NDEF) allows data to be exchanged between an NFC reader and an NFC tag. The data format consists of NDEF messages and records.

An NDEF message is a basic NDEF record transport mechanism, with each message containing one or more NDEF records. An NDEF record contains application data described by a type, a length, and an optional FileID. However, an empty NDEF message contains only one NDEF record.

The data structure of an NDEF message stored on an NFC Forum Type 4 Tag is based on ISO/IEC 7816-4 and employs a tree structure. Figure 19 illustrates the pictorial representation of the Type 4 Tag application file with a defined ADF, a defined Capability Container file (EF.CC), and a defined NDEF file.

The EF.CC file (see Chapter 5.2.5.1) is a read-only binary file which contains all information needed to identify, to read and to write an NDEF file. The relevant data is embedded in a file control TLV structure. This NDEF-File_Ctrl_TLV contains the FileID of the NDEF file (here: $E104_H$), the file size of the NDEF file and access conditions (read/write).

***Note**: The "read-only" condition of the EF.CC file only applies to Tag readers and the UPDATE BINARY command. Proprietary commands to lock the file are implementation-specific.*

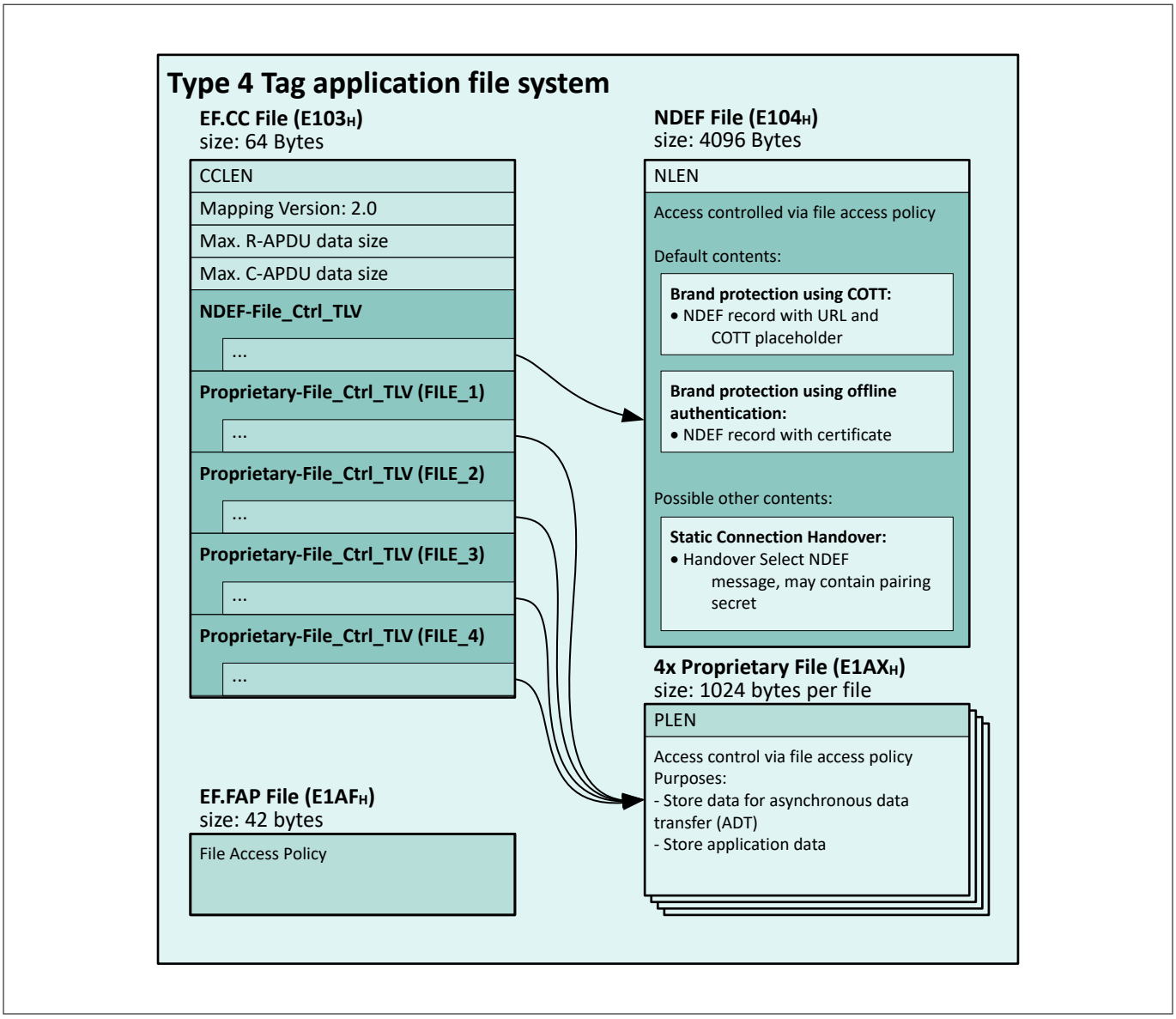


Figure 19 Type 4 Tag file structure

5.2.5.1 Capability Container (EF.CC) file

The EF.CC file with the FileID $E103_H$ is created with a file size of 64 bytes. The first 47 bytes of the EF.CC file contain all information needed to read and write the NDEF message in addition to the proprietary files existing within the Type 4 Tag application on the OPTIGA™ Authenticate NBT. The remaining 17 bytes are RFU with the value 00_H. Default values are created as listed in Table 16.

The EF.CC file is read-only by default; however, additional FAP conditions will be applicable if defined in the EF.FAP file, and upon achieving the conditions, the EF.CC file can be updated as well. The Type 4 Tag application will then allow to change the access conditions within the Proprietary-File_Ctrl_TLVs. The applet will not perform any consistency checks. Updates to the CC fields T4T_VNo, MLe, MLc, NDEF-File_Ctrl_TLV are not permitted at all.

Table 16 EF.CC file content

CC field	Offset	Size (bytes)	Data	Content
CCLEN	0000_H	2	$002F_H$	CCLEN indicates the length of valid data within the CC file and contains file-related information
T4T_VNo	0002_H	1	20_H	Mapping Version 2.0
MLe	0003_H	2	0100_H	Maximum R-APDU data size
MLc	0005_H	2	$00FF_H$	Maximum C-APDU data size
NDEF-File_Ctrl_TLV	0007_H	8	04_H 06_H $E10410000000_H$	NDEF file (refer to Table 17)
Proprietary-File_Ctrl_TLV	$000F_H$	32	05_H 06_H $E1A104000000_H$ 05_H 06_H $E1A204000000_H$ 05_H 06_H $E1A304000000_H$ 05_H 06_H $E1A404000000_H$	Pre-initialized to contain 4 TLVs for the 4 proprietary files (refer to Table 18)
RFU	$002F_H$	17	00000000000000000000 00000000000000_H	0's

By default, the NDEF file and Proprietary files will be read and write accessible, additional FAP conditions will apply if defined in the EF.FAP file.

When the FAP for the NDEF file is updated in the EF.FAP, the NFC read and write access setting will be updated in the NDEF-File_CTRL_TLV field of the EF.CC automatically. The NFC read and write settings of the NDEF file will be updated in the EF.CC file as listed in Table 17.

Table 17 NDEF-File_Ctrl_TLV

Tag	Length	Size (bytes)	Description/Value	Presence
04_H	06_H		NDEF-File_Ctrl_TLV	
		02_H	NDEF FileID Value = $E104_H$	Mandatory
		02_H	NDEF file size Value = 1000_H	Mandatory
		01_H	NDEF file READ access condition: According to [7], based on FAP for NFC access (refer to Table 19)	Mandatory
		01_H	NDEF file WRITE access condition: According to [7], based on FAP for NFC access (refer to Table 20)	Mandatory

When the FAP for Proprietary files is updated in the EF.FAP, the NFC read and write access setting will not be updated in the Proprietary-File_CTRL_TLV field of the EF.CC file by the applet. An explicit update is required to reflect the access conditions listed in Table 19 and Table 20 in the EF.CC file for Proprietary files, as Proprietary files must be accessible according to the FAP regardless of whether there are any corresponding Proprietary-File_Ctrl_TLV structures in the EF.CC file.

The NFC read and write policy of the Proprietary files will be updated in the EF.CC file as listed in Table 18.

Table 18 Proprietary-File_Ctrl_TLV

Tag	Length	Size (bytes)	Description/Value	Presence
05_H	06_H		Proprietary-File_Ctrl_TLV	
		02_H	Proprietary FileID Value = $E1A1_H$ I $E1A2_H$ I $E1A3_H$ I $E1A4_H$	Mandatory
		02_H	Proprietary file size Value = 0400_H	Mandatory
		01_H	Proprietary file READ access condition: According to [7], based on FAP for NFC access (refer to Table 19)	Mandatory
		01_H	Proprietary file WRITE access condition: According to [7], based on FAP for NFC access (refer to Table 20)	Mandatory

Table 19 lists the READ access condition values for the NDEF file and the Proprietary files.

Table 19 File READ access condition

Value	Description
00_H	READ access granted without any security
FF_H	No READ access granted
80_H	Limited READ Access

Table 20 lists the WRITE access condition values for the NDEF file and the Proprietary files.

Table 20 File WRITE access condition

Value	Description
00_H	WRITE access granted without any security
FF_H	No WRITE access granted
80_H	Limited WRITE access

5.2.5.2 NDEF file

The OPTIGA™ Authenticate NBT comes with a 4096 bytes NDEF file with FileID $E104_H$.
The applet will not perform any checks based on NLEN fields. For more information on NLEN, refer to [7].

5.2.5.3 Proprietary files

The OPTIGA™ Authenticate NBT comes with four proprietary files of 1024 bytes each. These files are referenced with the FileIDs $E1A1_H$, $E1A2_H$, $E1A3_H$, and $E1A4_H$. The contents of these files are transparent to the applet.
No checks are performed on the file content based on PLEN fields. For more information on PLEN, refer to [7].

5.2.5.4 File access policy file

The EF.FAP file is a binary file, which contains the settings to manage the access to all files within the Type 4 Tag application on the OPTIGA™ Authenticate NBT. The content of the EF.FAP file can be read with the READ BINARY command similar to any other binary file. Table 21 provides the data structure within the EF.FAP used to manage the access to a single application file. The EF.FAP contains entries for every application file.

Table 21 Access policy

Offset	Size	Field
0000_H	02_H	FileID
0002_H	01_H	Configuration byte for I2C read
0003_H	01_H	Configuration byte for I2C write
0004_H	01_H	Configuration byte for NFC read
0005_H	01_H	Configuration byte for NFC write

The Configuration byte defines the access condition. Additionally it contains a reference to the password by a Password ID. If a password protection is configured, then the password needs to be verified during file selection.

Table 22 Configuration byte

b[8]	b[7]	b[6]	b[5:1]	Description
0_B	0_B	RFU	NA	Operation NEVER allowed
0_B	1_B	RFU	NA	Operation ALWAYS allowed
1_B	0_B	RFU	Password ID	Operation password protected

***Note**: For NEVER and ALWAYS condition, the applet will completely ignore the b[6:1] bits. The Type 4 Tag applet will ignore the RFU bit.*

The content of the EF.FAP file defining the file access policy for all application files is shown in Table 23.

Table 23 EF.FAP content

FileID	I2C read	I2C write	NFC read	NFC write	Description
$E103_H$	40_H	00_H	40_H	00_H	EF.CC
$E104_H$	40_H	40_H	40_H	40_H	NDEF file
$E1A1_H$	40_H	40_H	40_H	40_H	Proprietary File 1
$E1A2_H$	40_H	40_H	40_H	40_H	Proprietary File 2
$E1A3_H$	40_H	40_H	40_H	40_H	Proprietary File 3
$E1A4_H$	40_H	40_H	40_H	40_H	Proprietary File 4
$E1AF_H$	40_H	40_H	40_H	40_H	EF.FAP

***Note**: Write to EF.CC file is set to "NEVER by default".*

The update of the EF.FAP data is done with the UPDATE BINARY command. This command will be processed as described in Chapter 5.4.3.

In order to enable password protection for the EF.FAP file the personalizer must create an appropriate password. This password is also known as the Master password. When this Master password is created, the write access policy of the EF.FAP file itself can be updated. Otherwise, the creation of a Master password using the CREATE PASSWORD command at a later point in time is not possible.

Additionally, the personalizer must update the EF.FAP file after deleting a password as the Type 4 Tag applet will not process the EF.FAP if the password is deleted.

***Note**: It is the responsibility of the personalizer to encode the FAP correctly and to validate the access policy in the EF.FAP file during the personalization.*

***Note**: The Master password is the password used to protect the update operation of the EF.FAP file respective of I2C and NFC interface.*

5.2.5.5 Password management

Password management is a mechanism that allows to create, verify, change, unblock, and delete passwords that are used to protect file operations.

5.2.5.5.1 Password verification

The password verification is triggered by adding the configured password value as parameter to the SELECT file command. A Password Response data is configured for each password during password creation. The response to the SELECT file command will contain the configured Password Response data to indicate a successful password verification.

In case the password verification fails, the SELECT file response data contains random data.

***Note**: Refer to Table 33 for password response data in case of successful password verification.*

5.2.5.5.2 UNBLOCK PASSWORD

The Type 4 Tag applet supports to unblock passwords by the CHANGE/UNBLOCK PASSWORD command sent with P2=00_H (see CHANGE/UNBLOCK PASSWORD). The command will not be executed if the password is already in the BLOCKED state.

If the EF.FAP file update operation is password protected, the Master password is required to unblock. If the Master password is blocked, all password management commands are blocked from execution.

5.2.5.5.3 CHANGE PASSWORD

The Type 4 Tag applet supports to change passwords by the CHANGE/UNBLOCK PASSWORD command sent with P2=01_H (see CHANGE/UNBLOCK PASSWORD). The command will not be executed if the password is already in the BLOCKED state.

If the EF.FAP file update operation is password protected, the Master password is required to change the password.

5.2.5.5.4 CREATE PASSWORD

The Type 4 Tag applet enables the creation of new passwords.

If the EF.FAP file update operation is password-protected, the Master password is required to create a password.

5.2.5.5.5 DELETE PASSWORD

The Type 4 Tag applet supports to delete existing passwords.

If the EF.FAP file update operation is password-protected, the Master password is required to delete a password.

5.2.6 Use cases operation

This section describes the operation of four primary product use cases in detail.

5.2.6.1 Asynchronous data transfer

The OPTIGA™ Authenticate NBT implements data exchange in asynchronous data transfer mode via "mailboxes". These mailbox files are part of the NFC Type 4 Tag application and can be accessed through the I2C and NFC interfaces. Depending on the needs of the application, the NFC reader or host system serves

as the initiator. They can write data to or read data from the NDEF message or one (or more) of the proprietary files.

5.2.6.2 Synchronous pass-through communication

The OPTIGA™ Authenticate NBT supports synchronous pass-through (PT) communication, where the device bridges data received from the NFC interface (Initiator) to the I2C interface connected to the host system (Responder). The device notifies the host system about the availability of data via its IRQ after receiving the NFC command data. The host system (as I2C controller) actively obtains the Initiators command, executes the operation, prepares a response, and sends the response back to the device. The device returns the response data to the Initiator without evaluating the content.

Figure 20 illustrates the NFC-to-I2C synchronous pass-through communication (PT) mode.

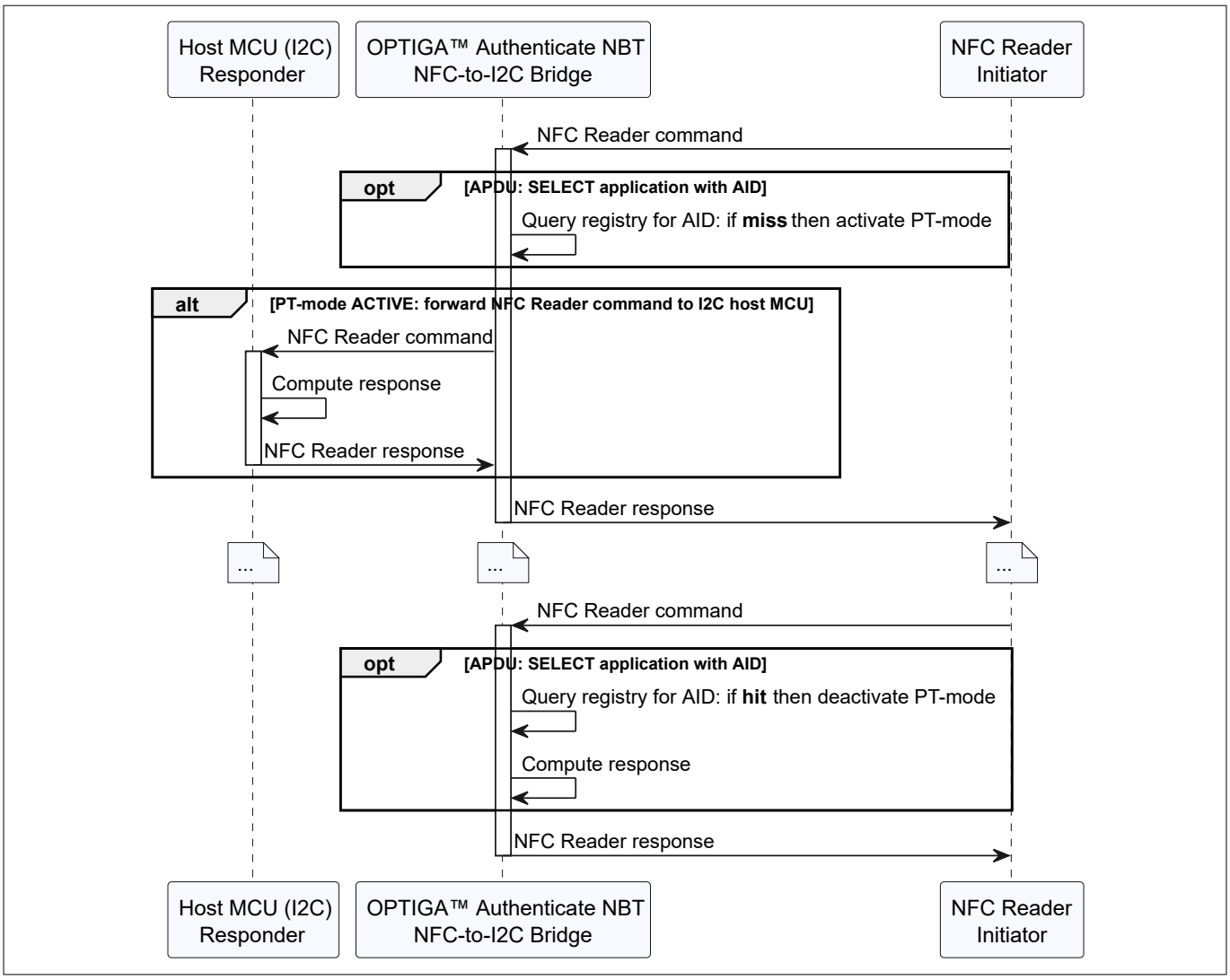


Figure 20 NFC-to-I2C pass-through (PT) communication mode

The PT communication mode is enabled by configuring the IRQ function of the OPTIGA™ Authenticate NBT to PT-IRQ. The IRQ then signals the availability of data on the I2C interface. Additionally, the IRQ is used in PT communication mode for PT-IRQ signaling and the data ready indication as I2C-IRQ.

For this reason, the I2C controller (host) must maintain a record to differentiate between:

- I2C-IRQ, if an I2C message (waiting for the device data ready signal) is previously sent by the host
- PT-IRQ, otherwise

Once the PT communication mode is enabled, a SELECT command with an unregistered Application Identifier (AID) from the NFC interface activates the PT communication mode on the OPTIGA™ Authenticate NBT.[4)] Henceforth, all commands will be transmitted to the host MCU via the I2C interface.

The host MCU must be ready to process the forwarded data while the PT communication mode is ACTIVE.

The IRQ pin is used to signal when PT data is ready. The I2C host needs to employ the following two commands to retrieve data from and transmit response data to the NFC reader, respectively:

- PASS-THROUGH FETCH DATA
- PASS-THROUGH PUT RESPONSE

Figure 21 depicts the NFC-to-I2C pass-through standard case communication flow.

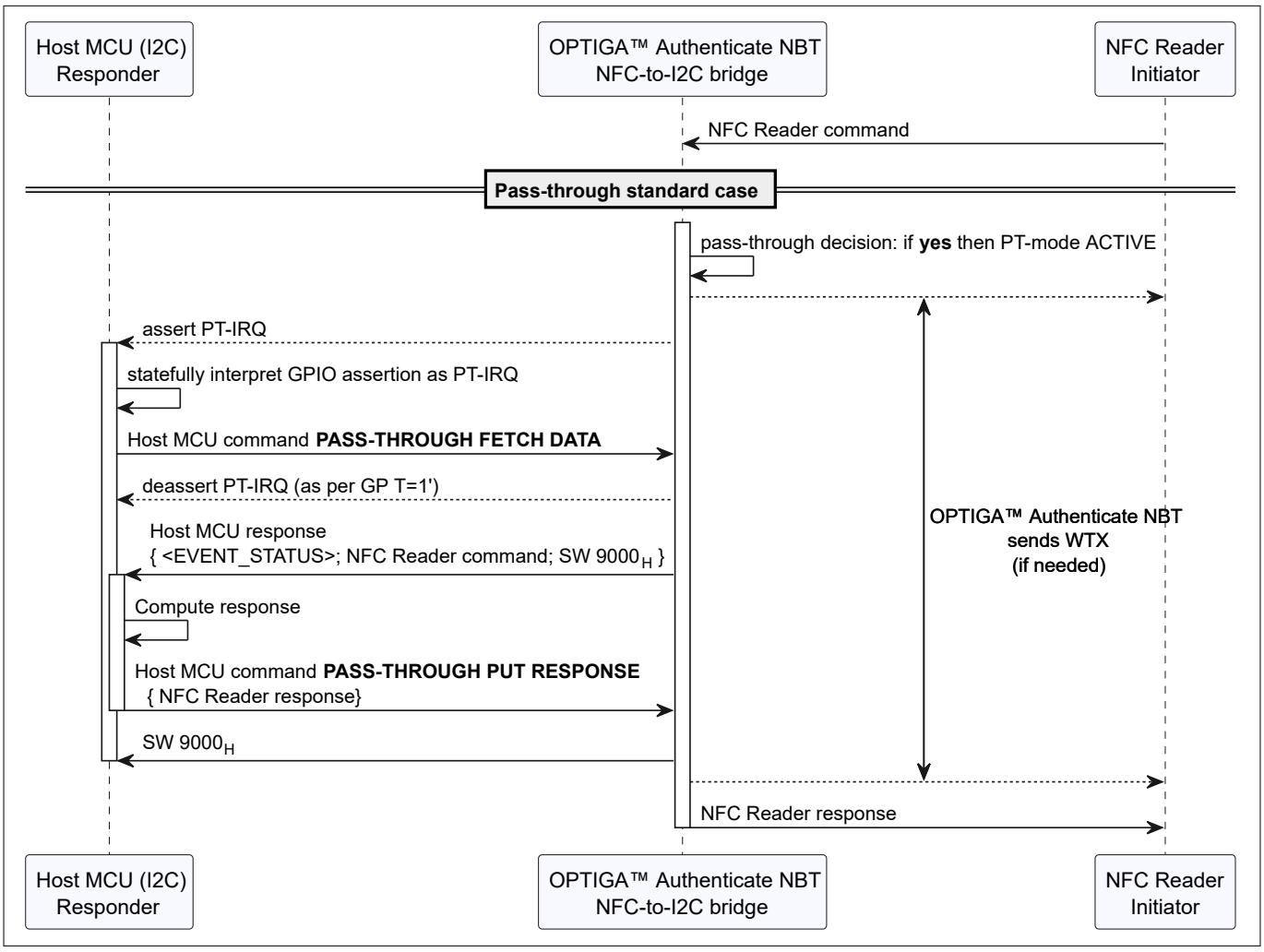


Figure 21 NFC-to-I2C pass-through standard case communication flow

The active PT communication mode session can be terminated by either selecting a registered application on the OPTIGA™ Authenticate NBT (Type 4 Tag or CONFIGURATOR) or by removing the device from the NFC reader field.

5.2.6.3 Brand protection with offline authentication

End customers who want to validate the authenticity of a product can tap the OPTIGA™ Authenticate NBT-equipped NFC tag attached to the product with any off-the-shelf NFC enabled mobile phone executing the brand's product authentication application. The mobile application retrieves the public-key certificate from the NDEF message in the device and validates it by utilizing the application's Root CA. Furthermore, the brand protection application may visually notify the end user of the result of the authentication process.

4 Logical channels are not supported.

The application performs the following tasks:

- Reading the NDEF file that contains the public-key certificate
- Validating the public-key certificate with a root public key or root CA certificate from the mobile application
- Performing challenge-response authentication using the private signing key (BSK) of the tag

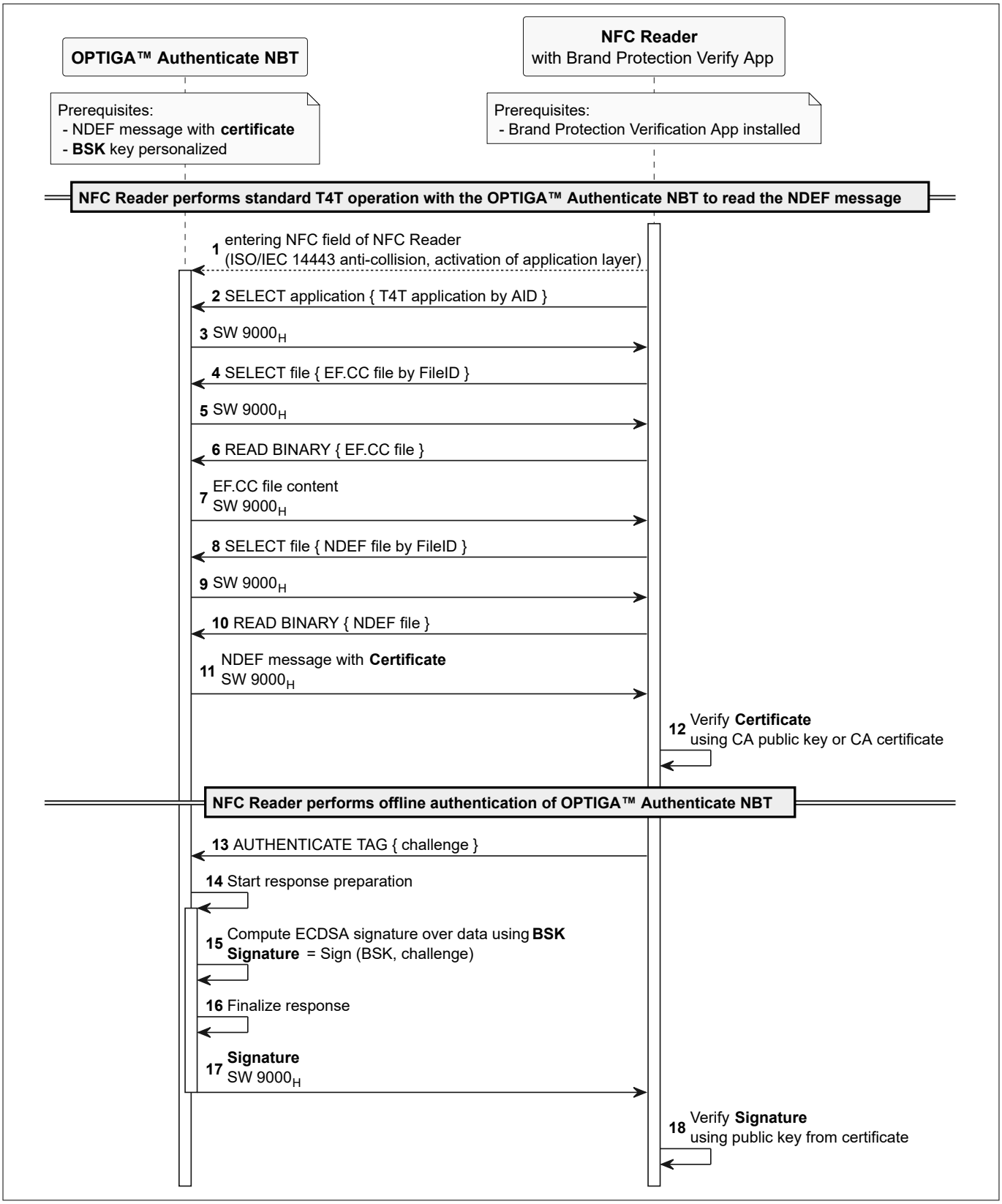


Figure 22 Brand protection with offline authentication

5.2.6.4 Brand protection with online authentication using COTT

Another option for verifying the authenticity of a product carrying an OPTIGA™ Authenticate NBT is brand verification with online authentication using a Cryptographic One-Time Token (COTT). This method involves verifying the authenticity of a product by connecting to the brand's cloud service. This service is accessible through the web browser of an NFC-enabled mobile phone.

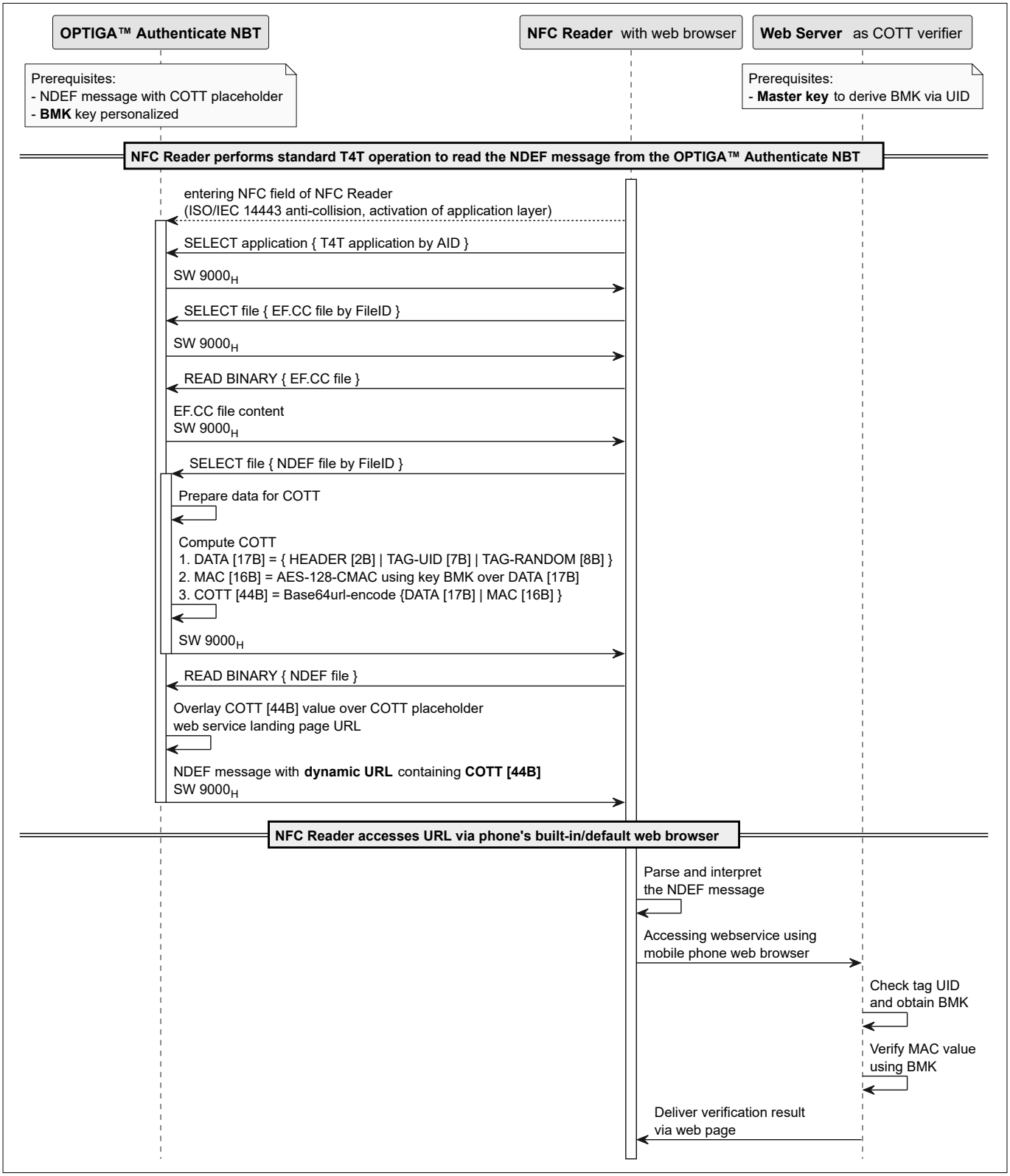
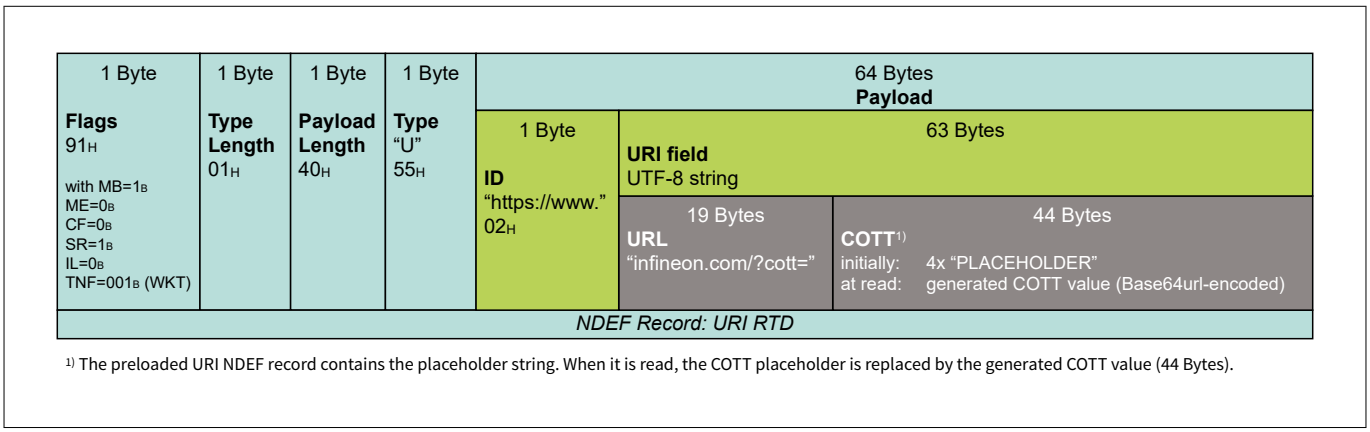


Figure 23 Brand protection with online authentication using COTT

Customers who want to validate the authenticity of a product can read the NFC tag/sticker on the product using any off-the-shelf NFC-enabled mobile device. When tapping the tag/sticker with an NFC-enabled mobile phone detects the NFC Type 4 Tag application and starts reading the contents.

Internally, the applet computes a 16-Byte MAC using the BMK from the OPTIGA™ Authenticate NBT secure key store using a two-byte header, the TAG-UID and a TAG-RANDOM as input data. Then the applet generates a dynamic URL by appending the base64url-encoded COTT value, and returns it as a response.



1) The preloaded URI NDEF record contains the placeholder string. When it is read, the COTT placeholder is replaced by the generated COTT value (44 Bytes).

Figure 24 NFC well-known record type

The mobile application detects the URL in the NDEF message and opens the link in one of the available browsers on the mobile phone. This URL is pointing to landing page of a authentication web service and contains the generated COTT value. Based on the COTT value the verification can be executed. The result is returned to the phone and displayed on a web page.

5.3 Product delivery condition and application configuration

The delivery condition of the OPTIGA™ Authenticate NBT is explained in the subsequent section.

5.3.1 Default product configuration

Table 24 summarizes the product configuration at delivery.

Table 24 Product configuration at delivery

Tag	Default value	Description
$C020_H$	$4E42542032303030000000000000000_H$	Product short name: "NBT2000"
$C021_H$	$5AA5_H$	Product life cycle state: PERSONALIZATION
$C030_H$	01_H	IRQ function: Disabled
$C031_H$	02_H	IRQ assert level: High level active
$C032_H$	01_H	IRQ output type: Push-pull
$C033_H$	01_H	IRQ pull type: No pull
$C034_H$	01_H	NFC IRQ event type: RF field on
$C040_H$	$01F4_H$	I2C idle timeout: 500 ms
$C041_H$	02_H	I2C drive strength: Strong
$C042_H$	02_H	I2C speed: 1000 kHz
$C043_H$	18_H	I2C target address: 18_H

(table continues...)

Table 24 (continued) Product configuration at delivery

Tag	Default value	Description
$C050_H$	$0C787770024E4254323030300000_H$	ATS according to ISO/IEC 14443 Type A for the OPTIGA™ Authenticate NBT containing the short version of the product's sales code ("NBT2000")
$C051_H$	01_H	NFC WTX mode: Multiplier equals to 1
$C052_H$	$4001\ldots_H$	NFC RF hardware configuration (312 bytes)
$C053_H$	00_H	NFC UID type for anti-collision: Unique, device specific 7-byte NFC UID
$C060_H$	11_H	Communication interface enable: NFC enabled | I2C enabled
$C061_H$	01_H	No current limitation
$C062_H$	06_H	Current limitation configuration

Refer to Table 15 for more information and possible values.

5.3.2 Default NFC tag application configuration

Table 25 summarizes the default configuration of the NFC tag application on the OPTIGA™ Authenticate NBT.

Table 25 Default configuration NFC tag application

Element	Default content
EF.CC file	Refer to Table 16
NDEF file	NLEN: 0326_H An NDEF message with two NDEF records: • NDEF Record 1: NFC Forum well known type "U" (URL) - Payload length: 64 bytes - Payload protocol field: "https://www." - Payload URI field[1)]: infineon.com/#cott=AAGhoqOkpaanAacEB5sP-YFN53YCMxxZ8xewMzicEVg4 • NDEF Record 2: NFC Forum external type "infineon.com:nfc-bridge-tag.x509" - Payload length: 700 bytes - Payload: Chip-individual X.509 certificate for the NBT device, see Figure 26
Proprietary file #1	PLEN: 0000_H Content: empty
Proprietary file #2	PLEN: 0000_H Content: empty
Proprietary file #3	PLEN: 0000_H Content: empty
Proprietary file #4	PLEN: 0000_H Content: empty

(table continues...)

Table 25 (continued) Default configuration NFC tag application

Element	Default content
File access policy	Content (refer to Chapter 5.2.5.4 for interpretation): $E10340004000_H$ $E10440404040_H$ $E1A140404040_H$ $E1A240404040_H$ $E1A340404040_H$ $E1A440404040_H$ $E1AF40404040_H$

1) The payload URI field contains a randomly generated "COTT" value. The value displayed here is an example.

5.3.3 Default keys

Table 26 summarizes the Infineon-defined keys at delivery.

Table 26 Default keys

Key	Default value
BMK	Infineon-defined secret key for demonstration purposes, must be replaced by OEM
BSK	Chip-individual private key, generated by Infineon root CA

5.4 Command reference

The commands to personalize and to operate the OPTIGA™ Authenticate NBT are listed in Table 27. The subsequent sections contain more information about these commands and possible responses.

Table 27 Command overview

Command	CLA	INS	Description
SELECT	00_H	$A4_H$	Select applications/files
PERSONALIZE DATA	00_H	$E2_H$	Personalize data elements[1)]
READ BINARY	00_H	$B0_H$	Retrieve data from the selected file
AUTHENTICATE TAG	00_H	88_H	Generate a signature on the challenge sent by the host
UPDATE BINARY	00_H	$D6_H$	Update data of the selected file
CHANGE/UNBLOCK PASSWORD	00_H	24_H	Change or unblock a password
CREATE PASSWORD	00_H	$E1_H$	Create a password
DELETE PASSWORD	00_H	$E4_H$	Delete a password
GET DATA	00_H	30_H	Retrieve application-specific information
BACKEND TEST	00_H	BE_H	Perform test operations
SET CONFIGURATION	20_H	20_H	Update product configuration[2)]
GET CONFIGURATION	20_H	30_H	Retrieve product configuration

(table continues...)

Table 27 (continued) Command overview

Command	CLA	INS	Description
PASS-THROUGH FETCH DATA	38_H	CA_H	Retrieve the NFC commands over the I2C interface
PASS-THROUGH PUT RESPONSE	38_H	DA_H	Send the response via the I2C interface to be forwarded over the NFC interface

1) The execution of this commands is limited to the PERSONALIZATION state.
2) Changes of the chip configuration are only possible in PERSONALIZATION state.

5.4.1 SELECT

This command is used to select one of the following:

- Application instances based on their AIDs (Application IDentifiers), or
- User elementary files based on their FileIDs (File IDentifiers)

Furthermore, password verifications for the application files can be triggered by adding corresponding information to the command data field.

5.4.1.1 Command message

The SELECT application command APDU is encoded according to the tables below:

Table 28 SELECT application command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	$A4_H$	04_H	00_H	Refer to Table 29		00_H

The command data contains the AID of the applet to select an application:

Table 29 SELECT application data fields

Lc	Data	Application
07_H	D2 76 00 00 85 01 01_H	Type 4 Tag application
$0D_H$	D2 76 00 00 04 15 02 00 00 0B 00 01 01_H	CONFIGURATOR application
NN_H	Any other AID (length range: 5..16 bytes)	Pass-through (virtual application)

The SELECT file command APDU is encoded according to the tables below:

Table 30 SELECT file command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	$A4_H$	00_H	$0C_H$	02_H	FileID only	00_H / Absent
00_H	$A4_H$	00_H	$0C_H$	08_H	FileID followed by password value for either READ or WRITE operations	00_H / Absent
00_H	$A4_H$	00_H	$0C_H$	$0E_H$	FileID followed by password value for both READ and WRITE operations	00_H / Absent

The command data contains the FileID to select the file. Optionally, the command data may additionally contain the password value(s) embedded into TLV structures to perform password-protected READ or/and WRITE operations on the selected file. The TLV data fields are described in Table 31.

Table 31 SELECT file data fields

Tag	Length	Value
-	-	FileID
52_H	04_H	YYYYYYYY 32 bit Password for READ
54_H	04_H	ZZZZZZZZ 32 bit Password for WRITE

5.4.1.2 Response message

For the SELECT application operation, the response data field does not contain any data. The following status words may be responded after SELECT application command execution.

Table 32 SELECT application response status words

SW1	SW2	Description
67_H	00_H	Incorrect Lc value
$6A_H$	80_H	Incorrect parameters in the command data field
$6A_H$	82_H	File or application not found
90_H	00_H	Successful command execution

In case the SELECT file command is sent without any password value, the response data field does not contain any data.

In case the SELECT file command is sent including password verification data (for a READ and/or a WRITE operation), and the password verification is successful, then the response data field contains the configured Password Response value(s) for these operation(s). These Password Response value(s) are embedded in a File Control Information structure as shown in Table 33.

Table 33 File control parameter - SELECT file response data

Tag	Length	Value		Presence
$6F_H$	04_H or 08_H	File Control Information		Conditional
	02_H	52_H	Configured Password Response for a READ operation	Conditional
	02_H	54_H	Configured Password Response for a WRITE operation	Conditional

In case the password verification fails, the applet responds with the random number in the corresponding File Control Information field.

In case the password to be verified is blocked, the applet returns $FFFF_H$.

The following status words may be responded after SELECT file command execution.

Table 34 SELECT file response status word

SW1	SW2	Description
67_H	00_H	• Incorrect Lc value • If Le is other than 00_H
$6A_H$	82_H	File or application not found

(table continues...)

Table 34 (continued) SELECT file response status word

SW1	SW2	Description
$6A_H$	80_H	Wrong TLV data format for the SELECT file command including password data
90_H	00_H	Successful command execution

5.4.2 PERSONALIZE DATA

The PERSONALIZE DATA command is used to personalize the data elements of the applet.

5.4.2.1 Command message

The PERSONALIZE DATA command is encoded according to the tables below:

Table 35 PERSONALIZE DATA: Command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	$E2_H$	00_H	00_H	XX_H	Refer to Table 36	-

The parameters P1 and P2 are always fixed as 0000_H.

The data field of the command message must be encoded as <Data Group ID> <length> <data>. The supported DGI is listed in Table 36.

Table 36 Supported DGIs in PERSONALIZE DATA command

DGI	Length	Data
$A001_H$	10_H	AES-128-CMAC key for online brand protection (BMK)
$A002_H$	20_H	EC private key for offline brand protection (BSK)
$A003_H$	09_H	Password data set <Password ID (1 byte)> <Password data (4 bytes)> <Password response (2 bytes)> <Password limit (2 bytes)>
$E104_H$	Variable	NDEF file content <Offset (2 bytes)> <NDEF file content>
$E1A1_H$ $E1A2_H$ $E1A3_H$ $E1A4_H$	Variable	Proprietary file content <Offset (2 bytes)> <Proprietary file content>
$E1AF_H$	$2A_H$	FAP configuration data Set of "<FileID (2 bytes)> <Config byte for I2C read> <Config byte for I2C write> <Config byte for NFC read> <Config byte for NFC write>"
$BF63_H$	00_H	Special data object to indicate the end of personalization, also referred as FINALIZE PERSONALIZATION Data is absent

When updating the content of the NDEF file or the proprietary files, multiple PERSONALIZE DATA commands will be used. The personalization of an NDEF file must be limited to 4096 bytes. Similarly, for the proprietary

files, the personalization must be limited to 1024 bytes. It is the responsibility of the personalizer to use appropriate offset values when updating the file content.

The FAP configuration data will be written in a single PERSONALIZE DATA. The applet will reject the command if the length of update FAP is other than 42 bytes.

The password data sets have to configured with multiple PERSONALIZE DATA commands.

In addition to the above mentioned command handling, the Type 4 Tag application will evaluate the transferred data of the PERSONALIZE DATA command as follows:

- The contents of the NDEF file, the proprietary files, the symmetric AES-128-CMAC key, the asymmetric ECC key, the password data, and the FAP configuration data are not evaluated
- The length of the received DGI's is checked. For example: the length of a symmetric AES-128-CMAC key DGI should be 16 bytes. In case of a mismatch, the applet will not personalize the key
- Related to the password response data, 0000_H and $FFFF_H$are RFU values. Therefore, these cannot be used as password responses; the application will reject them

Constraints for password try limit and password ID is mentioned in Chapter 5.4.6.1.

5.4.2.2 Response message

For the PERSONALIZE DATA operation, the response data field does not contain any data. The following status words may be responded after command execution.

Table 37 Status words

SW1	SW2	Description
67_H	00_H	Wrong Length: • If Lc is 00_H
69_H	85_H	Use of condition not satisfied: • If during personalization of password, password ID already exists • If trying to personalize more than 28 passwords • If PERSONALIZE DATA command is sent in OPERATIONAL state
$6A_H$	80_H	Incorrect parameters in the command data field: • If FAP configuration data is other than 42 bytes • If length of the password data set is other than 9 bytes • AES-128-CMAC key length is other than 16 bytes • ECC key length is other than 32 bytes • NDEF/Proprietary EF personalization is out of file size • If Le is present • If additional data is present in command • If password response in password data set is 0000_H or $FFFF_H$
$6A_H$	86_H	Incorrect P1-P2: • If P1-P2 is other than 00_H
$6A_H$	88_H	Unknown or unsupported data group, data object
90_H	00_H	Successful command execution

5.4.3 UPDATE BINARY

The UPDATE BINARY command is used to update data of the currently selected file.

5.4.3.1 Command message

The UPDATE BINARY command APDU is encoded according to the table below:

Table 38 UPDATE BINARY command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	$D6_H$	Offset		XX_H	Data to be written	-

The parameters P1 and P2 represent the offset within the selected file where the data needs to be updated (start address). The data field can contain any data in hexadecimal string format based on the user's requirement.

In case the selected file is the EF.CC file, then the update of data from offset 02_H to $0E_H$ is not allowed.

If the current selected file is the EF.FAP file, then

- An offset other than 0000_H will be ignored
- The 6 bytes of data contain a FileID and its access policy as shown in Table 21. If the applied FileID does not match any of the valid supported files then a status word indicating an error is returned

5.4.3.2 Response message

For the UPDATE BINARY operation, the response data field does not contain any data. The following status words may be responded after command execution.

Table 39 UPDATE BINARY response status words

SW1	SW2	Description
67_H	00_H	• If Lc is coded on extended length • If Lc is 00_H that is no command data is present • If Le is present • Length of update EF.FAP file is other than 6 bytes • If the offset mentioned in P1-P2 in UPDATE BINARY command is greater than the file size
69_H	82_H	Security condition not satisfied • When authentication with respective password is not successful • When file is locked that is access policy is never for write
69_H	85_H	EF.CC file is updated for 02_H to $0E_H$ offset
69_H	86_H	Command not allowed (no current EF)
$6A_H$	80_H	Wrong data, invalid FileID or format mismatch in FAP policy
$6A_H$	86_H	Incorrect P1-P2 • If P1-P2 is greater than file size
90_H	00_H	Successful command execution

5.4.4 READ BINARY

The READ BINARY command is used to retrieve data from the currently selected file.

5.4.4.1 Command message

The READ BINARY command APDU is encoded according to the table below:

Table 40 READ BINARY command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	$B0_H$	Offset		-	-	XX_H

The parameters P1 and P2 represent the offset within the selected file from which the data is read.

5.4.4.2 Response message

The data field of the READ BINARY response message contains the data read from the selected file, starting at the requested offset. The following status words may be responded after command execution.

Table 41 Status words

SW1	SW2	Description
67_H	00_H	Wrong length • The offset in P1-P2 is greater than the file size • If Le is absent • If Le is coded on extended length
69_H	82_H	Security conditions not satisfied • When authentication with respective password is not fulfilled • When selected file is locked (access policy is set to NEVER for the READ operation)
69_H	86_H	Command not allowed (file is not selected)
$6C_H$	XX_H	Wrong Le, XX_H is the exact number of available data bytes • Offset + Le is greater than the file size
90_H	00_H	Successful command execution

5.4.5 AUTHENTICATE TAG

The AUTHENTICATE TAG command is used to generate a signature on the challenge sent by host, which can be used for offline brand protection use case.

5.4.5.1 Command message

The AUTHENTICATE TAG command APDU is encoded according to the table below:

Table 42 AUTHENTICATE TAG command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	88_H	00_H	00_H	XX_H	Challenge	00_H

The parameters P1 and P2 are always 0000_H.

The application will accept the challenge of 1-255 bytes. This will generate a signature using the personalized ECC private key (BSK) based on NIST P-256.

5.4.5.2 Response message

The data field of the AUTHENTICATE TAG response message contains the ECDSA signature computed using SHA-256. The resulting ECDSA signature[5)] is returned as an DER-encoded ASN.1 SEQUENCE of two ASN.1 INTEGERs (henceforth, the signature value starts with tag 30_H).

The following status words may be responded after command execution.

Table 43 Status words

SW1	SW2	Description
67_H	00_H	Wrong length • If challenge length is 00_H • If Lc is coded on extended length • If Le is 00_H
69_H	85_H	Conditions of use not satisfied • ECC private key not personalized
$6A_H$	86_H	Incorrect parameters P1-P2 • If P1-P2 is other than 00_H
90_H	00_H	Successful command execution

5.4.6 CREATE PASSWORD

The CREATE PASSWORD command is used to create a new password.

5.4.6.1 Command message

The CREATE PASSWORD command APDU is encoded according to the tables below:

Table 44 CREATE PASSWORD command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	$E1_H$	00_H	00_H	$09_H \| \| 0D_H$	New password data set	-

The parameters P1 and P2 are always fixed as 0000_H.

The command data field contains context-specific data based on command length (Lc). The command data field is summarized in Table 45.

Table 45 CREATE PASSWORD command data field

Lc	Data Field
09_H	<New Password ID (1 byte)> <New Password (4 bytes)> <Password Response (2 bytes)> <Password Try Limit (2 bytes)>
$0D_H$	<Master password (4 bytes)> || <New Password ID (1 bytes)> <Password (4 bytes)> <Password Response (2 bytes)> <Password Try Limit (2 bytes)>

The settings of the file access policy for the EF.FAP must be considered when creating a new password. In case the EF.FAP file itself is password protected (Master password) then an authentication with this Master password must be performed in order to enable successful password creation.

5 An ECDSA signature contains two components, the numbers 'r' and 's' [26].

The following command data field combinations are possible:

- If the EF.FAP file update policy is ALWAYS, then no authentication is needed to create a new password
  - Lc field will be 09_H
  - Data field contains {Password ID || New Password || Password Response || Password Try Limit}
- If the EF.FAP file update policy is PASSWORD protected, then the Master password must be present in the command data
  - Lc field will be $0D_H$
  - Data field contains {Master password || New Password ID || New Password || Password Response || Password Try Limit}

The following constraints need to be considered for the Password Try Limit and the Password ID:

- Password ID is in the range of 01_H to $1F_H$
- Maximum number of passwords can be $1C_H$
- Password Try Limit is in the range of 0001_H to $007F_H$
  - It is recommended to set the Password Try Limit in the range of 0003_H to $007F_H$ for password checks performed for read/write operations
- If Password Try Limit is set as $FFFF_H$, the applet will treat this as an infinite try limit. In this case, password will never be blocked

***Note**: The applet will ignore bits b[6] to b[8] from Password ID.*

5.4.6.2 Response message

For the CREATE PASSWORD operation, the response data field does not contain any data. The following status words may be responded after command execution.

Table 46 Status words

SW1	SW2	Description
67_H	00_H	Wrong length • If Lc is other than 09_H and $0D_H$ bytes • If Le is present
69_H	82_H	Security status not satisfied • If EF.FAP Master password is applied for the FAP update and password is not verified successfully
69_H	85_H	Conditions of use not satisfied • Password ID already present • If trying to personalize more than 28 passwords
$6A_H$	80_H	Incorrect Data • Password Response is 0000_H and $FFFF_H$ • Password ID is 00_H • Password Try Limit value is 0000_H or 0080_H to $FFFE_H$
$6A_H$	86_H	Incorrect parameters P1-P2 • If P1-P2 is other than 00_H
90_H	00_H	Successful command execution

5.4.7 DELETE PASSWORD

The DELETE PASSWORD command is used to delete passwords.

5.4.7.1 Command message

The DELETE PASSWORD command APDU is encoded according to the tables below:

Table 47 DELETE PASSWORD command

CLA	INS	P1	P2	Lc	Data	Le
00_H	$E4_H$	00_H	XX_H	$00_H \| \| 04_H$	Table 49	-

The parameter P1 is always fixed as 00_H.

The parameter P2 contains the reference ID of the password to be deleted as defined in Table 48.

Table 48 Reference control parameter – P2

b[8]	b[7]	b[6]	b[5]	b[4]	b[3]	b[2]	b[1]	Meaning
0	0	0	-	-	-	-	-	RFU
-	-	-	x	x	x	x	x	Password ID to be deleted

***Note**: The applet will ignore the RFU bits.*

The command data field contains context-specific data based on command length (Lc). The command data field is summarized in Table 49.

Table 49 DELETE PASSWORD command data field

Lc	Data Field
00_H	-
04_H	Master password

The settings of the file access policy for the EF.FAP must be considered when deleting a password. In case the EF.FAP file itself is password protected (Master password) then an authentication with this Master password must be performed in order to enable successful password creation.

Following command data field combinations are possible:

- If the EF.FAP file update policy is ALWAYS, then no authentication is needed to delete the password
  - Lc field will be 00_H
  - Data field will be absent
- If the EF.FAP file update policy is PASSWORD protected, then the Master password must be present in the command data
  - Lc field will be 04_H
  - Data field contains the Master password

***Note**: If the Master password is deleted, then operations protected with this Master password will not be executed.*

5.4.7.2 Response message

For the DELETE PASSWORD operation, the response data field does not contain any data. The following status words may be responded after command execution.

Table 50 Status words

SW1	SW2	Description
67_H	00_H	Wrong length • If Lc is other than 00_H or 04_H • If Le is present
69_H	82_H	Security status not satisfied • If access condition applied for the FAP update is NEVER • If EF.FAP Master password is applied for the FAP update and password is not verified successfully
$6A_H$	86_H	Incorrect P1-P2 • If P1 is other than 00_H
$6A_H$	88_H	Reference data not found • Password ID not present
90_H	00_H	Successful command execution

5.4.8 CHANGE/UNBLOCK PASSWORD

The CHANGE/UNBLOCK PASSWORD command is used to change or to unblock passwords.

5.4.8.1 Command message

The CHANGE/UNBLOCK command APDU is encoded according to the tables below:

Table 51 CHANGE/UNBLOCK PASSWORD command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	24_H	00_H	XX_H	$00_H \| \| 04_H \| \| 08_H$	Table 54	-

The parameter P1 is always fixed as 00_H.

The parameter P2 indicates whether to unblock or change the password. Additionally, it contains the reference ID of the password to be changed or blocked as defined in Table 52.

Table 52 Reference control parameter – P2

b[8]	b[7]	b[6]	b[5]	b[4]	b[3]	b[2]	b[1]	Meaning
x	x	RFU	-	-	-	-	-	Refer to Table 53
-	-	-	x	x	x	x	x	Reference ID of password to be changed or unblock

***Note**: The applet will ignore the RFU bit.*

Table 53 Coding of CHANGE/UNBLOCK password options

P2.b[8]	P2.b[7]	Value
0_B	0_B	UNBLOCK password
0_B	1_B	CHANGE password

The settings of the file access policy for the EF.FAP must be considered when changing or unblocking a password. In case the EF.FAP file itself is password protected (Master password) then an authentication with this Master password must be performed in order to enable successful execution of the CHANGE/UNBLOCK PASSWORD command.

The data field of the command message contains context-specific data based on parameter P2. The command data field is summarized in Table 54.

Table 54 CHANGE/UNBLOCK PASSWORD command data field

P2.b[8]	P2.b[7]	Data field
0	0	No data Master password
0	1	New password data Master password | New password data

Following data field combinations are possible:

- If the EF.FAP file update policy is ALWAYS, then no authentication is needed to change or unblock the password
  - In the case of UNBLOCK password, the Lc field will be 00_H and the data field will be absent
  - In the case of CHANGE password, the Lc field will be 04_H and the data field will contain the four bytes of the new password
- If the EF.FAP file update policy is PASSWORD protected, then the Master password must be present in the command data
  - In the case of UNBLOCK password, the Lc field will be 04_H and the data field will contain the four bytes of Master password
  - In the case of CHANGE password, the Lc field will be 08_H and the data field will contain the four bytes of the Master password and the four bytes of the new password

The new password must be applied in the next file selection.

5.4.8.2 Response message

For the CHANGE/UNBLOCK PASSWORD operation, the response does not contain any data. The following status words may be responded after command execution.

Table 55 Status words

SW1	SW2	Description
67_H	00_H	Wrong length • If Lc is other than 00_H and 04_H in case of the UNBLOCK PASSWORD command • If Lc is other than 04_H and 08_H in case of the CHANGE PASSWORD command

(table continues...)

Table 55 (continued) Status words

SW1	SW2	Description
69_H	85_H	Conditions of use not satisfied • If the EF.FAP Master password is applied for the FAP update and the Master password is not personalized • If the EF.FAP Master password is blocked • If requested password is blocked in case of CHANGE PASSWORD command
$6A_H$	86_H	Incorrect P1-P2 • If P1 is other than 00_H • If P2's b[8]-b[7] are other than 00_B and 01_B
$6A_H$	88_H	Reference of data not found • Password ID not valid
90_H	00_H	Successful command execution

5.4.9 GET DATA

The GET DATA command is used to retrieve applet-specific information.

5.4.9.1 Command message

The GET DATA command APDU is encoded according to the table below:

Table 56 GET DATA command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	30_H	Refer to Table 57		-	-	00_H

Table 57 Reference control parameter

P1-P2	Meaning
$DF3A_H$	Applet version

5.4.9.2 Response message

The GET DATA operation will respond the File Control Information after selecting the Type 4 Tag application.

Table 58 File Control Parameter – NFC Applet version

Tag	Length	Value	
$6F_H$	07_H	File Control Information	
	04_H	$DF3A_H$	Applet Version (Major('01').Minor('01').BuildNumber('02'))

The following status words may be responded after command execution.

Table 59 Status words

SW1	SW1	Description
67_H	00_H	Wrong length • If Lc is present • If Le not equal to 00_H
$6A_H$	86_H	Wrong P1-P2 • If P1-P2 is other than $DF3A_H$
90_H	00_H	Successful command execution

5.4.10 BACKEND TEST

The BACKEND TEST command performs test operations which can be, for example, used for incoming goods inspection. The command is restricted to the PERSONALIZATION state and can only be executed via the I2C interface.

5.4.10.1 Command message

The BACKEND TEST command APDU is encoded according to the table below:

Table 60 BACKEND TEST command APDU

CLA	INS	P1	P2	Lc	Data	Le
00_H	BE_H	Refer to Table 61		-	-	-

The reference control parameter defines the usage of this command as follows:

Table 61 Command instruction parameters BACKEND TEST command APDU

P1	P2	Operation
00_H	XX_H	Perform BACKEND TEST operations as specified by P2 as shown in Table 62
FF_H	00_H	Disable BACKEND TEST command permanently

The following test operations can be performed.

Table 62 P2 command instruction parameter for BACKEND TEST command APDU

b[8]	b[7]	b[6]	b[5]	b[4]	b[3]	b[2]	b[1]	Description
							1_B	Generate random number
						1_B		Compute ECDSA signature
					1_B			Extract public key from certificate
				1_B				Verify ECDSA signature
			1_B					Extract UID from certificate
		1_B						Compare UID (compares the UID from the certificate versus the UID used by the NFC interface)
	1_B							Compute COTT
0_B								RFU

To trigger all available tests, the P2 command instruction parameter must be set to $7F_H$. The OPTIGA™ Authenticate NBT may also execute individual tests using a respective command instruction parameter P2 setting. Certain operations implicitly require the successful execution of other dependent tests:

- "Compute ECDSA signature" requires the successful generation of random number
- "Verify ECDSA signature" requires both the successful computation of an ECDSA signature and the successful extraction of the public key form the certificate
- "Compare UID" requires the successful extraction of the UID from the certificate

***Note**: The BACKEND TEST command can only be applied to the OPTIGA™ Authenticate NBT containing the production-default keys and certificates. Therefore, the command MUST be performed before any product personalization, otherwise the test may fail since the device may already contain customer-specific keys or certificates.*

5.4.10.2 Response message

For the BACKEND TEST operation, the response data field contains a bit mask. Successfully executed tests are indicated by corresponding bits set to 1_B (refer to Table 62). If all requested tests are performed successfully, the bit mask in the response message equals the P2 command instruction parameter.

The following status words may be responded after command execution.

Table 63 Status words

SW1	SW2	Description
69_H	85_H	Conditions of use not satisfied: • If the BACKEND TEST command is disabled previously • If the BACKEND TEST command is not received over the I2C interface • If the OPTIGA™ Authenticate NBT is not in the PERSONALIZATION state
$6A_H$	86_H	Incorrect P1-P2: • If P1 is FF_H and P2 is not 00_H
90_H	00_H	Successful command execution

5.4.11 SET CONFIGURATION

The SET CONFIGURATION command is used to adjust hardware-related configurations on the OPTIGA™ Authenticate NBT and to lock these configurations by setting product life cycle to OPERATIONAL state.

5.4.11.1 Command message

The SET CONFIGURATION command APDU is encoded according to the table below:

Table 64 SET CONFIGURATION command

CLA	INS	P1	P2	Lc	Data	Le
20_H	20_H	00_H	00_H	Length of configuration data	Configuration data	-

The parameters P1 and P2 are always 0000_H.

The *Configuration data* is of SIMPLE-TLV format according to ISO/IEC 7816-4 [6].

Table 65 Configuration data TLV structure

Configuration Tag	Configuration Length	Configuration Value
$TTTT_H$	LL_H	VV_H data bytes according to LL_H

Refer to Table 15 for configuration tag, length and value settings.

5.4.11.2 Response message

For the SET CONFIGURATION operation, the response data field does not contain any data. The following status words may be responded after command execution.

Table 66 Status words

SW1	SW2	Description
67_H	00_H	Incorrect Lc value
69_H	85_H	Conditions of use not satisfied
$6A_H$	80_H	Incorrect parameters in the command data field
$6A_H$	86_H	Incorrect P1, P2
$6D_H$	00_H	INS value not supported
$6E_H$	00_H	CLA value not supported
90_H	00_H	Successful command execution

5.4.12 GET CONFIGURATION

The GET CONFIGURATION command is used to obtain information about a specific product configuration.

5.4.12.1 Command message

The GET CONFIGURATION command APDU is encoded according to the table below:

Table 67 GET CONFIGURATION command

CLA	INS	P1	P2	Lc	Data	Le
20_H	30_H	00_H	00_H	02_H	Configuration data tag	-

To obtain a specific configuration value, the "configuration data tag" must be set according to Table 15.

5.4.12.2 Response message

The data field of the GET CONFIGURATION response message is a SIMPLE-TLV format according to ISO/IEC 7816-4, see Table 65. Table 15 provides a list of parameters and possible values and more details about the configuration Tag, Length and Value meanings.

The following status words may be responded after command execution.

Table 68 Status words

SW1	SW2	Description
67_H	00_H	Incorrect Lc value
69_H	85_H	Conditions of use not satisfied
$6A_H$	80_H	Incorrect parameters in the command data field
$6A_H$	86_H	Incorrect P1, P2

(table continues...)

Table 68 (continued) Status words

SW1	SW2	Description
$6D_H$	00_H	INS value not supported
$6E_H$	00_H	CLA value not supported
90_H	00_H	Successful command execution

5.4.13 PASS-THROUGH FETCH DATA

The PASS-THROUGH FETCH DATA command can be used in NFC-I2C pass-through communication mode to retrieve the NFC interface-specific status information concatenated with the NFC received ADPU over the I2C interface.

When the NFC-I2C pass-through communication mode is not active or the NFC APDU is received, only the NFC interface-specific status information is returned.

***Note**: This command is only applicable to the I2C communication interface.*

5.4.13.1 Command message

The PASS-THROUGH FETCH DATA command APDU is encoded according to the table below:

Table 69 PASS-THROUGH FETCH DATA command

CLA	INS	P1	P2	Lc	Data	Le
38_H	CA_H	00_H	00_H	-	-	-

5.4.13.2 Response message

The data field of the PASS-THROUGH FETCH DATA response message contains the pass-through status word concatenated with the complete APDU received over the NFC interface.

Table 70 PASS-THROUGH FETCH DATA response structure

PT-SW1	PT-SW2	NFC ADPU	SW1	SW2
XX_H	XX_H	NFC APDU	XX_H	XX_H

The NFC APDU can have a total maximal length of 261 bytes.

The total maximal length of the response is 265 bytes. This length is indicated according the GP T=1' protocol.

Table 71 Pass-through status word first byte (PT-SW1)

b[7]	b[6]	b[5]	b[4]	b[3]	b[2]	b[1]	b[0]	Description
x_B	x_B	x_B	x_B	x_B	x_B	x_B	x_B	RFU

Table 72 Pass-through status word second byte (PT-SW2)

b[7]	b[6]	b[5]	b[4]	b[3]	b[2]	b[1]	b[0]	Description
x_B								RFU
	1_B							Indicates a STATE_L4 exit since last status bit field retrieval by host
	0_B							No change
		1_B						Indicates a STATE_L4 entry since last status bit field retrieval by host

(table continues...)

Table 72 (continued) Pass-through status word second byte (PT-SW2)

b[7]	b[6]	b[5]	b[4]	b[3]	b[2]	b[1]	b[0]	Description
		0_B						No change
			1_B					Indicates a STATE_FIELD exit since last status bit field retrieval by host
			0_B					No change
				1_B				Indicates a STATE_L4 entry since last status bit field retrieval by host
				0_B				No change
					1_B			Pass-through APDU is available
					0_B			No pass-through APDU available
						1_B		Layer 4 is active
						0_B		Layer 4 is not active
							1_B	NFC field is present
							0_B	NFC field is off

Following status words may be responded after command execution.

Table 73 Status words

SW1	SW2	Description
68_H	00_H	CLA not supported
69_H	85_H	Condition not satisfied
90_H	00_H	Successful execution

5.4.14 PASS-THROUGH PUT RESPONSE

The PASS-THROUGH PUT RESPONSE command can be used in NFC-I2C pass-through communication mode to send the response to the fetched command (refer to Chapter 5.4.13) to be forwarded over the NFC interface.

This command is only applicable to the I2C communication interface. The command can only be executed after entering PT-Mode and executing the PASS-THROUGH FETCH DATA command. Otherwise, an exception is returned.

5.4.14.1 Command message

The PASS-THROUGH PUT RESPONSE command APDU is encoded according to the table below:

Table 74 PASS-THROUGH PUT RESPONSE command

CLA	INS	RFU	Lc1	Lc2	Data	Le
38_H	DA_H	00_H	XX_H	XX_H	Pass-through response data	-

The PASS-THROUGH PUT RESPONSE command uses a proprietary format. The payload data length is encoded in 2 bytes, Field Lc1 (byte 4) and Lc2 (byte 5) of the APDU header (big endian).

The response to be forwarded over the NFC communication, including the status words SW1 and SW2, must be included in the data section.

The data field must include at least the status word (2 bytes) that will be sent over the NFC interface. The maximum accepted payload size is 258 bytes.

Refer to Chapter 5.2.6.2 for more details.

5.4.14.2 Response message

The data field of the PASS-THROUGH PUT RESPONSE response message does not contain any data. The following status words may be responded after command execution.

Table 75 Status words

SW1	SW2	Description
68_H	00_H	CLA not supported
69_H	85_H	Condition not satisfied
69_H	$A1_H$	Pass-through not available
69_H	$A2_H$	Wrong sequence
90_H	00_H	Successful command execution

5.5 Host software

As illustrated in Figure 25, a typical system utilizing the OPTIGA™ Authenticate NBT, and a host microcontroller. From the perspective of the device, it is important to differentiate between on-chip software and off-chip software, as indicated.

- **On-chip software:** Describes the application operating on the OPTIGA™ Authenticate NBT, encompassing the intended functionality of the device undergoes the installation of this software during its manufacturing process, resulting in its unalterable state thereafter
- **Off-chip software:** Describes the software components of a system, executed on the remaining devices of a system (that is, off the focused chip)

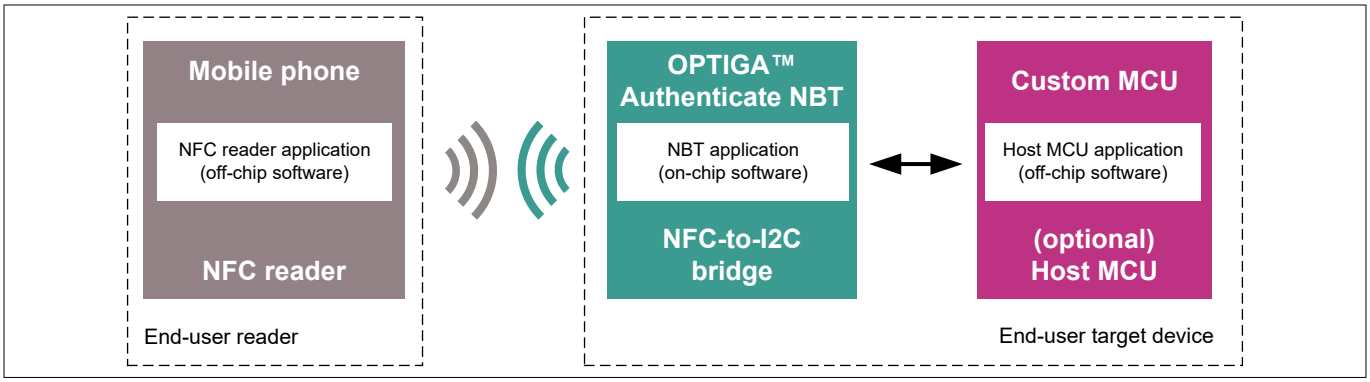


Figure 25 System software landscape

Since the OPTIGA™ Authenticate NBT's on-chip software is pre-installed on the device and is not intended for modification.

The off-chip software components focus on the software on the NFC reader and/or a host microcontroller. The host microcontroller is shown as optional in the figure since a subset of target applications (for example, brand protection) can be operated using the OPTIGA™ Authenticate NBT is powered through the NFC field and provides the target functionality without the support of a microcontroller.

For off-chip software, Infineon provides multiple host libraries that can be used by NFC reader applications as well as host MCU applications. Additionally, multiple example applications illustrate various use cases of the OPTIGA™ Authenticate NBT. The host libraries and example applications are described in more detail within the Software Integration Guide [18].

A Appendix

Infineon X.509 device certificate and PKI

In its delivery condition, the OPTIGA™ Authenticate NBT includes an NDEF message containing an Infineon X.509v3 DER-encoded certificate. This device-individual certificate is issued by an Infineon PKI and it facilitates the originality check: the certificate contains the public key that corresponds to the device's pre-installed brand protection signing key (BSK, EC P-256 private key). Henceforth, the public key is used to validate a signature computed by the production-default BSK.

The certificate is issued by an Infineon PKI using an intermediate manufacturing CA and a self-signed Infineon Root CA, as shown in Figure 26. These CA certificates are available via the product website [14].

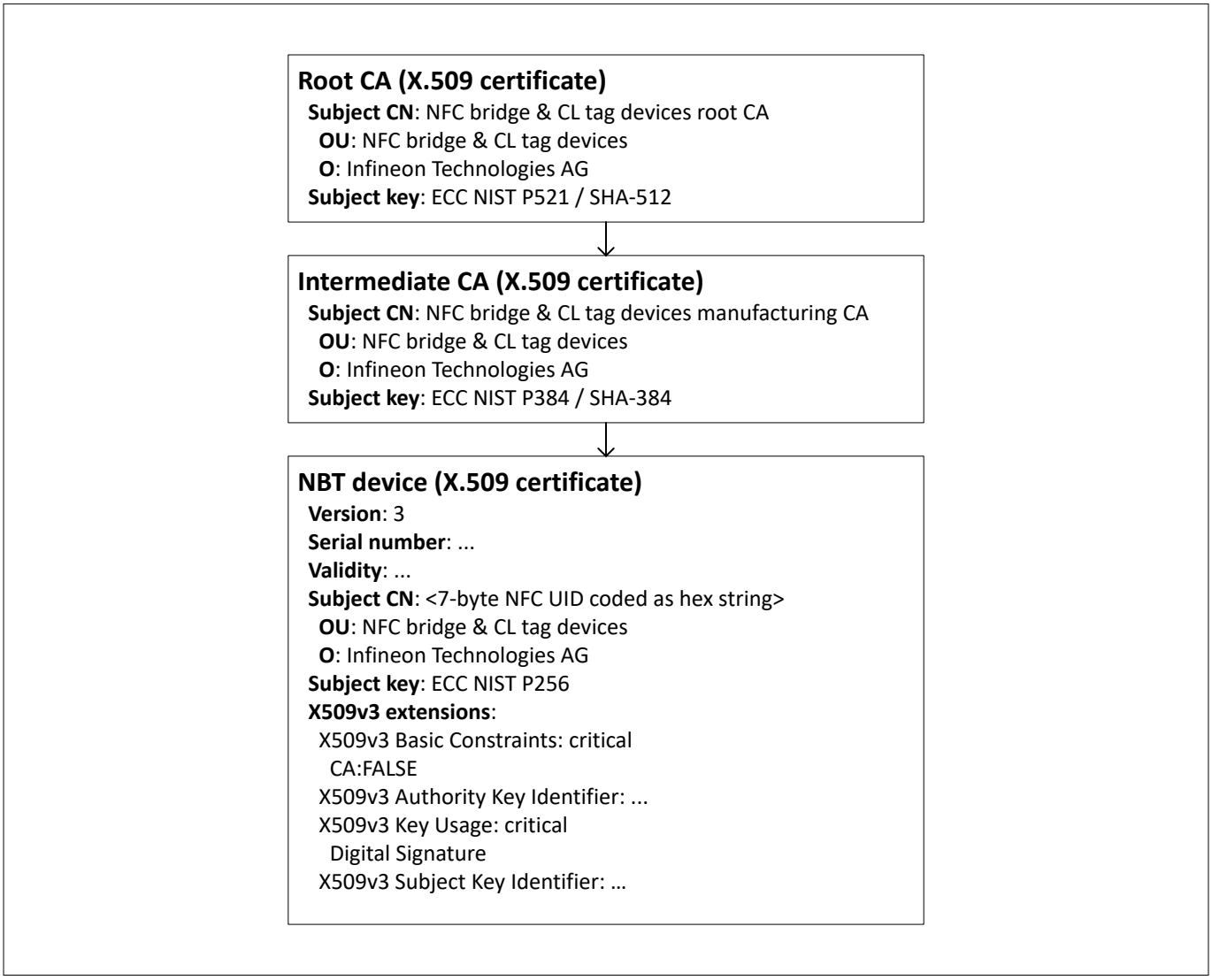


Figure 26 Infineon X.509 device certificate and PKI

The certificate subject common name (CN) contains the device's unique 7-byte NFC UID, which is encoded as a hex string with no delimiters, for example, 05848902954300_H as shown in Figure 27. This UID corresponds to the NFC UID used by the device during anti-collision.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1836660215 (0x6d7935f7)
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = DE, O = Infineon Technologies AG, OU = NFC bridge & CL tag devices,
                CN = NFC bridge & CL tag devices manufacturing CA
        Validity
            Not Before: Aug 28 13:38:43 2023 GMT
            Not After : Aug 28 13:38:43 2043 GMT
        Subject: C = DE, O = Infineon Technologies AG, OU = NFC bridge & CL tag devices,
                 CN = 05848902954300
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:d4:d2:da:90:1d:ea:42:37:3a:48:ec:a7:d9:f6:
                    d1:09:44:0e:a7:0a:24:20:6d:cd:76:24:56:60:ba:
                    77:83:1d:e3:8b:77:76:d4:b3:b9:30:37:e7:81:c9:
                    fd:f9:9f:c8:04:a8:47:97:d6:81:03:6b:bc:8e:b2:
                    04:39:c3:de:aa
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                6C:55:2F:86:10:AB:DE:28:26:42:73:17:A0:E8:13:61:67:E0:F4:3A
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:C4:3F:73:A2:1C:3B:66:BB:57:E2:89:ED:1B:72:03:7C:73:C0:58:68

    Signature Algorithm: ecdsa-with-SHA384
         30:63:02:2f:50:cb:43:f1:36:fc:a2:4c:4b:73:df:1a:6e:84:
         ec:d6:78:f0:2f:7d:cb:7d:20:2f:9a:fa:a0:cf:11:10:3d:b8:
         13:a9:eb:d6:2f:4b:23:05:a7:56:75:9d:cc:42:bc:02:30:01:
         e7:ae:66:8a:ff:0f:b5:0c:19:a6:e8:65:42:7a:7d:db:ca:1b:
         84:34:ec:4c:55:98:0e:58:4d:95:bf:bb:58:59:dd:a3:f8:b5:
         4e:0a:c7:38:e2:6f:14:58:71:4a:e5
```

Figure 27 Infineon X.509v3 device certificate

This pre-installed certificate can be used to implement an offline brand protection scheme. The scheme will then be based on the Infineon PKI and any Infineon OPTIGA™ Authenticate NBT with an original, pre-installed certificate will be seen as an authentic device.

If customers want to use their own device specific key pairs it is up to customers to design their own PKI. The customer created X.509 certificate containing the device specific public key needs to be embedded into an external record which gets loaded into the NDEF message. Additionally, the corresponding device specific private key (BSK) needs to be loaded into OPTIGA™ Authenticate NBT's secure key store.

Brand protection with COTT

In its delivery condition, the OPTIGA™ Authenticate NBT includes an NDEF message containing a well-known URI record type. This record contains an URL pointing to the Infineon website ("https://www.infineon.com/?cott=") as well as the COTT placeholder string.

The initial URI record, including the COTT placeholder string looks as follows:

https://www.infineon.com/?cott=PLACEHOLDERPLACEHOLDERPLACEHOLDERPLACEHOLDER

A new Cryptographic One-Time Token is computed each time the NDEF message file is selected on the OPTIGA™ Authenticate NBT. A Message Authentication Code (MAC) is computed by utilizing the chip individual information (TAG-UID), two header bytes, and a TAG-RANDOM (generated each time the NDEF file is selected) as inputs. The AES-128-CMAC calculation uses the AES-128 BMK from the device's secure key store. The input data and the MAC over this data are then merged and the Base64url-encoded value is inserted into the URL by replacing the COTT placeholder string.

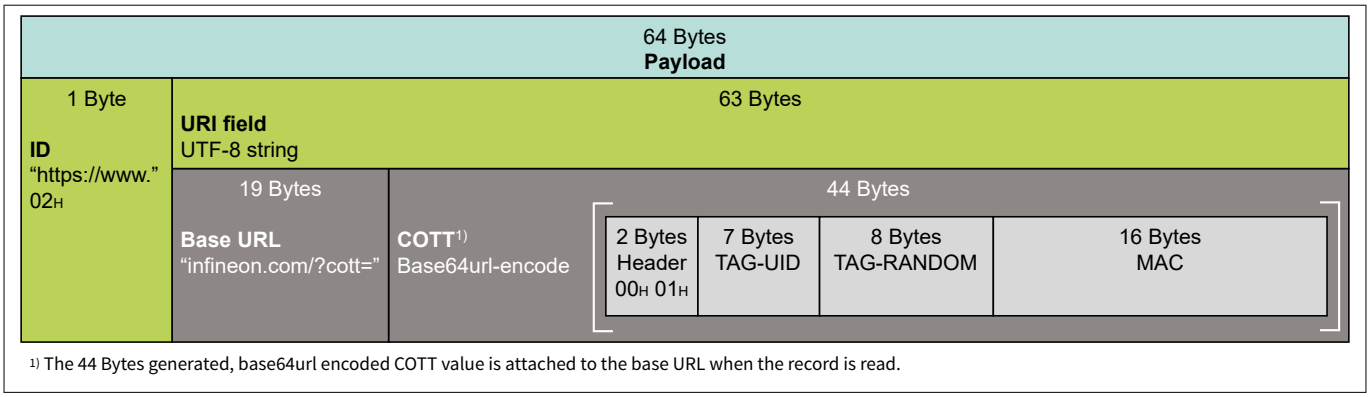


Figure 28 NFC well-known record type payload

Example: https://www.infineon.com/?cott=AQWPP9nUsgBNpDlMyEa1kWZR1FEQ6mBuxXmASo261wU=

OEM's personalizing the OPTIGA™ Authenticate NBT to use the device in an online brand protection application, shall update the NDEF message by exchanging the URL to an OEM-specific address and adding the COTT placeholder string. This record needs to be encoded accordingly within the well-known URI record. Additionally, the initial MAC'ing key BMK needs to be exchanged in the device's secure key store to a device specific, OEM-defined value.

References

ISO/IEC

[1] ISO/IEC 14443-1:2018: *Cards and security devices for personal identification - Contactless proximity objects - Part 1: Physical characteristics (Fourth edition)*; 2018-04

[2] ISO/IEC 14443-2:2020: *Cards and security devices for personal identification – Contactless proximity objects - Part 2: Radio frequency power and signal interface (Fourth edition)*; 2020-07

[3] ISO/IEC 14443-3:2018: *Cards and security devices for personal identification – Contactless proximity objects – Part 3: Initialization and anticollision (Fourth edition)*; 2018-07

[4] ISO/IEC 14443-4:2018: *Cards and security devices for personal identification – Contactless proximity objects – Part 4: Transmission protocols (Fourth edition)*; 2018-06

[5] ISO/IEC 7816-3:2006: *Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols (Third edition)*; 2006-11

[6] ISO/IEC 7816-4:2005: *Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange (Second edition)*; 2005-01

NFC Forum

[7] NFC Forum: *Type 4 Tag Technical Specification (Version 1.2)*; 2022-08-16

[8] NFC Forum: *Analog Technical Specification (Version 2.3)*; 2023-02-03

[9] NFC Forum: *Digital Protocol Technical Specification (Version 2.3)*; 2021-08-03

[10] NFC Forum: *Activity Technical Specification (Version 2.3)*; 2023-02-03

[11] NFC Forum: *NFC Data Exchange Format (NDEF) Technical Specification (Version 1.0);* 2006-07-24

GlobalPlatform

[12] GlobalPlatform: *Card Specification (Version 2.3.1);* 2018-03

[13] GlobalPlatform: *APDU Transport over SPI/I2C (Version 1.0);*2020-01

Infineon

[14] Infineon Technologies AG: *OPTIGA™ Authenticate NBT, product website* - https://www.infineon.com/OPTIGA-Authenticate-NBT

[15] Infineon Technologies AG: *OPTIGA™ Authenticate NBT, Release Notes (latest revision)*

[16] Infineon Technologies AG: *OPTIGA™ Authenticate NBT, Antenna Design Guide (latest revision)*

[17] Infineon Technologies AG: *OPTIGA™ Authenticate NBT, Hardware Integration Guide (latest revision)*

[18] Infineon Technologies AG: *OPTIGA™ Authenticate NBT, Software Integration Guide (latest revision)*

[19] Infineon Technologies AG: *Host parameterization via asynchronous data transfer (ADT), Use Case Guide (latest revision)*

[20] Infineon Technologies AG: *Host parameterization via pass-through (PT), Use Case Guide (latest revision)*

[21] Infineon Technologies AG: *Static connection handover, Use Case Guide (latest revision)*

[22] Infineon Technologies AG: *Brand protection, Use Case Guide (latest revision)*

[23] Infineon Technologies: *Package details PG-USON-8-8* - https://www.infineon.com/cms/en/product/packages/PG-USON/PG-USON-8-8/

[24] Infineon Technologies: *General recommendations for board assembly of Infineon packages* - https://www.infineon.com/dgdl/Infineon-Board_Assembly_Recommendations-General-Package-v05_00-EN.pdf?fileId=5546d4625cc9456a015ccaf4a1fe3a32

Inter-Integrated Circuit

[25] NXP Semiconductors: *I2C-bus specification and user manual (Revision 7.0);* 2021-10-01

Other

[26] FIPS 186-5: *Digital Signature Standard (DSS) (Revision 5.0);* 2023-02-03

Glossary

AC
alternating current (AC)

ADF
application dedicated file (ADF)

AES
Advanced Encryption Standard (AES)
The standard for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The algorithm described by AES is a symmetric-key algorithm (the same key is used for both encryption and decryption).

APDU
application protocol data unit (APDU)
The communication unit between a smart card reader and a smart card.

BMK
brand protection "MAC'ing" key (BMK)

BSK
brand protection signing key (BSK)

CB
contact-based (CB)
Used to refer to the controller operating in a contact-based power environment.

CC
capability container (CC)

COTT
cryptographic one time token (COTT)

DC
direct current (DC)
A synonym for static parameters of an electronic circuit, for example defining supply voltages or currents. Its antonym would be dynamic parameters see also AC.

DGI
data group identifier (DGI)

ECC
elliptic curve cryptography (ECC)

EF
elementary file (EF)
A file system component containing (user) data.

FAP
file access policy (FAP)

GND
ground (GND)

GP
GlobalPlatform (GP)

I2C
inter-integrated circuit (I2C)

ID
identifier (ID)

IEC
International Electrotechnical Commission (IEC)
The international committee responsible for drawing up electrotechnical standards.

IRQ
interrupt request (IRQ)
A type of exception that breaks the linear flow of a program. The requesting module needs a software service routine to evaluate its current state and take the necessary actions.

ISO
International Organization for Standardization (ISO)

Lc
The length field for coding Nc.

Le
The length field for coding Ne.

MAC
message authentication code (MAC)
Used to prove message integrity.

MCU
microcontroller unit (MCU)
One or more processor cores along with memory and programmable input/output peripherals.

NAK
not acknowledged (NAK)

NDEF
NFC data exchange format (NDEF)
A standardized data format specification by the NFC Forum to describe how a set of actions are to be encoded onto a NFC tag or to be exchanged between two active NFC devices.

NFC
near field communication (NFC)

NFCT4T
NFC Type 4 Tag (NFCT4T)

NLEN

NDEF length (NLEN)

A field in the NDEF message that indicates the size of the NDEF message.

OU

organization unit (OU)

PKI

public key infrastructure (PKI)

A set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

PLEN

proprietary length field (PLEN)

SCL

serial clock line (SCL)

SDA

serial data line (SDA)

TLV

tag length value (TLV)

UID

unique identifier (UID)

WTX

waiting time extension (WTX)

A waiting time extension request, available in the T=0 protocol. The smart card controller sends a 0x60 byte to the IFD, which in turn resets its timeout counter on this event.

Revision history

Reference	Description
Revision 2.1, 2024-04-18	
All	Editorial changes
Revision 2.0, 2024-03-28	
All	Major customer release
Revision 1.1, 2023-07-07	
All	Editorial changes
Revision 1.0, 2023-05-12	
All	Initial release

Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition 2024-04-18

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about any aspect of this document?

Email:
CSSCustomerService@infineon.com

Document reference
IFX-mjp1660293537850

Important notice

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie").

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

Warnings

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Infineon:

NBT2000A8K0T4USON8XTMA1 NBT2000A8K0T4USON8XTMA5