OPTIGA™ Authenticate NBT

Development kit guide

About this document

Scope and purpose

The scope of this document is to describe the functionality and components of the OPTIGA™ Authenticate NBT Development Kit bundle. It provides a quick and easy approach to evaluate the functionality of the OPTIGA™ Authenticate NBT and available example applications.

The purpose of this document is to assist end-users in setting up, using, and operating the OPTIGA™ Authenticate NBT Development Kit to explore the capabilities of the OPTIGA™ Authenticate NBT.

Intended audience

This document is primarily intended for solution providers, system integrators, application developers, and product marketers who want to evaluate and test the functionality provided by the OPTIGA™ Authenticate NBT.

Table of contents

List of tables

List of figures

1 Introduction

The OPTIGA™ Authenticate NBT Development Kit (shown in Figure 1) is an assembly of hardware components that allows to evaluate and develop applications for the OPTIGA™ Authenticate NBT.

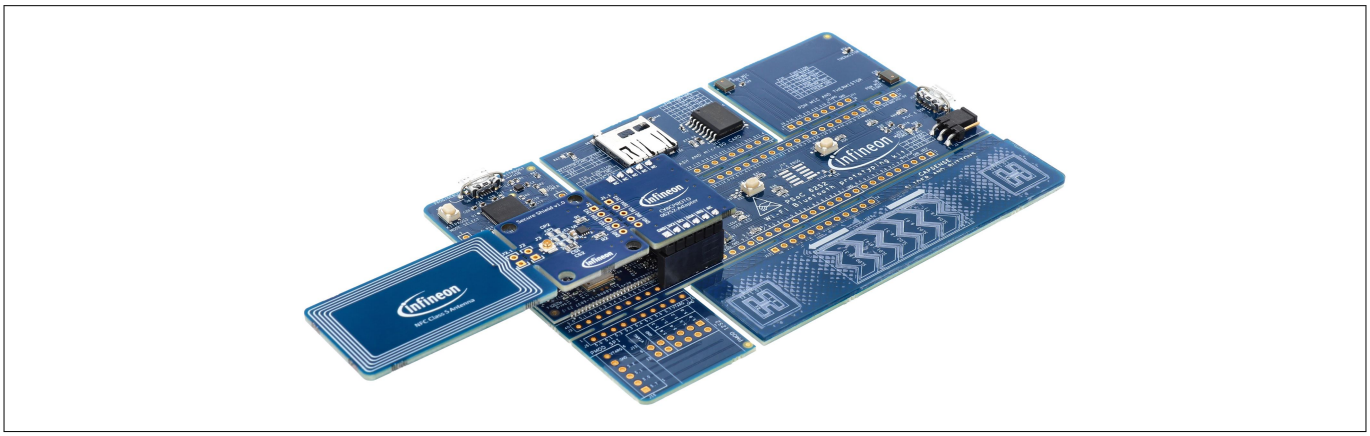

Figure 1 OPTIGA™ Authenticate NBT Development Kit with its main components

This chapter provides a short description of the OPTIGA™ Authenticate NBT, the NFC bridge tag used in the development kit, as well as an overview of its supporting materials.

Chapter 2 provides an overview of the development kit bundle, lists and defines its components, and describes the interfaces that connect them.

Chapter 3 demonstrates how to use the development kit bundle to test the functionality of the OPTIGA™ Authenticate NBT and introduces various usage scenarios.

***Note**: For an overview of related support material, refer to the OPTIGA™ Authenticate NBT's product page [1] and the OPTIGA™ Authenticate NBT Development Kit's product page [3].*

1.1 NFC I2C bridge tags

NFC Bridge Tags are dual-interface tags that enable contactless features for IoT devices via an I2C controller interface, allowing for a touch-and-go experience with a mobile phone. On one side, the NFC Bridge Tags include a contactless passive NFC interface and on the other side, a contact-based I2C target interface that connects to the MCU of the IoT device.

The OPTIGA™ Authenticate NBT harnesses the Integrity Guard 32 security architecture to provide an option for the end-user with symmetric and asymmetric cryptographic operations, as well as password-based data protection schemes. As a result, the device is ideal for security demanding applications.

This product includes device authentication, pass-through and asynchronous data transfer modes, which can be used for variety of applications such as:

- Keyless access and activation of shared mobility vehicles
- Controlled access to personal electronic devices such as HDD
- Theft prevention for electronic goods by authenticated activation

This tag can also be used in healthcare and industrial applications. The OPTIGA™ Authenticate NBT, in combination with healthcare sensors, enables access to information through an NFC-enabled mobile phone or reader. Furthermore, the device is an ideal product for industrial applications such as headless configuration and parametrization of devices, assembly line programming and fault diagnostics.

2 OPTIGA™ Authenticate NBT Development Kit bundle

This chapter provides a brief overview of the intended purpose and use case scenarios of the OPTIGA™ Authenticate NBT Development Kit bundle. The individual components of the kit bundle are listed, with the key parts described in detail.

2.1 Scope of the kit bundle

The OPTIGA™ Authenticate NBT Development Kit bundle enables a quick and easy evaluation of the device's core functionality using a variety of example applications. Additionally, system integrators can test the ease of integration of the OPTIGA™ Authenticate NBT into any target platform/application with the flexible OPTIGA™ Authenticate NBT Shield. Using the available host libraries and example applications, various device functionality can be integrated and tested.

The OPTIGA™ Authenticate NBT Development Kit bundle is specifically designed for the following purposes:

- Evaluation of the OPTIGA™ Authenticate NBT's use cases with the provided example applications, using the included kit components and an NFC-enabled mobile phone
- Development of custom applications, based on the provided example applications. While the embedded example applications are tailored to the development kit's host MCU, the application logic is generally applicable and can be reused on custom platforms
- Accelerated development of embedded PSoC™ applications: The provided host library package contains a reusable implementation of the platform abstraction layer for the development kit's host microcontroller, easily portable to any other PSoC™

Difference to the OPTIGA™ Authenticate NBT Development Shield bundle

In addition to the OPTIGA™ Authenticate NBT Development Kit bundle, Infineon also offers the OPTIGA™ Authenticate NBT Development Shield bundle (refer to the product page [4] or user guide [8] for more information). In contrast to the OPTIGA™ Authenticate NBT Development Kit bundle, the shield bundle does not include a host MCU board. If the OPTIGA™ Authenticate NBT is targeted to be operated in use cases with a host MCU, a custom host MCU board is required.

The OPTIGA™ Authenticate NBT Development Shield bundle is ideal for the evaluation and application development with custom MCU boards. The shield's default adapter enables easy attachment to Arduino UNO-compatible MCU boards. It is preferable, if no evaluation of the example applications with PSoC™ host MCU board is desired.

The OPTIGA™ Authenticate NBT Development Kit bundle is ideal for quick and simple evaluation of the OPTIGA™ Authenticate NBT with the provided use case implementations. It also simplifies the development of custom applications for PSoC™ host MCUs, based on the example applications. After detaching the adapter board, the shield may also be used *standalone* for evaluation and application development with custom MCU boards.

2.2 Kit bundle content

The OPTIGA™ Authenticate NBT Development Kit bundle is delivered with a set of main components and additional accessories (see Figure 2). These additional accessories increase the kit's flexibility and enhance its evaluation capabilities.

The development kit’s package contains the following components:

- OPTIGA™ Authenticate NBT Shield
- Host MCU board adapter for CY8CPROTO-062S2, connected to the OPTIGA™ Authenticate NBT Shield per default
- PSoC™ 62S2 Wi-Fi BT Prototyping Kit (CY8CPROTO-062S2-43439)
- Additional accessories
  - Class 6 shield antenna
  - Cables: UMCC antenna cable, five-pin jumper cable and micro USB cable

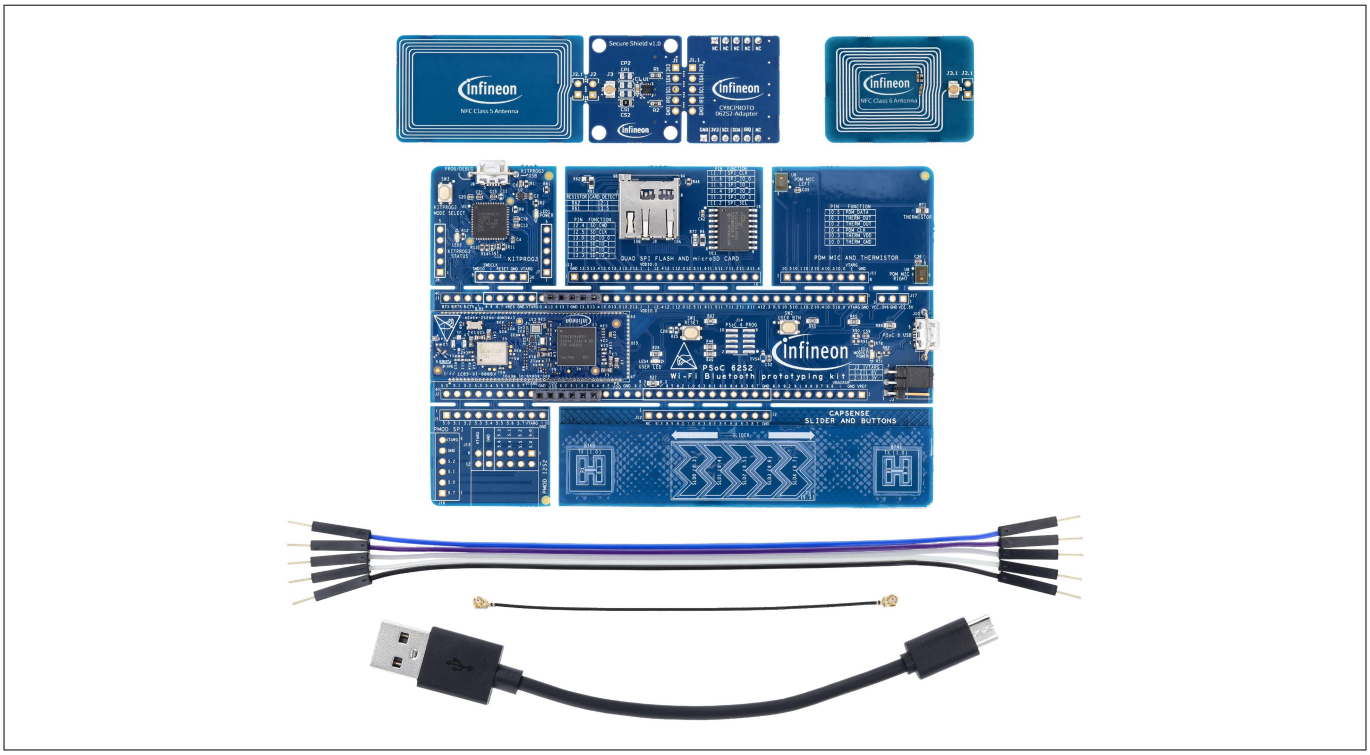

Figure 2 Components of the OPTIGA™ Authenticate NBT Development Kit bundle

2.3 OPTIGA™ Authenticate NBT Shield

This section describes the OPTIGA™ Authenticate NBT Shield in detail. The shield consists of two primary components which are initially connected to each other:

- NBT Secure Shield
- Class 5 shield antenna

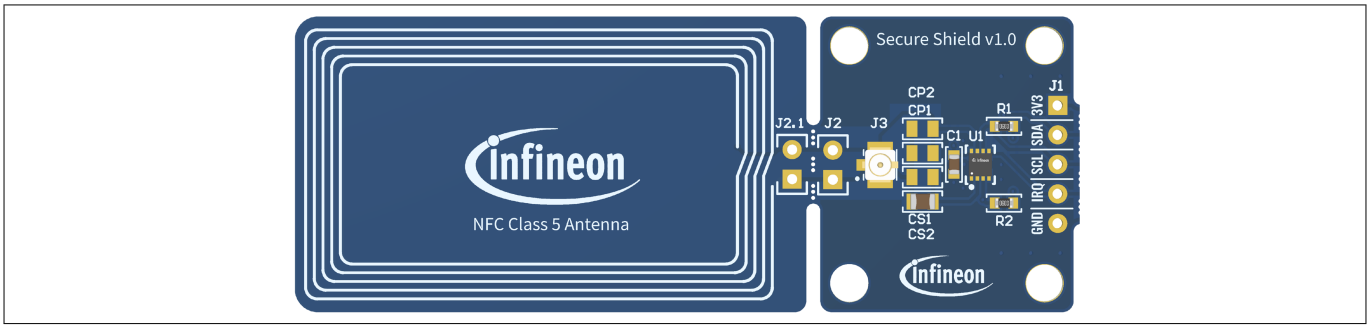

Figure 3 Composition of the OPTIGA™ Authenticate NBT Shield

The OPTIGA™ Authenticate NBT Shield, as shown in Figure 3, provides the pin header J1 that allows to easily connect the NBT Shield to various host MCU boards (for example via the included five-pin jumper cable). Alternatively, these pins can also be connected to an adapter board, which allows it to be directly plugged into specific host boards. By default, the OPTIGA™ Authenticate NBT Shield comes with a detachable host MCU adapter board (see Chapter 2.4).

2.3.1 NBT Secure Shield

The NBT Secure Shield is the primary component of the OPTIGA™ Authenticate NBT Shield, and it is designed to be simple, reusable, and adaptable. It is equipped with the OPTIGA™ Authenticate NBT device, which provides a contactless NFC interface as well as a contact-based I2C interface. The board provides two connectors to an NFC antenna on one side (J2 and J3) and to a microcontroller (or a specific adapter board) on the other side

(J1). In addition, a matching circuit allows the optimization of the OPTIGA™ Authenticate NBT's contactless performance to arbitrary antennas.

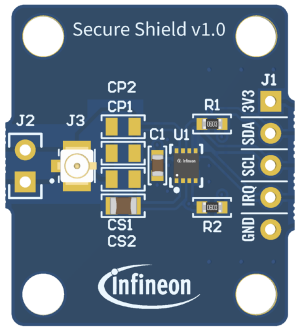

Figure 4 Board details of the NBT Secure Shield

Table 1 NBT Secure Shield antenna connections

NBT Secure Shield pins	OPTIGA™ Authenticate NBT pins	Function
J2	L_A/L_B	Antenna connection via two-pin header
J3	L_A/L_B	Antenna connection via U.FL socket (UMCC cable)

Table 2 NBT Secure Shield five-pin header (J1) to connect to microcontroller boards

NBT Secure Shield pins	OPTIGA™ Authenticate NBT pins	Function
3V3	V_{CC}	Power and pad supply
SDA	SDA	I2C data
SCL	SCL	I2C clock
IRQ	IRQ	Interrupt
GND	GND	Common ground reference

I2C address

The device operates as a target with the initial device address 18_H.

2.3.2 Class 5 shield antenna

The default antenna (see Figure 5) follows ISO/IEC 14443-1 Class 5 requirements. The antenna is designed to operate at a resonance frequency of 13,56 MHz. The design parameters of the (antenna) coil are adjusted to meet this requirement in combination with the 78 pF on-chip capacitance of the OPTIGA™ Authenticate NBT chip. The Antenna Design Guide [9] explains how to design custom antennas and match them to the OPTIGA™ Authenticate NBT.

***Note**: The Class 5 shield antenna may be removed from the OPTIGA™ Authenticate NBT Shield. In order to reconnect, use the antenna's L_A and L_B connector J2.1 and the NBT Secure Shield's respective header J2.*

Figure 5 Board details of the Class 5 shield antenna

Table 3 Class 5 shield antenna connector to NBT Secure Shield

Class 5 shield antenna pins	Description
J2.1	Antenna connections (L_A/L_B)

2.4 CY8CPROTO-062S2 Adapter

By default, the CY8CPROTO-062S2 Adapter (see Figure 6) is connected to the OPTIGA™ Authenticate NBT Shield. This adapter board connects the NBT Secure Shield's five-pin interface (shown in Table 4) to a subset of the PSoC™ 62S2 Wi-Fi BT Prototyping Kit's pin-out. This adapter can be used to directly connect the OPTIGA™ Authenticate NBT Shield to the included PSoC™ 62S2 Wi-Fi BT Prototyping Kit.

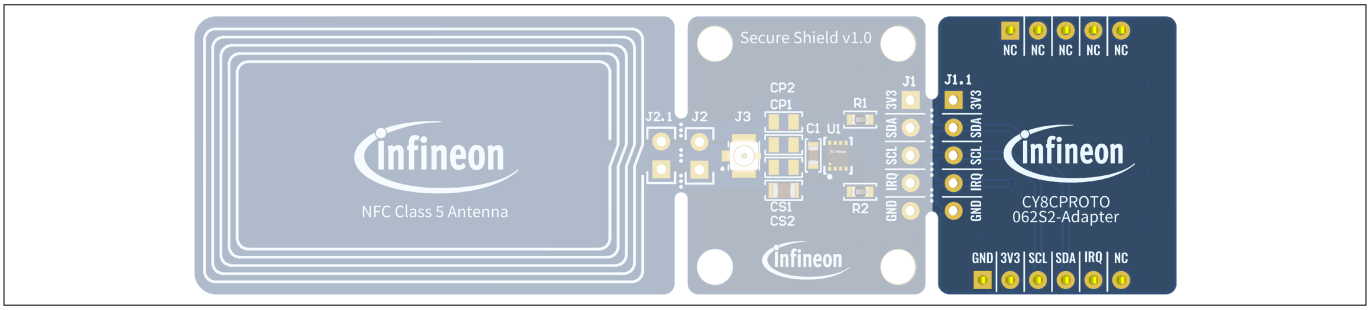

Figure 6 Board details of the CY8CPROTO-062S2 Adapter

Table 4 Mapping of the OPTIGA™ Authenticate NBT Shield's pins to the host microcontroller board

NBT Secure Shield pins	PSoC™ CY8CPROTO-062S2 pins	Function
3V3	V_{DD}	Power and pad supply
SDA	P6.1	I2C data
SCL	P6.0	I2C clock
IRQ	P6.2	Interrupt
GND	GND	Common ground reference

2.5 PSoC™ 62S2 Wi-Fi BT Prototyping Kit

The OPTIGA™ Authenticate NBT Development Kit bundle includes the PSoC™ 62S2 Wi-Fi BT Prototyping Kit (CY8CPROTO-062S2-43439) as its host board. The PSoC™ 62S2 Wi-Fi BT Prototyping Kit includes a PSoC™ 6 MCU, Bluetooth and Wi-Fi wireless interfaces, various types of input buttons, and a few LEDs for output. These board features are used to debug and demonstrate the capabilities of the OPTIGA™ Authenticate NBT. This board's specification can be found on Infineon's product website for the prototyping kit [5].

Figure 7 depicts the PSoC™ 62S2 Wi-Fi BT Prototyping Kit and highlights the pins used to connect the OPTIGA™ Authenticate NBT Development Shield via its CY8CPROTO-062S2 Adapter (refer to Chapter 2.4). The host board includes a micro USB cable for its power supply and/or to connect it to a development PC for flashing new MCU applications.

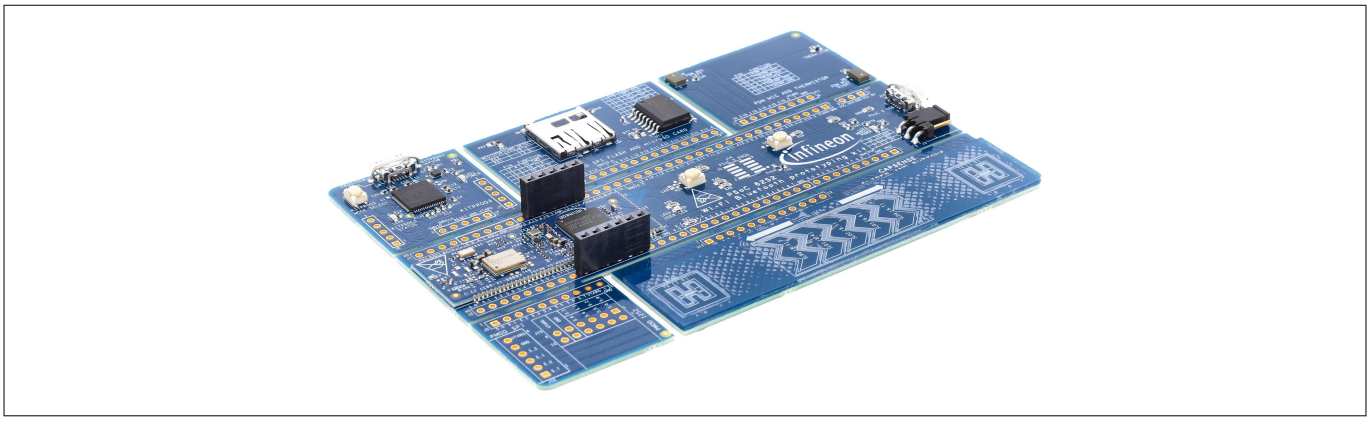

Figure 7 PSoC™ 62S2 Wi-Fi BT Prototyping Kit

Figure 8 depicts the development kit in its default configuration. The PSoC™ 62S2 Wi-Fi BT Prototyping Kit is connected to the OPTIGA™ Authenticate NBT Development Shield via a dedicated adapter board (connected to the NBT Shield per default, see CY8CPROTO-062S2 Adapter). In this setup, the NFC antenna extends to the left side without overlapping with the PSoC™ 62S2 Wi-Fi BT Prototyping Kit.

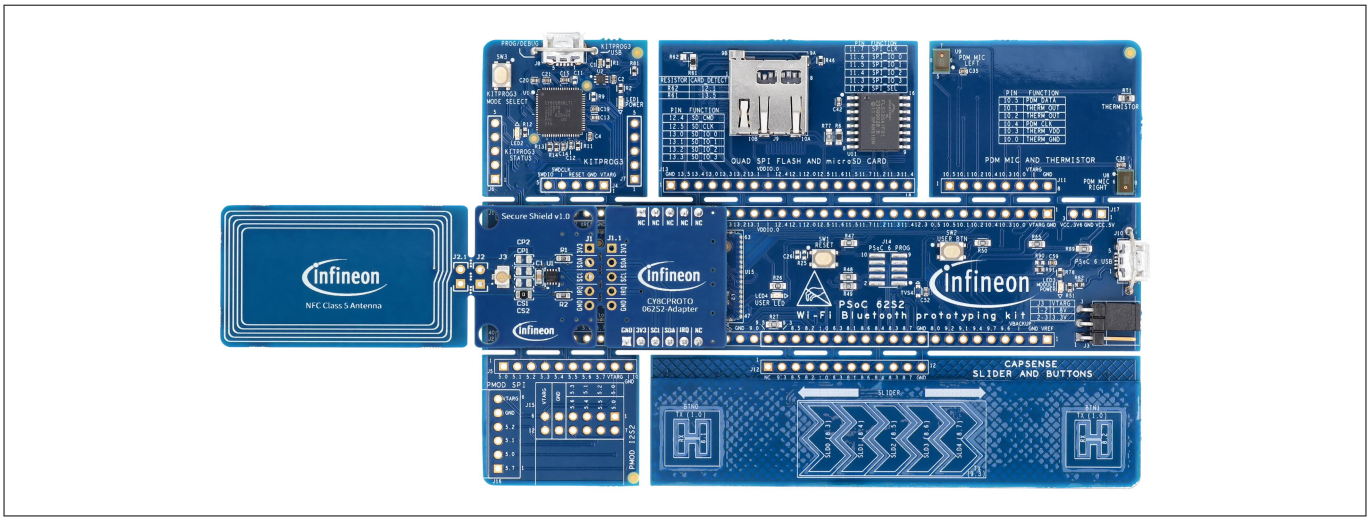

Figure 8 OPTIGA™ Authenticate NBT Development Shield mounted on the PSoC™ 62S2 Wi-Fi BT Prototyping Kit

2.6 Additional accessories

This section introduces the additional components included in the OPTIGA™ Authenticate NBT Development Kit bundle. While these components are not required for evaluation in the default configuration, they allow for easy rework for a variety of alternative usage scenarios.

2.6.1 Class 6 shield antenna

The Class 6 shield antenna is an accessory that allows the evaluation of a smaller antenna. Figure 9 depicts the board details for the Class 6 shield antenna. The board includes a U.FL antenna connector in addition to the standard two-pin antenna header, as shown in the figure. Given that this antenna is designed to be connected to the NBT Secure Shield via a flexible UMCC cable, arbitrary antenna placements can be evaluated.

In its default configuration, the antenna contains 7 windings and is designed to produce a 13,56 MHz resonance frequency when used with the included 10 cm UMCC cable and the OPTIGA™ Authenticate NBT's input capacitance of 78 pF. In addition, the antenna board includes a solder bridge for adapting the inductance for non-standard use (more details in the next chapter). The Antenna Design Guide [9] explains how to design custom antennas and match them to the OPTIGA™ Authenticate NBT.

Figure 9 **Class 6 shield antenna in its default configuration (usage with the included UMCC cable)**

Table 5 **Class 6 shield antenna connector pins to NBT Secure Shield**

Antenna connectors	Description
J2.1	Antenna connection to the NBT Secure Shield via two-pin header
J3.1	Antenna connection to the NBT Secure Shield via U.FL socket

2.6.2 Cables

Multiple cables are included into the package to enhance its flexibility (see Figure 10). After detaching the Class 5 shield antenna, the UMCC cable can be used to easily connect the Class 6 shield antenna to the NBT Secure Shield (default). The included five-pin jumper cable can be used for connecting the NBT Secure Shield to custom host MCU boards or adapter boards. When this cable is used to connect the system's components, it allows a flexible connection to the NBT Secure Shield at various lengths and allows the evaluation of alternative system compositions.

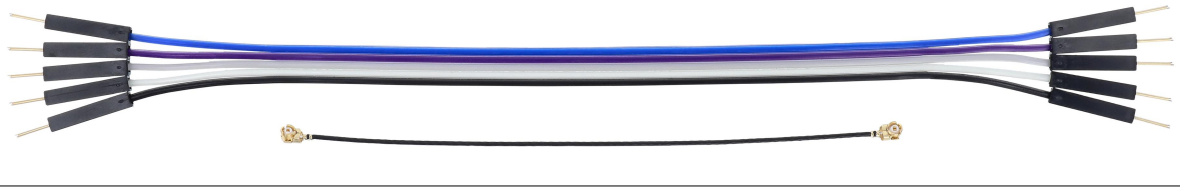

Figure 10 **UMCC cable to connect the Class 6 shield antenna (bottom), five-pin jumper cable (top)**

2.7 PCB design data

To support system integrators, the PCB design data of the OPTIGA™ Authenticate NBT Shield with its CY8CPROTO-062S2 Adapter is provided as a reference on the OPTIGA™ Authenticate NBT Development Kit's product page [3]. The design data includes:

- **Schematics:** This PDF document contains the schematics of the development shield with the host board adapter as well as the Class 5 shield antenna
- **Design data:** This zip file contains the kit's associated schematics and board layouts, as well as the board's Bill of Material (BOM)

The design information of the host MCU board is not included in this compilation and can be found on its individual product page [5].

2.8 Example applications

Infineon Technologies provides host libraries to support the integration of the OPTIGA™ Authenticate NBT into custom applications on different platforms. In addition, multiple example applications demonstrate the capabilities of the device in different use cases. These implementations utilize the host libraries to demonstrate minimum viable applications on mobile phones (Android and iOS) and on the reference host microcontroller (PSoC™ 6).

***Note**: All host libraries and example applications are shared as source code and are available as individual repositories on GitHub [2].*

The OPTIGA™ Authenticate NBT Development Kit bundle serves as the primary reference hardware and allows to evaluate both, the embedded microcontroller applications and the mobile phone apps. The embedded C/C++ applications are provided as ModusToolbox™ projects based on the development kit's host microcontroller board.

The OPTIGA™ Authenticate NBT Shield can also be used standalone to evaluate the mobile phone apps with the OPTIGA™ Authenticate NBT operated as NFC-only tag. The NBT Shield may also be connected to custom host MCU boards to integrate the OPTIGA™ Authenticate NBT into embedded applications on the respective platform. In that case, the provided applications can serve as examples for the implementation since their application logic can be easily re-used on other platforms.

***Note**: For more information about the example applications, refer to the Software Integration Guide [10].*

3 OPTIGA™ Authenticate NBT Development Kit usage

This chapter describes how to use the OPTIGA™ Authenticate NBT Development Kit bundle to evaluate the OPTIGA™ Authenticate NBT's example applications for various use cases. The general description is targeted for the usage of the kit in its default setup with the Class 5 shield antenna and the CY8CPROTO-062S2 Adapter still connected to the NBT Shield, mounted on the PSoC™ host MCU board (see Figure 8). However, the kit may also be used in a variety of other configurations and/or assemblies. Thus, this section also introduces several alternative usage scenarios as well as the necessary rework steps.

3.1 Getting started

The components of the evaluation setup depend on the type of the desired use case(s). The host MCU board is marked as optional for the reason that a subset of the use cases can be operated entirely through the NFC interface.

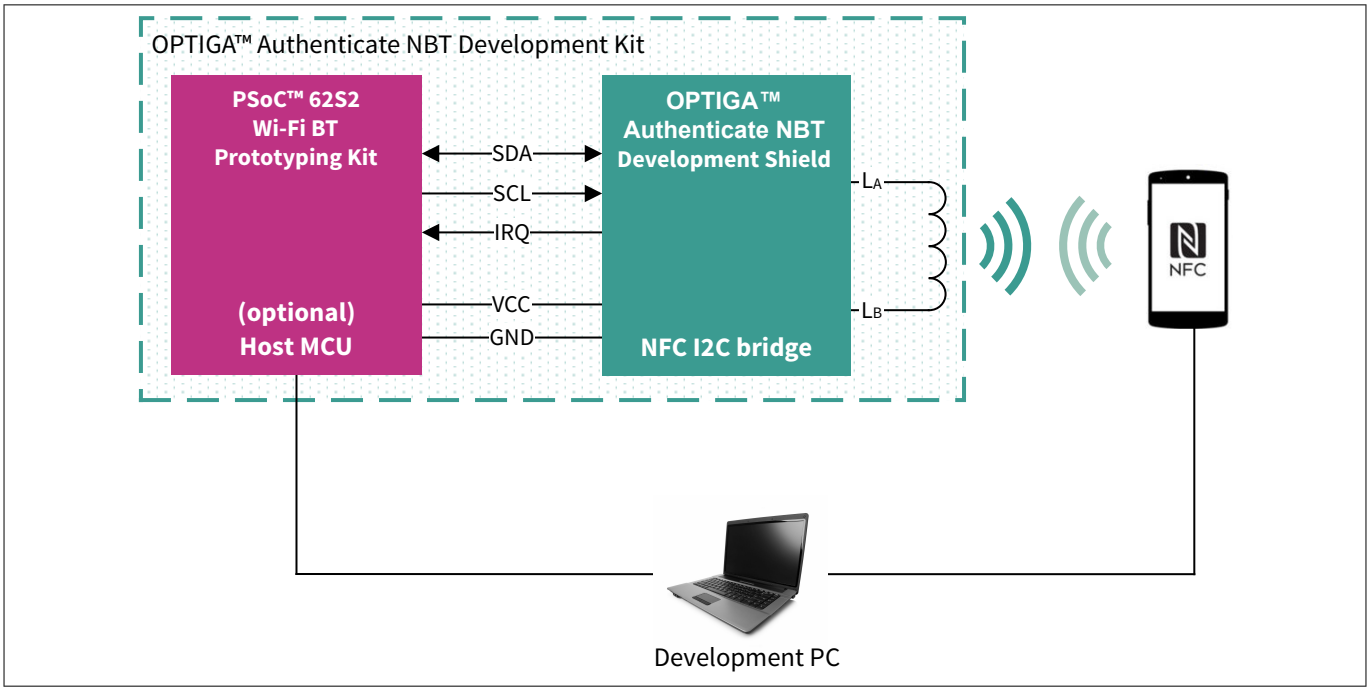

Figure 11 Evaluation setup with the OPTIGA™ Authenticate NBT Development Kit

As shown in Figure 11, the following components are required to evaluate the OPTIGA™ Authenticate NBT with all provided use case implementations:

- OPTIGA™ Authenticate NBT Development Kit (including the OPTIGA™ Authenticate NBT Shield with its CY8CPROTO-062S2 Adapter and the included PSoC™ 62S2 Wi-Fi BT Prototyping Kit as host MCU board)
- A development PC with Android Studio/Xcode and ModusToolbox™ for building the example applications (refer to Chapter 2.8)
- An NFC-enabled Android/iOS mobile phone for running the example mobile phone apps

3.2 Theory of operation

In typical usage scenarios, the OPTIGA™ Authenticate NBT needs to be configured for the target use case before it is ready to serve its actual target purpose (for example, asynchronous data transfer). This section describes these two phases during the evaluation of the OPTIGA™ Authenticate NBT with the development kit.

The two phases are closely related to the OPTIGA™ Authenticate NBT's life cycle states: PERSONALIZATION and OPERATIONAL. While the product is in PERSONALIZATION state, unrestricted altering of its configuration is possible (for example, interface settings, file access policies or initial file contents). In OPERATIONAL state, modification of the configuration is restricted to the permissions set during the personalization.

OPTIGA™ Authenticate NBT devices in productive settings are configured in the PERSONALIZATION life cycle state (for example, in the product assembly line). The configuration of the OPTIGA™ Authenticate NBT can be finalized and locked by activating the OPERATIONAL state. After executing this step, the product is ready for distribution.

The functional behavior of OPTIGA™ Authenticate NBT is identical in both life cycle state - with a single exception: in PERSONALIZATION state, the reconfiguration of the product is still possible. This product behavior can be used during application development and evaluation, where it is recommended to keep the OPTIGA™ Authenticate NBT samples in the PERSONALIZATION life cycle state for both, their configuration and their target usage. Omitting the one-way transition to OPERATIONAL allows a repetitive evaluation of various use cases and different configurations with a single device.

To allow unrestricted evaluation, the OPTIGA™ Authenticate NBT Development Kit samples are recommended to be permanently left in the PERSONALIZATION life cycle state. The upcoming subsections describe the procedure to configure and operate the development kit to evaluate the OPTIGA™ Authenticate NBT with the provided use case implementations.

3.2.1 Configuring device

Like any OPTIGA™ Authenticate NBT chip, the unit soldered on the OPTIGA™ Authenticate NBT Development Shield is in the PERSONALIZATION state after delivery. Therefore, the first step is to prepare the OPTIGA™ Authenticate NBT for the intended use case by personalizing the device's content and settings. In the PERSONALIZATION state, the OPTIGA™ Authenticate NBT's product configuration can be customized using both the NFC and the I2C interfaces. For example, it may be performed by an NFC reader within the production line, or by the microcontroller via I2C during the initial start-up.

The recommended method to personalize the shield's OPTIGA™ Authenticate NBT is to use the *NBT Personalization* mobile phone app (see Figure 12). This app utilizes the mobile phone's NFC interface to personalize the OPTIGA™ Authenticate NBT with the predefined configuration for the selected use case. System developers can utilize this application to (re-)configure the OPTIGA™ Authenticate NBT for the provided use case implementations.

While personalizing via NFC, the OPTIGA™ Authenticate NBT is powered from the NFC reader's field. A connection to a host board is not required. For this task, the development shield may be used standalone, however, it can also be connected to a host MCU board (for example, the PSoC™ 62S2 Wi-Fi BT Prototyping Kit).

In order to allow the repetitive evaluation of various use cases and different configurations, the *NBT Personalization* application skips the final command to trigger the transition into the OPERATIONAL state. This allows to use the product in the fully configured state, while still having the ability to reset the configuration and repeat the personalization flow.

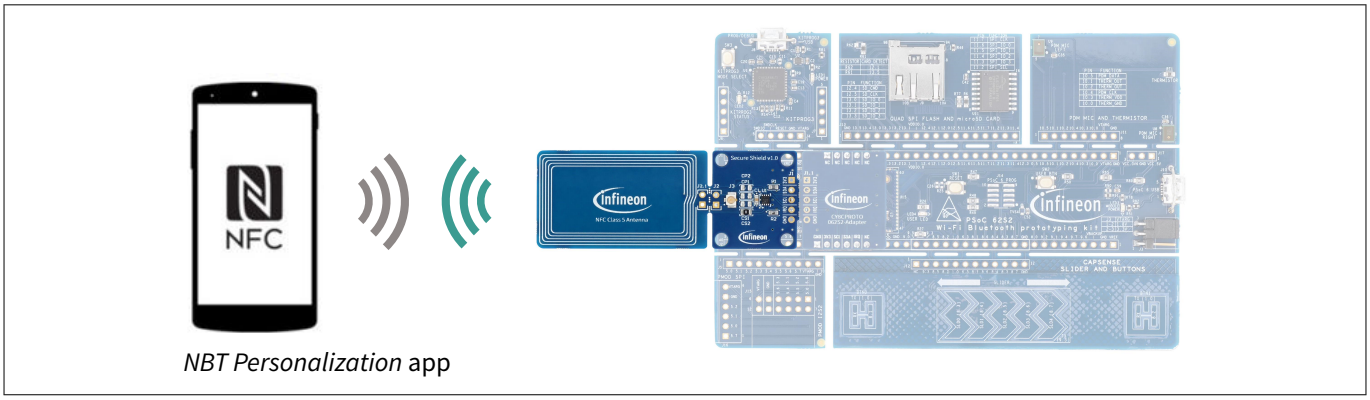

Figure 12 Personalization of the OPTIGA™ Authenticate NBT with the NBT Personalization mobile phone app

The following steps must be taken to personalize the OPTIGA™ Authenticate NBT with the mobile phone app:

- The *NBT Personalization* app must be installed on an Android/iOS mobile phone
  - Get the project source code from GitHub [2]
  - Build the mobile phone app in Android Studio or Xcode and transfer it onto the mobile phone

- Open the app on the mobile phone and select the target use case in the *NBT Personalization* app
- To personalize, tap the mobile phone's NFC antenna to the OPTIGA™ Authenticate NBT Development Shield's NFC antenna
  - For personalization via NFC, it makes no difference whether the development shield is used standalone (as NFC-only tag) or connected to a host MCU board (as embedded tag)

Alternatively, the personalization commands can also be transferred via the I2C interface. At start-up, all provided MCU example applications are checking the OPTIGA™ Authenticate NBT's configuration and execute the personalization steps for the targeted use case via I2C. As a result, performing personalization with the *NBT Personalization* mobile phone app is not required for evaluating the provided use case implementations that include an embedded example application.

***Note**: For more details on how to configure the OPTIGA™ Authenticate NBT for certain use cases during personalization state, refer to the provided Use Case Guides [11], [12], [13], [14].*

3.2.2 Target usage

After personalizing, the OPTIGA™ Authenticate NBT is ready to be used in the context of its target use case to provide it's desired functionality. Depending on the intended use case, the OPTIGA™ Authenticate NBT may perform interactions via the I2C and/or the NFC interface (see Figure 13).

When used as NFC-only tag, the OPTIGA™ Authenticate NBT only utilizes the interface to an NFC reader (for example, a mobile phone). In such cases, the NFC interface is used for the data exchange and to power the OPTIGA™ Authenticate NBT via the NFC field, eliminating the need for a contact-based power supply or a microcontroller.

Other use cases rely on the NFC-to-I2C bridge functionality (used as embedded tag). In such cases, a microcontroller is used along with an NFC-enabled device. For example, a custom NFC application on a mobile phone may be used to interact with the OPTIGA™ Authenticate NBT via NFC, the microcontroller recognizes the data transfer and responds appropriately (for example, by reconfiguring the host system).

Multiple example applications are available that can be used to evaluate and test the capabilities of the OPTIGA™ Authenticate NBT in various use cases. These applications can be used as base projects to develop custom applications on PSoC™-based platforms, or as examples to develop embedded applications on custom MCUs.

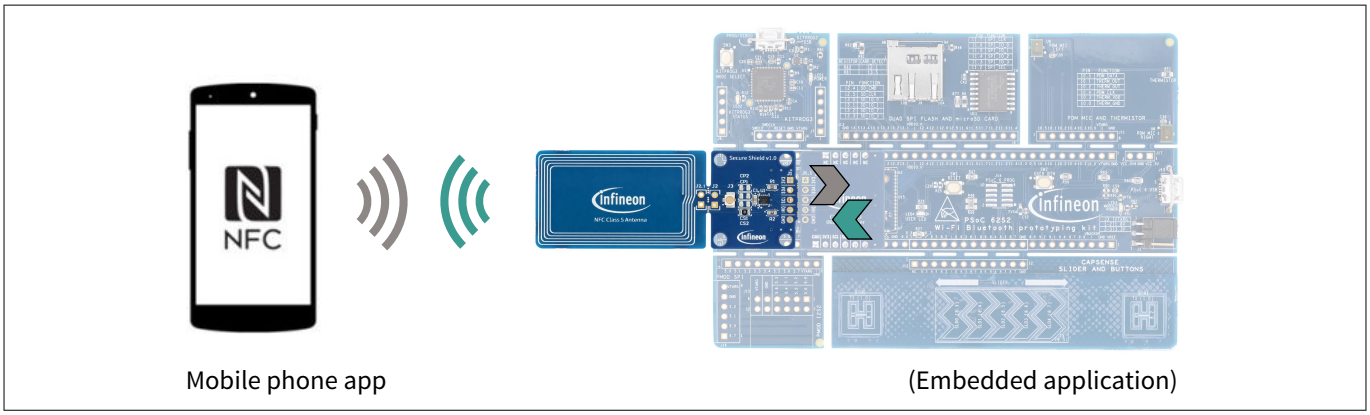

Figure 13 Target usage of the OPTIGA™ Authenticate NBT with mobile phone and MCU applications

The following steps must be taken in order to evaluate the provided use case implementations for the OPTIGA™ Authenticate NBT with the development kit:

- The use case-specific Android/iOS app must be installed on the mobile phone
  - Get the project source code from GitHub [2]
  - Build the mobile phone app in Android Studio or Xcode and transfer it onto the mobile phone
- The use case-specific embedded application must be loaded onto the PSoC™ microcontroller
  - Use ModusToolbox™ to build and flash the embedded application

- The OPTIGA™ Authenticate NBT Development Shield must be connected to the PSoC™ host MCU board's respective pins. For example, via the adapter board (see Chapter 2.4) or via flying wires
- A micro-USB cable is required to power the PSoC™ host MCU board

- Evaluate the flow of the respective use case
  - Launch the respective applications
  - Perform use case-specific interactions (tapping the mobile phone to the NFC antenna)
  - Depending on the use case, interaction with the microcontroller (for example, button press) may be required

***Note**: The installation steps for the embedded application/mobile phone app may be skipped if not designated for the target use case. For more information about the required steps to evaluate a specific use case, refer to the associated documentation on GitHub [2].*

3.3 Alternative usage scenarios

This section provides multiple examples on how to use the OPTIGA™ Authenticate NBT Development Kit bundle and its components in a non-standard configuration (for example, flexible antenna placement) or with a custom host MCU board.

3.3.1 Usage with custom microcontroller boards

Instead of connecting the OPTIGA™ Authenticate NBT Shield with its CY8CPROTO-062S2 Adapter to the included PSoC™ board, the NBT Shield can also be connected to any custom microcontroller board. The following steps must be taken:

- Optional: Remove (break off) the CY8CPROTO-062S2 Adapter
- Connect the five pins of the NBT Secure Shield to the respective pins of the custom MCU board. For example, by using the five-pin jumper cable included in the kit bundle (soldering may be required). Refer to Chapter 2.3.1) for the detailed pin descriptions

Figure 14 shows an example, where the NBT Shield is directly attached to a Raspberry Pi. In this special case, the shield can be directly attached since the Raspberry Pi's pin header fits to the NBT Secure Shield's pinout.

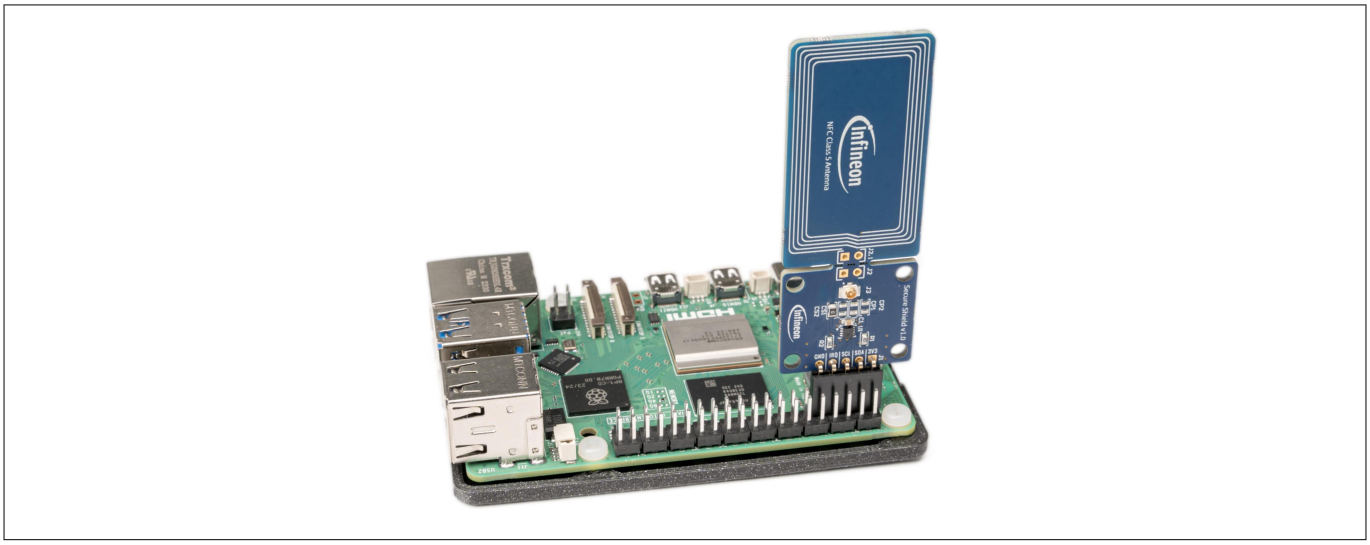

Figure 14 Attaching of the NBT Shield on a custom microcontroller board (direct mount)

Another example setup, where the OPTIGA™ Authenticate NBT is evaluated on a custom host MCU board is shown in Figure 15. Here, a breadboard is used with the included five-pin jumper to connect the OPTIGA™ Authenticate NBT Shield's pins to the corresponding pins of the custom host MCU board. This simple setup demonstrates the flexibility of the NBT Shield to enable the evaluation of the OPTIGA™ Authenticate NBT device on arbitrary MCU platforms.

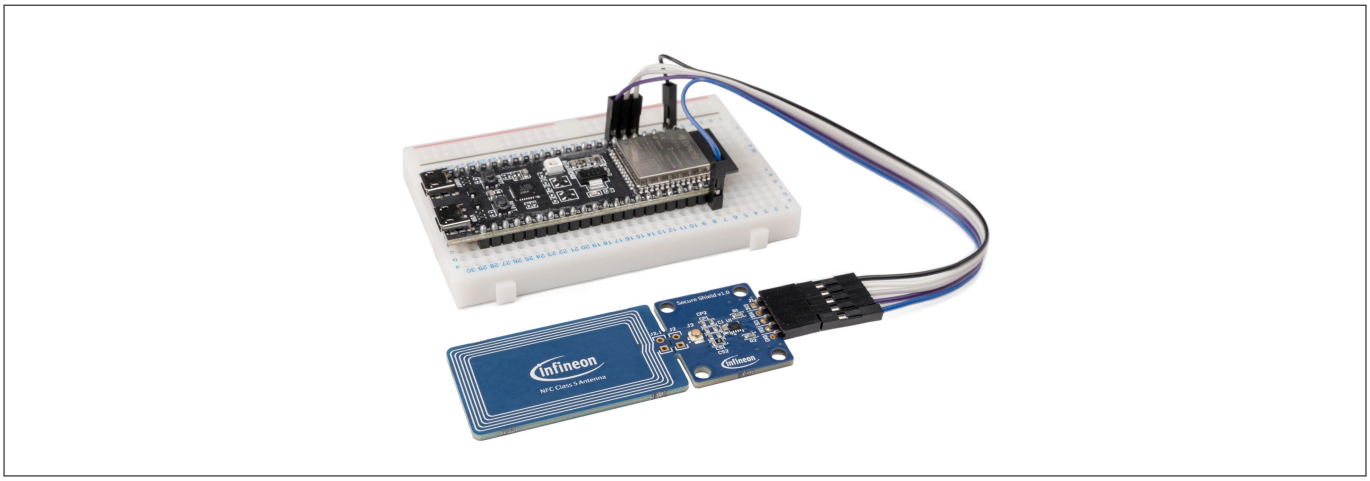

Figure 15 **Attaching the NBT Shield to a custom host microcontroller board using the five-pin jumper wire**

3.3.2 Rework for flexible shield placement

The provided five-pin cable can be used to connect to a custom microcontroller, additionally to position the OPTIGA™ Authenticate NBT Shield away from the microcontroller (for example, to allow easier access). The following steps must be taken:

- Detach (break away) the CY8CPROTO-062S2 Adapter
- Solder the five-pin jumper cable to the NBT Secure Shield's pins and connect the cables to the corresponding pins on the CY8CPROTO-062S2 Adapter

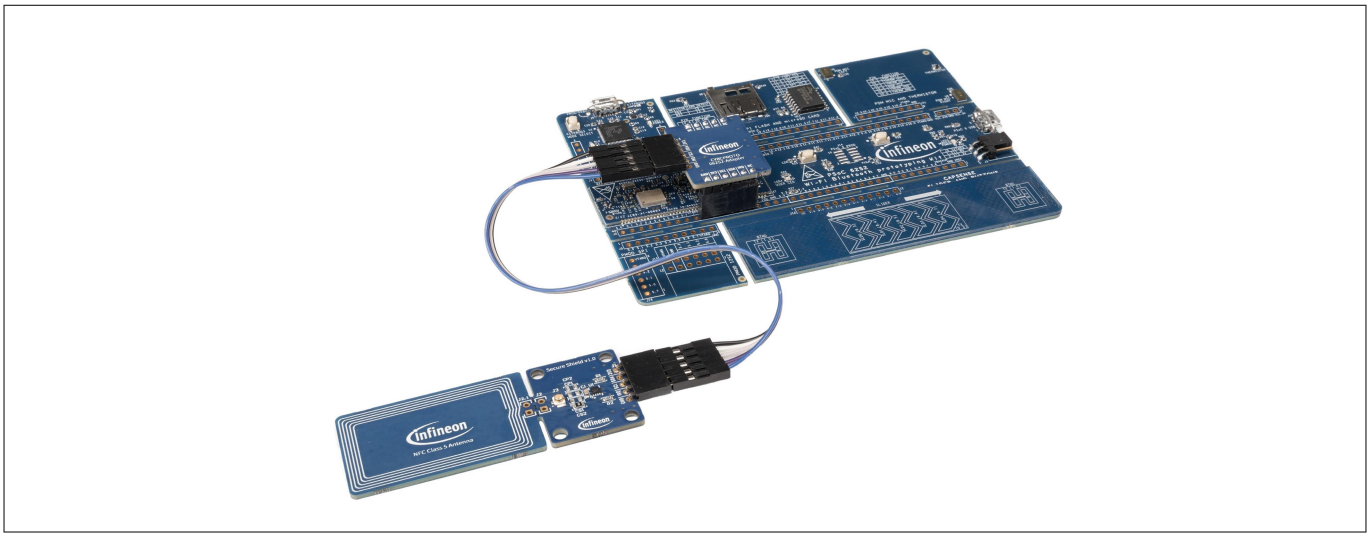

Figure 16 **Using the five-pin cable for flexible shield placement**

3.3.3 Rework for Class 6 shield antenna

To use the Class 6 shield antenna with the NBT Secure Shield, perform the following steps:

- Detach (break away) the Class 5 shield antenna from the OPTIGA™ Authenticate NBT Shield
- Connect the NBT Secure Shield and the Class 6 shield antenna (in its default configuration, see Figure 17) using the included 10 cm UMCC cable

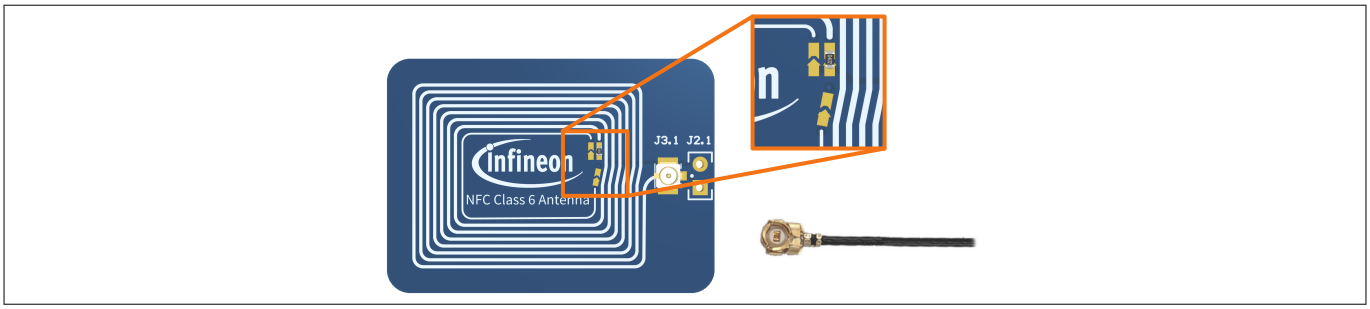

Figure 17 Class 6 shield antenna in its default configuration with the 10 cm UMCC cable (7 turns)

In addition, the antenna board can be directly connected to the NBT Secure Shield's L_A and L_B connectors (J2) using the two-pin header (J2.1). In this case, an optional 8th winding on the Class 6 shield antenna board must be activated. By closing dedicated solder bridges (see Figure 18), the additional winding is activated. When connecting to the antenna via the two-pin connector instead of the UMCC cable, this mitigates detuning of the system's resonance frequency.

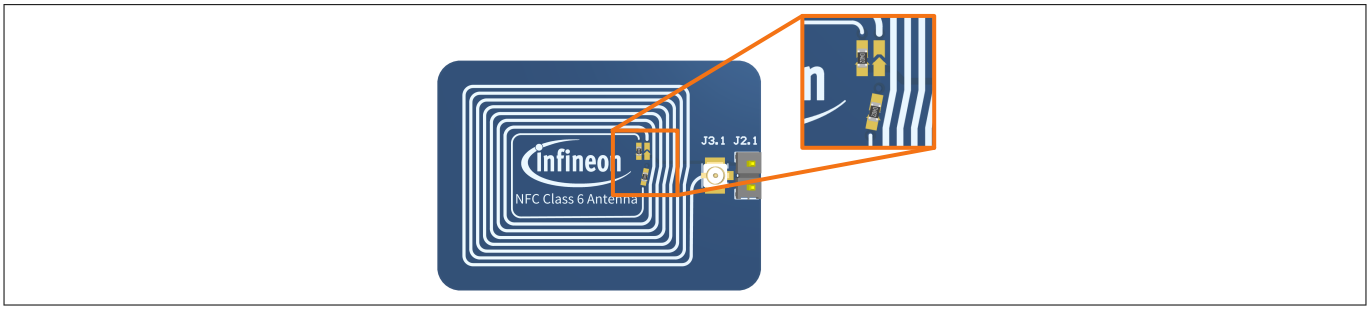

Figure 18 Class 6 shield antenna in its alternative configuration for direct mounting (8 turns)

***Note**: The NBT Secure Shield's matching circuit is optimized for use with the Class 5 shield antenna (direct two-pin connection) or the Class 6 shield antenna (flexible cable connection). Any other configuration (for example, a twisted pair cable connection) necessitates an update to the NBT Secure Shield's matching circuit to achieve the best performance.*

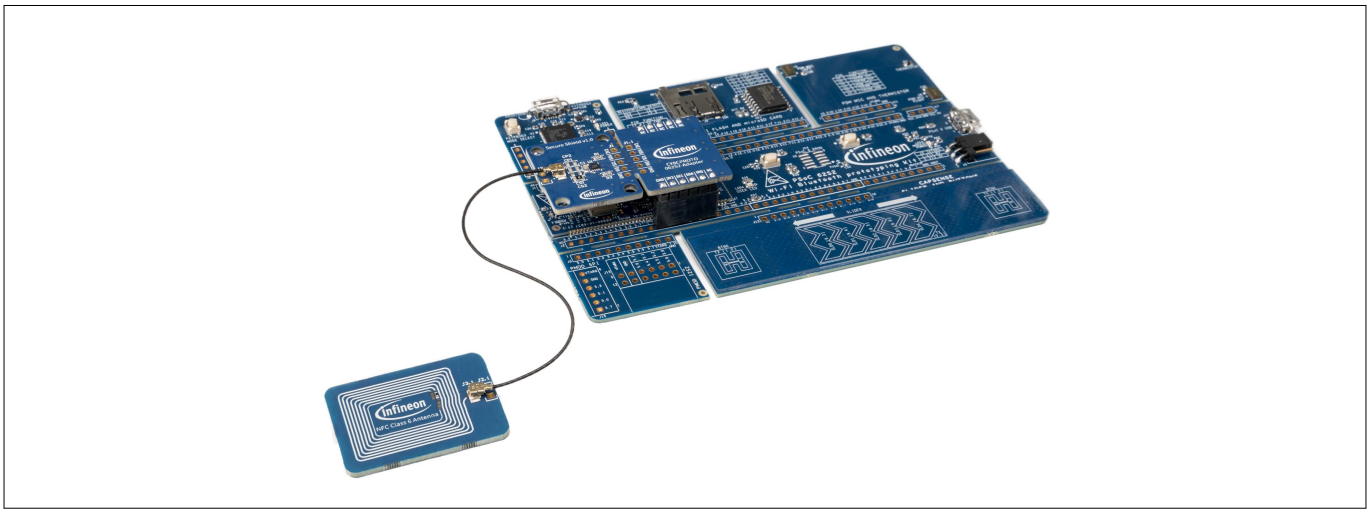

Figure 19 Example of using the Class 6 shield antenna with the OPTIGA™ Authenticate NBT Development Kit

References

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

[2] Infineon Technologies AG: *OPTIGA™ Authenticate NBT, GitHub overview repository* - github.com/Infineon/optiga-nbt

[3] Infineon Technologies AG: *OPTIGA™ Authenticate NBT Development Kit* - https://www.infineon.com/OPTIGA-Authenticate-NBT-Dev-Kit

[4] Infineon Technologies AG: *OPTIGA™ Authenticate NBT Development Shield* - https://www.infineon.com/OPTIGA-Authenticate-NBT-Dev-Shield

[5] Infineon Technologies AG: *PSoC™ 62S2 Wi-Fi BT Prototyping Kit* - www.infineon.com/cms/en/product/evaluation-boards/cy8cproto-062s2-43439

[6] Infineon Technologies AG: *PSoC™ 62S2 Wi-Fi BT Pioneer Kit* - www.infineon.com/cms/en/product/evaluation-boards/cy8ckit-062s2-43012

[7] Infineon Technologies AG: *Modus Toolbox* - www.infineon.com/cms/de/design-support/tools/sdk/modustoolbox-software/

[8] Infineon Technologies AG: *OPTIGA™ Authenticate NBT, Development Shield Guide (latest revision)*

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

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

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

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

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

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

Glossary

BoM
bill of materials (BoM)

BT
Bluetooth (BT)
A short-range wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances.

CC
capability container (CC)

I2C
inter-integrated circuit (I2C)

IDE
integrated development environment (IDE)
A software application that combines multiple tools used for software development into a single environment.

ID
identifier (ID)

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

iOS
iPhone operating system (iOS)
A mobile operating system created and developed by Apple Inc. exclusively for its hardware.

IoT
Internet of Things (IoT)

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)

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

NFC
near field communication (NFC)

NFCT4T
NFC Type 4 Tag (NFCT4T)

PCB

printed circuit board (PCB)

PSoC™ microcontroller

A range of general-purpose MCUs built on an ultra-low-power architecture ideal for battery-operated, low-power applications including embedded IoT applications.

SCL

serial clock line (SCL)

SDA

serial data line (SDA)

UID

unique identifier (UID)

UMCC

ultraminiature coax connector (UMCC)

USB

universal serial bus (USB)

Revision history

Reference	Description
Revision 2.1, 2024-05-03	
All	Editorial changes
Revision 2.0, 2024-03-28	
All	Major customer release
Revision 1.1, 2023-08-16	
All	Editorial changes
Revision 1.0, 2023-08-11	
All	Initial release

Trademarks

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

Edition 2024-05-03

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-psm1681281379200

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.