WHITEPAPER

Bridging the gap between secured contactless authentication and configuration in the IIoT

www.infineon.com/OPTIGA-Authenticate-NBT

Table of contents

Bridging the gap between secured contactless authentication and configuration in the Industrial Internet of Things

Having the ability to securely communicate with industrial devices like sensors, actuators and remote process controllers is critical for smart factory managers looking to harness the advantages of machine learning (ML) and artificial intelligence (AI) to improve production efficiency.

Equally, they need to be certain that their equipment and parts are authentic and can be trusted to operate as designed. As the Industrial Internet of Things (IIoT) proliferates, managers are also increasingly faced with the challenges of having to manually configure multiple devices to allow them to connect to factory networks while also keeping them sufficiently secured so that they don't become vulnerable to attack from intruders seeking to access sensitive process data or even disable production completely.

This white paper firstly reviews the limitations of current approaches used for configuring and securing industrial devices that make them unnecessarily large and difficult to manage, resulting in increased costs. Next, it shows how Infineon has brought together two tried and trusted technologies – Near Field Communication (NFC) and I2C – to create OPTIGA™ Authenticate NBT, a high-performance NFC-I2C bridge tag designed to enable secured contactless authentication and configuration of industrial equipment. It discusses the enhanced communication and security features of OPTIGA™ Authenticate NBT and how it can be used to authenticate headless devices using an ultra-fast and flexible interface that simplifies configuration and the safe transfer of data in various industrial use cases.

Limitations of current device configuration techniques

Pairing and configuration of industrial devices involves multiple steps which typically include interpreting instructions shown on a graphical display before providing inputs via several buttons and knobs/dials. This can make for a highly unsatisfactory user experience, especially since users are required to comprehend the configuration requirements for many different types of equipment, each with their own interfaces and menu options. For machine and equipment manufacturers, this approach also has the disadvantage of significantly increasing costs because they are expected to include a display as well as buttons and knobs for device configuration. These not only add to the bill of materials (BoM) but also place a de-facto lower limit on device form factor because space for a readable display and sufficiently large controls that can be touched comfortably must be accommodated in the design of a device.

During configuration, users can also often neglect to set up security features required to adequately protect a piece of equipment, and this can increase the risk of unauthorized access, data breaches, and compromises system integrity and reliability. Having the ability to authenticate of machines and equipment connecting to their networks is especially important for factory managers since counterfeit devices could potentially come preloaded with malware or other nefarious features that can threaten the brand reputation of equipment manufacturers (whose original equipment has not been recognized as having been cloned) as well as compromising safe factory operation.

NFC Type 4 Tag and I2C come together to enable seamless connection and configuration

NFC is a standards-based, secured contactless communication technology that allows devices which are in close proximity to each other to exchange data using a base signal frequency of 13.56 MHz. Today, NFC is enabled in over a billion smartphones and enjoys native support from mobile operating system platforms like iOS and Android. Widespread device adoption coupled with ease of use has resulted in the widespread deployment of NFC tags in a growing number of commercial and consumer technologies.

The potential benefits which these technologies can bring to industrial use cases are being increasingly recognized. NFC Forum defines 5 basic tag types represented as TxT with x representing either of the value from 1,2,3,4,5 with each tag type having a different format and capacity. OPTIGA™ Authenticate NBT being Tag 4 Tag is compatible with ISO/IEC14443 Type A standard and can be preconfigured during manufacture to be either read-only or rewritable. Type 4 Tags support communication rates between 106 kbit/s and 848 kbit/s. I2C is a serial communication protocol used to connect multiple electronic components on a single shared communications bus. It supports multi-controller and multi-target configurations and allows communication at various data transfer rates – standard mode (100kHz), fast mode (400kHz) and fast mode plus (1MHz).

Bringing NFC Type 4 Tag and I2C technologies together to create an NFC-I2C bridge tag can enable seamless data transfer between an NFC-enabled smartphone (or reader) and the MCU in an IIoT device. A significant advantage of this approach for industrial equipment manufacturers is that it enables “headless” designs (i.e. devices that do not have a display or other controls) resulting in significant space and cost savings due to smaller form factors. Furthermore, this type of bridge could also facilitate the implementation of robust security measures that only allow authorized personnel to configure or activate a device. Other industrial use cases include device pairing, configuration, activation and data logging. A later section in this paper discusses the benefits of each and how they can be implemented.

Use cases for secured IIoT device activation and configuration

Infineon's OPTIGA™ Authenticate NBT (Figure 1) is a high-performance single-tap NFC-I2C bridge tag for secured contactless device authentication and configuration which enables communication (106 kbit/s up to 848 kbit/s) between an NFC Type 4 Tag interface and an I2C connected host MCU. Supported I2C modes include standard mode (100kHz), fast mode (400kHz) and fast mode plus (1MHz). The higher communication rate enables ultra-fast data exchange even with large data volumes for a seamless user experience – a key bonus for demanding applications. In conjunction with the MCU, the bridge tag facilitates a secured communication channel for device activation and configuration use cases.

OPTIGA™ Authenticate NBT features multiple security options. It is based on CC EAL 6+ (high) certified hardware and provides high security thanks to our acclaimed Integrity Guard 32 security architecture. The chip includes a substantial 8 KB non-volatile memory (NVM) file system (to support large data volumes) with flexible file-based password management, asymmetric cryptography (NIST P-256) authentication with public key infrastructure (PKI) and certificates. It also features AES-128 based symmetric cryptography, with on-chip generated dynamic URL and online CMAC verification with every tag chip featuring a pre-provisioned certificate (UID based with individual key-pair and certificate). This offers customers the ability to customize their security settings, allowing them to update their certificates, as well as their AES and ECC keys. The hardware and the cryptographic library in this tag also have common criteria for EAL 6+ certification.

The OPTIGA™ Authenticate NBT can be powered from an NFC reader via a coil antenna connected to its contactless interface pads (LA, LB). In addition to the NFC interface, the device can also derive power from an external power supply (VCC, GND). Then, the integrated I2C target interface and the IRQ can be connected to external host systems to exchange data.

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. The tag supports open standards that allow for flexible application development (Java Card OS and applets, I2C, Global Platform T=1' over I2C). A tiny USON8 package (2mm x 2mm x 0.55 mm) combined with high 78 pF on-chip tuning capacitance, allows a designer to shrink antenna size considerably.

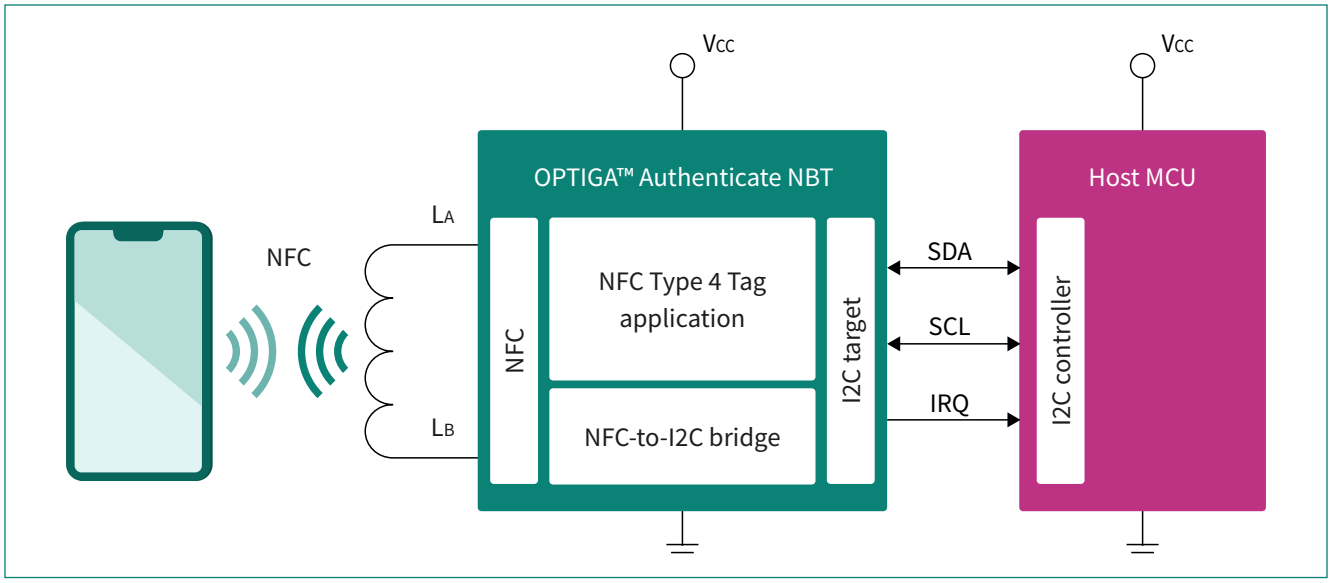

Figure 1 Infineon's OPTIGA™ Authenticate NBT supports secured contactless device authentication and configuration between an NFC application and I2C controller

OPTIGA™ Authenticate NBT supports multiple modes of operation

Authentication mode

The OPTIGA™ Authenticate NBT in authentication mode can be used for chip (NFC tag) verification. This mode is further sub-divided into offline authentication mode and online authentication mode. When OPTIGA™ Authenticate NBT is attached to an accessory or a device, a possible use case of this mode could be brand protection. Following are the two options through which brand protection can be achieved using OPTIGA™ Authenticate NBT.

Brand protection using ECDSA authentication – Offline authentication mode

The OPTIGA™ Authenticate NBT can provide brand protection by enabling a machine or some other piece of industrial equipment to authenticate a disposable or accessory which it uses. This approach (Figure 2) uses public key infrastructure (PKI) to eliminate the requirement for a cloud connection or other online services. Users wishing to validate the authenticity of a piece of equipment can tap the OPTIGA™ Authenticate NBT-equipped NFC tag included with a typical NFC-enabled mobile phone (running either the Android or iOS operating systems) executing the brand's product authentication application. The mobile application retrieves the public key certificate from the NFC Data Exchange Format (NDEF) message in the OPTIGA™ Authenticate NBT and validates it by utilizing the application's Root CA (certificate authority). In addition, the brand protection application may visually notify the end user of the result of the authentication process. As a second step, the application transfers a challenge to the OPTIGA™ Authenticate NBT which then computes a signature based on the elliptic curve digital signature algorithm (ECDSA) using the private brand protection signing key (BSK) stored in its secured key store. The signature reverted to the OEM application is then used to verify if the product is authentic.

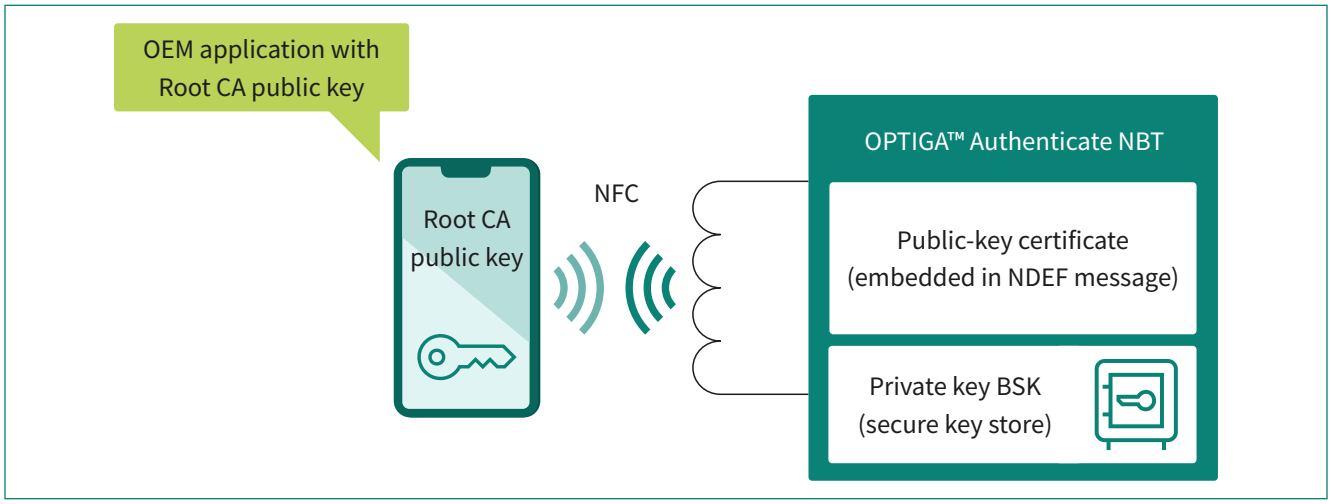

Figure 2 Infineon's OPTIGA™ Authenticate NBT offline authentication mode using PKI

Brand protection using AES-128-CMAC-based cryptographic one-time token (COTT) – Online authentication mode

Online authentication mode (Figure 3) can be used to verify the authenticity of a product by connecting to the brand's cloud service, which is accessible through the web browser of an NFC-enabled mobile phone. A user taps the branded item with the NFC-enabled mobile phone. The phone automatically detects the presence of the OPTIGA™ Authenticate NBT (a dedicated smartphone app is not required) and reads the NDEF message, containing a dynamically generated URL pointing to the web service and forwards the embedded cryptographic one-time token (COTT) value to the cloud authentication service. This verifies the authenticity of the tagged item with the result being returned and displayed by the web browser app on the phone. The web service can provide additional product-related information, like for example, manufacturing or purchase-related information.

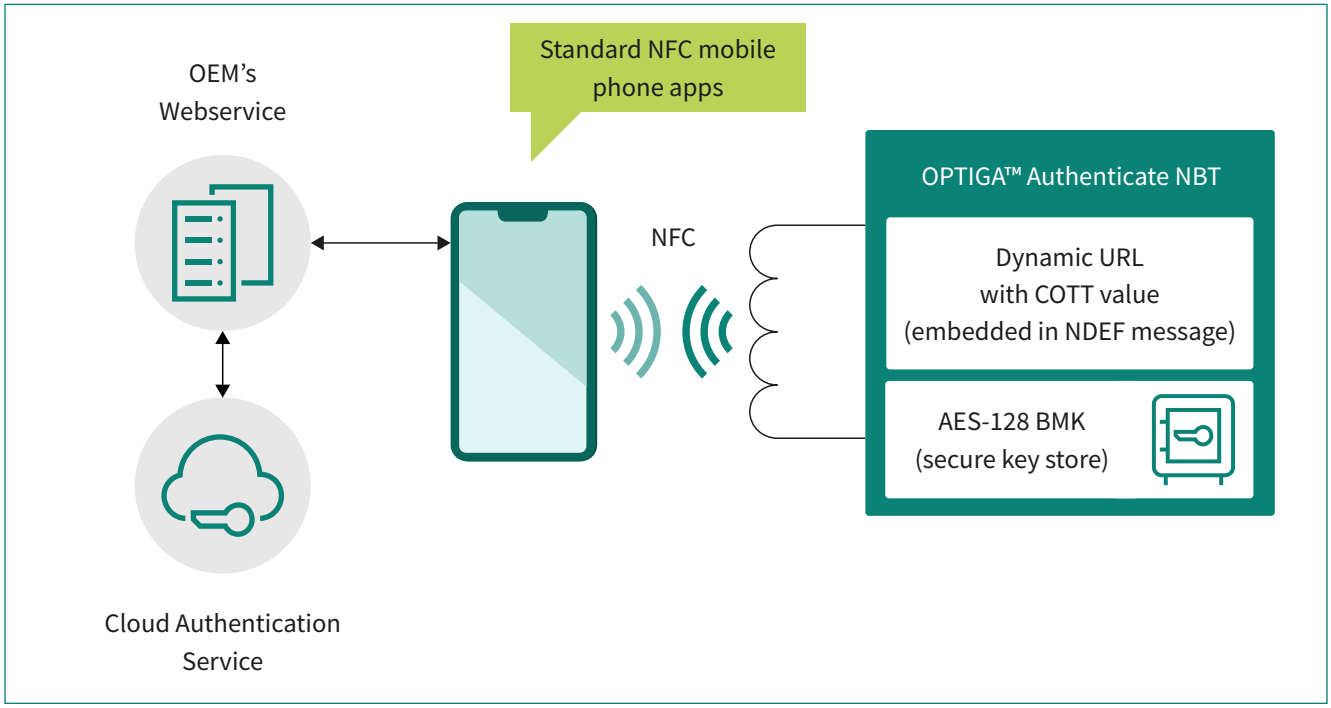

Figure 3 Infineon's OPTIGA™ Authenticate NBT online authentication mode using COTT

Pass-through mode

Pass-through (PT) mode enables synchronous data transfer between a remote NFC device (e.g. a mobile phone) and a host MCU via the NFC and I2C interfaces to facilitate use cases such as host parametrization or host card emulation. The pass-through mode also allows the downloading of a firmware update to a host system, configuring or controlling headless devices, card application emulation, keyless access to shared devices by authorized personnel and activation of critical electronic devices. The pass-through example use case shown in Figure 4, shows an OPTIGA™ Authenticate NBT and host MCU, communicating with an NFC-enabled mobile phone. The OPTIGA™ Authenticate NBT handles the NFC protocol for the mobile phone, which is used to transfer configuration data to the host. The NFC-enabled mobile phone tries to select an application using an AID that is not registered on the OPTIGA™ Authenticate NBT but is emulated by the host MCU. When the OPTIGA™ Authenticate NBT is configured for pass-through mode, this selection request is automatically routed to the host.

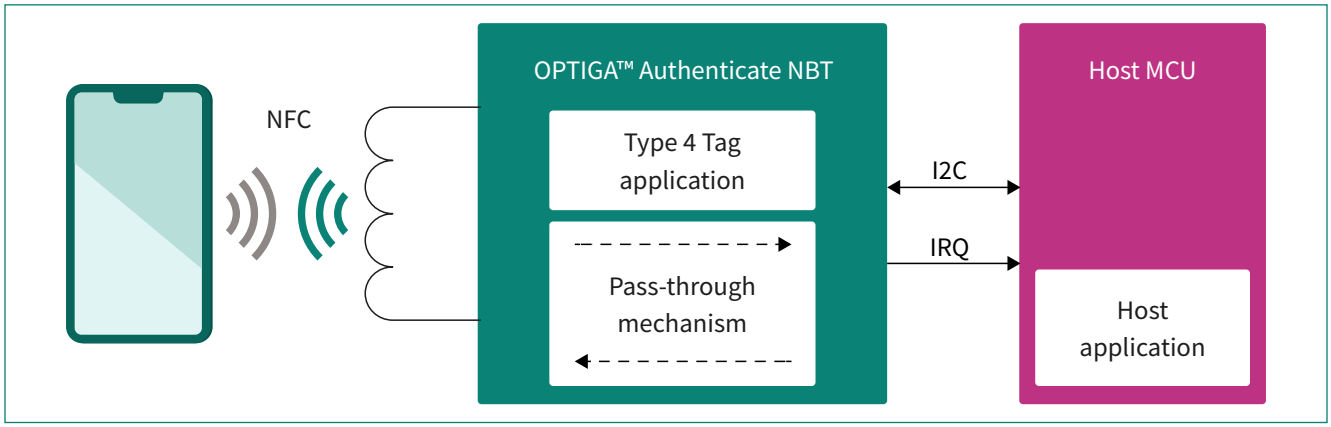

Figure 4 Using pass-through mode for host parametrization

Asynchronous data transfer mode

The OPTIGA™ Authenticate NBT also supports an asynchronous data transfer (ADT) mode which can be used for transferring and storing data when the I2C and NFC interfaces are not available for communication at the same time (Figure 5). The OPTIGA™ Authenticate NBT's file system allows information to be received via one of its interfaces (I2C or NFC), stored in a dedicated file, and transferred at another point in time via the other interface once it becomes available. This mode can allow offline configuration of sensors/actuators before they are installed in the field, as well as fault diagnosis and status read-back of data logs of offline equipment at the exact moment a failure or power outage occurred.

Other ADT use cases include passive configuration of headless equipment and obtaining/storing of Bluetooth/Wi-Fi pairing data. In the use case shown in Figure 5, the NFC-enabled mobile phone writes configuration data to the host. The OPTIGA™ Authenticate NBT stores this data in dedicated "mailbox" files, which the host can retrieve later via the I2C interface. These mailbox files can be optionally password-protected to restrict access from either the NFC and/or host MCU sides.

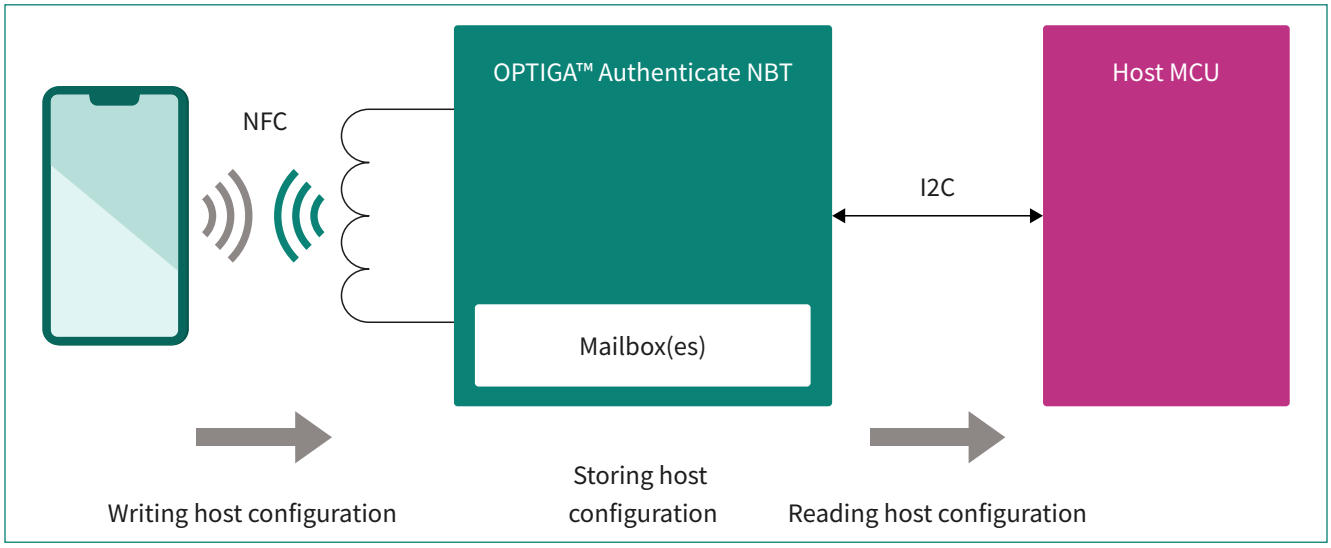

Figure 5 Host parametrization using asynchronous data transfer (ADT) mode

Static connection handover

NFC connections can be easily established in situations where there is a relatively small distance between the communicating parties. However, this scenario can't always be guaranteed, meaning NFC is not suitable where persistent connections or large data transfers are required. In these circumstances, switching to alternative data communication protocols makes sense.

The OPTIGA™ Authenticate NBT supports a static handover mode which manages connection handover from NFC to alternative wireless data carriers like Bluetooth or Wi-Fi. Specific records in the tag's NDEF message indicate the device's ability to support connection handover to alternative carriers. Both, Android and iOS NFC-enabled devices, provide services for automatically detecting NFC tags and reading their NDEF message. The mobile phone may choose one of the alternative carriers to continue data transmission with the host device. In the use case shown in Figure 6, the connection information is stored statically in the NDEF file of the Type 4 Tag application, meaning the OPTIGA™ Authenticate NBT used for static connection handover does not require a connection to a host. However, if the OPTIGA™ Authenticate NBT is connected to a host MCU via the I2C bus interface, an "in-field update" of connection information is also possible. In this case, the host can be used to modify the Wi-Fi credentials of a Wi-Fi router (for example) by modifying connection information such as the SSID and/or passphrase.

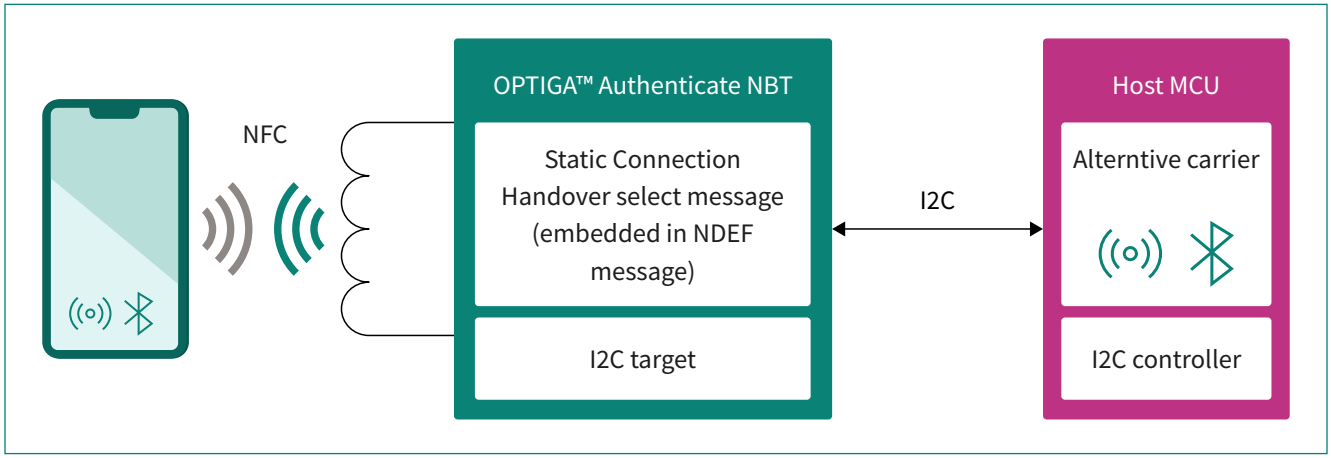

Figure 6 Static connection handover components

OPTIGA™ Authenticate NBT Design Resources and Supporting Collaterals

Infineon offers a comprehensive suite of tools, documentation and other supporting collateral to enable quick and easy evaluation and development of new use cases for the OPTIGA™ Authenticate NBT in industrial applications.
These resources include:

OPTIGA™ Authenticate NBT Development Kit

The OPTIGA™ Authenticate NBT Development Kit bundle (Figure 7) includes the CY8CPROTO-062S2-43439 main board, an OPTIGA™ Authenticate NBT eval shield, a Class 6 antenna and all associated software is ideal for quick and simple evaluation of OPTIGA™ Authenticate NBT using the example applications available through Infineon's GitHub repository (Android, iOS and embedded PSoC™ applications are available). The kit also simplifies the development of custom applications using Infineon's PSoC™ host MCUs based on the reference applications. Alternatively, by detaching the adapter board, the shield can also be used separately for application development using MCUs other than PSoC™. Examples of industrial use cases that this kit can easily evaluate include configuration and parametrization of electric relay switches, circuit breakers, etc.

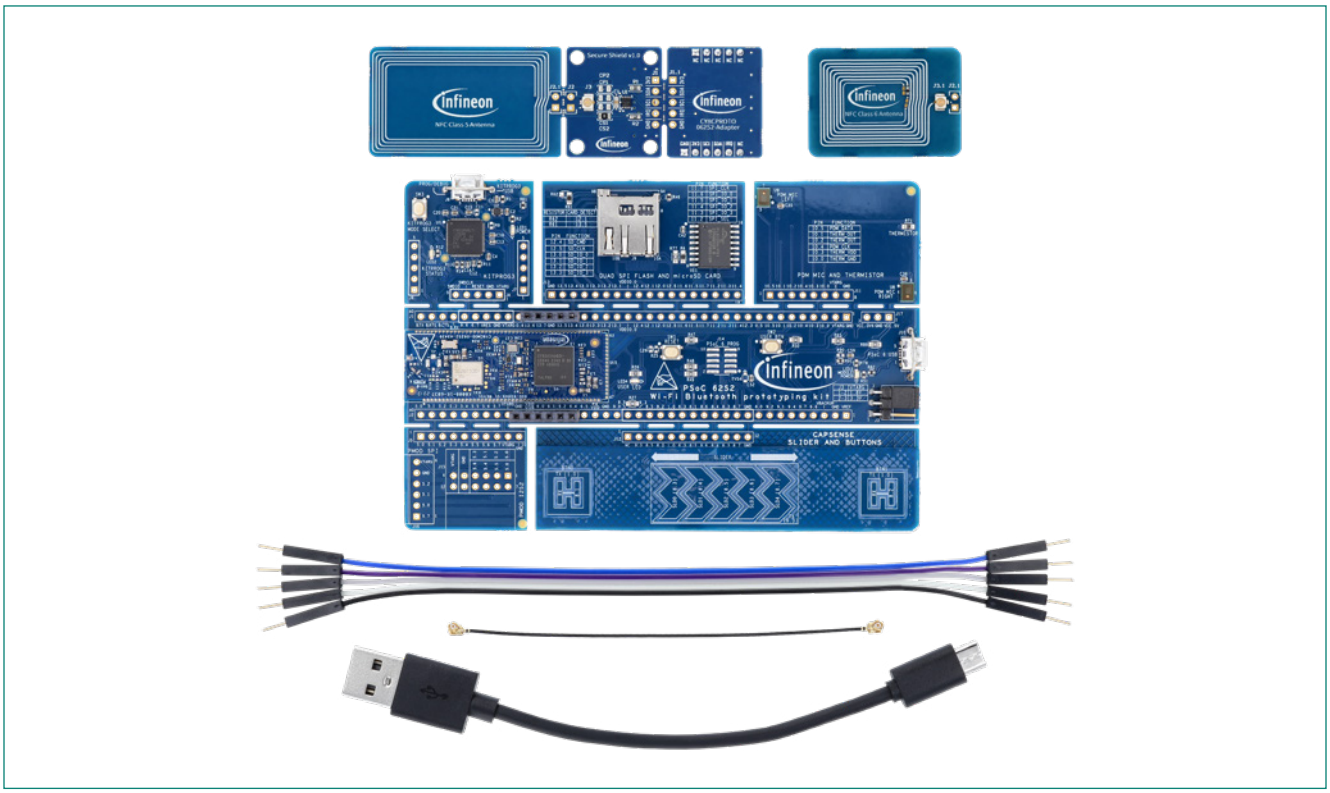

Figure 7 OPTIGA™ Authenticate NBT Development Kit

OPTIGA™ Authenticate NBT Development Shield

The OPTIGA™ Authenticate NBT Development Shield bundle (Figure 8) is ideal for evaluation and application development using custom MCU boards. The shield's default adapter enables easy attachment to Arduino UNO-compatible MCU boards, a quick and easy option for adapting and evaluating reference applications and host libraries.

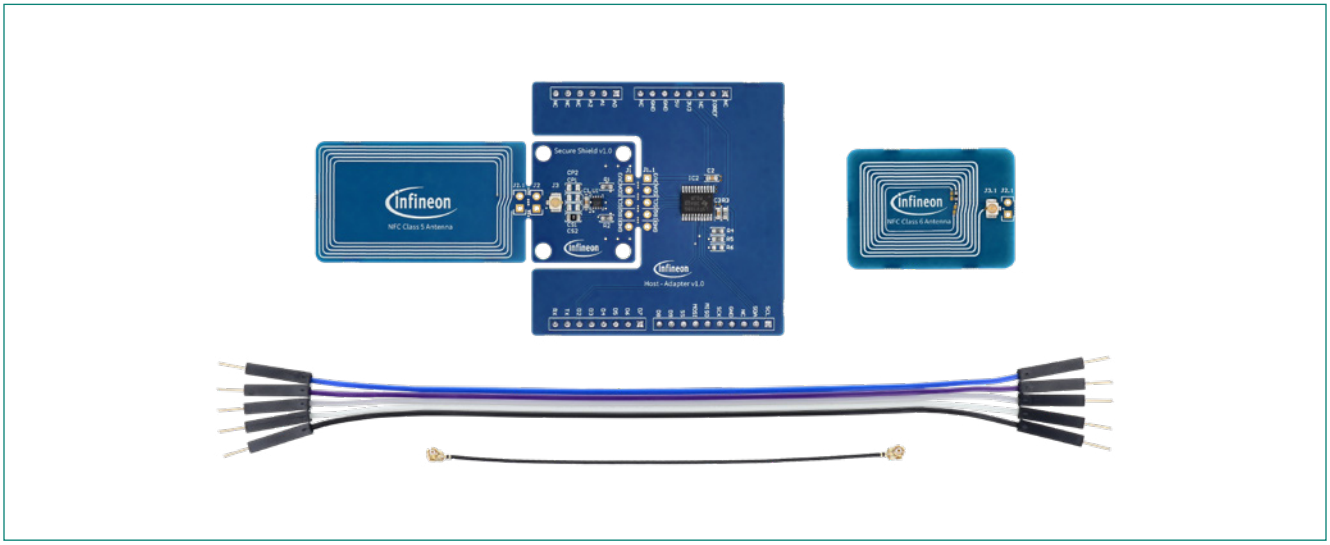

Figure 8 OPTIGA™ Authenticate NBT Development Shield

The accompanying documentation describes the functionality and components of the OPTIGA™ Authenticate NBT Development Kit/Shield bundle. It presents a quick and easy way to evaluate the functionality of the OPTIGA™ Authenticate NBT and also provides example applications. It is intended to assist end-users in setting up, using, and operating the evaluation hardware so that users can explore the capabilities of the OPTIGA™ Authenticate NBT itself.

Like other devices in the OPTIGA™ family, the OPTIGA™ Authenticate NBT offers flexibility with its interfaces, robust security, ease of use and is backed by Infineon's continuous commitment to quality, supply and support in scaling from basic authentication chips to sophisticated system-level security implementations.

Conclusion

Configuring industrial automation equipment has traditionally been time-consuming and difficult, typically requiring the use of unwieldy screens, knobs and pushbuttons. This approach has resulted in devices being unnecessarily large and not always properly secured against threats from third parties. Infineon recognized these shortcomings and has now brought together two proven technologies – NFC and I2C – to create OPTIGA™ Authenticate NBT, a high-performance NFC-I2C bridge tag which enables secured contactless authentication and configuration of headless industrial devices with considerably smaller form factors. The communication and security features of OPTIGA™ Authenticate NBT can be used to authenticate devices, using an ultra-fast, flexible and secured interface that simplifies configuration and enables safe transfer of data in various industrial use cases. OPTIGA™ devices are designed for easy integration into embedded systems and to provide robust protection of the confidentiality, integrity and authenticity of information and devices. Infineon is a trusted adviser with over 30 years of expertise in hardware security and assisting its customers in reducing system complexity and implementation costs.

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

Public

Version: V1.0_EN
Date: 09/2024

Stay connected!

Scan QR code and explore offering
www.infineon.com

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our 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 us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.