Enabling Bluetooth out-of-band pairing through NFC

Bluetooth pairing

Many services offered over Bluetooth can expose private data or let a connecting party control the Bluetooth device. Security reasons make it necessary to recognize specific devices, and thus enable control over which devices can connect to a given Bluetooth device.

To address this challenge, Bluetooth uses a process called bonding, and a bond is generated through a process called pairing. The pairing process is triggered either by a specific request from a user to generate a bond (for example, the user explicitly requests to "Add a Bluetooth device") or automatically when connecting to a service where the identity of a device is requested for the first time.

Pairing often involves some level of user interaction to confirm the identity of the devices. When pairing successfully completes, a bond forms between the two devices, enabling those two devices to connect to each other in the future without repeating the pairing process to confirm device identities.

During pairing, the two devices establish a relationship by creating a shared secret known as a link key. If both devices store the same link key, they are said to be “paired” or “bonded”. A device that wants to communicate with a bonded device can cryptographically authenticate its identity, ensuring it is effectively the device it previously paired with. Once a link key is generated, the devices can exchange data through an authenticated Asynchronous Connection-Less (ACL) link that may be encrypted to protect the transferred data against eavesdropping (a.k.a. man in the middle attacks).

Out-of-Band pairing

Bluetooth pairing is widely perceived as an inconvenient process. Users trying to connect an accessory to their phone often need to refer to the manual to understand how to make the new device discoverable. Security can even be compromised because few users change the factory default passkey to a number that potential hackers can guess easily. This process is difficult enough when the equipment has its own user input devices like buttons or switches. In a device like an IoT smart sensor having no display nor keyboard, it might even be impossible.

To help overcome pairing difficulties, the Bluetooth SIG introduced Secure Simple Pairing (SSP) from Bluetooth 2.0 onwards. SSP specifies four association models:

- Just Works
- Numeric Comparison
- Passkey Entry
- Out-of-Band (OOB)

Passkey Entry and Numeric Comparison require the user to enter a code or confirm that two codes are identical. Just Works pairing uses the same protocol as Numeric Comparison but requires no user confirmation. Although this could be used to pair a device with no user interface keys or display, it provides no protection against eavesdropping. OOB is thus the most suitable model for connecting devices that have no user interface in a secure way: instead of sharing the secret keys over the 2.4 GHz band used by the BLE protocol, it makes use of other mediums intrinsically hardened against eavesdropping.

OOB through NFC

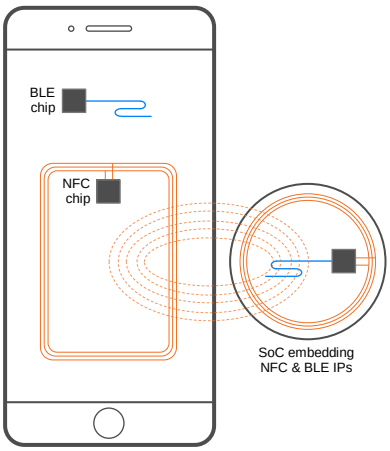
Near Field Communication (NFC) can be used to share the data needed for OOB pairing, and thus provides a convenient and secure means of establishing Bluetooth connections. Indeed, the short communication range of NFC contributes to both security and selectivity. Remote attacks are not possible when the unauthorized party needs to be physically present within a few centimeters of the equipment, and tapping allows the user to be quite sure that only the device to be connected has received the key.

NFC pairing is natively supported by most mobile operating systems (Android, iOS, KaiOS…) and has greatly simplified use for consumers by allowing “tap to pair” convenience when introducing new accessories like a headset or speakers to a smartphone.

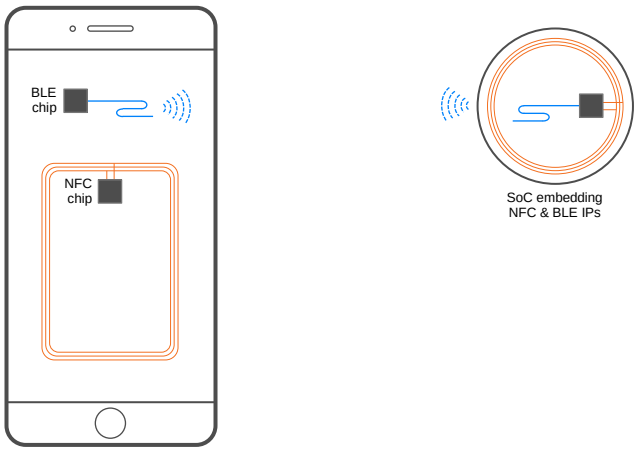
Taking advantage of built-in security provisions, NFC can be used to aid Bluetooth pairing of smart sensors without trading away any of the advantages of ubiquity that come with the widespread native BLE support on smartphones and tablets.

In addition to helping introduce new devices to the network securely, NFC can help facilitate other interactions with headless IoT devices. Some examples include removing a device from the network, replacing an old device with a new one and sending configuration data or retrieving information when the Bluetooth connection is not active. NFC also provides a means of waking up a device that has been fully powered down to maximize battery life, and helping it connect to a Bluetooth network.

NFC allows the passive device to harvest energy from the electromagnetic field. Therefore a passive NFC transceiver can communicate with a reader when the host system is powered down, data such as the network parameters and passkey needed to connect the device securely can be transferred to the device before it is powered up for the first time. This can be done by tapping the new device against an NFC-enabled smartphone or a gateway device such as a home automation hub. When the object is subsequently powered up, it can use the key to connect with the network and establish secure communication. The key is then deleted from the tag to prevent interception by a third party. Similarly, an NFC-enabled smartphone registered with the device can be used to connect headless devices to the network by tapping. Other commands such as resetting or decommissioning a device from the network can be accomplished the same way, and it is also possible to copy configuration settings from one device to another by tapping, aiding replacement or renewal of old equipment.



1. Tag wake-up and key transfer via NFC



2. Encrypted communication via BLE

The Bluetooth SIG and NFC Consortium have made provision for the two technologies to interoperate for purposes such as pairing devices and initiating communications to establish a Bluetooth connection. Not only do the current Bluetooth standards support OOB pairing to leverage the strengths of a standard like NFC, but also the NFC specification includes features for connecting devices to a network such as Bluetooth or Wi-Fi. There is also a protocol for connection handover, which allows a graceful transfer to Bluetooth immediately after pairing.

These features included in the two specifications allow NFC to be used for several purposes, including selecting a Bluetooth device, initiating a secure connection to a Bluetooth device, or starting an application on a Bluetooth device.

NFC simplifies device selection by eliminating the Bluetooth discovery procedure, which can require the user to select the desired device manually from a list containing any other devices within range. In this case, NFC allows the Bluetooth address to be captured directly from the tapped device.

When using OOB pairing to connect a Bluetooth device, NFC can be used to communicate the temporary key needed by BLE devices during the process. The key is included in the payload of a standard NDEF (NFC Data Exchange Format) message. After the OOB data has been exchanged, developers can take advantage of other features included in the Bluetooth specification to minimize the time to finish setting up the connection. One example is the support for fast connection establishment, which is included in the generic access profile (GAP). The GAP defines the procedures for Bluetooth devices to advertise, find each other, connect, and handle security.

The application document Bluetooth® Secure Simple Pairing Using NFC, published jointly by the NFC Forum and Bluetooth SIG, provides in-depth information about the interactions between devices and the handover mechanisms between NFC and Bluetooth.

Invia's contribution

To implement NFC pairing and NFC triggered host wake-up, the device shall embed both a BLE transceiver and a NFC transceiver supporting the card-emulation mode (a.k.a. smart card or tag modes). While these could be implemented as separate ICs, an integrated solution combining both transceivers offers a more small, cost effective and power-conscious solution.

In card-emulation mode, a NFC device behaves like a contactless smart card. For the lowest communication speed specified by the NFC standard (106 kbit/s), the card-emulation mode is totally compatible with the ISO 14443 Type A standard initially developed for smart card products.

At Invia, a semiconductor design house of the Thales Group, we design secure ICs for the most stringent applications. To enable the IoT, Invia's RF team conceives NFC-compliant transceivers based on various technologies and already deployed in million devices. Such transceivers are available as silicon IPs for integration in ASICs or SoCs; we deliver both analog front-ends and the digital controllers.

Invia is your partner of choice for the integration of NFC and security functionalities.

Conclusion

NFC helps connecting smart sensors with little or no user interface to a Bluetooth network. The Bluetooth SIG and NFC Forum have cooperated to make provision for NFC assisted pairing, including support for connection handover in the NFC specification and OOB pairing in the BLE specification. The integration of BLE and NFC transceivers streamlines this solution by combining the two technologies in one device. Last but not least, the supporting SDK provides software developers what they need to start pairing headless devices in a timely manner.

References

[1] Bluetooth® Secure Simple Pairing Using NFC - Version 1.2, NFC Forum, May 31, 2019

[2] Bluetooth Core Specification - Bluetooth Pairing Part 5: Legacy Pairing - Out of Band, Bluetooth SIG

[3] Leveraging Near Field Communication (NFC) to Connect with BLE Smart Sensors, Digi-Key's European Editors

[4] Bluetooth - Pairing and bonding - Motivation / Implementation, Wikipedia

[5] Deploying BLE and NFC for Secure Connections and Easy Pairing, Heiner Tendyck, eeNews Analog

[6] Understanding Bluetooth Security, Mark Loveless, Duo Security – Decipher, January 9, 2019

[7] Pairing Devices Using Data Exchanged in an Out-of-Band Channel, Motorola Solutions Inc