Bluetooth® Secure Simple Pairing Using NFC

Application Document

Version 1.2

2019-05-31

[BTSSP]

NFC Forum™

RESTRICTIONS ON USE

This License Agreement (Agreement) is a legal agreement between you and NFC Forum, Inc. a Delaware non-profit, non-stock corporation (collectively “Licensor”), which are the owners of the Application Document to which this Agreement is attached (“Application Document”). As used in this Agreement, "you" means the company, entity, or individual that is acquiring a license under this Agreement.

All copyrights in the Bluetooth Specifications are owned by Ericsson AB, Intel Corporation, Lenovo (Singapore) Pte. Ltd., Microsoft Corporation, Motorola Mobility, Inc., Nokia Corporation and Toshiba Corporation. Other third-party brands and names are the property of their respective owners.

By viewing, taking possession of or otherwise using the Application Document, you are agreeing that you will be bound by and are becoming a party to this Agreement. If you are an entity, and an individual is entering into this Agreement on your behalf, then you will be bound by this Agreement when that individual views, takes possession of, or otherwise uses the Application Document. When they do so, it will also constitute a representation by the individual that s/he is authorized to bind your entity as a party to this Agreement. If you do not agree to all of the terms of this Agreement, you are not authorized to view, take possession of, or otherwise use the Application Document.

1. LICENSE GRANT.

Licensor hereby grants Licensee the right, without charge, to copy (for internal purposes only) and share this Application Document with Licensee's members, employees and (to the extent related to Licensees use of this Application Document) consultants. This license grant does not include the right to sublicense, modify or create derivative works based upon the Application Document. This Application Document includes technology for which the Licensor has obtained licenses separate from the Application Document license [that Licensor grants Licensee] and any use of a commercial nature of the license granted herein will require necessary licenses obtained separately from Licensor.

2. NO WARRANTIES.

THE APPLICATION DOCUMENT IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL LICENSOR, ITS MEMBERS OR ITS CONTRIBUTORS BE LIABLE FOR ANY CLAIM, OR ANY DIRECT, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE APPLICATION DOCUMENT.

3. THIRD PARTY RIGHTS.

Without limiting the generality of Section 2 above, LICENSOR ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE APPLICATION DOCUMENT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE APPLICATION DOCUMENT, LICENSOR TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

4. FEEDBACK

If you are a member of either Licensor, Licensor would like to receive your input, suggestions, and other feedback ("Feedback") on the Application Document.

5. TERMINATION OF LICENSE.

In the event of a breach of this Agreement by Licensee or any of its employees or members, Licensor shall give Licensee written notice and an opportunity to cure. If the breach is not cured within thirty (30) days after written notice, or if the breach is of a nature that cannot be cured, then Licensor may immediately or thereafter terminate the licenses granted in this Agreement.

6. MISCELLANEOUS.

All notices required under this Agreement shall be in writing, and shall be deemed effective five days from deposit in the mails. Notices and correspondence to the NFC Forum and Bluetooth SIG, Inc. addresses as they appear below. This Agreement shall be construed and interpreted under the internal laws of the United States and the Commonwealth of Massachusetts, without giving effect to its principles of conflict of law.

NFC Forum, Inc.
401 Edgewater Place, Suite 600
Wakefield, MA, USA 01880

Updated December 29, 2018

Contents

Figures

Tables

1 Introduction

This Application Document provides examples for the implementation of Bluetooth Basic Rate / Enhanced Data Rate (BR/EDR) Secure Simple Pairing (SSP) and Bluetooth Low Energy (LE) Out-of-Band (OOB) pairing using NFC.

It is recommended that all NFC Forum members and Bluetooth SIG members refer to this Application Document when implementing Bluetooth OOB pairing using NFC.

Bluetooth SSP was introduced in Bluetooth Core Specification Version 2.1 + EDR, Bluetooth LE pairing was introduced in Bluetooth Core Specification Version 4.0 and Bluetooth LE Secure Connections pairing was introduced in Bluetooth Core Specification Version 4.2. Specific data formats might change in subsequent versions of the standard.

The format used for SSP related data exchange is the Extended Inquiry Response (EIR) format, which is described in Sections 3.1 and 3.2. The format used for Bluetooth LE OOB data exchange is the Advertising and Scan Response Data (AD) format, which is described in Sections 3.3 and 3.4. However, both the EIR and AD formats are specified by the Bluetooth Special Interest Group (SIG), and so either or both might be updated or changed independently of this document. Any conflict between the data format presentations made in this document and those defined by the Bluetooth SIG is resolved in favor of the Bluetooth SIG (as the originator of these formats).

1.1 Audience

The audience of this document is all NFC Forum members and Bluetooth SIG members who are interested in implementing the Bluetooth SSP or the Bluetooth LE pairing using NFC.

1.2 Applicable Documents or References

[BLUETOOTH_CORE]

Bluetooth Core Specification version 5.1 and later, Bluetooth SIG, January 21, 2019.

https://www.bluetooth.com/specifications/bluetooth-core-specification

In this document, references to sections or pages of the Bluetooth Core Specification refer to Version 5.1. Different paragraph numbers or page numbers might apply for different revisions of the Bluetooth Core Specifications.

[BLUETOOTH_CSS]

Bluetooth Core Specification supplement version 8 or later, Bluetooth SIG, January 21, 2019.

https://www.bluetooth.com/specifications/bluetooth-core-specification

In this document, references to sections or pages of the Bluetooth Core Specification supplement refer to Version 8. Different paragraph numbers or page numbers might apply for different revisions of the Bluetooth Core Specification supplement.

[BLUETOOTH_NUMBERS] Bluetooth Assigned Numbers, Bluetooth SIG, https://www.bluetooth.com/specifications/assigned-numbers

[CH] NFC Forum Connection Handover Technical Specification, NFC Forum

[NDEF] NFC Data Exchange Format, NFC Forum

[RFC2046] Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, RFC 2046 N. Freed, N. Borenstein, November 1996 Internet Engineering Task Force

[RTD] NFC Record Type Definition (RTD), NFC Forum

[URI_RTD] NFC URI Record Type Definition Technical Specification, NFC Forum

1.3 Administration

The Bluetooth® Secure Simple Pairing Using NFC Application Document is supported by the Near Field Communication Forum, Inc., located at:

401 Edgewater Place, Suite 600
Wakefield, MA, 01880

Tel.: +1 781-876-8955
Fax: +1 781-610-9864

http://www.nfc-forum.org/

The NFC Forum maintains this Application Document.

1.4 Name and Logo Usage

The Near Field Communication Forum's policy regarding the use of trademarks is described in the NFC Forum Brand Identity Guidelines and N-Mark Usage Guidelines, which can be found on the NFC Forum website.

1.5 Intellectual Property

The Bluetooth® Secure Simple Pairing Using NFC Application Document may contain elements that are subject to intellectual property rights of third parties. This document has not been submitted to an IPR Election pursuant to the NFC Forum IPR Policy, and therefore NFC FORUM MAKES NO REPRESENTATIONS WHATSOEVER REGARDING INTELLECTUAL PROPERTY CLAIMS BY NFC FORUM MEMBERS OR OTHER PARTIES. Such determination is the responsibility of the user.

1.6 Abbreviations

The abbreviations and acronyms used in this document are defined in Table 1.

Table 1: Abbreviations

Abbreviation	Context	Description
A2DP	Bluetooth SIG	Advanced Audio Distribution Profile
ac	NFC Forum	Alternative Carrier
AD	Bluetooth SIG	Advertising and Scan Response Data
BD_ADDR	Bluetooth SIG	Bluetooth Device Address
BR	Bluetooth SIG	Basic Rate
CF	NFC Forum	Chunk Flag
CoD	Bluetooth SIG	Class of Device
CPS	NFC Forum	Carrier Power State
EDR	Bluetooth SIG	Enhanced Data Rate
EIR	Bluetooth SIG	Extended Inquiry Response
Hr	NFC Forum	Handover Request Message
Hs	NFC Forum	Handover Select Message
HF	Bluetooth SIG	Hands-Free Unit
HFP	Bluetooth SIG	Hands-Free Profile
IL	NFC Forum	ID Length
LE	Bluetooth SIG	Low Energy
M	Bluetooth SIG	Mandatory
MB	NFC Forum	Message Begin
ME	NFC Forum	Message End
NDEF	NFC Forum	NFC Data Exchange Format
NFC	NFC Forum	Near Field Communication
O	Bluetooth SIG	Optional
OBEX	Bluetooth SIG	Object Exchange
OOB	Bluetooth SIG	Out-of-Band
PIN	N/A	Personal Identification Number
RFC	N/A	Request For Comments
SDP	Bluetooth SIG	Service Discovery Protocol

Abbreviation	Context	Description
SIG	Bluetooth SIG	Special Interest Group
SNK	Bluetooth SIG	Sink
SR	NFC Forum	Short Record
SSP	Bluetooth SIG	Secure Simple Pairing
TK	Bluetooth SIG	Temporary Key
TNF	NFC Forum	Type Name Format
UI	N/A	User Interface
UID	Bluetooth SIG	Unique Identifier
UUID	Bluetooth SIG	Universal Unique Identifier

1.7 Glossary

Advertising and Scan Response Data / Bluetooth *SIG*

A message that provides information about the local Bluetooth device sent in an Advertising or Scan Response event from Bluetooth Low Energy (LE) devices. Defined in [BLUETOOTH_CORE].

Alternative Carrier / NFC Forum

A (wireless) communication technology that can be used for data transfers between a Handover Requester and a Handover Selector.

Bluetooth Device

A device that implements [BLUETOOTH_CORE].

Carrier Configuration Data / NFC Forum

The information needed to connect to an alternative carrier. The exact information depends on the carrier technology.

Extended Inquiry Response / Bluetooth SIG

A response message providing information about the local Bluetooth device sent in response to an Inquiry from remote Bluetooth devices. Defined in [BLUETOOTH_CORE].

Handover Requester / NFC Forum

An NFC Forum Device that begins the Handover Protocol by issuing a Handover Request Message to another NFC Forum Device.

Handover Selector / NFC Forum

An NFC Forum Device that constructs and replies to a Handover Select Message as a result of a previously received Handover Request Message, or an NFC Forum Tag that provides a pre-set Handover Select Message for reading.

LE legacy pairing

Bluetooth Low Energy (LE) device pairing. as defined in [BLUETOOTH_CORE] Version 4.0 and 4.1

LE Secure Connections pairing

Bluetooth Low Energy (LE) device pairing introduced in [BLUETOOTH_CORE] Version 4.2 which uses different security algorithms compared to LE legacy pairing.

Negotiated Handover / NFC Forum

An exchange of NFC Data Exchange Format (NDEF) messages that allows two NFC Forum Devices to agree on a set of alternative carrier(s) to be used for further data exchange.

NFC Forum Device

A device that supports at least one communication protocol for at least one communication mode defined by the NFC Forum specifications. Currently the following NFC Forum Devices are defined:
NFC Universal Device, NFC Tag Device and NFC Reader Device.

NFC Forum Tag

A contactless tag or (smart) card supporting the NFC Data Exchange Format (NDEF).

NFC Tag Device

An NFC Forum Device that supports at least one communication protocol for Card Emulator and NFC Data Exchange Format (NDEF).

Out-of-Band / Bluetooth SIG

Communication that belongs to but occurs outside of an intended communication channel or method. In this document the term Out-of-Band (OOB) refers to data transmission over NFC for the purpose of pairing devices using Bluetooth Secure Simple Pairing (SSP) and discovering Bluetooth services.

Static Handover / NFC Forum

Provision of the Handover Select Message on an NFC Forum Tag that allows a reading NFC Forum Device to select and use alternative carriers for further data exchange.

2 Overview

The Bluetooth SIG publishes a set of specifications (available to its members) for wireless personal area networks. These specifications cover interoperability requirements, ranging from the behavior of the radio through core protocols up to application level profiles and services that enable specific use cases. The specifications are controlled by the Bluetooth SIG, which licenses the use of the specifications, provided that a product successfully completes all Bluetooth SIG qualification and listing requirements. The Bluetooth SIG also facilitates specification development by member companies.

The use of the NFC technology can enhance the user experience of applications that use the Bluetooth technology.

The enhancements can be in any of the following areas:

1. Select a Bluetooth device
2. Securely connect to a Bluetooth device
3. Start an application on a Bluetooth device.

2.1 Device Selection

Discovery of a Bluetooth enabled device in the vicinity of the discovering device typically uses the Inquiry procedure for Bluetooth Basic Rate / Enhanced Data Rate (BR/EDR) devices and the Discovery procedures for Bluetooth Low Energy (LE) devices.

NFC can simplify the discovery process by eliminating the Inquiry or Discovery procedure. It eliminates these procedures by providing the Bluetooth address and other optional parameters related to a specific Bluetooth-enabled device. This removes the need for the user to select the appropriate device from a (potentially long) list. The result is a more seamless wireless user experience.

2.2 Fast and Secure Connection

NFC can simplify the process of authenticated pairing between two Bluetooth devices by exchanging authentication information over an NFC link.

Devices that comply with [BLUETOOTH_CORE] and subsequent versions use Secure Simple Pairing (SSP) to securely connect devices over BR/EDR transport. SSP provides a stronger level of security, yet makes it easier for the user to perform pairing. SSP explicitly introduces the notion of Out-of-Band (OOB) pairing. The information (Hash C and Randomizer R used for Bluetooth BR/EDR devices and TK value and/or LE Secure Connections Confirmation Value and Random Value used for Bluetooth LE devices, described in Sections 3.2 and 3.4) can be exchanged over an NFC link that is used as part of the OOB pairing process.

Devices that comply with [BLUETOOTH_CORE] might support Bluetooth Interlaced Page Scan to speed up the Bluetooth connection setup. After Bluetooth OOB Data (see Table 2) have been exchanged over NFC, a device can enable Bluetooth Interlaced Page Scan to scan faster for a remote Bluetooth paging device and therefore to reduce the Bluetooth connection setup time. To improve interoperability it is recommended that the Bluetooth Interlaced Page Scan be enabled for a duration of at least 60 seconds. Since Bluetooth Interlaced Page Scan consumes more power than normal Bluetooth Page Scan, it is also recommended that the maximum duration of the Bluetooth Interlaced Page Scan be limited to 120 seconds.

After Bluetooth OOB data indicating LE transport have been exchanged over NFC it is recommended that the Central device and the Peripheral device use the fast connection establishment parameters recommended by the Bluetooth SIG ([BLUETOOTH_CORE] Volume 3, Part C, Sections 9.3.11 and 9.3.12) to reduce the Bluetooth LE connection setup time.

2.3 Start an Application

NFC can be used to start an application to provide good user experience. For example, the user touches one NFC Forum Device to another NFC Forum Device to exchange contact information. The specific method of starting an application via NFC 'touch' action is implementation specific. In some cases the 'touch' might even allow the user to select the application to execute.

3 Handover to a Bluetooth Carrier

The Bluetooth SIG defined the SSP mechanism ([BLUETOOTH_CORE], Volume 2, Part H, Section 7) to simplify the process of pairing two Bluetooth BR/EDR devices. Pairing between Bluetooth LE devices is defined in [BLUETOOTH_CORE], Volume 3, Part H.

SSP defines four different association models, one of them using an Out-of-Band channel such as NFC.

The [BLUETOOTH_CORE] Version 4.2 introduced the following terms for Bluetooth LE pairing:

- LE Secure Connections pairing
- LE legacy pairing (LE pairing as defined in [BLUETOOTH_CORE] Versions 4.0 and 4.1).

Four different association models are defined for LE Secure Connections pairing and three for LE legacy pairing. One model is the OOB association model, which is defined for both LE Secure Connections pairing and LE legacy pairing.

The NFC Forum Connection Handover technical specification ([CH]) defines the mechanism and format of the messages used to exchange Alternative Carrier information between NFC Forum Devices. Specifically, Bluetooth OOB data can be exchanged in Connection Handover Request and/or Select messages as Alternative Carrier information.

The Bluetooth SIG has defined one media type per [RFC2046] for Bluetooth BR/EDR Secure Simple Pairing OOB and one media type for Bluetooth LE OOB communication.

For Bluetooth BR/EDR devices, the Secure Simple Pairing OOB name “application/vnd.bluetooth.ep.oob” is used as the [NDEF] record type name. The payload for this record type is then defined by the Extended Inquiry Response (EIR) format specified in the Bluetooth Core Specification ([BLUETOOTH_CORE], Volume 3, Part C, Section 8).

For Bluetooth LE OOB the name “application/vnd.bluetooth.le.oob” is used as the [NDEF] record type name. The payload of this type of record is then defined by the Advertising and Scan Response Data (AD) format that is specified in the Bluetooth Core Specification ([BLUETOOTH_CORE], Volume 3, Part C, Section 11).

3.1 Secure Simple Pairing OOB Data

For Bluetooth BR/EDR devices, the Secure Simple Pairing Out-of-Band data format is used for OOB pairing ([BLUETOOTH_CORE], Volume 3, Part C, Section 5.2.2.7). This format is provided in Table 2. The format consists of a length field, the Bluetooth Device Address and an optional set of additional EIR data types.

Table 2: Bluetooth BR/EDR Secure Simple Pairing OOB Data

Name	Offset (Bytes)	Size	Mandatory / Optional	Description
OOB Data Length	0	2 bytes	M	The sum of the lengths of the fields OOB Data Length, Bluetooth Device Address and OOB Optional Data (see Section 3.1.1)
Bluetooth Device Address	2	6 bytes	M	Bluetooth Device Address of the device (see Section 3.1.2)
OOB Optional Data	8	N bytes	O	The remaining optional OOB data, in EIR format (see Section 3.2)

3.1.1 Secure Simple Pairing OOB Data Length

The value of this length field provides the absolute length of the total OOB data block[1] used for Bluetooth BR/EDR OOB communication, including the length field itself and the Bluetooth Device Address. The minimum length that can be represented in this field is 8.

The value in this field is (N + 8), where N is the length in bytes of the OOB Optional Data field, as shown in Table 2. This field is encoded in Little Endian order.

3.1.2 Bluetooth Device Address

The Bluetooth Device Address is uniquely assigned and is used to connect to another Bluetooth device. The details of this relationship are given in [BLUETOOTH_CORE] Volume 2, Part B, Section 1.2. As indicated in [BLUETOOTH_CSS] Part A, Section 1, this value is encoded in Little Endian order. For example, the Bluetooth Address 00:0c:78:51:c4:06 would be encoded as 0x06 0xC4 0x51 0x78 0x0C 0x00.

[1] [BLUETOOTH_CORE] Versions 2.1 + EDR and v3.0 + HS contain an inconsistency in the definition of the field OOB Optional Data Length. The field is described in Section 8.1.6 and Section 5.2.2.7. It appears that these two descriptions contradict each other, because the first indicates that the length field does not include the mandatory fields (Length and BD_ADDR), and the second indicates that they are included. The [BLUETOOTH_CORE] Version 5.1 has a consistent definition in both sections that states that the mandatory fields are included in the Length field. This issue is addressed in erratum 3476 in the Bluetooth SIG errata system, which specifies that the Length field conforms to the definition in Section 5.2.2.7 wherein the Length field includes the mandatory fields.

3.2 Secure Simple Pairing OOB Optional Data

The OOB Optional Data format is defined in [BLUETOOTH_CORE] Volume 3, Part C, Figure 8.1. A number of EIR data types are defined by the Bluetooth SIG (see the Generic Access Profile (GAP) section of [BLUETOOTH_NUMBERS] and the [BLUETOOTH_CSS]). This OOB Optional Data section highlights the use of the data types appropriate for the Connection Handover scenario. This coverage will not be exhaustive, and implementations might include other EIR data types.

An NFC handover implementation that receives OOB EIR formatted data needs to be prepared to receive, in any order, all possible EIR data type values, including values that are currently reserved for future use. Any EIR data type that is not supported by an implementation is ignored without inspecting the associated EIR data.

Table 3: Bluetooth EIR Data Types

Value (1 Byte)	Description
`0x09 or 0x08`	Bluetooth Local Name (Section 3.2.1)
`0x0E`	Simple Pairing Hash C (Section 3.2.2)
`0x0F`	Simple Pairing Randomizer R (Section 3.2.3)
`0x02, 0x03, 0x04, 0x05, 0x06, or 0x07`	Service Class UUID (different lengths based on Bluetooth SIG allocated base UUID) (Section 3.2.4)
`0x0D`	Class of Device (Section 3.2.5)

Additional EIR data types (not shown in Table 3) are defined by the Bluetooth SIG for other types of information. One is a manufacturer-specific type for proprietary information that is to be included within the standard format[2] (see [BLUETOOTH_CSS] Part A, Section 1.4).

3.2.1 Bluetooth Local Name Information

The Bluetooth Local Name, if configured on the Bluetooth device, is the user-friendly name presented over Bluetooth technology, as defined in [BLUETOOTH_CORE] Volume 3, Part C, Section 3.2.2. This name can be displayed to the device user as part of the user interface (UI) for operations with Bluetooth devices.

3.2.2 Simple Pairing Hash C Information

The Simple Pairing Hash C is defined in [BLUETOOTH_CORE] Volume 2, Part H, Section 7.2.2, which also provides information regarding whether inclusion of Hash C in the OOB data is appropriate. It is recommended in [BLUETOOTH_CORE] that the Hash C is generated anew for each pairing.

[2] There are different EIR data types to indicate additional semantics such as “partial” and “complete”. These are described in [BLUETOOTH_CORE] Volume 3, Part C, Section 8.

NOTE On NFC Forum Tags the provision of a freshly generated Hash C is not possible because the data are static and not modifiable[3].

3.2.3 Simple Pairing Randomizer R Information

The Simple Pairing Randomizer R is defined in [BLUETOOTH_CORE] Volume 2, Part H, Section 7.2.2. This specification provides details for scenarios in which inclusion of the Randomizer R value is appropriate[3].

NOTE The Randomizer R is optional. If it is not present, a value of 0 is assumed.

3.2.4 Service Class UUID Information

Service class information is used to identify the supported Bluetooth services of the device. A Service Class is represented by a UUID, which might be truncated from the full 128-bit UUID to a 16-bit or 32-bit abbreviated version that is based on the Bluetooth SIG BASE_UUID (see [BLUETOOTH_NUMBERS] Service Discovery).

The Service Class UUID element in the EIR format represents a list of UUIDs that are grouped together according to two properties of the list:

- The size of the UUID (16-bit, 32-bit, or 128-bit)
- Whether the UUID list is complete or partial.

A Service Class UUID list is defined to be complete when all service classes represented as service are recorded in the Bluetooth Service Discovery (SDP) database. A receiving device will use the complete/partial status of a UUID list to determine whether it performs an SDP query (once a Bluetooth link has been established) if the service class it requires is not listed.

The list of UUIDs is structured so that the payload contains contiguous UUIDs (the size of each UUID is determined by the EIR type associated with that payload). For example, if the length of an EIR tag 0x03 is 11, then the payload will contain 5 UUIDs in their 16-bit representations. The details are given in [BLUETOOTH_CSS] Part A, Section 1.1, [BLUETOOTH_CORE] Volume 3, Part B, and [BLUETOOTH_NUMBERS] Service Discovery.

3.2.5 Class of Device Information

The Class of Device information is used to provide a graphical representation to the user. This information is part of the UI that supports operations with Bluetooth devices. For example, it can provide a particular icon to represent the device.

[3] A special case is an NFC Tag Device that is able to dynamically modify its Data. This allows the inclusion of a freshly generated Simple Pairing Hash C and Randomizer R to establish a secure Bluetooth connection without further interaction beyond the “NFC touch”.

This field is not supposed to be used directly for determining whether or not a particular service can be employed, because it is intended only to provide information to the user about the type of device the user is engaging. One example is a workstation that provides a number of features (such as printing because it is connected to a printer). However, the service class field of the Class of Device information can indicate the general categories of services that the device can provide.

The determination of the support for services is based on the supported Service Class UUIDs (see Section 3.2.4).

Details about Class of Device values can be found in [BLUETOOTH_CORE] Volume 3, Part C, Section 3.2.4. The actual Class of Device values are defined in [BLUETOOTH_NUMBERS] Baseband.

3.3 Security Manager OOB Required Data Types

The format used for Bluetooth LE OOB data exchange is the Advertising and Scan Response Data (AD) format ([BLUETOOTH_CORE], Volume 3, Part C, Section 11). Each AD structure consists of an AD Length field of 1 byte, an AD Type field and an AD Data field. The value of the AD Length field is the sum of the numbers of bytes in the AD Type field and the AD Data field. The total OOB data length is defined by the [NDEF] record payload length.

The LE Role data type described in Section 3.3.2 is sent for Bluetooth LE OOB pairing over NFC.

The LE Bluetooth Device Address data type described in Section 3.3.1 is also sent for Bluetooth OOB pairing over NFC, with one exception for NFC Forum Tags. If a device uses a Public or Static Device Address, that address needs to be present on the NFC Forum Tag. If a device uses a Private Device Address and it is not possible to dynamically program the NFC Forum Tag, the LE Bluetooth Device Address field might not be present on the NFC Forum Tag. In any case, if the LE Bluetooth Device Address field is present on the NFC Forum Tag, its content matches the current Bluetooth Device Address of the Bluetooth device.

Bluetooth LE OOB data exchanged over NFC might contain other AD types.

Table 4: Bluetooth AD Types Required for OOB Pairing over NFC

Value (1 Byte)	Description
0x1B	LE Bluetooth Device Address (Section 3.3.1)[4]
0x1C	LE Role (Section 3.3.2)

[4] There is an exception for devices using a Private Device Address and an NFC Forum Tag that is not dynamically programmable.

3.3.1 LE Bluetooth Device Address

The LE Bluetooth Device Address data type is defined in [BLUETOOTH_CSS] Section 1.16. The LE Bluetooth Device Address consists of 7 bytes. Its 6 least significant bytes contain the 48 bit address that is used for the Bluetooth pairing over the LE transport and will identify the peer device to establish a connection with. The least significant bit in the most significant byte defines the address type. The address might be a Public Device Address or a Random Device Address. The Random Device Address is described in [BLUETOOTH_CORE], Volume 3, Part C, Section 10.8. The Public Address is defined in [BLUETOOTH_CORE], Volume 2, Part B, Section 1.2. The Address sent in the LE Bluetooth Device Address data type is intended to be used on the LE transport for at least ten minutes after the NFC data exchange.

The LE Bluetooth Device Address is encoded in Little Endian order. For example, the Bluetooth Device Address 00:0c:78:51:c4:06 would be encoded as 0x06 0xC4 0x51 0x78 0x0C 0x00.

3.3.2 LE Role

The Generic Access Profile defines four specific roles. These roles are described in [BLUETOOTH_CORE] Volume 3, part C, Section 2.2.2. During Bluetooth LE connection establishment, in order to be able to establish the connection one device will be in the Peripheral role and the other in the Central role. The LE Role data type, defined in [BLUETOOTH_CSS] Section 1.17, indicates role capabilities and role preference.

3.4 Security Manager OOB Pairing Optional Data Types

The following AD types are defined by the Bluetooth SIG: Security Manager TK Value, LE Secure Connections Confirmation Value, LE Secure Connections Random Value, Appearance, Flags, and Local Name. The following subsections give definitions for the AD types that are appropriate for Security Manager OOB pairing. This coverage is not exhaustive and implementations might include other AD types. An NFC handover implementation receiving OOB AD formatted data needs to be prepared to receive, in any order, all possible AD type values, including values that are currently reserved for future use. Any AD type that is not supported by an implementation is ignored without inspecting the associated AD values.

If the Security Manager TK Value, LE Secure Connections values and Flags data type are not present in a Handover Message, the Just Works mechanism will be used for pairing. If the Flags AD type and either the Security Manager TK Value or LE Secure Connections values are present, the OOB mechanism will be used for pairing. For details on Just Works pairing and OOB pairing, see [BLUETOOTH_CORE] Volume 3, Part H, Section 2.3.5.

Table 5: Bluetooth Optional AD Types

Value (1 Byte)	Description
0X10	Security Manager TK Value (Section 3.4.1)
0x19	Appearance (Section 3.4.2)
0x01	Flags (Section 3.4.3)
0x08 or 0x09	Local Name (Section 3.4.4)
0x22	LE Secure Connections Confirmation Value (Section 3.4.5)
0x23	LE Secure Connections Random Value (Section 3.4.6)

3.4.1 Security Manager TK Value

The Security Manager TK Value is defined in [BLUETOOTH_CSS] Section 1.8 and is used by the LE Security Manager, which is described in [BLUETOOTH_CORE] Volume 3, Part H. If the OOB association model and LE legacy pairing are used, the TK value might be exchanged over the OOB channel, in this case NFC. The TK value requirements for such exchange are described in [BLUETOOTH_CORE] Volume 3, Part H, Section 2.3.5.4.

The Security Manager TK Value is encoded in Little Endian order.

3.4.2 Appearance

The Appearance data type is defined in [BLUETOOTH_CSS] Section 1.12. The appearance characteristics define the representation of the external appearance of the device – for example, a mouse, generic remote control or keyboard. The appearance characteristics can be used by the discovering device to represent an icon, string or similar to the user. Attribute values for the appearance data type can be found in [BLUETOOTH_NUMBERS].

The Appearance data type is encoded in Little Endian order.

3.4.3 Flags

The Flags data type described in [BLUETOOTH_CSS] Section 1.3 contains information on which discoverable mode to use and the BR/EDR support and capability.

3.4.4 Local Name

The Local Name, if configured on the Bluetooth device, is the user-friendly name presented over Bluetooth technology, as defined in [BLUETOOTH_CORE] Volume 3, Part C, Section 3.2.2. This is the name that can be displayed to the device user as part of the UI related to the operations with the Bluetooth devices. The Local Name data type is defined in [BLUETOOTH_CSS] Section 1.2.

3.4.5 LE Secure Connections Confirmation Value

The LE Secure Connections Confirmation Value is defined in [BLUETOOTH_CSS] Section 1.6 and is used by the LE Security Manager, which is described in [BLUETOOTH_CORE] Volume 3, Part H. If the OOB association model and LE Secure Connections pairing are used, the LE Secure Connections Confirmation Value might be exchanged over the OOB channel, in this case NFC. The LE Secure Connections Confirmation Value requirements for such exchange are described in [BLUETOOTH_CORE] Volume 3, Part H, Section 2.3.5.6.4.

The LE Secure Connections Confirmation Value is encoded in Little Endian order.

3.4.6 LE Secure Connections Random Value

The LE Secure Connections Random Value is defined in [BLUETOOTH_CSS] Section 1.6 and is used by the LE Security Manager. These relationships are described in [BLUETOOTH_CORE] Volume 3, Part H. If the OOB association model and the LE Secure Connections pairing are used, the LE Secure Connections Random Value might be exchanged over the OOB channel, in this case NFC. The LE Secure Connections Random Value requirements for such exchange are described in [BLUETOOTH_CORE] Volume 3, Part H, Section 2.3.5.6.4.

The LE Secure Connections Random Value is encoded in Little Endian order.

4 Examples

[BLUETOOTH_CORE] requires that all numerical multi-byte entities and values associated with the following data types use Little Endian order. Therefore, in the examples presented in this document, all numerical multi-byte fields are encoded using Little Endian order. Examples of such fields include:

- Bluetooth OOB Data Length
- Simple Pairing Hash C
- Simple Pairing Randomizer R
- Security Manager TK Value
- Secure Connections Confirmation Value
- Secure Connections Random Value
- Appearance.

4.1 Negotiated Handover

4.1.1 BR/EDR Example

Figure 1 shows a sample Handover Request Message from an NFC Forum Device with the only alternative communication capability being Bluetooth using the mime-type “application/vnd.bluetooth.ep.oob”.

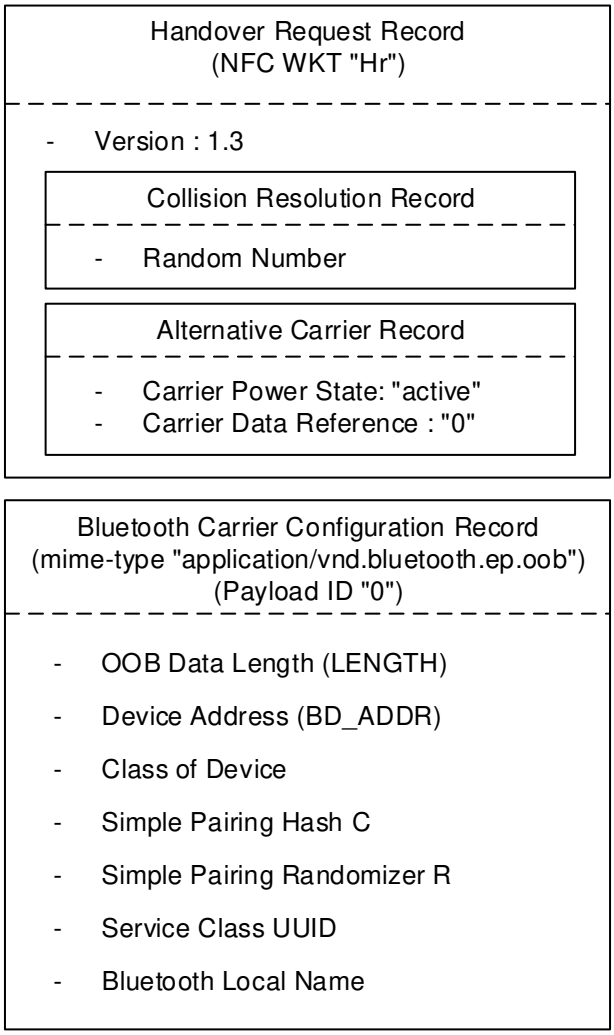

Figure 1: Bluetooth Handover Request Message

NOTE The Bluetooth OOB data block might contain only the LENGTH and BD_ADDR fields.

Bluetooth Simple Pairing in NFC Forum Peer-to-Peer mode allows for mutual authentication based on commitments of public keys exchanged Out-of-Band. An NFC Forum Device that is requesting handover to a Bluetooth carrier sends its public key commitment Hash C and Randomizer R with the Handover Request Message, and it receives the peer's commitment and randomizer with the Handover Select Message. The cryptographic details of the Bluetooth Out-of-Band pairing are described in [BLUETOOTH_CORE] Volume 2, Part H, Section 7.2.2.

Table 6 describes a sample Handover Request Message that could be sent by a camera device that has a Bluetooth radio available.

Table 6: Binary Content of a Sample Bluetooth Handover Request Message

Offset (Bytes)	Content	Length (Bytes)	Explanation
0	0x91	1	NDEF Record Header: MB=1b, ME=0b, CF=0b, SR=1b, IL=0b, TNF=001b
1	0x02	1	Record Type Length: 2 bytes
2	0x11	1	Payload Length: 17 bytes
3	0x48 0x72	2	Record Type: “Hr”
5	0x13	1	Version Number: Major = 1, Minor = 3
6	0x91	1	NDEF Record Header: MB=1b, ME=0b, CF=0b, SR=1b, IL=0b, TNF=001b
7	0x02	1	Record Type Length: 2 bytes
8	0x02	1	Payload Length: 2 bytes
9	0x63 0x72	2	Record Type: “cr”
11	0x01 0x02	2	Random Number: 0x01 0x02
13	0x51	1	NDEF Record Header: MB=0b, ME=1b, CF=0b, SR=1b, IL=0b, TNF=001b
14	0x02	1	Record Type Length: 2 bytes
15	0x04	1	Payload Length: 4 bytes
16	0x61 0x63	2	Record Type: “ac”
18	0x01	1	Carrier Flags: CPS=1, "active"
19	0x01	1	Carrier Data Reference Length: 1 byte
20	0x30	1	Carrier Data Reference: “0”
21	0x00	1	Auxiliary Data Reference Count: 0
22	0x5A	1	NDEF Record Header: MB=0b, ME=1b, CF=0b, SR=1b, IL=1b, TNF=010b
23	0x20	1	Record Type Length: 32 bytes
24	0x43	1	Payload Length: 67 bytes
25	0x01	1	Payload ID Length: 1 byte
26	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x62 0x6C 0x75 0x65 0x74 0x6F 0x6F 0x74 0x68 0x2E 0x65 0x70 0x2E 0x6F 0x6F 0x62	32	Record Type Name: application/vnd.bluetooth.ep.oob
58	0x30	1	Payload ID: “0”
59	0x43 0x00	2	Bluetooth OOB Data Length: 67 bytes
61	0x01 0x07 0x80 0x80 0xBF 0xA1	6	Bluetooth Device Address: A1:BF:80:80:07:01
67	0x04	1	EIR Data Length: 4 bytes
68	0x0D	1	EIR Data Type: Class of Device
69	0x20 0x06 0x08	3	Class of Device: 0x08: Service Class = Capturing 0x06: Major Device Class = Imaging 0x20: Minor Device Class = Camera
72	0x11	1	EIR Data Length: 17 bytes

Offset (Bytes)	Content	Length (Bytes)	Explanation
73	0x0E	1	EIR Data Type: Simple Pairing Hash C
74	0x0F 0x0E 0x0D 0x0C 0x0B 0x0A 0x09 0x08 0x07 0x06 0x05 0x04 0x03 0x02 0x01 0x00	16	Simple Pairing Hash C: 0x000102030405060708090A0B0C0D0E0F
90	0x11	1	EIR Data Length: 17 bytes
91	0x0F	1	EIR Data Type: Simple Pairing Randomizer R
92	0x0F 0x0E 0x0D 0x0C 0x0B 0x0A 0x09 0x08 0x07 0x06 0x05 0x04 0x03 0x02 0x01 0x00	16	Simple Pairing Randomizer R: 0x000102030405060708090A0B0C0D0E0F
108	0x05	1	EIR Data Length: 5 bytes
109	0x03	1	EIR Data Type: 16-bit Service Class UUID list (complete)
110	0x06 0x11 0x20 0x11	4	16-bit Service Class UUID list (complete): 0x1106 – OBEX File Transfer 0x1120 – Direct Printing Reference Object Service
114	0x0B	1	EIR Data Length: 11 bytes
115	0x09	1	EIR Data Type: Complete Local Name
116	0x44 0x65 0x76 0x69 0x63 0x65 0x4e 0x61 0x6d 0x65	10	Bluetooth Local Name: DeviceName

Figure 2 shows the structure of a Handover Select Message that is returned by an NFC Forum Device to acknowledge a Bluetooth carrier.

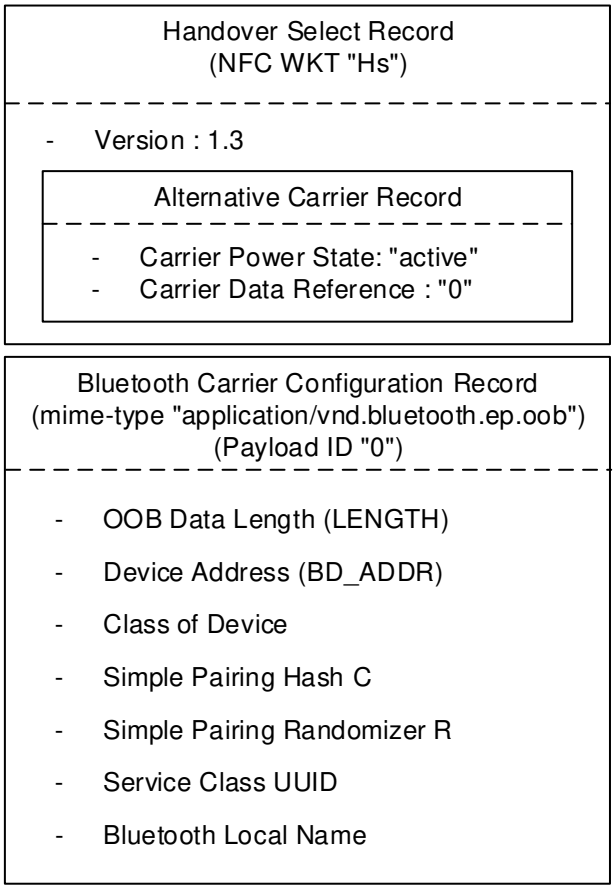

Figure 2: Bluetooth Handover Select Message

Table 7 describes a sample Handover Select Message that could be returned by a printer device that has a Bluetooth radio available.

Table 7: Binary Content of a Sample Bluetooth Handover Select Message

Offset (Bytes)	Content	Length (Bytes)	Explanation
0	0x91	1	NDEF Record Header: MB=1b, ME=0b, CF=0b, SR=1b, IL=0b, TNF=001b
1	0x02	1	Record Type Length: 2 bytes
2	0x0A	1	Record Type Length: 10 bytes
3	0x48 0x73	2	Record Type: “Hs”
5	0x13	1	Version Number: Major = 1, Minor = 3
6	0xD1	1	NDEF Record Header: MB=1b, ME=1b, CF=0b, SR=1b, IL=0b, TNF=001b
7	0x02	1	Record Type Length: 2 bytes
8	0x04	1	Payload Length: 4 bytes
9	0x61 0x63	2	Record Type: “ac”
11	0x01	1	Carrier Flags: CPS=1, "active"
12	0x01	1	Carrier Data Reference Length: 1 byte
13	0x30	1	Carrier Data Reference: “0”
14	0x00	1	Auxiliary Data Reference Count: 0
15	0x5A	1	NDEF Record Header: MB=0b, ME=1b, CF=0b, SR=1b, IL=1b, TNF=010b
16	0x20	1	Record Type Length: 32 bytes
17	0x43	1	Payload Length: 67 bytes
18	0x01	1	Payload ID Length: 1 byte
19	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x62 0x6C 0x75 0x65 0x74 0x6F 0x6F 0x74 0x68 0x2E 0x65 0x70 0x2E 0x6F 0x6F 0x62	32	Record Type Name: application/vnd.bluetooth.ep.oob
51	0x30	1	Payload ID: “0”
52	0x43 0x00	2	Bluetooth OOB Data Length: 67 bytes
54	0x03 0x07 0x80 0x88 0xbf 0x01	6	Bluetooth Device Address: 01:bf:88:80:07:03
60	0x04	1	EIR Data Length (4 bytes)
61	0x0D	1	EIR Data Type: Class of Device
62	0x80 0x06 0x04	3	Class of device: 0x04: Service class = Rendering 0x06: Major Device class = Imaging 0x80: Minor Device class = Printer
65	0x11	1	EIR Data Length: 17 bytes
66	0x0E	1	EIR Data Type: Simple Pairing Hash C
67	0x0F 0x0E 0x0D 0x0C 0x0B 0x0A 0x09 0x08 0x07 0x06 0x05 0x04 0x03 0x02 0x01 0x00	16	Simple Pairing Hash C: 0x000102030405060708090A0B0C0D0E0F
83	0x11	1	EIR Data Length: 17 bytes
84	0x0F	1	EIR Data Type: Simple Pairing Randomizer R
85	0x0F 0x0E 0x0D 0x0C 0x0B 0x0A 0x09 0x08 0x07 0x06 0x05 0x04 0x03 0x02 0x01 0x00	16	Simple Pairing Randomizer R: 0x000102030405060708090A0B0C0D0E0F
101	0x05	1	EIR Data Length: 5 bytes
102	0x03	1	EIR Data Type: 16-bit Service Class UUID list (complete)

Offset (Bytes)	Content	Length (Bytes)	Explanation
103	0x18 0x11 0x23 0x11	4	16-bit Service Class UUID list (complete): 0x1118 – Direct Printing 0x1123 – Printing Status
107	0x0B	1	EIR Data Length: 11 bytes
108	0x09	1	EIR Data Type: Complete Local Name
109	0x44 0x65 0x76 0x69 0x63 0x65 0x4e 0x61 0x6d 0x65	10	Bluetooth Local Name: DeviceName

4.1.2 LE Example

Figure 3 shows a Handover Request Message (using the mime-type "application/vnd.bluetooth.le.oob") issued from an NFC Forum Device that has only Bluetooth LE communication capability.

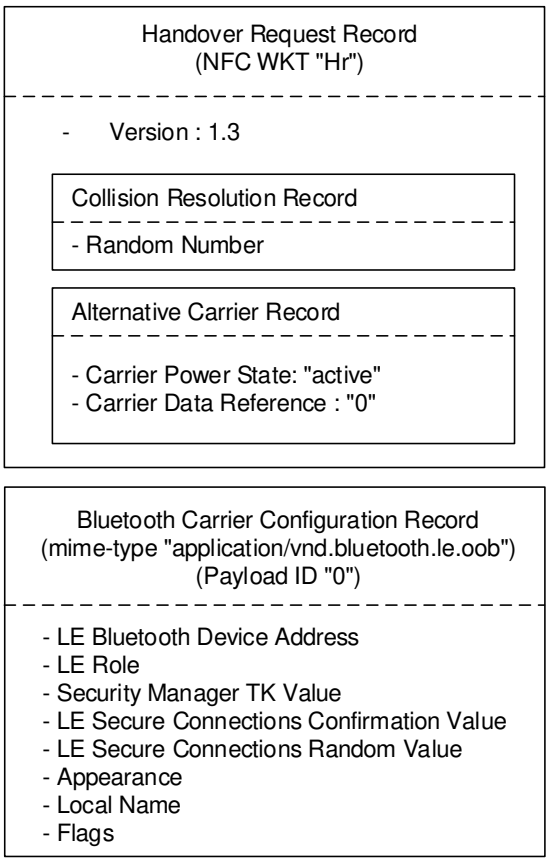

Figure 3: Bluetooth LE Handover Request Message

NOTE The Bluetooth Carrier Configuration Record might contain only the LE Bluetooth Device Address data type and the LE Role data type.

Table 8 describes a Handover Request Message from a generic computer. In this example the Public Address is used in the LE Bluetooth Device Address data type. The LE Role data type

states both peripheral and central role capabilities, with the central role as the preferred role.

In a Negotiated Handover scenario, conflicting roles can be resolved by retransmitting the Handover Request message with a new LE Role preference. If two NFC Forum Devices have the same role preferences and both have peripheral and central role capabilities, the Handover Requester will need to change its role.

Table 8: Binary Content of a Bluetooth LE Handover Request Message

Offset (Bytes)	Content	Length (Bytes)	Explanation
0	0x91	1	NDEF record header: MB=1b ME=0b CF=0b SR=1b IL=0b TNF=001b
1	0x02	1	NDEF record type length: 2 bytes
2	0x11	1	NDEF payload length: 17 bytes
3	0x48 0x72	2	Record type: ‘Hr’
5	0x13	1	Connection Handover specification version 1.3
6	0x91	1	NDEF Record Header: MB=1b, ME=0b, CF=0b, SR=1b, IL=0b, TNF=001b
7	0x02	1	Record Type Length: 2 bytes
8	0x02	1	Payload Length: 2 bytes
9	0x63 0x72	2	Record Type: “cr”
11	0x01 0x02	2	Random Number: 0x01 0x02
13	0x51	1	NDEF record header: MB=0b ME=1b CF=0b SR=1b IL=0b TNF=001b
14	0x02	1	NDEF record type length: 2 bytes
15	0x04	1	NDEF payload length: 4 bytes
16	0x61 0x63	2	Record Type: ‘ac’ alternative carrier
18	0x01	1	Carrier Flags: CPS=1 “active”
19	0x01	1	Carrier Date Reference Length: 1 byte
20	0x30	1	Carrier data reference: “0”
21	0x00	1	Auxiliary Data Reference Count: 0
22	0x5A	1	NDEF record header: MB=0b ME=1b CF=0b SR=1b IL=1b TNF=010b
23	0x20	1	NDEF Record Type length: 32 bytes
24	0x55	1	NDEF Payload length: 85 bytes
25	0x01	1	ID length
26	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x62 0x6C 0x75 0x65 0x74 0x6F 0x6F 0x74 0x68 0x2E 0x6c 0x65 0x2E 0x6F 0x6F 0x62	32	Record Type Name: application/vnd.bluetooth.le.oob
58	0x30	1	Payload ID: 0
59	0x08	1	LE Bluetooth Device Address length: 8 bytes
60	0x1B	1	LE Bluetooth Device Address data type
61	0x01 0x07 0x80 0x80 0xBF 0xA1 0x00	7	Bluetooth Device Address: Public Address A1:BF:80:80:07:01
68	0x02	1	LE Role Length: 2 bytes

Offset (Bytes)	Content	Length (Bytes)	Explanation
69	0x1C	1	LE Role data type
70	0x03	1	LE Role: Central and peripheral capabilities with central role preferred.
71	0x11	1	Security Manager TK value length: 17 bytes
72	0x10	1	Security Manager TK value data type
73	0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11	16	Security Manager TK value
89	0x11	1	LE Secure Connections Confirmation Value length: 17 bytes
90	0x22	1	LE Secure Connections Confirmation Value data type
91	0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11	16	LE Secure Connections Confirmation Value
107	0x11	1	LE Secure Connections Random Value length: 17 bytes
108	0x23	1	LE Secure Connections Random Value data type
109	0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12	16	LE Secure Connections Random Value
125	0x03	1	Appearance length: 3 bytes
126	0x19	1	Appearance data type
127	0x80 0x00	2	Appearance: Generic Computer
129	0x0B	1	Local name length: 11 bytes
130	0x09	1	Local name data type
131	0x44 0x65 0x76 0x69 0x63 0x65 0x4e 0x61 0x6d 0x65	10	Local name Ascii: “DeviceName”
141	0x02	1	Flags length: 2 bytes
142	0x01	1	Flags data type
143	0x06	1	Flags: LE General Discoverable Mode, BR/EDR not supported

Figure 4 shows a Handover Select Message returned by a Handover Selector that acknowledges a Bluetooth Low Energy carrier.

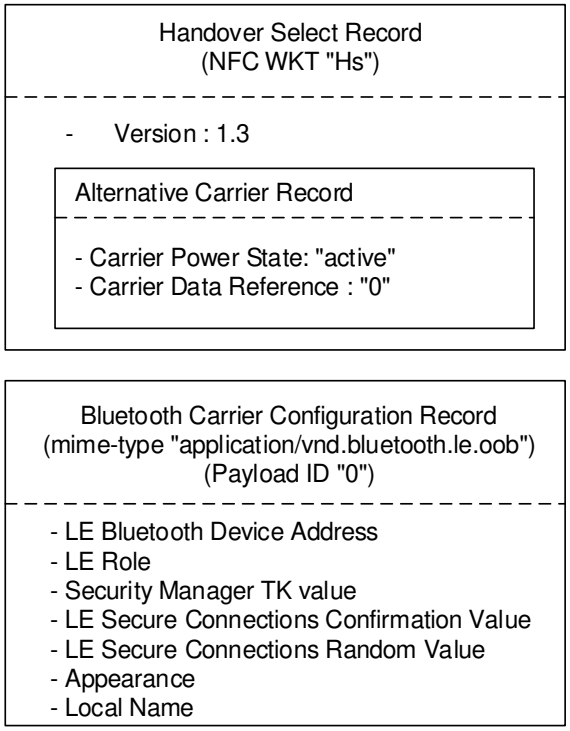

Figure 4: Bluetooth LE Handover Select Message

Table 9 describes a Handover Select Message that can be returned by a keyboard supporting Bluetooth LE. In this example a resolvable private address is used in the LE Bluetooth Device Address data type. The LE Role states only peripheral capabilities. User friendly device name is set to the value DeviceName in the Local Name data type.

In a Negotiated Handover scenario, conflicting roles can be resolved if the Selector changes its role. If two NFC Forum Devices have the same role preferences and both have peripheral and central role capabilities, the Handover Selector needs to keep its preferred role.

Table 9: Binary Content of a Bluetooth LE Handover Select Message

Offset (Bytes)	Content	Length (Bytes)	Explanation
0	0x91	1	NDEF record header: MB=1b ME=0b CF=0b SR=1b IL=0b TNF=001b
1	0x02	1	NDEF record type length: 2 bytes
2	0x0A	1	NDEF payload length: 10 bytes
3	0x48 0x73	2	Record type: 'Hs'
5	0x13	1	Connection Handover specification version 1.3
6	0xD1	1	NDEF record header: MB=1b ME=1b CF=0b SR=1b IL=0b TNF=001b
7	0x02	1	NDEF record type length: 2 bytes
8	0x04	1	NDEF payload length: 4 bytes
9	0x61 0x63	2	Record Type: "ac" alternative carrier
11	0x01	1	Carrier Flags: CPS = 1 "active"
12	0x01	1	Carrier Data Reference Length: 1 byte
13	0x30	1	Carrier Data Reference: "0"
14	0x00	1	Auxiliary Data Reference Count: 0
15	0x5A	1	NDEF record header: MB=0b ME=1b CF=0b SR=1b IL=1b TNF=010b
16	0x20	1	Record Type Length: 32 bytes
17	0x52	1	Payload Length: 82 bytes
18	0x01	1	Payload ID Length: 1 byte
19	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x62 0x6C 0x75 0x65 0x74 0x6F 0x6F 0x74 0x68 0x2E 0x6c 0x65 0x2E 0x6F 0x6F 0x62	32	Record Type Name: application/vnd.bluetooth.le.oob
51	0x30	1	Payload ID: 0
52	0x08	1	LE Bluetooth Device Address length: 8 bytes
53	0x1B	1	LE Bluetooth Device Address data type
54	0xC8 0xDC 0xF4 0x55 0x2A 0x77 0x01	7	Bluetooth Device Address: Resolvable Private Address: 77:2A:55:F4:DC:C8
61	0x02	1	LE Role Length: 2 bytes
62	0x1C	1	LE Role data type
63	0x00	1	LE Role: Only peripheral capabilities
64	0x11	1	Security Manager TK value length: 17 bytes
65	0x10	1	Security Manager TK value data type
66	0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11	16	Security Manager TK value
82	0x11	1	Secure Connections Confirmation Value length: 17 bytes
83	0x22	1	Secure Connections Confirmation Value data type
84	0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11	16	Secure Connections Confirmation Value
100	0x11	1	Secure Connections Random Value length: 17 bytes
101	0x23	1	Secure Connections Random Value data type
102	0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12	16	Secure Connections Random Value
118	0x03	1	Appearance Length: 3 bytes
119	0x19	1	Appearance data type
120	0xC1 0x03	2	Appearance: Keyboard
122	0x0B	1	Local name length: 11 bytes
123	0x09	1	Local name data type
124	0x44 0x65 0x76 0x69 0x63 0x65 0x4e 0x61 0x6d 0x65	10	Local name Ascii: "DeviceName"

4.2 Static Handover

When the Handover Selector is equipped only with an NFC Forum Tag, Static Handover can be used. In this case the Handover Selector cannot actively reply to a Handover Request Message. A Handover Requester detects this message during the NFC discovery phase and is then able to read data from the NFC Forum Tag. If the data that are read embody a Handover Select Message, the Handover Requester can use this information to choose one of the indicated alternative carriers and to attempt to establish a secondary connection.

In principle, the Handover Select Message stored on an NFC Forum Tag is identical to a Handover Select Message returned by an active NFC Forum Device. However, because the data on an NFC Forum Tag are static, a pre-stored Handover Select Message will always have to indicate all available carriers, since carriers cannot automatically be powered as a result of the NFC touch.

If alternative carriers cannot be ensured to be active, the carrier power state is set to either Inactive or Unknown, which results in undefined behavior in the Handover Requester. A possible strategy for the Handover Requester might be to request the user to perform a manual activation for a carrier that has been signaled as Inactive and to first try and then possibly request manual activation for a carrier that has the Unknown power state.

Dynamic carrier-specific protocol information, such as non-static IP addresses, cannot be provided.

4.2.1 BR/EDR Example

Figure 5 shows an example in which Bluetooth configuration data are included in a Handover Select Message stored on an NFC Forum Tag.

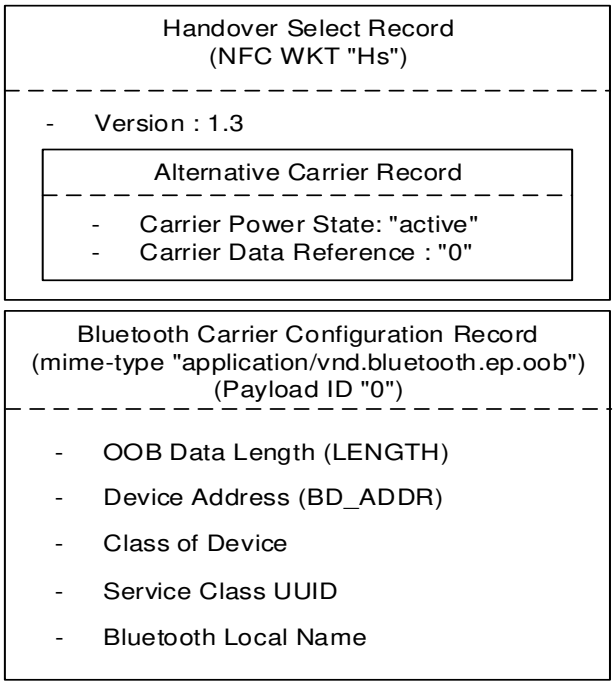

Figure 5: Bluetooth Configuration Data on an NFC Forum Tag

In this example the power state of a Bluetooth carrier is indicated as Active (that is, the Handover Requester device would expect both carriers to be operational and on-air).

The binary layout of a Handover Select Message for a Bluetooth carrier stored on an NFC Forum Tag is shown in Table 10, which presents the Bluetooth configuration data that can be advertised by a printer device that supports the Basic Printing Profile.

NOTE The Simple Pairing Hash C and Randomizer R are not present because of the inability to refresh the C and R values after each pairing attempt. More details about where C and R values are appropriate can be found in [BLUETOOTH_CORE], Volume 2, Part H, Section 7.2.2.

Table 10: Binary Content of a Sample Bluetooth Handover Select Message on an NFC Forum Tag

Offset (Bytes)	Content	Length (Bytes)	Explanation
0	0x91	1	NDEF Record Header: MB=1b, ME=0b, CF=0b, SR=1b, IL=0b, TNF=001b
1	0x02	1	Record Type Length: 2 bytes
2	0x0A	1	Record Type Length: 10 bytes
3	0x48 0x73	2	Record Type: “Hs”
5	0x13	1	Version Number: Major = 1, Minor = 3
6	0xD1	1	NDEF Record Header: MB=1b, ME=1b, CF=0b, SR=1b, IL=0b, TNF=001b
7	0x02	1	Record Type Length: 2 bytes
8	0x04	1	Payload Length: 4 bytes
9	0x61 0x63	2	Record Type: “ac”
11	0x03	1	Carrier Flags: CPS=3, "unknown"
12	0x01	1	Carrier Data Reference Length: 1 byte
13	0x30	1	Carrier Data Reference: “0”
14	0x00	1	Auxiliary Data Reference Count: 0
15	0x5A	1	NDEF Record Header: MB=0b, ME=1b, CF=0b, SR=1b, IL=1b, TNF=010b
16	0x20	1	Record Type Length: 32 bytes
17	0x1F	1	Payload Length: 31 bytes
18	0x01	1	Payload ID Length: 1 byte
19	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x62 0x6C 0x75 0x65 0x74 0x6F 0x6F 0x74 0x68 0x2E 0x65 0x70 0x2E 0x6F 0x6F 0x62	32	Record Type Name: application/vnd.bluetooth.ep.oob
51	0x30	1	Payload ID: “0”
52	0x1F 0x00	2	Bluetooth OOB Data Length: 31 bytes
54	0x03 0x07 0x80 0x88 0xbf 0x01	6	Bluetooth Device Address: 01:bf:88:80:07:03
60	0x04	1	EIR Data Length: 4 bytes
61	0x0D	1	EIR Data Type: Class of Device
62	0x80 0x06 0x04	3	Class of Device: 0x04: Service class = Rendering 0x06: Major Device class = Imaging 0x80: Minor Device class = Printer
65	0x05	1	EIR Data Length: 5 bytes
66	0x03	1	EIR Data Type: 16-bit Service Class UUID list (complete)
67	0x18 0x11 0x23 0x11	4	16-bit Service Class UUID list (complete): 0x1118 – Direct Printing 0x1123 – Printing Status
71	0x0B	1	EIR Data Length: 11 bytes
72	0x09	1	EIR Data Type: Complete Local Name
73	0x44 0x65 0x76 0x69 0x63 0x65 0x4e 0x61 0x6d 0x65	10	Bluetooth Local Name: DeviceName

4.2.2 LE Example

Figure 6 shows an example of a Bluetooth LE configuration in a Handover Select Message stored on an NFC Forum Tag.

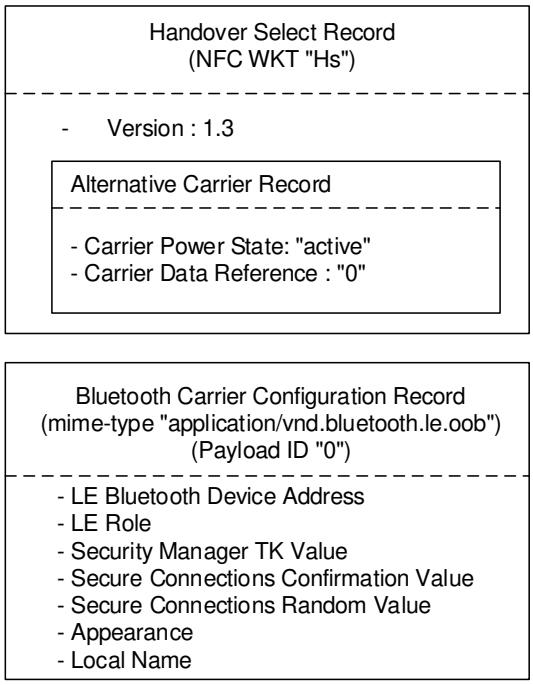

Figure 6: Bluetooth LE Configuration Data on an NFC Forum Tag

Table 11 describes a Handover Select Message stored on an NFC Forum Tag. In principle this message is identical to a Handover Select message returned by an active NFC Forum Device in the negotiated handover scenario. However, if data stored on an NFC Forum Tag cannot be changed, the TK value and the LE Secure Connections Random and Confirmation values are removed and a static private address is used.

Table 11: Binary Content of a Bluetooth LE Handover Select Message on an NFC Forum Tag

Offset (Bytes)	Content	Length (Bytes)	Explanation
0	0x91	1	NDEF record header: MB=1b ME=0b CF=0b SR=1b IL=0b TNF=001b
1	0x02	1	NDEF record type length: 2 bytes
2	0x0A	1	NDEF payload length: 10 bytes
3	0x48 0x73	2	Record type: 'Hs'
5	0x13	1	Connection Handover specification version 1.3
6	0xD1	1	NDEF record header: MB=1b ME=1b CF=0b SR=1b IL=0b TNF=001b
7	0x02	1	NDEF record type length: 2 byte
8	0x04	1	NDEF payload length: 4 bytes
9	0x61 0x63	2	Record Type "ac" alternative carrier
11	0x01	1	Carrier Flags CPS: 1 "active"
12	0x01	1	Carrier Data Reference Length: 1 byte
13	0x30	1	Carrier Data Reference: "0"
14	0x00	1	Auxiliary Data Reference Count: 0
15	0x5A	1	NDEF record header: MB=0b ME=1b CF=0b SR=1b IL=1b TNF=010b
16	0x20	1	Record Type Length: 32 bytes
17	0x52	1	Payload Length: 82 bytes
18	0x01	1	Payload ID Length: 1 byte
19	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x62 0x6C 0x75 0x65 0x74 0x6F 0x6F 0x74 0x68 0x2E 0x6c 0x65 0x2E 0x6F 0x6F 0x62	32	Record Type Name: application/vnd.bluetooth.le.oob
51	0x30	1	Payload ID: 0
52	0x08	1	LE Bluetooth Device Address length: 8 bytes
53	0x1B	1	LE Bluetooth Device Address data type
54	0x18 0x3B 0x4B 0x1C 0x3B 0xCA 0x01	7	Bluetooth Device Address: Static Address: CA:3B:1C:4B:3B:18
61	0x02	1	LE Role Length: 2 bytes
62	0x1C	1	LE Role data type
63	0x00	1	LE Role: Only peripheral role capabilities
64	0x11	1	Security Manager TK value length: 17 bytes
65	0x10	1	Security Manager TK value data type
66	0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11	16	Security Manager TK value
82	0x11	1	Secure Connections Confirmation Value data length: 17 bytes
83	0x22	1	Secure Connections Confirmation Value data type
84	0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11	16	Secure Connections Confirmation Value
100	0x11	1	Secure Connections Random Value data length: 17 bytes
101	0x23	1	Secure Connections Random Value data type
102	0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12	16	Secure Connections Random Value
118	0x03	1	Appearance length: 3 bytes
119	0x19	1	Appearance data type
120	0xC1 0x03	2	Appearance: Keyboard
122	0x0B	1	Local name length: 11 bytes
123	0x09	1	Local name data type
124	0x44 0x65 0x76 0x69 0x63 0x65 0x4e 0x61 0x6d 0x65	10	Local name Data Ascii: "DeviceName"

4.3 Simplified Tag Format for a Single Bluetooth Carrier

If a Handover Selector is advertising only one alternative carrier (i.e., a Bluetooth carrier), it can use a simplified format that does not contain the Handover Select record. In this case the NFC Forum Tag contains an NFC Data Exchange Format (NDEF) message with only the Bluetooth OOB information.

4.3.1 BR/EDR Example

Figure 7 illustrates how Bluetooth configuration data are included in an NDEF message.

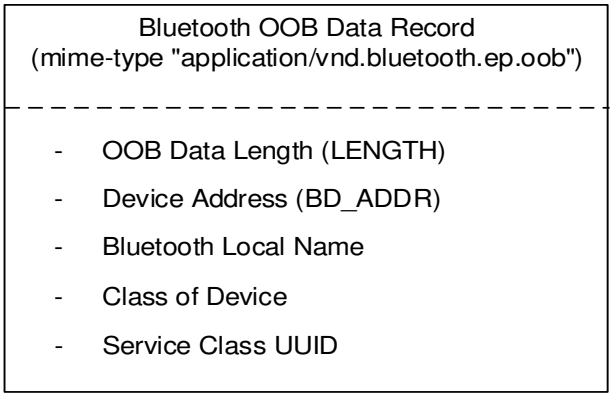

Figure 7: Bluetooth OOB Data on an NFC Forum Tag

Table 12 shows the binary layout of an NDEF message without the Handover Select record for a Bluetooth carrier stored on an NFC Forum Tag. The Bluetooth configuration data in this example indicate a type of headset and include the following optional OOB data fields: the Class of Device, Complete Local Name, and Service Class UUID.

Table 12: Binary Content of a Sample Bluetooth OOB Data on an NFC Forum Tag

Offset (Bytes)	Content	Length (Bytes)	Explanation
0	0xD2	1	NDEF Record Header: MB=1b, ME=1b, CF=0b, SR=1b, IL=0b, TNF=010b
1	0x20	1	Record Type Length: 32 bytes
2	0x21	1	Payload Length: 33 bytes
3	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x62 0x6C 0x75 0x65 0x74 0x6F 0x6F 0x74 0x68 0x2E 0x65 0x70 0x2E 0x6F 0x6F 0x62	32	Record Type Name: application/vnd.bluetooth.ep.oob
35	0x21 0x00	2	OOB Optional Data Length: 33 bytes
37	0x06 0x05 0x04 0x03 0x02 0x01	6	Bluetooth Device Address: 01:02:03:04:05:06
43	0x0D	1	EIR Data Length: 13 bytes
44	0x09	1	EIR Data Type: Complete Local Name
45	0x48 0x65 0x61 0x64 0x53 0x65 0x74 0x20 0x4E 0x61,0x6D 0x65	12	Bluetooth Local Name HeadSet Name
57	0x04	1	EIR Data Length: 4 bytes
58	0x0D	1	EIR Data Type: Class of Device
59	0x04 0x04 0x20	3	Class of Device: 0x20: Service class = Audio 0x04: Major Device class = Audio/Video 0x04: Minor Device class = Wearable Headset Device
62	0x05	1	EIR Data Length: 5 bytes
63	0x03	1	EIR Data Type: 16-bit Service Class UUID list (complete)
64	0x1E 0x11 0x0B 0x11	4	16-bit Service Class UUID list (complete): 0x111E – HFP-HF 0x110B - A2DP-SNK

4.3.2 LE Example

Figure 8 illustrates how Bluetooth LE configuration data are included in an NDEF message for the simplified Tag format.

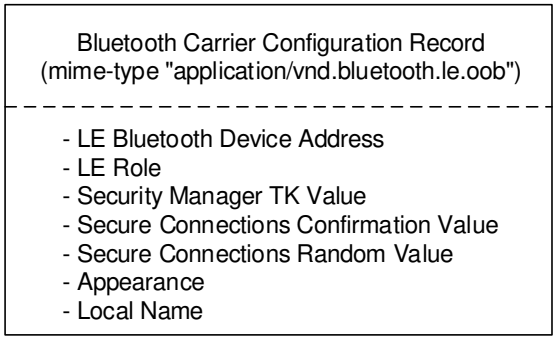

Figure 8: Bluetooth LE OOB Data on an NFC Forum Tag

Table 13 shows the binary layout of the simplified Tag format. The example is a Bluetooth LE configured mouse with its local name set to the value DeviceName with only peripheral role capabilities. A static private address is used.

Table 13: Binary Content of a Bluetooth LE OOB Data on an NFC Forum Tag

Offset (Bytes)	Content	Length (Bytes)	Explanation
0	0xD2	1	NDEF record header: MB=1b ME=1b CF=0b SR=1b IL=0b TNF=010b
1	0x32	1	Record Type Length 32 bytes
2	0x52	1	Payload Length: 82 bytes
3	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x62 0x6C 0x75 0x65 0x74 0x6F 0x6F 0x74 0x68 0x2E 0x6c 0x65 0x2E 0x6F 0x6F 0x62	32	Record Type Name: application/vnd.bluetooth.le.oob
35	0x08	1	LE Bluetooth Device Address length: 8 bytes
36	0x1B	1	LE Bluetooth Device Address data type
37	0x18 0x3B 0x4B 0x1C 0x3B 0xCA 0x01	7	Bluetooth Device Address: Static Address: CA:3B:1C:4B:3B:18
44	0x02	1	LE Role Length: 2 bytes
45	0x1C	1	LE Role data type
46	0x00	1	LE Role: Only peripheral role capabilities
47	0x11	1	Security Manager TK value length: 17 bytes
48	0x10	1	Security Manager TK value data type
49	0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11	16	Security Manager TK value
65	0x11	1	Secure Connections Confirmation Value data length: 17 bytes
66	0x22	1	Secure Connections Confirmation Value data type
67	0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11 0x00 0x00 0x00 0x11	16	Secure Connections Confirmation Value
83	0x11	1	Secure Connections Random Value data length: 17 bytes
84	0x23	1	Secure Connections Random Value data type
85	0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12 0x00 0x00 0x00 0x12	16	Secure Connections Random Value
101	0x03	1	Appearance Length: 3 bytes
102	0x19	1	Appearance data type
103	0xC2 0x03	2	Appearance Data: Mouse
105	0x0B	1	Local Name length: 11 bytes
106	0x09	1	Local Name data type
107	0x44 0x65 0x76 0x69 0x63 0x65 0x4e 0x61 0x6d 0x65	10	Local Name Ascii: “DeviceName”

A. Revision History

Table 14 outlines the revision history of Bluetooth® Secure Simple Pairing Using NFC.

Table 14: Revision History

Document Name	Revision and Release Date	Status	Change Notice	Supersedes
Bluetooth® Secure Simple Pairing Using NFC Application Note	Version 1.0, October 2011	Final	None	
Bluetooth® Secure Simple Pairing Using NFC Application Note	Version 1.0.1, October 2012	Final	Removes license restrictions; small editorial changes	Version 1.0
Bluetooth® Secure Simple Pairing Using NFC Application Note	Version 1.1, January 2014	Final		Version 1.0.1
Bluetooth® Secure Simple Pairing Using NFC Application Note	Version 1.2, May 2019	Final	Extended for Bluetooth Low Energy; editorial update.	Version 1.1