Bluetooth Secure Simple Pairing Using NFC

Application Document

NFC Forum™

NFCForum-AD-BTSSP_1.0.1

2012-11-16

RESTRICTIONS ON USE

This License Agreement (Agreement) is a legal agreement between you and NFC Forum, Inc./ Bluetooth SIG, Inc., each 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 you 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.

This Application Document and Agreement is a joint copyright © 2005-2011 by the NFC Forum and 2001-2011 Bluetooth SIG, Inc. This Application Document and Agreement was made available pursuant to a license agreement entered into between the recipient (Licensee) and Licensor and may be used only by Licensee, and in compliance with the terms of that license agreement (License). If you are not the Licensee, you may read this Application Document, but are not authorized to implement or make any other use of this Application Document. However, you may obtain a copy of this Application Document and implementation rights at the following page of Licensor's websites:

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

and

https://www.bluetooth.org/Technical/Specifications/whitepapers.htm

after entering into and agreeing to such license terms as Licensors then require.

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 address as it appears 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

Bluetooth SIG, Inc.
5209 Lake Washington Blvd NE, Suite 350
Kirkland, Washington 98033

Updated October 9, 2012

Contents

Figures

Tables

1 Introduction

This Application Document is intended to provide examples for implementation of *Bluetooth* Secure Simple Pairing (SSP) using NFC.

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

Bluetooth SSP has been introduced in *Bluetooth* Core Specification Version 2.1 + EDR, and specific data format may change in subsequent versions of the standard. Thus, this Application Document refers explicitly to version 2.1 + EDR.

The format used for SSP related data exchange is the Extended Inquiry Response (EIR) format , which is described in Section 3. However, the format is specified by the *Bluetooth* Special Interest Group (SIG), which may 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 the format).

1.1 Audience

The audience of this document is all the NFC Forum members and *Bluetooth* SIG members interested in implementing the *Bluetooth* SSP using NFC.

1.2 Applicable Documents or References

[BLUETOOTH_CORE] *Bluetooth* Core Specification version 2.1 + EDR and later, Bluetooth SIG, July 26, 2007.

https://www.bluetooth.org/Technical/Specifications/adopted.htm

In this document, references to sections or pages of *Bluetooth* Core Specification refer to Version 2.1 + EDR. Different paragraph numbers or page numbers may apply for different revisions of *Bluetooth* Core Specifications.

[BLUETOOTH_NUMBERS] *Bluetooth* Assigned Numbers, *Bluetooth* SIG, https://www.bluetooth.org/Technical/AssignedNumbers/home.htm

[CH] NFC Forum Connection Handover Technical Specification, Version 1.2, NFC Forum

[NDEF] NFC Data Exchange Format, Version 1.0, 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), Version 1.0, NFC Forum
[URI_RTD]	NFC URI Record Type Definition Technical Specification, Version 1.0, NFC Forum
[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, S. Bradner, March 1997, Internet Engineering Task Force

1.3 Administration

The NFC Forum *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 Reference Application Framework technical working group maintains this Application Document.

1.4 Name and Logo Usage

The Near Field Communication Forum's policy regarding the use of the trademarks *NFC Forum* and the NFC Forum logo is as follows:

- Any company MAY claim compatibility with NFC Forum specifications, whether a member of the NFC Forum or not.
- Permission to use the NFC Forum logos is automatically granted to designated members only as stipulated on the most recent Membership Privileges document, during the period of time for which their membership dues are paid.
- Member's distributors and sales representatives MAY use the NFC Forum logo in promoting member's products sold under the name of the member.
- The logo SHALL be printed in black or in color as illustrated on the Logo Page that is available from the NFC Forum at the address above. The aspect ratio of the logo SHALL be maintained, but the size MAY be varied. Nothing MAY be added to or deleted from the logos.
- Since the NFC Forum name is a trademark of the Near Field Communication Forum, the following statement SHALL be included in all published literature and advertising material in which the name or logo appears:

  NFC Forum and the NFC Forum logo are trademarks of the Near Field Communication Forum.

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 Special Word Usage

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

1.7 Abbreviations

Table 1: Abbreviations

Abbreviation	Context	Description
A2DP	*Bluetooth* SIG	Advanced Audio Distribution Profile
ac	NFC Forum	Alternative Carrier
BD_ADDR	*Bluetooth* SIG	*Bluetooth* Device Address
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
M	*Bluetooth* SIG	Mandatory
MB	NFC Forum	Message Begin
ME	NFC Forum	Message End
MITM	N/A	Man In The Middle
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
TNF	NFC Forum	Type Name Format
UI	N/A	User Interface
UID	*Bluetooth* SIG	Unique Identifier
UUID	*Bluetooth* SIG	Universal Unique Identifier

1.8 Glossary

Alternative Carrier / NFC Forum

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

Carrier Configuration Data / NFC Forum

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

Bluetooth Device

A device that implements [BLUETOOTH_CORE].

NFC Forum Device

A device that is certified by NFC Forum.

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.

Negotiated Handover / NFC Forum

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

Out-of-band / Bluetooth SIG

Communication that belongs to but occurs outside of an intended communication channel or method. In this document, "out-of-band" refers to data transmission over NFC for the purpose of pairing devices using *Bluetooth* SSP and discovering Bluetooth services.

Static Handover / NFC Forum

Provision of "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 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" that enable specific use cases. The specifications are controlled by the *Bluetooth* SIG that licenses the use of the specifications, provided that a product passes all required qualification tests and that the manufacturer lists its qualification results with the *Bluetooth* SIG. 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 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

Discovering a *Bluetooth*-enabled device typically uses the Inquiry procedure to discover other *Bluetooth* devices in the vicinity of the discovering device.

NFC can simplify the discovery process by eliminating the Inquiry process 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 Securely Connect

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). 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, described in Section 3.3) can be exchanged over an NFC link to be used as part of the OOB pairing process.

2.3 Start an Application

NFC can be used to start an application to provide good user experience. For example, the user touches their NFC Forum device to another NFC Forum device to exchange contact information. Starting an application upon NFC 'touch' action is implementation specific. In some cases, the 'touch' could even allow the user to select the application to execute.

3 Handover to a *Bluetooth* Carrier

The *Bluetooth* SIG defined a mechanism called "Secure Simple Pairing" ([BLUETOOTH_CORE], Volume 2, Part H, Section 7) to simplify the process of pairing two *Bluetooth* devices. Secure Simple Pairing defines four different association models, one of them using an Out-of-Band channel such as NFC.

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

The *Bluetooth* SIG has defined a Media-type per [RFC2046] for 'Secure Simple Pairing OOB' communication, and "application/vnd.bluetooth.ep.oob" should be used as the [NDEF] record type name. The payload for this type of record is then defined by the Extended Inquiry Response (EIR) format specified in the *Bluetooth* Core Specification ([BLUETOOTH_CORE], Volume 3, Part C, Section 8).

A description of the EIR format is provided in Table 2. However, the format is specified by the *Bluetooth* SIG, which may be updated or changed independently of this document. This Application Document explicitly refers to EIR data as defined in [BLUETOOTH_CORE].

Table 2 reports the generic structure of the *Bluetooth* OOB data. A detailed description of each field is reported in the following sub-sections.

Table 2: *Bluetooth* OOB Data

Name	Offset (Octets)	Size	Mandatory / Optional	Description
OOB Data Length	0	2 octets	M	The total length including the OOB Data Length, the Bluetooth Device Address, and the OOB Optional Data fields (see Section 3.1)
Bluetooth Device Address	2	6 octets	M	*Bluetooth* Device Address of the device (see Section 3.2)
OOB Optional Data	8	N octets	O	The remaining optional OOB data, in EIR format (see Section 3.3)

3.1 OOB Data Length

This length value provides the absolute length of total OOB data block[1], which includes the length field itself and the *Bluetooth* Device Address. The minimum length that may be represented in this field is 8.

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

3.2 *Bluetooth* Device Address

The *Bluetooth* Device Address is uniquely assigned and is used to connect to another *Bluetooth* device. For more details, see [BLUETOOTH_CORE] Volume 2, Part B, Section 1.2, on page 62. As indicated in [BLUETOOTH_CORE] Volume 3, Part C, Section 8.1, 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.

3.3 OOB Optional Data

The OOB Optional Data format is defined in [BLUETOOTH_CORE] Volume 3, Part C, Figure 8.1. There are a number of EIR data types defined by the *Bluetooth* SIG (for more details, see the Generic Access Profile (GAP) section of [BLUETOOTH_NUMBERS]). The 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 may include other EIR data types.

As such, an NFC handover implementation receiving OOB EIR formatted data should be prepared to receive all possible EIR data type values, including values that are currently reserved for future use, in any order. 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 Octet)	Description
0x09 or 0x08	*Bluetooth* Local Name (Section 3.3.1)
0x0E	Simple Pairing Hash C (Section 3.3.2)
0x0F	Simple Pairing Randomizer R (Section 3.3.3)

[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 should be included. The [BLUETOOTH_CORE] Version 4.0 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 such that the length field conforms to the definition in Section 5.2.2.7 wherein the length field includes the mandatory fields.

Value (1 Octet)	Description
0x02, 0x03, 0x04, 0x05, 0x06, or 0x07	Service Class UUID (different lengths based on *Bluetooth* SIG allocated base UUID) (Section 3.3.4)
0x0D	Class of Device (Section 3.3.5)

Additional EIR data types (not shown in [Table 3]) are defined by the *Bluetooth* SIG for other types of information, including a manufacturer-specific type for proprietary information to be included within the standard format[2] (see [BLUETOOTH_CORE] Volume 3, Part C, Section 8.1.4).

3.3.1 *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 is the name that may be displayed to the device user as part of the UI involving operations with *Bluetooth* devices.

3.3.2 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. It should be noted that on passive NFC Forum tags provision of the freshly generated Hash C is not possible due to the fact that data is static and not modifiable[3].

3.3.3 Simple Pairing Randomizer R Information

The Simple Pairing Randomizer R is defined in [BLUETOOTH_CORE] Volume 2, Part H, Section 7.2.2, which provides details for scenarios where inclusion of Randomizer R value is appropriate[3]. It is worth noting that the Randomizer R is optional, and if not present a value of 0 is assumed.

[2] There are different EIR data types to indicate additional semantics such as “partial” and “complete”. For more details, please refer to [BLUETOOTH_CORE] Volume 3, Part C, Section 8.

[3] Note the special case of an NFC Forum Tag that is able to dynamically modify its Data (active NFC Device performing Tag emulation or similar). This allows including freshly generated Simple Pairing Hash C and Randomizer R to establish a secure Bluetooth connection without user further interaction beyond the “NFC touch”.

3.3.4 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 may be truncated from the full 128-bit UUID to a 16-bit or 32-bit abbreviated version based on the *Bluetooth* SIG BASE_UUID (for more details, see [BLUETOOTH_NUMBERS] Service Discovery).

The Service Class UUID element in the EIR format represents a list of UUIDs that are grouped together based on 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 as being 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 such that the payload has contiguous UUIDs (the size of each UUID is determined by the EIR type associated with that payload). For example, if an EIR tag 0x03 has the length 11, then the payload will contain 5 UUIDs in their 16-bit representation. For more details, see [BLUETOOTH_CORE] Volume 3, Part C, Section 8.1.1, [BLUETOOTH_CORE] Volume 3, Part B, and [BLUETOOTH_NUMBERS] Service Discovery.

3.3.5 Class of Device Information

The Class of Device information is to be used to provide a graphical representation to the user as part of UI involving operations with *Bluetooth* devices. For example, it may provide a particular icon to present the device.

This field is not supposed to be directly used for determining whether or not a particular service can be used because it is aimed at providing information to the user about the type of device they are engaging with. An illustrative example is that a device may be a "Desktop workstation" and provide 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 may indicate the general categories of services that the device may provide.

Determining the support for services is based on the supported Service Class UUIDs (see Section 3.3.4).

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.

4 Examples

4.1 Negotiated Handover

Figure 1 shows a sample Handover Request Message from a device with only *Bluetooth* communication capability using the mime-type “application/vnd.bluetooth.ep.oob”.

Table 4 describes a sample Handover Request Message that could be sent by a camera device that has a *Bluetooth* radio available.

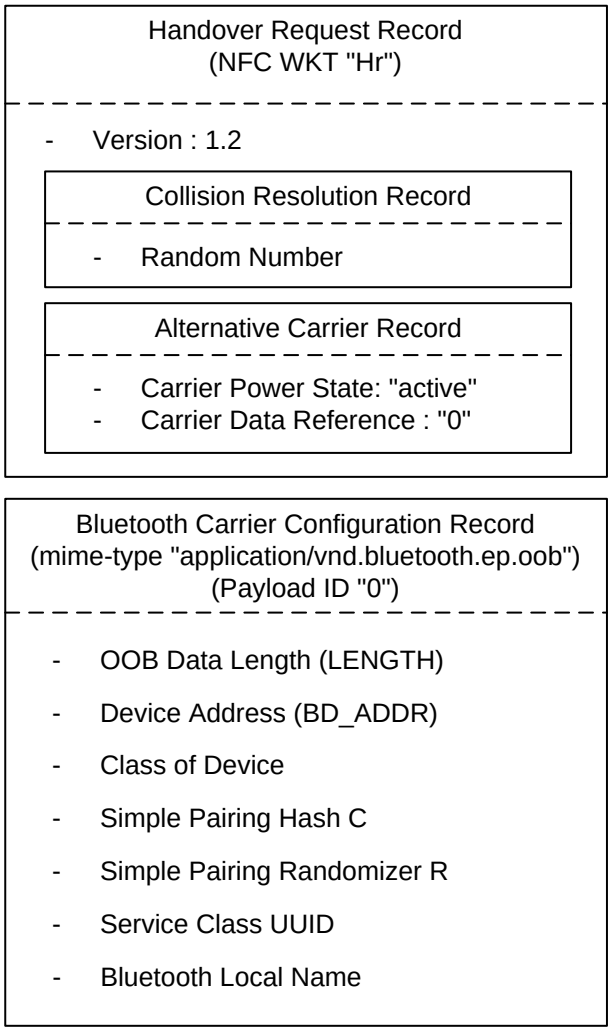

Figure 1: *Bluetooth* Handover Request Message

Note that 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. A device 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 4: Binary Content of a Sample *Bluetooth* Handover Request Message

Offset (Octets)	Content	Length (Octets)	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 octets
2	0x11	1	Payload Length: 17 octets
3	0x48 0x72	2	Record Type: "Hr"
5	0x12	1	Version Number: Major = 1, Minor = 2
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 octets
8	0x02	1	Payload Length: 2 octets
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 octets
15	0x04	1	Payload Length: 4 octets
16	0x61 0x63	2	Record Type: "ac"
18	0x01	1	Carrier Flags: CPS=1, "active"
19	0x01	1	Carrier Data Reference Length: 1 octet
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 octets
24	0x43	1	Payload Length: 67 octets
25	0x01	1	Payload ID Length: 1 octet
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 octets
61	0x01 0x07 0x80 0x80 0xBF 0xA1	6	*Bluetooth* Device Address: A1:BF:80:80:07:01
67	0x04	1	EIR Data Length: 4 octets

Offset (Octets)	Content	Length (Octets)	Explanation
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 octets
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 octets
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 octets
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 octets
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

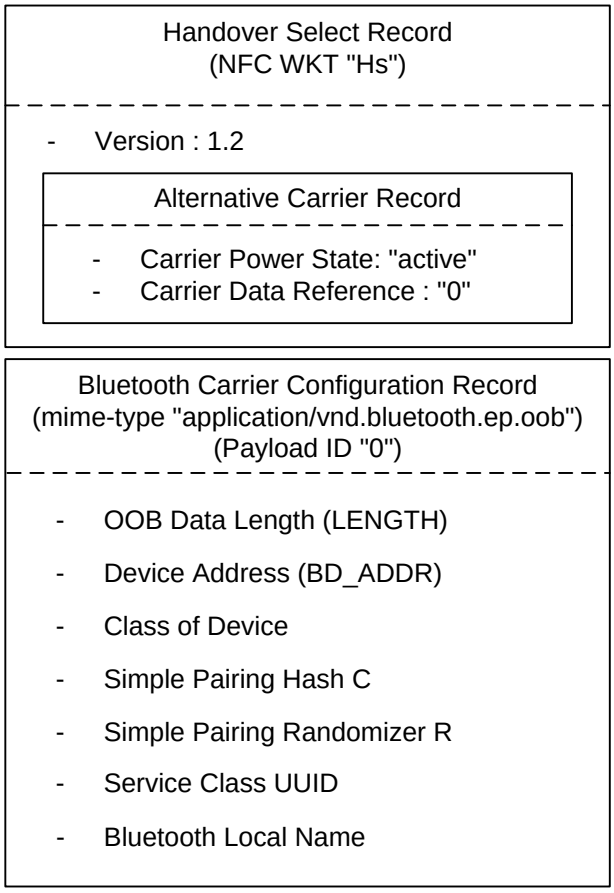

Figure 2: *Bluetooth* Handover Select Message

Figure 2 shows the structure of a Handover Select Message returned by a Handover Selector device that acknowledges a *Bluetooth* carrier.

Table 5 describes a sample Handover Select Message that could be returned by a printer device that has a *Bluetooth* radio available.

Note that [BLUETOOTH_CORE] requires all numerical multi-octet entities and values associated with the following data types use Little Endian order. Hence, in the examples presented in this document, the following fields are encoded using Little Endian order:

- '*Bluetooth* OOB Data Length';
- '*Bluetooth* Device Address';
- 'Class of Device';
- '16-bit Service Class UUID list (complete)';
- Simple Pairing Hash C;
- Simple Pairing Randomizer R.

Table 5: Binary Content of a Sample *Bluetooth* Handover Select Message

Offset (Octets)	Content	Length (Octets)	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 octets
2	0x0A	1	Record Type Length: 10 octets
3	0x48 0x73	2	Record Type: "Hs"
5	0x12	1	Version Number: Major = 1, Minor = 2
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 octets
8	0x04	1	Payload Length: 4 octets
9	0x61 0x63	2	Record Type: "ac"
11	0x01	1	Carrier Flags: CPS=1, "active"
12	0x01	1	Carrier Data Reference Length: 1 octet
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 octets
17	0x43	1	Payload Length: 67 octets
18	0x01	1	Payload ID Length: 1 octet
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 octets
54	0x03 0x07 0x80 0x88 0xbf 0x01	6	*Bluetooth* Device Address: 01:bf:88:80:07:03
60	0x04	1	EIR Data Length (4 octets)
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 octets

Offset (Octets)	**Content**	**Length** (Octets)	**Explanation**
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 octets
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 octets
102	0x03	1	EIR Data Type: 16-bit Service Class UUID list (complete)
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 octets
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

4.2 Static Handover

A Static Handover can be used in cases where the Handover Selector device is equipped with an NFC Forum Tag only. Therefore, it cannot actively reply to a Handover Request Message. A Handover Requester device detects this message during the NFC discovery phase and will then be able to read data from the NFC Forum Tag. If the data that is read embodies a Handover Select Message, the Handover Requester can use this information to choose one of the indicated alternative carriers and try to establish a secondary connection.

In principle, the Handover Select Message stored on a NFC Forum Tag is identical to a Handover Select Message returned by an active NFC Forum Device. However, due to the static nature of data on a tag, a pre-stored Handover Select Message will always have to indicate all available carriers because carriers cannot automatically be powered as a result of the NFC touch, and dynamic carrier-specific protocol information, such as non-static IP addresses, cannot be provided.

Figure 3 shows an example where *Bluetooth* configuration data is included into an Handover Select Message stored on an NFC Forum Tag.

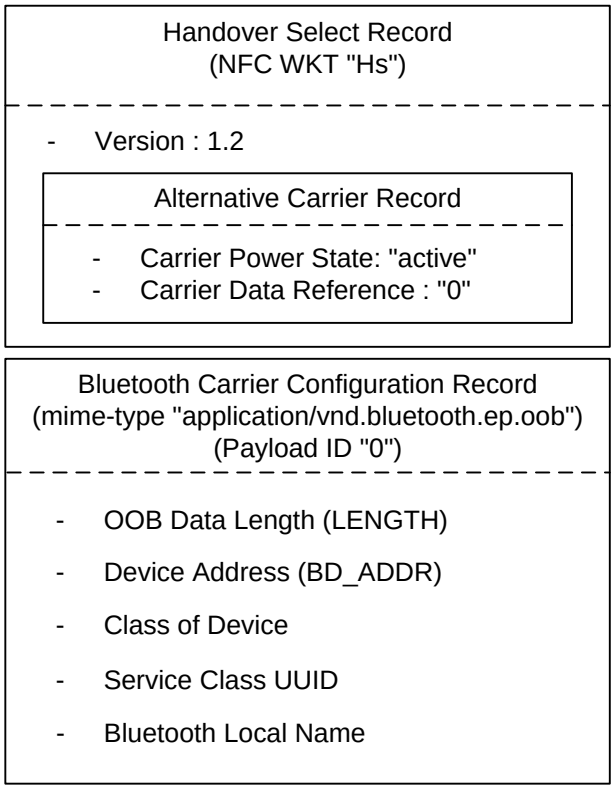

Figure 3: *Bluetooth* Configuration Data on NFC Forum Tag

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

If alternative carriers cannot be ensured to be active, the carrier power state should be set to either "inactive" or "unknown", which results in the behavior of the Handover requester as undefined. A possible strategy for the Handover requester could be to request the user to perform a manual activation for a carrier signaled as "inactive" and to first try and then possibly request manual activation for a carrier with "unknown" power state.

The binary layout of a Handover Select Message for a *Bluetooth* carrier stored on an NFC Forum Tag is shown in Table 6, which presents the *Bluetooth* Configuration Data that can be advertised by a printer device that supports the Basic Printing Profile. It is worth noting that 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 6: Binary Content of a Sample *Bluetooth* Handover Select Message on an NFC Forum Tag

Offset (Octets)	Content	Length (Octets)	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 octets
2	0x0A	1	Record Type Length: 10 octets
3	0x48 0x73	2	Record Type: "Hs"
5	0x12	1	Version Number: Major = 1, Minor = 2
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 octets
8	0x04	1	Payload Length: 4 octets
9	0x61 0x63	2	Record Type: "ac"
11	0x03	1	Carrier Flags: CPS=3, "unknown"
12	0x01	1	Carrier Data Reference Length: 1 octet
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 octets
17	0x1F	1	Payload Length: 31 octets
18	0x01	1	Payload ID Length: 1 octet
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 octets
54	0x03 0x07 0x80 0x88 0xbf 0x01	6	*Bluetooth* Device Address: 01:bf:88:80:07:03
60	0x04	1	EIR Data Length: 4 octets
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 octets

Offset (Octets)	**Content**	**Length** (Octets)	**Explanation**
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 octets
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

4.2.1 Simplified Tag Format for a Single *Bluetooth* Carrier

In case a Handover Selector device would advertise only one alternative carrier (i.e., a *Bluetooth* carrier), a simplified format without the Handover Select record may be used. In this case, the NFC Forum Tag contains an NDEF message with only the *Bluetooth* OOB information.

Figure 4 illustrates how *Bluetooth* configuration data is included in an NDEF message.

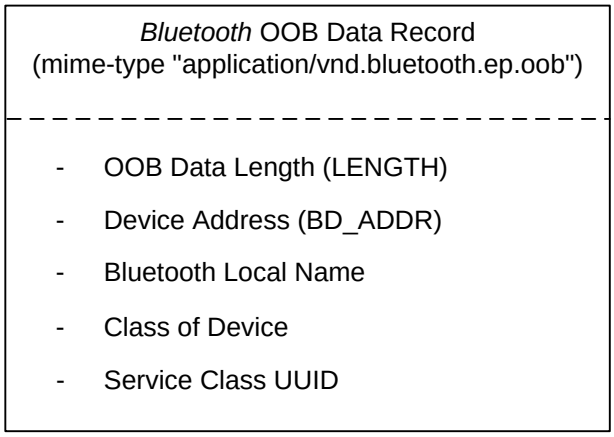

Figure 4: *Bluetooth* OOB Data on NFC Forum Tag

The binary layout of an NDEF message without the Handover Select Record for a *Bluetooth* carrier stored on an NFC Forum Tag is shown in Table 7. The *Bluetooth* Configuration Data is an example of a device indicating a type of headset, and it includes the following optional OOB data fields: the Class of Device, Complete Local Name, and Service Class UUID.

Table 7: Binary Content of a Sample *Bluetooth* OOB Data on an NFC Forum Tag

Offset (Octets)	Content	Length (Octets)	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 octets
2	0x21	1	Payload Length: 33 octets
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 octets)
37	0x06 0x05 0x04 0x03 0x02 0x01	6	*Bluetooth* Device Address: 01:02:03:04:05:06
43	0x0D	1	EIR Data Length: 13 octets
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 octets
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 octets
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

A. Revision History

The following table outlines the revision history of *Bluetooth* Secure Simple Pairing Using NFC.

Table 8: 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