Connection Handover

Technical Specification

NFC Forum^{TM}

Connection Handover 1.1

NFCForum-TS-ConnectionHandover_1.1

2008-11-06

RESTRICTIONS ON USE

Contents

Figures

Tables

1 Introduction

The Connection Handover specification defines NFC Forum Well Known Types and the corresponding message structure that allows negotiation and activation of an alternative communication carrier. The negotiated communication carrier would then be used to perform certain activities between the two devices, such as printing to a Bluetooth printer or streaming video to a WLAN television set.

1.1 Objectives

The objective of this specification is to provide a generic mechanism to negotiate and activate an alternative communication carrier between two NFC Forum devices. The mechanism is intended to allow for applications to be built that need to use a communication system other than NFC to transmit relatively large amounts of data or use services not available via the NFC link.

It is not the objective of this specification to provide any definitions that are specific to alternative communication carriers or to define how an application would accomplish a given task once switched to an alternative carrier. Such information needs to be given in other specifications, either released in the future by the NFC Forum or disclosed by other organizations. However, this document does provide informative examples of how to apply the Connection Handover specification to selected use cases.

1.2 Purpose

The Connection Handover specification aims to enable applications to take advantage of NFC technology for initiating and executing user-defined activities between devices. This specification delivers a toolset that ensures compatibility between the actors but requires further definitions to achieve full interoperability. Usage examples for some applications are provided as an appendix to this document, but normative definitions need to be provided by other specifications. It is intended that standardization bodies or industry alliances use this specification.

1.2.1 Mission Statement and Goals

Near Field Communication (NFC) technology can be used to design extremely intuitive user interfaces that involve activities between two devices. For example, a digital still picture camera might directly print an image that is currently shown in review mode when the user touches the camera’s NFC interface to an NFC-equipped printer. Likewise, music files could be automatically synchronized between a mobile player and a home media center upon a simple touch.

However, NFC alone might not be suitable for some scenarios, such as transferring large files, due to the inconvenience of keeping the interfaces of the two devices in close proximity for an extended period of time. Furthermore, many existing applications are designed to use other communication carriers and cannot be easily modified to use NFC.

The Connection Handover specification intends to solve these issues by providing the means for two NFC-equipped devices to negotiate and use an alternative communication carrier that is better suited to perform the desired task.

1.3 References

[NDEF] “NFC Data Exchange Format Specification”, NFC Forum, 2006.

[NFC RTD] “NFC Record Type Definition (RTD) Specification”, NFC Forum, 2006.

[NFC URI] “URI Record Type Definition (RTD) Specification”, NFC Forum, 2006.

[RFC 959] J. Postel, J. Reynolds, “File Transfer Protocol (FTP)”, RFC 959, ISI, October 1985.

[RFC 2119] S. Bradner, “Key words for use in RFCs to Indicate Requirement Levels”, RFC 2119, Harvard University, March 1997.

[RFC 3986] T. Berners-Lee, R. Fielding, L. Masinter, “Uniform Resource Identifiers (URI): Generic Syntax”, RFC 3986, MIT/LCS, U.C. Irvine, Xerox Corporation, January 2005.

[RFC 4234] D. Crocker, P. Overell, “Augmented BNF for Syntax Specifications: ABNF”, RFC 4234, October 2005.

[RFC 2616] R. Fielding, J. Gettys, J. C. Mogul, H. F. Nielsen, T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.1”, RFC 2616, U.C. Irvine, DEC W3C/MIT, DEC, W3C/MIT, W3C/MIT, January 1997.

[WFA WPS] Wi-Fi Protected Setup Specification 1.0, Wi-Fi Alliance, December 2006.

[BT2.1+EDR] Bluetooth Core Specification version 2.1 + EDR, Bluetooth SIG, 26 July 2007.

[UPNP UDA] UPnP Device Architecture 1.0, UPnP Forum, Version 1.0.1, July 2006.

1.4 Administration

The NFC Forum Connection Handover specification is an open specification 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 technical working group maintains this specification.

1.5 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 RFC 2119.

1.6 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.

1.7 Intellectual Property

The Connection Handover specification conforms to the Intellectual Property guidelines specified in the NFC Forum's Intellectual Property Right Policy, as approved on November 9, 2004 and outlined in the NFC Forum Rules of Procedures, as approved on December 17, 2004, and revised on June 23, 2007.

1.8 Glossary

Negotiated Handover

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.

Static Handover

Provision of an NDEF message on an NFC Forum Tag that allows a reading NFC Forum Device to select and use alternative carriers for further data exchange.

Handover Requester

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

Handover Selector

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.

Alternative Carrier

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

Carrier Configuration Data

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

2 Handover Protocol

2.1 Introduction

This specification defines NDEF messages that enable a Handover Requester to negotiate an alternative communication carrier with a Handover Selector over the NFC link. As a special case, it also enables a Handover Requester to retrieve the possible alternative communication carrier(s) from an NFC Forum Tag, but this has some limitations due to the static nature of information stored on a Tag. The first case is called “Negotiated Handover” and is described in section 2.2, while the second case is called “Static Handover” and is described in section 2.3.

The Handover Requester, in the scope of this specification, is defined to be the device that initiates the handover operation. The Handover Selector device is defined to be the device that is initially passive and that responds to the Handover Requester. The Handover Selector does not start any activity such as generating a handover message.

2.2 Negotiated Handover

Negotiated Handover allows two devices to negotiate one or more alternative carriers for further data exchange. The exemplary use case shown in Figure 1 illustrates how a Handover Requester uses the embedded NFC Forum Device to exchange connection handover information with the Handover Selector to finally select a matching alternative carrier. In the example, the application running on the Handover Requester first announces its alternative carriers (Wi-Fi and Bluetooth wireless technology) to the Handover Selector, and then receives a carrier selection (Bluetooth wireless technology) as the only choice and finally performs Bluetooth pairing and data exchange.

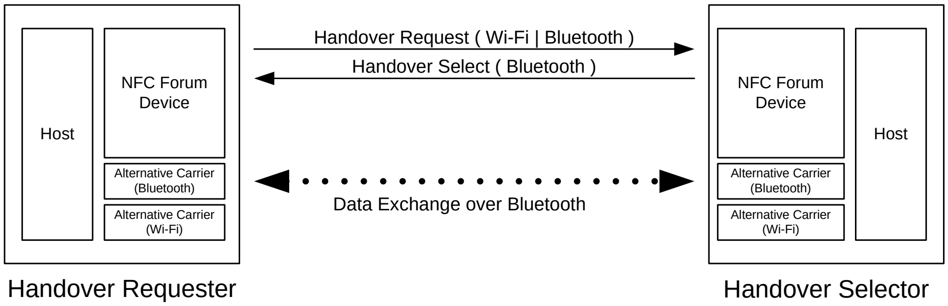

Host
NFC Forum Device
Alternative Carrier (Bluetooth)
Alternative Carrier (Wi-Fi)
Handover Request (Wi-Fi | Bluetooth)
Handover Select (Bluetooth)
Data Exchange over Bluetooth
NFC Forum Device
Alternative Carrier (Bluetooth)
Alternative Carrier (Wi-Fi)
Host
Handover Requester
Handover Selector

Figure 1: Negotiated Handover with Single Selection

If the Handover Selector supports multiple alternative carriers, it might return more than one selection (see Figure 2). In this case, the Handover Requester is free to choose any of the returned carriers or even try to simultaneously connect to more than one alternative carrier. However, if the Handover Requester attempts to choose one of the selected carriers, it should interpret the order that they are listed in the Handover Select message as a preference indication. In the example of Figure 2, the Handover Requester has decided against the Handover Selector’s preference for Wi-Fi and has used Bluetooth wireless technology instead.

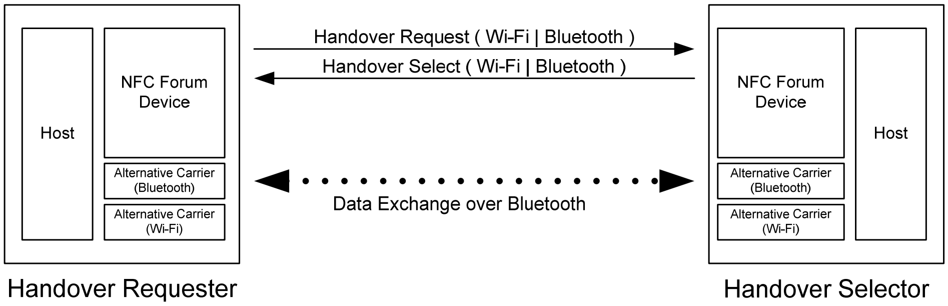

Handover Request (Wi-Fi | Bluetooth)
Handover Select (Wi-Fi | Bluetooth)
Host
NFC Forum Device
Alternative Carrier (Bluetooth)
Alternative Carrier (Wi-Fi)
Data Exchange over Bluetooth
NFC Forum Device
Alternative Carrier (Bluetooth)
Alternative Carrier (Wi-Fi)
Host
Handover Requester
Handover Selector

Figure 2: Negotiated Handover with Multiple Selections

A third example (Figure 3) illustrates how a Handover Requester might use a second alternative carrier selection to enhance the user experience. In the example, the Handover Selector again returns both Wi-Fi and Bluetooth wireless technology, but this time with Bluetooth wireless technology as the first preference. The Requester first tries to establish a Bluetooth connection which fails (for example, because the devices have moved outside of Bluetooth radio range). In this case, the application might decide to try the Wi-Fi connection before aborting.

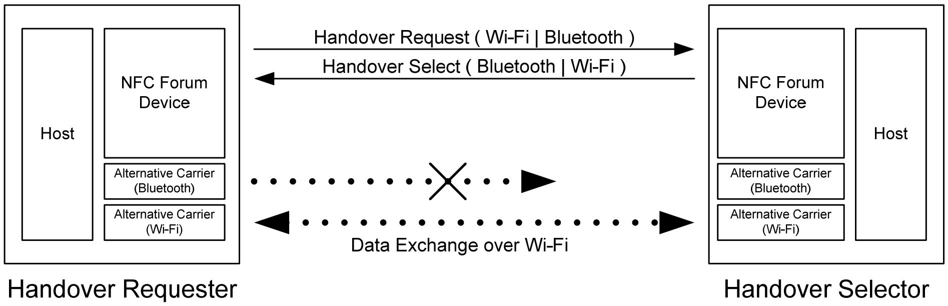

Handover Request (Wi-Fi | Bluetooth)
Handover Select (Bluetooth | Wi-Fi)
Host
NFC Forum Device
Alternative Carrier (Bluetooth)
Alternative Carrier (Wi-Fi)
Data Exchange over Wi-Fi
NFC Forum Device
Alternative Carrier (Bluetooth)
Alternative Carrier (Wi-Fi)
Host
Handover Requester
Handover Selector

Figure 3: Negotiated Handover with Multiple Selections

A Handover Selector device with limited power resources (for example, battery driven) might not want to activate all alternative carrier circuits in case it has more than a single carrier in common with the Handover Requester. In this situation, the Handover Selector MAY set the Carrier Power State flag of all returned Alternative Carrier Records to zero (inactive). This will cause the Handover Requester to send a subsequent Handover Request Message with only one of the previously received alternative carriers listed. The Handover Selector SHALL acknowledge this request with the return of a Handover Select Message (see Figure 4) where the Carrier Power State flag MUST be set to 1 (active). Note that the Handover Selector does not need to maintain state information between its two responses.

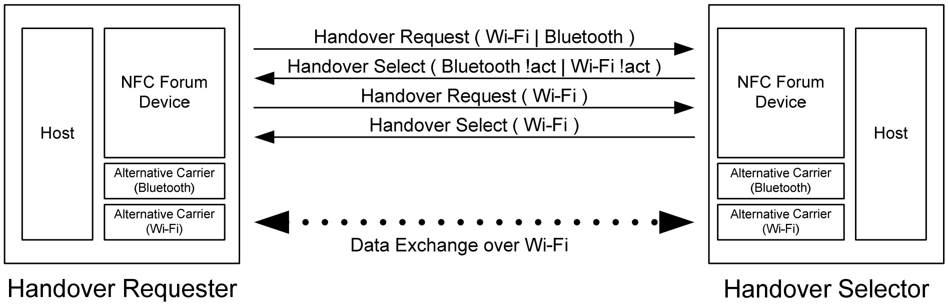

Handover Request (Wi-Fi | Bluetooth)
Handover Select (Bluetooth !act | Wi-Fi !act)
Handover Request (Wi-Fi)
Handover Select (Wi-Fi)
Host
NFC Forum Device
Alternative Carrier (Bluetooth)
Alternative Carrier (Wi-Fi)
Data Exchange over Wi-Fi
Handover Requester
Handover Selector

Figure 4: Negotiated Handover with a Power-constrained Device

As shown with the preceding examples, the process of a negotiated handover is performed with the exchange of two messages in the following sequence (see Figure 5):

1. The Handover Requester sends a Handover Request Message to the Handover Selector device. This message proposes a number of alternative communication carriers that the Handover Requester would be able to utilize for the intended activity. A proposed carrier might be provided with or without carrier configuration information. The message might state further carrier-associated requirements.
2. The Handover Selector device compares this list with its own communication facilities, possibly taking connectivity status and carrier specific requirements into account. It then returns a Handover Select Message containing a list of appropriate communication carriers, each associated with a carrier-specific configuration record. If it is not possible to use any of the proposed carriers, the Handover Selector returns an empty list.

If the Handover Selector device returns a non-empty list of alternative carriers, the handover protocol is successfully completed and establishing communication depends on the selected carrier(s). Information indicating how to establish a connection to the alternative carrier(s) MUST be provided in a carrier-specific configuration record inside the Handover Select Message and this record MUST be referenced as described in section 2.4. If the Handover Selector accepts a carrier that has been proposed with configuration information, it needs to copy the relevant information to the corresponding Handover Select Message.

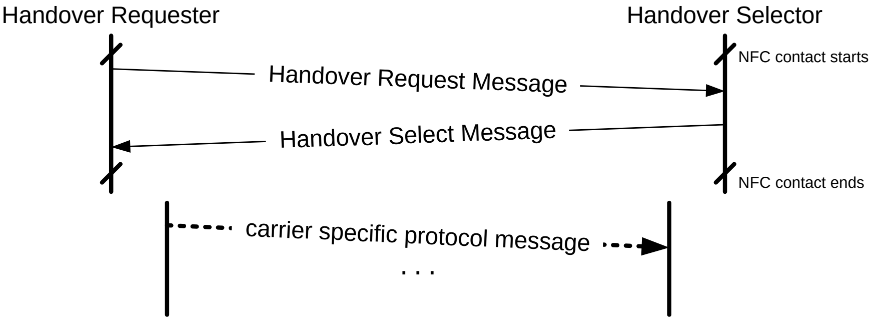


Figure 5: Negotiated Handover Message Sequence

If the Handover Selector device does not acknowledge at least one of the proposed alternative carriers, the Handover Requester might want to repeat the sequence with different settings. This could be useful if the Handover Requester has a strong preference on a certain communication carrier or properties. However, the Handover Selector device SHOULD compare the proposed carriers in the same order as they are listed in the Handover Request Message and give preference to those listed first.

A Handover Selector SHOULD answer a Handover Request Message within 1 second; otherwise, the Handover Requester MAY assume a processing error. Note that the message transport layer is assumed to guarantee delivery of Handover messages over the NFC link. See section 2.8 for more details.

2.3 Static Handover

The Static Handover can be used when the Handover Selector device does not constitute an NFC Forum Device but has a (cheaper) NFC Forum Tag attached (see Figure 6). NFC Forum Tags provide storage space that can be read or written but might not have an internal connection with the Host processor. It is not possible for an NFC Forum Tag to receive and interpret a Handover Request Message and to dynamically construct a corresponding Handover Select Message.

In this case the Tag contains a Handover Select Record plus additional information records that are referenced as described in section 2.4. Because this is static information, it cannot be adapted to any possible requirements that a Handover Requester might provide with Negotiated Handover. Also, dynamic information (for example, a dynamically-assigned IP address) cannot be provided sensibly.

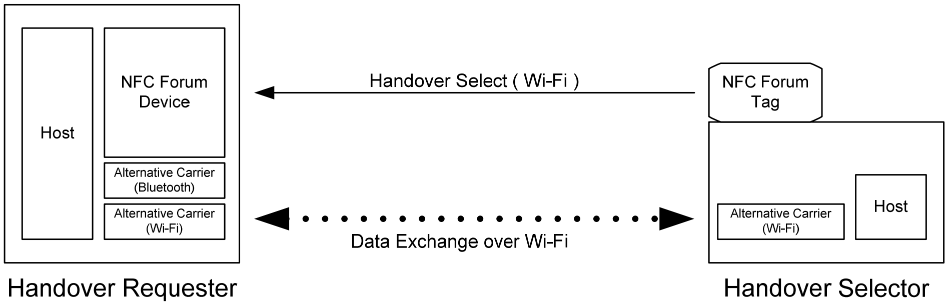

Host
NFC Forum Device
Alternative Carrier (Bluetooth)
Alternative Carrier (Wi-Fi)
Handover Select (Wi-Fi)
NFC Forum Tag
Alternative Carrier (Wi-Fi)
Host
Data Exchange over Wi-Fi
Handover Requester
Handover Selector

Figure 6: Static Handover

A further drawback of Static Handover is that the Handover Selector's Host processor will not be able to activate its alternative carrier circuits as part of the handover process. All carrier circuits either have to be continuously active or have to be activated explicitly by the user.

2.4 Message Composition

A handover message is composed of either a Handover Request Record (NFC Forum Global Type “Hr”) or a Handover Select Record (NFC Forum Global Type “Hs”), followed by an arbitrary number of other NDEF records.

Within a Handover Request or Handover Select Record, a sequence of Alternative Carrier Records (NFC Forum Local Type “ac”) defines the alternative carriers that are requested or selected, respectively. The actual information is provided with the NDEF records that follow the leading message record and the Alternative Carrier Record provides references to those belonging to the given alternative carrier (see Figure 7).

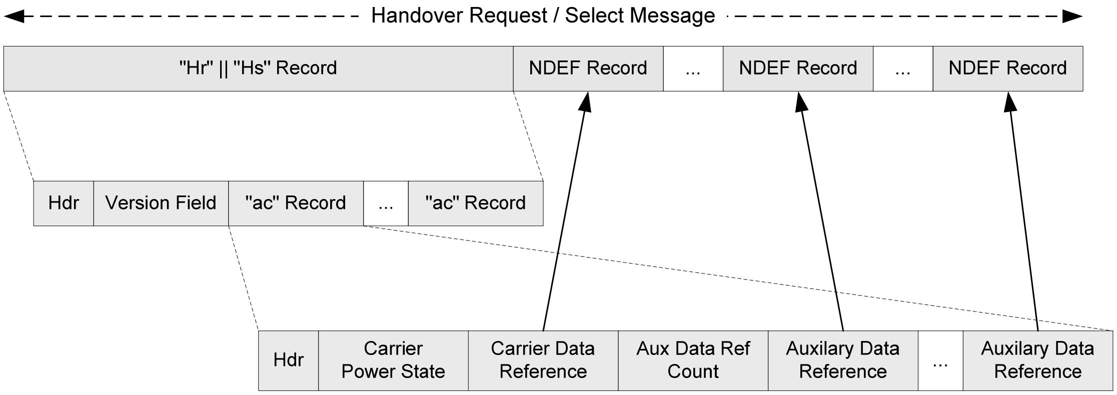


Figure 7: General Message Composition

The record references are established using the URI-based Payload Identification mechanism described in the NDEF specification [NDEF]. The URI reference values SHALL be encoded as relative URIs with the virtual base defined as “urn:nfc:handover:”.

The message generator is responsible for the uniqueness of the payload identifiers encoded into the ID field of the NDEF record header. While identifiers can be strings of length up to 255 characters, it is RECOMMENDED that short, possibly single character, strings are used. However, the generator SHALL NOT use the tilde character (“~”, hexadecimal 7E) at the first string position and a compliant parser SHALL ignore strings starting with a tilde character.

2.5 Carrier Type Identification

The type of carrier described by an Alternative Carrier Record is indirectly given via the Carrier Data Reference link.

If the referenced NDEF record is a Handover Carrier Record (NFC Forum Global Type “Hc”) as defined in this specification, the carrier type is identified by the Carrier Name structure within the payload of the Handover Carrier Record. The syntax of the Carrier Name structure is equivalent to the NDEF record type. The Handover Carrier Record MUST be used by a Handover Requester when an alternative carrier is proposed without configuration data.

If the referenced NDEF record is not a Handover Carrier Record, then the carrier type is identified with the NDEF record payload type (the triple {*TNF*, *TYPE_LENGTH*, *TYPE*}), and the payload of the record MUST provide carrier-specific configuration information as needed to connect to the carrier. For brevity, this type of NDEF record is called Carrier Configuration Record, but this is only a conceptual name, and no record named such is defined in this specification.

2.6 Carrier Power State

Handover devices with limited power resources might want to activate (that is, power up) carrier circuits only when they are requested by a handover activity. For this purpose, a device can indicate the power status for each of the proposed or available alternative carriers within the Alternative Carrier Record. The possible values for the Carrier Power State are defined in Table 2. For brevity, we will refer to them as “active”, “inactive”, “activating”, or “unknown”.

If a carrier is declared “active” and carrier configuration data is provided, the peer device MAY immediately use the configuration data and connect to the carrier.

If the carrier power state is “activating”, the peer device SHOULD expect a delay when trying to connect to the carrier because the circuit was not yet powered when the message was sent out. The exact time needed to activate the carrier is dependent on both technology and implementation and cannot be defined here. It MAY be defined by other organizations.

If a Handover Requester proposes carriers with power state “activating”, it MAY wait for the Handover Selector’s Handover Select Message before actually powering the circuit.

If a Handover Selector does acknowledge carriers with power state “activating”, it SHALL immediately start the activation process after returning the Handover Select Message.

A Handover Selector MAY return one or multiple alternative carriers (with carrier configuration data) that are declared “inactive” if the Handover Requester provided more than one alternative in the Handover Request Message. The Handover Requester SHOULD then request exactly one alternative carrier in a subsequent Handover Request Message. The Handover Selector SHALL respond to this request with the alternative carrier that is declared either “active” or “activating”.

If the Handover Selector is an NFC Forum Tag (Static Handover), it MAY provide a number of “inactive” alternative carriers inside a Handover Select Message stored on the tag. This usually means that the user is expected to manually activate carrier circuits on the device. Nevertheless, a Handover Requester could first try to connect to the carrier(s) as they might have been already activated.

The carrier power state “unknown” is used when the device does not directly support an interface for that carrier and can only be reached via the alternative carrier through a router. However, note that the device MUST be able to provide sufficient carrier configuration data for the peer device to connect to the alternative carrier.

The power state “unknown” MAY be used in both Handover Request and Handover Select messages.

If on-demand activation is used, the implementation should keep the carrier(s) active for a time interval long enough to allow the peer device to connect to the carrier. The value depends on the carrier technology.

2.7 Handover Request Collision

A handover request collision happens if both devices simultaneously send a Handover Request Message after the NFC communication link has been established by the underlying peer-to-peer protocol. Note that if a device intends to send a Handover Request message but receives a Handover Request message from the other device before sending, it SHALL NOT send a Handover Request message, but instead take the role of a “Handover Selector device”.

If a device detects that a Handover Request collision has occurred (that is, it has sent a Handover Request Message and then received a Handover Request Message), it might not be able to resolve the conflict without user guidance. This specification does not provide an automatic resolution process. However, solutions might be provided for specific alternative carrier systems in separate specifications.

2.8 Message Transport

The message exchange for the Negotiated Handover requires a bidirectional, symmetrical NFC communication link between the two NFC Forum devices. NFCIP-1 provides only an asymmetric communication mode, and a protocol layer above NFCIP-1 is needed to provide symmetry of operation as needed for the Handover functionality.

Further, the message transport layer is assumed to provide reliable communication; that is, messages either arrive complete and intact or an error is reported. Note that this includes arrival at the Handover application layer. If no error is reported, a Handover Requester can assume that the peer device also supports NFC Handover.

2.9 Version Handling

Both Handover Request Message and Handover Select Message carry a version number field that SHALL be set equal to the version number of the Connection Handover specification, after which the message content is encoded. The version number is divided into a major and a minor part. A change in the minor version number part indicates backward-compatible changes in the specification that does not affect interoperability. A change in the major version number part implies significant modifications in syntax or semantics, and parsers supporting only prior versions SHALL NOT further interpret the data.

If version numbers do not match exactly, the following rules apply:

- If a Handover Selector reads a Handover Request message with a version number that differs only in the minor part, it SHALL reply with a Handover Select Message formatted according to its own version number.
- If a Handover Selector reads a Handover Request Message with a version number that differs in the major part and is higher than its own version number, it SHALL reply with an empty Handover Select Message (one that does not contain any Alternative Carrier records), and the version number field SHALL be set to the highest supported value.
- If a Handover Selector reads a Handover Request message with a version number that differs in the major part and is lower than its own version number, it MAY reply with an empty Handover Select Message indicating only the version number conflict, or it MAY reply with a Handover Select Message formatted according to the major version used by the Handover Requester.

2.10 Security Considerations

This section is meant to inform application developers and users of the security limitations in the Negotiated and Static Handover protocol described in this specification.

The Handover Protocol requires transmission of network access data and credentials (the carrier configuration data) to allow one device to connect to a wireless network provided by another device. Because of the close proximity needed for communication between NFC Devices and Tags, eavesdropping of carrier configuration data is difficult, but not impossible, without recognition by the legitimate owner of the devices. Transmission of carrier configuration data to devices that can be brought to close proximity is deemed legitimate within the scope of this specification.

In case the legitimate owner of the devices has concerns over the confidentiality of the data, an additional security analysis is necessary that takes the system in question and the operating environment into account.

3 NDEF Structure

The ABNF definition of the Handover messages and records is given in normative Appendix A.

3.1 Message Definitions

3.1.1 Handover Request Message

The Handover Request message is used by a Handover Requester device to propose a number of alternative carriers to the Handover Selector device. The message MUST start with a Handover Request Record that has the message begin (MB) flag set and MUST be followed by a number of NDEF records. The last NDEF record closes the message with the message end (ME) flag set.

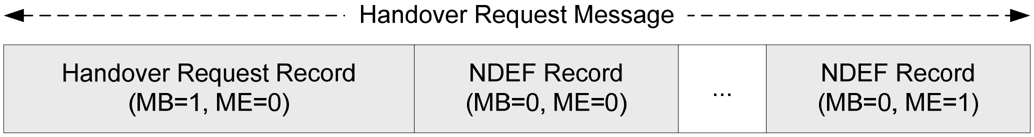


Figure 8: Handover Request Message Structure

Note that a sole Handover Request record with MB and ME set to 1 would not be valid because a Handover Request Message transmits at least one Handover Carrier or Carrier Configuration record to indicate a single alternative carrier.

3.1.2 Handover Select Message

The Handover Select Message is used by the Handover Selector device to acknowledge alternative carriers that were listed in the previously received Handover Request Message. The message MUST start with a Handover Select Record that has the message begin (MB) flag set and MAY be followed by a number of NDEF records, the last one closing the message with the message end (ME) flag set. In case no additional records are transmitted, the Handover Select Record SHALL have both the MB and ME flag set to one.

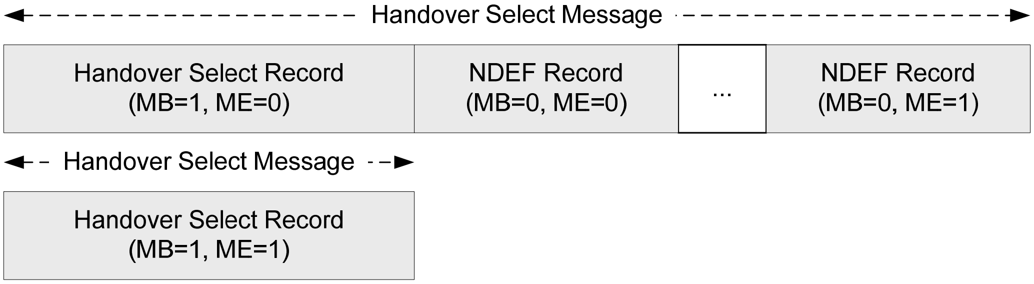


Figure 9: Handover Select Message Structure

Note that a sole Handover Select Record with both MB and ME set to 1 is a valid Handover Select Message that is transmitted if either no matching alternative carrier could be identified or if the version number in the Handover Request Message indicates a message format not supported by the Handover Selector.

3.2 Global Record Definitions

3.2.1 Handover Request Record

The Handover Request Record identifies a list of possible alternative carriers that the Handover Requester device would be able to use for further communication with the Handover Selector. At least a single alternative carrier MUST be specified by the Handover Requester. If multiple alternative carriers are specified, the Handover Selector SHOULD process the records in order and acknowledge the first appropriate match, if any.

Only Alternative Carrier Records have a defined meaning in the payload of a Handover Request Record. However, an implementation SHALL silently ignore and SHALL NOT raise an error if it encounters other unknown record types.

The NFC Forum Well Known Type [NDEF], [NFC RTD] for the Handover Request Record is “Hr” (in NFC binary encoding: 0x48, 0x72).

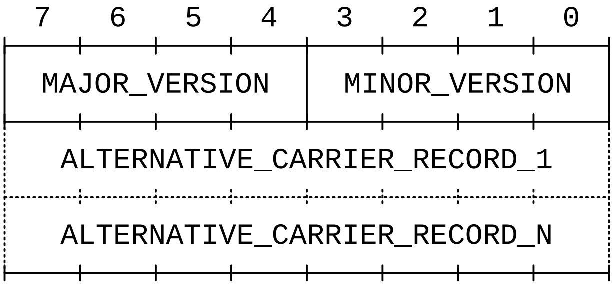


Figure 10: Payload of the Handover Request Record

Semantics for the Handover Request Record:

MAJOR_VERSION: This 4-bit field equals the major version number of the Connection Handover specification and SHALL be set to 0x1 by an implementation that conforms to this specification. When an NDEF parser reads a different value, it SHALL NOT assume backward compatibility.

MINOR_VERSION: This 4-bit field equals the minor version number of the Connection Handover specification and SHALL be set to 0x0 by an implementation that conforms to this specification. When an NDEF parser reads a different value, it MAY assume backward compatibility.

ALTERNATIVE_CARRIER_RECORD: Each record specifies a single alternative carrier that the Handover Requester would be able to utilize for further communication with the Handover Selector device. The Alternative Carrier Record is defined in section 3.3.1.

3.2.2 Handover Select Record

The Handover Select Record identifies the alternative carriers that the Handover Selector device selected from the list provided within the previous Handover Request Message. The Handover Selector MAY acknowledge zero, one, or more of the proposed alternative carriers at its own discretion.

Only Alternative Carrier Records have a defined meaning in the payload of a Handover Select Record. However, an implementation SHALL NOT raise an error if it encounters other record types, but SHOULD silently ignore them.

The NFC Forum Well Known Type [NDEF], [NFC RTD] for the Handover Select record is “Hs” (in NFC binary encoding: 0x48, 0x73).

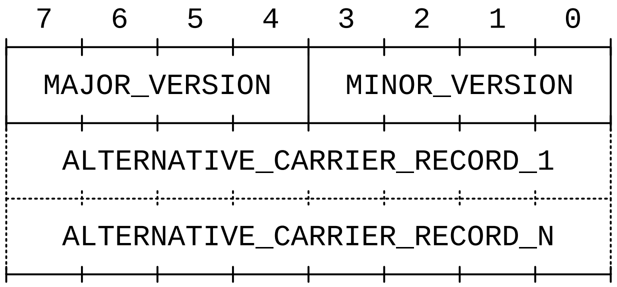


Figure 11: Payload of the Handover Select Record

Semantics for the Handover Select Record:

MAJOR_VERSION: This 4-bit field equals the major version number of the Connection Handover specification and SHALL be set to 0x1 by an implementation that conforms to this specification. When an NDEF parser reads a different value, it SHALL NOT assume backward compatibility.

MINOR_VERSION: This 4-bit field equals the minor version number of the Connection Handover specification and SHALL be set to 0x0 by an implementation that conforms to this specification. When an NDEF parser reads a different value, it MAY assume backward compatibility.

ALTERNATIVE_CARRIER_RECORD: Each record specifies a single alternative carrier that the Handover Selector would be able to utilize for further communication with the Handover Requester device. The order of the Alternative Carrier Records gives an implicit preference ranking that the Handover Requester SHOULD obey. The Alternative Carrier Record is defined in section 3.3.1.

3.2.3 Handover Carrier Record

The Handover Carrier Record provides a unique identification of an alternative carrier technology in Handover Request messages when no carrier configuration data is to be provided. If the Handover Selector has the same carrier technology available, it would respond with a Carrier Configuration record with payload type equal to the carrier type (that is, the triples {TNF, TYPE_LENGTH, TYPE} and {CTF, CARRIER_TYPE_LENGTH, CARRIER_TYPE} match exactly).

The NFC Forum Well Known Type [NDEF], [NFC RTD] for the Handover Carrier Record is “Hc” (in NFC binary encoding: 0x48, 0x63).

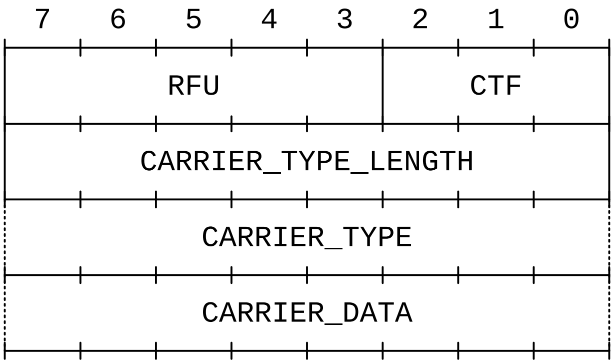


Figure 12: Handover Carrier Record Encoding

Semantics for the Handover Carrier Record:

CTF (Carrier Type Format): This is a 3-bit field that indicates the structure of the value of the *CARRIER_TYPE* field. Allowed values are listed in Table 1; other values SHALL NOT be used. The *CNF* field has the same semantics as the NDEF record *TNF* (Type Name Format) field and further explanation can be found in the NDEF specification [NDEF].

Table 1: Allowed CTF Field Values

Value	Carrier Type Format
0x01	NFC Forum well-known type [NFC RTD]
0x02	Media-type as defined in RFC 2046 [RFC 2046]
0x03	Absolute URI as defined in RFC 3986 [RFC 3986]
0x04	NFC Forum external type [NFC RTD]

CARRIER_TYPE: The value of the *CARRIER_TYPE* field gives a unique identification of the alternative carrier (see section 2.5). The value of the *CARRIER_TYPE* field MUST follow the structure, encoding, and format implied by the value of the *CTF* field.

CARRIER_DATA: A sequence of octets that provide additional information about the alternative carrier enquiry. The syntax and semantics of this data are determined by the *CARRIER_TYPE* field. The number of *CARRIER_DATA* octets is equal to the NDEF record *PAYLOAD_LENGTH* minus the *CARRIER_TYPE_LENGTH* minus 2.

3.3 Local Record Definitions

3.3.1 Alternative Carrier Record

The Alternative Carrier Record is used in the Handover Request Record or the Handover Select Record to describe a single alternative carrier. It SHALL NOT be used elsewhere.

The carrier type structure is the basic identification of an alternative carrier. The possible values are the same as those that can be assigned to the NDEF payload type field (see [NDEF]).

The list of Payload ID References is used to provide additional information by referencing other NDEF records within the Handover Request or Handover Select Message. This list can contain any number of links, including none.

The NFC Forum Well Known Local Type [NDEF], [NFC RTD] for the Alternative Carrier Record is “ac” (in NFC binary encoding: 0x61, 0x63).

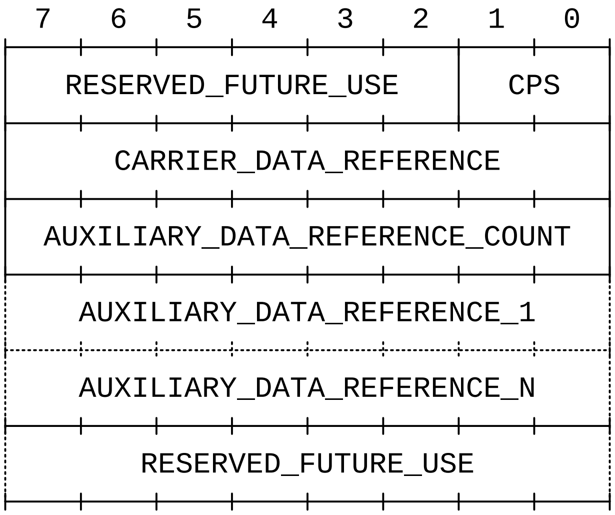

7 6 5 4 3 2 1 0
RESERVED_FUTURE_USE
CPS
CARRIER_DATA_REFERENCE
AUXILIARY_DATA_REFERENCE_COUNT
AUXILIARY_DATA_REFERENCE_1
AUXILIARY_DATA_REFERENCE_N
RESERVED_FUTURE_USE

Figure 13: Alternative Carrier Record Layout

Semantics for the Alternative Carrier Record:

CPS (Carrier Power State): This is a 2-bit field that indicates the carrier power state. Possible values are described in Table 2.

Table 2: Carrier Power State Values

Value	Carrier Power State
0x00	Inactive; the carrier is currently off
0x01	Active; the carrier is currently on
0x02	Activating; the device is in the process of activating the carrier, but it is not yet active.
0x03	Unknown; the device is only reachable via the carrier through a router, and it does not directly support an interface for the carrier.

CARRIER_DATA_REFERENCE: The Carrier Data Reference is a pointer to an NDEF record that uniquely identifies the carrier technology. The pointed record MAY be either a Handover Carrier record (see section 3.2.3) or a Carrier Configuration record (see section 2.5). A Carrier Data Reference is encoded as an 8-bit length field that determines the number of the following carrier data reference characters (see Figure 14).

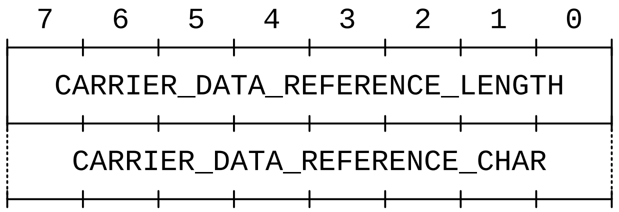


Figure 14: Carrier Data Reference Encoding

AUXILIARY_DATA_REFERENCE_COUNT: This is an 8-bit integer field that defines the number of the following Auxiliary Data References.

AUXILIARY_DATA_REFERENCE: An Auxiliary Data Reference is a pointer to an NDEF record that gives additional information about the alternative carrier. No limitations are imposed on the type of record being pointed to. An Auxiliary Data Reference is encoded as an 8-bit length field that determines the number of the following auxiliary data reference characters.

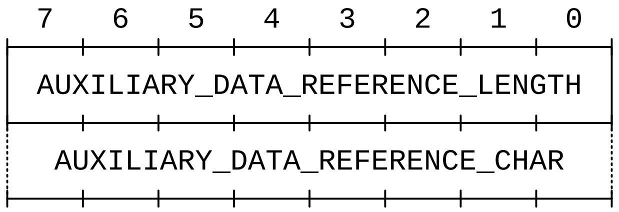

7
6
5
4
3
2
1
0
AUXILIARY_DATA_REFERENCE_LENGTH
AUXILIARY_DATA_REFERENCE_CHAR

Figure 15: Auxiliary Data Reference Encoding

A. ABNF Definition of Handover Messages and Records

This section defines the normative requirements for the handover messages and records. The language used is the ABNF format as defined in Augmented BNF for Syntax Specifications: ABNF [RFC 4234].

```
handover_request_message        = handover_request_record 1*NDEF_record
handover_select_message         = handover_select_record *NDEF_record

handover_request_record         = NDEF_header “Hr” handover_request_payload
handover_select_record          = NDEF_header “Hs” handover_select_payload

NDEF_header                     = header_flags record_type_length payload_length
header_flags                    = OCTET
record_type_length              = OCTET
payload_length                  = OCTET / UINT32

handover_request_payload        = version_number 1*alternative_carrier_record
handover_select_payload         = version_number *alternative_carrier_record

version_number                  = OCTET

alternative_carrier_record      = carrier_state_flags
                                  carrier_data_reference
                                  auxiliary_data_reference_count
                                  *auxiliary_data_reference
                                  *reserved_bytes

carrier_state_flags             = OCTET
carrier_data_reference          = payload_reference

auxiliary_data_reference_count  = OCTET
auxiliary_data_reference        = payload_reference

payload_reference               = payload_reference_length
                                  payload_reference_name

payload_reference_length        = payload_id_length
payload_reference_name          = payload_id

handover_carrier_record         = NDEF_header ID_length “Hc” payload_ID
                                  handover_carrier_payload

handover_carrier_payload        = carrier_type_flags carrier_type_length
                                  carrier_type [carrier_data]

carrier_type_flags              = OCTET
carrier_type_length             = OCTET
carrier_type                    = 1*OCTET
carrier_data                    = 1*OCTET

payload_id_length               = OCTET
payload_id                      = 1(ALPHA / DIGIT / "-" / "_" / "." / ":")
                                  *(ALPHA / DIGIT / "-" / "_" / "." / ":" / "~")

reserved_bytes                  = OCTET
```

Notes:

- *_length and *_count fields. All elements in the grammar with a suffix of "_length" or "_count" contain unsigned 8-bit binary integers indicating the size or number of corresponding fields in the record. For example, payload_reference_count indicates the number of payload_reference fields that follow.
- version_number. This octet consists of two 4-bit subfields. The high-order 4 bits contain the major version number. The low-order 4 bits contain the minor version number. By convention, backward compatibility is assured unless the major version number changes. For example, 0x10 corresponds to version 1.0.
- carrier_state_flags. The two low-order bits of carrier_state_flags reflect the status of the alternative carrier interface with values defined in Table 2. The high-order six bits of carrier_state_flags are reserved for future use and MUST be ignored by version 1.0 implementations.
- carrier_type_flags. The three low-order bits of carrier_type_flags define the format of the carrier_type filed with values as defined in Table 1. The high-order five bits of carrier_type_flags are reserved for future use and MUST be ignored by version 1.0 implementations.
- reserved_bytes. This is a placeholder for future backward-compatible extensions of the alternative_carrier_record. If reserved_bytes octets are present, Version 1.0 implementations MUST ignore them.
- NDEF_header (header_flags, record_type_length, payload_length). These fields are as documented in the NFC Data Exchange Format [NDEF] specification.
- UINT32. This field corresponds to a 32-bit unsigned integer in network byte order.

B. Use Case Examples (Informative)

B.1 Basic Handover to a Wi-Fi Carrier

The Wi-Fi Alliance has defined a method to store wireless LAN parameters and credentials on NFC Forum Tags as part of its Wi-Fi Protected Setup (WPS) specification [WFA WPS]. The information is stored in the payload of an NDEF record identified by the mime-type “application/vnd.wfa.wsc”. For brevity, this is known as the “WPS Record”.

The information provided inside a WPS Record includes the 802.11 Service Set Identifier (SSID), authentication and encryption type deployed by the wireless network, the (secret) network key that a wireless station needs to authenticate with the network, and the MAC address of the device receiving the configuration (if unknown, this address is set to all-zeros). The WPS specification uses the term “Registrar” for a device that is able to provide WLAN credentials and “Enrollee” for a device that wants to join a wireless network.

A basic handover to a Wi-Fi network does not require any additional specification. However, the Enrollee will not be able to identify the device on the Wi-Fi network that has been touched initially unless further address information is returned as described in Appendix B.4.

A Handover Requester with Wi-Fi capability that has not yet joined a wireless domain would format a Handover Request Message as schematically shown in Figure 16. The same message is shown as binary content in Table 3. The Handover Selector would deduce from this message that the Handover Requester supports exactly one alternative carrier, which is a Wi-Fi certified 802.11 radio.

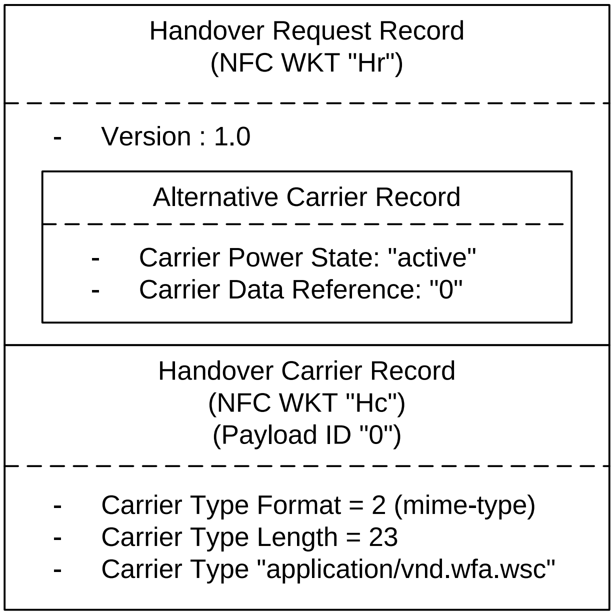

Handover Request Record
(NFC WKT "Hr")
- Version : 1.0
Alternative Carrier Record
- Carrier Power State: "active"
- Carrier Data Reference: "0"
Handover Carrier Record
(NFC WKT "Hc")
(Payload ID "0")
- Carrier Type Format = 2 (mime-type)
- Carrier Type Length = 23
- Carrier Type "application/vnd.wfa.wsc"

Figure 16: Minimum Wi-Fi Handover Request Message

If the Handover Selector is a Wi-Fi device with wireless connectivity, it should respond with the Handover Select Message as shown in Figure 17 and, again, shown as binary content in Table 4. Note that all blocks with TLV postfix are Wi-Fi Alliance-defined WPS information and that TLV denotes Type-Length-Value format. Note also that other WPS TLV information blocks not shown in the example might be present.

The Handover Requester would typically use the SSID and Network Key to enroll on the same Wi-Fi network that the Handover Selector is connected to. Further possible actions depend on the provision of an IP address identifying the Handover Selector, the available services, and the Handover Requester's intended activity.

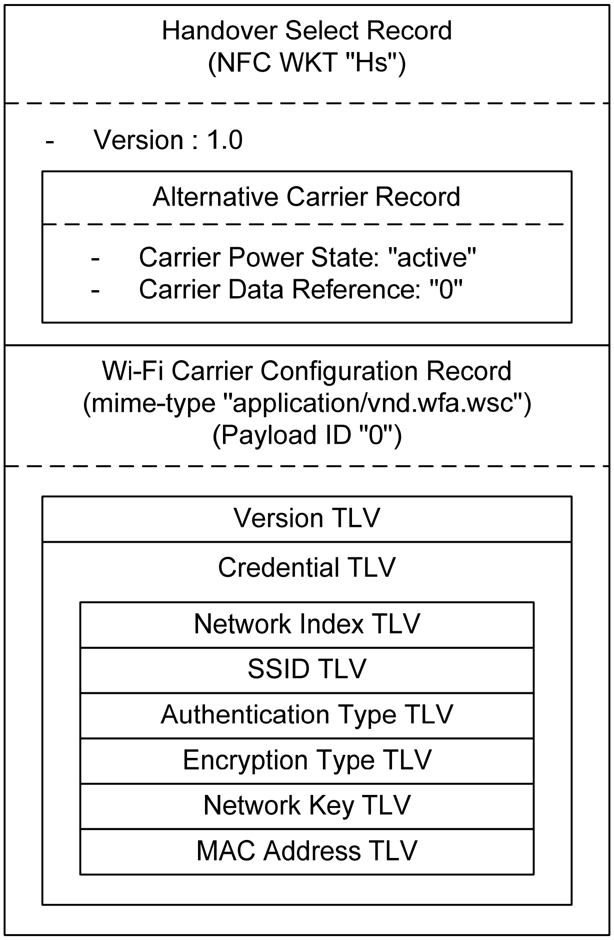


Figure 17: Minimum Wi-Fi Handover Select Message

Table 3: Binary Content of a Minimum Wi-Fi Handover Request Message

Offset	Content	Length	Explanation
0	0x91	1	NDEF record header (TNF=0x01, SR=1, MB=1, ME=0, IL=0)
1	0x02	1	Record type length (2 byte)
2	0x0A	1	Payload length (10 byte)
3	0x48, 0x72	2	Record type: “Hr”
5	0x10	1	Version number (major, minor)
6	0xD1	1	NDEF record header (TNF = 0x01, SR=1, MB=1, ME=1, IL=0)
7	0x02	1	Record type length (2 byte)

Offset	Content	Length	Explanation
8	0x04	1	Payload length (4 byte)
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
14	0x00	1	Auxiliary Data Reference Count (0)
15	0x59	1	NDEF record header (TNF=0x01, SR=1, MB=0, ME=1, IL=1)
16	0x02	1	Record type length (2 byte)
17	0x19	1	Payload length (25 byte)
18	0x01	1	Payload ID length (1 byte)
19	0x48, 0x63	2	Record type: "Hc"
21	0x30	1	Payload ID “0”
22	0x02	1	Carrier Type Format CTF = 0x02
23	0x17	1	Carrier Type Length (23 byte)
24	“application/vnd.wfa.wsc”	23	Carrier Type

Table 4: Binary Content of a Minimum Wi-Fi Handover Select Message

Offset	Content	Length	Explanation
0	0x91	1	NDEF record header (TNF=0x01, SR=1, MB=1, ME=0, IL=0)
1	0x02	1	Record type length (2 byte)
2	0x0A	1	Payload length (10 byte)
3	0x48, 0x73	2	Record type: “Hs”
5	0x10	1	Version number (major, minor)
6	0xD1	1	NDEF record header (TNF = 0x01, SR=1, MB=1, ME=1, IL=0)
7	0x02	1	Record type length (2 byte)
8	0x04	1	Payload length (4 byte)
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)

Offset	Content	Length	Explanation
15	0x5A	1	NDEF record header (TNF=0x02, SR=1, MB=0, ME=1, IL=1)
16	0x17	1	Record type length (23 bytes)
17	0x42	1	Payload length (66 byte)
18	0x01	1	Payload ID length (1 byte)
19	“application/vnd.wfa.wsc”	23	Record type
42	0x30	1	Payload ID “0”
43	0x104A	2	WPS Attribute Type: Version
45	0x0001	2	Version Length: 1 byte
47	0x10	1	Version = 1.0
48	0x100E	2	WPS Attribute: Credential
50	0x0039	2	Credential Length: 57 byte
52	0x1026	2	WPS Attribute: Network Index
54	0x0001	2	Network Index Length: 1 byte
56	0x01	1	Network Index = 1
57	0x1045	2	WPS Attribute: SSID
59	0x0008	2	SSID Length: 8 byte
61	“HomeWLAN”	8	SSID = “HomeWLAN”
69	0x1003	2	WPS Attribute: Authentication Type
71	0x0002	2	Authentication Type Length: 2 byte
73	0x0020	2	Authentication Type: WPA2PSK
75	0x100F	2	WPS Attribute: Encryption Type
77	0x0002	2	Encryption Type Length: 2 byte
79	0x0008	2	Encryption Type: AES
81	0x1027	2	WPS Attribute: Network Key
83	0x000E	2	Network Key Length: 14 byte
85	“MyPreSharedKey”	14	Network Key = “MyPreSharedKey”
99	0x1020	2	WPS Attribute: MAC Address
101	0x0006	2	MAC Address Length: 6 byte
103	00:07:E9:4C:A8:1C	6	MAC Address

B.2 Handover to a Bluetooth Carrier

The Bluetooth Special Interest Group (SIG) recently defined a mechanism called “Secure Simple Pairing” ([BT2.1+EDR] Volume 2, Part H, Section 7.2.2) to simplify the process of pairing two

Bluetooth devices. Secure Simple Pairing defines four different association models, one of them being the transmission of device discovery information and cryptographic numbers through an Out-of-Band channel such as NFC.

To make the Bluetooth OOB data block ([BT2.1+EDR] Volume 3, Part C, Section 8.1.6) usable with NFC Forum Devices and Tags, a suitable NDEF record type name needs to be allocated and made available by the Bluetooth SIG. The examples in this specification use a fictional record type name for identification of the Bluetooth OOB data that is not intended to be used in product implementations.

Figure 18 shows an exemplary Handover Request Message from a device with only Bluetooth communication capability using the fictional mime-type “application/vnd.bogus.oob”. Table 5 shows an example message as it could be issued by a Bluetooth camera.

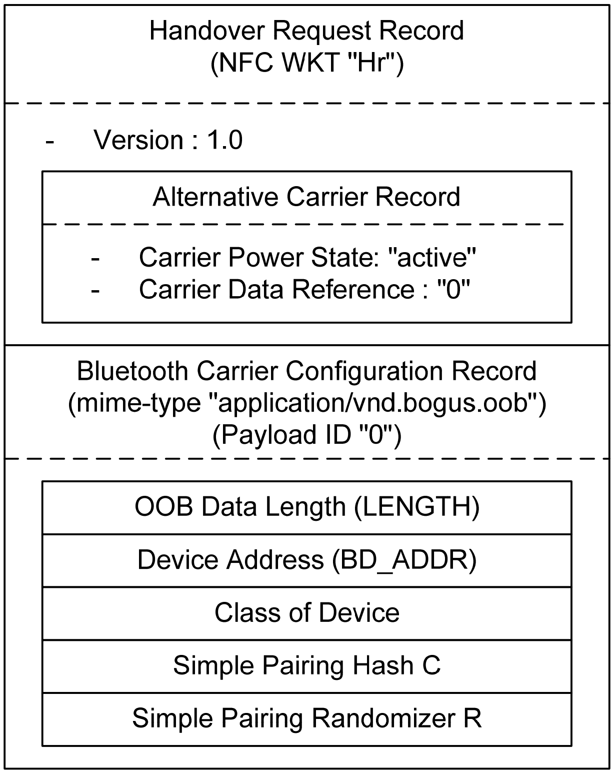

Handover Request Record
(NFC WKT "Hr")
- Version : 1.0
Alternative Carrier Record
- Carrier Power State: "active"
- Carrier Data Reference : "0"
Bluetooth Carrier Configuration Record
(mime-type "application/vnd.bogus.oob")
(Payload ID "0")
OOB Data Length (LENGTH)
Device Address (BD_ADDR)
Class of Device
Simple Pairing Hash C
Simple Pairing Randomizer R

Figure 18: Bluetooth Handover Request Message

Note that the Bluetooth OOB data block might contain only the LENGTH and BD_ADDR field.

The Bluetooth Simple Pairing over a bidirectional OOB channel is symmetrical; that is, both devices send the same type of information to their peer device. The Handover Request Message can therefore be constructed using a Bluetooth Carrier Configuration record instead of a Handover Carrier (“Hc”) record as in the Wi-Fi example in Appendix B.1.

Figure 19 shows the structure of a Handover Select Message returned by a Handover Selector device that acknowledges a Bluetooth carrier. Table 6 details an example Handover Select Message that could be returned by a printer device that has a Bluetooth radio available.

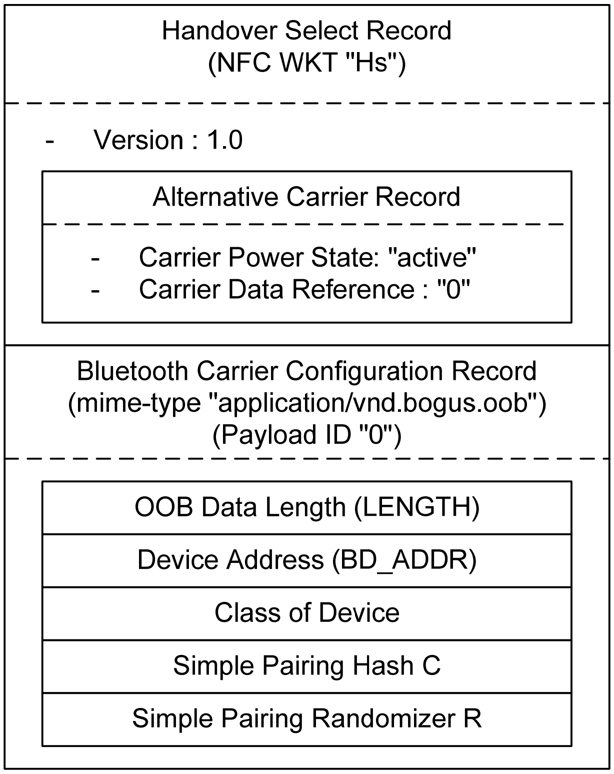

Handover Select Record
(NFC WKT "Hs")
- Version : 1.0
Alternative Carrier Record
- Carrier Power State: "active"
- Carrier Data Reference : "0"
Bluetooth Carrier Configuration Record
(mime-type "application/vnd.bogus.oob")
(Payload ID "0")
OOB Data Length (LENGTH)
Device Address (BD_ADDR)
Class of Device
Simple Pairing Hash C
Simple Pairing Randomizer R

Figure 19: Bluetooth Handover Select Message

Table 5: Binary Content of a Bluetooth Handover Request Message

Offset	Content	Length	Explanation
0	0x91	1	NDEF record header (TNF=0x01, SR=1, MB=1, ME=0, IL=0)
1	0x02	1	Record type length (2 byte)
2	0x0A	1	Payload length (10 byte)
3	0x48, 0x72	2	Record type: “Hr”
5	0x10	1	Version number (major, minor)
6	0xD1	1	NDEF record header (TNF = 0x01, SR=1, MB=1, ME=1, IL=0)
7	0x02	1	Record type length (2 byte)
8	0x04	1	Payload length (4 byte)
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)

Offset	Content	Length	Explanation
15	0x5A	1	NDEF record header (TNF=0x02, SR=1, MB=0, ME=1, IL=1)
16	0x10	1	Record type length (16 byte)
17	0x31	1	Payload length (49 byte)
18	0x01	1	Payload ID length (1 byte)
19	“application/vnd.bogus.oob”	25	Record type
44	0x30	1	Payload ID: “0”
45	0x0031	2	Bluetooth OOB Data Length (49 byte)
47	01:07:80:80:bf:A1	6	Bluetooth Device Address
53	0x04	1	EIR Data Length (4 byte)
54	0x0D	1	EIR Data Type: Class of Device
55	08:06:20	3	Camera Device
58	0x11	1	EIR Data Length (17 byte)
59	0x0E	1	EIR Data Type
60	01:02:03:04:05:06:07:08: 09:10:11:12:13:14:15:16	16	Simple Pairing Hash C
76	0x11	1	EIR Data Length (17 byte)
77	0x0F	1	EIR Data Type
78	01:02:03:04:05:06:07:08: 09:10:11:12:13:14:15:16	16	Simple Pairing Randomizer R

Table 6: Binary Content of a Bluetooth Handover Select Message

Offset	Content	Length	Explanation
0	0x91	1	NDEF record header (TNF=0x01, SR=1, MB=1, ME=0, IL=0)
1	0x02	1	Record type length (2 byte)
2	0x0A	1	Payload length (10 byte)
3	0x48, 0x73	2	Record type: “Hs”
5	0x10	1	Version number (major, minor)
6	0xD1	1	NDEF record header (TNF = 0x01, SR=1, MB=1, ME=1, IL=0)
7	0x02	1	Record type length (2 byte)
8	0x04	1	Payload length (4 byte)
9	0x61, 0x63	2	Record type: “ac”

Offset	Content	Length	Explanation
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 (TNF=0x02, SR=1, MB=0, ME=1, IL=1)
16	0x10	1	Record type length (16 bytes)
17	0x31	1	Payload length (49 byte)
18	0x01	1	Payload ID length (1 byte)
19	“application/vnd.bogus.oob”	25	Record type
44	0x30	1	Payload ID: “0”
45	0x0031	2	Bluetooth OOB Data Length (49 byte)
47	03:07:80:88:bf:01	6	Bluetooth Device Address
53	0x04	1	EIR Data Length (4 byte)
54	0x0D	1	EIR Data Type: Class of Device
55	04:06:08	3	Printer Device
58	0x11	1	EIR Data Length (17 byte)
59	0x0E	1	EIR Data Type
60	01:02:03:04:05:06:07:08: 09:10:11:12:13:14:15:16	16	Simple Pairing Hash C
76	0x11	1	EIR Data Length (17 byte)
77	0x0F	1	EIR Data Type
78	01:02:03:04:05:06:07:08: 09:10:11:12:13:14:15:16	16	Simple Pairing Randomizer R

B.3 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 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 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; carriers cannot automatically be powered as a result of the NFC touch and dynamic carrier-specific protocol information as non-static IP addresses cannot be provided.

Figure 20 shows an example where Wi-Fi and Bluetooth configuration data are combined in a Handover Select Message stored on an NFC Forum Tag.

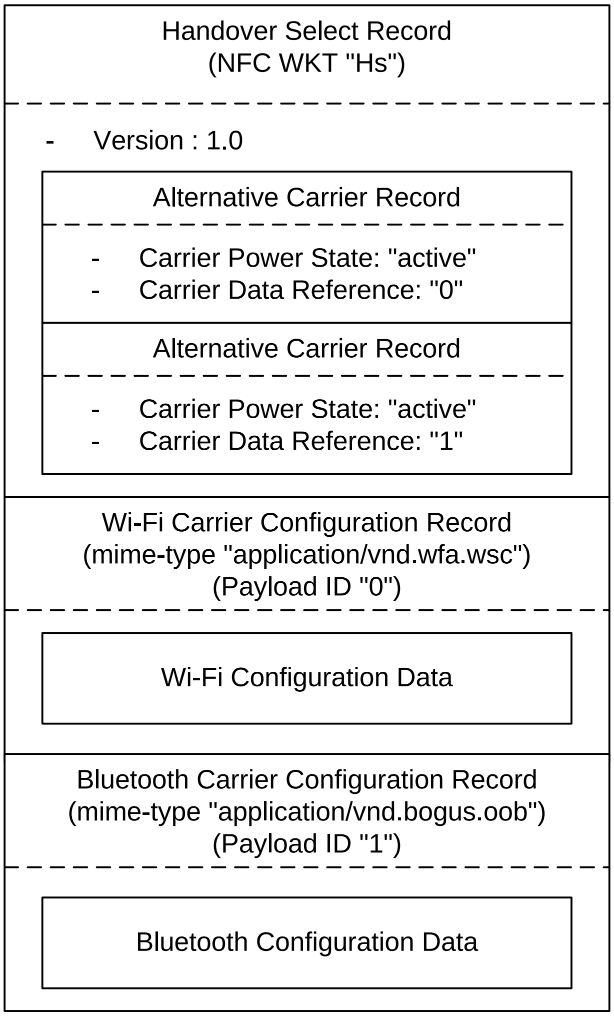

Handover Select Record
(NFC WKT "Hs")
- Version : 1.0
Alternative Carrier Record
- Carrier Power State: "active"
- Carrier Data Reference: "0"
Alternative Carrier Record
- Carrier Power State: "active"
- Carrier Data Reference: "1"
Wi-Fi Carrier Configuration Record
(mime-type "application/vnd.wfa.wsc")
(Payload ID "0")
Wi-Fi Configuration Data
Bluetooth Carrier Configuration Record
(mime-type "application/vnd.bogus.oob")
(Payload ID "1")
Bluetooth Configuration Data

Figure 20: Wi-Fi and Bluetooth Configuration Data on NFC Forum Tag

In the example, the power state of both Wi-Fi and Bluetooth carrier are 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 Wi-Fi and Bluetooth carrier stored on an NFC Forum Tag is shown in Table 7.

Table 7: Wi-Fi and Bluetooth Handover Select Message on NFC Forum Tag

Offset	Content	Length	Explanation
0	0x91	1	NDEF record header (TNF=0x01, SR=1, MB=1, ME=0, IL=0)
1	0x02	1	Record type length (2 byte)
2	0x13	1	Payload length (19 byte)
3	0x48, 0x73	2	Record type: "Hs"
5	0x10	1	Version number (major, minor)
6	0x91	1	NDEF record header (TNF = 0x01, SR=1, MB=1, ME=0, IL=0)
7	0x02	1	Record type length (2 byte)
8	0x04	1	Payload length (4 byte)
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	0x51	1	NDEF record header (TNF = 0x01, SR=1, MB=0, ME=1, IL=0)
16	0x02	1	Record type length (2 byte)
17	0x04	1	Payload length (4 byte)
18	0x61, 0x63	2	Record type: "ac"
20	0x01	1	Carrier Flags (CPS=1), active
21	0x01	1	Carrier Data Reference Length (1 byte)
22	0x31	1	Carrier Data Reference: "1"
23	0x00	1	Auxiliary Data Reference Count: 0
24	0x1A	1	NDEF record header (TNF=0x02, SR=1, MB=0, ME=0, IL=1)

Offset	Content	Length	Explanation
25	0x17	1	Record type length (23 bytes)
26	0x42	1	Payload length (66 byte)
27	0x01	1	Payload ID length (1 byte)
28	“application/vnd.wfa.wsc”	23	Record type
51	0x30	1	Payload ID “0”
52	0x104A	2	WPS Attribute Type: Version
54	0x0001	2	Version Length: 1 byte
56	0x10	1	Version = 1.0
57	0x100E	2	WPS Attribute: Credential
59	0x0039	2	Credential Length: 57 byte
61	0x1026	2	WPS Attribute: Network Index
63	0x0001	2	Network Index Length: 1 byte
65	0x01	1	Network Index = 1
66	0x1045	2	WPS Attribute: SSID
68	0x0008	2	SSID Length: 8 byte
70	“HomeWLAN”	8	SSID = “HomeWLAN”
78	0x1003	2	WPS Attribute: Authentication Type
80	0x0002	2	Authentication Type Length: 2 byte
82	0x0020	2	Authentication Type: WPA2PSK
84	0x100F	2	WPS Attribute: Encryption Type
86	0x0002	2	Encryption Type Length: 2 byte
88	0x0008	2	Encryption Type: AES
90	0x1027	2	WPS Attribute: Network Key
92	0x000E	2	Network Key Length: 14 byte
94	“MyPreSharedKey”	14	Network Key = “MyPreSharedKey”
108	0x1020	2	WPS Attribute: MAC Address
110	0x0006	2	MAC Address Length: 6 byte
112	00:07:E9:4C:A8:1C	6	MAC Address
118	0x5A	1	NDEF record header (TNF=0x02, SR=1, MB=0, ME=1, IL=1)
119	0x10	1	Record type length (16 bytes)
120	0x31	1	Payload length (49 byte)
121	0x01	1	Payload ID length (1 byte)

Offset	Content	Length	Explanation
122	“application/vnd.bogus.oob”	25	Record type
147	0x31	1	Payload ID “1”
148	0x0031	2	Bluetooth OOB Data Length (49 byte)
150	03:07:80:88:bf:01	6	Bluetooth Device Address
156	0x04	1	EIR Data Length (4 byte)
157	0x0D	1	EIR Data Type: Class of Device
160	04:06:08	3	Printer Device
161	0x11	1	EIR Data Length (17 byte)
162	0x0E	1	EIR Data Type
163	01:02:03:04:05:06:07:08: 09:10:11:12:13:14:15:16	16	Simple Pairing Hash C
179	0x11	1	EIR Data Length (17 byte)
180	0x0F	1	EIR Data Type
181	01:02:03:04:05:06:07:08: 09:10:11:12:13:14:15:16	16	Simple Pairing Randomizer R

B.4 Initiating FTP File Exchange

A number of protocols can be expressed using URIs (Uniform Resource Identifiers) and the NFC Forum URI RTD [NFC URI] specification provides a record type to encode URIs in NDEF messages. An application might use URI records to indicate FTP (File Transfer Protocol) [RFC 959] capability in a Handover Request Message and transmit back the server name or IP address in a Handover Select Message.

In this example, the Handover Requester device might be a digital camera running an FTP client, while the Handover Selector might be a Network Attached Storage (NAS) device running an FTP server. The camera could then send a Handover Request Message as shown in Figure 21 to indicate Wi-Fi and FTP capability. The Auxiliary Data Reference within the Alternative Carrier Record points to a URI record that specifies an incomplete URI with only the scheme part.

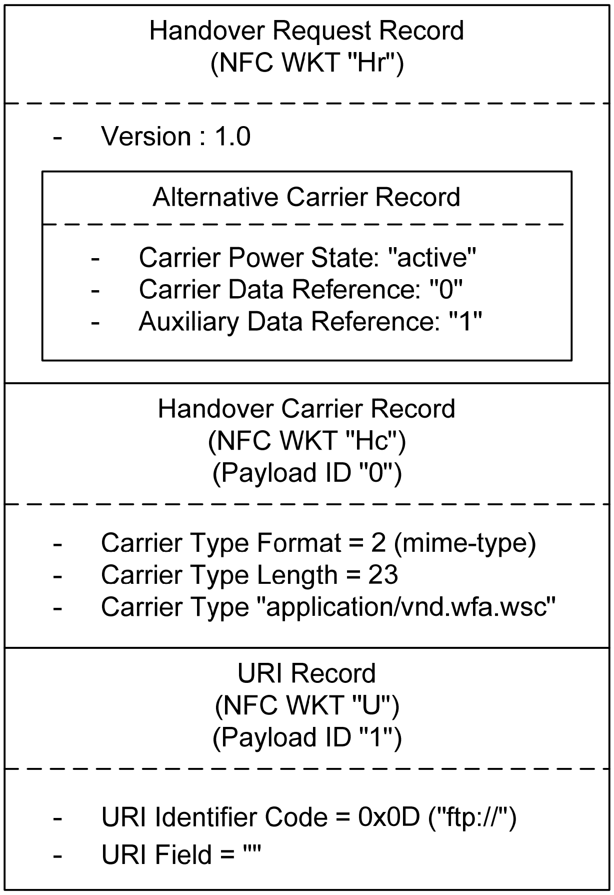

Handover Request Record
(NFC WKT "Hr")
- Version : 1.0
Alternative Carrier Record
- Carrier Power State: "active"
- Carrier Data Reference: "0"
- Auxiliary Data Reference: "1"
Handover Carrier Record
(NFC WKT "Hc")
(Payload ID "0")
- Carrier Type Format = 2 (mime-type)
- Carrier Type Length = 23
- Carrier Type "application/vnd.wfa.wsc"
URI Record
(NFC WKT "U")
(Payload ID "1")
- URI Identifier Code = 0x0D ("ftp://")
- URI Field = ""

Figure 21: Handover Request Message with Wi-Fi Carrier and FTP Protocol Inquiry

The NAS device in this example is assumed to be connected to a wired IP network and be able to act as a Wi-Fi WPS Registrar; that is, it knows about the presence of a Wi-Fi access point and can deliver credentials for the wireless network. Furthermore, the NAS device is running an FTP server on standard IP port 21.

With the given assumptions, the device might return the Handover Select Message as shown in Figure 22. Note that, unlike in previous examples, the power state of the alternative carrier is set to “unknown” because the NAS cannot control the Wi-Fi carrier circuitry.

Similar to the Handover Request Message shown before, the Handover Select Message appends a URI record via an Auxiliary Data Reference structure.

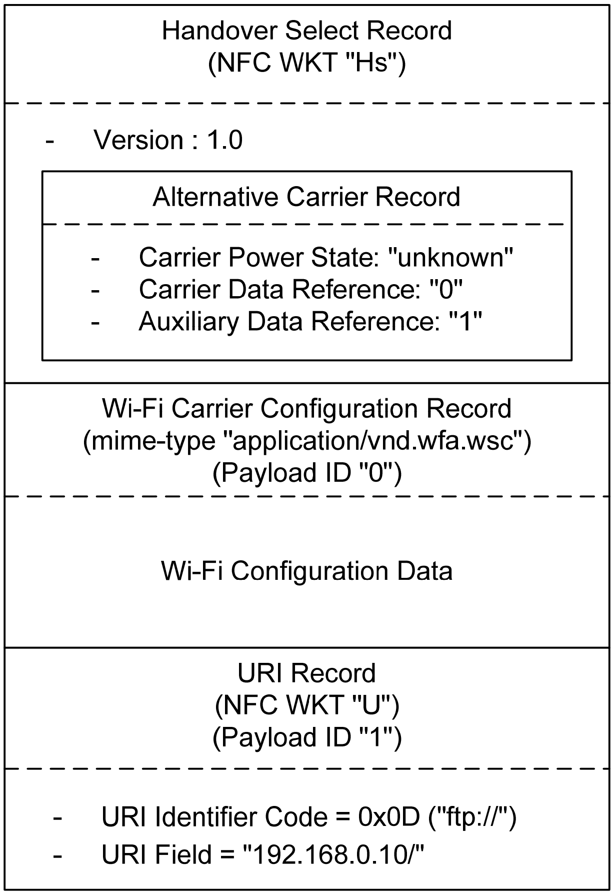

Handover Select Record
(NFC WKT "Hs")
- Version : 1.0
Alternative Carrier Record
- Carrier Power State: "unknown"
- Carrier Data Reference: "0"
- Auxiliary Data Reference: "1"
Wi-Fi Carrier Configuration Record
(mime-type "application/vnd.wfa.wsc")
(Payload ID "0")
Wi-Fi Configuration Data
URI Record
(NFC WKT "U")
(Payload ID "1")
- URI Identifier Code = 0x0D ("ftp://")
- URI Field = "192.168.0.10/"

Figure 22: Handover Select Message with Wi-Fi Credentials and FTP Server Address

The URI field of the URI record contains the NAS device’s IP address which, together with the URI identifier code, makes the full URI string read as “ftp://192.168.0.10/”. Given this information and the Wi-Fi configuration data, the camera can connect to the wireless IP network and establish an FTP session with the NAS device using standard port assignments.

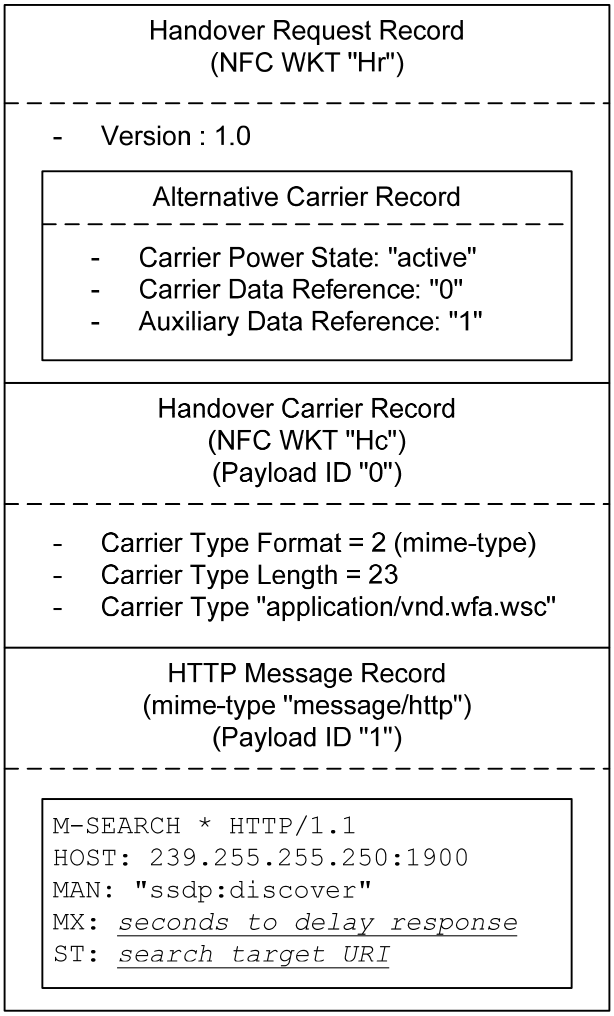
Logging onto an FTP server usually requires that the client provide a username and a password. Depending on the configuration, an FTP server might accept anonymous login with the username “anonymous” and any password string. The URI record provides an abbreviation for anonymous FTP URIs with the identifier code 0x07, which makes the first part of the full URI read as “ftp://anonymous:anonymous@”. Combined with the URI field shown in Figure 22, the full URI would then read “ftp://anonymous:anonymous@192.168.0.10/” and allow open access to the NAS. Likewise, the Handover Requester device could request an anonymous login if it does not know any credentials for an FTP server.

An alternative setup would be to configure the camera with username and password settings (which could be product serial numbers, for example) and configure the NAS to accept exactly these credentials, thus allowing only the user’s own camera to access the storage device.

B.5 UPnP Device Discovery

The Universal Plug and Play (UPnP) architecture [UPNP UDA] offers peer-to-peer network connectivity within home or office networks based on TCP/IP technology. Devices within the network discover each other by multicasting advertisement or search messages using the Simple Service Discovery Protocol (SSDP). SSDP uses the Hypertext Transport Protocol (HTTP) packet format with an empty HTTP body and UPnP specific attributes in the HTTP header. HTTP packets can be embedded in NDEF records using the mime type “message/http” [RFC 2616].

A Handover Requester device can provide an SSDP search request within a Handover Request Message as a separate NDEF record that is referenced from within an Alternative Carrier Record using an Auxiliary Data Reference. Figure 23 gives an example of a Handover Request Message to enquire about Wi-Fi connectivity and UPnP protocol ability at the Handover Selector device.



Handover Request Record
(NFC WKT "Hr")

- Version : 1.0

Alternative Carrier Record

- Carrier Power State: "active"
- Carrier Data Reference: "0"
- Auxiliary Data Reference: "1"

Handover Carrier Record
(NFC WKT "Hc")
(Payload ID "0")

- Carrier Type Format = 2 (mime-type)
- Carrier Type Length = 23
- Carrier Type "application/vnd.wfa.wsc"

HTTP Message Record
(mime-type "message/http")
(Payload ID "1")

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: seconds to delay response
ST: search target URI
```

Figure 23: Handover Request Message Specifying Wi-Fi and UPnP

The payload of the HTTP message record contains the raw SSDP search request shown with all mandatory lines. Values in italic underlined font are placeholders for actual values. For details about individual header lines, refer to the UPnP Device Architecture (UDA) document available at the UPnP Forum’s website.

The maximum delay time specified with the MX header line is used in UPnP implementations as an upper limit to choose a random delay for the SSDP response. This value has no relevance in an NFC Forum Handover application and can be omitted.

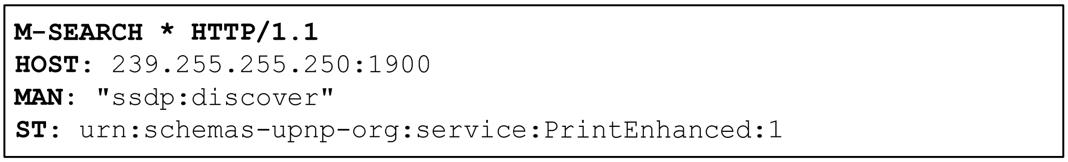
The Search Target (ST) line contains a single URI indicating what type of device or service the Handover Requester is interested in. The format of this URI is given in the UDA document. Note that searching for a particular device with a Universally Unique Identifier (UUID) might not make sense in a Handover Request Message.

A typical example for an SSDP search request is given in Figure 24, where the Handover Requester would be interested in getting access to a UPnP Printer device.

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
ST: urn:schemas-upnp-org:device:Printer:1
```

Figure 24: Search for a UPnP Printer Device

An SSDP request for a specific service type would be encoded as shown in Figure 25.



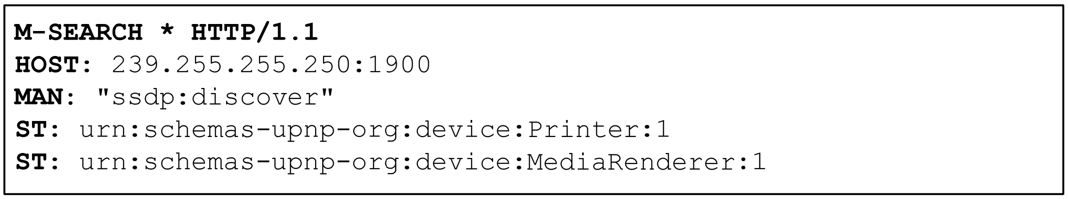
```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
ST: urn:schemas-upnp-org:service:PrintEnhanced:1
```

Figure 25: Search for a UPnP-enhanced Print Service

Similarly, the Handover Requester could query for only a root device description, using the Search Target "upnp:rootdevice" or all device (the root device and any embedded devices) and service information with the Search Target "ssdp:all".

It should be noted that a Search Target "ssdp:all" can produce a large NDEF response message because 3+2*d*+*k* SSPD responses have to be encoded into the Handover Select Message for a root device with *d* embedded devices and *k* distinct services.

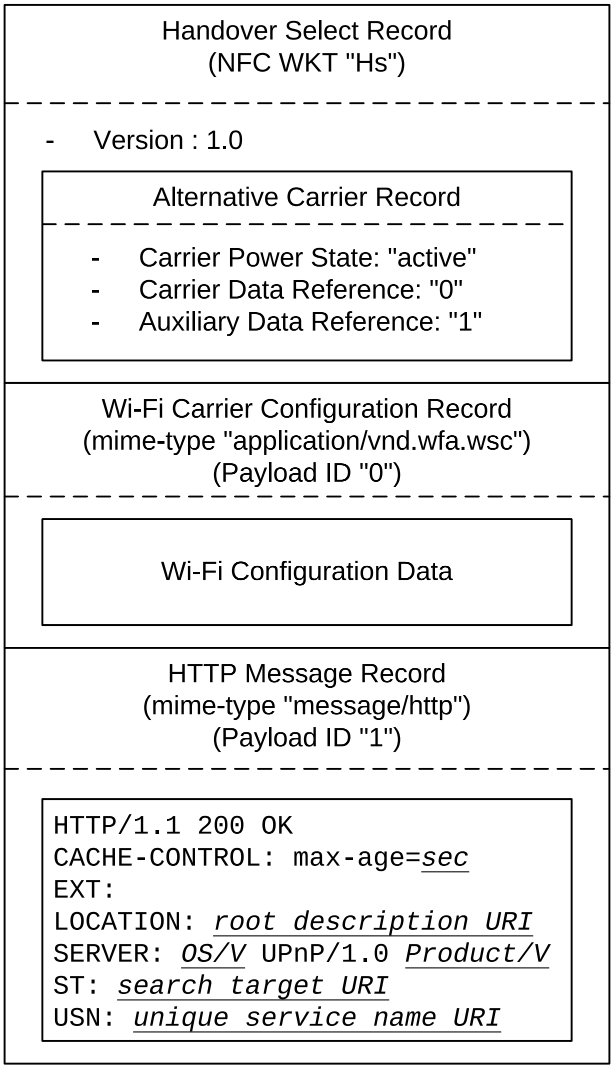
If a UPnP device wants to discover different devices or services without using an "ssdp:all" Search Target, it would multicast separate SSDP request messages. In an NFC Forum Handover application, it should be allowed to combine them into a single SSDP packet to save bandwidth. Thus, a digital picture camera that is able to either print an image or send it to a display device might provide a search request as shown in Figure 26.



```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
ST: urn:schemas-upnp-org:device:Printer:1
ST: urn:schemas-upnp-org:device:MediaRenderer:1
```

Figure 26: Search for a Printer or Media Renderer Device

A Handover Selector device that has Wi-Fi connectivity and UPnP protocol stack available would acknowledge the request shown in Figure 23 with a Handover Select Message that contains Wi-Fi configuration data and an SSDP search response encapsulated in an HTTP Message Record as shown in Figure 27. Note that if either the Search Target given in the Handover Request Message does not match with the UPnP capabilities of the Handover Selector device, or if the device does not have a UPnP protocol stack running, it could respond with only the Wi-Fi configuration data given that Wi-Fi is available.



Handover Select Record
(NFC WKT "Hs")

- Version : 1.0

Alternative Carrier Record

- Carrier Power State: "active"
- Carrier Data Reference: "0"
- Auxiliary Data Reference: "1"

Wi-Fi Carrier Configuration Record
(mime-type "application/vnd.wfa.wsc")
(Payload ID "0")

Wi-Fi Configuration Data

HTTP Message Record
(mime-type "message/http")
(Payload ID "1")

```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age=sec
EXT:
LOCATION: root description URI
SERVER: OS/V UPnP/1.0 Product/V
ST: search target URI
USN: unique service name URI
```

Figure 27: Handover Select Message with Wi-Fi Configuration Data and SSPD Response

In Figure 27, all UPnP mandated lines of the SSDP search response packet are shown and values in italic underlined font are again placeholders for real values. An NFC Forum Handover application should be allowed to omit the Search Target, as the same information is also contained in the Unique Service Name (USN) string.

An exemplary SSDP response of a UPnP printer given an SSDP search request as in Figure 24 is shown in Figure 28. The Search Target that is omitted in this sample response would be equal to the second half of the USN (the part following the double-colon).

The IP layer address and port information for the Handover Selector device is given with the Location URI. This enables the Handover Requester to directly address its target once the Wi-Fi connectivity has been established. The full Location URI would be used to fetch the UPnP root device description which gives further leads to the service control points and other information.

```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age:1800
EXT:
LOCATION: http://192.168.0.10:8080/description.xml
SERVER: Linux/2.6.22.5 UPnP/1.0 PicturePrinter/1.2
USN: uuid:550e8400-e29b-11d4-a716-446655440000::\
urn:schemas-upnp-org:device:Printer:1
```

Note: The backslash "\" denotes line continuation and is not part of the URI

Figure 28: SSPD Search Response from a UPnP Printer Device

According to the UPnP Device Architecture (UDA), a device sends multiple SSDP search responses if a Search Target produces multiple matches. If, for example, the Search Target URI was “ssdp:all”, there would be 3+2*d*+*k* SSDP responses for a device with *d* embedded devices and *k* distinct services. An NFC Forum Handover application should be allowed to collect these responses into a single SSDP packet and to omit the messages, providing a sole UUID within the USN URI.

Figure 29 shows an example where the Handover Requester specifies “ssdp:all” as the Search Target URI and the Handover Selector device is a Printer/Scanner multi-function device. It can be seen that only two USNs are used to specify the root device and that one USN is used to specify each embedded device and each distinct service.

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
ST: ssdp:all
```

```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age:1800
EXT:
LOCATION: http://192.168.0.10:8080/description.xml
SERVER: Linux/2.6.22.5 UPnP/1.0 PrinterScanner/1.2
USN: uuid:622addb0-522f-11dc-8314-0800200c9a66::upnp:rootdevice
USN: uuid:622addb0-522f-11dc-8314-0800200c9a66::\
urn:schemas-upnp-org:device:Basic:1.0
USN: uuid:753e0be8-522f-11dc-8314-0800200c9a66::\
urn:schemas-upnp-org:device:Printer:1
USN: uuid:18d098fa-5230-11dc-8314-0800200c9a66::\
urn:schemas-upnp-org:device:Scanner:1
USN: uuid:753e0be8-522f-11dc-8314-0800200c9a66::\
urn:schemas-upnp-org:service:PrintEnhanced:1
USN: uuid:18d098fa-5230-11dc-8314-0800200c9a66::\
urn:schemas-upnp-org:service:Scan:1
```

Note: The backslash "\" denotes line continuation and is not part of the URI

Figure 29: SSDP Search and Response for a Print/Scan Multifunction Device

C. Revision History

The following table outlines the revision history of Connection Handover.

Table 8: Revision History

Document Name	Revision and Release Date	Status	Change Notice	Supersedes
Connection Handover Candidate Technical Specification	1.0, April 2008	Candidate	None	
Connection Handover Technical Specification	1.1, November 2008	Final		1.0