NFC Controller Interface (NCI)

Technical Specification

Version 2.0

2016-11-30

[NCI]

NFC Forum™

RESTRICTIONS ON USE

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

Contents

1 Introduction 1
- 1.1 Objectives 1
- 1.2 Scope 1
- 1.3 Audience 2
- 1.4 Applicable Documents or References 2
- 1.5 Administration 4
- 1.6 Name and Logo Usage 4
- 1.7 Intellectual Property 4
- 1.8 Special Word Usage 4
- 1.9 Abbreviations 5
- 1.10 Glossary 7
- 1.11 Coding Conventions 11

2 NCI Architecture 13
- 2.1 Components 13
- 2.2 Concepts 14
  - 2.2.1 Control Messages 14
  - 2.2.2 Data Messages 14
  - 2.2.3 Interfaces 15
  - 2.2.4 RF Interface Extensions 15
  - 2.2.5 RF Communication 16
  - 2.2.6 NFCEE Communication 16
  - 2.2.7 Identifiers 17
  - 2.2.8 NFCC as Shared Resource 17

3 NCI Core Framework 18
- 3.1 Overview 18
- 3.2 NCI Control Messages 19
  - 3.2.1 Flow Control for Control Messages 19
  - 3.2.2 Exception Handling for Control Messages 20
- 3.3 NCI Data Messages 21
  - 3.3.1 Flow Control for Data Packets 22
  - 3.3.2 Exception Handling for Data Messages 22
- 3.4 Packet Formats 23
  - 3.4.1 Common Packet Header 23
  - 3.4.2 Format of Control Packets 24
  - 3.4.3 Format of Data Packets 25
- 3.5 Segmentation and Reassembly 26
- 3.6 Logical Connections 27

4 NCI Core Control Messages 29
- 4.1 Reset of NFCC 29
- 4.2 Initialization of NFCC 32
- 4.3 NFCC Configuration 36
  - 4.3.1 Setting the Configuration 36
  - 4.3.2 Retrieve the Configuration 37
- 4.4 Logical Connection Management 38
  - 4.4.1 Destination Type 38
  - 4.4.2 Connection Creation 39
  - 4.4.3 Connection Closure 42

4.4.4 Connection Credit Management 43
4.5 Generic Error 44
4.6 Interface Error 44
5 RF Communication 45
5.1 RF Interface Architecture 45
5.2 State Machine 46
5.2.1 State RFST_IDLE 48
5.2.2 State RFST_DISCOVERY 48
5.2.3 State RFST_W4_ALL_DISCOVERIES 49
5.2.4 State RFST_W4_HOST_SELECT 49
5.2.5 State RFST_POLL_ACTIVE 50
5.2.6 State RFST_LISTEN_ACTIVE 51
5.2.7 State RFST_LISTEN_SLEEP 52
5.3 RF Field Information 52
6 RF Communication Configuration 54
6.1 Configuration Parameters 54
6.1.1 Poll A Parameters 56
6.1.2 Poll B Parameters 56
6.1.3 Poll F Parameters 58
6.1.4 Poll ISO-DEP Parameters 58
6.1.5 Poll NFC-DEP Parameters 59
6.1.6 Poll Active Parameters 60
6.1.7 Poll V Parameters 60
6.1.8 Listen A Parameters 61
6.1.9 Listen B Parameters 63
6.1.10 Listen F Parameters 64
6.1.11 Listen T3T Parameters 65
6.1.12 Listen ISO-DEP Parameters 69
6.1.13 Listen NFC-DEP Parameters 70
6.1.14 Common Parameters 71
6.2 RF Interface Mapping Configuration 73
6.3 Listen Mode Routing Configuration 74
6.3.1 Listen Mode Routing Table Design 75
6.3.2 Configure Listen Mode Routing 78
6.3.3 Read Listen Mode Routing 84
6.3.4 Set Power State for Route Selection 85
6.3.5 AID-based Route Selection Process 86
6.3.6 APDU Pattern-based Route Selection Process 87
6.3.7 System Code-based Route Selection Process 87
6.3.8 Protocol-based Route Selection Process 89
6.3.9 Technology-based Route Selection Process 89
6.3.10 Forced NFCEE Routing 89
7 RF Discovery 92
7.1 Starting RF Discovery 92
7.2 Select Discovered Target 101
7.3 RF Interface Activation and Deactivation 101
7.3.1 RF Interface Activation Notification 101
7.3.2 RF Interface Deactivation 104
7.4 RF Interface Extension Starting and Stopping 106

7.4.1 RF Interface Extension Start 106
7.4.2 RF Interface Extension Stop 107
7.5 RF Discovery Request from NFCEEs 107
7.6 RF NFCEE Action 108

8 RF Interfaces 112
8.1 NFCEE Direct RF Interface 112
8.1.1 Discovery and Interface Activation 112
8.1.2 Interface Deactivation 112
8.2 Frame RF Interface 112
8.2.1 Data Mapping between the DH and RF 112
8.2.2 Frame RF Interface specific Control Messages 116
8.2.3 Poll-side Frame RF Interface Management 120
8.2.4 Listen-side Frame RF Interface Management 121
8.3 ISO-DEP RF Interface 124
8.3.1 Data Mapping between the DH and RF 124
8.3.2 Poll-side ISO-DEP RF Interface Management 126
8.3.3 Listen-side ISO-DEP RF Interface Management 129
8.4 NFC-DEP RF Interface 131
8.4.1 Data Mapping between the DH and RF 131
8.4.2 NFC-DEP RF Interface Configuration 132
8.4.3 Poll-side NFC-DEP RF Interface Management 133
8.4.4 Listen-side NFC-DEP RF Interface Management 136
8.5 NDEF RF Interface 137
8.5.1 NCI Data Message Format 138
NDEF RF Interface specific Control Messages 142
8.5.2 142
8.5.3 NDEF RF Interface Management 142
8.5.4 Failures during Data Exchange 144

9 RF Interface Extensions 146
9.1 Frame Aggregation RF Interface Extension 146
9.1.1 Startup conditions 146
9.1.2 Starting the RF Interface Extension 146
9.1.3 RF Interface Extension functionality 147
9.1.4 Stopping the RF Interface Extension 150
9.2 LLCP Symmetry RF Interface Extension 150
9.2.1 Startup conditions 151
9.2.2 Starting the RF Interface Extension 151
9.2.3 RF Interface Extension functionality 152
9.2.4 Stopping the RF Interface Extension 153

10 NFCEE Discovery and Mode Set 155
10.1 NFCEE ID 155
10.2 NFCEE Discovery 156
10.2.1 HCI-NFCEE Specific Handling 161
10.2.2 NDEF-NFCEE Specific Handling 162
10.3 NFCEE Enabling and Disabling 162
10.3.1 HCI-NFCEE Specific Handling 163
10.4 NDEF-NFCEE 164
10.5 NFCEE Status 164
10.5.1 HCI- NFCEE Specific Handling 165

10.6 NFCEE Power Supply and Communication Link Control 165
10.6.1 HCI- NFCEE Specific Handling 167
11 NFCEE Interfaces 168
11.1 APDU NFCEE Interface 168
11.1.1 Data Exchange 168
11.1.2 Failures during Data Exchange 170
11.2 Type 3 Tag Command Set NFCEE Interface 170
11.2.1 Data Exchange 170
11.3 Transparent NFCEE Interface 171
11.3.1 Data Exchange 171
12 Transport Mappings 172
12.1 UART Transport 172
12.2 I2C Transport 173
12.3 Half Duplex SPI Transport 173
12.3.1 Physical 173
12.3.2 Data Transfer 174
13 Testing 180
13.1 Local Loopback Mode 180
A. Exhibit A 181
B. Common Tables 182
C. Revision History 194

Figures

Figure 1: NCI Scope 1
Figure 2: NCI Components 13
Figure 3: NCI concepts 14
Figure 4: Control Message Exchange 19
Figure 5: Data Exchange 21
Figure 6: NCI Core Packet Format 23
Figure 7: Control Packet Structure 24
Figure 8: Data Packet Structure 25
Figure 9: RF Interface Architecture 45
Figure 10: RF Communication State Machine 47
Figure 11: Format for Frame RF Interface (NFC-A) for Transmission 113
Figure 12: Format for Frame RF Interface (NFC-B) for Transmission 114
Figure 13: Format for Frame RF Interface (NFC-F) for Transmission 114
Figure 14: Format for Frame RF Interface (NFC-V) for Transmission 114
Figure 15: Format for Frame RF Interface (NFC-A) for Reception 115
Figure 16: Format for Frame RF Interface (NFC-B) for Reception 116
Figure 17: Format for Frame RF Interface (NFC-F) for Reception 116
Figure 18: Format for Frame RF Interface (NFC-V) for Reception 116
Figure 19: Format for ISO-DEP RF Interface for Transmission 125
Figure 20: Format for ISO-DEP RF Interface for Reception 125
Figure 21: Format for NFC-DEP RF Interface for Transmission 132
Figure 22: Format for NFC-DEP RF Interface for Reception 132
Figure 23: Format for Data Message from DH to NFCC 147
Figure 24: Format for Data Message from NFCC to DH 148
Figure 25: NFCEE State Transitions 161
Figure 26: Mapping of Command APDU 169
Figure 27: Mapping of Response APDU 170
Figure 28: Data Message Format for Type 3 Tag Command Set Interface 171
Figure 29: SPI Operation 174
Figure 30: SPI Data Transfer from the DH to the NFCC without CRC 175
Figure 31: SPI Data Transfer from the DH to the NFCC with CRC 176
Figure 32: SPI Data Transfer from the NFCC to the DH without CRC 177
Figure 33: SPI Data Transfer from the NFCC to the DH with CRC 178

Figure 34: SPI Race Condition 1 178
Figure 35: SPI Race Condition 2 179

Tables

Table 1: Abbreviations 5
Table 2: MT Values 23
Table 3: PBF Values 23
Table 4: Conn ID 28
Table 5: Control Messages to Reset the NFCC 29
Table 6: NCI Version 30
Table 7: Configuration Status 30
Table 8: Control Messages to Initialize the NFCC 32
Table 9: Values for Feature Enable Bit Mapping 33
Table 10: NFCC Features 34
Table 11: Control Messages for Setting Configuration Parameters 36
Table 12: Control Messages for Reading Current Configuration 37
Table 13: Destination Types 39
Table 14: Control Messages for DH Connection Creation 39
Table 15: Initial Number of Credits 40
Table 16: Destination-specific Parameters 40
Table 17: Control Messages for Connection Closure 42
Table 18: Control Messages for Connection Credit Management 43
Table 19: Control Messages for Generic Error 44
Table 20: Control Messages for Interface Error 44
Table 21: Notification for RF Field information 52
Table 22: RF Field Status 52
Table 23: RF Field Information Configuration Parameter 53
Table 24: Discovery Configuration Parameters for Poll A 56
Table 25: Discovery Configuration Parameters for Poll B 56
Table 26: Values for PB_SENSB_REQ_PARAM 57
Table 27: Discovery Configuration Parameters for Poll F 58
Table 28: Discovery Configuration Parameters for ISO-DEP 58
Table 29: Discovery Configuration Parameters for Poll NFC-DEP 59
Table 30: Values for PN_ATR_REQ_CONFIG 60
Table 31: Poll Mode Discovery Configuration Parameters for Active Mode 60
Table 32: Discovery Configuration Parameters for Poll V 60
Table 33: Discovery Configuration Parameters for Listen A 61

Table 34: LA_SEL_INFO coding 61
Table 35: Discovery Configuration Parameters for Listen B 63
Table 36: LB_SENSB_INFO values 64
Table 37: LB_FWI_ADC_FO values 64
Table 38: Discovery Configuration Parameters for Listen F 65
Table 39: Supported Protocols for Listen F 65
Table 40: Discovery Configuration Parameters for Listen T3T 66
Table 42: Discovery Configuration Parameters for Listen ISO-DEP 69
Table 43: Values for LI_A_RATS_TC1 69
Table 44: Discovery Configuration Parameters for Listen NFC-DEP 70
Table 45: Values for LN_ATR_RES_CONFIG 70
Table 46: Common Parameters for Discovery Configuration 71
Table 47: Values for CON_DISCOVERY_PARAM 72
Table 48: Control Messages for RF Interface Mapping Configuration 73
Table 49: Value Field for Mode 74
Table 50: Control Messages to Configure Listen Mode Routing 78
Table 51: More field values 78
Table 53: Listen Mode Routing Entry Types 79
Table 54: Value Field for Technology-based Routing 80
Table 55: Value Field for Protocol-based Routing 80
Table 56: Value Field for AID-based Routing 80
Table 57: Value Field for System Code-based Routing 80
Table 58: Value Field for APDU Pattern-based Routing 81
Table 59: Value Field for Power State 81
Table 60: Control Messages to Read the NFCC’s Listen Mode Routing 84
Table 61: Control Messages to Set the NFCC Route Selection Power State 85
Table 62: Control Messages to Configure Forced NFCEE Routing 90
Table 63: Value Field for Forced NFCEE Routing 90
Table 64: NFCC Configuration Control 92
Table 65: Value Field for NFCC Configuration Control 93
Table 66: Control Messages to Start Discovery 94
Table 67: RF Discovery ID 95
Table 68: Specific Parameters for NFC-A Poll Mode 97
Table 69: Specific Parameters for NFC-A Listen Mode 97

Table 70: Specific Parameters for NFC-B Poll Mode 98
Table 71: Specific Parameters for NFC-B Listen Mode 98
Table 72: Specific Parameters for NFC-F Poll Mode 99
Table 73: Specific Parameters for NFC-F Listen Mode 99
Table 75: Specific Parameters for NFC-ACM Poll Mode 100
Table 76: Specific Parameters for NFC-ACM Listen Mode 100
Table 77: Control Messages to select a Discovered Target 101
Table 78: Notification for RF Interface activation 102
Table 79: Control Messages for RF Interface Deactivation 104
Table 80: Deactivation Types 104
Table 81: Deactivation Reasons 105
Table 84: Notification for RF Discovery Request from NFCEE 108
Table 85: TLV Coding for RF Discovery Request from NFCEE 108
Table 86: Value Field for RF Discovery Request Information 108
Table 87: Notification to Report an NFCEE Action 109
Table 88: Trigger in NFCEE Action Notification 109
Table 89: RF_NFCEE_ACTION configuration parameter 111
Table 90: Control Messages for RF Parameter Update 117
Table 91: TLV Coding for RF Communication Parameter ID 117
Table 92: NFC-B Data Exchange Configuration Parameter 118
Table 93: Control Messages to Request the NFCC to send a Type 3 Tag Polling Command 119
Table 94: Pre-activation states and the split of commands between NFCC and DH 123
Table 95: Activation Parameters for NFC-A/ISO-DEP Poll Mode 126
Table 96: Activation Parameters for NFC-B/ISO-DEP Poll Mode 127
Table 97: Control Messages to Request the NFCC to send an ISO-DEP R(NAK) 128
Table 98: Activation Parameters for NFC-A/ISO-DEP Listen Mode 130
Table 99: Activation Parameters for NFC-B/ISO-DEP Listen Mode 130
Table 100: Specific Parameters for NFC-DEP RF Interface 132
Table 101: NFC-DEP Operation Parameter 133
Table 102: Activation Parameters for NFC-DEP Poll Mode 135
Table 103: Activation Parameters for NFC-DEP Listen Mode 137
Table 111: Frame Aggregation RF Interface Extension Start Parameter 146
Table 112: Aggregation TLV Objects 148
Table 113: Control Messages for Aggregation Abort 149

Table 114: LLCP Symmetry RF Interface Extension Start Parameter 151
Table 115: LLCP Version Parameter 153
Table 116: NFCEE IDs 155
Table 117: Control Messages for NFCEE Discovery 156
Table 118: TLV Coding for NFCEE Discovery 158
Table 119: Value Field for T3T Command Set Interface Supplementary Information 159
Table 121: Control Messages to Enable and Disable a Connected NFCEE 162
Table 122: Control Messages to report the status of an NFCEE 165
Table 123: Control Messages to constrain the Power Supply and link of an NFCEE 166
Table 124: SPI modes 173
Table 125: SPI Header Coding (DH to NFCC) without CRC 175
Table 126: SPI Header Coding (DH to NFCC) with CRC 175
Table 127: SPI Header Coding (NFCC to DH) without CRC 176
Table 128: SPI Header Coding (NFCC to DH) with CRC 177
Table 129: Status Codes 182
Table 130: RF Technologies 183
Table 131: RF Technology and Mode 184
Table 132: Bit Rates 184
Table 133: RF Protocols 185
Table 134: RF Interfaces 185
Table 136: NFCEE Protocols / Interfaces 186
Table 137: Length Reduction Values 186
Table 138: Configuration Parameter Tags 187
Table 139: GID and OID Definitions 191
Table 140: Revision History 194

1 Introduction

This document specifies a communication protocol called the NFC Controller Interface (NCI) between an NFC Controller (NFCC) and a Device Host (DH).

1.1 Objectives

NCI is defined to meet the following requirements:

- Be independent of a specific transport layer (independent of the physical connection and any associated link protocol). Transport Mappings define the details on how to run NCI on top of different NCI Transport layers.
- Accommodate different levels of functionality in the NFCC with regard to RF communications. Different levels of functionality imply different splits of the NFC Forum protocol stack between the NFCC and the DH. To achieve this, NCI specifies RF Interfaces, each of which can be communicated with a DH and each of which interfaces to a defined functional block implemented on the NFCC. An NCI implementation on an NFCC will be tailored to include the RF Interfaces that match the functionalities of the NFCC.
- Provide features to allow DH to NFC Execution Envrionment (NFCEE) communication. NCI therefore includes methods to discover and enumerate connected NFCEEs and the NFCEE Interfaces they support, and to establish connections between DH and NFCEE Interfaces. NCI also contains definitions of the data formats that can be exchanged over a connection to NFCEE Interfaces.
- Be extensible, to allow future extensions and vendor specific functionality.

1.2 Scope

The following figure outlines a typical architecture of an NFC Forum Device.

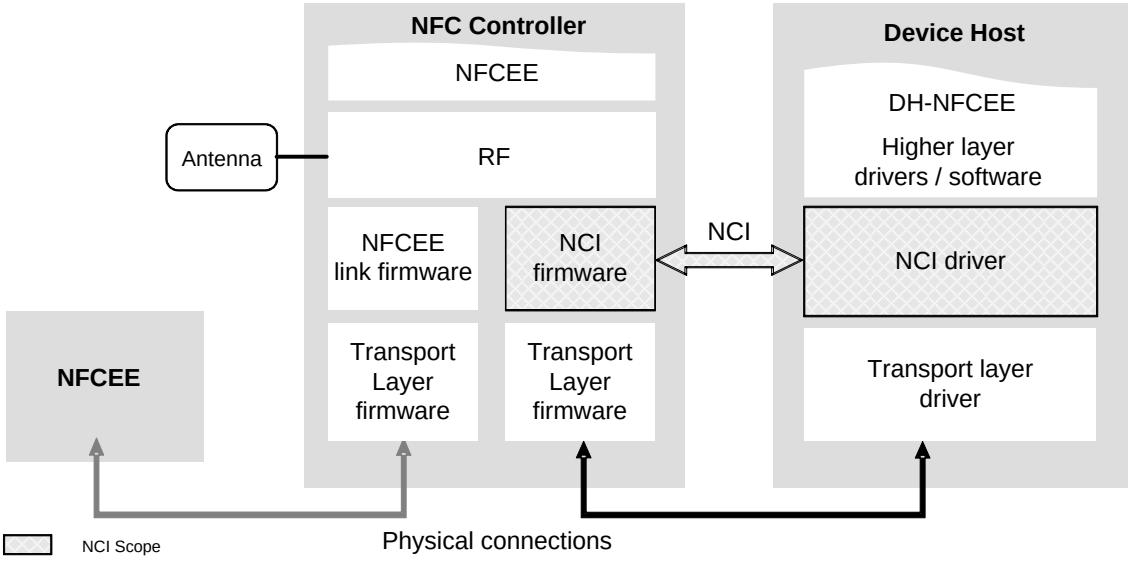

Figure 1: NCI Scope

The NFCC is connected to the Device Host, which is the main application processor in the device.

The DH higher layer software can contain one or more NFC Execution Environments, or one or more NFC Execution Environments can be connected to the DH (e.g. on an SD card). All NFC Execution Environments on or connected to the DH are logically viewed as one entity, called a DH-NFCEE.

In addition, one or more NFC Execution Environments can be integrated or connected to the NFCC. These are referred to as NFCEEs. Some NFCEEs integrated in, or connected to, the NFCC can be used to emulate an NFC Forum Tag. Such an NFCEE is called an NDEF-NFCEE.

The scope of NCI is to define the communication between the DH and the NFCC. The communication between the NFCC and NFCEEs is out of scope of this specification.

1.3 Audience

This document is intended for use by all manufacturers who implement NFC Controllers, NFC Forum Devices or NFC protocol stacks.

1.4 Applicable Documents or References

[ACTIVITY]	Activity Technical Specification, NFC Forum
[DIGITAL]	Digital Protocol Technical Specification, NFC Forum
[ISO/IEC_14443]	Identification cards – Contactless integrated circuit cards – Proximity cards Includes: [ISO/IEC 14443-1:2008], Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics [ISO/IEC 14443-2:2010], Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal balance [ISO/IEC 14443-3:2001], Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision [ISO/IEC_14443-3:2001/Amd.1], Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and Anti-collision, 1 February 2001 with Amendment 1: Bit rates of fc/64, fc/32 and fc/16, 15 June 2005; Amendment 3: Handling of reserved fields and values, 22 March 2006; and Corrigendum 1: Amendment 1 - Corrigendum, 29 August 2006 [ISO/IEC 14443-4:2008], Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol
[ETSI_102622]	ETSI TS 102 622, Smart Cards; UICC – Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) Release 10 2011, ETSI

[ETSI_102613] ETSI TS 102 613,
Smart Cards;
UICC – Contactless Front-end (CLF) Interface;
Part 1: Physical and data link layer characteristics
Release 11
2012,
ETSI

[ISO/IEC_7816-3] ISO/IEC 7816-3,
Identification cards - Integrated circuit cards - Part 3:
Cards with contacts – Electrical interface and transmission protocols
ISO/IEC

[ISO/IEC_7816-4] ISO/IEC 7816-4,
Identification cards - Integrated circuit cards. Organization, security, and commands for interchange,
2005,
ISO/IEC

[ISO/IEC_28361] ISO/IEC 28361
Information technology - Telecommunications and information exchange between systems - Near Field Communication Wired Interface (NFC-WI),
2007,
ISO/IEC

[I2C] I^2C-bus specification and user manual, Rev 03,
June 2007,
NXP

[LLCP] Logical Link Control Protocol Technical Specification,
NFC Forum

[MANU] Register of IC manufacturers, ISO/IEC JTC1/SC17,
Standing Document 5

[NDEF] NFC Data Exchange Format (NDEF) Technical Specification,
NFC Forum

[RFC2119] Key words for use in RFCs to Indicate Requirement Levels, RFC 2119,
S. Bradner,
March 1997,
Internet Engineering Task Force

[T1TOP] NFC Forum Type 1 Tag Operation Technical Specification,
NFC Forum

[T2TOP] NFC Forum Type 2 Tag Operation Technical Specification,
NFC Forum

[T3TOP] NFC Forum Type 3 Tag Operation Technical Specification,
NFC Forum

[T4TOP] NFC Forum Type 4 Tag Operation Technical Specification,
NFC Forum

[T5TOP] NFC Forum Type 5 Tag Operation Technical Specification, NFC Forum

1.5 Administration

The NFC Forum NFC Controller Interface (NCI) Technical 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 NFC Forum, Inc. maintains this specification.

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 NFC Controller Interface (NCI) Specification conforms to the Intellectual Property guidelines specified in the NFC Forum's *Intellectual Property Rights Policy*, as outlined in the NFC Forum *Rules of Procedure*. These documents are available on the NFC Forum website.

1.8 Special Word Usage

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT" and "MAY" in this document, with the exception of the RESTRICTIONS ON USE section, are to be interpreted as described in [RFC2119].

1.9 Abbreviations

Table 1 contains the definitions of the abbreviations and acronyms used in this specification.

Table 1: Abbreviations

Abbreviation	Description
AID	Application IDentifier
APDU	Application Protocol Data Unit
Conn ID	Connection Identifier
CRC	Cyclic Redundancy Check
CUP	Check Command, Update Command or Proprietary Command for the Type 3Tag Platform
DF	Dedicated File
DH	Device Host
GID	Group Identifier
HCI	Host Controller Interface
HCP	Host Controller Protocol
ISO	International Organization for Standardization
LLCP	Logical Link Control Protocol
LR	Length Reduction
LSB	Least Significant Byte
lsb	least significant bit
MSB	Most Significant Byte
msb	most significant bit
MT	Message Type
MTU	Maximum Transmission Unit
NCI	NFC Controller Interface
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCC	NFC Controller
NFCEE	NFC Execution Environment
OID	Opcode Identifier
PBF	Packet Boundary Flag
PDU	Protocol Data Unit
RF	Radio Frequency

Abbreviation	Description
RFU	Reserved for Future Use
SAR	Segmentation and Reassembly
SDD	Single Device Detection
SWIO	Single Wire protocol Input/Output
UART	Universal Asynchronous Receiver/Transmitter

1.10 Glossary

Active Communication Mode

A communication mode in which each device generates an Operating Field when it has to send a frame to a peer device.

Application IDentifier (AID)

Defined in [ISO/IEC_7816-4], this is a specific type of Dedicated File (DF) name that is used in a SELECT command to identify applications.

Battery Off State

State in which an internal battery or external power source is not available. For example, the battery is removed or empty, so the Device Host (DH) is switched off. The NFC Forum Device can only act in Listen Mode when the NFC Controller (NFCC) and certain NFC Execution Environments (NFCEEs) might be powered by a remote NFC device via magnetic coupling.

Big Endian

A method of recording or transmitting numerical data of more than 2 bytes, with the highest byte placed at the beginning.

Command Message

A request sent from the Device Host (DH) to the NFC Controller (NFCC) for action by the NFCC.

Connection Identifier (Conn ID)

A unique 4-bit identifier for a Logical Connection.

Control Message

A generic name when referring to a Command, Response, or Notification Message, but not a Data Message.

NOTE The terms ‘Command’, ‘Response’ and ‘Notification’, as used in this document, mean the same as ‘Command Message’, ‘Response Message’ and ‘Notification Messsage’.

Cyclic Redundancy Check (CRC)

A checksum appended within the data segment before transmission, and verified afterward by the recipient to detect Transmission Errors.

Data Message

A message containing data carried over a Logical Connection.

Destination Type

Identifies an entity (NFCC, NFCEE, or Remote NFC Endpoint) for which a Dynamic Logical Connection is intended.

Device Host (DH)

An Execution Environment responsible for the overall management of the NFC Forum Device and any peripherals. This includes the management (e.g., initialization, configuration, power management, etc.) of the NFC Controller peripheral.

DH-NFCEE

An NFCEE residing on or connected to the DH. There is logically only one DH-NFCEE, but it might be composed of more than one environment (for example, an environment on the DH and an environment on a peripheral connected to the DH). The manner in which the DH manages the DH-NFCEE is implementation-specific.

Dynamic Logical Connection

A Logical Connection that is created and closed dynamically as needed.

HCI Network

A Network, as described in [ETSI_102622], consisting of a host controller and one or more hosts.

HCI-NFCEE

A specific type of NFCEE that is connected via the NFCC's HCI Network, as described in [ETSI_102622].

ISO-DEP Protocol

Half-duplex block transmission protocol as defined in [DIGITAL].

Listen Mode

The mode of an NFC Forum Device where it receives RF commands and sends RF responses as defined in [DIGITAL].

Little Endian

A method of recording or transmitting numerical data of more than 2 bytes, with the lowest byte placed at the beginning.

Logical Connection

A communication channel between the Device Host (DH) and the NFC Controller (NFCC) that is used for data communication toward the NFCC itself, an NFCEE, or a Remote NFC Endpoint.

Message

A generic term for a Command, Response, Notification, or Data object communicated between the DH and NFCC.

NCI

The logical interface between a Device Host (DH) and an NFC Controller (NFCC).

NCI Core

The basic NCI functionality between the Device Host (DH) and NFC Controller (NFCC).

NCI Transport

The physical connection (e.g., SPI, I2C, UART, USB, etc.) and any associated link level protocol between the DH and NFCC. Each supported NCI Transport has a Transport Mapping that defines the characteristics of the NCI Transport. An NCI Transport provides the ability to reliably transfer data without intimate knowledge of the data being transferred. The NCI specification defines multiple Transport Mappings.

NDEF-NFCEE

An NFCEE configured to emulate an NFC Forum Tag. An NDEF-NFCEE always stores an NDEF message, which can be empty, as defined in [NDEF].

NFC Controller (NFCC)

The entity responsible for the transmission of data via NFC. The NFC Controller has a connection to the Device Host (DH) and might have connections to additional NFC Execution Environments (NFCEEs). Those connections are out of scope of this specification, but the impacts to the NCI are in scope.

NFC Execution Environment (NFCEE)

An environment, either built into the NFCC or connected to the NFCC, where NFC applications are executed. The NFCEE might be included in entities with various form factors, some of which can be removable or replaceable.

NFC-DEP Initiator

The role of an NFC Forum Device reached when an NFC Forum Device in Poll Mode has gone through a number of Activities. In this mode, the NFC Forum Device communicates using the NFC-DEP Protocol.

NFC-DEP Protocol

The half-duplex block transmission protocol as defined in [DIGITAL].

NFC-DEP Target

The role of an NFC Forum Device, reached when the NFC Forum Device in Listen Mode has gone through a number of Activities. In this mode, the NFC Forum Device communicates using the NFC-DEP Protocol.

NFCEE Discovery Process

Functionality that allows detection of NFCEEs that are physically connected to the NFCC.

NFCEE Interface

A logical entity on the NFCC that communicates with the DH on one side and an NFCEE on the other side.

NFCEE Protocol

A protocol used in the communication between the NFCC and an NFCEE.

NFC Forum Device

A device that supports the following Modus Operandi: Initiator, Target, and Reader/Writer. It might also support Card Emulator.

NFC Forum Tag

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

Notification Message

A message that can only be sent by an NFCC to the DH. It is sent asynchronously and typically contains informational parameters.

Packet

A structure that is used to transmit a Message over the NCI Transport. There are both Control Packets (for transporting Control Messages) and Data Packets (for transporting Data Messages).

Passive Communication Mode

A communication mode in which one device generates an Operating Field and sends Commands to a second device. To respond, this second device uses load modulation, which means that it does not generate an Operating Field but it draws power from a Remote Field.

Poll Mode

The mode of an NFC Forum Device where it sends RF commands and receives RF responses as defined in [DIGITAL].

Remote NFC Endpoint

Refers to a remote device, card, or tag, connected wirelessly via NFC to the local NFC Forum Device.

Response Message

Sent by the NFCC for each Command Message received from the DH. The Response Message might contain status information pertaining to the results of the Command Message.

RF Discovery Process

Functionality that allows detection of a Remote NFC Endpoint and detection by a Remote NFC Endpoint. The DH can configure the RF Discovery Process, which then runs autonomously within the NFCC.

RF Interface

Logical entities that might contain some protocol logic (e.g., an ISO-DEP RF Interface or an NFC-DEP RF Interface) or might be a transparent conduit (e.g. a Frame RF Interface). The DH can only communicate with a Remote NFC Endpoint via an RF Interface, designated as the “Active RF Interface”. The NFCC contains multiple RF Interfaces.

RF Interface Extension

An RF Interface Extension extends the functionality of an RF Interface. It is a defined set of tasks in the NFCC that can be invoked by the DH via NCI Commands. Each RF Interface Extension defines its own behavior. Each RF Interface Extension defines the conditions – e.g. active RF Interface(s), Protocol(s) and Mode(s) - under which the RF Interface Extension can be started and stopped. Each RF Interface Extension also defines relationships and conflicts, if any, with other RF Interface Extensions.

RF Protocol

A protocol used in the communication between the NFCC and a Remote NFC Endpoint.

Static RF Connection

A Logical Connection with a fixed Connection Identifier that always exists after NFCC initialization and is never closed. It is used by the DH to communicate with a Remote NFC Endpoint via an active RF Interface.

Switched On State

In this state, the DH, the NFCC, and all connected NFCEEs are switched on and powered either by internal battery or external power source. The NFC Forum device can act in both Poll and Listen Modes. NCI is only applicable in Switched On State.

Switched Off State

In this state, the DH is switched off, and the NFCC and all connected NFCEEs are powered either by internal battery or external power source. The NFC Forum Device can only act in Listen Mode.

UICC

A Smart Card that conforms to the specifications written and maintained by the TC ETSI Smart Card Platform. It is a platform to resident applications (e.g., USIM, CSIM, ISIM, banking, transport, etc.).

1.11 Coding Conventions

The following coding conventions apply in this document if not stated otherwise.

- Each octet is represented by bits b0 to b7, where b7 is the most significant bit (msb) and b0 the least significant bit (lsb). In all representations the leftmost bit is the msb.
- All values greater than 1 octet are sent and received in Little Endian format.
- In representations of octet arrays, each octet is numbered, starting at 0. Octet numbered 0 is sent over the NCI Transport first.

This document uses the following notations for numbers:

- Values expressed in hexadecimal form are preceded by ‘0x’.
- Values expressed in binary form are followed by a lower case ‘b’.

In this document, the following rules apply for fields or values defined as Reserved for Future Use (RFU):

- For an NCI message including fields with a subset of octets or bits defined as RFU, the sender SHALL set these octets or bits to the value indicated in this document or to zero if no value is given.
- For an NCI message including fields with a subset of octets or bits defined as RFU, the receiver SHALL disregard these octets or bits and SHALL keep the same interpretation of any other field of the whole message, unless explicitly stated otherwise.

For fields that could contain values that are defined as RFU, the sender of an NCI message SHALL NOT set these fields to the RFU values.

If a parameter is defined as meaningless in certain conditions, the message sender SHALL include the parameter, but MAY set its value to any value. The message receiver SHALL ignore the parameter value.

Values defined as Proprietary MAY be used by implementations for extensions that are out of scope of this specification.

In this specification, Control Messages are defined by tables that specify the message parameters. Control Messages SHALL be coded in the order and length specified by the corresponding definition table (the first parameter is defined in the topmost table row).

The names of Parameters that can be present multiple times in a Control Message are followed by square brackets containing the number of times the parameter is to be included. This information is expressed by an index range (e.g., [1..10]). The upper bound of this range might be a variable defined by another parameter. The parameter instances SHALL follow each other sequentially. The corresponding parameter length indicates the length of a single parameter instance (not the length of the complete parameter set).

2 NCI Architecture

This section outlines the basic concepts used in the NCI. It is an informal introduction to the normative statements later in this document.

2.1 Components

The NCI can be split into the following logical components:

- NCI Core

  The NCI Core defines the basic functionality of the communication between a Device Host (DH) and an NFC Controller (NFCC). This enables Control Message (Command, Response, and Notification) and Data Message exchange between an NFCC and a DH.

- Transport Mappings

  Transport Mappings define how the NCI messaging is mapped to an underlying NCI Transport, which is a physical connection (and optional associated protocol) between the DH and the NFCC. Each Transport Mapping is associated with a specific NCI Transport.

- NCI modules

  NCI modules build on top of the functionality provided by the NCI Core. Each module provides a well-defined functionality to the DH. NCI modules provide the functionality to configure the NFCC and to discover and communicate with Remote NFC Endpoints or with local NFCEEs.

  Some NCI modules are mandatory parts of an NCI implementation, others are optional.

  There can also be dependencies between NCI modules in the sense that a module might only be useful if there are other modules implemented as well. For example, all modules that deal with communication with a Remote NFC Endpoint (the RF Interface modules) depend on the RF Discovery to be present.

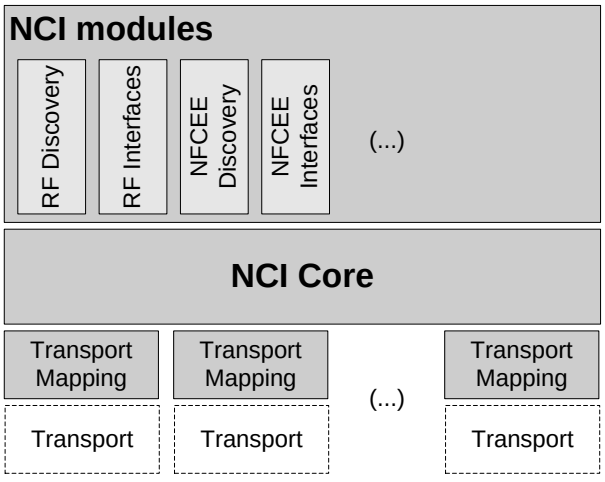

Figure 2: NCI Components

2.2 Concepts

This section outlines the basic concepts used in the NCI design.

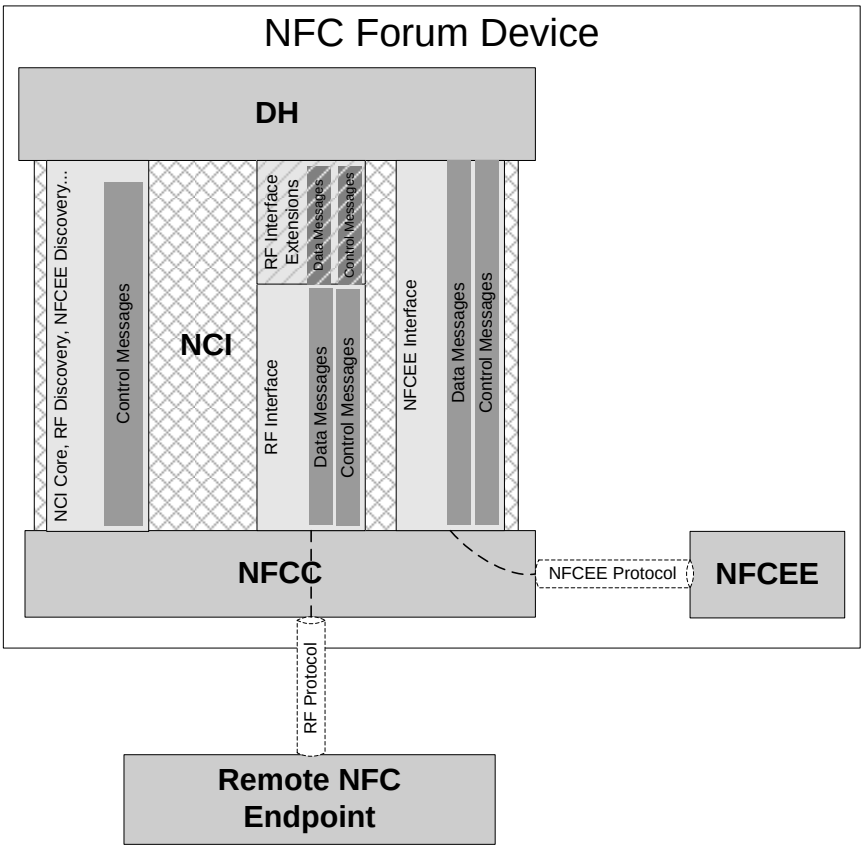

Figure 3: NCI concepts

2.2.1 Control Messages

A DH uses NCI Control Messages to manage and configure an NFCC. Control Messages consist of Commands, Responses, and Notifications. Commands are only allowed to be sent in the direction from DH to NFCC, and Responses and Notifications are only allowed to be sent in the other direction. Control Messages are transmitted in NCI Control Packets, and NCI supports segmentation of Control Messages into multiple Packets.

The NCI Core defines a basic set of Control Messages (e.g., for setting and retrieving NFCC configuration parameters). Additional Control Messages can be defined by NCI modules .

2.2.2 Data Messages

Data Messages are used to transport data to either a Remote NFC Endpoint (in NCI called“RF Communication”) or to an NFCEE (in NCI called “NFCEE Communication”). NCI defines Data Packets that enable the segmentation of Data Messages into multiple Packets.

Data Messages can only be exchanged in the context of a Logical Connection. A Logical Connection has to be established before any Data Messages can be sent. One Logical Connection, the Static RF Connection, is always established during initialization of NCI. The Static RF Connection is dedicated to RF Communication. Additional Logical Connections can be created for RF and/or NFCEE Communication.

Logical Connections provide flow control for Data Messages in the direction from DH to NFCC.

2.2.3 Interfaces

An NCI module might contain a single Interface. Each Interface defines how a DH can communicate via NCI with a Remote NFC Endpoint or NFCEE. Each Interface is defined to support specific protocols and can only be used for those protocols (the majority of Interfaces support exactly one protocol). NCI defines two types of Interfaces: RF Interfaces and NFCEE Interfaces.

Protocols used to communicate with a Remote NFC Endpoint are called RF Protocols. Protocols used to communicate with an NFCEE are called NFCEE Protocols.

An NFCEE Interface has a one-to-one relationship to an NFCEE Protocol. However, there might be multiple RF Interfaces for one RF Protocol. The multiple RF Interfaces allow NCI to support different splits of the protocol implementation between the NFCC and DH. An NCI implementation on an NFCC includes the RF Interfaces that match the functionality implemented on the NFCC.

Interfaces need to be activated before they can be used and deactivated when they are no longer used.

An Interface can define its own configuration parameters and Control Messages. But, most important, it defines both the mapping of the Data Message payload to the payload of the respective RF or NFCEE Protocol and, in the case of RF Communication, whether the Static RF Connection and/or Dynamic Logical Connections are used to exchange those Data Messages between the DH and the NFCC.

2.2.4 RF Interface Extensions

An RF Interface Extension adds a specific, clearly defined set of functions to one or more RF Interfaces. Each RF Interface Extension defines which RF Interfaces it can extend.

The availability of an RF Interface Extension is bound to the time one of these RF Interfaces is activated. The availability can additionally depend on other conditions, e.g. the currently used protocol in RF communication. If an RF Interface is active, available RF Interface Extensions can be started and stopped by the DH. RF Interface Extensions are never started automatically but are stopped when the RF Interface is deactivated. Each RF Interface Extension defines the Control Messages for starting and stopping its functionality.

While started, an RF Interface Extension can overrule definitions of the active RF Interface to provide its functionality. RF Interface Extensions can define the interface's own configuration parameters and Control Messages. They can also provide a format for Data Messages that is different from the one defined by the RF Interface. However, RF Interface Extensions can not overrule the deactivation behavior of the active Interface.

For a given RF Interface there can be multiple RF Interface Extensions. It is possible to start multiple RF Interface Extensions at the same time, as long as they are not mutually exclusive. Each RF Interface Extension defines with which other RF Interface Extension it can be used.

However, the extension process cannot be compounded: RF Interface Extensions are not intended to extend the functionality of other RF Interface Extensions.

2.2.5 RF Communication

RF Communication is started by configuring and running the RF Discovery process. The RF Discovery is an NCI module that discovers and enumerates Remote NFC Endpoints.

For each Remote NFC Endpoint the RF Discovery Process provides the DH with the Remote NFC Endpoint information that was gathered during the RF Discovery Process. This information includes the RF Protocol that is used to communicate with the Remote NFC Endpoint. During RF Discovery configuration the DH sets up a mapping that associates an RF Interface for each RF Protocol. If only a single Remote NFC Endpoint is detected during a discovery cycle, the RF Interface for this Endpoint is automatically activated. If there are multiple Remote NFC Endpoints detected in Poll Mode, the DH can select the Endpoint it wants to communicate with. This selection also triggers activation of the mapped Interface.

After an RF Interface has been activated, the DH can communicate with the Remote NFC Endpoint using the activated RF Interface. An activated RF Interface can be deactivated by either the DH or the NFCC (e.g., on behalf of the Remote NFC Endpoint). However, each RF Interface can define which of those methods are allowed. The deactivation options vary, depending on which part of the protocol stack is executed on the DH. For example, if a protocol command to tear down the communication is handled on the DH, the DH will deactivate the RF Interface. If such a command is handled on the NFCC, the NFCC will deactivate the Interface.

This specification describes the possible Control Message sequences for RF Communication in the form of a state machine.

2.2.6 NFCEE Communication

The DH can learn about the NFCEEs connected to the NFCC by employing the NFCEE Discovery module. During NFCEE Discovery the NFCC assigns an identifier for each NFCEE. When the DH wants to communicate with an NFCEE, it opens a Logical Connection to the NFCEE that includes the corresponding identifier and specifies the NFCEE Protocol to be used.

Opening a Logical Connection to an NFCEE automatically activates the NFCEE Interface associated with the protocol specified. As there is always a one-to-one relationship between an NFCEE Protocol and Interface, there is no mapping step required (unlike RF Interface activation).

After the Interface has been activated, the DH can communicate with the NFCEE using the activated Interface.

Closing the connection to an NFCEE Interface deactivates the NFCEE Interface.

NCI also includes functionality to allow the DH to enable or disable the communication between an NFCEE and the NFCC.

2.2.7 Identifiers

NCI uses different Identifiers for Remote NFC Endpoints and NFCEEs. These identifiers are dynamically assigned by the NFCC. The DH learns them in the contexts of RF Discovery and NFCEE Discovery. The identifiers for Remote NFC Endpoints are called RF Discovery IDs. They usually have a short lifetime as they are only valid for the time the DH wants to be able to communicate with the Remote NFC Endpoint. In contrast, the identifiers for NFCEEs have a longer lifetime, since NFCEEs usually are not frequently added to or removed from a device. The identifiers for NFCEEs are called "NFCEE IDs". There is one reserved and static NFCEE ID, value 0, which represents the DH-NFCEE.

Logical Connections take a third type of identifier, Destination Type, as a first parameter to identify the destination for the data. Depending on the Destination Type, there can be a second parameter for identifying the data destination. For example, if the Destination Type is 'Remote NFC Endpoint', the second parameter will be an RF Discovery ID.

2.2.8 NFCC as Shared Resource

The NFCC might not only be used by the DH but also by the NFCEEs in the device (in such a case the NFCC is a shared resource). NFCEEs differ in the way they are connected to the NFCC, and the protocol used on such a link determines how an NFCEE can use the NFCC. For example, some protocols allow the NFCEE to provide its own configuration for RF parameters to the NFCC (similar to the NCI Configuration Parameters for RF Discovery). In other cases the NFCEE might not provide such information.

NFCCs can have different implementation in how they deal with multiple configurations from DH and NFCEEs. For example, they might switch between those configurations so that only one is active at a time, or they might attempt to merge the different configurations. During initialization, NCI provides information for the DH as to whether the configuration it provides is the only one or if the NFCC supports configuration by NFCEEs as well.

NCI includes a module, called "Listen Mode Routing", with which the DH can define where to route received data when the device has been activated in Listen Mode. The Listen Mode Routing allows the DH to maintain a routing table on the NFCC. Routing can be done based on the technology or on the protocol of the incoming traffic, based on the System Code if the T3T protocol is used, or based on application identifiers if 7816-4 APDU commands are used on top of ISO-DEP.

In addition, NCI enables the DH to get informed if communication between an NFCEE and a Remote NFC Endpoint occurs.

3 NCI Core Framework

3.1 Overview

The NCI Core includes the following required functionality:

- Packet formats to transmit Commands, Responses, Notifications, and Data Messages over NCI.
- Definition of the Commands, Responses, and Notifications used for different operations (specified in Section 4) between a Device Host and an NFC Controller. (Some later sections in this specification define additional Commands, Responses, and Notifications that are not part of the NCI Core.)
- A flow control mechanism for Command/Response Message exchange.
- A Logical Connection concept for Data Messages.
- A credit-based flow control mechanism for Data Messages sent from the DH to the NFCC.
- Segmentation and reassembly for Control and Data Messages.
- An addressing scheme for NFC Execution Environments (NFCEE). The NCI Core supports communication between the DH and NFCEEs connected to the NFCC.

NOTE NCI only covers the link between a DH and an NFCC, so communication from a DH to an NFCEE will only be possible if it is also supported by the protocols used between the NFCC and the NFCEE.

- An addressing scheme for Remote NFC Endpoints. The NCI Core uses Logical Connections to support communication between the DH and targets (NFCEEs or Remote NFC Endpoints), which are discovered by the NFCC.
- Reset, initialization, and configuration of the NFCC.
- Exception handling, including Control Messages for indicating errors, and rules for how to use them.

3.2 NCI Control Messages

Control Messages contain Commands, Responses, and Notifications. They control the interaction between the DH and the NFCC. See Figure 4.

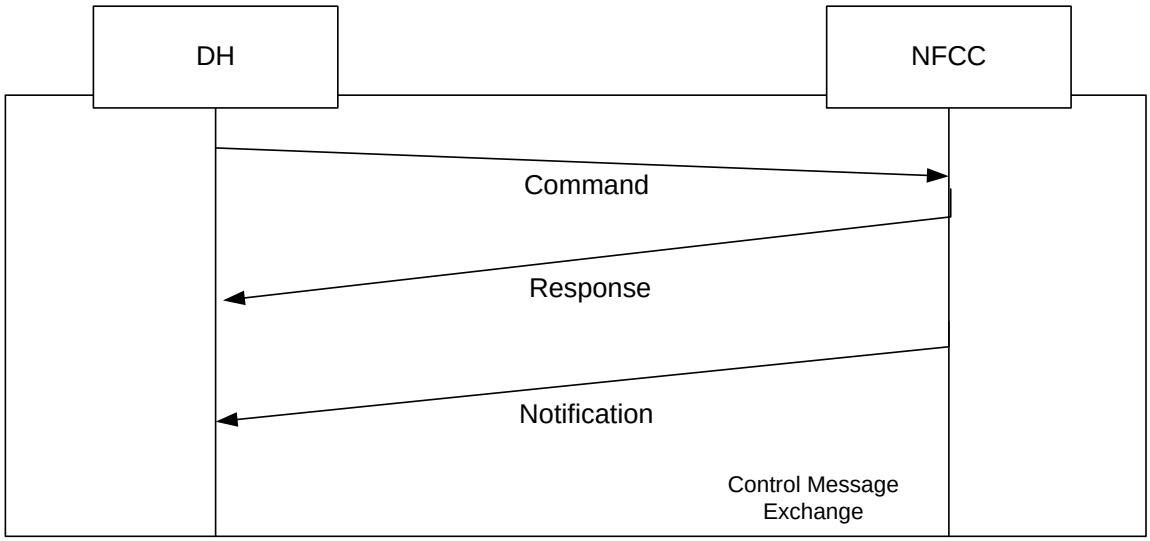

Figure 4: Control Message Exchange

A Command can be sent by the DH to instruct the NFCC to perform a specific action. For each Command received, the NFCC SHALL answer with a Response to acknowledge the receipt of the Command. The Response MAY also indicate changes that the Command caused at the NFCC.

Notifications SHALL only be sent from the NFCC to the DH. A Notification can be sent to deliver additional information related to a Command. A Notification can also be sent independently of any Command or Response, unless specified otherwise.

The payload of Control Messages is sent over the NCI Transport as a payload of Control Packets. A Control Packet payload contains either a complete or a segment of a Control Message payload.

Both the DH and the NFCC SHALL be capable of supporting Control Messages with a payload of 255 octets, which is the maximum size of any Control Message payload.

The maximum payload length of a Control Packet is also 255 octets. The DH SHALL be capable of receiving Control Packets with 255 octet payloads. However, the NFCC MAY specify a smaller maximum Control Packet payload size, as defined by the parameter Max Control Packet Payload Size. See Section 4.2.

As a result, Control Messages can be segmented into multiple Control Packets when sent over the NCI (described in Section 3.5).

3.2.1 Flow Control for Control Messages

The DH and NFCC are allowed to send a complete Control Message over the NCI in as many Packets as needed. There is no Packet-based flow control for Control Messages in NCI.

The following flow control rules apply to Control Messages:

- After sending a Command, the DH SHALL NOT send any Command until it receives a Response for that Command, or until it has taken steps to restore the capability to exchange Messages with the NFCC if it determines that too much time has elapsed waiting for a Response.
- After sending a Command, the DH SHALL be able to receive a Response.
- After sending a Response, the NFCC SHALL be ready to receive the next Command from the DH.
- The DH SHALL be able to receive a Notification from the NFCC at any time.

3.2.2 Exception Handling for Control Messages

The rules in this section define the exception processing to be performed by a receiver of an erroneous Control Message.

Any Command received by the DH SHALL be ignored. Any Response or Notification received by the NFCC SHALL be ignored.

A Control Message that is consistent with this specification, apart from the presence of additional bytes at the end, SHALL NOT be treated as a syntax error, but the additional bytes SHALL be ignored.

In all other cases of a Control Message with syntax errors, meaning that the coding of the Control Packet is not consistent with this specification and where the receiver can still determine the type of the Control Message:

- If the Control Message is a Command, the NFCC SHALL ignore the content of the Command and send a Response with the same Group Identifier (GID) and Opcode Identifier (OID) field values as in the Command and with a Status value STATUS_SYNTAX_ERROR. The Response SHALL NOT contain any additional fields.
- If the Control Message is a Response, the DH SHALL ignore the content of the Response and is free to send another Command.
- If the Control Message is a Notification, the DH SHALL ignore the Notification.

In case of a Control Message with a semantic error, meaning that a Control Message with valid syntax is received when it is not expected:

- An unexpected Response or Notification SHALL be ignored by the DH.
- An unexpected Command SHALL NOT cause any action by the NFCC. Unless otherwise specified, the NFCC SHALL send a Response with a Status value of STATUS_SEMANTIC_ERROR and no additional fields.

The NFCC SHALL respond to an unknown Command (unknown GID or OID) with a Response having the same GID and OID field values as the Command, followed by a Status field with the value of STATUS_SYNTAX_ERROR and no additional fields.

The DH SHALL ignore any unknown Response or Notification (unknown GID or OID).

An NFCC implementation that employs proprietary Notifications SHOULD take into account the fact that any DH that does not support those proprietary extensions will silently discard the Notifications.

If the NFCC cannot perform the action requested in a valid Command, the NFCC SHALL inform the DH using a Response with one of the Status field values defined in Table 129. Allowed Status values are specified for each Response. Reasons for not being able to perform a Command could be buffer overflow, limited processing power, limited resources, etc.

If the DH determines that too much time has elapsed waiting for a Response after it has sent a Command, possibly indicating a loss of ability to exchange Messages with the NFCC, it MAY resort to out-of-band measures to restore communication.

NOTE Such measures, which could include a hard reset or power cycling of the NFCC, are out of scope of this specification.

3.3 NCI Data Messages

Data Messages are used to exchange data over Logical Connections between a DH and NFCC target (NFCEE or Remote NFC Endpoint). See Figure 5.

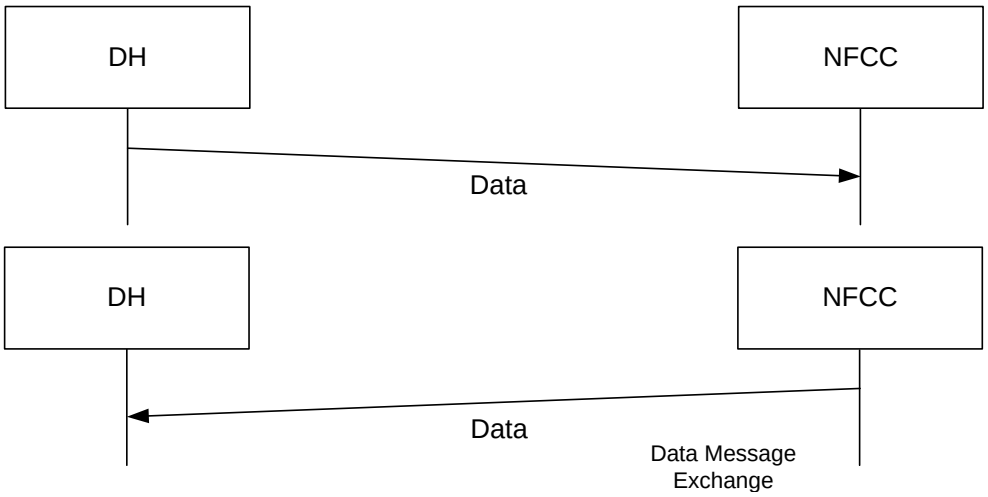

Figure 5: Data Exchange

The Data Message payload is sent over the NCI Transport as one or more payloads of Data Packets. A Data Packet payload contains either a complete or a segment of a Data Message payload.

Data Messages can be sent by either the DH (subject to flow control) or the NFCC at any time once a Logical Connection has been created.

The DH SHALL be capable of supporting any Data Message payload size sent by the NFCC (it is assumed that DH is able to handle any data received either from a local NFCEE or Remote NFC Endpoint). At any time, the maximum data size the NFCC is able to receive for a Logical Connection is defined by the Max Data Packet Payload Size announced during RF Interface activation in a case of Static RF Connection (see Section 7.3) or during Dynamic Logical Connection (see Section 4.4), times the number of unused credits given by the NFCC for that connection.

The maximum payload of a Data Packet is 255 octets. The DH SHALL be capable of receiving Data Packets with 255 octet payloads. However, the NFCC MAY specify a smaller maximum Data Packet payload size, on a Logical Connection basis.

The DH SHALL NOT send Data Packets with a payload length exceeding the Max Data Packet Payload Size that was announced during creation of the corresponding Logical Connection.

Data Messages can be segmented as described in Section 3.5.

3.3.1 Flow Control for Data Packets

A credit-based Data flow control mechanism is defined for data sent from the DH to the NFCC and MAY be invoked by the NFCC to eliminate buffer overflow conditions. It is assumed that the DH has sufficient buffering to handle all data sent from the NFCC, so credit-based flow control is not supported in that direction.

The credit-based flow control mechanism applies to Data Packets. Each Data Packet (that can contain either a complete Data Message or a segment of a Data Message) requires one credit.

Flow control is configured per Logical Connection during connection establishment (see Section 7.3 for Static RF Connection and Section 4.4 for Dynamic Logical Connection). It might be enabled or disabled differently for each Logical Connection and with different parameters.

The DH SHALL support credit-based flow control, though the NFCC MAY request the DH to use flow control.

Section 4.4.4 specifies the normative rules for the credit-based flow control mechanism.

3.3.2 Exception Handling for Data Messages

The rules in this section define the exception processing to be performed by a receiver of an erroneous Data Message.

In case of a Data Message with syntax error, meaning that the coding of the Data Message or any of the Data Packets in which it is transmitted is not consistent with this specification (including any definitions for the coding of fields inside the Payload of Data Packets for the currently active RF Interface, as defined in Section 8):

- If the receiver is the NFCC, it SHALL send a CORE_INTERFACE_ERROR_NTF message with a Status value of STATUS_SYNTAX_ERROR.
- If the receiver is the DH, it SHALL ignore the Data Message.

3.4 Packet Formats

3.4.1 Common Packet Header

All Packets have a common header, consisting of a Message Type (MT) field and a Packet Boundary Flag (PBF) field, as shown in Figure 6.

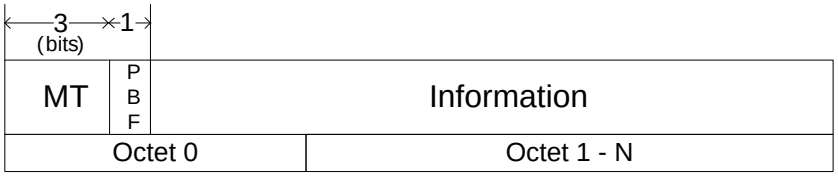

Figure 6: NCI Core Packet Format

Message Type (MT)

The MT field indicates the contents of the Packet and SHALL be a 3-bit field containing one of the values listed in Table 2. The content of the Information field is dependent on the value of the MT field. The receiver of an MT designated as RFU SHALL silently discard the packet.

Table 2: MT Values

MT	Description
000b	Data Packet- Section 3.4.3.
001b	Control Packet - Command Message as a payload- Section 3.4.2
010b	Control Packet - Response Message as a payload- Section 3.4.2
011b	Control Packet – Notification Message as a payload - Section 3.4.2
100b-111b	RFU

Packet Boundary Flag (PBF)

The Packet Boundary Flag (PBF) is used for Segmentation and Reassembly and SHALL be a 1 bit field containing one of the values listed in Table 3.

Table 3: PBF Values

PBF	Description
0b	The Packet contains a complete Message, or the Packet contains the last segment of a segmented Message
1b	The Packet contains a segment of a Message that is not the last segment.

The following rules apply to the PBF flag in Packets:

- If the Packet contains a complete Message, the PBF SHALL be set to 0b.
- If the Packet contains the last segment of a segmented Message, the PBF SHALL be set to 0b.

- If the packet does not contain the last segment of a segmented Message, the PBF SHALL be set to 1b.

See Section 3.5 for more details about Segmentation and Reassembly.

3.4.2 Format of Control Packets

The Control Packet structure is detailed in Figure 7.

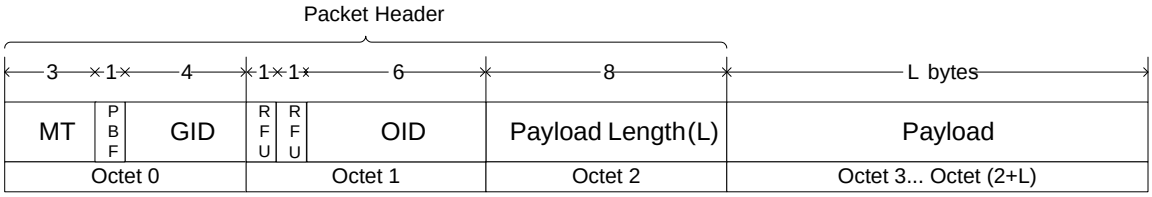

Figure 7: Control Packet Structure

Each Control Packet SHALL have a 3-octet Packet Header and MAY have additional payload for carrying a Control Message payload or a segment of a Control Message payload.

NOTE In the case of an 'empty' Control Message, only the Packet Header is sent.

Message Type (MT)

Refer to Table 2 for details of the MT field.

Packet Boundary Flag (PBF)

Refer to Table 3 for details of the PBF field.

Group Identifier (GID)

The NCI supports Commands, Responses, and Notifications that are categorized according their individual groups. The Group Identifier (GID) indicates the categorization of the message and SHALL be a 4-bit field containing one of the values listed in Table 139.

Opcode Identifier (OID)

The Opcode Identifier (OID) indicates the identification of the Control Message and SHALL be a 6-bit field that is a unique identification of a set of Command, Response or Notification Messages within the group. OID values are defined along with the definition of the respective Control Messages described in Table 139.

Payload Length (L)

The Payload Length SHALL indicate the number of octets present in the payload. The Payload Length field SHALL be an 8-bit field containing a value from 0 to 255.

3.4.3 Format of Data Packets

The Data Packet structure is detailed in Figure 8.

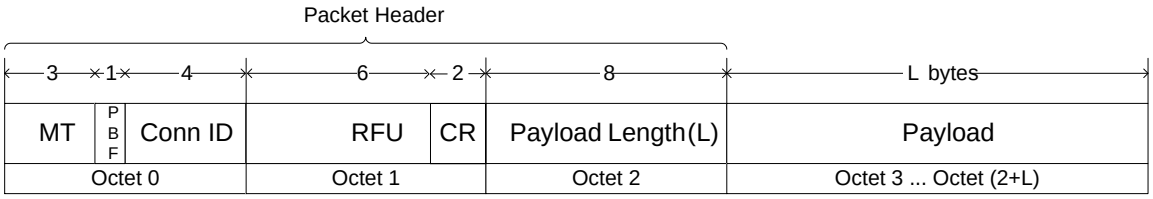

Figure 8: Data Packet Structure

Each Data Packet SHALL have a 3-octet Packet Header and MAY have additional Payload for carrying a Data Message payload or a segment of a Data Message payload.

NOTE In the case of an 'empty' Data Message, only the Packet Header is sent.

Message Type (MT)

Refer to Table 2 for details of the MT field.

NOTE MT always contains 000b to indicate a Data Packet, as defined in Table 2.

Packet Boundary Flag (PBF)

Refer to Table 3 for details of the PBF field.

Connection Identifier (Conn ID)

The Connection Identifier (Conn ID) SHALL be used to indicate the previously setup Logical Connection to which this data belongs. Refer to Section 4.4 for details on setting up a Logical Connection and the assignment of the Conn ID. The Conn ID is a 4-bit field containing a value from 0 to 15.

Credits (CR)

The Credits field is a 2-bit field containing a value from 0 to 3. In data packets sent from the DH to the NFCC, it SHALL contain a value of zero (0). If the NFCC uses Credit Based Flow Control (see Section 3.3.1 and Section 4.4.4), then the NFCC MAY give the DH credits for the Logical Connection used by the Data Packet by setting a non-zero value in this field. Otherwise the NFCC SHALL set a value of 0 in this field.

Payload Length (L)

The Payload Length field SHALL indicate the number of octets present in the payload. The Payload Length field SHALL be an 8-bit field containing a value from 0 to 255.

3.5 Segmentation and Reassembly

The Segmentation and Reassembly functionality SHALL be supported by both the DH and the NFCC.

Segmentation and Reassembly of Messages SHALL be performed independently for Control Packets and Data Packets of each Logical Connection.

Any NCI Transport Mapping is allowed to define a fixed Maximum Transmission Unit (MTU) size in octets. If such a Mapping is defined and used, then, if either DH or NFCC needs to transmit a Message (either Control or Data Message) that would generate a Packet (including Packet Header) larger than the MTU, the Segmentation and Reassembly (SAR) feature SHALL be used on the Message.

The following rules apply to segmenting Control Messages:

- For each segment of a Control Message, the header of the Control Packet SHALL contain the same MT, GID and OID values.
- **From DH to NFCC:** The Segmentation and Reassembly feature SHALL be used when sending a Command Message from the DH to the NFCC that would generate a Control Packet with a payload larger than the "Max Control Packet Payload Size" reported by the NFCC at initialization (see Section 4.2). Each segment of a Command Message except for the last SHALL contain a payload with the length of "Max Control Packet Payload Size".
- **From NFCC to DH:** When an NFCC sends a Control Message to the DH, regardless of the length, it MAY segment the Control Message into smaller Control Packets if needed for internal optimization purposes.

The following rules apply to segmenting Data Messages:

- For each segment of a Data Message, the header of the Data Packet SHALL contain the same MT and Conn ID.
- **From DH to NFCC:** If a Data Message payload size exceeds the Max Data Packet Payload Size of the connection, then the Segmentation and Reassembly feature SHALL be used on the Data Message.
- **From NFCC to DH:** When an NFCC sends a Data Message to the DH, regardless of the payload length, it MAY segment the Data Message into smaller Data Packets for any internal reason; for example, for transmission buffer optimization.

For both Control and Data Messages, the PBF bit SHALL be set as defined in **Table 3**.

3.6 Logical Connections

Logical Connections are used to exchange Data Messages between the DH and the NFCC. Logical Connections provide a common context for related Data Messages. Depending on the information exchanged during Logical Connection establishment, the NFCC can be the endpoint of the Data communication, or it has to forward the Payload of the Data Messages to or from a Remote NFC Endpoint or NFCEE (the latter two being the main use cases for Logical Connections).

A Logical Connection is set up through negotiation between the NFCC and the DH (described in Section 4.4). The following is an overview of the Logical Connection concept.

Dynamic Logical Connection:

- The DH MAY create a Dynamic Logical Connection.
- The NFCC MAY reject an incoming connection request.
- An identifier (Conn ID) will be assigned by the NFCC to identify the Dynamic Logical Connection, and this remains valid for the life of the Dynamic Logical Connection. The Conn ID is released when the Dynamic Logical Connection is closed.
- The DH can close a Dynamic Logical Connection.
- Data can be transported only after the Dynamic Logical Connection has been successfully created.
- Both the DH and the NFCC SHALL ignore Data Packets with unassigned Conn IDs.

Static RF Connection:

- The Static RF Connection both exists after NFCC Initialization without requiring creation using the connection Control Messages (defined in Section 4.4.2) and is never closed.
- The Initial Number of Credits and Max Data Packet Payload Size of the Static RF Connection are (re)established by the NFCC each time it sends RF_INTF_ACTIVATED_NTF.
- The DH SHALL NOT send data over the Static RF Connection if there is no active RF Interface. See Section 7.3.
- If there is no active RF Interface, both the DH and the NFCC SHALL ignore Data Packets with the Conn ID of the Static RF Connection.

NOTE All RF Interfaces included in this version of the specification use only the Static RF Connection. However, Dynamic Logical Connections might be used by RF Interfaces included in future versions of this specification.

Static HCI Connection:

If the NFCC reports in the CORE_INIT_RSP that it implements an HCI Host Controller (as defined in [ETSI_102622]), then:

- The Static HCI Connection both exists after NFCC Initialization without requiring creation using the connection Control Messages (defined in Section 4.4.2) and is never closed.
- The Initial Number of Credits and Max Data Packet Payload Size of the Static HCI Connection are reported by the NFCC in the CORE_INIT_RSP (see Section 4.2).

The payload of the Data Packets sent on the Static HCI Connection SHALL be valid host controller protocol (HCP) packets, as defined in [ETSI_102622]. Each Data Packet SHALL contain a single HCP packet. NCI Segmentation and Reassembly SHALL NOT be applied to Data Messages in either direction. The HCI fragmentation mechanism is used if required.

The Conn ID has a range of 0 to 15 (see Table 4). The Conn ID of 0 is reserved for the Static RF Connection used for RF communication, which exists after NFCC Initialization. However, that is not available for use unless an RF Interface is activated. Each RF Interface defines whether the Static RF Connection is used and whether Dynamic Logical Connections are permitted.

Table 4: Conn ID

Conn ID	Description
0000b	Static RF Connection between the DH and a Remote NFC Endpoint
0001b	Static HCI Connection between the DH and the HCI Network
0010b-1111b	Dynamically assigned by the NFCC

4 NCI Core Control Messages

Following are the descriptions of the Commands, Responses, and Notifications that are part of the NCI Core.

4.1 Reset of NFCC

These Control Messages are used to reset the NFCC.

Table 5: Control Messages to Reset the NFCC

CORE_RESET_CMD			
Payload Field(s)	**Length**	**Value/Description**	
Reset Type	1 Octet	0x00	Keep Configuration Reset the NFCC and keep the NCI RF Configuration (if supported).
		0x01	Reset Configuration Reset the NFCC including the NCI RF Configuration.
		0x02 – 0xFF	RFU

CORE_RESET_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

CORE_RESET_NTF			
Payload Field(s)	**Length**	**Value/Description**	
Reset Trigger	1 Octet	0x00	Unrecoverable error occurred in the NFCC
		0x01	NFCC was powered on
		0x02	CORE_RESET_CMD was received
		0x03-0x9F	RFU
		0xA0-0xFF	For proprietary use
Configuration Status	1 Octet	See Table 7.	
NCI Version	1 Octet	See Table 6.	
Manufacturer ID	1 Octet	IC Manufacturer ID, as defined in [MANU]. If this information is not available, the NFCC SHALL set this field to 0x00.	
Manufacturer Specific Information Length	1 Octet	The length of the manufacturer specific information. If this information is not available, or if the Manufacturer ID is equal to 0x00, the NFCC SHALL set a length of 0x00.	
Manufacturer Specific Information	n Octets	This field contains NFCC manufacturer specific information, such as chip version, firmware version, etc., encoded in a manufacturer-specific way.	

Table 6: NCI Version

NCI Version Identifier	Definition
0x10	NCI Version 1.0
0x11	NCI Version 1.1
0x20	NCI Version 2.0
Other values	RFU

Table 7: Configuration Status

Value	Definition
0x00	NCI RF Configuration has been kept
0x01	NCI RF Configuration has been reset
0x02-0xFF	RFU

The NCI Version parameter SHALL be encoded as an 8-bit field consisting of two 4-bit unsigned values representing the major and minor release levels of this specification. The most significant 4 bits SHALL denote the major release level. The least significant 4 bits SHALL denote the minor release level of this specification.

The DH SHALL continue the communication if it supports the major version reported by the NFCC and it SHALL NOT use Commands, RFU values, or RFU fields from a greater minor version than reported by the NFCC.

The CORE_RESET_CMD is issued by the DH to reset the NFCC. This Command MAY be issued anytime following power-up of the NFCC. If the DH sends CORE_RESET_CMD, it SHALL ignore all messages except CORE_RESET_RSP. Once the DH has received CORE_RESET_RSP, it SHALL NOT send any other command until it receives CORE_RESET_NTF.

On receipt of CORE_RESET_CMD, the NFCC SHALL respond with CORE_RESET_RSP with status set to STATUS_OK and begin its reset procedure. On completion of the reset procedure, the NFCC SHALL send CORE_RESET_NTF informing the DH that the NFCC has been reset.

Following successful reset, proprietary commands MAY be sent by the DH, and proprietary responses and notifications MAY be sent by the NFCC. The CORE_RESET_CMD allows defining different reset types using the Reset Type parameter. The Configuration Status parameters in CORE_RESET_NTF inform the DH about the status of the NCI RF configuration after the reset.

NOTE This allows different NFCC implementations: Some NFCCs might have persistent memory for the NCI RF Configuration and therefore do not require the DH to re-configure after a reset. Others might not have persistent memory for the NCI RF Configuration. The DH can force a reset of the configuration by using the Reset Type parameter. The DH knows, based on the Configuration Status value, whether it needs to configure the NFCC after the reset or not.

If Reset Type has been set to 0x00, the Configuration Status in CORE_RESET_NTF SHALL be set to either 0x00 or 0x01.

If Reset Type has been set to 0x01, the Configuration Status in CORE_RESET_NTF SHALL be set to 0x01.

For all Configuration Status values, all data in Buffers used for NCI Data and Control Packet exchange SHALL be deleted and the Buffer SHALL be freed.

In this context NCI RF Configuration SHALL comprise:

- The Listen Mode Routing Table and Forced NFCEE Routing state (see Section 6.3)
- All Configuration Parameters (see Table 138 for a list of Configuration Parameters)
- RF Interface Mapping configuration (see Section 6.2).

If Configuration Status in CORE_RESET_NTF is equal to 0x01, the NCI RF Configuration SHALL have been reset, which includes:

- Removing all entries of the Listen Mode Routing Table and disabling Forced NFCEE Routing
- Reverting all Configuration Parameter to their default values
- Erasing the RF Interface Mapping configuration.

If Configuration Status is equal to 0x00, the NCI RF Configuration SHALL be the same as before the reset. In this case, the NFCC internal mapping of NFCEEs to NFCEE IDs SHALL also be unchanged (as otherwise the Listen Mode Routing Table would be corrupted).

The NFCC MAY also reset itself (without having received a CORE_RESET_CMD); e.g., in the case of an internal error. In these cases, the NFCC SHALL inform the DH with the CORE_RESET_NTF. The Reason code SHALL reflect the internal reset reason and the Configuration Status the status of the NCI RF Configuration.

Following successful reset, the NCI initialization specified in Section 4.2 SHALL be performed.

4.2 Initialization of NFCC

These Control Messages are used to initialize the NFCC.

Table 8: Control Messages to Initialize the NFCC

CORE_INIT_CMD		
Payload Field(s)	**Length**	**Value/Description**
Feature Enable	2 Octets	A set of bits that are used to enable or disable certain NFCC features that might cause compatibility problems for a DH that implements an earlier minor release level of the specification. In all cases, 0 means disable the feature to ensure backwards compatible operation. See Table 9.

CORE_INIT_RSP			
Payload Field(s)	**Length**	**Value/Description**	
Status	1 Octet	See Table 129.	
NFCC Features	4 Octets	See Table 10.	
Max Logical Connections	1 Octet	0x00 – 0x0E	Maximum number of Dynamic Logical Connections supported by the NFCC.
		0x0F – 0xFF	RFU
Max Routing Table Size	2 Octets	Indicates the maximum amount of data in Octets that are possible in a routing configuration (see Section 6.3). If Listen Mode Routing is not supported, then the value SHALL be 0x0000.	
Max Control Packet Payload Size	1 Octet	Indicates the maximum payload length of a NCI Control Packet that the NFCC is able to receive. Valid range is 32 to 255. NOTE All Control Messages exchanged prior to this have a length that is smaller than 32 octets.	
Max Data Packet Payload Size of the Static HCI Connection	1 Octet	The maximum payload length of an NCI Data Packet that the NFCC is able to receive on the Static HCI Connection. If the NFCC implements an HCI Host Controller, the valid range is 32 to 255. If not, the value SHALL be 0.	

CORE_INIT_RSP				
Payload Field(s)	**Length**	**Value/Description**		
Number of Credits of the Static HCI Connection	1 Octet	Number of credits allocated by the NFCC to the Static HCI Connection. If the NFCC implements an HCI Host Controller, the value SHALL be filled according to Table 15. If not, the value SHALL be 0		
Max NFC-V RF Frame Size	2 Octets	This field contains the maximum Payload_Data size of an NFC-V Standard Frame (as defined in [DIGITAL]) supported by the NFC Controller for transfer of Commands and reception of Responses, when configured to Poll for NFC-V technology. The NFCC SHALL support a Max NFC-V RF Frame Size with at least 64 bytes.		
Number of Supported RF Interfaces	1 Octet	Number of Supported RF Interface fields to follow (n).		
Supported RF Interfaces [1..n]	x+2 Octets	Interface	1 Octet	See Table 134. All interfaces, including the pseudo interface NFCEE Direct RF Interface, supported by the NFCC SHALL be reported.
		Number of Extensions	1 Octet	The number of RF Interface Extensions supported for this Interface (x).
		Extension List [0..x]	1 Octet	See Table 135. The list of supported RF Interface Extensions

Table 9: Values for Feature Enable Bit Mapping

	Bit Mask								**Description**
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	0	0	0	0	0	0	0	0	RFU
Octet 1	0	0	0	0	0	0	0	0	RFU

The CORE_INIT_CMD is used by the DH to initialize the NFCC. This Command SHALL be issued following indication that the NFCC has been successfully reset (see Section 4.1), and at no other time.

On execution of the Command, the NFCC SHALL send a CORE_INIT_RSP to inform the DH that the NFCC has executed the Command. If the initialization was successful, the Status SHALL be STATUS_OK. If the NFCC is unable to execute the Command, the Status SHALL be set to STATUS_FAILED (see Table 129), and the other parameters of the CORE_INIT_RSP SHALL be ignored by the DH.

No other Command that is defined in this specification except for CORE_RESET_CMD or CORE_INIT_CMD SHALL be sent prior to the NFCC being successfully initialized.

After sending a CORE_INIT_CMD, the DH SHALL discard any information that was previously provided by the NFCC concerning discovery requests from NFCEE(s).

Table 10: NFCC Features

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	0	0	0						RFU
				X					Active Communication Mode. If equal to 1 the NFCC supports Active Communication Mode. Otherwise the NFCC does not support Active Communication Mode.
					X				HCI Network Support If equal to 1b, the NFCC implements the HCI Network as defined in [ETSI_102622]. Otherwise the NFCC does not implement the HCI Network.
						X	X		Discovery Configuration Mode: This parameter informs the DH how the NFCC uses the RF Configuration provided by the DH if multiple NFCEEs exist in the NFC Forum Device. If set to 00b, the DH is the only entity that configures the NFCC. If set to 01b, the NFCC can receive configurations from the DH and other NFCEEs. This implies that the NFCC can manage or merge multiple configurations, including RF Configuration Parameters, the Listen Mode Routing Configuration, and the RF Technology and Mode list (described in Section 7.1). Other values are RFU. See Section 7.1 for more details about the use of this parameter.
								X	If equal to 1b, Discovery Frequency configuration in RF_DISCOVER_CMD is supported. If equal to 0b the Discovery Frequency value is ignored and the value of 0x01 SHALL be used by the NFCC.

Octet 1	0							RFU
		X						Forced NFCEE Routing: Supported if the bit is equal to 1b; otherwise not supported.
			X					APDU Pattern based routing: Supported if the bit is equal to 1b; otherwise not supported.
				X				System Code based routing; Supported if the bit is equal to 1b; otherwise not supported.
					X			AID based routing; Supported if the bit is equal to 1b (NFCC supports 7816-4 Command parsing of SELECT command); otherwise not supported.
						X		Protocol based routing; Supported if bit is equal to 1b; otherwise not supported.
							X	Technology based routing; Supported if the bit is equal to 1b; otherwise not supported.
							0	RFU
Octet 2	0	0	0	0				RFU
					X			RF Configuration in Switched Off State Supported if the bit is equal to 1b, otherwise not supported. This bit can be equal to 1b only when b1 of this octet is also equal to 1b.
						X		Switched On Sub-Mode States: Supported if the bit is equal to 1b; otherwise not supported.
							X	Switched Off State; Supported if the bit is equal to 1b; otherwise not supported.
							X	Battery Off State; Supported if the bit is equal to 1b; otherwise not supported.
Octet 3	0	0	0	0	0	0	0	0	Octet 3 is reserved for proprietary capabilities

If no routing type is supported in Octet 1 of the NFCC Features, then the NFCC does not support Listen Mode Routing. In that case the DH SHALL NOT use any Command defined in Section 6.3.

NOTE RF Configuration in Switched Off State might be offered by NFCCs that are capable of being connected by more than one NFCEE.

4.3 NFCC Configuration

4.3.1 Setting the Configuration

These Control Messages are used to set configuration parameters on the NFCC.

Table 11: Control Messages for Setting Configuration Parameters

CORE_SET_CONFIG_CMD				
Payload Field(s)	**Length**	**Value/Description**		
Number of Parameters	1 Octet	The number of Parameter fields to follow (n).		
Parameter [1..n]	m+2 Octets	ID	1 Octet	The identifier of the configuration parameter. See Table 138 for a list of IDs.
		Len	1 Octet	The length of Val (m). If Len is equal to 0x00, then the Val field is omitted, and the NFCC SHALL set the configuration parameter to its default value.
		Val	m Octets	The value of the configuration parameter.

CORE_SET_CONFIG_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129
Number of Parameters	1 Octet	The number of Parameter ID fields to follow (n). Value SHALL be 0x00 and no Parameter IDs listed unless Status = STATUS_INVALID_PARAM.
Parameter ID [0..n]	1 Octet	The identifier of the invalid configuration parameter. See Table 138 for a list of IDs.

All configuration parameters in the NFCC are set to default values, but the DH MAY use CORE_SET_CONFIG_CMD to change these values. The NFCC responds with CORE_SET_CONFIG_RSP, and the Status indicates whether the setting of these configuration parameters was successful or not. A Status of STATUS_OK SHALL indicate that all configuration parameters have been set to these new values in the NFCC.

If the DH tries to set a parameter that is not applicable for the NFCC, the NFCC SHALL respond with a CORE_SET_CONFIG_RSP with a Status field of STATUS_INVALID_PARAM and including one or more invalid Parameter ID(s). All other configuration parameters SHALL have been set to the new values in the NFCC.

Based on the maximum size of the payload of a Control Message and on the length of the Payload Fields in CORE_GET_CONFIG_RSP, the maximum length of a parameter is limited to 251 octets. The parameter length fields (Parameter Len [n]) SHALL be set to a value between 0x00 and 0xFB. The values 0xFC - 0xFF are RFU.

4.3.2 Retrieve the Configuration

These Control Messages are used by the DH to retrieve current configuration parameters of the NFCC.

Table 12: Control Messages for Reading Current Configuration

CORE_GET_CONFIG_CMD		
Payload Field(s)	**Length**	**Value/Description**
Number of Parameters	1 Octet	The number of Parameter ID fields to follow (n).
Parameter ID [1..n]	1 Octet	The identifier of the configuration parameter. See Table 138 for a list of IDs.

CORE_GET_CONFIG_RSP				
Payload Field(s)	**Length**	**Value/Description**		
Status	1 Octet	See Table 129.		
Number of Parameters	1 Octet	The number of Parameter fields to follow (n).		
Parameter [1..n]	m+2 Octets	ID	1 Octet	The identifier of the configuration parameter. See Table 138 for a list of IDs.
		Len	1 Octet	Length of Val (m). If Len = 0x00, then Val field is omitted.
		Val	m Octets	Value of the configuration parameter.

The DH MAY use CORE_GET_CONFIG_CMD to retrieve the current configuration parameters of the NFCC. If the NFCC is able to respond with all requested parameters, the NFCC SHALL respond with the CORE_GET_CONFIG_RSP with a Status of STATUS_OK.

NOTE In the STATUS_OK case, parameter values can be ‘empty’ and therefore have a Len of 0x00 and no Val field (e.g., if the default value of the parameter is ‘empty’).

If the DH tries to retrieve any parameter(s) that are not available in the NFCC, the NFCC SHALL respond with a CORE_GET_CONFIG_RSP with a Status field of STATUS_INVALID_PARAM, containing each unavailable Parameter ID with a Parameter Len field of value zero. In this case, the CORE_GET_CONFIG_RSP SHALL NOT include any parameter(s) that are available on the NFCC.

NOTE This failure case (STATUS_INVALID_PARAM) is intended for when the DH tries to retrieve a Parameter that is not supported at all by the NFCC.

NOTE After receiving the list of unavailable Parameters, the DH can assume that the other Parameters requested in the CORE_GET_CONFIG_CMD are available, and the DH might initiate another CORE_GET_CONFIG_CMD to retrieve those Parameters.

If CORE_GET_CONFIG_RSP message payload size with all requested parameters would exceed the maximum Control Message payload size (255 octets), then the NFCC SHALL only send the limited set of parameters that will not exceed the maximum payload size. In this case, the Status field SHALL have a value of STATUS_MESSAGE_SIZE_EXCEEDED. The DH MAY retrieve any unreturned parameters by sending another CORE_GET_CONFIG_CMD requesting only those specific IDs.

If both of these conditions happen: 1) the DH tries to retrieve unavailable Parameters and 2) Response would exceed maximum Control Message payload size, then case (1) has higher priority; i.e., the NFCC SHALL return a status of STATUS_INVALID_PARAM to the DH.

4.4 Logical Connection Management

4.4.1 Destination Type

Destination Type is used during Logical Connection creation. It identifies the type of an entity in the system: NFCC, NFCEE or Remote NFC Endpoint.

Destination Types can also identify specific functionality in an entity, such as the loopback function in the NFCC.

The valid Destination Types are defined in Table 13.

Table 13: Destination Types

Destination Type	Description
0x00	RFU
0x01	NFCC Loopback This is used to create a Logical Connection between the DH and the NFCC for loopback mode. See Section 13.1.
0x02	Remote NFC Endpoint This is used to create a Dynamic Logical Connection for communicating with a Remote NFC Endpoint.
0x03	NFCEE This is used to create a Dynamic Logical Connection for communicating with an NFCEE that is not part of the HCI Network.
0x04 – 0xC0	RFU
0xC1 – 0xFE	Proprietary This is for proprietary use; e.g., to create a Logical Connection between the DH and the NFCC for firmware update purposes.
0xFF	RFU

4.4.2 Connection Creation

Control Messages are used when the DH creates a Dynamic Logical Connection to the NFCC.

Table 14: Control Messages for DH Connection Creation

CORE_CONN_CREATE_CMD				
Payload Field(s)	**Length**	**Value/Description**		
Destination Type	1 Octet	See Table 13.		
Number of Destination-specific Parameters	1 Octet	Based on the Destination Type of the connection, the number of Destination-specific Parameter fields following (n).		
Destination-specific Parameter [0..n]	m+2 Octets	Type	1 Octet	Type of the Destination-specific Parameter See Table 16.
		Length	1 Octet	Length of Value (m)
		Value	m Octets	Value of the Destination-specific Parameter

CORE_CONN_CREATE_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.
Max Data Packet Payload Size	1 Octet	A number from 1 – 255. See Section 3.3.
Initial Number of Credits	1 Octet	See Table 15.
Conn ID	1 Octet	The four least significant bits of the octet SHALL contain the Conn ID as defined in Table 4. The four most significant bits are RFU.

Table 15: Initial Number of Credits

Value	Description
0x00– 0xFE	Number of credits
0xFF	Data flow control is not used

Table 16: Destination-specific Parameters

Type	Length	Value
0x00	2 Octets	First octet: An RF Discovery ID (see Table 67). Second octet: RF Protocol (see Table 133).
0x01	2 Octets	First octet: NFCEE ID as defined in Table 116. The value of 0x00 (DH-NFCEE ID) SHALL NOT be used. Second octet: NFCEE Interface Protocol. See Table 136.
0x02-0x9F		RFU
0xA0-0xFF		For proprietary use

To create a Logical Connection, the DH sends the CORE_CONN_CREATE_CMD to the NFCC and identifies the Destination Type (see Section 4.4.1) to which this Logical Connection will apply.

The combination of Destination Type and Destination Specific Parameters SHALL uniquely identify a single destination for the Logical Connection.

If the Destination Type is 0x01, then no Destination-specific Parameters are allowed.

If the Destination Type is that of a Remote NFC Endpoint (0x02), then only the Destination-specific Parameter with Type 0x00 or proprietary parameters as defined in Table 16 SHALL be present.

NOTE This version of the specification does not actually use Dynamic Logical Connections for communication with Remote NFC Endpoints.

If the Destination Type is that of an NFCEE (0x03), then only the Destination-specific Parameter with Type 0x01 or proprietary parameters as defined in Table 16 SHALL be present.

After receipt of a CON_CREATE_CMD, the NFCC SHALL determine whether to accept the request and, if so, continue with the actual creation of the Logical Connection. The NFCC SHALL respond with a CORE_CONN_CREATE_RSP where the Status SHALL indicate whether the Logical Connection has been established (STATUS_OK) or failed. In failure case and if no different Status value is specified for the concrete case, the Status value SHALL be STATUS_REJECTED.

NOTE For example, NFCEE Interface activation (Section 11) defines a specific Status value for the NFCEE Interface activation failure.

If the Logical Connection has been established, the Conn ID SHALL indicate the Connection Identifier for this Logical Connection.

The CORE_CONN_CREATE_RSP SHALL contain the actual Conn ID used for the Logical Connection.

If data flow control is requested by the NFCC, the NFCC also indicates the Initial Number of Credits that the NFCC has allocated for this connection’s receive path. If data flow control is not requested, the NFCC SHALL set the parameter value for Initial Number of Credits to 0xFF.

4.4.3 Connection Closure

These Control Messages are used to close a Dynamic Logical Connection.

Table 17: Control Messages for Connection Closure

CORE_CONN_CLOSE_CMD		
Payload Field(s)	**Length**	**Value/Description**
Conn ID	1 Octet	The identifier of the connection to be closed. The four least significant bits of the octet SHALL contain the Conn ID as defined in Table 4. The four most significant bits are RFU.

CORE_CONN_CLOSE_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

To close a Logical Connection, the DH sends the CORE_CONN_CLOSE_CMD to the NFCC indicating the Conn ID to be closed.

On receiving a CORE_CONN_CLOSE_CMD for an existing connection, the NFCC SHALL accept the connection closure request by sending a CORE_CONN_CLOSE_RSP with a Status of STATUS_OK, and the Logical Connection is closed.

If there is no connection associated to the Conn ID in the CORE_CONN_CLOSE_CMD, the NFCC SHALL reject the connection closure request by sending a CORE_CONN_CLOSE_RSP with a Status of STATUS_REJECTED. When a DH receives this status, it SHOULD assume that the Conn ID is unknown, and therefore the connection no longer exists on the NFCC and SHOULD proceed as in a normal closing.

The DH SHOULD make sure that the last Data Message has arrived at the NFCC before sending the CORE_CONN_CLOSE_CMD. The NFCC SHOULD attempt to send any pending data to a Remote NFC Endpoint or NFCEE even though the corresponding connection is being closed.

The DH SHALL clean up all resources associated with the Conn ID after it sends the CORE_CONN_CLOSE_CMD. The NFCC SHALL clean up all resources associated with the Conn ID after receiving the CORE_CONN_CLOSE_CMD.

NOTE “Clean up all resources” means deleting all data from buffers related to the closed Logical Connection, setting *NFCC_Credits_Avail* to initial value, and releasing the Conn ID for later use.

4.4.4 Connection Credit Management

These Control Messages are used to manage the credits on a Logical Connection that uses credit-based flow control.

Table 18: Control Messages for Connection Credit Management

CORE_CONN_CREDITS_NTF				
Payload Field(s)	**Length**	**Value/Description**		
Number of Entries	1 Octet	Number of Entry fields to follow (n).		
Entry [1..n]	2 Octet	Conn ID	1 Octet	The identifier of the Logical Connection for which credits are given. The four least significant bits of the octet SHALL contain the Conn ID as defined in Table 4. The four most significant bits are RFU.
		Credits	1 Octet	The number of credits given.

For each Logical Connection, the DH stores the initial credits value received as part of the connection setup (Initial Number of Credits parameter) in a variable, namely *NFCC_Credits_Avail*, which is used to track the number of Data Packets that can be sent to the NFCC.

NOTE If there are not enough credits to send the whole Data Message, the DH is allowed to send as many Data Packets as number of credits available.

When the DH wants to send a Data Packet on a Logical Connection and flow control is enabled, the DH SHALL check that the *NFCC_Credits_Avail* variable for that connection is greater than 0. If so, the DH SHALL reduce the *NFCC_Credits_Avail* by 1 and transfer the Data Packet over the Logical Connection. The DH SHALL NOT send any Data Packet on a connection when the corresponding *NFCC_Credits_Avail* is 0.

If the NFCC receives a Data Packet that was subject to credit-based flow control, it needs to tell the DH when the buffer is again available for use. It does this either by sending CORE_CONN_CREDITS_NTF or by setting a non-zero value into the CR field of a Data Packet that is transmitted to the DH. When the DH receives this Notification or a Data Packet with a non-zero CR field, it SHALL add the credits to variable *NFCC_Credits_Avail* for the appropriate Logical Connection(s).

The DH SHALL set the *NFCC_Credits_Avail* variable to the initial value on the following scenarios:

- A Dynamic Logical Connection is created. See Section 4.4.2.
- For the Static RF Connection, if an RF Interface Activated Notification is received. See Section 7.3.1.

4.5 Generic Error

This Notification is used to inform the DH about a generic error situation.

Table 19: Control Messages for Generic Error

CORE_GENERIC_ERROR_NTF		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

This Notification is used in error situations when the error cannot be notified using an error status in a Response Message. This Notification SHALL NOT be used to report error scenarios related to NFCEE or RF Interface communication using Logical Connections.

To notify a generic error situation, the NFCC SHALL send CORE_GENERIC_ERROR_NTF to the DH with the Status code identifying the error case.

4.6 Interface Error

These Control Messages are used to inform the DH about an RF or NFCEE Interface communication specific error situation.

Table 20: Control Messages for Interface Error

CORE_INTERFACE_ERROR_NTF		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.
Conn ID	1 Octet	The identifier of the Logical Connection where the error occurred. The four least significant bits of the octet SHALL contain the Conn ID as defined in Table 4. The four most significant bits are RFU.

This Notification is used in error situations when the error cannot be notified using an error status in a Response Message.

This Notification SHALL only be used to notify error scenarios related to NFCEE or RF Interface communication using Logical Connections.

To notify a Logical Connection or RF / NFCEE Interface specific error situation, the NFCC SHALL send CORE_INTERFACE_ERROR_NTF to the DH with the Status code identifying the error and the affected Conn ID.

5 RF Communication

Communication with a Remote NFC Endpoint is performed by the use of RF Interfaces. RF Interfaces are logical entities on the NFCC that allow the DH to use specific layers in the protocol stack implemented on the NFCC. The DH can only communicate with a Remote NFC Endpoint via an RF Interface that has been activated during the Discovery process.

Section 5.1 gives an overview about the available RF Interfaces.

Section 5.2 defines the NCI state machine for RF Communication.

Section 5.3 defines a mechanism to get information about an external RF field.

5.1 RF Interface Architecture

All data exchanged between the DH and a Remote NFC Endpoint flows through an RF Interface, designated as the "Active RF Interface".

Figure 9 shows an overview of the RF Interfaces.

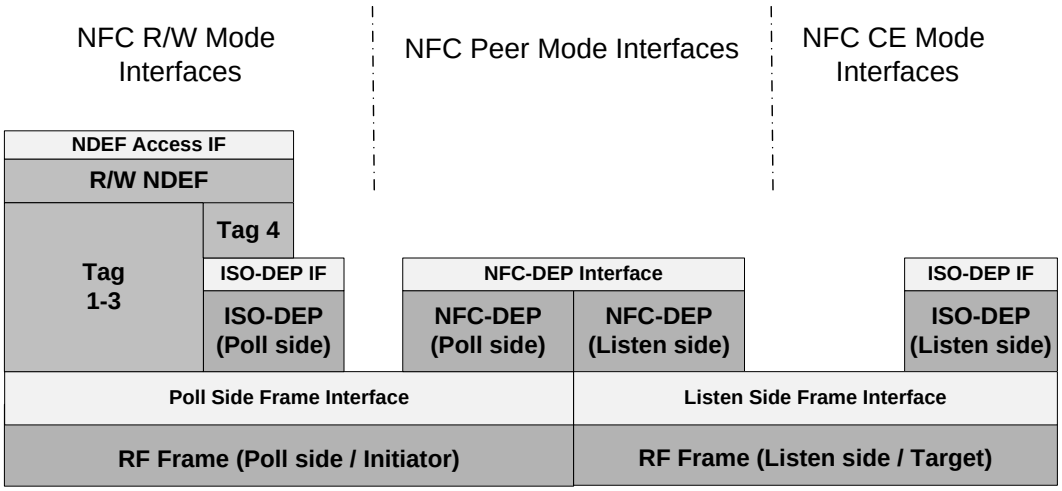

Figure 9: RF Interface Architecture

The following has to be noted:

- The ISO-DEP RF Interface is applicable for both Reader/Writer Mode and Card Emulation Mode.
- Specific to the Frame RF Interface
  - The Poll Side Frame RF Interface is applicable for both Reader/Writer Mode and the NFC-DEP Initiator side of the Peer Mode.
  - Listen Side Frame RF Interface is applicable for both Card Emulation Mode and the NFC-DEP Target side of the Peer Mode.

An RF Interface is automatically activated by the NFCC in the following cases:

- When in Poll Mode, a single Remote NFC Endpoint supporting a single protocol has been discovered.
- In Listen Mode the NFCC has been discovered/selected by a Remote NFC Endpoint.

In both cases the RF Interface to activate is determined by the current mapping between RF Protocols and RF Interfaces that can be configured using the RF_DISCOVER_MAP_CMD Command defined in Section 6.2.

If, in Poll Mode, multiple Remote NFC Endpoints or a Remote NFC Endpoint supporting more than one RF Protocol have been discovered, the DH has to select a Remote NFC Endpoint and RF Protocol using the RF_DISCOVER_SELECT_CMD Command. After receipt of this Command, the NFCC activates the RF Interface specified in the RF_DISCOVER_SELECT_CMD Command.

The activation of an RF Interface depends on the Mode:

- For Poll Mode one Remote NFC Endpoint is selected (if only one Remote NFC Endpoint is detected, it is selected automatically by the NFCC) and, depending on the RF Interface to activate, the NFCC might need to first establish one or more lower-level protocol(s) before activating an RF interface. The NFCC might even have to start exchanging some data (for instance, to check if the remote NFC Endpoint stores NDEF-compliant data) before activating the RF Interface.
- For Listen Mode the NFCC might only have to be detected/selected by a Remote NFC Endpoint before activating the RF interface. Or, it might need to first wait for the Remote NFC Endpoint to establish one or more lower-level protocol(s).

Section 8 describes dependencies and explains how the RF Interfaces are used.

5.2 State Machine

The NCI process for RF Communication is described using the RF Communication State Machine shown in Figure 10.

The DH or NFCC MAY implement the state machine explicitly. However all DH and NFCC implementations SHALL follow NCI behavior exactly *as if* they had implemented the state machine.

Each transition from one state to another is accompanied by an appropriate NCI Command, Response, or Notification, so both the DH and NFCC can always unambiguously know the current state.

The following Control Messages SHALL NOT be sent unless permitted by the rules of the state machine:

- RF_DISCOVER_CMD, RF_DISCOVER_RSP, RF_DISCOVER_NTF
- RF_DISCOVER_SELECT_CMD, RF_DISCOVER_SELECT_RSP
- RF_INTF_ACTIVATED_NTF
- RF_DEACTIVATE_CMD, RF_DEACTIVATE_RSP, RF_DEACTIVATE_NTF
- CORE_INTERFACE_ERROR_NTF with a Conn ID of a Logical Connection that is used in the context of an RF Interface.

In addition, the following Control Messages, specified in the corresponding sections, can only be sent in certain states:

- RF_NFCEE_ACTION_NTF (see Section 7.6)
- RF_PARAMETER_UPDATE_CMD/RSP (see Section 8.2.2.1)
- RF_T3T_POLLING_CMD/RSP/NTF (see Section 8.2.2.2).

If the NFCC or DH receives a Control Message in a state where that Control Message is not allowed, it SHALL treat this as a semantic error, as defined in 3.2.2.

Other Commands, Responses, and Notifications that are not explicitly forbidden by this specification MAY be exchanged in any state.

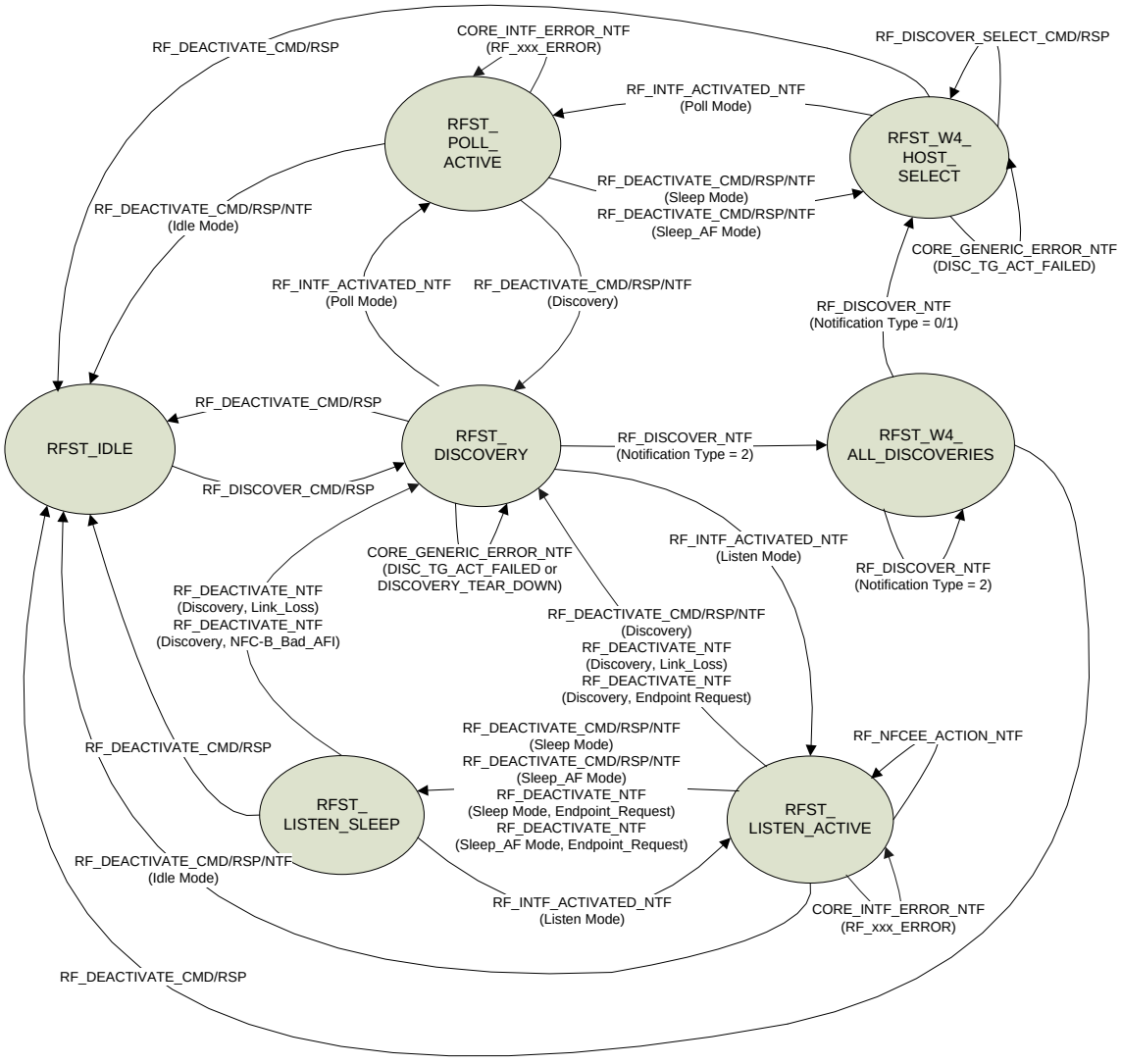

Figure 10: RF Communication State Machine

Upon successful DH and NFCC initialization (see Section 4.2), the RF Communication State Machine SHALL be in **RFST_IDLE** state. Before the first transition out of the **RFST_IDLE** state, the DH SHALL set its RF Communication Configuration as specified in Section 6.

For Poll Mode, the RF Communication State Machine relates to the Activities defined in [ACTIVITY] in the following way:

- Technology Detection is handled in **RFST_DISCOVERY** and **RFST_W4_ALL_DISCOVERIES.**
- Collision Resolution is handled in **RFST_DISCOVERY** and **RFST_W4_ ALL_DISCOVERIES.**
- Device Activation is handled in **RFST_DISCOVERY**, **RFST_W4_ALL_DISCOVERIES**, and **RFST_W4_HOST_SELECT**, depending on the number of Remote NFC Endpoints discovered and the RF Interface mapping. Depending on the RF Interface, part of the Device Activation Activity is handled by the DH in **RFST_POLL_ACTIVE**.
- RF Data Exchange is handled in state **RFST_POLL_ACTIVE**
- Depending on the RF Interface, the Device Deactivation Activity is fully handled by the NFCC or split between the DH and the NFCC. The DH is responsible for handling its part in **RFST_POLL_ACTIVE**. The NFCC handles Device Deactivation when moving from state **RFST_POLL_ACTIVE** to either **RFST_DISCOVERY, RFST_IDLE**, or **RFST_W4_HOST_SELECT**.

The Listen Mode state machine defined in [ACTIVITY] is handled in states **RFST_DISCOVERY**, **RFST_LISTEN_ACTIVE**, and **RFST_LISTEN_SLEEP**. The IDLE state defined in [ACTIVITY] is hosted inside the **RFST_DISCOVERY** NCI state.

5.2.1 State RFST_IDLE

Unless otherwise specified, discovery related configuration defined in Sections 6.1, 6.2, 6.3 and 7.1 SHALL only be set while in this state.

NOTE Although CORE_SET_CONFIG_CMD can be sent in any state, parameters that relate to RF Discovery are only included in state **RFST_IDLE**.

The NFCC SHALL turn the RF field OFF in this state. The greedy collection [ACTIVITY] is cleared in this state.

When the DH issues a valid RF_DISCOVER_CMD Command and the NFCC returns RF_DISCOVER_RSP with status STATUS_OK, the state is changed to **RFST_DISCOVERY**.

5.2.2 State RFST_DISCOVERY

In this state, the NFCC stays in Poll Mode and/or Listen Mode (based on the discovery configuration) until at least one Remote NFC Endpoint is detected or the RF Discovery Process is stopped by the DH.

The parameters and duty cycle for Poll Mode and Listen Mode are as configured by the DH.

The NFCC is expected to start filling up the greedy collection [ACTIVITY] in this state.

If discovered by a Remote NFC Endpoint in Listen mode, once the Remote NFC Endpoint has established any underlying protocol(s) needed by the configured RF Interface, the NFCC SHALL send RF_INTF_ACTIVATED_NTF (Listen Mode) to the DH and the state is changed to **RFST_LISTEN_ACTIVE**.

While polling, if the NFCC discovers more than one Remote NFC Endpoint, or a Remote NFC Endpoint that supports more than one RF Protocol, it SHALL start sending RF_DISCOVER_NTF messages to the DH. At this point, the state is changed to **RFST_W4_ALL_DISCOVERIES**.

While polling, if the NFCC discovers just one Remote NFC Endpoint that supports just one Protocol, the NFCC SHALL try to automatically activate it. The NFCC SHALL first establish any underlying protocol(s) with the Remote NFC Endpoint that are needed by the configured RF Interface. On completion, the NFCC SHALL activate the RF Interface and send RF_INTF_ACTIVATED_NTF (Poll Mode) to the DH. At this point, the state is changed to **RFST_POLL_ACTIVE**. If the protocol activation is not successful, the NFCC SHALL send CORE_GENERIC_ERROR_NTF to the DH with status DISCOVERY_TARGET_ACTIVATION_FAILED and stay in **RFST_DISCOVERY**.

In this state, the NFCC MAY detect a command during the RF communication, which forces it to come back to the IDLE state, as defined in the [ACTIVITY] Listen Mode state machine. If the RF Protocol deactivation is completed, the NFCC SHALL send CORE_GENERIC_ERROR_NTF (DISCOVERY_TEAR_DOWN), and the state will remain **RFST_DISCOVERY**.

NOTE RF Protocol deactivation while in state **RFST_DISCOVERY** can happen if during protocol activation in Listen Mode, a teardown command is received (e.g., an NFC-DEP RLS_REQ when waiting for a potential PSL_REQ).

If the DH sends RF_DEACTIVATE_CMD, the NFCC SHALL ignore the Deactivation Type parameter, stop the RF Discovery Process, and send RF_DEACTIVATE_RSP. The state will then change to **RFST_IDLE**.

5.2.3 State RFST_W4_ALL_DISCOVERIES

In this state, the NFCC has discovered more than one Remote NFC Endpoint or a Remote NFC Endpoint that supports more than one RF Protocol, while polling.

The NFCC SHOULD stay in Poll Mode while in this state.

Discover notifications with Notification Type set to 2 SHALL NOT change the state.

When the NFCC sends the last RF_DISCOVER_NTF (Notification Type not equal to 2) to the DH, the state is changed to **RFST_W4_HOST_SELECT**.

If the DH sends RF_DEACTIVATE_CMD, the NFCC SHALL ignore the Deactivation Type parameter, stop the RF Discovery Process and send RF_DEACTIVATE_RSP. The state will then change to **RFST_IDLE**.

5.2.4 State RFST_W4_HOST_SELECT

The NFCC SHOULD stay in Poll Mode while in this state.

In this state the NFCC has its greedy collection intact and is waiting for the DH to select one of the Remote NFC Endpoints from the greedy collection [ACTIVITY] to activate. The greedy collection [ACTIVITY] might contain Remote NFC Endpoints that are in sleep state.

NOTE If the T3T protocol is used, there is no action on RF required to activate a Remote NFC Endpoint.

When the DH sends RF_DISCOVER_SELECT_CMD with a valid RF Discovery ID, RF Protocol and RF Interface, the NFCC SHALL try to activate the associated Remote NFC Endpoint (depending on the state of the Remote NFC Endpoint). The NFCC SHALL first establish any underlying protocol(s) with the Remote NFC Endpoint that are needed by the configured RF Interface. On completion, the NFCC SHALL activate the RF Interface and send RF_INTF_ACTIVATED_NTF (Poll Mode) to the DH. At this point, the state is changed to **RFST_POLL_ACTIVE**.

If the activation was not successful, the NFCC SHALL send CORE_GENERIC_ERROR_NTF to the DH with a Status of DISCOVERY_TARGET_ACTIVATION_FAILED and the state will remain as **RFST_W4_HOST_SELECT**.

If the DH sends RF_DEACTIVATE_CMD, the NFCC SHALL ignore the Deactivation Type parameter, stop the RF Discovery Process and send RF_DEACTIVATE_RSP. The state will then change to **RFST_IDLE**.

5.2.5 State RFST_POLL_ACTIVE

In this state the NFCC device is activated in Poll Mode.

The NFCC SHALL stay in Poll Mode while in this state.

In this state an RF Interface is activated, which allows the NFCC to communicate with a Remote NFC Endpoint. The NFCC SHALL accept and send Data Messages to or from the DH as specified by the active RF Interface. Even if a failure occurs during Data Exchange as defined in the relevant RF Interface section, the state will remain **RFST_POLL_ACTIVE**.

In this state the DH MAY send RF_DEACTIVATE_CMD (Sleep Mode or Sleep_AF Mode) to deactivate communication with the Remote NFC Endpoint. The NFCC SHALL send RF_DEACTIVATE_RSP with STATUS_OK. Depending on the activated interface and protocol, the NFCC might issue RF commands to put the Remote NFC Endpoint into sleep state. If there was an error in executing the protocol deactivation procedures defined by the RF Interface, the NFCC SHALL notify the DH by sending RF_DEACTIVATE_NTF (Sleep Mode or Sleep_AF Mode, DH request failed due to error), and the state will remain **RFST_POLL_ACTIVE**. Otherwise, the NFCC internally marks the state of that particular RF Discovery ID device as “sleeping”, and SHALL send RF_DEACTIVATE_NTF (Sleep Mode or Sleep_AF Mode, DH Request). The state will then change to **RFST_W4_HOST_SELECT**.

In this state the DH MAY send RF_DEACTIVATE_CMD (Idle Mode) to deactivate communication with the Remote NFC Endpoint and stop RF Discovery. The NFCC SHALL send RF_DEACTIVATE_RSP with STATUS_OK and, depending on the activated interface and protocol, might issue RF commands to deactivate the Remote NFC Endpoint. If there was an error in executing the protocol deactivation procedures defined by the RF Interface, the NFCC SHALL notify the DH by sending RF_DEACTIVATE_NTF (Idle Mode, DH request failed due to error). Otherwise the NFCC SHALL send RF_DEACTIVATE_NTF (Idle Mode, DH Request). In either case, the state will change to **RFST_IDLE**.

In this state the DH MAY send RF_DEACTIVATE_CMD (Discovery) to deactivate communication with the Remote NFC Endpoint and restart RF Discovery. The NFCC SHALL send RF_DEACTIVATE_RSP with STATUS_OK and depending on the activated interface and protocol, might need to issue RF commands to deactivate the Remote NFC Endpoint. If there was an error in executing the protocol deactivation procedures defined by the RF Interface, the NFCC SHALL notify the DH sending RF_DEACTIVATE_NTF (Discovery, DH request with error). Otherwise the NFCC SHALL send RF_DEACTIVATE_NTF (Discovery, DH Request). In either case, the state will change to **RFST_DISCOVERY**.

5.2.6 State RFST_LISTEN_ACTIVE

In this state the NFCC is activated in Listen Mode.

In this state an RF Interface is activated, which allows the NFCC to communicate with a Remote NFC Endpoint, as specified by the active RF Interface. The NFCC SHALL accept and send Data Messages to or from the DH or NFCEE based on the routing tables.

NOTE By configuring the NFCC to send RF_NFCEE_ACTION_NTF notifications, the DH will be informed if a decision is made by the NFCC based on the routing algorithm to route to a different NFCEE (see Section 7.5). The local routing destination can change when using AID based routing (see Section 6.3.1) if the Remote NFC Endpoint selects an AID for which the corresponding application is hosted on a different NFCEE than the one previously selected. Routing can also change when using System Code based routing, or if the NFC Forum Device appears to the Remote NFC Endpoint as not one but multiple endpoints and the Remote NFC Endpoint switches communication between these endpoints.

In this state the NFCC MAY be put to sleep mode by the DH sending RF_DEACTIVATE_CMD (Sleep Mode or Sleep_AF Mode) (e.g., if ISO-DEP or NFC-DEP implementation on the DH use Frame RF Interface) or by the Remote NFC Endpoint. If the deactivation to sleep is successful, the NFCC SHALL send an RF_DEACTIVATE_NTF (Sleep Mode or Sleep_AF Mode, DH Request, or Endpoint Request) to the DH. The state will then change to **RFST_LISTEN_SLEEP**.

If the DH sends an RF_DEACTIVATE_CMD (Idle Mode), the NFCC SHALL send an RF_DEACTIVATE_RSP followed by an RF_DEACTIVATE_NTF (Idle, DH Request) upon successful deactivation. The state will then change to **RFST_IDLE**.

If the NFC Forum Device exits Listen Mode according to the rules defined in [ACTIVITY], the NFCC SHALL send an RF_DEACTIVATE_NTF (Discovery, RF Link Loss) to the DH. The state will then change to **RFST_DISCOVERY.**

When the Frame RF Interface is being used and the DH detects (during the RF communication) a command or an error that forces it to return to the IDLE state (as defined in the [ACTIVITY] Listen Mode state machine), the DH SHALL send an RF_DEACTIVATE_CMD (Discovery) to the NFCC. The NFCC SHALL then answer by sending an RF_DEACTIVATE_RSP followed by an RF_DEACTIVATE_NTF (Discovery, DH Request). The state will then change to **RFST_DISCOVERY.**

When the NFC-DEP RF interface is being used and the NFCC (during the RF communication) detects a RLS_REQ command that forces it to return to the IDLE state (as defined in the [ACTIVITY] Listen Mode state machine), the NFCC SHALL send an RF_DEACTIVATE_NTF (Discovery, Endpoint_Request) to the DH. The state will then change to **RFST_DISCOVERY**.

When the Frame RF Interface is being used and the NFCC determines that the Remote NFC Endpoint has switched to a different RF Protocol that requires a different RF Interface, the NFCC SHALL first send an RF_DEACTIVATE_NTF (Discovery, Endpoint Request).

NOTE For example, a change from Frame RF Interface to NFC-DEP RF Interface or ISO-DEP RF Interface can occur if the NFCC receives a valid ATR_REQ or RATS command while it still is in either ACTIVE_A, ACTIVE_A*, or READY_F state of the Listen Mode state machine (defined in [ACTIVITY]) . In this case none of the frames received after the activation of the Frame RF Interface has triggered a response and therefore a transition to another state.

Even if a failure occurs during Data Exchange (as defined in the relevant RF Interface section), the state will remain **RFST_LISTEN_ACTIVE**.

5.2.7 State RFST_LISTEN_SLEEP

In this state the NFCC is not supposed to respond to any RF commands until it receives a valid RF wake up command such as ALL_REQ, ALLB_REQ,SENSF_REQ or CUP (for details see [ACTIVITY] and [DIGITAL]).

If the NFCC receives a valid RF wake up command(s) followed by successful activation procedure, the NFCC SHALL send RF_INTF_ACTIVATED_NTF (Listen mode) to the DH. At that point, the state is changed back to **RFST_LISTEN_ACTIVE**.

If the NFC Forum Device exits Listen Mode according to the rules defined in [ACTIVITY], the NFCC SHALL send RF_DEACTIVATE_NTF (Discovery, RF Link Loss) to the DH. The state will then change to **RFST_DISCOVERY.**

For NFC-B Technology, when the NFCC detects a command during the RF communication, which forces returning to the IDLE state, as defined in the [ACTIVITY] Listen Mode state machine, the NFCC SHALL send an RF_DEACTIVATE_NTF (Discovery, NFC-B_Bad_AFI) to the DH. The state will then change to **RFST_DISCOVERY**.

If the DH sends an RF_DEACTIVATE_CMD (Idle Mode), the NFCC SHALL send an RF_DEACTIVATE_RSP. The state will then change to **RFST_IDLE**.

5.3 RF Field Information

This Notification is used to inform the DH about operating fields generated by Remote NFC Endpoints.

Table 21: Notification for RF Field information

RF_FIELD_INFO_NTF		
Payload Field(s)	**Length**	**Value/Description**
RF Field Status	1 Octet	See Table 22.

Table 22: RF Field Status

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	0	0	0	0	0	0	0		RFU
								X	1b: Operating field generated by Remote NFC Endpoint 0b: No Operating field generated by Remote NFC Endpoint.

The DH can configure whether the NFCC is allowed to send RF Field Information Notifications by setting the RF Field Information Configuration parameter specified in Table 23.

Table 23: RF Field Information Configuration Parameter

ID	Length	Value	Description
RF_FIELD_INFO	1 Octet	0x00 (default)	The NFCC is not allowed to send RF Field Information Notifications to the DH.
		0x01	The NFCC is allowed to send RF Field Information Notifications to the DH.
		0x02-0xFF	RFU

The NFCC SHALL send RF_FIELD_INFO_NTF immediately if the DH sends CORE_SET_CONFIG_CMD with RF_FIELD_INFO equal to 0x01. This allows the DH to retrieve the current RF field status. In states in which the NFCC does not sense the Operating Field it SHALL send an RF_FIELD_INFO_NTF with RF Field Status equal to 0x00.

If RF_FIELD_INFO is equal to 0x01 and the NFCC is either in state RFST_DISCOVERY, RFST_LISTEN_ACTIVE or RFST_LISTEN_SLEEP, the following rules apply:

- If an operating field from a Remote NFC Endpoint has been detected (bit 0 of RF Field Status is equal to 1b) and if not specified otherwise by the Transport Mapping that is employed, the NFCC SHALL send RF_FIELD_INFO_NTF.

  Transport Mappings MAY restrict the sending of RF_FIELD_INFO_NTF if the transport requires time to become operational after detecting an external field and if the DH can use the start of this transport activation as an indication of the presence of an external field. Transport Mappings SHALL NOT restrict the sending of RF_FIELD_INFO_NTF for any other reason.

- While Passive Communication Mode is being used, if the loss of an operating field from a Remote NFC Endpoint has been detected (bit 0 of RF Field Status is equal to 0b), the NFCC SHALL send RF_FIELD_INFO_NTF.

- While Active Communication Mode is being used, RF_FIELD_INFO_NTF SHALL only be sent if, after the operating field has been turned off by the local device, the Remote NFC Endpoint fails to establish an operating field within the corresponding timeframe (as specified in [ACTIVITY]).

If RF_FIELD_INFO is equal to 0x00, the NFCC SHALL NOT send RF_FIELD_INFO_NTF notifications.

6 RF Communication Configuration

Before it starts the RF Discovery Process by moving to the **RFST_DISCOVERY** state described in Section 5.2, the DH SHALL have first configured:

- Any non-default Poll Mode and Listen Mode parameters
- The mapping between protocols and interfaces
- Any Listen Mode routing that is needed.

The above steps need to be followed before the first time the RF Discovery Process is started, and, after that, only when something changes. They are described in detail in the following sections.

6.1 Configuration Parameters

These are configuration parameters related to discovery. The Commands used to set and get these parameters are specified in Section 4.3.

The subsections below describe all configurable RF Discovery parameters.

Table 138 contains a list of all parameters with their Parameter Tags. All parameters have default values, so the DH is not required to configure any RF Discovery parameter.

Also, some parameters are relevant only for either Listen or Poll Mode or only to specific RF Interface(s). These parameters are described in the corresponding RF Interface sections.

If the DH has changed any parameter, the DH MAY reset the parameter back to its default value by sending a CORE_SET_CONFIG_CMD with a Parameter field containing the ID of the parameter, a length of 0x00, and no value field.

In the particular case of the NFCC combining configuration parameters from the DH and some NFCEEs (as reported in CORE_INIT_RSP; see Table 10), the NFCC MAY modify the configuration parameters set by the DH before they are visible on the RF or read back by the DH. The means of modification is out of the scope of this document.

In the particular case of the NFCC supporting the RF Configuration in the Switched Off State (as reported in CORE_INIT_RSP; see Table 11), the DH SHALL set an additional POWER_STATE parameter as the first parameter of CORE_SET_CONFIG_CMD to define that the provided configuration parameters of this command applies only for the Switched Off State. To read the configuration parameters for Switched Off State, the DH SHALL set the Parameter ID of the POWER_STATE parameter as the first Parameter ID of the CORE_GET_CONFIG_CMD. If the requested configuration parameters for the Switched Off State were configured before, the NFCC supporting the RF Configuration in Switched Off State SHALL respond with CORE_GET_CONFIG_RSP containing the POWER_STATE parameter followed by the requested configuration parameters for the Switched Off State. Otherwise, the NFCC SHALL response with CORE_GET_CONFIG_RSP containing the POWER_STATE parameter followed by configuration parameter containing no value field (length of 0x00). To delete the configuration parameters for Switched Off State, the DH SHALL send a CORE_SET_CONFIG_CMD containing the POWER_STATE parameter followed by configuration parameters containing no value field (length of 0x00).The POWER_STATE parameter is only supported in conjunction with the following configuration parameters:

- Listen A Parameters according to Table 33
- Listen B Parameters according to Table 35

- Listen ISO-DEP Parameters according to Table 42.

The DH SHALL NOT set the POWER_STATE parameter in CORE_SET_CONFIG_CMD and CONFIG_GET_CONFIG_CMD with other configuration parameters than listed above. If other configuration parameters are received together with the POWER_STATE parameter, the NFCC supporting RF Configuration in Switched Off State SHALL respond with STATUS_INVALID_PARAM containing the invalid configuration parameters in the Parameter ID field.

The DH SHALL NOT set the POWER_STATE parameter in CORE_SET_CONFIG_CMD and CORE_GET_CONFIG_CMD when the NFCC has not indicated the support of RF Configuration in Switched Off State in the CORE_INIT_RSP. The NFCC not supporting RF Configuration in Switched Off State will ignore the POWER_STATE parameter and will manage the configuration parameters for Switched On State instead.

While operating in Switched Off State, the NFCC supporting the RF Configuration in Switched Off State SHALL use the configuration parameters received together with the POWER_STATE parameter, and if the NFCC supports the merging of RF configuration and the NFCC is allowed to manage the RF configuration, the NFCC MAY merge the provided RF configuration with the RF configurations received from NFCEEs.

The NFCC, which supports Switched Off State but not the RF Configuration in Switched Off State, MAY use different configuration parameters when operating in Switched Off state. The configuration parameters used in Switched-Off state are implementation specific, thus out-of-scope of this specification.

NOTE The NFCC can use configuration parameters directly received from connected NFCEEs while operating in Switched Off State.

The NFCC supporting Battery Off State MAY use different configuration parameters when operating in Battery-Off State. The configuration parameters used in Battery Off state are implementation specific, thus out-of-scope of this specification.

NOTE The NFCC can use configuration parameters directly received from connected NFCEEs while operating in Battery Off State.

If the DH retrieves a Parameter whose current value is decided by the NFCC, the NFCC SHALL send the actual value of the parameter, as set by the NFCC.

6.1.1 Poll A Parameters

Table 24: Discovery Configuration Parameters for Poll A

ID	Length	Value	Description
PA_BAIL_OUT	1 Octet	0x00 (default)	No bail out during Poll Mode in Discovery activity (as defined in [ACTIVITY]).
		0x01	Bail out when NFC-A Technology has been detected during Poll Mode in Discovery activity (as defined in [ACTIVITY]).
		0x02-0xFF	RFU
PA_DEVICES_LIMIT	1 Octet	variable	As defined in [ACTIVITY] for the Collision Resolution Activity. Default: NFCC decides (based on its capabilities).

6.1.2 Poll B Parameters

Table 25: Discovery Configuration Parameters for Poll B

ID	Length	Value	Description
PB_AFI	1 Octet	variable	Application family identifier (as defined in [DIGITAL]). Default: 0x00 (all application families) [DIGITAL] mandates a value of 0x00.
PB_BAIL_OUT	1 Octet	0x00 (default)	No bail out during Poll Mode in Discovery activity (as defined in [ACTIVITY]).
		0x01	Bail out when NFC-B Technology has been detected during Poll Mode in Discovery activity (as defined in [ACTIVITY]).
		0x02-0xFF	RFU
PB_ATTRIB_PARAM1	1 Octet	variable	The values and coding of this parameter SHALL be as defined in [DIGITAL] for Param 1 of the ATTRIB command. There is no default because this is a read only parameter.

			The DH SHALL NOT attempt to write this parameter
PB_SENSB_REQ_PARAM	1 Octet	variable	Control of what is sent in the PARAM byte of an ALLB_REQ or SENSB_REQ (as defined in [DIGITAL]). See Table 26 Default: 0x00
PB_DEVICES_LIMIT	1 Octet	variable	As defined in [ACTIVITY] for the Collision Resolution Activity. Default: NFCC decides (based on its capabilities).

NOTE The information provided by PB_ATTRIB_PARAM1 can be used by the DH to construct a valid ATTRIB command when using the Frame RF Interface or the Aggregated Frame RF Interface.

Table 26: Values for PB_SENSB_REQ_PARAM

	Bit Mask								**Description**
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	0	0	0						RFU
				X					If set to 1b, the NFCC SHALL indicate support for extended SENSB_RES in an ALLB_REQ or SENSB_REQ. Otherwise it SHALL NOT indicate support.
					0	0	0	0	The NFCC MAY set these bits independently of what is set by the DH. The DH SHOULD NOT attempt to interpret the value set by the NFCC.

6.1.3 Poll F Parameters

Table 27: Discovery Configuration Parameters for Poll F

ID	Length	Value	Description
PF_BIT_RATE	1 Octet	1 – 2	The initial bit rate for Passive Communication Mode. For value coding see Table 132. Default: 0x01
PF_BAIL_OUT	1 Octet	0x00 (default)	No bail out during Poll Mode in Discovery activity (as defined in [ACTIVITY]).
		0x01	Bail out when NFC-F Technology has been detected during Poll Mode in Discovery activity (as defined in [ACTIVITY]).
		0x02-0xFF	RFU
PF_DEVICES_LIMIT	1 Octet	variable	As defined in [ACTIVITY] for the Collision Resolution Activity. Default: NFCC decides (based on its capabilities).

6.1.4 Poll ISO-DEP Parameters

Table 28: Discovery Configuration Parameters for ISO-DEP

ID	Length	Value	Description
PI_B_H_INFO	0-15 Octets		Higher layer INF field of the ATTRIB Command (as defined in [DIGITAL]). Default: empty (NFCC will send ATTRIB Command without Higher Layer – INF field).
PI_BIT_RATE	1 Octet	0-3	Maximum allowed bit rate Default: 0x00 (106 Kbit/s) For value coding see Table 132. Depending on the capabilities of NFCC, the NFCC MAY adjust a lower bit rate than specified by this field even if a higher bit rate would be supported by the Remote NFC Endpoint.

6.1.5 Poll NFC-DEP Parameters

Those parameters MAY be configured if polling for NFC-A and/or NFC-F or P2P-Active.

Table 29: Discovery Configuration Parameters for Poll NFC-DEP

ID	Length	Value	Description
PN_NFC_DEP_PSL	1 Octet	0x00 (Default)	Highest available Bit Rates and highest available Length Reduction. The NFCC is responsible for determining the highest Bit Rates available and the highest LR available, and SHALL use them for Data Exchange. If necessary, a PSL_REQ will be sent by the NFCC to change the BRS and consequently the LR.
		0x01	Maintain the Bit Rates and LR. The NFCC SHALL use the same Bit Rates and LR for Data Exchange as were used for Device Activation. This means that a PSL_REQ is not sent by the NFCC.
		0x02-0xFF	RFU
PN_ATR_REQ_GEN_BYTES	0-n Octets		General Bytes for ATR_REQ. Default: empty (no General Bytes SHALL be sent in ATR_REQ).
PN_ATR_REQ_CONFIG	1 Octet		Configuration to be used in the Optional Parameters (**PP**$_l$) within ATR_REQ. See Table 30. Default: 0x30

Table 30: Values for PN_ATR_REQ_CONFIG

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	0	0			0	0	0	0	RFU
			X	X					Value for $\mathbf{LR}_I$ (as defined in [DIGITAL]) NOTE Needs to be always set to 11b for LLCP

6.1.6 Poll Active Parameters

Table 31: Poll Mode Discovery Configuration Parameters for Active Mode

ID	Length	Value	Description
PACM_BIT_RATE	1 Octet	Variable	The initial bit rate for Active Communication Mode. For value coding see Table 132. Default: 0x01.

6.1.7 Poll V Parameters

Table 32: Discovery Configuration Parameters for Poll V

ID	Length	Value	Description
PV_DEVICES_LIMIT	1 Octet	variable	As defined in [ACTIVITY] for the Collision Resolution Activity. Default: NFCC decides (based on its capabilities).

6.1.8 Listen A Parameters

Table 33: Discovery Configuration Parameters for Listen A

ID	Length	Description
LA_BIT_FRAME_SDD	1 Octet	Bit Frame SDD value to be sent in Byte 1 of SENS_RES. This is a 5-bit value that SHALL be contained in the 5 least significant bits of the octet. Default: NFCC decides (the NFCC SHALL set the value as defined in [DIGITAL]).
LA_PLATFORM_CONFIG	1 Octet	Platform Configuration value to be sent in Byte 2 of SENS_RES. This is a 4-bit value that SHALL be contained in the 4 least significant bits of the octet. Default: NFCC decides (the NFCC SHALL set the value as defined in [DIGITAL]).
LA_SEL_INFO	1 Octet	This value is used to generate SEL_RES (as defined in [DIGITAL]). Bits set in this field SHALL be set in the SEL_RES sent by the NFCC. See Table 34. Default: NFCC decides (the NFCC SHALL set the default value corresponding to the RF Interfaces implemented on the NFCC).
LA_NFCID1	4, 7, or 10 Octets	NFCID1 as defined in [DIGITAL]. As specified in [DIGITAL], in case of a single size NFCID1 (4 Bytes), a value of $nfcid1_0$ set to 08h indicates that $nfcid1_1$ to $nfcid1_3$ SHALL be dynamically generated. In such a situation the NFCC SHALL ignore the $nfcid1_1$ to $nfcid1_3$ values and generate them dynamically. Otherwise NFCC SHALL use the NFCID1 provided. Default: NFCC dynamically generates a single size NFCID1 (4 Bytes) (as defned in [DIGITAL]).

Table 34: LA_SEL_INFO coding

	Bit Mask	Description

	b7	b6	b5	b4	b3	b2	b1	b0	
Octet 0	X			X	X		X	X	For proprietary use
						0			The NFCC MAY set these bits independently of what is set by the DH. The DH SHOULD NOT attempt to interpret the value set by the NFCC.
		X							If set to 1b, NFC-DEP Protocol is supported by the NFC Forum Device in Listen Mode. Otherwise it is not supported.
			X						If set to 1b, ISO-DEP Protocol is supported by the NFC Forum Device in Listen Mode. Otherwise it is not supported.

6.1.9 Listen B Parameters

Table 35: Discovery Configuration Parameters for Listen B

ID	Length	Description
LB_SENSB_INFO	1 Octet	Byte 2 of Protocol Info within SENSB_RES, as defined in [DIGITAL]. See Table 36. Default: NFCC decides. The NFCC SHALL set the default value corresponding to the protocols implemented on the NFCC.
LB_NFCID0	4 Octets	NFCID0, as defined in [DIGITAL]. Default: NFCC dynamically generates the NFCID0 (as defined in [DIGITAL]).
LB_APPLICATION_DATA	4 Octets	Application Data (Bytes 6-9) of SENSB_RES (as defined in [DIGITAL]). Default: All octets are set to 0x00.
LB_SFGI	1 Octet	Start-Up Frame Guard Time, as defined in [DIGITAL]. Default: NFCC decides.
LB_FWI_ADC_FO	1 Octet	Byte 3 of Protocol Info within SENSB_RES (as defined in [DIGITAL]). See Table 37. Default: NFCC decides.
LB_BIT_RATE	1 Octet	Maximum supported bit rate for NFC-B. Default: 0x00 (106 Kbit/s) For value coding see Table 132. Depending on the capabilities of NFCC, the NFCC MAY reduce the maximum supported bit rate reported to the RF reader.

Table 36: LB_SENSB_INFO values

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	0	0	0	0	0	0	0		The NFCC MAY set these bits independently of what is set by the DH. The DH SHOULD NOT attempt to interpret the value set by the NFCC.
								X	If set to 1b, ISO-DEP Protocol is supported by the NFC Forum Device in Listen Mode. Otherwise it is not supported.

Table 37: LB_FWI_ADC_FO values

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0					0		0		The NFCC MAY set these bits independently of what is set by the DH. The DH SHOULD NOT attempt to interpret the value set by the NFCC.
	X	X	X	X					Frame Waiting time Integer for NFC-B as defined in [DIGITAL]
						X			b3 of ADC Coding field of SENSB_RES (Byte 12) as defined in [DIGITAL]
								X	If set to 1b DID MAY be used. Otherwise it SHALL NOT be used.

6.1.10 Listen F Parameters

The NFC-F listen configuration supports the configuration for the NFC-DEP Target functionality by the DH.

Using the configuration for the NFC-DEP functionality, the DH can provide the information required by the Listen Mode state machine described in [ACTIVITY] for moving from the IDLE state to the READY_F State. The NFC-DEP configuration SHALL be used by the NFCC for this purpose.

If the DH is interested in NFC-DEP based communication it SHALL set the b1 of LF_PROTOCOL_TYPE to 1, which will enable the generation of SENSF_RES indicating NFC-DEP capabilities as a response to a SENSF_REQ having a System Code of FFFFh. Otherwise the DH SHALL set the b1 of this field to 0.

Table 38: Discovery Configuration Parameters for Listen F

ID	Length	Description
LF_PROTOCOL_TYPE	1 Octet	Protocols supported by the NFC Forum Device in Listen Mode for NFC-F. See Table 39. Default: NFCC decides. The NFCC SHALL set the default value corresponding to the protocols implemented on the NFCC.

Table 39: Supported Protocols for Listen F

	Bit Mask								Description
	b7	b6	b5	b4	b3	b2	b1	b0	
Octet 0	0	0	0	0	0	0		0	RFU
							X		If set to 1b, NFC-DEP Protocol is supported by the NFC Forum Device in Listen Mode. Otherwise it is not supported.

6.1.11 Listen T3T Parameters

The T3T listen configuration supports the configuration for the NFC Forum Type 3 Tag Platform by the DH.

Using the configuration for the Type 3 Tag Platform, the DH can provide the information required by the Listen Mode state machine described in [ACTIVITY] for answering a SENSF_REQ Command in IDLE state or READY_F State. The Type 3 Tag Platform configuration SHALL be used by the NFCC for this purpose.

If the NFCC is allowed to merge multiple configurations (based on the Discovery Configuration Mode in CORE_INIT_RSP and CON_DISCOVERY_PARAM), the parameters for the Type 3 Tag Platform SHALL NOT be modified by this process.

The Type 3 Tag Platform configuration uses a set of parameters whose names start with LF_T3T_IDENTIFIERS_and a following number. This document refers to the trailing number as the index and uses the term LF_T3T_IDENTIFIERS without index to reference the whole parameter set.

Table 40: Discovery Configuration Parameters for Listen T3T

ID	Length	Value	Description
LF_T3T_MAX	1 Octet	0 – 16	The maximum index of LF_T3T_IDENTIFIERS supported by the NFCC. There is no default because this is a read only parameter. The DH SHALL NOT attempt to write this parameter.
		17 – 255	RFU
LF_T3T_IDENTIFIERS_1	18 Octets	For each identifier: Octet 0 and Octet 1 indicate the System Code of a Type 3 Tag Emulation occurring on the DH. Octet 2 – Octet 9 indicates NFCID2 for the Type 3 Tag Platform. Octet 10 – Octet 17 indicate PAD0, PAD1, MRTI_check, MRTI_update and PAD2 of SENSF_RES as defined in [DIGITAL] for the Type 3 Tag Platform. Default: Octet 0 and 1 SHALL be set to 0xFF. Octet 2 SHALL be set to 0x02. Octet 3 SHALL be set to 0xFE. Octets 4-9 SHALL be set to 0x00. Octets 10-17 SHALL be set to 0xFF.	
LF_T3T_IDENTIFIERS_2	18 Octets		
…			
LF_T3T_IDENTIFIERS_16	18 Octets		
LF_T3T_FLAGS	2 Octets	A bit field indicating which LF_T3T_IDENTIFIERS are enabled in the process to create a response to a SENSF_REQ. The mapping between the bits and the LF_T3T_IDENTIFIERS is defined in Table 41. Default: 0x0000.	
LF_T3T_RD_ALLOWED	1 Octet	0x00 (default)	The NFCC SHALL NOT include RD bytes in its SENSF_RES if it receives a SENSF_REQ with RC set to 0x02
		0x01	The NFCC MAY include RD bytes in its SENSF_RES if it receives a SENSF_REQ with RC set to 0x02
		0x02-0xFF	RFU

Table 41: Mapping between the bits in LF_T3T_FLAGS and LF_T3T_IDENTIFIERS

	Bit Mask								LF_T3T_IDENTIFIER
	b7	b6	b5	b4	b3	b2	b1	b0	
Octet 0								X	LF_T3T_IDENTIFIERS_1
							X		LF_T3T_IDENTIFIERS_2
						X			LF_T3T_IDENTIFIERS_3
					X				LF_T3T_IDENTIFIERS_4
				X					LF_T3T_IDENTIFIERS_5
			X						LF_T3T_IDENTIFIERS_6
		X							LF_T3T_IDENTIFIERS_7
	X								LF_T3T_IDENTIFIERS_8
Octet 1								X	LF_T3T_IDENTIFIERS_9
							X		LF_T3T_IDENTIFIERS_10
						X			LF_T3T_IDENTIFIERS_11
					X				LF_T3T_IDENTIFIERS_12
				X					LF_T3T_IDENTIFIERS_13
			X						LF_T3T_IDENTIFIERS_14
		X							LF_T3T_IDENTIFIERS_15
	X								LF_T3T_IDENTIFIERS_16

In order to generate the SENSF_RES for the Type 3 Tag Platform on the DH, the following process SHALL be performed:

Starting from LF_T3T_IDENTIFIERS_1 to the LF_T3T_IDENTIFIERS parameter with index equal to the value of LF_T3T_MAX:

- if the corresponding bit of LF_T3T_FLAGS is equal to 1 and if the System Code in the SENSF_REQ matches Octets 0 and 1 of the LF_T3T_IDENTIFIERS parameter (according to the rules defined in [ACTIVITY]), then the content of this LF_T3T_IDENTIFIERS parameter SHALL be used to generate the SENSF_RES and the process SHALL stop (as a consequence, for a single SENSF_REQ there will be at most one SENSF_RES generated for the Type 3 Tag Platform on the DH).
- otherwise, the next entry SHALL be processed.

If LF_T3T_FLAGS is equal to the default 0x0000, sending of SENSF_RES for Type 3 Tag platform is disabled.

The DH SHALL only enable an LF_T3T_IDENTIFIERS within LF_T3T_FLAGS after the DH has configured the corresponding LF_T3T_IDENTIFIERS.

NOTE For the Type 3 Tag Platform on the DH the LF_T3T_IDENTIFIERS for which the bit(s) in LF_T3T_FLAGS are set to 1 and which have an index smaller or equal than the value of LF_T3T_MAX, correspond to the CON_SYS_CODE and CON_SENSF_RES configuration parameters in [ACTIVITY].

As an exception to the rule described in Section 5.2.1, the NFCC SHALL accept modification of the LF_T3T_FLAGS parameter value in state **RFST_LISTEN_ACTIVE** as well as in state **RFST_IDLE**.

The Octets 0 and 1 of an LF_T3T_IDENTIFIERS value (representing a Type 3 Tag Platform System Code) SHALL NOT be configured to be equal to Octets 0 and 1 of any other LF_T3T_IDENTIFIERS value.

Except when setting them to their default value, the DH SHALL NOT set:

- The Octets 0 and 1 of an LF_T3T_IDENTIFIERS value (representing a Type 3 Tag Platform System Code) to be equal to Octets 0 and 1 of any other LF_T3T_IDENTIFIERS value
- The Octets 2 to 9 of an LF_T3T_IDENTIFIERS value (representing a Type 3 Tag Platform NFCID2) to be equal to Octets 2 to 9 of any other LF_T3T_IDENTIFIERS value.

NOTE The NFCC does not need to check if the LF_T3T_IDENTIFERS value set by the DH is a duplicate of any other LF_T3T_IDENTIFIERS value.

The NFCC SHALL answer by sending CORE_SET_CONFIG_RSP with a Status of STATUS_REJECTED, if the CORE_SET_CONFIG_CMD contains either:

- The parameter LF_T3T_MAX
- A parameter of type LF_T3T_IDENTIFIERS with a higher index than the value of LF_T3T_MAX.

The NFCC SHALL answer by sending CORE_GET_CONFIG_RSP with a Status of STATUS_REJECTED, if the CORE_GET_CONFIG_CMD contains:

- A parameter of type LF_T3T_IDENTIFIERS with a higher index than the value provided by LF_T3T_MAX.

NOTE If the value of LF_T3T_MAX is equal to 0, the NFCC does not support generating SENSF_RES Responses for the Type 3 Tag Platform.

6.1.12 Listen ISO-DEP Parameters

These parameters MAY be configured if listening for NFC-A or NFC-B.

Table 42: Discovery Configuration Parameters for Listen ISO-DEP

ID	Length	Description
LI_A_RATS_TB1	1 Octet	RATS Response Interface Byte TB(1) (defined in [DIGITAL]). Default: NFCC decides.
LI_A_HIST_BY	0 – n Octets	Historical Bytes (only applicable for Type 4A Tag) (defined in [DIGITAL]). Default: empty (do not send historical bytes).
LI_B_H_INFO_RESP	0 – 15 Octets	Higher Layer – Response field of the ATTRIB response (defined in [DIGITAL]). Default: empty (send ATTRIB response without Higher Layer – Response field).
LI_A_BIT_RATE	1 Octet	Maximum supported bit rate for NFC-A. Default: 0x00 (106 Kbit/s) For value coding see Table 132. Depending on the capabilities of NFCC, the NFCC MAY reduce the maximum supported bit rate reported to the RF reader.
LI_A_RATS_TC1	1 Octet	RATS Response Interface Byte TC(1)

Table 43: Values for LI_A_RATS_TC1

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	0	0	0	0	0	0		0	Will be set by the NFCC independently of what is configured by DH
							X		If set to 1b DID MAY be used. Otherwise it SHALL NOT be used.

6.1.13 Listen NFC-DEP Parameters

These parameters MAY be configured if listening for NFC-A and/or NFC-F.

Table 44: Discovery Configuration Parameters for Listen NFC-DEP

ID	Length	Description
LN_WT	1 Octet	Waiting Time defined in [DIGITAL]. Default: 10. The 4 most significant bits are RFU. NOTE The maximum allowed WT value for the target is set according to LLCP: 10.
LN_ATR_RES_GEN_BYTES	0-n Octets	General Bytes in ATR_RES (defined in [DIGITAL]). Default: empty (no General Bytes SHALL be sent in ATR_RES).
LN_ATR_RES_CONFIG	1 Octet	Used to generate the Optional parameters ($\mathbf{PP}_T$) in ATR_RES. See Table 45. Default: 0x30 (NFCC indicates a maximum payload size of 254 bytes).

Table 45: Values for LN_ATR_RES_CONFIG

	Bit Mask								Description
	b7	b6	b5	b4	b3	b2	b1	b0	
Octet 0	0	0			0	0			RFU
							0	0	The NFCC MAY set these bits independently of what is set by the DH. The DH SHOULD NOT attempt to interpret the value set by the NFCC.
			X	X					Value for $\mathbf{LR}_T$ (defined in [DIGITAL]). Default: 11b NOTE Need to be set to 11b for LLCP

6.1.14 Common Parameters

Table 46: Common Parameters for Discovery Configuration

ID	Length	Description
TOTAL_DURATION	2 Octets	0x0000 – 0xFFFF defines the Total Duration of the single discovery period in [ms]. This time definition provides only a rough target value for the NFCC, but NFCC might adjust the duration time due to the current limitation of active RF Protocols and hardware limitations. Default: NFCC decides.
CON_DISCOVERY_PARAM	1 Octet	This parameter is used to enable/disable specific operating modes. See Table 47. As an exception to the rule described in Section 5.2.1, the NFCC SHALL accept modification of this parameter value in any state. If the DH changes the value of this parameter in RFST_DISCOVERY state, the NFCC SHALL re-evaluate the RF Discovery Process based on the new value (described in Section 7.1).
POWER_STATE	1 Octet	This parameter is used to indicate that the configuration parameters of the current CORE_GET_CONFIG_CMD apply for Switched Off State. This parameter SHALL be set to 0x02. All other values are RFU.

Table 47: Values for CON_DISCOVERY_PARAM

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0			0	0	0	0			RFU
								X	If equal to 1b, Polling Mode is enabled; otherwise disabled. Default: 1b
							X		This bit only applies if the NFCC supports the Listen Mode Routing Table. If equal to 1b, the DH-NFCEE is considered as a disabled NFCEE, as defined in Section 6.3. Otherwise the DH-NFCEE is considered as enabled. Default: 0b
	X	X							For proprietary use.

6.2 RF Interface Mapping Configuration

The NFCC SHALL set the default mapping of RF Interface to RF Protocols / Modes to the following values:

- If the NFCC supports the ISO-DEP RF interface, the NFCC SHALL map the ISO-DEP RF protocol to the ISO-DEP RF Interface for Poll and Listen Modes.
- If the NFCC supports the NFC-DEP RF interface, the NFCC SHALL map the NFC-DEP RF protocol to the NFC-DEP RF Interface for Poll and Listen Modes.
- If the NFCC supports the NDEF RF interface, the NFCC SHALL map the NDEF RF protocol to the NDEF RF Interface for Poll Mode.
- Otherwise, the NFCC SHALL map to the Frame RF Interface by default.

The following Control Messages are used to configure the mapping between RF Protocols and RF Interfaces, when the DH wants to use a mapping that is different from the default.

Table 48: Control Messages for RF Interface Mapping Configuration

RF_DISCOVER_MAP_CMD				
Payload Field(s)	**Length**	**Value/Description**		
Number of Mapping Configurations	1 Octet	The number of Mapping Configuration fields to follow (n).		
Mapping Configuration [1..n]	3 Octets	RF Protocol	1 Octet	See Table 133.
		Mode	1 Octet	See Table 49.
		RF Interface	1 Octet	See Table 134. The value 0 (NFCEE Direct RF Interface) SHALL NOT be used.

RF_DISCOVER_MAP_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

Table 49: Value Field for Mode

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	0	0	0	0	0	0			RFU
							X		If equal to 1b, the RF Interface is mapped to the RF Protocol in Listen Mode. Otherwise it is not mapped.
								X	If equal to 1b, the RF Interface is mapped to the RF Protocol in Poll Mode. Otherwise it is not mapped.
	At least one of the bits b0 or b1 SHALL be set to 1b.								

A Mapping Configuration defines the RF Interface that SHALL be used for the communication from the DH to a Remote NFC Endpoint using the specified RF Protocol and Mode, when the NFCC autonomously transfers to the **RFST_POLL_ACTIVE** or **RFST_LISTEN_ACTIVE** states.

If the DH initiates the transfer to the **RFST_POLL_ACTIVE** state by sending an RF_DISCOVER_SELECT_CMD, the DH SHALL specify the interface to use as a parameter to the RF_DISCOVER_SELECT_CMD which overrules any values that might be in the RF Interface Mapping configuration.

Only one RF Interface SHALL be mapped to each RF Protocol.

To perform RF Interface mapping, the DH SHALL send a RF_DISCOVER_MAP_CMD to the NFCC.

The NFCC SHALL set the RF Interface for all RF Protocols / Modes not included in the RF_DISCOVER_MAP_CMD to the value Frame RF Interface.

If the NFCC accepts the RF Interface mapping configuration, it SHALL respond using a RF_DISCOVER_MAP_RSP with a Status of STATUS_OK.

If the RF Interface mapping is invalid, the NFCC SHALL reject the mapping configuration by sending a RF_DISCOVER_MAP_RSP with a Status of STATUS_REJECTED. In this case the DH MAY attempt an alternative configuration.

If the mapping configuration is rejected, the state of the RF Interface Mapping configuration in the NFCC SHALL be invalid. As long as the table is invalid, starting of the RF Discovery Process is not possible (see Section 6).

The DH SHALL only use RF Interface values that are supported by the NFCC. The RF Interfaces supported by the NFCC are made known to the DH in the CORE_INIT_RSP.

6.3 Listen Mode Routing Configuration

If, as part of the Discovery Process, the DH wants the NFCC to enter Listen Mode and the NFCC has indicated support for listen mode routing, the DH SHALL configure the Listen Mode Routing Table. This is required to provide the NFCC the information on where to route received data when activated in Listen Mode.

If the DH wants the NFCC in Listen Mode to bypass the Listen Mode Routing Table and force all received frames of Card Emulation applications to be routed to a specific NFCEE, and the NFCC has indicated support for Forced NFCEE Routing, the DH SHALL enable Forced NFCEE Routing. When Forced NFCEE Routing is enabled, the NFCC will determine the route for the received frames as described in Section 6.3.10. Otherwise the NFCC will determine the route by searching the Listen Mode Routing Table (described in Section 6.3.1).

If an NFCEE for which a routing entry exists becomes disabled or unresponsive, the NFCC SHALL stop the routing to that NFCEE until the NFCEE is enabled again. The corresponding routing entries SHALL be ignored for the time the NFCEE is disabled or unresponsive. Similarly, a routing entry SHALL be ignored if the received RF communication cannot be forwarded to the configured NFCEE due to a non-operational communication channel between the NFCC and the NFCEE.

NOTE The DH might need to evaluate whether to reconfigure the Listen Mode Routing Table if an NFCEE is disabled, or the DH detects that an NFCEE is physically removed, for which protocol or technology based routing entries exist that can be handled by other NFCEEs.

NOTE For NFCEEs connected by HCI to the NFCC, a communication channel can be non-operational if, for example any of the following is true:
- The whole HCI communication is inhibited.
- The corresponding pipe is not created.
- The corresponding pipe is closed.
- The corresponding RF gate was disabled.

6.3.1 Listen Mode Routing Table Design

The Listen Mode Routing Table consists of different types of routing entries. These are:

- AID-based routing entries
- APDU Pattern-based routing entries
- System Code-based routing entries
- Protocol-based routing entries
- Technology-based routing entries.

The DH knows which type(s) of routing the NFCC supports from the NFCC capabilities returned in the CORE_INIT_RSP.

AID-based routing is only possible if the NFCC terminates the ISO-DEP Protocol and understands at least the SELECT by DF name command defined in [ISO/IEC_7816-4].

NOTE Although this specification refers to AID-based routing, the routing is actually based on the DF name. For NCI routing purposes, the DF name and AID are treated the same.

APDU pattern-based routing is only possible if the NFCC terminates the ISO-DEP Protocol.

System Code-based routing entries are used during the handling of SENSF_REQ Commands in case a SENSF_RES indicating that the Type 3 Tag RF Protocol is to be returned. The routing for Type 3 Tag RF Protocol is determined during the handling of the SENSF_REQ. Each SENSF_RES is associated with one NFCEE, and therefore the route for the following Commands is determined by the SENSF_RES that is sent.

For each protocol, except for proprietary protocols, there SHALL be at most one protocol-based route configured for each supported Power State. The rules for routing entries for proprietary protocols are out-of-scope of this specification.

NOTE Transitions between Power States Switched On, Switched Off and Battery Off are implementation specific issues, thus out-of-scope of this specification.

For each technology there SHALL be at most one technology-based route configured for each supported Power State.

The order of searching through the routing table SHALL be (1) AID-based (if applicable), (2) APDU Pattern-based (if applicable), (3) System Code-based (if applicable), (4) Protocol-based and (5) Technology-based.

In the description below, the term "EE_ROUTE" refers to a variable used to contain the route. It contains one of three types of values – "unknown", "blocked" and "valid NFCEE ID".

EE_ROUTE is initialized to "unknown" on each entry to states RFST_DISCOVERY or RFST_LISTEN_SLEEP, and its value is persistent in states RFST_DISCOVERY, RFST_LISTEN_SLEEP_and RFST_LISTEN_ACTIVE with the following exception:

- The value of EE_ROUTE SHALL NOT be changed either:
  - If the transition to RFST_DISCOVERY was caused by detecting remote RF field off while using Type 3 Tag RF Protocol in RFST_LISTEN_ACTIVE
  - If remote RF field off is detected in RFST_DISCOVERY after EE_ROUTE has been set by System Code-based route selection for Type 3 Tag RF Protocol

  and if the Remote NFC Endpoint activates again the Type 3 Tag Protocol in Listen Mode by sending a CUP command (see [ACTIVITY]).
  This exception SHALL NOT apply when in Battery Off State.

NOTE This exception allows for handling temporary RF glitches or short RF off periods during a transaction using the Type 3 Tag RF Protocol.

Additionally, if the NFCC receives an ATR_REQ Command using NFC-F Technology in accordance with the Listen Mode State Machine as defined in [ACTIVITY], EE_ROUTE SHALL be set to "unknown". This allows a Reader to switch from Type 3 Tag Protocol to NFC-DEP Protocol.

For each received frame from RF that needs routing the NFCC SHALL follow the steps below (skipping steps for routing types it does not support):

1. If the Listen-side ISO-DEP RF Interface is not activated, go to Step 2.
   a) If the APDU is a SELECT command (0xA4) as defined in [ISO/IEC_7816-4] with parameter P1 set to "Select by DF name" (0x04) and the "File occurrence" field of parameter P2 set to "First or only occurrence" (00b), then set EE_ROUTE using the process in Section 6.3.5 on AID-based route selection.
   b) If EE_ROUTE is not equal to "unknown", then go to Step 6.
   c) Set EE_ROUTE using the process in Section 6.3.6 on APDU Pattern-based route selection.
   d) If EE_ROUTE is not equal to "unknown", then go to Step 6.

2. If the received frame uses NFC-F Technology, and is a SENSF_REQ Command, then handle it using the process in Section 6.3.7, which could also change EE_ROUTE and terminate the routing process.
3. If EE_ROUTE is not equal to “unknown”, then go to Step 6.
4. Set EE_ROUTE using the process in Section 6.3.8 on Protocol-based route selection. If EE_ROUTE is not equal to “unknown”, then go to Step 6.
5. Set EE_ROUTE using the process in Section 6.3.9 on Technology-based route selection.
6. Take the following actions based on the value of EE_ROUTE:
   a. **“valid NFCEE ID”**
      Route the received frame to the NFCEE with that ID.
   b. **“unknown”**
      If no route is found for the received frame, the NFCC handles the frame in an implementation-specific manner.
   c. **“blocked”**
      If the protocol is ISO-DEP, then:
      - Respond with the status word “6A82” (File not found error) if a SELECT by DF name was received.
      - Respond with the status word “6F00” (Checking error with no precise diagnosis) for all other received commands.

      For all other protocols, ignore the received frame.
      The received frame SHALL NOT be forwarded to any NFCEE.

6.3.2 Configure Listen Mode Routing

These Control Messages are used to configure the Listen Mode Routing Table.

Table 50: Control Messages to Configure Listen Mode Routing

RF_SET_LISTEN_MODE_ROUTING_CMD				
Payload Field(s)	**Length**	**Value/Description**		
More	1 Octet	See Table 51.		
Number of Routing Entries	1 Octet	The number of Routing Entry fields to follow (n). This Control Message SHALL be at least one Routing Entry.		
Routing Entry [1..n]	x+2 Octets	Qualifier-Type	1 Octet	Type and qualifier, as defined in Table 52.
		Length	1 Octet	The length of Value (x).
		Value	x Octets	Value of the Routing TLV.

RF_SET_LISTEN_MODE_ROUTING_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

Table 51: More field values

Value	Description
0x00	Last Message
0x01	More Message(s) to follow
0x02 – 0xFF	RFU

Table 52: Qualifier-Type Field values

	Bit Mask								Description
	b7	b6	b5	b4	b3	b2	b1	b0	
Octet 0	0								RFU
		X							If set, indicates that routing is blocked for the power modes where it is not supported
			X						Only applies to AID routing entries. If set, indicates a match is allowed when the SELECT AID is shorter than the AID in this routing table entry.
				X					Only applies to AID routing entries. If set, indicates a match is allowed when the SELECT AID is longer than the AID in this routing table entry.
					X	X	X	X	Listen Mode Routing Entry Type as defined in Table 53.

Table 53: Listen Mode Routing Entry Types

Listen Mode Routing Entry Type	Length	Value
0x0	3 Octets	Technology-based routing entry, value field coded according to Table 54.
0x1	3 Octets	Protocol-based routing entry, value field coded according to Table 55.
0x2	2+n Octets	AID-based routing entry, value field coded according to Table 56.
0x3	2+2n Octets	System Code-based routing entry, value field coded according to Table 57
0x4	2+2n Octets	APDU Pattern-based routing entry, value field coded according to Table 58
0x5-0x9		RFU
0xA-0xF		For proprietary use

Table 54: Value Field for Technology-based Routing

Payload Field(s)	Length	Value/Description
Route	1 Octet	An NFCEE ID as defined in Table 116
Power State	1 Octet	See Table 59.
Technology	1 Octet	A valid RF Technology as defined in Table 130.

Table 55: Value Field for Protocol-based Routing

Payload Field(s)	Length	Value/Description
Route	1 Octet	An NFCEE ID as defined in Table 116
Power State	1 Octet	See Table 59.
Protocol	1 Octet	A valid RF Protocol as defined in Table 133

Table 56: Value Field for AID-based Routing

Payload Field(s)	Length	Value/Description
Route	1 Octet	An NFCEE ID as defined in Table 116
Power State	1 Octet	See Table 59.
AID	0-16 Octets	Application Identifier

Table 57: Value Field for System Code-based Routing

Payload Field(s)	Length	Value/Description
Route	1 Octet	An NFCEE ID as defined in Table 116
Power State	1 Octet	See Table 59.
SC Route List	2n Octets	1 <= n <= 32. A list of n entries consisting each of a System Code (2 Octets). The DH SHALL NOT use the wildcard value 0xFF as part of the System Code.

Table 58: Value Field for APDU Pattern-based Routing

Payload Field(s)	Length	Value/Description
Route	1 Octet	An NFCEE ID as defined in Table 116
Power State	1 Octet	See Table 59.
Reference data	n Octets	1 <= n <= 124 Data pattern for the comparison with the result of the AND operation between data and Mask.
Mask	n Octets	1 <= n <= 124 Mask pattern for AND operation with data. The Mask field contains the same amount of octets as the Reference data field.

Table 59: Value Field for Power State

	Bit Mask								Description
	b7	b6	b5	b4	b3	b2	b1	b0	
	0	0							RFU
			X						Applies to Switched On Sub-State 3 if the bit is equal to 1b. Otherwise it does not apply to Switched On Sub-State 3.
				X					Applies to Switched On Sub-State 2 if the bit is equal to 1b. Otherwise it does not apply to Switched On Sub-State 2.
					X				Applies to Switched On Sub-State 1 if the bit is equal to 1b. Otherwise it does not apply to Switched On Sub-State 1.
						X			Applies to Battery Off State if the bit is equal to 1b. Otherwise it does not apply to Battery Off State.
							X		Applies to Switched Off State if the bit is equal to 1b. Otherwise it does not apply to Switched Off State.
								X	Applies to Switched On State if the bit is equal to 1b. Otherwise it does not apply to Switched On State.

The Power State includes 3 Sub-States (1, 2 and 3) that are applicable only when the Device Host is in Switched On State. These Switched On Sub-States are generic definitions that can be custom-mapped to define the behavior of any product. However, an NFC Forum Device with a screen (e.g. a phone or tablet) that wants to use the Sub-States SHOULD use the following mappings:

- Switched On State applies when the screen is on and device is unlocked.
- Switched On Sub-State1 applies when the screen is off and device is unlocked.
- Switched On Sub-State2 applies when the screen is on and device is locked.
- Switched On Sub-State3 applies when the screen is off and device is locked.

When configuration of the NFCC for Listen Mode communication is necessary, the DH SHALL always send the complete Listen Mode Routing Table.

The Routing Entries sent by the DH in RF_SET_LISTEN_MODE_ROUTING_CMD SHALL be in the following order:

- All AID-based Routing Entries (if any)
- All APDU Pattern-based Routing Entries (if any)
- All System Code-based Routing Entries (if any)
- All Protocol-based Routing Entries (if any)
- All Technology-based Routing Entries (if any).

The NFCC uses the More field to determine if it has received all the Commands necessary to configure the routing. The new routing SHALL only become effective following receipt of all configuration information.

The DH SHALL keep the total size of the routing configuration information smaller than the ‘Max Routing Table Size’ indicated during Initialization (see Section 4.2).

All parameters except ‘More’ and ‘Number of Routing Entries’ are included in the calculation to determine if the routing configuration size exceeds the Max Routing Table Size.

The DH SHALL NOT try to configure routing of a specific Listen Mode Routing Entry Type unless the NFCC has indicated support for routing that type in the NFCC Features sent in the CORE_INIT_RSP. Also, the DH SHALL NOT try to configure routing for a specific Power State unless the NFCC has indicated support for that Power State in the NFCC Features sent in the CORE_INIT_RSP.

On receipt of the RF_SET_LISTEN_MODE_ROUTING_CMD with a valid routing configuration, the NFCC SHALL respond with the RF_SET_LISTEN_MODE_ROUTING_RSP with a Status of STATUS_OK.

In case of an error the NFCC SHALL respond with the RF_SET_LISTEN_MODE_ROUTING_RSP with a Status of STATUS_FAILED and the routing table SHALL be emptied.

Also if a new routing configuration is comprised of several Commands, and any one of these Commands fail, then the new routing configurations SHALL be ignored and the routing table SHALL be emptied

After above failure cases, the DH SHALL retry to configure the routing table until the NFCC accepts the routing table.

NOTE Failure in routing table configuration might lead to an empty routing table. As the routing table can only be configured in the **RFST_IDLE** state, this cannot happen during ongoing RF communication.

6.3.3 Read Listen Mode Routing

These Control Messages are used by the DH to read the NFCC's Listen Mode Routing Table.

Table 60: Control Messages to Read the NFCC's Listen Mode Routing

RF_GET_LISTEN_MODE_ROUTING_CMD		
Payload Field(s)	**Length**	**Value/Description**
Empty Payload		

RF_GET_LISTEN_MODE_ROUTING_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

RF_GET_LISTEN_MODE_ROUTING_NTF				
Payload Field(s)	**Length**	**Value/Description**		
More	1 Octet	See Table 51.		
Number of Routing Entries	1 Octet	The number of Routing Entry fields to follow (n). If the Listen Mode Routing Table is empty, the value of this field is 0x00 and there are no Routing Entries following.		
Routing Entry [0..n]	x+2 Octets	Qualifier-Type	1 Octet	Type and qualifier, as defined in Table 52.
		Length	1 Octet	The length of Value (x).
		Value	x Octets	Value of the Routing TLV.

To retrieve the current routing information from the NFCC, the DH sends the RF_GET_LISTEN_MODE_ROUTING_CMD to the NFCC.

The NFCC SHALL respond with the RF_GET_LISTEN_MODE_ROUTING_RSP with a Status of STATUS_OK followed by one or more RF_GET_LISTEN_MODE_ROUTING_NTF(s) containing the current routing information.

All but the last RF_GET_LISTEN_MODE_ROUTING_NTF SHALL have the More Parameter set to 1. The last RF_GET_LISTEN_MODE_ROUTING_NTF SHALL have the More Parameter set to 0.

Routing Entry fields will only be present if the value of Number of Routing Entries is greater than zero.

In case of an error, the NFCC SHALL respond with RF_GET_LISTEN_MODE_ROUTING_RSP with a Status indicating the failure reason, and the RF_GET_LISTEN_MODE_ROUTING_NTF SHALL NOT be sent.

6.3.4 Set Power State for Route Selection

These Control Messages are used by the DH to inform the NFCC to use one of the Switched On Sub-States when looking for a route in the routing table:

Table 61: Control Messages to Set the NFCC Route Selection Power State

CORE_SET_POWER_SUB_STATE_CMD			
Payload Field(s)	**Length**	**Value/Description**	
Power State	1 Octet	0x00	Switched On State This SHALL be the default sub state in the NFCC after initialization.
		0x01	Switched On Sub-State 1
		0x02	Switched On Sub-State 2
		0x03	Switched On Sub-State 3
		0x04 – 0xFF	RFU

CORE_SET_POWER_SUB_STATE_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

The DH MAY use the CORE_SET_POWER_SUB_STATE_CMD to inform the NFCC that the Power State to be used in route selection has changed from the default Switched On State.

If the NFCC receives a CORE_SET_POWER_SUB_STATE_CMD but has not indicated support for Switched On Sub-Mode States in CORE_INIT_RSP, the NFCC SHALL respond with CORE_SET_POWER_SUB_STATE_RSP with a Status field of STATUS_REJECTED.

The NFCC SHALL accept this Command in any state except RFST_LISTEN_ACTIVE. If the NFCC receives the Command in RFST_LISTEN_ACTIVE, it SHALL respond with a CORE_SET_POWER_SUB_STATE_RSP with a Status field of STATUS_SEMANTIC_ERROR, according to Section 3.2.2.In all other cases the NFCC SHALL respond with a CORE_SET_POWER_SUB_STATE_RSP with a Status field of STATUS_OK (this includes the case when the DH sets the same power sub-state as is already active in the NFCC).

6.3.5 AID-based Route Selection Process

The following process SHALL be followed when looking through the routing table for an AID match.

Starting at the first AID based routing entry, and for every subsequent AID based routing entry:

- If the bit representing the current Power State is ‘1b’ in the routing entry and the AIDs match based on the comparison rules below, then set EE_ROUTE with the NFCEE identifier stored in the corresponding routing entry, and terminate the AID-based Routing Selection Process.
- If the bit representing the current Power State is ‘0b’ in the routing entry and the route blocked bit is equal to ‘1b’ and the AIDs match based on the comparison rules below, then set EE_ROUTE to “blocked”, and terminate the AID-based Routing Selection Process.

If the end of the table is reached, then set EE_ROUTE to “unknown”.

The specific comparison rule used from the three below is based on whether the length of the AID in the SELECT command is equal to, less than, or greater than the length of the AID in the routing entry. Bits b4 and b5 are in the Qualifier-Type field (defined in Table 52).

- If the AID in the SELECT is equal in length to the AID in the routing entry:
  - The comparison result SHALL be a match if the entire AID values are equal.
- If the AID in the SELECT is shorter than the AID in the routing table entry:
  - The comparison result SHALL be a match only if b5 is equal to 1b and the AID values are equal up to the length of the AID in the SELECT command.
- If the AID in the SELECT is longer than the AID in the routing table entry:
  - The comparison result SHALL be a match only if b4 is equal to 1b and the AID values are equal up to the length of the AID in the routing table entry.

NOTE If b4 is equal to 1b, a routing table entry with a zero length AID will match a SELECT command with any AID.

6.3.6 APDU Pattern-based Route Selection Process

The following process SHALL be followed when looking through the routing table for an APDU Pattern-based match.

Starting at the first APDU Pattern-based routing entry, and for every subsequent APDU Pattern-based routing entry:

- If the bit representing the current Power State is equal to '1b' in the routing entry and the pattern matches based on the rules below, then set EE_ROUTE with the NFCEE identifier stored in the corresponding routing entry, and terminate the APDU Pattern-based Routing Selection Process.
- If the bit representing the current Power State is equal to '0b' in the routing entry and the route blocked bit is '1b' and the pattern matches based on the rules below, then set EE_ROUTE to "blocked" , and terminate the APDU Pattern-based Routing Selection Process.

If the end of the table is reached, then terminate the APDU Pattern-based Route Selection Process without changing EE_ROUTE.

An APDU matches with a routing table entry if both:

- The number of APDU octets is equal or higher than the number of Reference data octets.
- The Reference data octets are equal to the result of the AND operation of the Mask octets with the octets of the APDU starting with the first octet.

6.3.7 System Code-based Route Selection Process

The System Code-based Route Selection Process is performed as part of the SENSF_REQ handling on the NFCC.

The following process SHALL be followed each time a SENSF_REQ is received:

If the NFC Forum Device is not in either IDLE, READY_F, SLEEP_AF or CARD_EMULATOR_3 state, as defined in [ACTIVITY], terminate the System Code-based Route Selection Process without changing EE_ROUTE.

If all of the following conditions are met:

- The NFC Forum Device is in IDLE, READY_F or SLEEP_AF state as defined in [ACTIVITY]
- The NFCC configuration allows sending a SENSF_RES Response indicating support for NFC-DEP
- The SENSF_REQ meets the conditions for sending an SENSF_RES Response indicating NFC-DEP as defined in [DIGITAL]and [ACTIVITY]

then send a SENSF_RES Response indicating support for NFC-DEP and terminate the process without changing EE_ROUTE.

Otherwise, select one NFCEE ID according to the following rules:

- Starting at the first System Code-based Routing entry, and for every subsequent System Code-based Routing entry:

- If the bit representing the current Power State is ‘1b’ in the routing entry and one of the System Code values contained in the SC Route List of the System Code-based Routing entry matches the System Code of the SENSF_REQ Command based on the comparison rules below, then select the NFCEE ID contained in the Route field of the System Code-based Routing entry.
- If the bit representing the current Power State is ‘0b’ in the routing entry and the route blocked bit is equal to ‘1b’, the System Code of the SENSF_REQ is not equal to 0xFFFF, and one of the System Code values contained in the SC Route List of the System Code-based Routing entry matches the System Code of the SENSF_REQ Command based on the comparison rules below, then set EE_ROUTE to “blocked”, and terminate the System Code-based Route Selection Process..

The comparison between the System Code of the SENSF_REQ and the System Codes in SC Route List starts with the first entry in the SC Route List and continues sequentially until a match is found or all entries have been compared. A match is determined according to the rules defined as part of the IDLE state of the Listen Mode State Machine in [ACTIVITY] for comparing System Codes.

NOTE Based on the comparison rules defined in [ACTIVITY], a SENSF_REQ Command with a SC set to 0xFFFF will always match the first entry whose current Power State value is equal to ‘1b’ in the SC Route List of the System Code-based Routing entry.

- If no NFCEE ID has been selected and if a Protocol-based routing entry for Type 3 Tag RF Protocol matching the current power state exists, select the corresponding NFCEE ID.
- If no NFCEE ID has been selected and if a Technology-based routing entry for NFC-F Technology matching the current power state exists, select the corresponding NFCEE ID.

If no NFCEE ID is selected, terminate the System Code-based Route Selection Process without sending a SENSF_RES and without changing EE_ROUTE.

Otherwise, receive the SENSF_RES Response from the NFCEE whose NFCEE ID has been selected. The SENSF_RES Response is generated either by the NFCC, as in the case of the DH-NFCEE, or by forwarding the SENSF_REQ Command to the selected NFCEE.

If no SENSF_RES Response is received, terminate the System Code-based Route Selection Process without sending a SENSF_RES and without changing EE_ROUTE.

Otherwise, send the selected SENSF_RES Response according to [DIGITAL] and [ACTIVITY].

If the SENSF_RES Response indicated support for the Type 3 Tag Platform, set EE_ROUTE to be the selected NFCEE ID. Otherwise, terminate the System Code-based Route Selection Process without changing EE_ROUTE.

NOTE Since the NFCC creates the SENSF_RES Response for a Type 3 Tag Platform on the DH based on the LF_T3T parameters, the NFCID2 in the SENSF_RES Response from the DH-NFCEE is equal to a value of one of the LF_T3T_IDENTIFIERS (see Section 6.1.8). The DH is responsible for providing a consistent configuration for the LF_T3T_IDENTIFIERS and the System Code-based routing entries for the DH.

6.3.8 Protocol-based Route Selection Process

The following process SHALL be followed when scanning through the routing table for a Protocol-based match.

Starting at the first Protocol-based routing entry, and for every subsequent Protocol-based routing entry until a match is found or the scan through the table is completed:

- If the bit representing the current Power State is equal to '1b' in the routing entry and the protocols match, then set EE_ROUTE with the NFCEE identifier that is stored in the corresponding routing entry
- If the bit representing the current Power State is equal to '0b' in the routing entry, the route blocked bit is '1b' and the protocols match, then set EE_ROUTE to "blocked".

If the end of the table is reached, then terminate the Protocol-based Route Selection Process without changing EE_ROUTE.

6.3.9 Technology-based Route Selection Process

The following process SHALL be followed when scanning through the routing table for a Technology-based match.

Starting at the first Technology-based routing entry, and for every subsequent Technology-based routing entry until a match is found or the scan through the table is completed:

- If the bit representing the current Power State is equal to '1b' in the routing entry and the technologies match, then set EE_ROUTE with the NFCEE identifier stored in the corresponding routing entry.
- If the bit representing the current Power State is equal to '0b' in the routing entry and the route blocked bit is '1b' and the technologies match, then set EE_ROUTE to "blocked".

If the end of the table is reached, then terminate the Technology-based Route Selection Process without changing EE_ROUTE.

6.3.10 Forced NFCEE Routing

The DH enables and disables Forced NFCEE Routing by sending RF_SET_FORCED_NFCEE_ROUTING_CMD.

To enable Forced NFCEE Routing, the DH SHALL set the Forced NFCEE Routing State field to 1, set Forced NFCEE field with a valid NFCEE ID, and set Forced Power State field to indicate in which Power State(s) the Force NFCEE can be routed to. A valid NFCEE ID is one that is neither disabled nor non-responsive.

To disable Forced NFCEE Routing, the DH SHALL set the Forced NFCEE Routing State field to 0.

On receipt of the RF_SET_FORCED_NFCEE_ROUTING_CMD with valid parameters, the NFCC SHALL respond with RF_SET_FORCED_NFCEE_ROUTING_RSP with a Status of STATUS_OK. If the parameters are considered invalid, the NFCC SHALL respond with RF_SET_FORCED_NFCEE_ROUTING_RSP with a Status of STATUS_INVALID_PARAM, and Forced NFCEE Routing SHALL be disabled.

Failure in Forced NFCEE Routing configuration SHALL result in Forced NFCEE Routing being disabled. The DH SHALL NOT configure Forced NFCEE Routing in any state other than RFST_IDLE, so this cannot happen during ongoing RF communication.

If the Forced NFCEE becomes disabled or unresponsive, the DH SHALL disable Forced NFCEE Routing.

Table 62: Control Messages to Configure Forced NFCEE Routing

RF_SET_FORCED_NFCEE_ROUTING_CMD		
Payload Field(s)	**Length**	**Value/Description**
Forced NFCEE Routing State	1 Octet	0 – Forced NFCEE Routing Disabled 1 - Forced NFCEE Routing Enabled.
Forced NFCEE Value field	0 or 2 Octets	Value Field for Forced NFCEE Routing as defined in Table 63. This field SHALL NOT be present if Forced NFCEE Routing State is set to 0 (Disabled).

RF_SET_FORCED NFCEE_ROUTING_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

Table 63: Value Field for Forced NFCEE Routing

Payload Field(s)	Length	Value/Description
Forced NFCEE	1 Octet	An NFCEE ID as defined in Table 116
Forced Power State	1 Octet	See Table 59.

The DH SHALL NOT enable the Forced NFCEE Routing unless the NFCC has indicated support for it in the NFCC Features sent in the CORE_INIT_RSP.

While Forced NFCEE Routing is enabled, the NFCC SHALL use the RF Configuration and the Discovery Configuration Parameters for the Listen Mode received from the Forced NFCEE. If the NFC-DEP RF Protocol is mapped to the NFC-DEP RF Interface and the actual RF Technology and Mode is configured in RF_DISCOVER_CMD, the NFCC SHALL additionally use the Discovery Configuration Parameters for Listen NFC-DEP received from the DH. If the DH has additionally configured LA_SEL_INFO to indicate NFC-DEP support, the NFCC SHALL also indicate NFC-DEP support in the SEL_RES Response. Otherwise the NFCC decides about the indication of NFC-DEP support. In case the Forced NFCEE requests no NFC-A communication and the DH has mapped the NFC-DEP RF Protocol on NFC-DEP RF Interface and configured for NFC_A_PASSIVE_LISTEN_MODE, the Discovery Configuration Parameters for Listen A provided by the DH SHALL be used for NFC-DEP protocol activation where additionally the NFC-DEP RF Protocol is indicated in the SEL_RES Response.

While Forced NFCEE Routing is enabled, and the NFCC is in RFST_ DISCOVERY, if the bit representing the current Power State is ‘0b’ in the Forced Power State, the NFCC SHALL only answer to NFC-DEP protocol activation commands from the Remote NFC Endpointwhen the NFC-DEP RF Protocol is mapped to the NFC-DEP RF Interface and the actual RF Technology and Mode is configured in RF_DISCOVER_CMD.

While Forced NFCEE Routing is enabled, and the NFCC is in RFST_LISTEN_ACTIVE:

- When the NFC-DEP RF Protocol is activated, the NFCC SHALL route received frames according to the Protocol-based Route Selection Process defined in Section 6.3.8.
- When another RF Protocol is activated, the NFCC SHALL check the Forced Power State value. If the bit representing the current Power State is 1b, the NFCC SHALL route the received frame to the Forced NFCEE. Otherwise the NFCC SHALL ignore the received frame.

7 RF Discovery

This section describes the Control Messages required for moving through the state machine defined in Section 5.2.

7.1 Starting RF Discovery

RF Discovery Process is a periodic activity consisting of poll and listen cycles, configured by different discovery configurations. The TOTAL_DURATION configuration parameter in Table 46 specifies the duration of one discovery period (=Total Duration). This parameter is used to define the length of listen or idle cycles.

The following rules are applied for the Total Duration parameter:

- If both Poll and Listen Modes are configured, then Listen Duration length is Total Duration minus Poll Duration, where Poll Duration is the time required to execute the Technology Detection Activity (see [ACTIVITY]) for the configured technologies when no Remote NFC Endpoint is detected. During the Listen Duration, the NFCC SHALL NOT generate an RF Field but SHALL detect an RF Field.
- If only Poll Mode is configured, then Idle Duration length is Total Duration minus Poll Duration. During the Idle Duration the NFCC SHALL NOT generate an RF Field and SHALL NOT detect an RF Field.
- If only Listen Mode is configured, then this parameter is not applicable.
- The NFCC MAY extend Total Duration if it is not long enough to cover the Configurations provided in the RF_DISCOVER_CMD.

NOTE [ACTIVITY] defines some limits to the length of polling for each technology, but there can be NFCC implementation specific variations. Also the minimum length of listening for each technology can vary per implementation. Thus the DH might not know the exact minimum value to be used for Total Duration.

If the Discovery Configuration Mode in Octet 0 of the NFCC Features as returned in CORE_INIT_RSP is equal to 00b, the DH is responsible for defining not just the configuration parameters, but the Listen Mode Routing Table, and the RF Technology and Mode list in the RF_DISCOVER_CMD. The NFCC is unable to modify these items so the entire process of RF Discovery is as defined by the DH.

If the Discovery Configuration Mode in Octet 0 of the NFCC Features as returned in CORE_INIT_RSP is equal to 01b, it signifies that the NFCC can receive configurations from the DH and other NFCEEs. This implies that the NFCC can manage or merge multiple configurations, including RF Configuration Parameters, the Listen Mode Routing Configuration, and the RF Technology and Mode list.

If the DH wants to allow the NFCC to exercise its configuration management logic, the DH SHALL set Bit 0 of parameter NFCC_CONFIG_CONTROL to a value of 1b.

Table 64: NFCC Configuration Control

ID	Length	Description
NFCC_CONFIG_CONTROL	1 Octet	See Table 65

Table 65: Value Field for NFCC Configuration Control

Bit Mask								Description
b7	b6	b5	b4	b3	b2	b1	b0	
0	0	0	0	0	0	0		RFU
							X	0b: NFCC is not allowed to manage RF configuration 1b: NFCC is allowed to manage RF configuration Default: 0b

If Bit 0 of NFCC_CONFIG_CONTROL is equal to 0b, the NFCC SHALL NOT change any of the RF configuration parameters after they are set by the DH.

NOTE If the DH had set Bit 0 of NFCC_CONFIG_CONTROL to a value of 1b, and later wishes to change it back to a value of 0b, it is the responsibility of the DH to configure any aspects of configuration that the NFCC might have changed.

The following Control Messages are used to initiate the RF Discovery Process.

Table 66: Control Messages to Start Discovery

RF_DISCOVER_CMD					
Payload Field(s)	**Length**	**Value/Description**			
Number of Configurations	1 Octet	The number of Configuration fields to follow (n). n can be 0 if the RF Discovery is enabled for NFCEE(s) only (e.g. in response to a RF_NFCEE_DISCOVERY_REQ_NTF and an NFCEE(s) providing configuration settings directly to the NFCC). If n is 0, this Command contains no Configuration fields.			
Configuration [0..n]	2 Octets	RF Technology and Mode	1 Octet	RF Technology and Mode of the local device. See Table 131.	
		Discovery Frequency	1 Octet	0x00	RFU
				0x01	RF Technology and Mode will be executed in every discovery period.
				0x02-0x0A	These values are allowed for Poll Mode RF Technology and Mode values. This value specifies how often the Poll period of the specific RF Technology will be executed. For example, a value of 10 indicates that this Polling will be executed in every 10th discovery period.
				0x0B-0xFF	RFU

RF_DISCOVER_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

RF_DISCOVER_NTF			
Payload Field(s)	**Length**	**Value/Description**	
RF Discovery ID	1 Octet	See Table 67.	
RF Protocol	1 Octet	RF Protocol supported by the Remote NFC Endpoint. See Table 133.	
RF Technology and Mode	1 Octet	RF Technology and Mode of the local device. See Table 131.	
Length of RF Technology Specific Parameters	1 Octet	The length of RF Technology Specific Parameters field to follow.	
RF Technology Specific Parameters	0 – n Octets	Refer to one of the tables listed below, depending on the value of the RF Technology and Mode; See Table 68 for NFC-A Poll Mode. See Table 70 for NFC-B Poll Mode. See Table 72 for NFC-F Poll Mode. See Table 74 for NFC-V Poll Mode. Proprietary parameters if the value of RF Technology and Mode is reserved for a proprietary technology.	
Notification Type	1 Octet	0	Last Notification
		1	Last Notification (due to NFCC reaching its resource limit)
		2	More Notification to follow
		3-255	RFU

Table 67: RF Discovery ID

Value	Description
0	RFU
1 – 254	Dynamically assigned by the NFCC
255	RFU

The DH requests that the NFCC starts Discovery activity by sending the RF_DISCOVER_CMD. The parameters RF Technology and Mode and Discovery Frequency are provided by the DH to configure the manner in which the NFCC performs the RF Discovery Process. If the parameters are acceptable for the NFCC, the NFCC SHALL return the RF_DISCOVER_RSP with a Status of STATUS_OK and will start the RF Discovery Process accordingly. If the parameters are not acceptable to the NFCC, the NFCC SHALL return RF_DISCOVER_RSP with a Status of STATUS_REJECTED and remain in the RFST_IDLE state.

When the RF Communication State Machine is not in the state **RFST_IDLE**, the NFCC SHALL return RF_DISCOVER_RSP with a Status of DISCOVERY_ALREADY_STARTED. In this error case, the current ongoing RF Discovery Process SHALL continue without any changes.

During the RF Discovery Process, if CON_DISCOVERY_PARAM is changed, the RF Discovery MAY have to be reconfigured by the NFCC:

- If bit b0 is equal to 1b, the RF Discovery Process SHALL include the Poll Mode RF Technology and Mode values of the Discovery configuration. Otherwise, the RF Discovery Process SHALL exclude the Poll Mode RF Technology and Mode values of the Discovery configuration.
- If bit b1 is equal to 1b and the NFCC supports the Listen Mode Routing Table, the DH-NFCEE SHALL be considered as disabled, and the NFCC SHALL behave as defined in Section 6.3 for disabled NFCEEs. Otherwise, the DH-NFCEE SHALL be considered as enabled.

If CON_DISCOVERY_PARAM is changed while RF communication is ongoing, this RF communication SHALL NOT be interrupted.

In Poll Mode, if there are multiple Remote NFC Endpoints detected, or if a Remote NFC Endpoint supports multiple RF Protocols, the NFCC SHALL send RF_DISCOVER_NTF to the DH for each combination of Remote NFC Endpoint and RF Protocol detected during the RF Discovery Process.

- The NFCC SHALL assign a unique RF Discovery ID to each detected Remote NFC Endpoint. The combination of RF Discovery ID and RF Protocol SHALL be unique across all RF_DISCOVER_NTFs sent within a series of RF Discovery Notifications. The NFCC SHALL assign the same RF Discovery ID in all notifications send for a single Remote NFC Endpoint supporting multiple protocols.

NOTE If a Remote NFC Endpoint supports multiple protocols, the NFCC uses the same RF Discovery ID for each Notification, but different RF Protocol values. If a Remote NFC Endpoint uses separate polling responses to indicate support of multiple protocols, the NFCC cannot know that the responses came from a single Remote NFC Endpoint. In that case, the NFCC assigns different RF Discovery ID.

- All assigned RF Discovery IDs are released when the RF State machine defined in Section 5.2 moves into state **RFST_IDLE**.
- The Notification Type field SHALL be set to 0 or 1 if the current RF_DISCOVER_NTF is the last notification being sent or set to 2 if there is another RF_DISCOVER_NTF to follow (called series of RF Discovery Notifications).

NOTE Since RF_DISCOVER_NTF is only sent when there are multiple Remote NFC Endpoints in the field or if a Remote NFC Endpoint supports multiple RF Protocols, the first notification sent after starting the RF Discovery Process will always have the Notification Type set to 0x02 (more notifications to follow)

- A value of 0x00 SHALL be used for the Notification Type if the NFCC has completed the collision resolution process and no further Remote NFC Endpoints have been identified. A value of 1 SHALL be used if the NFCC has aborted the collision resolution process due to internal restrictions and therefore further Remote NFC Endpoints might not have been detected.

After receiving RF_DISCOVER_NTF with a Notification Type field set to 0x00 or 0x01, the DH SHALL either select the Remote NFC Endpoint by sending RF_DISCOVER_SELECT_CMD or stop the RF Discovery Process by sending RF_DEACTIVATE_CMD.

Table 68: Specific Parameters for NFC-A Poll Mode

Parameter	Length	Description
SENS_RES Response	2 Octets	Defined in [DIGITAL].
NFCID1 Length	1 Octet	Length of NFCID1 Parameter. If an NFC Forum Type 1 Tag is detected then the NFCID1 Parameter is the 4-Byte UID collected from the response to the RID command. In all other cases NFCID1 Length value SHALL be 0x04, 0x07 or 0x0A. Other values are RFU.
NFCID1	4, 7, or 10 Octets	Defined in [DIGITAL].
SEL_RES Response Length	1 Octets	Length of SEL_RES Response Parameter. If an NFC Forum Type 1 Tag is detected then no SEL_RES Response is available and the value of this parameter is set to 0x00. In all other cases the value of the SEL_RES Response Length SHALL be 0x01. Other values are RFU.
SEL_RES Response	0 or 1 Octet	Defined in [DIGITAL].
HRx Length	1 Octets	Length of HRx Parameters collected from the response to the RID command. If an NFC Forum Type 1 Tag is detected and HR0 and HR1 are available in the response to the RID command, then the value of this parameter is set to 0x02 and the HRx field SHALL be present. In all other cases the value of the HRx Length SHALL be 0x00 and the HRx field SHALL NOT be present. Other values are RFU.
HRx	0 or 2 Octets	If present, the first byte SHALL contain HR0 and the second byte SHALL contain HR1, as defined in [DIGITAL].

Table 69: Specific Parameters for NFC-A Listen Mode

Parameter	Length	Description
No parameters are currently defined.		

Table 70: Specific Parameters for NFC-B Poll Mode

Parameter	Length	Description
SENSB_RES Response Length	1 Octet	Length of SENSB_RES Response Parameter. Allowed values SHALL be 0x0B and 0x0C. Other values are RFU.
SENSB_RES Response	11 or 12 Octets	Byte 2 – Byte 12 or 13 of SENSB_RES, as defined in [DIGITAL].

Table 71: Specific Parameters for NFC-B Listen Mode

Parameter	Length	Description
SENSB_REQ Command	1 Octet	Byte 2 (AFI) of last received SENSB_REQ or ALLB_REQ, as defined in [DIGITAL].

Table 72: Specific Parameters for NFC-F Poll Mode

Parameter	Length	Description	
Bit Rate	1 Octet	1	212 kbps
		2	424 kbps
		0 and 3 to 255	RFU
SENSF_RES Response Length	1 Octet	Length of SENSF_RES Response Parameter Allowed values SHALL be 0x10 and 0x12. Other values are RFU.	
SENSF_RES Response	16 or 18 Octets	Byte 2 – Byte 17 or 19 of SENSF_RES as defined in [DIGITAL].	

Table 73: Specific Parameters for NFC-F Listen Mode

Parameter	Length	Description
Local NFCID2 Length	1 Octet	Length of Local NFCID2 Parameter. If NFCID2 is available, then Local NFCID2 Length SHALL be 0x08. If NFCID2 is not available, then Local NFCID2 Length SHALL be 0x00, and Local NFCID2 field is not present. Other values are RFU.
Local NFCID2	0 or 8 Octets	This parameter only applies to the Frame RF Interface. If the NFC-DEP Protocol is used, the NFCID2 is generated by the Local NFCC. If the T3T Protocol is used, the NFCID2 in the command that triggered activating the RF Interface.

Table 74: Specific Parameters for NFC-V Poll Mode

Parameter	Length	Description
RES_FLAG	1 Octet	1st Byte of the INVENTORY_RES Response as defined in [DIGITAL]
DSFID	1 Octet	2nd Byte of the INVENTORY_RES Response as defined in [DIGITAL]
UID	8 Octets	3rd Byte to last Byte of the INVENTORY_RES Response as defined in [DIGITAL]

Table 75: Specific Parameters for NFC-ACM Poll Mode

Parameter	Length	Description
ATR_RES Response Length	1 Octet	Length of ATR_RES Response Parameter (n)
ATR_RES Response	n Octets	All Bytes of ATR_RES Response starting from and including Byte 3 as defined in [DIGITAL]

Table 76: Specific Parameters for NFC-ACM Listen Mode

Parameter	Length	Description
ATR_REQ Command Length	1 Octet	Length of ATR_REQ Command Parameter (n)
ATR_REQ Command	n Octets	All Bytes of the ATR_REQ Command as defined in [DIGITAL] starting from and including Byte 3.

7.2 Select Discovered Target

These Control Messages are used to select an RF Discovery ID and RF Protocol (identifying a Remote NFC Endpoint as reported by a previous RF_DISCOVER_NTF) and the RF Interface to use for communicating with the Remote NFC Endpoint, which might differ from the one defined in the RF_DISCOVER_MAP_CMD.

Table 77: Control Messages to select a Discovered Target

RF_DISCOVER_SELECT_CMD		
Payload Field(s)	**Length**	**Value/Description**
RF Discovery ID	1 Octet	See Table 67.
RF Protocol	1 Octet	See Table 133.
RF Interface	1 Octet	See Table 134. The value 0x00 (NFCEE Direct RF Interface) SHALL NOT be used.

RF_DISCOVER_SELECT_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

The DH SHALL send RF_DISCOVER_SELECT_CMD to the NFCC to inform the NFCC which RF Discovery ID, RF Protocol and RF Interface are to be used for subsequent communication.

In case the RF Discovery ID, RF Protocol or RF Interface is not valid the NFCC SHALL respond with RF_DISCOVER_SELECT_RSP with a Status of STATUS_REJECTED.

Otherwise, the NFCC SHALL respond with RF_DISCOVER_SELECT_RSP with a Status of STATUS_OK. After that, the NFCC SHALL perform activation for the RF Protocol, depending on the RF Technology or RF Interface associated with the parameters of the RF_DISCOVER_SELECT_CMD.

The specified RF Interface parameter value is only valid for the following RF Interface activation and does not cause any change to the RF Interface Mapping configuration (see Section 6.2).

7.3 RF Interface Activation and Deactivation

The NFCC can activate an RF Interface either in **RFST_DISCOVERY**, **RFST_LISTEN_SLEEP** or **RFST_W4_HOST_SELECT** state by sending RF_INTF_ACTIVATED_NTF. The RF_INTF_ACTIVATED_NTF causes the state to change as described in Section 5.2.

At most one RF Interface SHALL be active at any time.

7.3.1 RF Interface Activation Notification

This Notification is used by the NFCC to inform the DH that a specific RF Interface has been activated.

Table 78: Notification for RF Interface activation

RF_INTF_ACTIVATED_NTF		
Payload Field(s)	**Length**	**Value/Description**
RF Discovery ID	1 Octet	See Table 67.
RF Interface	1 Octet	See Table 134. If this contains a value of 0x00 (NFCEE Direct RF Interface), then all following parameters SHALL contain a value of 0 and SHALL be ignored.
RF Protocol	1 Octet	See Table 133.
Activation RF Technology and Mode	1 Octet	RF Technology and Mode of the local device that were used for the collection of the RF Technology Specific Parameters below. See Table 131.
Max Data Packet Payload Size	1 Octet	Max Data Packet Payload Size the NFCC can receive for the Static RF Connection. A number from 1 – 255.
Initial Number of Credits	1 Octet	Initial Number of Credits given by the NFCC to the DH for the Static RF Connection, as defined in Table 15.
Length of RF Technology Specific Parameters	1 Octet	The length of RF Technology Specific Parameters field to follow.
RF Technology Specific Parameters	0 – n Octets	One of the below tables depending on the value of the RF Technology and Mode; Depends on RF Technology and Mode. See Table 68 for NFC-A Poll Mode. See Table 69 for NFC-A Listen Mode. See Table 70 for NFC-B Poll Mode. See Table 71 for NFC-B Listen Mode. See Table 72 for NFC-F Poll Mode. See Table 73 for NFC-F Listen Mode. See Table 74 for NFC-V Poll Mode See Table 75 for NFC-ACM Poll Mode See Table 76 for NFC-ACM Listen Mode Proprietary parameters if the value of RF Technology and Mode is reserved for a proprietary technology.
Data Exchange RF Technology and Mode	1 Octet	RF Technology and Mode that will be used for Data Exchange. See Table 131.
Data Exchange Transmit Bit Rate	1 Octet	Bit rate that will be used for Data Exchange in the transmit direction. For a polling device this is the bit rate from poll to listen, and for a listening device this is the bit rate from listen to poll. See Table 132.

RF_INTF_ACTIVATED_NTF		
Payload Field(s)	**Length**	**Value/Description**
Data Exchange Receive Bit Rate	1 Octet	Bit Rate that will be used for Data Exchange in the receive direction. For a polling device this is the bit rate from listen to poll, and for a listening device this is the bit rate from poll to listen. See Table 132.
Length of Activation Parameters	1 Octet	The length of Activation Parameters field to follow.
Activation Parameters	0 – n Octets	Activation Parameters are defined in the RF Interface section that corresponds to the RF Interface value. If a proprietary interface is activated, proprietary parameters MAY be used. For a list of possible ISO-DEP RF Interface Activation Parameters, see Table 95, Table 96, Table 98 and Table 99. For a list of possible NFC-DEP RF Interface Activation Parameters, see Table 102 and Table 103. There are no Activation Parameters for the Frame RF Interface.

The RF Interface to be activated is selected based on the current RF Interface Mapping configuration (see Section 6.2) or the parameter in the RF_DISCOVER_SELECT_CMD (see Section 7.2).

Depending on the selected RF Discovery ID and RF Protocol, the NFCC performs protocol activation procedures before activating the RF Interface. The protocol activation is described in each RF Interface section.

When all phases before RF Interface activation are performed successfully, the NFCC SHALL send RF_INTF_ACTIVATED_NTF with information about the activated RF Interface (RF Interface field).

After the NFCC sends RF_INTF_ACTIVATED_NTF with an RF Interface other than NFCEE Direct, the Static RF Connection can be used. The Max Data Packet Payload Size and Initial Number of Credits parameters of the RF_INTF_ACTIVATED_NTF apply to the Static RF Connection.

NOTE The NFCC can choose any permitted values for Max Data Packet Payload Size and Initial Number of Credits when activating an RF Interface, regardless of any values that might have been used in previous activations.

The Data Exchange RF Technology and Mode, Data Exchange Transmit Bit Rate and Data Exchange Receive Bit Rate parameters inform the DH about the RF Technology and Bit Rates in use at the time the RF_INTF_ACTIVATED_NTF is sent. For the Frame RF Interface the DH might subsequently process commands and responses that will cause changes in the values used for Data Exchange. For other RF Interfaces these are the values that will be used during Data Exchange.

RF_INTF_ACTIVATED_NTF can include Activation Parameters. Activation Parameters depend on the RF Interface field. Each RF Interface section defines the parameters to be included.

Other parameters in the RF_INTF_ACTIVATED_NTF are the same as in the RF_DISCOVER_NTF.

The RF Discovery ID value communicated in an RF_INTF_ACTIVATED_NTF SHALL be valid until the state is changed to **RFST_IDLE**.

7.3.2 RF Interface Deactivation

These Control Messages are used to deactivate an active RF Interface (to stop communication between the DH or NFCEE with a Remote NFC Endpoint) or to stop the Discovery process.

Table 79: Control Messages for RF Interface Deactivation

RF_DEACTIVATE_CMD		
Payload Field(s)	**Length**	**Value/Description**
Deactivation Type	1 Octet	See Table 80.

RF_DEACTIVATE_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129

RF_DEACTIVATE_NTF		
Payload Field(s)	**Length**	**Value/Description**
Deactivation Type	1 Octet	See Table 80.
Deactivation Reason	1 Octet	See Table 81

Table 80: Deactivation Types

Deactivation Type	Description
0x00	Idle Mode
0x01	Sleep Mode
0x02	Sleep_AF Mode
0x03	Discovery
0x04 – 0xFF	RFU

NOTE “Sleep Mode” and “Sleep_AF Mode” refer to the sleep states of the Listen Mode state machine defined in [ACTIVITY]. Depending on the technology, “Sleep Mode” refers to SLEEP_A for NFC-A or SLEEP_B for NFC-B, and “Sleep_AF” refers to the SLEEP_AF state.

Table 81: Deactivation Reasons

Deactivation Reason	Description
0x00	DH_Request
0x01	Endpoint_Request
0x02	RF_Link_Loss
0x03	NFC-B_Bad_AFI
0x04	DH request failed due to error
0x05 – 0xFF	RFU

The RF State Machine in Section 5.2 specifies for each state the possible deactivation cases.

The following rules apply in addition to the definitions in Section 5.2:

- Started RF Interface Extensions are implicitly stopped by deactivating the RF Interface.The NFCC SHALL perform deactivation procedures defined by the RF Interface Extensions (if any) before deactivating the RF Interface. Any error that occurs during performing the RF Interface Extension deactivation SHALL be ignored by the NFCC.
- For the RF_DEACTIVATE_CMD the Deactivation Type values ‘Sleep Mode’ and ‘Sleep_AF Mode’ are allowed only for some RF Interfaces. Each RF Interface specifies whether it supports these deactivation cases. If an RF_DEACTIVATE_CMD with Deactivation Type set to ‘Sleep Mode’ or ‘Sleep_AF Mode’ is received when using an RF Interface where those values are not allowed, the NFCC SHALL send RF_DEACTIVATE_RSP with a Status of STATUS_REJECTED. The NFCC SHALL NOT send RF_DEACTIVATE_NTF in this case.
- If not defined otherwise in the corresponding interface section, the value of the Deactivation Type parameter of the RF_DEACTIVATE_NTF SHALL be the same as in the RF_DEACTIVATE_CMD. If the RF_DEACTIVATE_NTF is sent following a RF_DEACTIVATE_CMD/RSP the Deactivation Reason SHALL be set to ‘DH Request’.
- If the activated RF Interface defines that the NFCC has to perform protocol deactivation procedures, the NFCC SHALL perform those deactivation procedures before sending the RF_DEACTIVATE_NTF.
- Prior to sending an RF_DEACTIVATE_NTF, the NFCC SHOULD send all data pending to be sent to the Remote NFC Endpoint and send all completely received Data Messages to the DH.
- After sending a RF_DEACTIVATE_NTF, the NFCC SHALL stop sending any Data Messages related to the RF Interface.
- Upon receipt of a RF_DEACTIVATE_NTF, the DH SHALL NOT send any Data Messages related to the RF Interface.

After an RF Interface has been deactivated:

No further communication operations defined by the RF Interface (including Data Messages) SHALL be performed.

- All remaining data in the NFCC and DH buffers that was exchanged in the context of the RF Interface SHALL be removed.

7.4 RF Interface Extension Starting and Stopping

An RF Interface Extension can be in one of two different states: stopped or started. The Control Messages in this section allow transitioning between those two states.

7.4.1 RF Interface Extension Start

The following Control Messages are used to start RF Interface Extensions.

Table 82: Control Messages to Start RF Interface Extensions

RF_INTF_EXT_START_CMD				
Payload Field(s)	**Length**	**Value/Description**		
RF Interface Extension	x+2 Octets	Extension	1 Octet	See Table 135
		Start Parameter Length	1 Octet	The length of the following Start Parameter field (x).
		Start Parameter	x Octets	The start parameters as defined for the respective RF Interface Extension

RF_INTF_EXT_START_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129

The RF_INTF_EXT_START_CMD SHALL NOT be sent in states other than **RFST_POLL_ACTIVE** and **RFST_LISTEN_ACTIVE**.

The DH SHALL NOT use RF_INTF_EXT_START_CMD to start an RF Interface Extension except if all startup conditions defined for the RF Interface Extension are fulfilled. Startup conditions are defined for each RF Interface Extension in the section defining the RF Interface Extension.

On execution of the Command the NFCC SHALL send RF_INTF_EXT_START_RSP to inform the DH that the NFCC has executed the Command. If the RF Interface Extensions has been started successfully, the Status SHALL be STATUS_OK. If the NFCC is unable to start the RF Interface Extension, the Status SHALL be set to STATUS_FAILED.

The DH MAY send RF_INTF_EXT_START_CMD for an RF Interface Extension that is already started. In this case the NFCC SHALL use the Start Parameter values provided in the latest RF_INTF_EXT_START_CMD (if any).

7.4.2 RF Interface Extension Stop

Table 83: Control Messages to Stop RF Interface Extensions

RF_INTF_EXT_STOP_CMD		
Payload Field(s)	**Length**	**Value/Description**
RF Interface Extension	1 Octet	See Table 135.
Stop Parameter Length	1 Octet	The length of the following Stop Parameter field (x).
Stop Parameter	x Octets	The stop parameters as defined for the respective RF Interface Extension

RF_INTF_EXT_STOP_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129

The RF_INTF_EXT_STOP_CMD SHALL NOT be sent unless the RF Interface Extension is started**.**

On execution of the Command the NFCC SHALL send RF_INTF_EXT_STOP_RSP to inform the DH that the NFCC has executed the Command. The Status SHALL be STATUS_OK.

7.5 RF Discovery Request from NFCEEs

This notification informs the DH of changes to the list of RF Discovery tasks requested on behalf of NFCEE(s) that are attached to the NFCC. Information is sent in this notification as a list of TLVs as defined in Table 85.

- If an attached NFCEE wishes to start using RF communication for a given combination of RF Protocol / RF Technology and Mode, a TLV is included in which the Type field is set to 0x00, and the value is set according to Table 86.
- If an attached NFCEE wishes to stop using RF communication for a given combination of RF Protocol / RF Technology and Mode, a TLV is included in which the Type field is set to 0x01, and the value is set according to Table 86.

This notification can be sent at any time after the first NFCEE Discovery has been run, even if RF Discovery is already in progress.

The NFCC SHALL consider any previously transmitted RF_NFCEE_DISCOVERY_REQ_NTF with a given NFCEE ID as discarded by the DH when the NFCEE with this NFCEE ID is disabled or unresponsive.

For HCI-NFCEEs the NFCC MAY determine the NFCEE RF Discovery requirements based on the opened pipes. Otherwise, the method the NFCC uses to find out the NFCEE's RF Discovery requirements is implementation specific.

The DH SHOULD take the NFCEE's request under consideration, based on its own requirements and requests for other NFCEEs. Therefore the action taken by the DH on receipt of this notification is implementation specific.

Table 84: Notification for RF Discovery Request from NFCEE

RF_NFCEE_DISCOVERY_REQ_NTF				
Payload Field(s)	**Length**	**Value/Description**		
Number Of Information Entries	1 Octet	The number of information entries to follow (n).		
Information Entry [1..n]	x+2 Octets	Type	1 Octet	One of the types defined in Table 85.
		Length	1 Octet	The length of Value (x).
		Value	x Octets	Value of the Information Entry.

Table 85: TLV Coding for RF Discovery Request from NFCEE

Type	Length	Value
0x00	3 Octets	Information about the particular discovery request in this TLV is to be added to the list, value field coded according to Table 86.
0x01	3 Octets	Information about the particular discovery request in this TLV is to be removed from the list, value field coded according to Table 86.
0x02-0x7F		RFU
0x80-0xFF		For proprietary use

Table 86: Value Field for RF Discovery Request Information

Payload Field(s)	Length	Value/Description
NFCEE	1 Octet	An NFCEE ID as defined in Table 116 The value of 0 (DH-NFCEE) SHALL NOT be used.
RF Technology and Mode	1 Octet	An RF Technology and Mode as defined in Table 131.
RF Protocol	1 Octet	An RF Protocol as defined in Table 133.

7.6 RF NFCEE Action

RF NFCEE Action is the mechanism used to indicate that an action involving one of the NFCEEs in the device has occurred that might be of interest to the DH.

Actions could be routing decisions made by the NFCC or the availability of application-level information about a transaction with a Remote NFC Endpoint.

For example, this indication could provide a mechanism for a User Interface application on the DH to perform any application specific behaviors based on the knowledge that a specific NFCEE or application on an NFCEE has been accessed by a Remote NFC Endpoint. For example, the User Interface application could display branding and/or request an action from a consumer.

This notification SHALL NOT be sent in states other than **RFST_LISTEN_ACTIVE**.

Table 87: Notification to Report an NFCEE Action

RF_NFCEE_ACTION_NTF		
Payload Field(s)	**Length**	**Value/Description**
NFCEE ID	1 Octet	An NFCEE ID as defined in Table 116. The value of 0x00 (DH-NFCEE ID) SHALL NOT be used.
Trigger	1 Octet	See Table 88.
Supporting Data Length	1 Octet	The length of Supporting Data field to follow (n)
Supporting Data	n Octets	Depends on Trigger

The Trigger value indicates the type of trigger that has caused this notification to be sent (as defined in Table 88).

Table 88: Trigger in NFCEE Action Notification

Trigger	Description	Supporting Data
0x00	[ISO/IEC_7816-4] SELECT command with an AID	The AID in the SELECT command.
0x01	Protocol-based Route Selection Process	The RF Protocol. See Table 133.
0x02	Technology-based Route Selection Process	The RF Technology. See Table 130.
0x03	System Code-based Route Selection Process	The SC in the received command.
0x04	APDU Pattern-based Route Selection Process	The reference data followed by the mask, as defined in Table 58.
0x05	Forced NFCEE Routing is used	The RF Technology. See Table 130.
0x06-0x0F	RFU	
0x10 – 0x7F	Application specific	Application specific. Could be an AID for an [ISO/IEC_7816-4] type application.
0x7F-0xFF	RFU	

If RF_NFCEE_ACTION is equal to 0x01, the following triggers apply:

- 0x00 – this trigger SHALL be sent by the NFCC when the NFCC is capable of determining the Application Identifier of the accessed application. In the case of [ISO/IEC_7816-4] SELECT commands (applies to NFC Forum Tag Type 4), the RF_NFCEE_ACTION_NTF Notification SHALL be sent for each such SELECT command received and the value of the Supporting Data SHALL contain the AID contained in the SELECT command. The NFCEE ID field SHALL identify the NFCEE on which the corresponding application is hosted.
- 0x01 – this trigger SHALL be sent when EE_ROUTE is set to a valid NFCEE ID during the Protocol-based Route Selection Process. The Supporting Data SHALL contain the corresponding RF Protocol. The NFCEE ID field SHALL identify the NFCEE to which the traffic is routed.
- 0x02 – this trigger SHALL be sent when EE_ROUTE is set to a valid NFCEE ID during the Technology-based Route Selection Process. The Supporting Data SHALL contain the corresponding RF Technology. The NFCEE ID field SHALL identify the NFCEE to which the traffic is routed.
- 0x03 - this trigger SHALL be sent when a CUP command is forwarded to an NFCEE that has a valid NFCEE ID most recently set to EE_ROUTE during the System Code-based Route Selection Process. The Supporting Data SHALL contain the corresponding SC. The NFCEE ID field SHALL identify the NFCEE to which the traffic is routed.
- 0x04 - this trigger SHALL be sent when EE_ROUTE is set to a valid NFCEE_ID during the APDU Pattern-based Route Selection Process. The Supporting Data SHALL contain the corresponding reference data and mask. The NFCEE ID field SHALL identify the NFCEE to which the traffic is routed.
- 0x05 – this trigger SHALL be sent when the first frame is received from the Remote NFC Endpoint after each RF Interface activation while Forced NFCEE Routing is enabled. The Supporting Data SHALL contain the corresponding RF Technology. The NFCEE ID field SHALL identify the NFCEE to which the traffic is routed.
- 0x10 – 0x7F – these triggers MAY be sent if and when the NFCEE provides the information to the NFCC. The manner in which the application on the NFCEE communicates with the NFCC to provide the information is outside the scope of this specification as is the content of the Supporting Data. The NFCEE ID field SHALL identify the NFCEE providing the information.

EE_ROUTE is a variable to indicate the route to an NFCEE. See Section 6.3.1 for details about the EE_ROUTE.

For all cases above, an RF_NFCEE_ACTION_NTF notification SHALL NOT be sent when the NFCEE ID is equal to 0x00 (DH-NFCEE ID).

The DH can configure whether the NFCC is allowed to send NFCEE Action notifications by setting the following configuration parameter:

Table 89: RF_NFCEE_ACTION configuration parameter

ID	Length	Value	Description
RF_NFCEE_ACTION	1 Octet	0x00	The NFCC SHALL NOT send RF_NFCEE_ACTION_NTF to the DH.
		0x01 (default)	The NFCC SHALL send RF_NFCEE_ACTION_NTF to the DH upon the triggers described in this section.
		0x02-0xFF	RFU

8 RF Interfaces

8.1 NFCEE Direct RF Interface

The NFCEE Direct RF Interface is a pseudo interface that is used when the NFCC in state **RFST_DISCOVERY** can determine that the RF communication has to be routed to an NFCEE connected to, or inside, the NFC Controller. One example for such a case is if an NFCEE is directly coupled to the RF (e.g. when the NFC Wired Interface (see [ISO/IEC_28361] is used). NFCEE Direct RF Interface cannot be used when any of the possible routing options are to the DH-NFCEE

The NFCEE Direct RF Interface does not enable NCI Data Message exchange between the DH and the NFCC (and as a consequence no communication between the DH and the Remote NFC Endpoint). Therefore this RF Interface does not define a Data Mapping or Discovery Configuration. The NFCEE Direct RF Interface can not be mapped to an RF Protocol.

The following sections apply for Poll Mode and Listen Mode.

8.1.1 Discovery and Interface Activation

When the DH has enabled an NFCEE and the NFCC, which is in the state **RFST_DISCOVERY**, determines that the RF communication has to be routed to an NFCEE, the NFCC sends an RF_INTF_ACTIVATED_NTF to the DH to indicate that this Interface has been activated.

8.1.2 Interface Deactivation

Using this interface deactivation cases with Deactivation Types ‘Sleep Mode’ or ‘Sleep_AF Mode’ SHALL NOT be allowed.

8.2 Frame RF Interface

Both the Poll-side and Listen-side Frame RF Interfaces provide access to the Payload of the RF frames exchanged between the NFC Forum device and a Remote NFC Endpoint. The RF frame formats are technology dependent. Any higher layer protocols (for example ISO-DEP or NFC-DEP) are handled on the DH. In addition, when using Frame RF Interface, the activation of the RF Interface does not always coincide with the completion of Device Activation. For the ISO-DEP Protocol, the RATS or ATTRIB commands/responses are not handled by the NFCC but are handled by the DH, and are sent over NCI as the Payload of Data Messages. The same is true for ATR_REQ/RES and PSL_REQ/RES when activating NFC-DEP Protocol.

All Protocols defined in Table 133 can be mapped to this Interface (see Section 6.2).

NOTE The NFC Forum Device needs to be fast enough to conform to the timing requirements of any higher layer protocol that is handled on the DH. Corresponding timings are defined in [DIGITAL] for ISO-DEP and NFC-DEP. One specific example of strict timing is the maximum response time for the RATS command in ISO-DEP, which is below 5ms.

8.2.1 Data Mapping between the DH and RF

The DH and the NFCC SHALL only use the Static RF Connection for data communication with a Remote NFC Endpoint.

The DH MAY send a Data Message to the NFCC according to Section 8.2.1.1. The NFCC SHALL populate an RF frame of the currently used Technology with this data and send the RF frame to the Remote NFC Endpoint.

When the NFCC receives an RF frame from the Remote NFC Endpoint, then the NFCC SHALL extract the Payload from the RF frame and send it as Payload of a Data Message to the DH according to Section 8.2.1.2.

NCI Segmentation and Reassembly MAY be applied to Data Messages in either direction.

The format of the Data in the Data message used for the Frame RF Interface (NFC-A / NFC-B / NFC-F / NFC-V) differs depending on the transmission direction of the message.

8.2.1.1 Data from the DH to RF

For NFC-A, NFC-B and NFC-V the Data Message SHALL correspond to the Payload of the Data and Payload Format as defined in [DIGITAL].

For NFC-F the Data Message SHALL correspond to the SoD and Payload of the Data and Payload Format as defined in [DIGITAL].

When the NFCC operates in Listen Mode, the DH responds to commands sent by the Remote NFC Endpoint after RF Interface Activation. If the DH does not have any response to send to a received command, the DH SHALL send an NCI Data Packet with the Payload Length equal to 0 within the maximum command waiting time of the currently used RF Protocol.

When the NFCC in Listen Mode receives an NCI Data Packet with the Payload Length equal to 0, the NFCC SHALL NOT send any RF Frame to the Remote NFC Endpoint.

After receiving a Data Message, the NFCC SHALL append the appropriate EoD and send the result in an RF Frame of the currently used technology to the Remote NFC Endpoint.

Figure 11, Figure 12 and Figure 13 illustrate the mapping between the Data Message Format and the RF frame for each Frame RF Interface when the RF frame is sent to the Remote NFC Endpoint.

NOTE These figures show the case when the NCI Segmentation and Reassembly feature is not used.

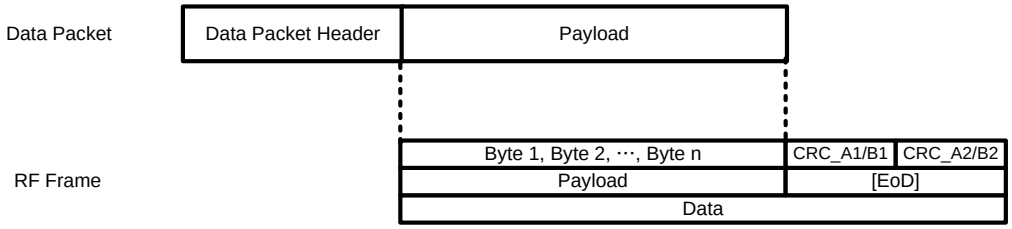

Figure 11: Format for Frame RF Interface (NFC-A) for Transmission

For NFC-A the Data Message SHALL NOT contain the parity bits used by Standard Frame. When sending the RF Frames, the NFCC SHALL insert the parity bits (as defined in [DIGITAL]).

For the Type 1 Tag Platform, and when it is in Poll Mode, the first octet of the Data Message SHALL consist of 0b as the most significant bit followed by the 7-bit Command Code. The RF Frame format is defined in [DIGITAL].

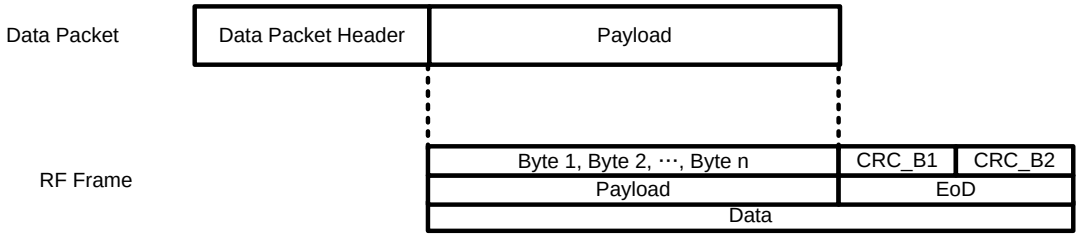

Figure 12: Format for Frame RF Interface (NFC-B) for Transmission

For NFC-B the Data Message SHALL NOT contain the start and stop bits used by the frame format. When sending the RF Frames, the NFCC SHALL insert the start and stop bits (as defined in [DIGITAL]).

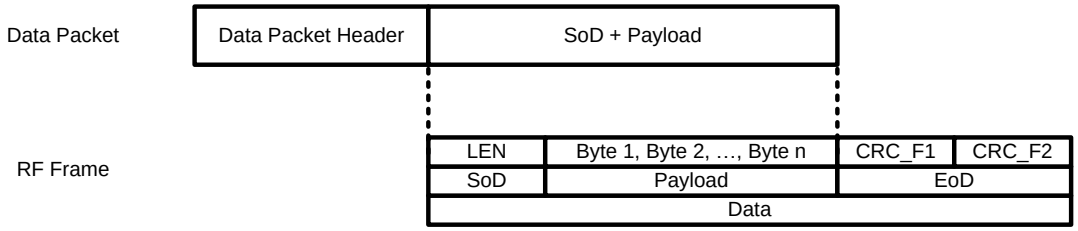

Figure 13: Format for Frame RF Interface (NFC-F) for Transmission

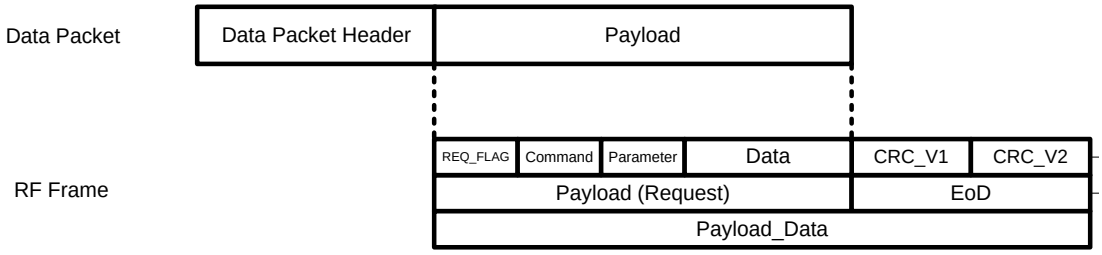

Figure 14: Format for Frame RF Interface (NFC-V) for Transmission

For NFC-V the Data Message SHALL NOT contain the Start of Frame and End of Frame patterns used by the frame format. When sending the RF Frames, the NFCC SHALL insert the Start of Frame and End of Frame patterns (as defined in [DIGITAL]). The DH SHALL neither transfer a Data message containing a Command payload exceeding the Max NFC-V RF Frame Size reported in CORE_INIT_RSP, nor generate a Command requesting a Payload response that would exceed the Max NFC-V RF Frame Size. Although the Frame RF interface is a transparent interface, for NFC-V, the following exception applies:

- The NFCC SHALL parse the bit OPTION_FLAG (bit b7 in the REQ_FLAG Byte, as defined in [T5TOP]) to check if this bit is set by the DH or not. If this bit requests the use of Special Frame for some commands as defined in [T5TOP]), then the NFCC SHALL use the Special Frame format for this command.

The DH SHALL force the bit High Data Rate (bit b2 in the REQ_FLAG Byte, as defined in [T5TOP])) to be equal to 1b (High Data rate). The DH SHALL also force the bit Single Subcarrier (bit b1 in the REQ_FLAG Byte, as defined in [T5TOP])) to be equal to 0b (single subcarrier only). This is done on the REQ_FLAG Byte transmitted on RF as shown on Figure 14 .

8.2.1.2 Data from RF to the DH

For NFC-A, NFC-B and NFC-V the Data Message SHALL correspond to the Payload of the Data and Payload Format defined in [DIGITAL] followed by a Status field of 1 octet.

For NFC-F the Data Message SHALL correspond to the SoD and Payload of the Data and Payload Format as defined in [DIGITAL] followed by a Status field of 1 octet.

After receiving an RF frame, the NFCC SHALL check and remove the EoD and send the result in a Data Message to the DH.

In case of an error the Data Message MAY consist of only a part of the Payload of the received RF frame but SHALL include the trailing Status field. A Data Message consisting of only the Status field is a valid message.

If the RF frame was received correctly, the NFCC SHALL set the Status field of Data Message to a value of STATUS_OK, except when the RF Frame is a Short Frame in NFC-A. In that particular case, the NFCC SHALL set the Status Field to a value of STATUS_OK_n_BIT, where ‘n’ is the number of bits in the Short Frame (between 1 and 7, as defined in [DIGITAL]).

NOTE For example, when the NFCC receives a T2T ACK/NACK response from a T2T Tag, it sets the Status Field to the value STATUS_OK_4_BIT.

If the NFCC detected an error when receiving the RF frame, the NFCC SHALL set the Status field of the Data Message to a value of RF_FRAME_CORRUPTED (see Table 129).

Figure 15, Figure 16 and Figure 17 illustrate the mapping of the RF frame received from the Remote NFC Endpoint to the Data Message format to be sent to the DH for each Technology.

NOTE These figures show the case when the NCI Segmentation and Reassembly feature is not used.

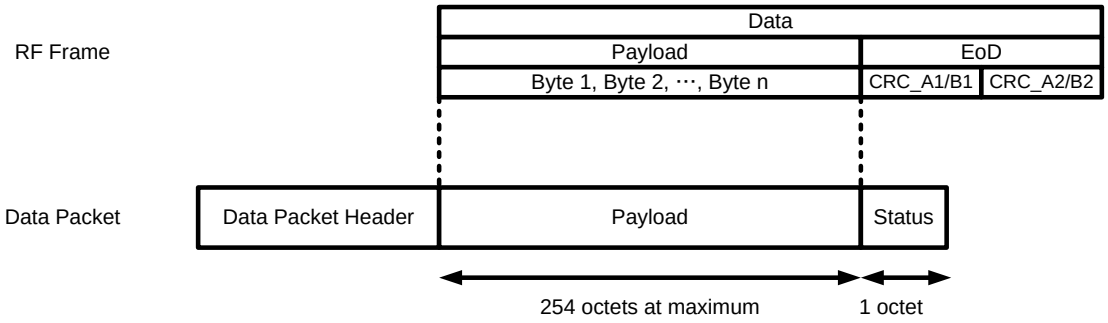

Figure 15**: Format for Frame RF Interface (NFC-A) for Reception**

For NFC-A the Data Message SHALL NOT contain the parity bits present in the Standard Frame and Bit Oriented Frame. When receiving RF Frames, the NFCC SHALL check and remove these parity bits (as defined in [DIGITAL]). When the NFCC receives a Short Frame on RF, having a length of n bits (n between 1 and 7, as defined in [DIGITAL]), the NFCC SHALL populate the n bits to the lower order bits of the first and only payload octet while each higher order bit is set to 0b.

For the Type 1 Tag Platform the RF Frame format is defined in [DIGITAL], where EoD consists of CRC_B1 and CRC_B2.

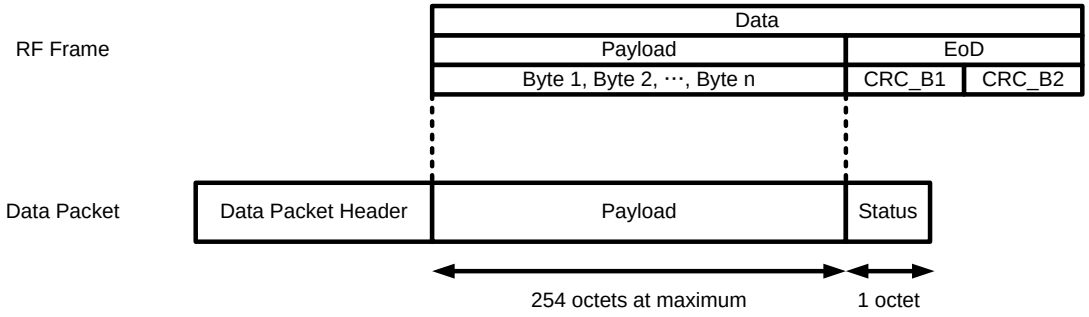

Figure 16: Format for Frame RF Interface (NFC-B) for Reception

For NFC-B the Data Message SHALL NOT contain the start and stop bits used by NFC-B frame format. When receiving the RF Frames, the NFCC SHALL remove the start and stop bits (as defined in [DIGITAL]).

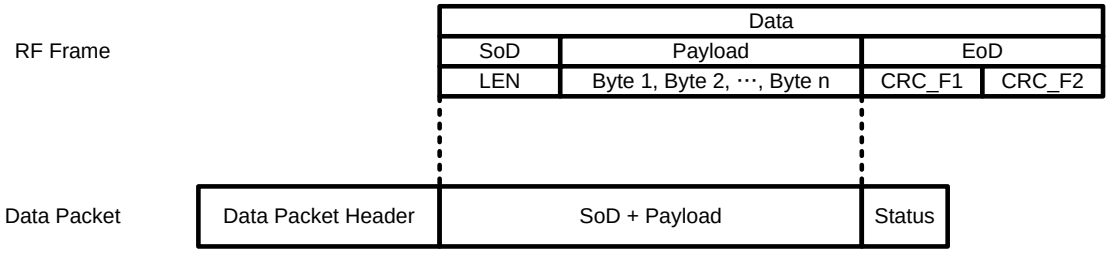

Figure 17: Format for Frame RF Interface (NFC-F) for Reception

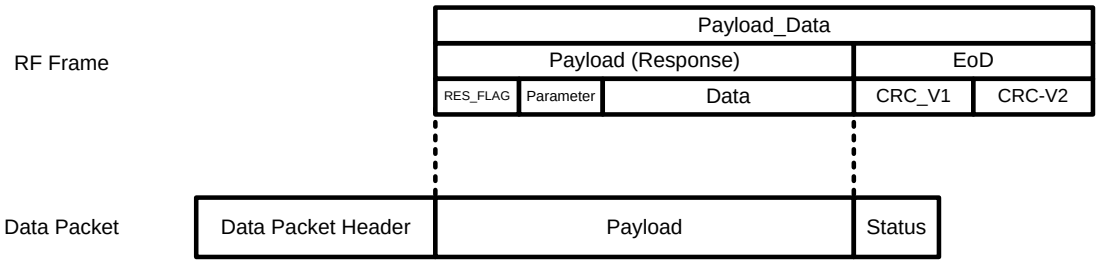

Figure 18: Format for Frame RF Interface (NFC-V) for Reception

For NFC-V the Data Message SHALL NOT contain the Start of Frame and End of Frame patterns used by the frame format. When Receiving the RF Frames, the NFCC SHALL remove the Start of Frame and End of Frame patterns (as defined in [DIGITAL]).

8.2.2 Frame RF Interface specific Control Messages

8.2.2.1 RF Communication Parameter Update

These Control Messages are used to update RF Communication parameters once the Frame RF Interface has been activated.

The RF_PARAMETER_UPDATE_CMD SHALL NOT be sent in states other than **RFST_POLL_ACTIVE** and **RFST_LISTEN_ACTIVE**.

Table 90: Control Messages for RF Parameter Update

RF_PARAMETER_UPDATE_CMD				
Payload Field(s)	**Length**	**Value/Description**		
Number of Parameters	1 Octet	The number of RF Communication Parameter fields to follow (n).		
RF Communication Parameter [1..n]	x+2 Octets	ID	1 Octet	The identifier of the RF Communication Parameter as defined in Table 91.
		Length	1 Octet	The length of Value (x).
		Value	x Octets	Value of the RF Communication Parameter.

RF_PARAMETER_UPDATE_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.
Number of Parameters	1 Octet	The number of RF Communication Parameter ID fields to follow (n). Value SHALL be 0x00 and no Parameter IDs listed unless Status = STATUS_INVALID_PARAM.
RF Communication Parameter ID [0..n]	1 Octet	The identifier of the invalid RF Communication Parameter. See Table 91 for a list of IDs.

Table 91: TLV Coding for RF Communication Parameter ID

Type	Length	Value
0x00	1 Octet	RF Technology and Mode, coded as defined in Table 131.
0x01	1 Octet	Transmit Bit Rate, coded as defined in Table 132.
0x02	1 Octet	Receive Bit Rate, coded as defined in Table 132.
0x03	1 Octet	NFC-B Data Exchange Configuration, coded as defined in Table 92.
0x04-0x7F		RFU
0x80-0xFF		Proprietary

If any of the RF Communication parameters listed in Table 91 to be used for Data Exchange differ from those used during Device Activation, the DH SHALL send the new values to the NFCC using an RF_PARAMETER_UPDATE_CMD.

Not all RF Communication parameter settings are permissible in all modes of operation; the DH is responsible for ensuring values sent to the NFCC are correct. There is no obligation for the NFCC to check whether a given parameter value is permitted.

The RF Technology and Mode parameter specifies the RF Technology and Mode that SHALL be used by the NFCC when transmitting and receiving. Refer to [DIGITAL] for permitted values of RF Technology and Mode for a given RF Interface activation.

The Transmit Bit Rate parameter specifies the bit rate that SHALL be used by the NFCC when transmitting. For a polling device this is the bit rate from poll to listen, and for a listening device this is the bit rate from listen to poll. Refer to [DIGITAL] for permitted values of bit rate for a given RF Interface activation.

The Receive Bit Rate parameter specifies the bit rate that SHALL be used by the NFCC when receiving. For a polling device this is the bit rate from listen to poll, and for a listening device this is the bit rate from poll to listen. Refer to [DIGITAL] for permitted values of bit rate for a given RF Interface activation.

The NFC-B Data Exchange Configuration parameter specifies a number of NFC-B related values. Not all values are relevant to a given operating mode. Values that are relevant to the current state SHALL be used by the NFCC as defined in [DIGITAL] during subsequent Data Exchange. They consist of Minimum TR0, Minimum TR1, Minimum TR2, Suppression of SoS, and Suppression of EoS. The format of the octet is defined below.

Table 92: NFC-B Data Exchange Configuration Parameter

	Bit Mask								**Description**
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	X	X							Minimum TR0 as defined in [DIGITAL]
			X	X					Minimum TR1 as defined in [DIGITAL]
					X				Suppression of EoS as defined in [DIGITAL]
						X			Suppression of SoS as defined in [DIGITAL]
							X	X	Minimum TR2 as defined in [DIGITAL]

On receipt of the RF_PARAMETER_UPDATE_CMD Command:

- If the NFCC is in state **RFST_POLL_ACTIVE**, it SHALL update the RF Communication parameters contained in the Command, before responding with an RF_PARAMETER_UPDATE_RSP.

NOTE For the NFC-DEP RF Protocol the RF Communication parameters need to be aligned with the parameter values contained in the PSL_REQ, and the update Command is issued after the PSL_RES is received from the Remote NFC Endpoint, but before the first DEP_REQ is sent.

- If the NFCC is in state **RFST_LISTEN_ACTIVE**, it SHALL respond with an RF_PARAMETER_UPDATE_RSP and then SHALL wait until it has sent the next RF Frame before updating the RF Communication parameters contained in the Command.

  NOTE For the NFC-DEP RF Protocol the RF Communication parameters need to be aligned with the parameter values contained in the PSL_REQ, and the update Command is issued after the PSL_REQ is received from the Remote NFC Endpoint, but before the PSL_RES is sent.

The Status field in the RF_PARAMETER_UPDATE_RSP indicates whether the setting of these RF Communication parameters was successful or not. A Status of STATUS_OK SHALL indicate that all RF Communication parameters have been set to these new values in the NFCC.

If the DH tries to set a parameter that is not applicable for the NFCC, the NFCC SHALL respond with an RF_PARAMETER_UPDATE_RSP with a Status field of STATUS_INVALID_PARAM and including one or more invalid RF Communication parameter ID(s). All other RF Communication parameters SHALL have been set to the new values in the NFCC.

8.2.2.2 Request Type 3 Tag Polling

In the **RFST_POLL_ACTIVE** state, the SENSF_REQ Command, which is also part of the T3T command set, cannot be handled by the DH over the Frame RF Interface, therefore specific Commands are introduced for this case.

The following Control Messages are used to request the NFCC to send a Type 3 Tag Polling Command.

Table 93: Control Messages to Request the NFCC to send a Type 3 Tag Polling Command

RF_T3T_POLLING_CMD		
Payload Field(s)	**Length**	**Value/Description**
SENSF_REQ_PARAMS	4 Octets	Byte 2-5 of SENSF_REQ as defined in [DIGITAL].

RF_T3T_POLLING_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

RF_T3T_POLLING_NTF				
Payload Field(s)	**Length**	**Value/Description**		
Status	1 Octet	See Table 129.		
Number of Responses	1 Octet	The number of Response fields to follow (n).		
Response [1..n]	m+1 Octets	Length	1 Octet	Length of following SENSF_RES field (m). Allowed values SHALL be 0x10 or 0x12. Other values are RFU.
		SENSF_RES	m Octets	Byte 2-17/19 of SENSF_RES Response as defined in [DIGITAL].

The DH is allowed to use this Command only if both:

- It is in the **RFST_POLL_ACTIVE** state.
- The activated RF Interface is the Poll-side Frame RF Interface for PROTOCOL_T3T.

After receiving a RF_T3T_POLLING_CMD and if above conditions are met, the NFCC SHALL answer with a RF_T3T_POLLING_RSP with a Status value of STATUS_OK and send a SENSF_REQ Command with Bytes 2-5 set as specified in the Command parameter to the RF field.

When the NFCC receives SENSF_RES Response(s) from the Remote NFC Endpoint (s), the NFCC SHALL populate the corresponding parameters of a RF_T3T_POLLING_NTF and send it with Status set to STATUS_OK to the DH. If no valid response is received, the NFCC SHALL send a RF_T3T_POLLING_NTF with Status set to STATUS_FAILED and containing no other Payload Fields.

If above conditions are not met, the NFCC SHALL send a RF_T3T_POLLING_RSP with a Status value of STATUS_SEMANTIC_ERROR. In this case the NFCC SHALL NOT send a RF_T3T_POLLING_NTF.

8.2.3 Poll-side Frame RF Interface Management

This Interface can be used if the NFC Forum Device is operating in Poll Mode (Reader/Writer Mode or Peer Mode – NFC-DEP Initiator).

8.2.3.1 Discovery Configuration

The Discovery configuration parameters defined in the following tables are relevant depending on the NFC technology used in Discovery (RF Technology and Mode in RF_DISCOVER_CMD). They MAY be changed from defaults by using the CORE_SET_CONFIG_CMD before moving to state **RFST_DISCOVERY**.

- Table 24: Discovery Configuration Parameters for Poll A
- Table 25: Discovery Configuration Parameters for Poll B
- Table 27: Discovery Configuration Parameters for Poll F
- Table 31: Poll Mode Discovery Configuration Parameters for Active Mode

For Active Communication Mode the parameters PN_ATR_REQ_GEN_BYTES and PN_ATR_REQ_CONFIG are also applicable when using this RF Interface.

For Active Communication Mode the NFCC SHALL set DID_i of the ATR_REQ Command to the value 0 (as [DIGITAL] mandates this configuration for Active Communication Mode).

8.2.3.2 Discovery and Interface Activation

To enable Poll Mode, the DH sends the RF_DISCOVER_CMD to the NFCC containing at least one configuration for a Poll Mode RF Technology and Mode.

In the case in which multiple Remote NFC Endpoints are detected and the DH has selected the NFC Endpoint to be used, or in the case that only a single Remote NFC Endpoint is detected, then the NFCC sends an RF_INTF_ACTIVATED_NTF to the DH to indicate that this Interface has been activated.

The protocol activation is fully under the control of the DH when the Frame RF Interface is used. Therefore for all RF Technologies the RF_INTF_ACTIVATED_NTF SHALL NOT contain any Activation Parameters.

8.2.3.3 Interface Deactivation

The deactivation cases for the Poll-side Frame RF Interface are described in Section 5.2 for **RFST_POLL_ACTIVE**.

The DH is responsible for sending the necessary deactivation commands before RF_DEACTIVATE_CMD.

8.2.3.4 Failures during Data Exchange

Even if there are any failures during data exchange, the NFCC SHALL NOT send any CORE_INTERFACE_ERROR_NTF to the DH. The DH itself identifies TRANSMISSION ERROR, PROTOCOL ERROR, or TIMEOUT ERROR in communication with the Remote NFC Endpoint.

The DH MAY deactivate the RF Interface when it identifies such errors.

8.2.4 Listen-side Frame RF Interface Management

This Interface can be used if the NFC Forum Device is operating in Listen Mode (Card Emulation Mode or Peer Mode – NFC-DEP Target).

8.2.4.1 Discovery Configuration

The Discovery configuration parameters defined in the following tables are relevant depending on the NFC technology used in Discovery (RF Technology and Mode in RF_DISCOVER_CMD). They MAY be changed from defaults by using the CORE_SET_CONFIG_CMD before moving to state **RFST_DISCOVERY** state.

- Table 33: Discovery Configuration Parameters for Listen A
- Table 35: Discovery Configuration Parameters for Listen B
- Table 40: Discovery Configuration Parameters for Listen T3T
- Table 44: Discovery Configuration Parameters for Listen NFC-DEP (applicable only for Active Communication Mode when using this RF Interface)

In the case of NFC Forum Type 4 Tag Emulation by the DH, the DH sends the CORE_SET_CONFIG_CMD to configure the Listen A Parameters and/or the Listen B Parameters as defined in Table 33 and Table 35.

In the case of NFC Forum Type 3 Tag Emulation by the DH, the DH sends the CORE_SET_CONFIG_CMD to configure the Listen F Parameters as defined in Table 40.

The RF_SET_LISTEN_MODE_ROUTING_CMD MAY be used to route the received data from the Remote NFC Endpoint to specific NFCEEs, which will in this case include routing some or all received data to the DH (for example, if an NFC Forum Type 4 Tag is being emulated by an NFCEE on the DH.)

8.2.4.2 Discovery and Interface Activation

To enable Listen Mode, the DH sends the RF_DISCOVER_CMD to the NFCC containing at least one configuration for a Listen Mode RF Technology and Mode.

When the NFCC has, based on the communication with the Remote NFC Endpoint (see [ACTIVITY]), determined whether to activate the Frame RF Interface, the NFCC sends the RF_INTF_ACTIVATED_NTF to the DH to indicate that this Interface has been activated to be used for communication with the specified Remote NFC Endpoint.

To provide the RF Protocol information in the RF_INTF_ACTIVATED_NTF, the NFCC needs to recognize the corresponding protocol activation command (for example ATTRIB, RATS or ATR_REQ) before activating the Frame RF Interface and forwarding the command to the DH.When it uses the Active Communication Mode, the NFCC needs to wait for the next command following the initial ATR_REQ before activating the Frame RF Interface. This avoids unnecessary activation in case of ATR_RES collisions.

If the NFCC has not determined which protocol is being activated, the RF Protocol value SHALL be PROTOCOL_UNDETERMINED.

For Passive Communication Mode there are five different states in the Listen state machine (defined in [ACTIVITY]) from which the NFCC can activate the Frame RF Interface. These five “pre-activation” states are listed in the Table 94. Once in one of these pre-activation states, some commands received from the remote NFC Endpoint are managed by the NFCC, others are forwarded to and then managed by the DH. Table 94 details which commands the NFCC handles when using the Frame RF Interface in Listen Mode. Any other commands are forwarded to the DH.

Table 94: Pre-activation states and the split of commands between NFCC and DH

Technology	Pre-activation state	Commands handled by the NFCC
NFC-A	ACTIVE_A and ACTIVE_A*	SENS_REQ, ALL_REQ, SLP_REQ, SDD_REQ, SEL_REQ, Command with Transmission Error (as defined in [DIGITAL], e.g. CRC errors, Parity errors)
NFC-B	READY_B_DECL	SENSB_REQ, ALLB_REQ, SLPB_REQ, Command with Transmission Error (as defined in [DIGITAL], e.g. CRC errors)
NFC-F	IDLE and READY_F	SENSF_REQ Command with Transmission Error (as defined in [DIGITAL], e.g. CRC errors)

In Active Communication Mode, the only pre-activation state is IDLE in which the NFCC handles the ATR_REQ.

When the NFCC receives a command while it is in one of these pre-activation states:

- Based on the information in Table 94, if the command has to be managed by the DH and if configured accordingly, the NFCC SHALL activate the Frame RF Interface.
- In any other case, the NFCC SHALL not activate the Frame RF Interface.

The protocol activation is fully under the control of the DH when the Frame RF Interface is used, therefore for all RF Technologies the RF_INTF_ACTIVATED_NTF SHALL NOT contain any Activation Parameters.

8.2.4.3 Interface Deactivation

Additional rules apply for the following deactivation cases described in Section 5.2 for **RFST_LISTEN_ACTIVE**:

- RF_DEACTIVATE_CMD/RSP/NTF(Sleep Mode)

  Before sending the RF_DEACTIVATE_NTF, the NFCC SHALL move to the following state of the Listen Mode state machine defined in [ACTIVITY]

  - SLEEP_A when NFC-A is the technology currently in use
  - SLEEP_B when NFC-B is the technology currently in use

If the currently used technology is NFC-F, the NFCC SHALL respond with a RF_DEACTIVATE_RSP with Status set to STATUS_REJECTED, not send a RF_DEACTIVATE_NTF and keep the Frame RF Interface activated.

- RF_DEACTIVATE_CMD/RSP/NTF(Sleep_AF Mode)

Before sending the RF_DEACTIVATE_NTF, the NFCC SHALL move to the following state of the Listen Mode state machine defined in [ACTIVITY]

- SLEEP_AF when NFC-A or NFC-F is the technology currently in use

If the currently used technology is NFC-B, the NFCC SHALL respond with a RF_DEACTIVATE_RSP with Status set to STATUS_REJECTED, not send a RF_DEACTIVATE_NTF and keep the Frame RF Interface activated.

- RF_DEACTIVATE_NTF (Sleep Mode, Endpoint Request)

  After receiving a SLP_REQ or sending a SLPB_RES the NFCC SHALL send the DEACTIVATE_NTF.

When using this RF Interface, the following deactivation cases described in Section 5.2 for **RFST_LISTEN_ACTIVE** SHALL NOT be allowed:

- RF_DEACTIVATE_NTF (Sleep_AF Mode, Endpoint Request)

8.2.4.4 Failures during Data Exchange

Even if there are any failures during data exchange, the NFCC SHALL NOT send any CORE_INTERFACE_ERROR_NTF to the DH.

The DH itself identifies TRANSMISSION ERROR and PROTOCOL ERROR in communication with the Remote NFC Endpoint from the Data in the Data Packet.

The DH MAY deactivate the RF Interface when it identifies such errors.

8.3 ISO-DEP RF Interface

Both the Poll-side and Listen-side ISO-DEP RF Interface provides access to the Payload of the ISO-DEP I-Blocks exchanged between the NFC Forum Device and a Remote NFC Endpoint. Using this interface, the DH does not need any knowledge about ISO-DEP block formats, however any higher layer protocol (e.g. based on 7816 APDU exchange) is handled on the DH.

The following Protocols can be mapped to this Interface (see Section 6.2):

- PROTOCOL_ISO_DEP.

8.3.1 Data Mapping between the DH and RF

The DH and the NFCC SHALL only use the Static RF Connection for data communication with a Remote NFC Endpoint.

NCI Segmentation and Reassembly MAY be applied to Data Messages in either direction.

8.3.1.1 Data from the DH to RF

When receiving a Data Message from the DH, the NFCC SHALL send the data contained in the Data Message as a Payload of an I-Block or as multiple Payloads of a chained series of I-Blocks to the Remote NFC Endpoint using the activated technology.

The last octet of the Data Packet with the Packet Boundary Flag set to 0b SHALL be the last byte of the Payload of an I-Block not indicating chaining sent by the NFCC to the Remote NFC Endpoint.

Figure 19 illustrates the mapping between the Data Packet and the RF Frame when the frame is sent to the Remote NFC Endpoint.

NOTE This figure shows the case when the NCI Segmentation and Reassembly feature is not used. However, ISO-DEP chaining is used when one Data Message is sent with multiple I-Blocks to the Remote NFC Endpoint. APDUs can be very large (e.g. several KBs). In this case the Data Message will be split into several Data Packets and the NFCC can already start sending the first ISO-DEP Blocks while receiving the remaining Data Packets of the Data Message.

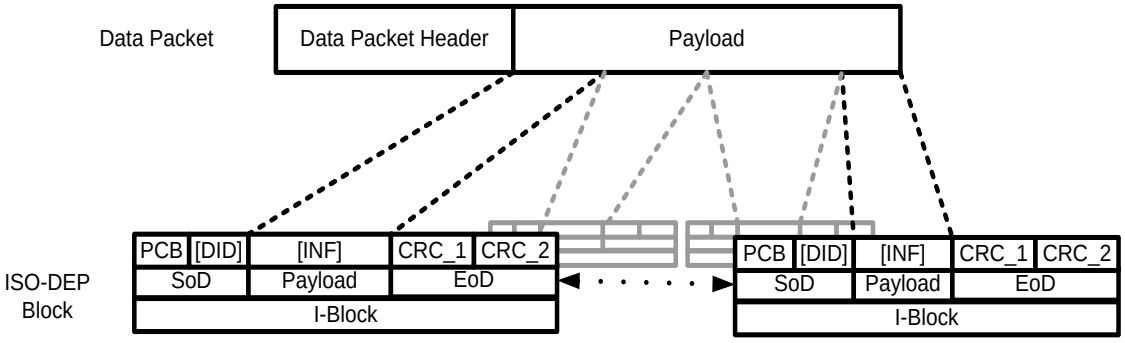

Figure 19: Format for ISO-DEP RF Interface for Transmission

8.3.1.2 Data from RF to the DH

The NFCC SHALL transfer the Payload of received I-Blocks to the DH.

The Payload of an ISO-DEP I-Block not indicating chaining or the combined Payload of a chained series of ISO-DEP I-Blocks SHALL be sent as one Data Message.

The last byte of the Payload of an I-Block not indicating chaining received by the NFCC from the Remote NFC Endpoint SHALL be the last octet of the Data Packet with Packet Boundary Flag set to 0b.

Figure 20 illustrates the mapping between the NCI Data Message format and the ISO-DEP I-blocks for the ISO-DEP RF Interface.

NOTE This figure shows the case when the NCI Segmentation and Reassembly feature is not used. However, ISO-DEP chaining is used where one Data Message is received by multiple I-Blocks from the Remote NFC Endpoint. APDUs can be very large (e.g. several KBs). In this case the Data Message will be split into several Data Packets and the NFCC can already start sending the first Data Packets to DH while receiving the remaining ISO-DEP Blocks.

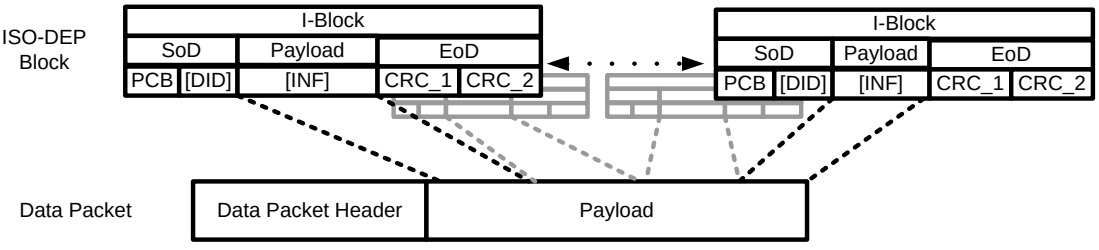

Figure 20: Format for ISO-DEP RF Interface for Reception

8.3.2 Poll-side ISO-DEP RF Interface Management

The Poll-side ISO-DEP RF Interface MAY be used for Reader/Writer Mode when the Remote NFC Endpoint supports ISO-DEP based on NFC-A or NFC-B.

8.3.2.1 Discovery Configuration

The Discovery configuration parameters defined in the following tables are relevant depending on the NFC technology used in Discovery (NFC-A or NFC-B as set by RF Technology and Mode in RF_DISCOVER_CMD). They MAY be changed from defaults by using the CORE_SET_CONFIG_CMD before moving to state **RFST_DISCOVERY**.

- Table 24: Discovery Configuration Parameters for Poll A
- Table 25: Discovery Configuration Parameters for Poll B
- Table 28: Discovery Configuration Parameters for ISO-DEP

8.3.2.2 Discovery and Interface Activation

To enable Poll Mode for ISO-DEP, the DH sends the RF_DISCOVER_CMD to the NFCC containing configurations with RF Technology and Mode values of NFC_A_PASSIVE_POLL_MODE and/or NFC_B_PASSIVE_POLL_MODE.

When the NFCC is ready to exchange data (that is, after receiving a response to the protocol activation command from the Remote NFC Endpoint), it sends the RF_INTF_ACTIVATED_NTF to the DH to indicate that this Interface has been activated to be used with the specified Remote NFC Endpoint.

Detailed ISO-DEP RF Interface activation handling in the NFCC

For NFC-A:

Following the anticollision sequence, if the Remote NFC Endpoint supports ISO-DEP Protocol, the NFCC sends the RATS Command to the Remote NFC Endpoint and after receiving the RATS response, the NFCC SHALL send the RF_INTF_ACTIVATED_NTF to the DH to indicate a Remote NFC Endpoint based on ISO-DEP has been activated.

For NFC-A the RF_INTF_ACTIVATED_NTF SHALL include the Activation Parameters defined in Table 95.

Table 95: Activation Parameters for NFC-A/ISO-DEP Poll Mode

Parameter	Length	Description
RATS Response Length	1 Octet	Length of RATS Response Parameter (n)
RATS Response	n Octets	All Bytes of the RATS Response as defined in [DIGITAL] starting from and including Byte 2.

For NFC-B:

Following the anticollision sequence, if the Remote NFC Endpoint supports ISO-DEP Protocol, the NFCC sends the ATTRIB command to the Remote NFC Endpoint and following receipt of the ATTRIB response, the NFCC SHALL send the RF_INTF_ACTIVATED_NTF to the DH to indicate a Remote NFC Endpoint based on ISO-DEP has been activated.

For NFC-B the RF_INTF_ACTIVATED_NTF SHALL include the Activation Parameters defined in Table 96.

Table 96: Activation Parameters for NFC-B/ISO-DEP Poll Mode

Parameter	Length	Description
ATTRIB Response Length	1 Octet	Length of ATTRIB Response Parameter (n)
ATTRIB Response	n Octets	ATTRIB Response as defined in [DIGITAL]

8.3.2.3 Interface Deactivation

Additional rules apply for the following deactivation cases described in Section 5.2 for **RFST_POLL_ACTIVE**:

- RF_DEACTIVATE_CMD/RSP/NTF(Idle Mode),
  RF_DEACTIVATE_CMD/RSP/NTF(Discovery)
  RF_DEACTIVATE_CMD/RSP/NTF(Sleep Mode).

  Before sending the RF_DEACTIVATE_NTF to the DH, the NFCC SHALL de-activate the Remote NFC Endpoint according to the De-activation rules for ISO-DEP specified in [DIGITAL].

When using this RF Interface, the following deactivation cases described in Section 5.2 for **RFST_POLL _ACTIVE** SHALL NOT be allowed:

- RF_DEACTIVATE_CMD/RSP/NTF(Sleep_AF Mode)

8.3.2.4 Failures during Data Exchange

If an ISO-DEP Unrecoverable Timeout Exception occurs, the NFCC SHALL send the CORE_INTERFACE_ERROR_NTF with the Status of RF_TIMEOUT_EXCEPTION. The NFCC SHALL accept all waiting time extension requests from the Remote NFC Endpoint. As the higher layer knows what the maximum expected time is for a given operation, the DH is responsible to abort the communication (for example, if the operation is taking too long), by sending RF_DEACTIVATE_CMD.

If an ISO-DEP Unrecoverable Transmission Exception occurs, the NFCC SHALL send the CORE_INTERFACE_ERROR_NTF with the Status of RF_TRANSMISSION_EXCEPTION.

If an ISO-DEP Unrecoverable Protocol Exception occurs, the NFCC SHALL send the CORE_INTERFACE_ERROR_NTF with the Status of RF_PROTOCOL_EXCEPTION.

8.3.2.5 ISO-DEP R(NAK) Presence Check

If the DH wants to use the R(NAK) presence check as defined in Method 2(a) of Part 4 of [ISO/IEC_14443], the following Control Messages are used:

Table 97: Control Messages to Request the NFCC to send an ISO-DEP R(NAK)

RF_ISO_DEP_NAK_PRESENCE_CMD		
Payload Field(s)	**Length**	**Value/Description**

RF_ISO_DEP_NAK_PRESENCE_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

RF_ISO_DEP_NAK_PRESENCE_NTF		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

When the DH wants to use this Command, it SHALL use this Command only if all of the following conditions are met:

- If it is in the **RFST_POLL_ACTIVE** state
- If the activated RF Interface is the Poll-side ISO-DEP RF Interface
- If there is no outstanding APDU command waiting for a response.

If above conditions are not met, the NFCC SHALL send a RF_ISO_DEP_NAK_PRESENCE_RSP with a Status value of STATUS_SEMANTIC_ERROR. In this case the NFCC SHALL NOT send a RF_ISO_DEP_NAK_PRESENCE_NTF.

After receiving a RF_ISO_DEP_NAK_PRESENCE_CMD and if above conditions are met, the NFCC SHALL answer with a RF_ISO_DEP_NAK_PRESENCE_RSP with a Status value of STATUS_OK and send a R(NAK) frame to the RF field, as defined in Method 2(a) of Part 4 of [ISO/IEC_14443].

When the NFCC receives the correct response frame from the Remote NFC Endpoint, the NFCC SHALL send RF_ISO_DEP_NAK_PRESENCE_NTF with Status set to STATUS_OK to the DH. If no valid response is received, the NFCC SHALL send a RF_ISO_DEP_NAK_PRESENCE_NTF with Status set to STATUS_FAILED.

If the DH has received RF_ISO_DEP_NAK_PRESENCE_RSP with STATUS_OK, it SHALL NOT send any APDU command until it has received the corresponding RF_ISO_DEP_NAK_PRESENCE_NTF.

8.3.3 Listen-side ISO-DEP RF Interface Management

This Listen-side ISO-DEP RF Interface MAY be used for Card Emulation Mode when the Remote NFC Endpoint uses ISO-DEP based on NFC-A or NFC-B.

In Listen Mode, if the NFCC receives an I-Block from the Remote NFC Endpoint with an empty Payload as part of the presence check mechanism defined in [ISO/IEC_14443], the NFCC SHALL respond with an I-Block and not forward the received I-Block to the DH.

8.3.3.1 Discovery Configuration

The Discovery configuration parameters defined in the following tables are relevant depending on the NFC technology used in Discovery (NFC-A or NFC-B as set by RF Technology and Mode in RF_DISCOVER_CMD). They MAY be changed from defaults by using the CORE_SET_CONFIG_CMD before moving to state **RFST_DISCOVERY**.

- Table 33: Discovery Configuration Parameters for Listen A
- Table 35: Discovery Configuration Parameters for Listen B
- Table 42: Discovery Configuration Parameters for Listen ISO-DEP

To use this Interface, at least one of the Parameters LA_SEL_INFO and LB_SENSB_INFO SHALL be configured to indicate ISO-DEP support.

In the case of Type 4 Tag Emulation being hosted on the DH, the DH sends the CORE_SET_CONFIG_CMD to configure the Listen A Parameters and/or the Listen B Parameters defined in Table 33 and Table 35, and to set the Selected Interface to ISO-DEP.

The DH MAY send the RF_SET_LISTEN_MODE_ROUTING_CMD to set the routing information on the NFCC that will route the received data to the specific NFCEEs and in this case to the DH.

8.3.3.2 Discovery and Interface Activation

To enable Listen Mode for ISO-DEP, the DH sends the RF_DISCOVER_CMD to the NFCC containing configurations with RF Technology and Mode values of NFC_A_PASSIVE_LISTEN_MODE and/or NFC_B_PASSIVE_LISTEN_MODE.

When the NFCC is ready to exchange data with the DH (that is, after receiving protocol activation command from the Remote NFC Endpoint), it sends the RF_INTF_ACTIVATED_NTF to the DH to indicate that this Interface has been activated to be used with the specified Remote NFC Endpoint.

Detailed ISO-DEP RF Interface activation handling in the NFCC:

For NFC-A:

Following the anticollision sequence, the NFCC sends the SEL_RES – indicating (as defined in [DIGITAL]) to the Remote NFC Endpoint that the NFC Forum Device might support the Type 4A Tag Platform. The NFCC then receives the RATS command and sends the RATS response to the Remote NFC Endpoint. The NFCC SHALL then send the RF_INTF_ACTIVATED_NTF to the DH to indicate that a Remote NFC Endpoint based on ISO-DEP has been detected.

For NFC-A the RF_INTF_ACTIVATED_NTF SHALL include the Activation Parameters defined in Table 98.

Table 98: Activation Parameters for NFC-A/ISO-DEP Listen Mode

Parameter	Length	Description
RATS Command Param	1 Octet	Byte 2 (‘PARAM’) of the RATS Command as defined in [DIGITAL]

For NFC-B:

Following the anticollision sequence, the NFCC sends the SENSB_RES to the Remote NFC Endpoing, indicating whether the NFC Forum Device supports the Type 4B Tag Platform (bit 1 = 1b in the Protocol Type) . The NFCC then receives the ATTRIB Command and sends the ATTRIB Response to the Remote NFC Endpoint. The NFCC SHALL then send the RF_INTF_ACTIVATED_NTF to the DH to indicate that a Remote NFC Endpoint based on ISO-DEP has been detected.

For NFC-B, the RF_INTF_ACTIVATED_NTF SHALL include the Activation Parameters defined in Table 99.

Table 99: Activation Parameters for NFC-B/ISO-DEP Listen Mode

Parameter	Length	Description
ATTRIB Command Length	1 Octet	Length of ATTRIB Command Parameter (n)
ATTRIB Command	n Octets	All Bytes of the ATTRIB Command as defined in [DIGITAL] starting from and including Byte 2.

8.3.3.3 Interface Deactivation

Additional rules apply for the following deactivation cases described in Section 5.2 for **RFST_LISTEN_ACTIVE**:

- RF_DEACTIVATE_NTF (Sleep Mode, Endpoint Request).

  After sending an S(DESELECT) response block to the Remote NFC Endpoint, the NFCC SHALL send the RF_DEACTIVATE_NTF.

When using this RF Interface, the following deactivation cases described in Section 5.2 for **RFST_LISTEN_ACTIVE** SHALL NOT be allowed:

- RF_DEACTIVATE_NTF (Discovery, Endpoint_Request)

- RF_DEACTIVATE_NTF (Sleep_AF Mode, Endpoint Request)
- RF_DEACTIVATE_CMD/RSP/NTF (Sleep_AF Mode)
- RF_DEACTIVATE_CMD/RSP/NTF (Sleep Mode).

8.3.3.4 Failures during Data Exchange

If an ISO-DEP Unrecoverable Protocol Exception as defined in [DIGITAL] occurs, the NFCC SHALL send the CORE_INTERFACE_ERROR_NTF with the Status of RF_PROTOCOL_EXCEPTION.

When the DH receives the CORE_INTERFACE_ERROR_NTF, the DH MAY initiate ISO-DEP RF Interface deactivation or perform some other error handling procedure.

8.4 NFC-DEP RF Interface

Both the Poll-side and Listen-side NFC-DEP RF Interfaces provide access to the Transport Data Bytes of the NFC-DEP frames exchanged between the NFC Forum Device and a Remote NFC Endpoint. Using this interface, the DH does not need to have any knowledge related to the NFC-DEP frame format, however any higher layer protocol (e.g. LLCP exchange) is handled on the DH.

The following Protocols can be mapped to this Interface (see Section 6.2):

- PROTOCOL_NFC_DEP.

8.4.1 Data Mapping between the DH and RF

The DH and the NFCC SHALL only use the Static RF Connection for data communication with a Remote NFC Endpoint.

NCI Segmentation and Reassembly MAY be applied to Data Messages in either direction.

8.4.1.1 Data from the DH to RF

When receiving a Data Message from the DH, the NFCC SHALL send the payload data contained in the Data Message as an information PDU transferred in the Transport Data Bytes of one or a chained series of DEP_REQ commands (if the NFCC is an NFC-DEP Initiator) or DEP_RES responses (if the NFCC is an NFC-DEP Target) to the Remote NFC Endpoint using the activated technology.

The last octet of a Data Packet with Packet Boundary Flag set to 0b SHALL be the last byte of the Transport Data Bytes of the DEP_REQ or DEP_RES frame not indicating chaining, sent by the NFCC to the Remote NFC Endpoint. Figure 21 illustrates the mapping between the Data Packet and the NFC-DEP – DEP_REQ frame when a frame is sent to the Remote NFC Endpoint.

NOTE This figure shows the case in which NCI Segmentation and Reassembly are not used. However, NFC-DEP chaining is employed; one Data Message is sent in multiple DEP_REQ frames to the Remote NFC Endpoint.

NOTE In a DEP_RES frame the first Byte will be 0xD5 and the second Byte 0x07.

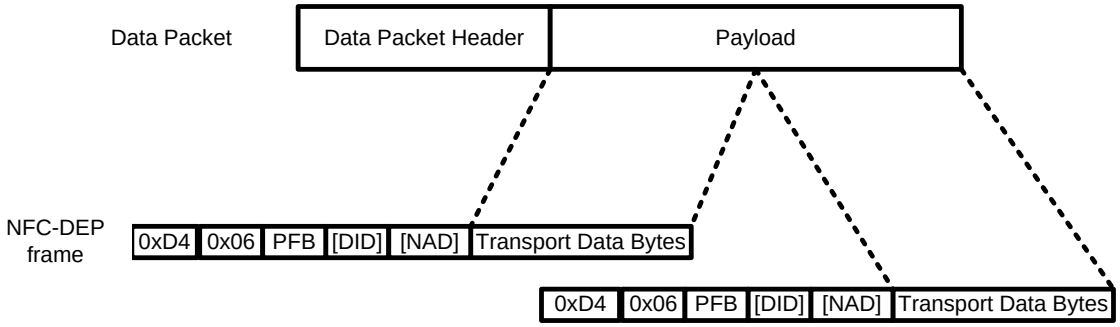

Figure 21: Format for NFC-DEP RF Interface for Transmission

8.4.1.2 Data from RF to the DH

The NFCC SHALL transfer the Information PDU received in the Transport Data Bytes of one or a chained series of DEP_RES responses (if the NFCC is an NFC-DEP Initiator) or DEP_REQ commands (if the NFCC is an NFC-DEP Target) to the DH.

The last byte of the Transport Data Bytes of a DEP_RES or DEP_REQ frame not indicating chaining, received by the NFCC from the Remote NFC Endpoint SHALL be the last octet of the Data Packet with the Packet Boundary Flag set to 0b.

Figure 22 illustrates the mapping between the Data Message format and the NFC-DEP – DEP_RES frame.

NOTE This figure shows the case in which the NCI Segmentation and Reassembly feature is not used. However, NFC-DEP chaining is used when one Data Message is received by multiple DEP_RES frames from the Remote NFC Endpoint.

NOTE In the DEP_REQ frame case the first Byte would be 0xD4 and the second Byte 0x06.

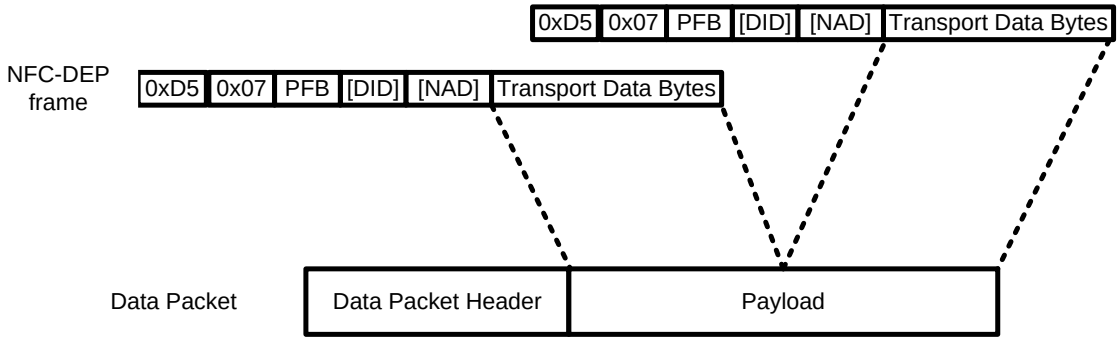

Figure 22: Format for NFC-DEP RF Interface for Reception

8.4.2 NFC-DEP RF Interface Configuration

The behavior of the NFC-DEP Protocol MAY be configured using CORE_SET_CONFIG_CMD indicating the following parameter:

Table 100: Specific Parameters for NFC-DEP RF Interface

ID	Length	Description
NFCDEP_OP	1 Octet	See Table 101

		Default : 0x1F

Table 101: NFC-DEP Operation Parameter

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	0	0	0						RFU
				X					If set to 1b, **WT** at target SHALL use the value of 10 or less., Otherwise **WT** at target SHALL use the value of $WT_{NFCDEP,MAX}$ or less
					X				If set to 1b, all PDUs indicating chaining (MI bit set) SHALL use the maximum number of Transport Data Bytes. Otherwise this restriction does not apply.
						X			If set to 1b, Information PDU with no Transport Data Bytes SHALL NOT be sent. Otherwise this restriction does not apply.
							X		If set to 1b, the NFC-DEP Initiator SHALL use the ATTENTION command only as part of the error recovery procedure described in [DIGITAL]. Otherwise this restriction does not apply.
								X	If set to 1b, the NFC-DEP Target SHALL NOT send RTOX requests. Otherwise this restriction does not apply.

This parameter SHALL only be configured when the NFCC is in **RFST_IDLE** state.

Some settings are only relevant for NFC-DEP Target or NFC-DEP Initiator respectively. The settings not matching the current role of the device SHALL be ignored.

NOTE These settings allow configuring the NFC-DEP Protocol to comply with the requirements stated in the NFC Forum Logical Link Control Protocol [LLCP] for the NFC-DEP Protocol binding.

8.4.3 Poll-side NFC-DEP RF Interface Management

The Poll-side NFC-DEP RF Interface MAY be used when the device operates as an NFC-DEP Initiator when in Peer Mode and the Remote NFC Endpoint supports NFC-DEP based on NFC-A or NFC-F.

8.4.3.1 Discovery Configuration

The Discovery configuration parameters defined in the following tables are relevant. They MAY be changed from defaults by using the CORE_SET_CONFIG_CMD before moving to state **RFST_DISCOVERY**.

- Table 24: Discovery Configuration Parameters for Poll A (if the RF_DISCOVER_CMD contains a Configuration for NFC-A)
- Table 27: Discovery Configuration Parameters for Poll F (if the RF_DISCOVER_CMD contains a Configuration for NFC-F)
- Table 29: Discovery Configuration Parameters for Poll NFC-DEP
- Table 31: Poll Mode Discovery Configuration Parameters for Active Mode

The NFCC SHALL set DID_i of the ATR_REQ Command to the value 0, since the NFC-DEP RF Interface does not provide a mechanism that would allow it to communicate with multiple activated targets when using the NFC-DEP Protocol.

8.4.3.2 Discovery and Interface Activation

To enable Poll Mode for NFC-DEP, the DH sends the RF_DISCOVER_CMD to the NFCC containing configurations with RF Technology and Mode values of NFC_A_PASSIVE_POLL_MODE, NFC_F_PASSIVE_POLL_MODE and/or NFC_ACTIVE_POLL_MODE.

When the NFCC is ready to exchange data (that is, after successful protocol activation), it SHALL send the RF_INTF_ACTIVATED_NTF to the DH to indicate that the NFC-DEP Protocol has been activated as follows:

Following the Passive Communication Mode anticollision sequence, if the Remote NFC Endpoint supports NFC-DEP Protocol, the NFCC sends an ATR_REQ with PN_ATR_REQ_GEN_BYTES configured during Discovery Configuration to the Remote NFC Endpoint.

For Active Communication Mode a corresponding ATR_REQ is sent as part of the initialization and protocol activation sequence.

When an ATR_RES is received from the Remote NFC Endpoint, the NFCC SHALL forward the ATR_RES to the DH in the RF_INTF_ACTIVATED_NTF (using the Activation Parameters in Passive Communication Mode or the RF Technology Specific Parameters in Active Communication Mode). Based on the current bit rate, the current length reduction and the configured PN_NFC_DEP_PSL value, the NFCC determines whether to send a PSL_REQ before sending the RF_INTF_ACTIVATED_NTF.

The NFCC SHALL determine whether the LLCP Link Activation Procedure has been performed by checking if the General Bytes fields of the ATR_REQ and the ATR_RES start with the LLCP magic number (see [LLCP]). If the magic number is present in both fields, the NFCC SHALL assume that LLCP Link Activation Procedure has been performed, SHALL ignore the NFCDEP_OP configuration and act as defined by the NFCDEP_OP default values.

If PSL_RES is valid, the values in the four Data Exchange parameters of the RF_INTF_ACTIVATED_NTF SHALL reflect the technology, bit rates and length reduction value used for data exchange that were set with the PSL_REQ. Otherwise they SHALL indicate the technology, bit rates and length reduction value used during the protocol activation.

If using Active Communication Mode the RF_INTF_ACTIVATED_NTF SHALL NOT include any Activation Parameters.

If using Passive Communication Mode, the RF_INTF_ACTIVATED_NTF SHALL include the Activation Parameters defined in Table 102.

Table 102: Activation Parameters for NFC-DEP Poll Mode

Parameter	Length	Description
ATR_RES Response Length	1 Octet	Length of ATR_RES Command Parameter (n)
ATR_RES Response	n Octets	All Bytes of ATR_RES Response starting from and including Byte 3 as defined in [DIGITAL]
Data Exchange Length Reduction	1 Octet	Length Reduction that will be used for Data Exchange in both receive and transmit directions for NFC-DEP RF Interface when the PSL_REQ and PSL_RES are used. See Table 137.

8.4.3.3 Interface Deactivation

Additional rules apply for the following deactivation cases described in Section 5.2 for **RFST_POLL_ACTIVE**:

- RF_DEACTIVATE_CMD/RSP/NTF(Idle Mode), RF_DEACTIVATE_CMD/RSP/NTF(Discovery)

  Before sending the RF_DEACTIVATE_NTF to the DH, the NFCC SHALL release the Remote NFC Endpoint by sending an NFC-DEP Release Request (RLS_REQ) to the Remote NFC Endpoint (as specified in [DIGITAL]).

- RF_DEACTIVATE_CMD/RSP/NTF(Sleep_AF Mode) when using Passive Communication Mode

  Before sending the RF_DEACTIVATE_NTF to the DH, the NFCC SHALL deselect the Remote NFC Endpoint by sending an NFC-DEP Deselect Request (DSL_REQ) to the Remote NFC Endpoint (as specified in [DIGITAL]).

When using this RF Interface, the following deactivation cases described in Section 5.2 for **RFST_POLL_ACTIVE** SHALL NOT be allowed:

- RF_DEACTIVATE_CMD/RSP/NTF(Sleep Mode)
- RF_DEACTIVATE_CMD/RSP/NTF(Sleep_AF Mode) when using Active Communication Mode.

8.4.3.4 Failures during Data Exchange

If an NFC-DEP Unrecoverable Timeout Exception as defined in [DIGITAL] occurs, the NFCC SHALL send the CORE_INTERFACE_ERROR_NTF with the Status of RF_TIMEOUT_EXCEPTION.

If an NFC-DEP Unrecoverable Transmission Exception as defined in [DIGITAL] occurs, the NFCC SHALL send the CORE_INTERFACE_ERROR_NTF with the Status of RF_TRANSMISSION_EXCEPTION.

If an NFC-DEP Unrecoverable Protocol Exception as defined in [DIGITAL] occurs, the NFCC SHALL send the CORE_INTERFACE_ERROR_NTF with the Status of RF_PROTOCOL_EXCEPTION.

8.4.4 Listen-side NFC-DEP RF Interface Management

The Listen-side NFC-DEP RF Interface MAY be used when the device operates as an NFC-DEP Target in Peer Mode and the Remote NFC Endpoint supports NFC-DEP based on NFC-A or NFC-F.

8.4.4.1 Discovery Configuration

The Discovery configuration parameters defined in the following tables are relevant. They MAY be changed from defaults by using the CORE_SET_CONFIG_CMD before moving to state **RFST_DISCOVERY**.

- Table 33: Discovery Configuration Parameters for Listen A (if the RF_DISCOVER_CMD contains a Configuration for NFC-A)
- Table 38: Discovery Configuration Parameters for Listen F
- Table 44: Discovery Configuration Parameters for Listen NFC-DEP.

When this Interface is used for Passive Mode Communication, the DH SHOULD configure the parameters LA_SEL_INFO (see Table 33) to indicate NFC-DEP support and SHALL configure the LF_PROTOCOL_TYPE (seeTable 38) to indicate NFC-DEP support.

8.4.4.2 Discovery and Interface Activation

To enable Listen Mode for NFC-DEP, the DH sends the RF_DISCOVER_CMD to the NFCC containing configurations with RF Technology and Mode values of NFC_A_PASSIVE_LISTEN_MODE, NFC_F_PASSIVE_LISTEN_MODE and/or NFC_ACTIVE_LISTEN_MODE.

When the NFCC is ready to exchange data with the DH (that is, after successful protocol activation), it SHALL send the RF_INTF_ACTIVATED_NTF to the DH to indicate that the NFC-DEP Protocol has been activated as follows:

When an ATR_REQ has been received from the Remote NFC Endpoint, the NFCC SHALL send an ATR_RES to the Remote NFC Endpoint with LN_ATR_RES_GEN_BYTES configured during Discovery Configuration, but then wait until it receives either a PSL_REQ or a first command. It SHALL then forward the ATR_REQ and the updated data rate and technology information to the DH in the RF_INTF_ACTIVATED_NTF (using the Activation Parameters in Passive Communication Mode or the RF Technology Specific Parameters in Active Communication Mode).

The NFCC SHALL determine whether the LLCP Link Activation Procedure has been performed by checking if the General Bytes fields of the ATR_REQ and the ATR_RES start with the LLCP magic number (see [LLCP]). If the magic number is present in both fields, the NFCC SHALL assume that LLCP Link Activation Procedure has been performed, SHALL ignore the NFCDEP_OP configuration and act as defined by the NFCDEP_OP default values.

If using Active Communication Mode the RF_INTF_ACTIVATED_NTF SHALL NOT include any Activation Parameters.

If using Passive Communication Mode, for NFC-A and NFC-F the RF_INTF_ACTIVATED_NTF SHALL include the Activation Parameters defined in Table 103.

Table 103: Activation Parameters for NFC-DEP Listen Mode

Parameter	Length	Description
ATR_REQ Command Length	1 Octet	Length of ATR_REQ Command Parameter (n)
ATR_REQ Command	n Octets	All Bytes of the ATR_REQ Command as defined in [DIGITAL] starting from and including Byte 3.
Data Exchange Length Reduction	1 Octet	Length Reduction that will be used for Data Exchange in both receive and transmit directions for NFC-DEP RF Interface when the PSL_REQ and PSL_RES are used. See Table 137.

8.4.4.3 Interface Deactivation

Additional rules apply for the following deactivation cases described in Section 5.2 for **RFST_LISTEN_ACTIVE**:

- RF_DEACTIVATE_NTF (Sleep_AF Mode, Endpoint Request)

  After sending a Deselect response (DSL_RES) to the Remote NFC Endpoint, the NFCC SHALL send the DEACTIVATE_NTF.

- RF_DEACTIVATE_NTF (Discovery, Endpoint_Request)

  After sending a Release response (RLS_RES) to the Remote NFC Endpoint, the NFCC SHALL send the DEACTIVATE_NTF.

When using this RF Interface, the following deactivation cases described in Section 5.2 for **RFST_LISTEN_ACTIVE** SHALL NOT be allowed:

- RF_DEACTIVATE_NTF (Sleep Mode, Endpoint Request)
- RF_DEACTIVATE_CMD/RSP/NTF (Sleep Mode)
- RF_DEACTIVATE_CMD/RSP/NTF (Sleep_AF Mode).

8.4.4.4 Failures during Data Exchange

If an NFC-DEP Unrecoverable Protocol Exception [DIGITAL] occurs, the NFCC SHALL send the CORE_INTERFACE_ERROR_NTF with the Status of RF_PROTOCOL_EXCEPTION.

When the DH receives the CORE_INTERFACE_ERROR_NTF, the DH MAY initiate NFC-DEP RF Interface deactivation or perform some other error handling procedure.

8.5 NDEF RF Interface

The NDEF RF Interface allows an NFC Forum Device to interact with an NFC Forum Tag by allowing the DH to read and write a complete NDEF Message in byte form. The Discovery process provides the DH with the current life cycle of the tag. If allowed, the DH can instruct the NFCC to read an existing NDEF Message from the tag, or to write a new NDEF Message to the tag. It can also change the life cycle state of the tag by locking it for writing

For a Type 1 Tag, Type 2 Tag or Type 5 Tag the NFCC uses the procedures in [T1TOP], [T2TOP] or [T5TOP] to interact with the Capability Container bytes and the NDEF Message TLV on the Remote NFC Endpoint.

For a Type 3 Tag the NFCC uses the procedures in [T3TOP] to interact with the Attribute Information Block and the Blocks assigned for NDEF storage on the Remote NFC Endpoint.

For a Type 4 Tag the NFCC uses the procedures in [T4TOP] to interact with the Capability Container File and the NDEF File on the Remote NFC Endpoint.

The NDEF RF Interface is not applicable to the Listen side. The following RF Protocols can be mapped to the NDEF RF Interface in Poll Mode:

- PROTOCOL_NDEF.

NOTE An attempt to activate NDEF RF Interface is only made if this mapping exists in the RF Interface Mapping Configuration, as defined in Section 6.2.

8.5.1 NCI Data Message Format

When the NDEF RF Interface is used, Data Messages exchanged over the Static RF Connection are used to manage Tag Operations, and to provide resultant information and status. The payload of the Data Message from DH to NFCC consists of a Command field, which might be followed by Length and Information fields. The payload of the Data Message from NFCC to DH consists of a Status field, which might be preceded by Length and Information fields.

Table 104: Data Message from DH to NFCC Payload Format

Payload Field(s)	Length	Value/Description
Command	1 Octet	The NDEF access command. This field SHALL contain one of the NDEF access command values defined in Table 105.
Length	0 or 4 Octets	If the command value in the Command field has one or more parameters, the Length field SHALL be 4 octets, representing a 32-bit unsigned integer that specifies the total length in octets of the Information field. Transmission order SHALL be most significant octet first. Otherwise, the Length field SHALL not be present.
Information	n Octets	If the command value in the Command field has one or more parameters, the Information field SHALL contain the parameters in the order defined for the value of the Command field. The Information field is omitted if the value of the Length field is zero. Otherwise, the Information field SHALL not be present.

Table 105: NDEF Access Command Values

NDEF access command value	Definition
0x00	NDEF_OPERATION_GET
0x01	NDEF_OPERATION_PUT
0x02	NDEF_OPERATION_WRITE_LOCK
0x03-0xFF	RFU

Table 106: Data Message from NFCC to DH Payload Format

Payload Field(s)	Length	Value/Description
Length	0 or 4 Octets	If the response to the Command has one or more parameters, the Length field SHALL be 4 octets, representing a 32-bit unsigned integer that specifies the total length in octets of the Information field. Transmission order SHALL be most significant octet first. Otherwise, the Length field SHALL not be present.
Information	n Octets	If the response to the Command has one or more parameters, the Information field SHALL contain the parameters in the order defined for the response to the Command. The Information field is omitted if the value of the Length field is zero. Otherwise, the Information field SHALL not be present.
Status	1 Octet	The NDEF access status. This field SHALL contain one of the NDEF access status values defined in Table 107.

Table 107: NDEF Access Status Values

NDEF access status value	Definition
0x00	NDEF_OPERATION_SUCCEEDED
0x01	NDEF_OPERATION_INVALID
0x02	NDEF_OPERATION_FAILED
0x03	NDEF_OPERATION_DISALLOWED
0x04	NDEF_OPERATION_OVERFLOW
0x05-0xFF	RFU

8.5.1.1 NDEF Get

NDEF Get is used to retrieve a complete NDEF Message from an NFC Forum Tag. The DH SHALL only send an NDEF Get if it determines that the operation is allowed by the current life cycle state of the tag. To perform an NDEF Get, the DH SHALL send an NCI Data Message with the Command field set to the value NDEF_OPERATION_GET, and no parameters.

When the NFCC receives a valid NDEF Get, it uses the procedures defined in the appropriate tag operation specification to read the NDEF Message TLV, Block, or File.

If the Remote NFC Endpoint is a Type 1 Tag, then the NFCC SHALL perform the following operations as defined in [T1TOP]:

- Read NDEF Message.

If the Remote NFC Endpoint is a Type 2 Tag, then the NFCC SHALL perform the following operations as defined in [T2TOP]:

- NDEF Read Procedure.

If the Remote NFC Endpoint is a Type 3 Tag, then the NFCC SHALL perform the following operations as defined in [T3TOP]:

- Read NDEF Message.

If the Remote NFC Endpoint is a Type 4 Tag, then the NFCC SHALL perform the following operations as defined in [T4TOP]:

- NDEF Read Procedure.

If the Remote NFC Endpoint is a Type 5 Tag, then the NFCC SHALL perform the following operations as defined in [T5TOP]:

- NDEF Read Procedure.

The NFCC does not need to check that the NDEF Message from the tag is well formed. It is the responsibility of the DH to check and interpret the NDEF Message.

If the NDEF Get completes successfully, the NFCC SHALL send an NCI Data Message with a single parameter that represents the complete NDEF Message from the tag as a sequence of bytes, followed by the Status field set to the value NDEF_OPERATION_SUCCEEDED.

If the NFCC is unable to buffer the entire NDEF Message, then it SHALL use chained NCI Data Packets to send parts of the message to the DH as they are read. If the NDEF Get fails during this process, the NFCC SHALL send the bytes that were read, followed by the Status field set to the value NDEF_OPERATION_FAILED. In this case the Information field can contain less data bytes than indicated by the corresponding Length field.

The Status field is always the final byte of the NCI Data Packet that does not indicate chaining.

8.5.1.2 NDEF Put

NDEF Put is used to store a complete NDEF Message on an NFC Forum Tag. The DH SHALL only send an NDEF Put if it determines that the operation is allowed by the current life cycle state of the tag. To perform an NDEF Put, the DH SHALL send an NCI Data Message with the Command field set to the value NDEF_OPERATION_PUT, followed by a single parameter that represents the complete NDEF Message as a sequence of bytes. The NFCC does not need to check that the NDEF Message from the DH is well formed. It is the responsibility of the DH to ensure that the NDEF Message is valid.

When the NFCC receives a valid NDEF Put, it uses the procedures defined in the appropriate tag operation specification to update the NDEF Message TLV, Block or File.

If the Remote NFC Endpoint is a Type 1 Tag, then the NFCC SHALL perform the following operations as defined in [T1TOP]:

- NDEF Storage.

If the Remote NFC Endpoint is a Type 2 Tag, then the NFCC SHALL perform the following operations as defined in [T2TOP]:

- NDEF Write Procedure.

If the Remote NFC Endpoint is a Type 3 Tag, then the NFCC SHALL perform the following operations as defined in [T3TOP]:

- Write NDEF Message.

If the Remote NFC Endpoint is a Type 4 Tag, then the NFCC SHALL perform the following operations as defined in [T4TOP]:

- NDEF Update Procedure.

If the Remote NFC Endpoint is a Type 5 Tag, then the NFCC SHALL perform the following operations as defined in [T5TOP]:

- NDEF Write Procedure.

The NFCC SHALL leave all other TLVs, Blocks, or Files on the NFC Forum Tag unchanged. If the NDEF Put completes successfully, the NFCC SHALL send an NCI Data Message with no parameters, and the Status field set to the value NDEF_OPERATION_SUCCEEDED. On receiving this Data Message, the DH SHALL determine the current life cycle state of the tag if it has changed.

8.5.1.3 NDEF Write Lock

NDEF Write Lock is used to prevent further write access for the NDEF Message on the Remote NFC Endpoint. The DH SHALL only send an NDEF Write Lock command if it determines that the operation is allowed by the current life cycle state of the tag. To perform an NDEF Write Lock, the DH SHALL send an NCI Data Message with the Command field set to the value NDEF_OPERATION_WRITE_LOCK, and no parameters.

If the Remote NFC Endpoint is a Type 1 Tag, then the NFCC SHALL update the Remote NFC Endpoint according to the following section of [T1TOP]:

- READ ONLY State.

If the Remote NFC Endpoint is a Type 2 Tag, then the NFCC SHALL perform the following operations as defined in [T2TOP]:

- Transitions from READ/WRITE to READ-ONLY.

If the Remote NFC Endpoint is a Type 3 Tag, NDEF Write Lock is not allowed.

If the Remote NFC Endpoint is a Type 4 Tag, NDEF Write Lock is not allowed.

If the Remote NFC Endpoint is a Type 5 Tag, then the NFCC SHALL perform the following operations as defined in [T5TOP]:

- Transitions from READ/WRITE to READ-ONLY.

If the NDEF Write Lock completes successfully, the NFCC SHALL send an NCI Data Message with no parameters, and the Status field set to the value NDEF_OPERATION_SUCCEEDED. On receiving this Data Message, the DH SHALL determine the current life cycle state of the tag if it has changed.

8.5.2 NDEF RF Interface specific Control Messages

8.5.2.1 NDEF Abort

The RF_NDEF_ABORT_CMD SHALL NOT be sent in states other than RFST_POLL_ACTIVE.

Table 108: Control Messages for NDEF Abort

RF_NDEF_ABORT_CMD		
Payload Field(s)	**Length**	**Value/Description**
Empty payload		

RF_NDEF_ABORT_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

On receiving the RF_NDEF_ABORT_CMD, the NFCC SHALL NOT send any further commands to the Remote NFC Endpoint. It SHALL wait for response to the current command if already sent. The NFCC SHALL discard any data read from the tag before sending the RF_NDEF_ABORT_RSP.

To maintain the NCI flow control mechanism, if used, the NFCC SHALL give credits to the DH for any packets it discards without transmission, and for which it had not yet sent a credit to the DH.

8.5.3 NDEF RF Interface Management

The Poll-side NDEF RF Interface MAY be used when the device operates as a Reader/Writer and the Remote NFC Endpoint is an NFC Forum Tag.

8.5.3.1 Discovery Configuration

The Discovery configuration parameters defined in the following tables are relevant depending on the NFC technology used in Discovery (NFC-A, NFC-B, or NFC-F as set by RF Technology and Mode in RF_DISCOVER_CMD). They MAY be changed from defaults by using the CORE_SET_CONFIG_CMD before moving to state **RFST_DISCOVERY**.

- Table 24: Discovery Configuration Parameters for Poll A
- Table 25: Discovery Configuration Parameters for Poll B

- Table 27: Discovery Configuration Parameters for Poll F
- Table 28: Discovery Configuration Parameters for ISO-DEP
- Table 32: Discovery Configuration Parameters for Poll V

8.5.3.2 Discovery and Interface Activation

To enable Poll Mode for NDEF RF Interface, the DH sends the RF_DISCOVER_CMD to the NFCC containing configurations with RF Technology and Mode values of NFC_A_PASSIVE_POLL_MODE and/or NFC_B_PASSIVE_POLL_MODE and/or NFC_F_PASSIVE_POLL_MODE and/or NFC_V_PASSIVE_POLL_MODE.

When the NFCC has successfully completed protocol activation, it SHALL determine whether the Remote NFC Endpoint is an NFC Forum Tag.

If the RF Protocol is PROTOCOL_T1T, then the NFCC SHALL perform the following operations as defined in [T1TOP]:

- Identification as NFC Forum Type 1 Tag
- Version Treatment
- Confirmation of Presence of NDEF Message in Type 1 Tag

If the RF Protocol is PROTOCOL_T2T, then the NFCC SHALL perform the following operations as defined in [T2TOP]:

- Version Treatment
- NDEF Detection Procedure

If the RF Protocol is PROTOCOL_T3T, then the NFCC SHALL perform the following operations as defined in [T3TOP]:

- Version Treatment
- NDEF Detection

If the RF Protocol is PROTOCOL_ISO_DEP, then the NFCC SHALL perform the following operations as defined in [T4TOP]:

- Version Treatment
- NDEF Detection Procedure

If the RF Protocol is PROTOCOL_T5T, then the NFCC SHALL perform the following operations as defined in [T5TOP]:

- Version Treating
- NDEF Detection Procedure

If it detects the presence of an NDEF Message on the Remote NFC Endpoint, the NFCC SHALL send an RF_INTF_ACTIVATED_NTF to the DH with the Activation Parameters defined in as shown in Table 109.

Table 109: Activation Parameters for NDEF Poll Mode

Parameter	Length	Description
Life Cycle Information	1 Octet	The life cycle information of the NFC Forum Tag. See Table 110.
NDEF Message Length	4 Octets	Number of bytes in the NDEF Message that is present on the tag.
Maximum NDEF Message Length	4 Octets	Maximum number of bytes that are available to store an NDEF Message on the tag.

Table 110: Life Cycle Information

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	X								Write Lock permission 1b: Write Lock is allowed 0b: Write Lock is not allowed
		0	0	0	0				RFU
						X	X	X	Life Cycle state 000b: INITIALIZED 001b: READ_WRITE 010b: READ_ONLY 011b-111b: RFU

If it does not detect the presence of an NDEF Message on the Remote NFC Endpoint, then the use of NDEF RF Protocol is not possible. In this case, the NFCC SHALL restore the Remote NFC Endpoint to the state it would be in following protocol activation. The NFCC SHALL then proceed with its normal rules for determining the RF Interface Mapping as defined in Section 6.2, based on the RF Protocol supported by the Remote NFC Endpoint.

8.5.3.3 Interface Deactivation

The deactivation cases for the Poll-side NDEF RF Interface are specified in Section 5.2 for **RFST_POLL_ACTIVE**, with the addition of the following requirement. If the NFCC determines that the Remote NFC Endpoint is no longer present, it SHALL send RF_DEACTIVATE_NTF (Discovery, RF Link Loss) to the DH.

8.5.4 Failures during Data Exchange

If the NFCC receives an NCI Data Message that does not conform to the requirements in8.5.1, it SHALL send an NCI Data Message with no parameters, and the Status field set to the value NDEF_OPERATION_INVALID.

If an operation fails, and the NFCC is able to determine that it is because the operation is not allowed given the current life cycle information of the tag, it SHALL send an NCI Data Message with no parameters, and the Status field set to the value NDEF_OPERATION_DISALLOWED.

If an NDEF Put fails, and the NFCC is able to determine that it is because there is not enough space on the tag, it SHALL send an NCI Data Message with no parameters, and the Status field set to the value NDEF_OPERATION_OVERFLOW.

If an operation fails, and the NFCC is unable to determine the reason, it SHALL send an NCI Data Message with no parameters, and the Status field set to the value NDEF_OPERATION_FAILED.

9 RF Interface Extensions

9.1 Frame Aggregation RF Interface Extension

The Frame Aggregation RF Interface Extension offers the ability to combine multiple RF frames into a single NCI Data Message, as well as basic retry and timeout functions.

9.1.1 Startup conditions

After activation of the Frame RF Interface, the Frame Aggregation RF Interface Extension SHALL be in stopped state.

The Frame Aggregation RF Interface Extension can be started under the following conditions:

- The NFCC had shown support for the Frame Aggregation RF Interface Extension in the CORE_INIT_RSP.
- The Frame RF Interface is activated in POLL mode (state RFST_POLL_ACTIVE).
- The Remote NFC Endpoint is using one of the following RF Protocols:
    - PROTOCOL_T1T
    - PROTOCOL_T2T
    - PROTOCOL_T3T
    - PROTOCOL_T5T.
- The DH is not waiting for a response to a command sent to the Remote NFC Endpoint.

There are no relationships to other RF Interface Extensions defined in this document.

9.1.2 Starting the RF Interface Extension

The Frame Aggregation RF Interface Extension can be started by adding a corresponding RF Interface Extension field to the RF_INTF_EXT_START_CMD.

The DH can control certain aspects of the Frame Aggregation RF Interface Extension using the Start Parameter defined below.

In the RF Interface Extension field for the Frame Aggregation RF Interface Extension, the value of the Start Parameter Length field SHALL be 2 and the Start Parameter field SHALL contain a value according to Table 111.

Table 111: Frame Aggregation RF Interface Extension Start Parameter

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0		0	0	0	0				RFU
	X								NFCC Aggregation Enabled
						X	X	X	Retry Count (0 – 7)
Octet 1	X	X	X	X	X	X	X	X	Command Timeout (CTI)

The CTI field only applies to Aggregation TLV object type 0x00, since TLV object types 0x01 and 0x02 both contain their own timeouts. The actual timeout used by the NFCC for TLV object type 0x00 is CTI * 5ms. If CTI is equal to 0x00, the NFCC SHALL NOT monitor for a timeout.

If the NFCC Aggregation Enabled field is equal to 0b, the NFCC SHALL send each RF frame received from the Remote RF Endpoint to the DH in a separate NCI message, with no aggregation.

If the NFCC Aggregation Enabled field is equal to 1b, the NFCC MAY aggregate RF frames received from the Remote RF Endpoint into NCI messages for transmission to the DH.

The Retry Count applies to Aggregation TLV object types 0x00 and 0x01. If it is equal to 0, the NFCC SHALL NOT try to retransmit any RF frames for which it detects an error. Otherwise, the NFCC SHALL attempt to retry up to Retry Count times.

After the DH has sent RF_INTF_EXT_START_CMD, it SHALL NOT send any NCI Data Packet to the NFCC until it has received RF_INTF_EXT_START_RSP.

9.1.3 RF Interface Extension functionality

The definitions and requirements in this section SHALL apply only while the Frame Aggregation RF Interface Extensions is started.

9.1.3.1 NCI Data Message Format

All Data Messages exchanged over the Static RF Connection SHALL be composed of TLV objects, as defined in Table 112.

For Data Messages from the DH to RF the procedures described in Section 8.2.1.1 apply, with the "Data Message" being mapped to the RF_CMD field in Aggregation TLV objects of type 0x00, 0x01 and 0x02. Figure 23 shows such a scenario.

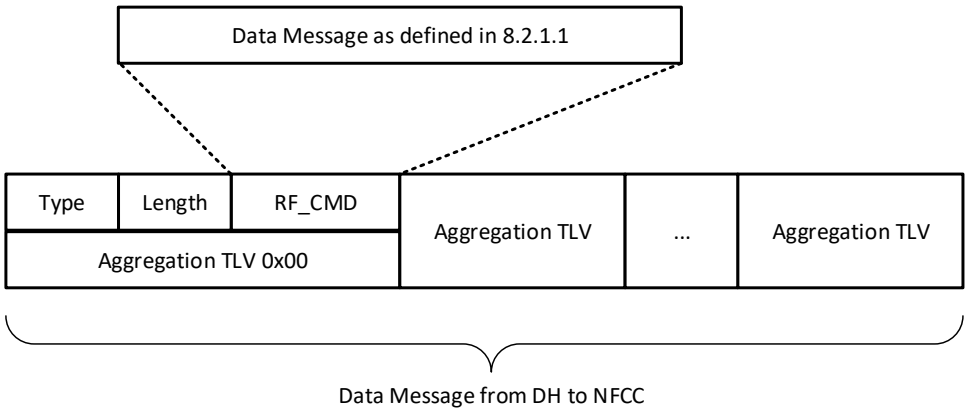

Figure 23: Format for Data Message from DH to NFCC

For Data from RF to the DH the procedures described in Section 8.2.1.2 apply, with the "Data Message" being mapped to the RF_RES field in Aggregation TLV object of type 0x03, and the "Status field" being mapped to the RF_STAT field in Aggregation TLV object of type 0x03. Figure 24 shows such a scenario.

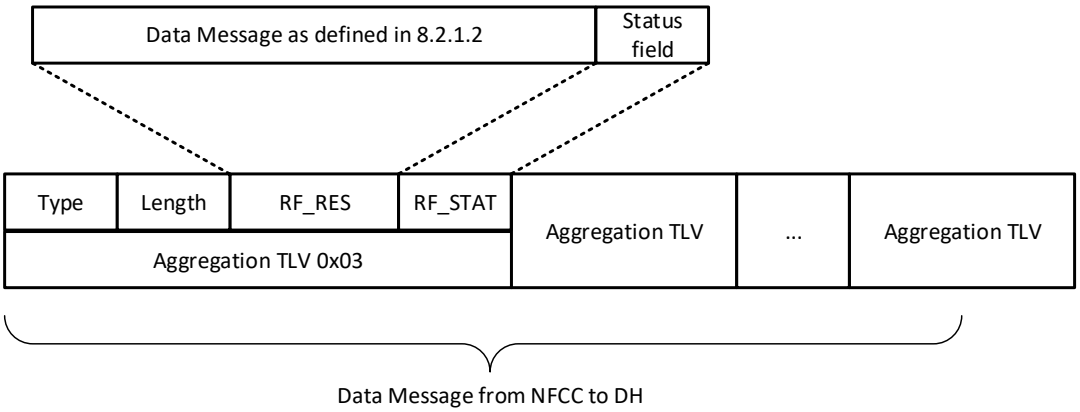

Figure 24: Format for Data Message from NFCC to DH

Table 112: Aggregation TLV Objects

Type	Length	Value		
		Field	**Length**	**Description**
0x00	N	RF_CMD	N	Command to be sent to Remote NFC endpoint, from which a response is expected.
0x01	N + 1	TO	1	Time out value to be used for this RF_CMD Effective Time-out = 5ms * TO.
		RF_CMD	N	Command to be sent to Remote NFC endpoint, from which a response is expected.
0x02	N + 1	WT	1	Time to wait for silent acknowledgement of this RF_CMD Effective Time-out = 1ms * WT.
		RF_CMD	N	Command to be sent to Remote NFC endpoint, from which no response is expected.
0x03	N + 1	RF_RES	N	Response received from Remote NFC Endpoint
		RF_STAT	1	The status of the received frame.
0x04 – 0x7F		RFU		
0x80 – 0xFF		Proprietary		

All TLV object type fields SHALL be coded in one octet. All TLV object length fields SHALL be coded in one octet.

Aggregation TLV object types 0x00, 0x01 and 0x02 SHALL only be sent from the DH to the NFCC.

Aggregation TLV object type 0x03 SHALL only be sent from the NFCC to the DH.

Aggregation TLV object type 0x00 is used by the DH for commands where the NFCC SHALL apply the default timeout that is configured for the Aggregated Frame RF Interface Extension, see Section 9.1.2.

Aggregation TLV object type 0x01 is used by the DH when the DH wishes to specify a timeout value to override the default timeout that is configured for the Aggregated Frame RF Interface, see Section 9.1.2. If TO is equal to 0x00, the NFCC SHALL NOT monitor for any timeout.

Aggregation TLV object type 0x02 is used by the DH for commands where it does not expect a response, and for which a response would be considered as an error. After sending the RF_CMD for Aggregation TLV object type 0x02, the NFCC SHALL wait up to WT milliseconds. If data is received from the Remote RF Endpoint during this time, the NFCC SHALL treat this as an error and send the DH an Aggregation TLV object type 0x03 containing the received data and status of RF_UNEXPECTED_DATA. If no data is received during this time, the NFCC SHALL send the DH an Aggregation TLV object type 0x03 containing a zero-length RF_RES field and status of STATUS_OK.

The DH SHALL NOT fragment an Aggregation TLV object into multiple NCI packets. The NFCC MAY fragment an Aggregation TLV object into multiple NCI packets. Control of aggregation in the path NFCC to DH is described in Section 9.1.2.

9.1.3.2 Aborting a Pending Transmission

The DH SHALL NOT send RF_EXT_AGG_ABORT_CMD except in state RFST_POLL_ACTIVE when the Frame Aggregation RF Interface Extension is started.

Table 113: Control Messages for Aggregation Abort

RF_EXT_AGG_ABORT_CMD		
Payload Field(s)	**Length**	**Value/Description**
Empty payload		

RF_EXT_AGG_ABORT_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

On receiving the RF_EXT_AGG_ABORT_CMD, the NFCC SHALL discard any remaining commands from previous NCI Data Messages. It SHALL wait for response to the current command if already sent, but SHALL NOT attempt retransmission of the current command if any error is detected. The NFCC SHALL send NCI Data Message(s) to the DH with any queued responses before sending the RF_EXT_AGG_ABORT_RSP.

To maintain the NCI flow control mechanism, if used, the NFCC SHALL give credits to the DH for any packets it discards without transmission, and for which it had not yet sent a credit to the DH.

Sending or receiving RF_EXT_AGG_ABORT_CMD and RF_EXT_AGG_ABORT_RSP SHALL NOT stop the Frame Aggregation RF Interface Extension. It SHALL still be in state started.

9.1.3.3 Error Handling

If the NFCC detects a transmission error, protocol error, or timeout error, for Aggregation TLV object types 0x00 and 0x01, it SHALL retransmit the last command subject to the configured Retry Count.

For Aggregation TLV object type 0x02, if the NFCC receives from the Remote RF Endpoint during the waiting time, then that is considered as an error and the NFCC SHALL not retry.

If the NFCC fails to complete any operation, the NFCC SHALL inform the DH by sending an Aggregation TLV object of type 0x03 with the status byte set to RF_TRANSMISSION_EXCEPTION, RF_FRAME_CORRUPTED, RF_PROTOCOL_EXCEPTION, RF_UNEXPECTED_DATA or RF_TIMEOUT_EXCEPTIONas appropriate. The NFCC SHALL then discard all TLV objects that were pending RF transmission.

Errors that the NFCC cannot detect are handled by the DH in the same manner as for Frame RF Interface (see Section 8.2.3.4).

The Frame Aggregation RF Interface Extension SHALL remain started after any error notification, unless stopped by the DH sending RF_INTF_EXT_STOP_CMD.

9.1.4 Stopping the RF Interface Extension

The Frame Aggregation RF Interface Extension can be stopped by using the RF_INTF_EXT_STOP_CMD. The Frame Aggregation RF Interface Extension requires no stop parameters.

When stopping the Frame Aggregation RF Interface Extension using RF_INTF_EXT_STOP_CMD, the value of the Stop Parameter Length field SHALL be 0 and there SHALL be no Stop Parameter fields present.

The DH SHALL NOT send RF_INTF_EXT_STOP_CMD if it is waiting for a response to any command(s) sent to the Remote NFC Endpoint.

After the DH has sent RF_INTF_EXT_STOP_CMD, it SHALL NOT send any NCI Data Packet to the NFCC until it has received RF_INTF_EXT_STOP_RSP.

9.2 LLCP Symmetry RF Interface Extension

If the LLCP Symmetry RF Interface Extension is supported by the NFC-DEP RF Interface, the DH MAY use it to offload the task of sending and receiving LLCP SYMM PDUs while the NFC-DEP Interface is active.

The LLCP Symmetry RF Interface Extension exposes messages for the DH to start or stop the symmetry procedure on the NFCC at any time during an active LLCP link. If the LLCP Symmetry RF Interface Extension is stopped, the DH handles the symmetry procedure. Note that it is, however, the responsibility of the NFCC to ensure compliance to the NFC-DEP Protocol and to LLCP NFC-DEP MAC mapping. For instance, the NFCC will not interrupt an NFC-DEP chaining procedure upon reception of any of those control messages.

9.2.1 Startup conditions

The LLCP Symmetry RF Interface Extension extends the NFC-DEP RF Interface in case the LLCP protocol is used on top of NFC-DEP. If the NFC-DEP RF Interface Activation is successful, the DH uses the General Bytes received in ATR_RES to determine whether LLCP link activation is possible. If the General Bytes meet the requirements in [LLCP], the DH performs the LLCP link activation procedure. If the LLCP link activation succeeds, the DH can use this RF Interface Extension.

After activation of the NFC-DEP RF Interface, the LLCP Symmetry RF Interface Extension SHALL be in stopped state.

The LLCP Symmetry RF Interface Extension can be started under the following conditions:

- The NFCC had shown support for the LLCP Symmetry RF Interface Extension in the CORE_INIT_RSP
- The NFC-DEP RF Interface is activated in either Poll or Listen mode.
- The LLCP Link Activation Procedure (as defined in [LLCP]) has been successfully performed. On Poll-side this requires LLCP compliant configuration of PN_ATR_REQ_GEN_BYTES, PN_ATR_REQ_CONFIG and NFCDEP_OP. On Listen-side of LN_ATR_RES_GEN_BYTES and LN_ATR_RES_CONFIG.

There are no relationships to other RF Interface Extensions defined in this document.

9.2.2 Starting the RF Interface Extension

The LLCP Symmetry RF Interface Extension can be started by adding a corresponding RF Interface Extension field to the RF_INTF_EXT_START_CMD.

In the RF Interface Extension field for the LLCP Symmetry RF Interface Extension, the value of the Start Parameter Length field SHALL be 2 and the Start Parameter field SHALL contain a value according to Table 114.

Table 114: LLCP Symmetry RF Interface Extension Start Parameter

Payload Field(s)	Length	Value/Description
Remote Link Timeout	1 Octet	An 8-bit unsigned integer that specifies the value of the Remote NFC Endpoint's link timeout. In order to align with [LLCP], the value is expressed in multiples of 10 ms.
Local Link Timeout	1 Octet	An 8-bit unsigned integer that specifies the value of symmetry timeout. In order to align with [LLCP], the value is expressed in multiples of 10 ms.

The first parameter, Remote Link Timeout, is the value of the LTO parameter sent by the Remote NFC Endpoint in the ATR_RES General Bytes. It represents the maximum time interval within which the Remote NFC Endpoint will send an NFC-DEP frame. The NFCC uses this parameter to detect link timeout errors.
After sending an NFC-DEP frame, the NFCC SHALL wait for an NFC-DEP frame from the Remote NFC Endpoint for the time defined by the Remote Link Timeout.

The second parameter, Local Link Timeout, represents the maximum time interval within which the local device SHALL send an NFC-DEP frame. If the device is acting in the role of NFC-DEP Initiator, the value is derived from the value of the LTO parameter sent to the Remote NFC Endpoint in the ATR_REQ General Bytes. If the device is acting in the role of an NFC-DEP Target, the value is derived from the value of WT advertised in the ATR_RES. Although LLCP Symmetry timeout is constrained by [DIGITAL] and [LLCP], the DH MAY choose a legal value different from the limit in order to suit its present system requirements.

On receipt of the RF_INTF_EXT_START_CMD Command,

- If the local LLC is supposed to send a PDU to the remote LLC, i.e. during the Local Link Timeout waiting period, the NFCC SHALL start the symmetry procedure by sending immediately an LLC SYMM PDU (if no transmit data from DH is available) to the remote NFC end point.
- If the local LLC is waiting for the remote LLC for a PDU response, i.e. during the Remote Link Timeout waiting period, the NFCC SHALL begin the LLCP symmetry procedure using the Remote Link Timeout as an indication of when the LLCP link timeout occurs if no NFC-DEP frame is received from the remote NFC Endpoint.

In order to minimize the latencies of this command the DH SHOULD send the RF_INTF_EXT_START_CMD command right after sending an LLC PDU to the NFCC. This will ensure that the NFCC doesn't unnecessarily send a SYMM PDU. This recommendation applies only in the case in which the DH has an LLC PDU to send to the remote NFC endpoint.

If the DH chooses to change the timeout parameters, it MAY send a subsequent RF_INTF_EXT_START_CMD with the new parameters. The NFCC uses the new values once the associated waiting time in progress has completed.

9.2.3 RF Interface Extension functionality

The definitions and requirements in this section SHALL apply only while the LLCP Symmetry RF Interface Extensions is started.

While the LLCP Symmetry RF Interface Extension is started, NFC-DEP frames that contain LLC SYMM PDUs SHALL be generated by, and handled by the NFCC. All other LLC PDUs, are generated by, and handled by, the DH.

9.2.3.1 Configuration

There are no configuration parameters for the LLCP Symmetry RF Interface Extension. Restrictions on the use of NFC-DEP as defined in [LLCP] SHALL be applied by the NFCC. Therefore the parameter NFCDEP_OP is not applicable to the LLCP Symmetry RF Interface Extension.

The DH can use the CORE_GET_CONFIG_CMD to read the version of the portion of LLCP supported by the NFCC by reading the read-only configuration parameter LLCP_VERSION.

Table 115: LLCP Version Parameter

	Bit Mask								Description
	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
Octet 0	X	X	X	X					LLCP Major Version
					X	X	X	X	LLCP Minor Version

If the DH determines that the version of LLCP implemented by the NFCC is acceptable, it can choose to start the LLCP Symmetry Procedure on the NFCC. Otherwise it can choose to handle LLCP Symmetry on the DH.

9.2.3.2 Error Handling

While the LLCP Symmetry Procedure is started, the NFCC SHALL handle failures during data exchange at the NFC-DEP level, as specified for the NFC-DEP RF Interface.

In addition

- if the LLCP Symmetry Procedure has been started on the NFCC and if reception of a PDU from the Remote NFC Endpoint does not commence within the time interval determined by the Remote Link Timeout parameter of the previous LLCP_SYMMETRY_START, the NFCC SHALL send the CORE_INTERFACE_ERROR_NTF with the Status of RF_TIMEOUT_EXCEPTION.
- if the LLCP Symmetry Procedure has been started on the NFCC, the NFCC SHALL stop the LLCP Symmetry Procedure before sending any CORE_INTERFACE_ERROR_NTF.

9.2.4 Stopping the RF Interface Extension

The LLCP Symmetry RF Interface Extension can be stopped by using the RF_INTF_EXT_STOP_CMD. The LLCP Symmetry RF Interface Extension requires no stop parameters.

When stopping the LLCP Symmetry RF Interface Extension using RF_INTF_EXT_STOP_CMD, the value of the Stop Parameter Length field SHALL be 0 and there SHALL be no Stop Parameter fields present.

On receipt of the RF_INTF_EXT_STOP_CMD Command:

- The NFCC SHALL begin forwarding all received LLC PDUs to the DH, and SHALL NOT send any LLC PDUs other than those received from the DH.
- If the local LLC is supposed to send a PDU to the remote NFC endpoint, i.e. during the Local Link Time Out waiting period, the NFCC SHALL stop the symmetry procedure by sending immediately a last LLC SYMM PDU (if no transmit data from DH is available).
- If the local LLC is waiting for the remote NFC endpoint for a LLC PDU response, i.e. in the remote LTO waiting period, the NFCC SHALL stop the LLCP symmetry procedure immediately.

This guarantees that, after the symmetry procedure is stopped, the DH has a full local Link timeout period to respond to the next PDU.

In order to minimize the latencies of this command the DH SHOULD send the RF_INTF_EXT_STOP_CMD command right after sending an LLC PDU to the NFCC. This will ensure that the NFCC doesn't unnecessarily send a SYMM PDU. This recommendation applies only in the case in which the DH has an LLC PDU to send to the remote NFC endpoint.

10 NFCEE Discovery and Mode Set

10.1 NFCEE ID

The NFCC dynamically assigns IDs for NFCEEs (called “NFCEE IDs”). The DH learns the ID values by performing NFCEE Discovery. NFCEE IDs are valid until the NFCC is reset with a Configuration Status of 0x01.

An ID with a value of 0x00 is referred to in this specification as a DH-NFCEE ID, and SHALL represent the DH-NFCEE.

Apart from the static NFCEE IDs, the NFCC dynamically assigns IDs for NFCEEs. The NFCEEs are separated into two groups:

- NFCEEs that are outside the HCI Network, for which the ID is called NFCEE IDand is in the range 0x10 to 0x7F.
- NFCEEs that are inside the HCI Network, called HCI-NFCEEs, for which the ID is called HCI-NFCEE IDand is in the range 0x80 to 0xFE.

The DH learns the dynamic ID values by performing NFCEE Discovery.

Table 116: NFCEE IDs

Value	Description
0x00	DH NFCEE ID, a static ID representing the DH-NFCEE
0x01	HCI Network NFCEE ID, a static ID representing the HCI-NTWK-NFCEE (RFU)
0x02-0x0F	Reserved for further static IDs
0x10-0x7F	NFCEE IDs, for NFCEEs that are outside of the HCI Network. Dynamically assigned by the NFCC
0x80-0xFE	HCI-NFCEE IDs, for HCI-NFCEEs that are inside of the HCI Network. Dynamically assigned by the NFCC
0xFF	RFU

NOTE The HCI Network NFCEE ID (HCI-NTWK-NFCEE) is currently not supported by this version of the NCI specification.

NOTE [ETSI_102622] uses different terms from those employed in this specification:
- “Terminal” in [ETSI_102622] corresponds to DH in this specification.
- “CLF” in [ETSI_102622] corresponds to NFCC in this specification.
- “Host controller” in [ETSI_102622] is implemented by the NFCC.
- “UICC” is a specific implementation of an NFCEE that also has a link with the DH via the HCI Access Interface.

10.2 NFCEE Discovery

These Control Messages are used to discover whether one or more NFCEEs are connected to the NFCC.

Table 117: Control Messages for NFCEE Discovery

NFCEE_DISCOVER_CMD		
Payload Field(s)	**Length**	**Value/Description**
Empty payload		

NFCEE_DISCOVER_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.
Number of NFCEEs	1 Octet	0 – 255 Indicates the number of NFCEE_DISCOVER_NTFs that SHALL be sent following this response

NFCEE_DISCOVER_NTF				
Payload Field(s)	**Length**	**Value/Description**		
NFCEE ID	1 Octet	An NFCEE ID as defined in Table 116. The value of 0x00 (DH-NFCEE ID) SHALL NOT be used.		
NFCEE Status	1 Octet	0x00	NFCEE enabled	
		0x01	NFCEE disabled	
		0x02	NFCEE unresponsive	
		0x03 – 0xFF	RFU	
Number of Protocol Information Entries	1 Octet	The number of Supported NFCEE Protocol fields to follow (n). For HCI-NFCEEs this value SHALL be 0, since HCI-NFCEEs are part of the HCI Network, so all communications are through that HCI Network,		
Supported NFCEE Protocols [0..n]	n Octet	See Table 136.		
Number of NFCEE Information TLVs	1 Octet	Number of NFCEE Information TLV fields to follow (m).		
NFCEE Information TLV[0..m]	x+2 Octets	Type	1 Octet	The Type of the NFCEE Information TLV. See Table 118.
		Length	1 Octet	The length of Value (x).
		Value	x Octets	The Value of the NFCEE Information TLV
NFCEE Power Supply	1 Octet	0x00	The NFCC has no control of the NFCEE Power Supply	
		0x01	The NFCC has control of the NFCEE Power Supply	
		0x02-0xFF	RFU	

Table 118: TLV Coding for NFCEE Discovery

<table>
<tr><th>Type</th><th>Length</th><th>Value</th></tr>
<tr><td>0x00</td><td>n</td><td>Hardware / Registration Identification
The Hardware/Registration Identification can be used by the DH to validate that any communication between the DH and an NFCEE only occurs with a valid NFCEE. It can be used by the NFC upper layer protocols or a DH application to enable security for communicating with NFCEEs. The value field coding is out of scope of this document and can be defined by each NFCEE manufacturer.</td></tr>
<tr><td>0x01</td><td>n</td><td>ATR Bytes
ATR information contains the transmission parameters, such as T = 0 and T = 1, that are supported by the NFCEE. It also carries all the necessary information that MAY be required by the DH such as Data transmission rate, Mask Version number, NFCEE Serial number, NFCEE hardware parameters etc. The format of ATR is defined in [ISO/IEC_7816-3].</td></tr>
<tr><td>0x02</td><td>9 – 169</td><td>T3T Command Set Interface Supplementary Information
The T3T Command Set Interface Supplementary Information MAY be present when one of the Supported NFCEE Protocol parameters contains the value Type 3 Tag Command Set. It SHALL NOT be present otherwise. If the T3T Command Set Interface Supplementary Information is present, it SHALL contain the PMm and Number of Entries field as outlined in Table 119. If the value for Number of Entries is larger than 0, it SHALL be followed by the corresponding number of Entries. Each Entry SHALL consist of the System Code and Idm fields as defined in Table 119.</td></tr>
<tr><td>0x03</td><td>1</td><td>Host ID in the HCI Network
Indicates the Host ID assigned by the NFCC/Host Controller to this NFCEE/Host, as defined in [ETSI_102622].</td></tr>
<tr><td>0x04</td><td>6</td><td>This Type indicates that the NFCEE supports NDEF storage.
The following field SHALL be provided:
<table>
<tr><th>Field</th><th>Length</th><th>Description</th></tr>
<tr><td>NDEF max size</td><td>4 Octets</td><td>Maximum size in Octets of the NDEF message that can be stored on this NFCEE</td></tr>
<tr><td>Power States</td><td>1 Octet</td><td>Power States supported by this NFCEE.
See Table 59</td></tr>
<tr><td>NDEF-NFCEE characteristics</td><td>1 Octet</td><td>See Table 120</td></tr>
</table></td></tr>
<tr><td>0x05-0x9F</td><td></td><td>RFU</td></tr>
<tr><td>0xA0-0xFF</td><td></td><td>For proprietary use</td></tr>
</table>

Table 119: Value Field for T3T Command Set Interface Supplementary Information

Payload Field(s)	Length	Value/Description
PMm	8 Octets	PMm as defined in [T3TOP]
Number of Entries	1 Octets	The number of Entries to follow (n). An entry consists of System Code and Idm parameters. Allowed values SHALL be from 0x00 to 0x10. Other values are RFU.
System Code[n]	2 Octets	System Code as defined in [T3TOP]
Idm[n]	8 Octets	Idm as defined in [T3TOP]

Table 120: NDEF-NFCEE Characteristics

	Bit Mask								Description
	b7	b6	b5	b4	b3	b2	b1	b0	
Octet 0								X	If this bit equals 0b, the NDEF message is not persistent over a power off/on and NCI initialization sequence. If this bit equals 1b, the NDEF message is persistent over a power off/on and NCI initialization sequence.
	0	0	0	0	0	0	0		RFU

To discover whether one or more NFCEEs are connected to the NFCC, the NFCEE_DISCOVER_CMD is sent by the DH to the NFCC.

On receipt of the NFCEE_DISCOVER_CMD, the NFCC SHALL respond to the DH with the NFCEE_DISCOVER_RSP with a Status of STATUS_OK and the maximum number of NFCEEs that can be connected to the NFCC (including NFCEEs inside the NFCC). A value of 0x00 indicates no NFCEE can be connected to the NFCC and no NFCEE is present inside the NFCC, 0x01 indicates one NFCEE can be connected to or is present inside the NFCC, etc. The DH-NFCEE SHALL be excluded from this number.

Following the NFCEE_DISCOVER_RSP, for each NFCEE the NFCC SHALL send an NFCEE_DISCOVER_NTF to the DH indicating the following:

- The unique NFCEE ID assigned by the NFCC to the NFCEE.
- The current NFCEE Status.
- Each NFCEE Protocol supported by the NFCEE
- Zero or more NFCEE Information Records to provide additional information on the NFCEE

NOTE NFCEE Protocols and NFCEE Interfaces have one-to-one mapping, and values for these are defined in the common definitions.

NOTE If an NFCEE supports certain NFCEE Protocol(s) reported with NFCEE_DISCOVER_NTF, then one of supported protocols can be used for communication between the DH and the NFCEE. A creation of that communication channel is called “NFCEE Interface activation”.

The assigned NFCEE ID remains valid until the NFCC is reset with a Configuration Status of 0x01.

After the NFCC has performed NCI initialization, the initial state of all NFCEEs SHALL be disabled (NFCEE Status value set to 0x01).

If a new NFCEE is connected to the NFCC, the initial state of this NFCEE SHALL be disabled (NFCEE Status value set to 0x01), or unresponsive (NFCEE Status value set to 0x02).

If the NFCEE Discovery Process fails, then NFCEE_DISCOVER_RSP SHALL be sent with Status of STATUS_FAILED (see Table 129). In the failure case the Number of NFCEEs SHALL be 0.

NFCEE_DISCOVER_CMD MAY be sent by the DH regardless of any reported NFCEE status.

On receipt of a valid NFCEE_DISCOVER_CMD, if the NFCC has not yet sent all the expected NFCEE_ DISCOVER_NTFs for a previous NFCEE_DISCOVER_CMD, the NFCC SHALL respond with NFCEE_DISCOVER_RSP with a Status of STATUS_SEMANTIC_ERROR. Otherwise, the NFCC SHALL respond with NFCEE_DISCOVER_RSP with a Status of STATUS_OK

The following diagram gives an indication of the NFCEE state transitions. Note that the NFCEE_MODE_SET_NTF (Enable) notation indicates an NFCEE_MODE_SET_NTF associated to an NFCEE_MODE_SET_CMD(Enable).

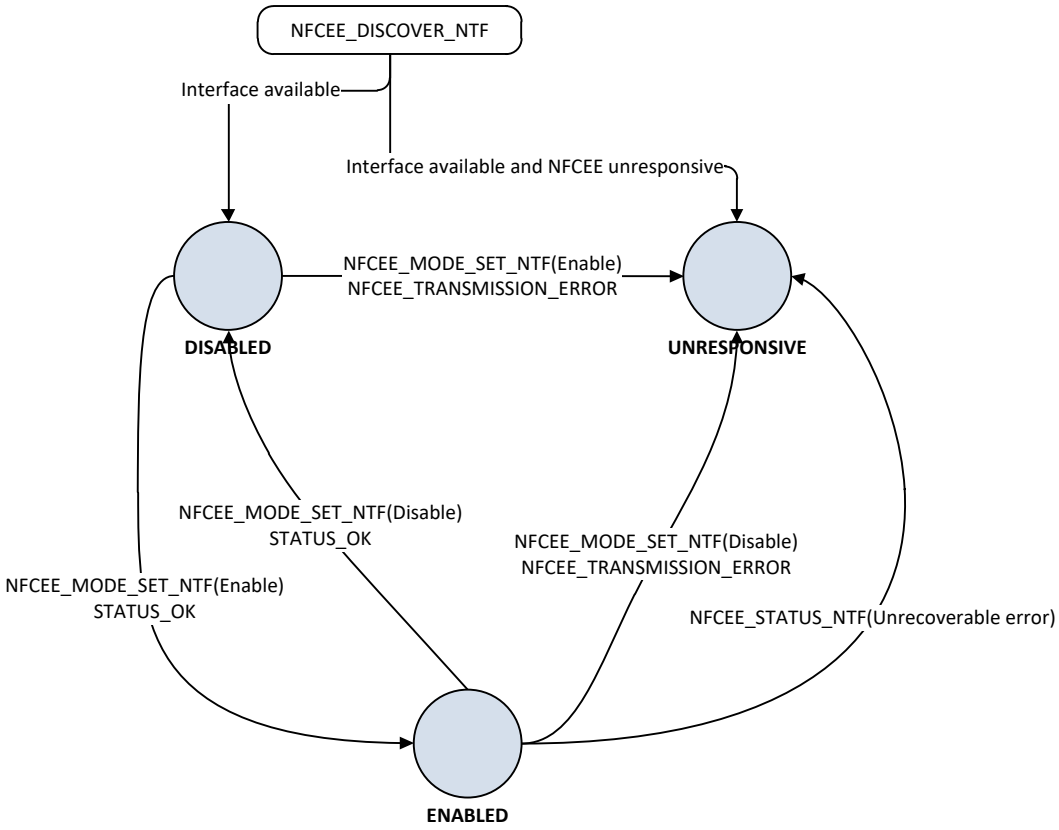

Figure 25: NFCEE State Transitions

10.2.1 HCI-NFCEE Specific Handling

If the NFCC implements an HCI Host Controller as reported in CORE_INIT_RSP, the following rules apply to the NFCEE_DISCOVER_NTF for an HCI-NFCEE:

- The NFCC SHALL set the Number of Protocol Information Entries to 0
- The NFCC SHALL use an NFCEE information TLV of value Host ID in the HCI Network.
- The NFCC SHALL NOT provide any Hardware/Registration Identification; The Length of Hardware/Registration Identification SHALL be set to 0. The Hardware/Registration Identification information of the different hosts in the HCI Network can be received by HCP packets (as defined in [ETSI_102622]).

In addition, the following rules also apply:

- The DH SHALL NOT use the HCI-NFCEE ID returned by the NFCC in the NFCEE_DISCOVER_NTF to create a logical connection to this HCI-NFCEE. The DH SHALL use the static HCI Connection instead.
- If the NFCEE Status field has a value of “0x00 – NFCEE enabled”, the HCI-NFCEE is allowed to perform RF communication (under the conditions given by the RF State Machine).

If the NFCEE Status field has a value of “0x01 – NFCEE disabled” or “0x02 – NFCEE unresponsive”, then RF communication is not allowed for this HCI-NFCEE.

10.2.2 NDEF-NFCEE Specific Handling

The following rules apply to the NFCEE_DISCOVER_NTF for an NFCEE supporting NDEF storage:

- The NFCC SHALL set the Number of Protocol Information Entries to 1 and use the following NFCEE Protocol value:
    - For T4T emulation: NFCEE Protocol = APDU
    - For T3T emulation: NFCEE Protocol = Type 3 Tag Command Set
- The NFCC SHALL add an NFCEE Information TLV of Type 0x04 to inform the DH about the maximum size of the NDEF message that can be stored on the NFCEE, for which Power States this NFCEE can operate.
- If emulating a T3T, the NDEF-NFCEE SHALL use an NFCID2 starting with 0x02FE (as defined in [DIGITAL]). The NFCC SHALL inform the DH about the T3T parameters by including the T3T Command Set Interface Supplementary Information TLV in the NFCEE_DISCOVER_NTF.

10.3 NFCEE Enabling and Disabling

These Control Messages are used to enable or disable an NFCEE.

Table 121: Control Messages to Enable and Disable a Connected NFCEE

NFCEE_MODE_SET_CMD			
Payload Field(s)	**Length**	**Value/Description**	
NFCEE ID	1 Octet	NFCEE ID as defined in Table 116. The value of 0x00 (DH-NFCEE ID) SHALL NOT be used.	
NFCEE Mode	1 Octet	0x00	Disable the NFCEE
		0x01	Enable the NFCEE
		0x02 – 0xFF	RFU

NFCEE_MODE_SET_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

NFCEE_MODE_SET_NTF		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

To enable or disable an NFCEE, the DH sends the NFCEE_MODE_SET_CMD to the NFCC. The NFCEE ID identifies the NFCEE on which the action occurs and the NFCEE Mode identifies whether that NFCEE is enabled or disabled.

After sending an NFCEE_MODE_SET_CMD, the DH SHALL NOT send another NFCEE_MODE_SET_CMD until it has received either an NFCEE_MODE_SET_RSP with a failed status, or an NFCEE_MODE_SET_NTF.

On receipt of a valid NFCEE_MODE_SET_CMD, if the NFCC has not yet sent the NFCEE_MODE_SET_NTF for a previous NFCEE_MODE_SET_CMD, the NFCC SHALL respond to the DH with the NFCEE_MODE_SET_RSP with a Status of STATUS_SEMANTIC_ERROR. Otherwise, the NFCC SHALL respond to the DH with the NFCEE_MODE_SET_RSP with a Status of STATUS_OK.

The NFCC SHALL wait for the completion of the necessary processing, which might include an initialization sequence, before the NFCC indicates whether the action was successful or unsuccessful by sending the NFCEE_MODE_SET_NTF to the DH. In a failure case the Status SHALL be set to STATUS_FAILED (see Table 129) or NFCEE_TRANSMISSION_ERROR if the corresponding NFCEE is unresponsive.

If an NFCEE is disabled, the DH and the NFCC SHALL NOT consider the NFCEE enabled until the DH gets an NFCEE_MODE_SET_NTF with a Status set to STATUS_OK following an NFCEE_MODE_SET_CMD(Enable).

If an NFCEE is enabled, the DH and the NFCC SHALL NOT consider the NFCEE disabled until the DH gets an NFCEE_MODE_SET_NTF following an NFCEE_MODE_SET_CMD(Disable) or the DH receives an NFCEE_STATUS_NTF (Non recoverable error), as defined in Section 10.5.

If the DH gets an NFCEE_MODE_SET_NTF with a status NFCEE_TRANSMISSION_ERROR, the NFCEE SHALL be considered unresponsive.

If an NFCEE is unresponsive, the DH SHALL NOT attempt to enable or disable this NFCEE. If the NFCC receives the NFCEE_MODE_SET_CMD with the NFCEE ID of an unresponsive element, the NFCC SHALL respond to the DH with the NFCEE_MODE_SET_RSP with a Status of STATUS_SEMANTIC_ERROR.

The NFCC SHALL NOT route communication to or from a disabled or unresponsive NFCEE. This also includes any communication from a Remote NFC Endpoint or from another NFCEE routed via the NFCC.

The NFCC SHALL only enable an NFCEE when triggered by an NFCEE_MODE_SET_CMD.

If the NFCEE is disabled by the DH with NFCEE_MODE_SET_CMD, then Logical Connection to this NFCEE SHALL be closed implicitly (without sending of a CORE_CONN_CLOSE_CMD) and corresponding NFCEE Interface SHALL be deactivated immediately.

10.3.1 HCI-NFCEE Specific Handling

If the NFCEE Mode field of the NFCEE_MODE_SET_CMD is set to “Enable the NFCEE”, the HCI-NFCEE is allowed to perform RF communication. Therefore, if it was not already activated, the communication interfaces to the HCI-NFCEE SHALL be activated. If the HCI-NFCEE is already enabled while receiving the NFCEE_MODE_SET_CMD (Enable), the NFCC SHALL activate the communication interface to the HCI-NFCEE (the communication interface might have been deactivated earlier, e.g. for power consumption reasons).

If the NFCEE Mode field of the NFCEE_MODE_SET_CMD is set to “Disable the NFCEE”, the HCI-NFCEE is not allowed to perform any further RF communication. Therefore it MAY be no longer necessary to keep the communication interface to the HCI-NFCEE activated.

For HCI-NFCEEs the initialization sequence referenced in Section 10.5 is the HCI Session Initialization (defined in [ETSI_102622]).

10.4 NDEF-NFCEE

Once the DH has discovered an NDEF-NFCEE that can be embedded inside the NFCC, all the NCI mechanisms defined to manage an NFCEE can be used:

- The DH can enable/disable the NDEF-NFCEE with the NFCEE_MODE_SET_CMD. The NDEF message in the NDEF-NFCEE SHALL be persistent over a disable/enable sequence.
- The DH can include the NDEF-NFCEE ID in the Listen Routing Table, for the Power States the NFCEE supports.
- The NFCC will notify the DH about an action that took place with the NDEF-NFCEE by using the RF_NFCEE_ACTION_NTF (e.g. reporting the AID selected for the T4T)
- The NFCC will notify the DH about the RF Discovery Requirements of an NDEF-NFCEE (typically NFC-A/Listen or NFC-B/Listen for T4T and NFC-F/Listen for T3T) through the RF_NFCEE_DISCOVERY_REQ_NTF
- The DH can create a Dynamic Logical Connection to an NDEF-NFCEE to read or write the content of the NDEF message.
    - The regular procedures defined in the Tag Specifications (T3T or T4T) for Check NDEF, Read NDEF, Write NDEF are used by the DH.
    - The Data mapping to be used by the DH is defined by the APDU NFCEE Interface for T4T and the Type 3 Tag Command Set NFCEE Interface for T3T.

The DH SHALL NOT communicate with an NDEF-NFCEE over a Dynamic Logical Connection except in state RFST_IDLE.

In this version of the NCI specification, the NDEF message stored inside an NDEF NFCEE cannot be written by a contactless Reader/Writer. Therefore, the NDEF Tag SHALL appear in state "READ ONLY" on the contactless access, while it SHALL appear in state "READ/WRITE" on the NCI access.

- For an NDEF-NFCEE emulating a T4T for mapping version 2.0, that means that the NDEF file write access condition present in the NDEF Control TLV in the CC file has a value 0xFF on the contactless access, while it has a value 0x00 on the NCI access. See [T4TOP] for further details.
- For an NDEF-NFCEE emulating a T3T for mapping version 1.0, that means that the RWFlag in the Attribute Information Block has a value of 00h on the contactless access, while it has a value of 0x01 on the NCI access. In addition the Service 0009h is only available on the NCI access but not on the contactless access. See [T3TOP] for further details.

10.5 NFCEE Status

This Control Message is used by the NFCC to inform the DH about a change in the status of an enabled NFCEE.

Table 122: Control Messages to report the status of an NFCEE

NFCEE_STATUS_NTF			
Payload Field(s)	**Length**	**Value/Description**	
NFCEE ID	1 Octet	NFCEE ID as defined in Table 116. The value of 0x00 (DH-NFCEE ID) SHALL NOT be used.	
NFCEE Status	1 Octet	0x00	Unrecoverable error
		0x01	NFCEE Initialization sequence started
		0x02	NFCEE Initialization sequence completed
		0x03 – 0x7F	RFU
		0x80-0xFF	Proprietary

The NFCC sends the NFCEE_STATUS_NTF to report a change in the status of an enabled NFCEE. The NFCC SHALL NOT send an NFCEE_STATUS_NTF for any disabled or unresponsive NFCEE. When an NFCEE is enabled and the NFCC detects that there is a unrecoverable error while communicating with this NFCEE, the NFCC SHALL send an NFCEE_STATUS_NTF with the NFCEE Status field set to 'Unrecoverable error'. The DH and the NFCC SHALL then consider the NFCEE as being unresponsive.

When an NFCEE is enabled and the NFCC detects that the NFCEE has started an initialization sequence, the NFCC SHALL send an NFCEE_STATUS_NTF with the NFCEE Status field set to 'NFCEE Initialization sequence started'. The NFCEE remains enabled.

When an NFCEE is enabled and the NFCC detects that the NFCEE has completed an initialization sequence, the NFCC SHALL send an NFCEE_STATUS_NTF with the NFCEE Status field set to 'NFCEE Initialization sequence completed'. The NFCEE remains enabled.

10.5.1 HCI- NFCEE Specific Handling

For HCI-NFCEEs the initialization sequence referenced in Section 10.5 is the HCI Session Initialization (defined in [ETSI_102622]).

10.6 NFCEE Power Supply and Communication Link Control

This Control Message is used by the DH to constrain the way the NFCC manages the power supply and communication links between the NFCC and its connected NFCEEs.

Table 123: Control Messages to constrain the Power Supply and link of an NFCEE

NFCEE_POWER_AND_LINK_CNTRL_CMD			
Payload Field(s)	**Length**	**Value/Description**	
NFCEE ID	1 Octet	NFCEE ID as defined in Table 116. The value of 0x00 (DH-NFCEE ID) SHALL NOT be used.	
NFCEE Power and Link Configuration	1 Octet	0x00	NFCC decides (default state).
		0x01	NFCEE Power Supply always On.
		0x02	NFCC to NFCEE Communication link always active when the NFCEE is powered on.
		0x03	NFCEE Power supply and NFCC to NFCEE communication link are always On.
		0x04 – 0xFF	RFU

NFCEE_POWER_AND_LINK_CNTRL_RSP		
Payload Field(s)	**Length**	**Value/Description**
Status	1 Octet	See Table 129.

The NFCC SHALL use the default value “0x00 – NFCC decides” for the NFCC Constraints field of all NFCEEs.

The DH MAY send NFCEE_POWER_AND_LINK_CNTRL_CMD at any time after NCI initialization, even for an NFCEE that is disabled or unresponsive. The NFCC SHALL use the DH settings when the NFCEE is enabled.

If the NFCC receives an NFCEE_POWER_AND_LINK_CNTRL_CMD with an NFCEE Power and Link Configuration field equal to “0x01 - NFCEE Power Supply always On”, but the NFCC has no control of the NFCEE Power Supply (as reported in the NFCEE_DISCOVER_NTF), then the NFCC SHALL respond with NFCEE_POWER_AND_LINK_CNTRL_RSP with a Status of STATUS_REJECTED.

The behavior of any NFCEE that is enabled is based on the value of its NFCEE Power and Link Configuration field:

- **0x00 – NFCC decides**

  The NFCC makes its own best effort to optimize the power consumption by switching off the NFCEE power supply and deactivating the NFCC to NFCEE Communication link when applicable. The NFCC also determines the activation/deactivation timings for the communication link and the power supply.

- **0x01 - NFCEE Power Supply always On**

  The NFCC SHALL keep the NFCEE Power Supply on. The NFCC MAY, however, save power by deactivating the NFCC to NFCEE communication link when applicable.

- **0x02 - NFCC to NFCEE Communication link always active when the NFCEE is powered on.**

The NFCC SHALL keep the communication link between the NFCC and the NFCEE active when the NFCEE is powered on.

- **0x03 - NFCEE Power supply and NFCC to NFCEE communication link are always On.**

  The NFCC SHALL keep the communication link between the NFCC and the NFCEE active and the NFCEE power supply always On.

10.6.1 HCI- NFCEE Specific Handling

For HCI-NFCEEs the communication link is active when the NFCC keeps SWIO either in state SUSPENDED or ACTIVATED (as defined in [ETSI_102613]).

The NFCC SHOULD ensure that the SWIO link is not deactivated for a minimum of 1 second after the last activity on the link when the NFCC constraints is set to its default value: '0x00 – NFCC Decides '.

11 NFCEE Interfaces

This section describes the supported NFCEE Interfaces. Unless defined otherwise, all NFCEE Interfaces are optional.

The DH learns which NFCEE Interfaces are supported by an NFCEE during the NFCEE Discovery Process (see Section 10.1). The “Supported NFCEE Protocol parameter” field(s) in NFCEE_DISCOVER_NTF identifies the supported NFCEE Protocol(s).

The DH SHALL only initiate NFCEE Interface activation for an NFCEE Protocol that was reported during the NFCEE Discovery Process.

NFCEE Interface activation and deactivation is performed automatically when a Logical Connection to an NFCEE is either being created or closed (see Section 4.4). There are no specific Control Messages for NFCEE Interface activation or deactivation.

The combination of NFCEE ID and NFCEE Protocol (as reported in the NFCEE_DISCOVER_NTF) employed in the connection creation uniquely identifies a specific NFCEE Interface to be activated.

If there is an error during NFCEE Interface activation, the NFCC SHALL set the Status in the CORE_CONN_CREATE_RSP to NFCEE_INTERFACE_ACTIVATION_FAILED.

There MAY be multiple simultaneous active NFCEE Interfaces, but there SHALL be only one active NFCEE Interface for each NFCEE. For each NFCEE, only one Logical Connection is allowed between the DH and one NFCEE.

An NFCEE Interface SHALL be deactivated when the corresponding Logical Connection is closed. The DH MAY initiate connection closure by referencing the Conn ID used for the NFCEE Interface (details in Section 4.4.3).

If there are unrecoverable transmission errors of a message between the NFCC and the NFCEE, the NFCC SHALL send a CORE_INTERFACE_ERROR_NTF with the Status set to NFCEE_TRANSMISSION_ERROR.

11.1 APDU NFCEE Interface

11.1.1 Data Exchange

This communication is the transmission and receipt of APDU command-response pairs using short message lengths (described in Section 12 of [ISO/IEC_7816-3]). That is, $\mathbf{L}_c$ and $\mathbf{L}_e$ are coded on one byte.

The DH MAY send a Data Message to the NFCC as specified in Section 11.1.1.1. The NFCC will extract and send the Command APDU data contained in the payload of the Data Message(s) to the NFCEE.

When the NFCC receives Response APDU data from the NFCEE, the NFCC SHALL populate the payload of a Data Message with the Response APDU and send the Data Message to the DH as specified in Section 11.1.1.2.

NCI Segmentation and Reassembly MAY be applied to Data Messages in either direction.

The NFCC is responsible for managing the variances necessary for the communication and receipt of Command and Response APDUs between itself and the NFCEE and this SHALL be transparent to the DH and NCI.

11.1.1.1 Format for Data Messages sent from DH to NFCC

When receiving a Data Message from the DH, the NFCC SHALL send the Data Message, i.e. Command APDU to the NFCEE. If a single Command APDU is split across multiple Data Packets, the NFCC SHALL receive all relevant Data Packets and combine the Command APDU data from all Data Packets prior to sending the Command APDU to the NFCEE.

Figure 26 illustrates the mapping between the Data Packet(s) and the Command APDU to be sent to the NFCEE.

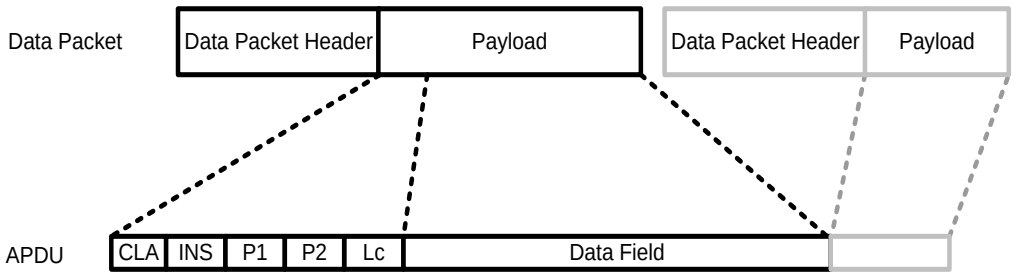

Figure 26: Mapping of Command APDU

The following is the structure of the Command APDU in the Data Message and is dependent on the case of the command.

For Case 1: CLA | INS| P1 | P2

For Case 2: CLA | INS| P1 | P2 | Le

For Case 3: CLA | INS | P1 | P2 | Lc | Data Field

For Case 4: CLA | INS | P1 | P2 | Lc | Data Field | Le

It is the responsibility of the NFCC to correctly map these to the protocol used between the NFCC and the NFCEE. In the case that T=0 is being used as this protocol, it is the responsibility of the NFCC to manage the 0x6Cxx and 0x61xx status words and these status words are not sent from the NFCC to the DH. In these cases the NFCC SHALL transfer the full response.

11.1.1.2 Format for Data Messages sent from NFCC to DH

The NFCC SHALL retrieve the complete APDU Response from the NFCEE and handle it as a Data Message and send it to the DH in one or more Data Packets. If the retrieved APDU Response(s) from an NFCEE does not fit in a single Data Packet, the NFCC SHALL split the APDU Response across multiple Data Packets.

Figure 27 illustrates the mapping between Response APDU and the Data Packets to be sent to the DH.

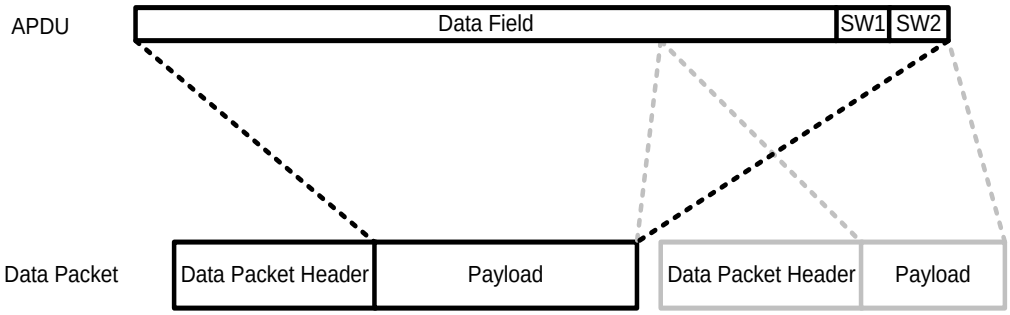

Figure 27: Mapping of Response APDU

11.1.2 Failures during Data Exchange

If the NFCEE fails to respond to an APDU command within the appropriate time interval, the NFCC SHALL send a CORE_INTERFACE_ERROR_NTF with its Status set to NFCEE_TIMEOUT_ERROR.

If the data received from the DH is not formatted correctly (for instance, is less than 4 octets in length or the value provided for Lc in the Command Header does not match the length of the data field), the NFCC SHALL send a CORE_INTERFACE_ERROR_NTF with its Status set to NFCEE_PROTOCOL_ERROR.

11.2 Type 3 Tag Command Set NFCEE Interface

The DH uses the Type 3 Tag Command Interface to communicate with NFCEEs connected to the NFCC by exchanging Type 3 Tag Commands and Responses (as defined in [T3TOP]).

11.2.1 Data Exchange

The payload of the Data Messages sent on the Logical Connection SHALL be Type 3 Tag Commands and Responses (as defined in [T3TOP]), preceded by a 1 octet length field. Data Messages MAY be segmented into multiple Data Packets when sent over the NCI.

The length field value SHALL equal the length of the Type 3 Tag Command or Response plus one.

Type 3 Tag Commands SHALL only be sent in the direction DH to NFCC. Type 3 Tag Responses SHALL only be sent in the direction NFCC to DH.

Figure 28 illustrates the mapping between the Data Packet Format and the Type 3 Tag Command Set Format when there is no segmentation.

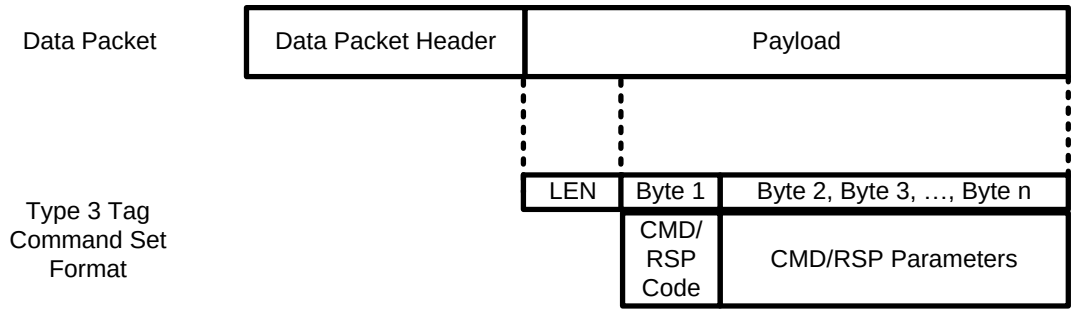

Figure 28: Data Message Format for Type 3 Tag Command Set Interface

11.2.1.1 Polling Command and Response

If a SENSF_REQ is sent by the DH to the NFCEE, it SHALL be coded as defined in [DIGITAL] and SHALL have a TSN value of 0x00.

The DH SHOULD choose a larger value for ΔTPoll (as defined in [DIGITAL]) to accommodate a potentially longer transmission time of the SENS_RES from the NFCEE to the DH, compared to the RF communication.

11.3 Transparent NFCEE Interface

The Transparent Interface is used by the DH to communicate with NFCEEs connected to the NFCC by exchanging data that are not understood by the NFCC, but just passed without modification.

11.3.1 Data Exchange

The DH MAY send Data Messages on such a connection to the NFCC for transmission to the NFCEE. The NFCC SHALL extract and forward the payload of the Data Messages – in the appropriate message format – directly to the NFCEE without any modification.

When the NFCC receives a message from the NFCEE, the NFCC SHALL extract the data from the message, populate it to the payload of a Data Message and send the Data Message to the DH on the relevant connection. The mechanism used to transmit such data between the NFCC and the NFCEE is implementation specific. The NFCC is responsible for managing the variances necessary for the communication between itself and the NFCEE and this SHALL be transparent to the DH and NCI.

NCI Segmentation and Reassembly MAY be applied to Data Messages in either direction.

12 Transport Mappings

The NCI Core design is intended to be independent of any specific underlying transport layer or its speed.

The following are requirements for any underlying Transport Mapping:

- Transport Mappings SHALL provide means to transport Data and Control Packets in both directions between the DH and NFCC.
- Transport Mappings SHALL provide a reliable data transfer.
- Transport Mappings MAY include flow control mechanisms. However, if possible they SHOULD rely on the flow control built into the NCI protocol.
- Transport Mappings providing framing SHALL NOT forward Packets with a size smaller than 3 bytes to the NCI Core.

The following subsections describe Transport Mappings for NCI.

It is not mandated to use any of the Transport Mapping defined on the following subsections. The device implementation MAY use a proprietary Transport Mapping that fulfills the above requirements (even for transport layers where this specification contains a mapping).

12.1 UART Transport

NCI Frames SHALL be transmitted over the UART between an DH and an NFCC with no additional framing. Since there is no additional framing, the UART transport cannot introduce any errors. Otherwise the NCI messages stream might be unrecoverable. So the UART connection SHALL be of a sufficiently high quality as to provide a reliable data transfer at the configured baud rate.

The NCI UART Transport SHOULD use the following settings for RS232:

- 8 data bits
- 1 stop bit
- No parity
- Automatic (i.e. h/w based) RTS/CTS Flow control.

The baud rate is manufacturer-specific.

Flow control with RTS/CTS is used to prevent temporary UART buffer overrun, and is not intended to be used other than temporarily. NCI has its own credit-based logical flow control mechanism, which is better suited to the different types of NCI data that flow across the transport.

If CTS is 1, then the DH/NFCC is allowed to send. If CTS is 0, then the DH/NFCC is not allowed to send.

The RS232 signals SHOULD be connected in a null-modem fashion; i.e. the local TXD SHOULD be connected to the remote RXD and the local RTS SHOULD be connected to the remote CTS and vice versa.

12.2 I2C Transport

NCI Frames SHALL be transmitted over the I^2C [I2C] between a DH and an NFCC with no additional framing. Since there is no additional framing, the I^2C transport cannot introduce any errors. Otherwise the NCI messages stream might be unrecoverable. So the I^2C connection SHALL be of a sufficiently high quality as to provide a reliable data transfer at the configured transfer rate.

The DH SHOULD operate as a bus master and MAY also be able operate as a bus slave if addressed by another bus master. The NFCC MAY operate as either bus master or slave. In the latter case ‘out-of-band’ means SHOULD be provided in order for the NFCC to request the DH to initiate a data transfer as a bus master. However, if ‘out-of-band’ method is not available, the DH SHALL poll frequently the NFCC. Polling frequency is implementation specific.

The I2C transport SHOULD support standard (up to 100kbps) and Fast-Speed mode (up to 400kbps) and MAY support Fast-Mode Plus (up to 1 Mbit/s) and High Speed mode (up to 3.4Mbit/s).

Additionally, 10-bit addressing mode and clock stretching MAY be supported on the I^2C transport.

12.3 Half Duplex SPI Transport

12.3.1 Physical

NCI control and data messages are transmitted over SPI. The DH SHALL be the master of the communication. The communication SHALL use standard SPI signal lines i.e. SPI_CSN, SPI_CLK, SPI_MOSI and SPI_MISO. In addition to attain flow control there SHALL be an additional SPI_INT signal line that SHALL be driven by the slave. The clock rate negotiation is manufacturer specific and is out of scope of this document. The data sent through the transport is assumed to be in Little Endian format.

12.3.1.1 SPI Modes

SPI can be operated in one of the four modes described below. The mode selection procedure is manufacturer specific and is out of scope of this document.

Table 124: SPI modes

SPI mode	CPOL	CPHA
0	0	0
1	0	1
2	1	0
3	1	1

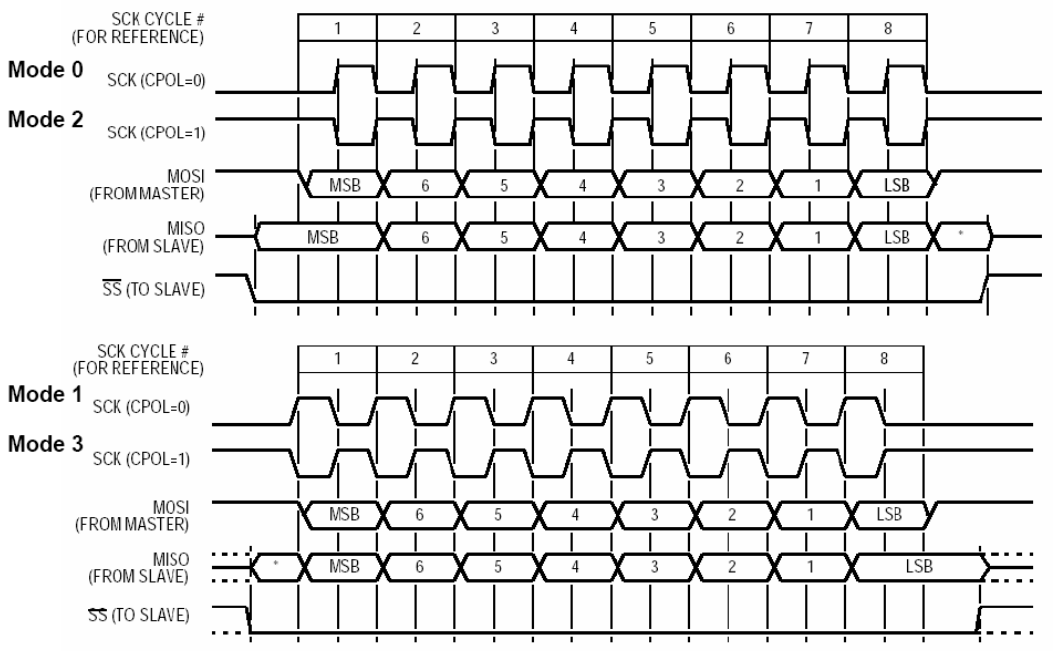

Figure 29: SPI Operation

12.3.2 Data Transfer

This proposal reduces the full-duplex nature of the Generic SPI transport to a half-duplex interface. Packet framing and flow-control mechanisms are gained in exchange for the loss of bandwidth. These are more important as the intended clock rate far exceeds the NCI bandwidth requirement.

The transport mechanism has the capability to send a maximum sized NCI packet in a single SPI frame.

The following Data Transfer sections define two modes of operation: acknowledged and unacknowledged. Which mode is used is determined by the Second Octet. In the acknowledged mode a CRC is following the Payload and the receiver sends an positive acknowledge for correctly received payloads or a negative acknowledge for erroneous payloads.

12.3.2.1 Data Transfer from DH to NFCC

The master SHALL use the “DirectWrite” command to send data to a slave. The master can initiate a data transfer in the following fashion:

Step 1. Master asserts SPI_CSN.

Step 2. Slave asserts SPI_INT.

Step 3. Master sends 2-byte DirectWrite header, followed by 2-byte SPI payload length parameter.

Step 4. Master sends SPI payload.

Step 5. Slave deasserts SPI_INT.

Step 6. Master deasserts SPI_CSN.

SPI_CSN MAY be toggled (deasserted and asserted) in every 8-bit transfer.

If the Second Octet is equal to 0x00, the DirectWrite header is sent as shown in the table below.

Table 125: SPI Header Coding (DH to NFCC) without CRC

	First Octet	Second Octet	Third Octet	Fourth Octet
Master	0x01	0x00	MSB (Payload Length	LSB (Payload Length)
Slave	0x00	0x00	0x00	0x00

The Payload length is the length of the whole NCI packet inclusive of the NCI header. Since the NCI packet can be as long as 258 octets we need a 2 octet payload length field.

Figure 30 illustrates the procedure, described above, that transfers data from the DH to the NFCC.

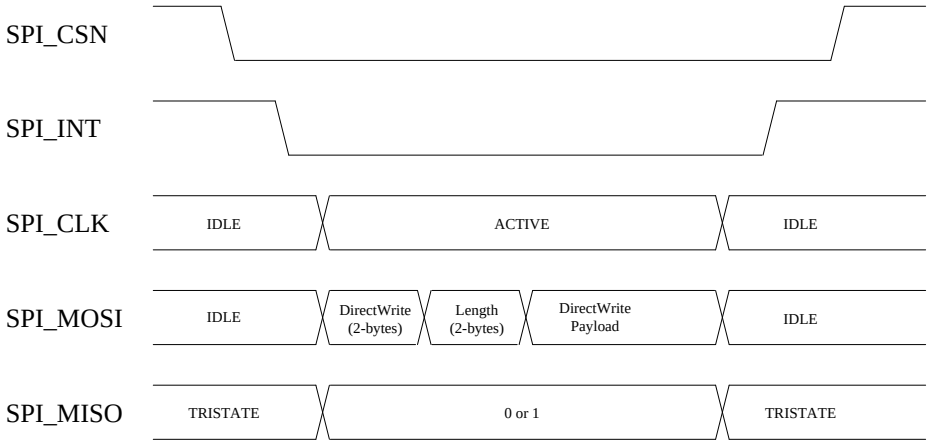

Figure 30: SPI Data Transfer from the DH to the NFCC without CRC

If the second octet is equal to 0x01, the DirectWrite header is sent as shown in Table 126 and 2-octet CRC SHALL follow the Payload:

The CRC SHALL be a CRC-16-CCITT using the polynomial x16 + x12 + x5 + 1, calculated for all octets of Header and Payload. The initial value SHALL be FFFFh. The first CRC octet transmitted SHALL be the MSB.

The master SHALL send ACK if the CRC is correct when receiving data from the slave.

The master SHALL send NAK if the CRC is not correct when receiving data from the slave.

Table 126: SPI Header Coding (DH to NFCC) with CRC

	First Octet	Second Octet	Third Octet	Fourth Octet
Master	0x01	0x01	b8: NAK if set to 1b b7: ACK if set to 1b b6-b1: MSB (Payload Length)	LSB (Payload Length)
Slave	0x00	0x00	0x00	0x00

Figure 31 illustrates the procedure to transfer data from the DH to the NFCC when the Second Octet is equal to 0x01.

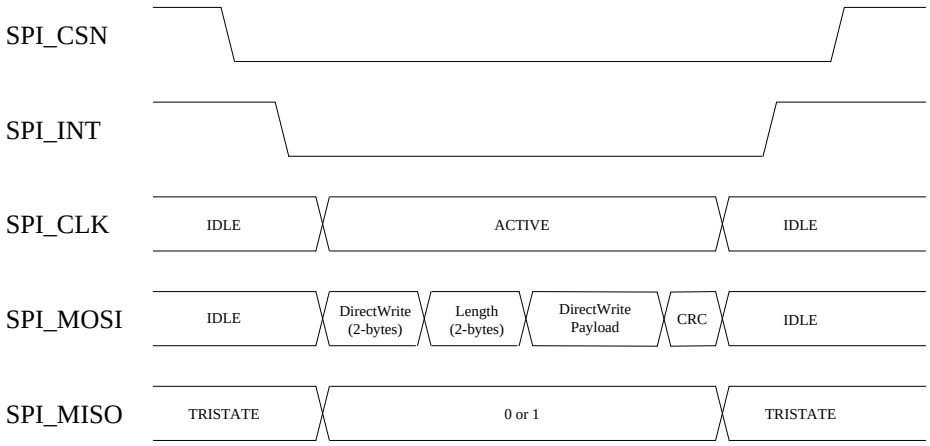

Figure 31: SPI Data Transfer from the DH to the NFCC with CRC

If the slave does not assert SPI_INT in a timely fashion, the master is allowed to deassert SPI_CSN and use the SPI bus to talk to a different peripheral. This can happen if the slave is busy processing its FIFOs.

12.3.2.2 Data Transfer from NFCC to DH

The “DirectRead” command is used to transfer data from slave to the master. Data can be transferred from the slave to the master in the following fashion:

Step 1. Slave asserts SPI_INT

Step 2. Master asserts SPI_CSN

Step 3. Master send 2-octet SPI header

Step 4. Slave sends 2-octet SPI payload length

Step 5. Slave sends SPI payload

Step 6. Master deasserts SPI_CSN

Slave MAY deassert SPI_INT at any time after step 2.

Slave SHALL deassert SPI_INT before step 6.

SPI_CSN MAY be toggled (deasserted and asserted) in every 8-bit transfer.

If the Second Octet is equal to 0x00, the DirectRead header is sent as shown in Table 127.

Table 127: SPI Header Coding (NFCC to DH) without CRC

	First Octet	Second Octet	Third Octet	Fourth Octet
Master	0x02	0x00	0x00	0x00
Slave	0x00	0x00	MSB (Payload Length)	LSB (Payload Length)

The payload length is defined in the same manner as above. Figure 32 illustrates the procedure to transfer data from NFCC to the DH.

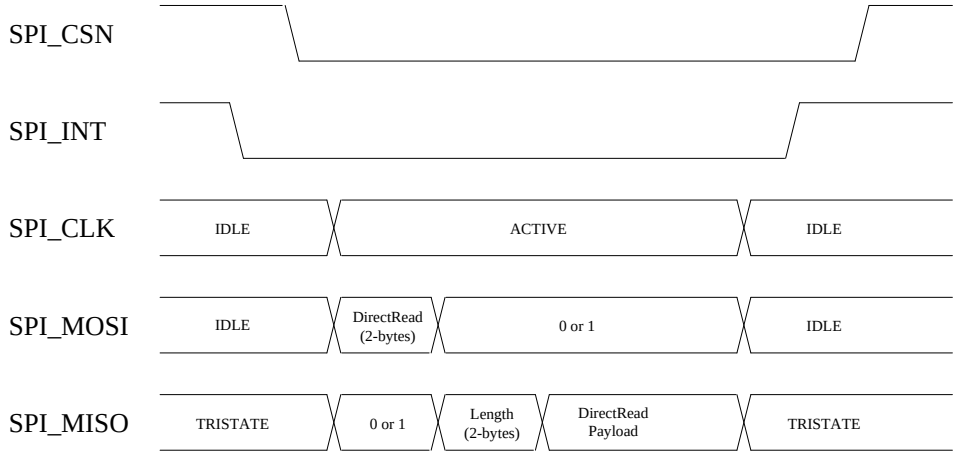

Figure 32: SPI Data Transfer from the NFCC to the DH without CRC

If the second octet is equal to 0x01, the DirectRead header is sent as shown in the table below and 2-octet CRC SHALL follow the Payload:

The CRC SHALL be the same as defined in Section 12.3.2.1.

The slave SHALL send ACK if the CRC is correct when receiving data from the master.

The slave SHALL send NAK if the CRC is not correct when receiving data from the master.

Table 128: SPI Header Coding (NFCC to DH) with CRC

	First Octet	Second Octet	Third Octet	Fourth Octet
Master	0x02	0x01	0x00	0x00
Slave	0x00	0x00	b8: NAK if set to 1b b7: ACK if set to 1b b6-b1: MSB (Payload Length	LSB (Payload Length)

Figure 33 illustrates the procedure to transfer data from NFCC to the DH when the Second Octet is equal to 0x01.

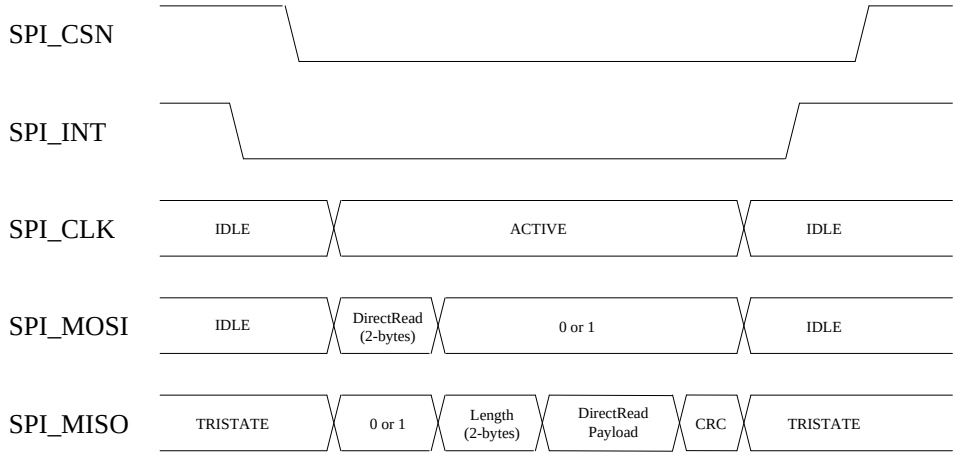

Figure 33: SPI Data Transfer from the NFCC to the DH with CRC

If the master does not assert SPI_CSN in a timely fashion, the slave is allowed to deassert SPI_INT. This can happen if the master is busy processing its FIFOs.

12.3.2.3 Race Condition

Since this is a half-duplex interface there is a possibility that both master (DH) and slave (NFCC) would want to send data at the same time. In such a race condition the master would deassert the SPI_CSN at the same time as the slave would deassert the SPI_INT. In such a situation the 2-octet header sent by the master determines the transaction type. A consequence of this is that the slave SHALL only deassert SPI_INT when it is capable of receiving a maximum-sized Direct-Write command. Figure 34 and Figure 35 illustrate such a scenario.

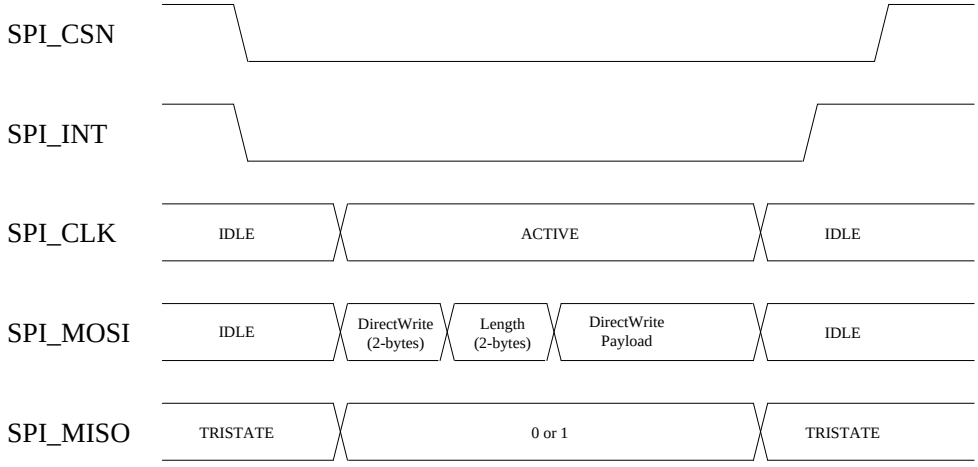

Figure 34: SPI Race Condition 1

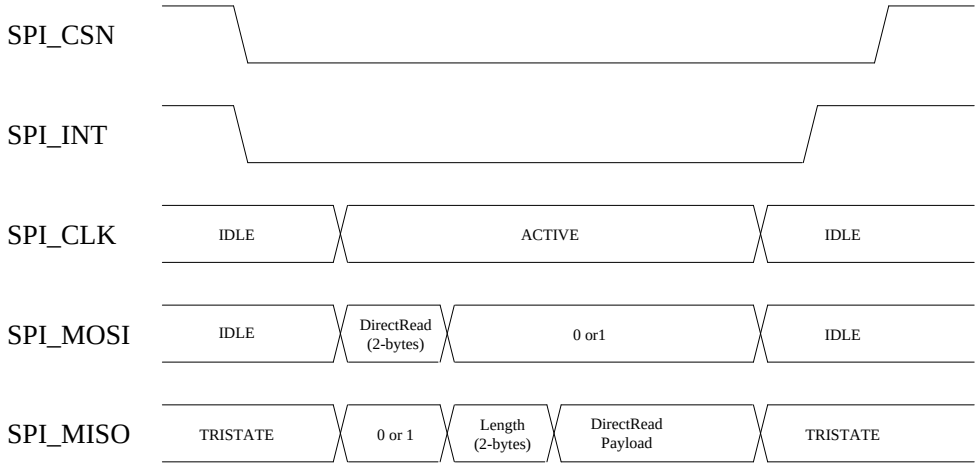

Figure 35: SPI Race Condition 2

13 Testing

The Commands, Responses and Notifications in this section provide mechanisms to facilitate testing.

13.1 Local Loopback Mode

The local loopback mode is used to verify that the NFCC can receive and loopback data.

For testing purposes the DH can enable the loopback mode by creating a Logical Connection with Destination Type value 0x01.

After the successful creation of the Logical Connection the DH MAY send Data Messages over that connection, and the NFCC SHALL loopback the same Data Messages to the DH. Flow control and segmentation and reassembly mechanisms apply also for the loopback connection.

NOTE Data Messages can be segmented differently when returning them to the DH.

A. Exhibit A

Exhibit A is left blank intentionally.

B. Common Tables

Table 129: Status Codes

Status Code	Description
Generic Status Codes	
0x00	STATUS_OK
0x01	STATUS_REJECTED
0x03	STATUS_FAILED
0x04	STATUS_NOT_INITIALIZED
0x05	STATUS_SYNTAX_ERROR
0x06	STATUS_SEMANTIC_ERROR
0x07 – 0x08	RFU
0x09	STATUS_INVALID_PARAM
0x0A	STATUS_MESSAGE_SIZE_EXCEEDED
0x0B-0x10	RFU
0x11	STATUS_OK_1_BIT
0x12	STATUS_OK_2_BIT
0x13	STATUS_OK_3_BIT
0x14	STATUS_OK_4_BIT
0x15	STATUS_OK_5_BIT
0x16	STATUS_OK_6_BIT
0x17	STATUS_OK_7_BIT
0x18-0x9F	RFU
RF Discovery Specific Status Codes	
0xA0	DISCOVERY_ALREADY_STARTED
0xA1	DISCOVERY_TARGET_ACTIVATION_FAILED
0xA2	DISCOVERY_TEAR_DOWN
0xA3-0xAF	RFU
RF Interface Specific Status Codes	
0x02	RF_FRAME_CORRUPTED
0xB0	RF_TRANSMISSION_EXCEPTION
0xB1	RF_PROTOCOL_EXCEPTION
0xB2	RF_TIMEOUT_EXCEPTION
0xB3	RF_UNEXPECTED_DATA

Status Code	Description
0xB4-0xBF	RFU
NFCEE Interface Specific Status Codes	
0xC0	NFCEE_INTERFACE_ACTIVATION_FAILED
0xC1	NFCEE_TRANSMISSION_ERROR
0xC2	NFCEE_PROTOCOL_ERROR
0xC3	NFCEE_TIMEOUT_ERROR
0xC4-0xDF	RFU
Proprietary Status Codes	
0xE0-0xFF	For proprietary use

Table 130: RF Technologies

RF Technology value	Definition
0x00	NFC_RF_TECHNOLOGY_A
0x01	NFC_RF_TECHNOLOGY_B
0x02	NFC_RF_TECHNOLOGY_F
0x03	NFC_RF_TECHNOLOGY_V
0x04 – 0x7F	RFU
0x80-0xFE	For proprietary use
0xFF	RFU

Table 131: RF Technology and Mode

Value	Description
0x00	NFC_A_PASSIVE_POLL_MODE
0x01	NFC_B_PASSIVE_POLL_MODE
0x02	NFC_F_PASSIVE_POLL_MODE
0x03	NFC_ACTIVE_POLL_MODE
0x04 – 0x05	RFU
0x06	NFC_V_PASSIVE_POLL_MODE
0x07 – 0x6F	RFU
0x70 – 0x7F	Reserved for Proprietary Technologies in Poll Mode
0x80	NFC_A_PASSIVE_LISTEN_MODE
0x81	NFC_B_PASSIVE_LISTEN_MODE
0x82	NFC_F_PASSIVE_LISTEN_MODE
0x83	NFC_ACTIVE_LISTEN_MODE
0x84 – 0xEF	RFU
0xF0 – 0xFF	Reserved for Proprietary Technologies in Listen Mode

Table 132: Bit Rates

Bit Rate value	Definition
0x00	NFC_BIT_RATE_106: 106 Kbit/s
0x01	NFC_BIT_RATE_212: 212 Kbit/s
0x02	NFC_BIT_RATE_424: 424 Kbit/s
0x03	NFC_BIT_RATE_848: 848 Kbit/s
0x04	NFC_BIT_RATE_1695: 1695 Kbit/s
0x05	NFC_BIT_RATE_3390: 3390 Kbit/s
0x06	NFC_BIT_RATE_6780: 6780 Kbit/s
0x07 – 0x1F	RFU
0x20	NFC_BIT_RATE_26: 26 Kbit/s
0x21-0x7F	RFU
0x80-0xFE	For proprietary use
0xFF	RFU

The allowed values for each technology SHALL be as defined in [DIGITAL] and [ACTIVITY].

Table 133: RF Protocols

RF Protocol value	Definition
0x00	PROTOCOL_UNDETERMINED
0x01	PROTOCOL_T1T
0x02	PROTOCOL_T2T
0x03	PROTOCOL_T3T
0x04	PROTOCOL_ISO_DEP
0x05	PROTOCOL_NFC_DEP
0x06	PROTOCOL_T5T
0x07	PROTOCOL_NDEF
0x08 – 0x7F	RFU
0x80-0xFE	For proprietary use
0xFF	RFU

NOTE The Type 4 Tag Platform is based on the ISO-DEP Protocol.

Table 134: RF Interfaces

RF Interface value	Definition
0x00	NFCEE Direct RF Interface
0x01	Frame RF Interface
0x02	ISO-DEP RF Interface
0x03	NFC-DEP RF Interface
0x04-0x05	RFU
0x06	NDEF RF Interface
0x07 – 0x7F	RFU
0x80-0xFE	For proprietary use
0xFF	RFU

Table 135: RF Interface Extensions

RF Interface value	Definition
0x00	Frame Aggregated RF Interface Extension
0x01	LLCP Symmetry RF Interface Extension
0x02 – 0x7F	RFU
0x80-0xFE	For proprietary use
0xFF	RFU

Table 136: NFCEE Protocols / Interfaces

NFCEE Interface / Protocol value	Definition
0x00	APDU
0x01	RFU
0x02	Type 3 Tag Command Set
0x03	Transparent
0x04-0x7F	RFU
0x80-0xFE	For proprietary use
0xFF	RFU

Table 137: Length Reduction Values

Value	Definition
0x00	No PSL_REQ and PSL_RES were exchanged
0x01	NFC_LR_254: 254 Bytes
0x02	NFC_LR_192: 192 Bytes
0x03	NFC_LR_128: 128 Bytes
0x04	NFC_LR_64: 64 Bytes
0x05-0xFF	RFU

Table 138: Configuration Parameter Tags

Parameter Name	Tag
Common Discovery Parameters	
TOTAL_DURATION	0x00
RFU	0x01
CON_DISCOVERY_PARAM	0x02
POWER STATE	0x03
RFU	0x04-0x07
Poll Mode – NFC-A Discovery Parameters	
PA_BAIL_OUT	0x08
PA_DEVICES_LIMIT	0x09
RFU	0x0A-0x0F
Poll Mode – NFC-B Discovery Parameters	
PB_AFI	0x10
PB_BAIL_OUT	0x11
PB_ATTRIB_PARAM1	0x12
PB_SENSB_REQ_PARAM	0x13
PB_DEVICES_LIMIT	0x14
RFU	0x15-0x17
Poll Mode – NFC-F Discovery Parameters	
PF_BIT_RATE	0x18
PF_BAIL_OUT	0x19
PF_DEVICES_LIMIT	0x1A
RFU	0x1B-0x1F
Poll Mode – ISO-DEP Discovery Parameters	
PI_B_H_INFO	0x20
PI_BIT_RATE	0x21
RFU	0x22-0x27
Poll Mode – NFC-DEP Discovery Parameters	
PN_NFC_DEP_PSL	0x28
PN_ATR_REQ_GEN_BYTES	0x29
PN_ATR_REQ_CONFIG	0x2A
RFU	0x2B-0x2E

Parameter Name	Tag
Poll Mode – NFC-V Discovery Parameters	
PV_DEVICES_LIMIT	0x2F
Listen Mode – NFC-A Discovery Parameters	
LA_BIT_FRAME_SDD	0x30
LA_PLATFORM_CONFIG	0x31
LA_SEL_INFO	0x32
LA_NFCID1	0x33
RFU	0x34-0x37
Listen Mode – NFC-B Discovery Parameters	
LB_SENSB_INFO	0x38
LB_NFCID0	0x39
LB_APPLICATION_DATA	0x3A
LB_SFGI	0x3B
LB_FWI_ADC_FO	0x3C
RFU	0x3D
LB_BIT_RATE	0x3E
RFU	0x3F
Listen Mode – T3T Discovery Parameters	
LF_T3T_IDENTIFIERS_1	0x40
LF_T3T_IDENTIFIERS_2	0x41
LF_T3T_IDENTIFIERS_3	0x42
LF_T3T_IDENTIFIERS_4	0x43
LF_T3T_IDENTIFIERS_5	0x44
LF_T3T_IDENTIFIERS_6	0x45
LF_T3T_IDENTIFIERS_7	0x46
LF_T3T_IDENTIFIERS_8	0x47
LF_T3T_IDENTIFIERS_9	0x48
LF_T3T_IDENTIFIERS_10	0x49
LF_T3T_IDENTIFIERS_11	0x4A
LF_T3T_IDENTIFIERS_12	0x4B
LF_T3T_IDENTIFIERS_13	0x4C
LF_T3T_IDENTIFIERS_14	0x4D

Parameter Name	Tag
LF_T3T_IDENTIFIERS_15	0x4E
LF_T3T_IDENTIFIERS_16	0x4F
RFU	0x51
LF_T3T_MAX	0x52
LF_T3T_FLAGS	0x53
LF_T3T_RD_ALLOWED	0x55
Listen Mode – NFC-F Discovery Parameters	
LF_PROTOCOL_TYPE	0x50
RFU	0x54
RFU	0x56-0x57
Listen Mode – ISO-DEP Discovery Parameters	
LI_A_RATS_TB1	0x58
LI_A_HIST_BY	0x59
LI_B_H_INFO_RESP	0x5A
LI_A_BIT_RATE	0x5B
LI_A_RATS_TC1	0x5C
RFU	0x5D-0x5F
Listen Mode – NFC-DEP Discovery Parameters	
LN_WT	0x60
LN_ATR_RES_GEN_BYTES	0x61
LN_ATR_RES_CONFIG	0x62
RFU	0x63-0x67
Active Poll Mode Parameters	
PACM_BIT_RATE	0x68
RFU	0x69 – 0x7F
Other Parameters	
RF_FIELD_INFO	0x80
RF_NFCEE_ACTION	0x81
NFCDEP_OP	0x82
LLCP_VERSION	0x83
RFU	0x84
NFCC_CONFIG_CONTROL	0x85

Parameter Name	Tag
RFU	0x86-0x9F
Reserved for Proprietary Use	
Reserved	0xA0-0xFE
Reserved for Extension	
RFU	0xFF

Table 139: GID and OID Definitions

GID	OID	Message Name
NCI Core 0000b	000000b	CORE_RESET_CMD CORE_RESET_RSP CORE_RESET_NTF
	000001b	CORE_INIT_CMD CORE_INIT_RSP
	000010b	CORE_SET_CONFIG_CMD CORE_SET_CONFIG_RSP
	000011b	CORE_GET_CONFIG_CMD CORE_GET_CONFIG_RSP
	000100b	CORE_CONN_CREATE_CMD CORE_CONN_CREATE_RSP
	000101b	CORE_CONN_CLOSE_CMD CORE_CONN_CLOSE_RSP
	000110b	CORE_CONN_CREDITS_NTF
	000111b	CORE_GENERIC_ERROR_NTF
	001000b	CORE_INTERFACE_ERROR_NTF
	001001b	CORE_SET_POWER_SUB_STATE_CMD CORE_SET_POWER_SUB_STATE_RSP
	001010b- 111111b	RFU
RF Management 0001b	000000b	RF_DISCOVER_MAP_CMD RF_DISCOVER_MAP_RSP
	000001b	RF_SET_LISTEN_MODE_ROUTING_CMD RF_SET_LISTEN_MODE_ROUTING_RSP
	000010b	RF_GET_LISTEN_MODE_ROUTING_CMD RF_GET_LISTEN_MODE_ROUTING_RSP RF_GET_LISTEN_MODE_ROUTING_NTF
	000011b	RF_DISCOVER_CMD RF_DISCOVER_RSP RF_DISCOVER_NTF
	000100b	RF_DISCOVER_SELECT_CMD RF_DISCOVER_SELECT_RSP
	000101b	RF_INTF_ACTIVATED_NTF
	000110b	RF_DEACTIVATE_CMD RF_DEACTIVATE_RSP

GID	OID	Message Name
		RF_DEACTIVATE_NTF
	000111b	RF_FIELD_INFO_NTF
	001000b	RF_T3T_POLLING_CMD RF_T3T_POLLING_RSP RF_T3T_POLLING_NTF
	001001b	RF_NFCEE_ACTION_NTF
	001010b	RF_NFCEE_DISCOVERY_REQ_NTF
	001011b	RF_PARAMETER_UPDATE_CMD RF_PARAMETER_UPDATE_RSP
	001100b	RF_INTF_EXT_START_CMD RF_INTF_EXT_START_RSP
	001101b	RF_INTF_EXT_STOP_CMD RF_INTF_EXT_STOP_RSP
	001110b	RF_EXT_AGG_ABORT_CMD RF_EXT_AGG_ABORT_RSP
	001111b	RF_NDEF_ABORT_CMD RF_NDEF_ABORT_RSP
	010000b	RF_ISO_DEP_NAK_PRESENCE_CMD RF_ISO_DEP_NAK_PRESENCE_RSP RF_ISO_DEP_NAK_PRESENCE_NTF
	010001b	RF_SET_FORCED_NFCEE_ROUTING_CMD RF_SET_FORCED_NFCEE_ROUTING_RSP
	010010b-111111b	RFU
NFCEE Management 0010b	000000b	NFCEE_DISCOVER_CMD NFCEE_DISCOVER_RSP NFCEE_DISCOVER_NTF
	000001b	NFCEE_MODE_SET_CMD NFCEE_MODE_SET_RSP NFCEE_MODE_SET_NTF
	000010b	NFCEE_STATUS_NTF
	000011b	NFCEE_POWER_AND_LINK_CNTRL_CMD NFCEE_POWER_AND_LINK_CNTRL_RSP
	000100b-111111b	RFU
NFCC Management	000000b-	RFU

GID	OID	Message Name
0011b	011111b	
	100000b-111111b	For proprietary use
Test Management 0100b	000000b-011111b	RFU
	100000b-111111b	For proprietary use
RFU 0101b – 1110b	000000b-111111b	RFU
Proprietary 1111b		

C. Revision History

Table 140 outlines the revision history of the NFC Controller Interface (NCI) Technical Specification.

Table 140: Revision History

Document Name	Revision and Release Date	Status	Change Notice	Supesedes
NFC Controller Interface (NCI)	Version 1 November 2012	Final		None
NFC Controller Interface (NCI)	Version 1.1 January 2014	Final	LLCP Low RF Interface Aggregated Frame RF Interface NFCID2-based listen mode routing Incorporate Cmts and TCs	Version 1November 2012
NFC Controller Interface (NCI)	Candidate Version 2.0 Mayy 2015	Candidate	Active Communication Mode Extended Listen Mode Routing NDEF-NFCEE NDEF RF Interface RF Interface extension concept Type V technology	Version 1.1 January 2014
NFC Controller Interface (NCI)	Version 2.0 Final October 2016	Final	Support of Type 5 Tags Forced NFCEE routing mechanism RF configuration for Switched Off mode	Candidate Version 2.0 Draft May 2015