NEAR FIELD COMMUNICATION

NEAR FIELD COMMUNICATION

FROM THEORY TO PRACTICE

Vedat Coskun, Kerem Ok and Busra Ozdenizci
NFC Lab – Istanbul, ISIK University, Turkey

WILEY
A John Wiley & Sons, Ltd., Publication

IPR2025-01238
Apple EX1026 Page 2

This edition first published 2012
© 2012 John Wiley & Sons Ltd

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

Coskun, Vedat.
Near field communication : from theory to practice / Vedat Coskun, Kerem Ok, and Busra Ozdenizci.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-119-97109-2 (cloth)
1. Near field communication. I. Ok, Kerem. II. Ozdenizci, Busra. III. Title.
TK6570.N43C67 2012
621.384–dc23
2011033663

A catalogue record for this book is available from the British Library.

ISBN: 9781119971092

Typeset in 10/12pt Times by Aptara Inc., New Delhi, India

The popular cards are the proximity contactless smart cards which enable a wide range of usage in a wide range of areas from health to entertainment. Various proximity coupling smart card technologies have emerged; however, only a few of them have become ISO/IEC 14443 standard which also provides interface for NFC transactions depending on the operating modes. Currently, the most famous and competing proximity contactless smart cards are MIFARE, Calypso, and FeliCa.

(i) *MIFARE*
MIFARE is a well-known and widely used 13.56 MHz contactless proximity smart card system that is being developed and is owned by NXP Semiconductors which is a spin-off company of Philips Semiconductors. MIFARE is ISO/IEC 14443 Type A Standard. Today, MIFARE is used in more than 80% of all contactless smart cards in the world.

(ii) *Calypso*
Calypso is an international electronic ticketing standard for a microprocessor contactless smartcard, originally designed by a group of European transit operators from Belgium, Germany, France, Italy and Portugal. It ensures multi-sources of compatible products, and makes possible the interoperability between several transport operators in the same area.

(iii) *FeliCa*
FeliCa is a 13.56 MHz contactless proximity high speed smart card system from Sony and is primarily used in electronic money cards. However, FeliCa did not become an ISO/IEC standard.

1.2.5 NFC as a New Technology

NFC operates between two devices over a very short communication range. NFC communication uses the 13.56 MHz spectrum as in RFID. Currently data transfer speed options are 106, 212, and 424 kbps. NFC technology operates in different operating modes; reader/writer, peer-to-peer, and card emulation where communication occurs between an NFC mobile on one side, and a passive RFID tag (NFC tag), an NFC mobile or an NFC reader on the other side. NFC technology is compared with the other technologies in terms of data transfer rate in Chapter 2, Figure 2.23. One of the NFC technology's major properties is its implicit security because of short communication distance. Close proximity of two devices makes the signal interception probability very low. The other property is the automatic implicit pairing capability of NFC. An installed application on a mobile device is automatically launched when it finds the matching pair.

1.3 NFC Essentials

As the basics of the used technology are provided above, we can now introduce essential NFC technical details. In order to do this, NFC structure and the NFC devices (NFC tag, NFC reader, and NFC mobile) must be explained in enough detail. The communication is based on the existing standards, and the devices stick to those standards for a seamless activation. Hence, we also will provide information on the standardization bodies which steer NFC technology.

IPR2025-01238
Apple EX1026 Page 4

1.3.1 Smart NFC Devices

NFC devices are the acting components of NFC. NFC is available using three NFC devices: the NFC mobile, NFC reader and NFC tag.

- *NFC enabled mobile phone:* NFC enabled mobile phones which are also referred to as NFC mobiles are the most important NFC devices. Currently, integration of NFC technology with mobile phones (thus introducing NFC enabled mobile phones) creates a big opportunity for the ease of use and acceptance of the NFC ecosystem.
- *NFC reader:* An NFC reader is capable of data transfer with an NFC component. The most common example is the contactless POS (Point of Sale) terminal which can perform contactless NFC enabled payments when an NFC device is touched against the NFC reader.
- *NFC tag:* An NFC tag is actually an RFID tag that has no integrated power source.

NFC works in a very intuitive way. Two NFC devices immediately start their communication as they are touched. The touching action is taken as the triggering condition for NFC communication. This is actually an important feature of NFC technology. In the NFC case, the NFC application is designed so that when the mobile touches some NFC component with the expected form of data, it boots up. Hence, the user does not need to interact with the mobile device after she touches one appropriate NFC device which may be an NFC tag, an NFC reader, or another NFC enabled mobile phone. This is a very useful property of NFC communication that provides ubiquitous computing.

For each NFC communication session, the party that starts or initiates the communication is called the initiator, whereas the device that responds to the requests of the initiator is called the target. This case is analogous to the well-known client server architecture. Remember that in a client server communication the client initiates the communication and the server responds. In NFC communication, it is no different.

In an active/passive device approach, when an NFC component has an embedded power source, it can generate its own RF field, and naturally initiates and leads communication. This device is called an active device. On the other hand, if it does not have any embedded power source, it is called a passive device and can only respond to the active device.

The initiator always needs to be an active device, because it requires a power source to initiate the communication. The target, however, may be either an active or a passive device. If the target is an active device, then it uses its own power source to respond; if it is a passive device, it uses the energy created by the electromagnetic field which is generated by the initiator that is an active device.

Consider an NFC tag which is a low cost and low capacity device. It does not contain any power source and needs an external power source to perform any activity. Thus, an NFC tag is always a passive device and always a target, since it does not include any energy source by design. It stores data that can be read by an active device.

1.3.2 Standardization of NFC Enabled Mobile Phones

NFC technology was jointly developed by Philips and Sony in late 2002 for contactless communications. Europe's ECMA International adopted the technology as a standard in December

IPR2025-01238
Apple EX1026 Page 5

2002. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) adopted NFC technology in December 2003. In 2004, Nokia, Philips, and Sony founded the NFC Forum to promote the technology. NFC technology standards are acknowledged by ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission), ETSI (European Telecommunications Standards Institute), and ECMA (European Computer Manufacturers Association).

NFC is a joint adventure of various technologies. Smart cards, mobile phones, card readers, short range communication, secure communication, transaction and payment systems are the most significant leading technologies. As several technologies are involved, related organization bodies have provided the respective standards. The integrated form of those standards will hopefully define a common vision for secure and yet functional usage and transaction. An interoperable set of standards is essential for a successful NFC ecosystem. The most dominant standardization organizations are:

(i) *NFC Forum*

NFC Forum is an alliance for specifying the NFC standards built on ISO/IEC standards. NFC Forum was established with the aim of enabling NFC technology and making it spread throughout the world. NFC Forum is a non-profit industry association formed to improve the use of NFC short range wireless interaction in consumer electronics, mobile devices, and PCs. NFC Forum promotes implementation and standardization of NFC technology to ensure interoperability between devices and services. The mission of the NFC Forum is to promote the usage of NFC technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology.

NFC Forum has standardized two operating modes (reader/writer and peer-to-peer operating modes) up to now. Record Type Definition (RTD) and NFC Data Exchange Format (NDEF) specifications are provided by NFC Forum for reader/writer mode communication. Within peer-to-peer mode, Logical Link Control Protocol (LLCP) is used to connect peer-to-peer based application to the RF layer. Card emulation mode on the other hand, provides smart card capability for mobile phones.

Another important development introduced by NFC Forum is the "N-Mark" trademark which is a universal symbol for NFC, so that consumers can easily identify where their NFC enabled devices can be used.

(ii) *GlobalPlatform*

GlobalPlatform is a cross industry, non-profit association which identifies, develops and publishes specifications that facilitate secure and interoperable deployment and management of multiple embedded applications on secure smart cards. The goal of the GlobalPlatform specifications is to ensure interoperability on content management of smart cards, managing smart cards without any dependencies on hardware, manufacturers, or applications.

(iii) *GSM Association* (*GSMA*)

GSMA is an association of mobile operators and related companies devoted to supporting the standardization, deployment and promotion of GSM. GSMA represents the interests of the worldwide mobile communications industry. GSMA is focused on innovating, incubating and creating new opportunities for its members, all with the ultimate goal of driving the growth of the mobile communications industry.

(iv) *ISO/IEC*
ISO is the world's largest developer and publisher of international standards. It is a non-governmental organization that forms a bridge between the public and private sectors. IEC is a non-profit international organization that prepares and publishes international standards for all electrical, electronic and related technologies. ISO and IEC work together to provide worldwide standards.

(v) *ECMA International*
ECMA International is an international non-profit standardization organization for information and communications systems. ECMA studies include mobile devices and NFC.

(vi) *ETSI and ETSI Smart Card Platform* (*ETSI SCP*)
ETSI is a non-profit organization with 700+ members. The ETSI produces globally applicable standards for Information and Communications Technologies (ICT), including fixed/mobile, radio, broadcast and Internet technologies. ETSI SCP handles Subscriber Identity Module (SIM) specifications that would enable SIM cards to carry NFC applications or to play other roles within NFC phones.

(vii) *Java Community Process* (*JCP*)
JCP holds the responsibility for the development of Java technology which indeed is a prominent candidate for NFC applications as well. As an open, inclusive organization of active members and non-member public input, it primarily guides the development and approval of Java technical specifications.

(viii) *Open Mobile Alliance* (*OMA*)
OMA develops open standards for the mobile phone industry. OMA members include many companies including the world's leading mobile operators, device and network suppliers, information technology companies and content and service providers.

(ix) *3rd Generation Partnership Project* (*3GPP*)
3GPP is a collaboration between groups of telecommunications associations to make a globally applicable third generation (3G) mobile phone system specification. 3GPP specifications are based on evolved GSM specifications.

(x) *EMVCo*
EMVCo aims to ensure global interoperability between chip cards and terminals on a global basis regardless of the manufacturer, the financial institution or the card issuer. EMV 2000 specifications are an open standard set for smart card based payment systems worldwide and seek collaboration in mobile payment standards.

1.3.3 General Architecture of NFC Enabled Mobile Phones

Mobile devices those are integrated with NFC technology contain NFC specific ICs such as SEs and an NFC interface (see Chapter 3, Figure 3.7). The NFC interface is composed of an analog/digital front-end called an NFC Contactless Front-end (NFC CLF), an NFC antenna and an NFC controller to enable NFC communication. The NFC controller enables NFC communication of the mobile phone with the external NFC device. An NFC enabled mobile phone requires an SE for performing secure transactions with the external NFC devices. The SE provides a secure environment for related programs and data. It enables storage of sensitive data of the user. It also enables secure storage and execution of NFC enabled services such as

IPR2025-01238
Apple EX1026 Page 7

contactless payments. Various standards have already been defined for NFC communication between two NFC enabled devices, and data transfer within the NFC mobile phone such as Single Wire Protocol (SWP) or the NFC Wired Interface (NFC-WI).

The host controller can be identified as the heart of any mobile phone. A Host Controller Interface (HCI) creates a bridge between the NFC controller and the host controller. The HCI is a logical interface which allows an NFC interface including front-end to communicate directly with an application processor and multiple SEs in mobile devices.

1.3.4 Near Field Communication Interface and Protocol (NFCIP)

At the physical layer, the Near Field Communication Interface and Protocol (NFCIP) is standardized in two forms as NFCIP-1 which defines the NFC communication modes on the RF layer and other technical features of the RF layer, and NFCIP-2 which supports mode switching by detecting and selecting one communication mode.

(i) *Near Field Communication Interface and Protocol-1 (NFCIP-1)*
NFCIP-1 standard defines two communication modes as active and passive. It also defines RF field, RF communication signal interface, and general protocol flow. Moreover, it defines transport protocol including protocol activation, data exchange protocol with frame architecture and error detecting code calculation (CRC for both communication mode at each data rate), and protocol deactivation methods.

(ii) *Near Field Communication Interface and Protocol-2* (*NFCIP-2)*
NFCIP-2 standard specifies the communication mode selection mechanism and is designed not to disturb any on-going communication at 13.56 MHz for devices implementing NFCIP-1, ISO/IEC 14443 and ISO/IEC 15693.

1.4 NFC Operating Modes and Essentials

Remember that there may three major smart devices in NFC; NFC enabled mobile phones, NFC readers, and NFC tags. NFC communication occurs between two NFC devices with some valid combinations. For example, a mobile phone may communicate with an NFC reader.

As NFC occurs within a very close range, it is very common to touch the communicating devices against each other. For this reason, this process is called touching paradigm. User awareness is definitely a must in order to perform NFC. The user first interacts with a smart object (that is either an NFC tag, NFC reader, or another NFC mobile) using a mobile phone (see Chapter 4, Figure 4.3). After the touching activity occurs, the mobile device may make use of the received data and use mobile services as well, such as opening a web page, making a web service connection and so on.

1.4.1 NFC Operating Modes

There are three operating modes, reader/writer, peer-to-peer, and card emulation, as already mentioned. The reader/writer mode enables one NFC mobile to exchange data with one NFC tag. The peer-to-peer mode enables two NFC enabled mobiles to exchange data with each

other. In card emulation mode, a mobile phone can be used as a smart card to interact with an NFC reader. Each operating mode has a different technical infrastructure as well as benefits for the users.

(i) *Reader/writer mode*
This mode provides communication of an NFC mobile with an NFC tag. The purpose of the communication is either reading or writing data from or to a tag by the mobile phone. We can further categorize the mode into two different modes: reader mode and writer mode. In reader mode, the mobile reads data from an NFC tag; whereas in writer mode, the mobile phone writes data to an NFC tag.

(ii) *Peer-to-peer mode*
Two NFC mobiles using this mode exchange any data between each other. Since both mobiles have integrated power, each one uses its own energy by being in active mode in this mode. Bidirectional half duplex communication is performed in this mode similar to other modes, meaning that when one device is transmitting, the other has to listen and can start transmitting data after the first one finishes.

(iii) *Card emulation mode*
This mode provides the opportunity for an NFC mobile to function as a contactless smart card. Some examples of emulated contactless smart card are credit cards, debit cards, loyalty cards and so on. One NFC mobile may even store multiple contactless smart card applications concurrently. The card emulation mode is an important mode since it enables payment and ticketing applications and is compatible with existing smart card infrastructure.

1.4.2 Reader/Writer Mode Essentials

As already mentioned, the underlying technical architecture of each mode differs. The standards and specifications used by each mode may also differ. In reader/writer operating mode, an active NFC enabled mobile phone initiates the wireless communication, and can read and alter data stored in NFC tags. First, the used RF interface in this mode is compliant to ISO/IEC 14443 Type A, Type B and FeliCa schemes which are contactless smart card interfaces (see Chapter 3, Figure 3.24). The applications operating in reader/writer mode usually do not need a secure area in the NFC enabled mobile phone; the process is only reading data stored inside the tag and writing data to the tag.

In this operating mode, NFC Forum performed various specifications and standards in tag types, operation of tag types, and data exchange format between devices. An NFC enabled mobile phone is capable of reading NFC Forum mandated tag types. Four tag types have been defined by NFC Forum, and are designated as Type 1, Type 2, Type 3 and Type 4. Each tag type has a different format and capacity. NFC tag type formats are based on either ISO 14443 Type A, ISO 14443 Type B, or Sony FeliCa.

The other important standard is the NDEF. NDEF is a data format to exchange information between two NFC devices; namely, between an active NFC mobile and a passive tag, or an active NFC mobile and an active NFC mobile.

NDEF is a binary message format designed to encapsulate one or more application-defined payloads into a single message construct. An NDEF message contains one or more NDEF

IPR2025-01238
Apple EX1026 Page 9

records and those records can be chained together to support larger payloads. Various record types for NDEF messaging format are defined by NFC Forum for specific cases; smart posters, URIs, digital signature, and text.

The record types defined for smart posters are the most used. For example, with the defined smart poster record types, URLs, SMSs or phone numbers can be put on an NFC Forum mandated tag. By touching an NFC device to the tag, this information can be read and processed afterwards. The smart poster contains data that will trigger an application in the device such as launching a browser to view a website, sending an SMS to a premium service to receive a ring tone, and so on.

1.4.3 Peer-to-Peer Mode Essentials

In peer-to-peer mode, two NFC enabled mobile phones establish a bidirectional, link level connection to exchange information as depicted in Chapter 3, Figure 3.29. They can exchange virtual business cards, digital photos, and any other kind of data or perform Bluetooth pairing, and so on. Peer-to-peer operating mode's RF communication interface is standardized by ISO/IEC 18092 as NFCIP-1. Also NDEF message is used in this mode which is received over LLCP that is also defined by NFC Forum. The data format is the same as that used in reader/writer mode.

LLCP as a data link layer protocol supports peer-to-peer communication between two NFC enabled devices which is essential for any NFC application that involves a bidirectional communication. LLCP specification defines five major services: connectionless transport, connection oriented transport, link activation-supervision-deactivation, asynchronous balanced communication and protocol multiplexing.

1.4.4 Card Emulation Mode Essentials

In card emulation mode, an NFC enabled mobile phone acts as a smart card. Either an NFC enabled mobile phone emulates an ISO 14443 smart card or a smart card chip integrated in a mobile phone is connected to the antenna of the NFC module. When the user touches the mobile phone to an NFC reader, the NFC reader initiates the communication. This operating mode is useful for secure transactions such as contactless payment, ticketing applications and access control.

As depicted in Chapter 3, Figure 3.32, when an NFC reader interacts with an NFC device, the NFC device acts like a standard smart card, thus the NFC reader interacts with the SE and its applications. Only the card emulation mode uses an SE efficiently and performs functions securely.

1.4.5 Case Studies

We present the following three case studies at the end of Chapter 4 to clarify the three operating modes and their usages thoroughly:

1. The NFC enabled shopping system enables users to shop online anywhere they want, so that no geographical restrictions are set. This use case employs the reader/writer mode.

2. The NFC based gossiping application works in the same way as gossiping and disseminates information between the parties. This use case employs the peer-to-peer mode.
3. The cinema ticketing application enables payment to be made. This use case employs the card emulation mode.

In each use case, initially the description of the case is given. Use case diagrams, activity diagrams, and generic usage models follow. The first and second use cases are also implemented with Java in Chapter 5. The codes may run in emulator or mobile phone after successful implementation. The third use case's ecosystem environment and business models are analyzed in Chapter 7.

1.5 SE and Its Management

In order to provide secure storage and execution of NFC enabled applications, an SE is essential. The SE is actually a combination of hardware, software, interfaces, and protocols. Since secure functions are mostly provided in card emulation mode, an SE is mostly used in that mode as well. When an SE is used appropriately, that is, according to the provided standards, the users and service providers are assured about the security of the overall process. Currently various SE alternatives are being considered, but the most popular ones are (see Chapter 3, Figure 3.10):

- Embedded hardware;
- Secure Memory Card (SMC);
- Universal Integrated Circuit Card (UICC).

(i) *Embedded hardware*
The embedded SE is a non-removable component within a mobile phone. This chip is embedded into a mobile phone during the manufacturing stage and it must be personalized after the device is delivered to the end user. This embedded SE chip obviously cannot be transferred to other mobile phones. It has to be replaced and personalized every time the mobile phone is used by another user. The SE of a new mobile phone must be personalized for the user.

(ii) *SMC*
A removable SMC is made up of memory, embedded smart card element and smart card controller. In other words, it is a combination of a memory card and a smart card. With the removable property and a large capacity memory, the SMC based SE can host a large number of applications, and does not need to be reissued when the customer buys a new mobile phone.

(iii) *UICC*
The UICC is the physical smart card that the Subscriber Identity Module (SIM) or Universal Subscriber Identity Module (USIM) is implemented upon. Therefore it is commonly known as a SIM or USIM. A UICC based SE is a removable smart card used in mobile terminals in GSM and UMTS networks.

IPR2025-01238
Apple EX1026 Page 11

well as non-telecom applications such as payment, loyalty, ticketing, e-passport, and so on.

Today, UICC based SEs provide an ideal environment for NFC applications. They are personal, secure, portable and easily managed remotely via OTA technology (see Chapter 8). The cardholders can be reassured that transactions are executed with their personal information protected. Service providers, who deploy NFC enabled applications, do not risk losing customers when cardholders change handsets.

3.3.2 NFC Interface

The NFC interface is composed of a contactless, analog/digital front-end called an NFC Contactless Front-end (NFC CLF), an NFC antenna and an IC called an NFC controller to enable NFC transactions as shown in Figure 3.11.

The NFC controller enables the NFC link in a mobile phone. It works as a modulator and demodulator between the analog RF signal and the NFC antenna. To connect the NFC antenna to the NFC controller, usually a few passive components are needed such as capacitors, resistors, and inductors. The NFC controller supports both active and passive communication with various modulation types. Typically, an NFC controller is compliant with NFCIP-1 protocol (peer-to-peer mode), and with other two operating modes (reader/writer and card emulation modes). Also, other RFID protocols such as ISO/IEC 15693 are often supported.

NFC CLF is the analog front-end of the NFC controller. The NFC CLF logical interface defines the protocol on top of the data link layer, as well as how the messages are transmitted between the SE and the NFC CLF. It is theoretically independent from the underlying interface (i.e., physical and data link interface) which carries the messages.

All SE design models have an interface between the SE and the NFC controller and also between the host controller and the NFC controller. The data transmitted via the contactless interface are directly forwarded by the NFC controller to the SE and vice versa. The host controller (i.e., the non-secure part of the system) is not involved in the transaction.

3.3.3 Interface between SE and NFC Controller

There are various technical options for designing the interface between the SE and the NFC controller. The most promising two options are NFC-WI and SWP. The most important difference between them is that SWP uses one physical line whereas NFC-WI uses two lines. It is worth mentioning that they are not alternatives to each other but options to be used in certain places instead.

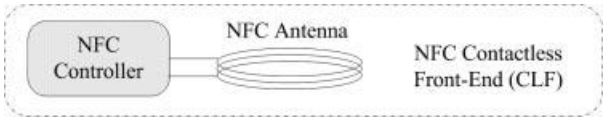

Figure 3.11 NFC interface.

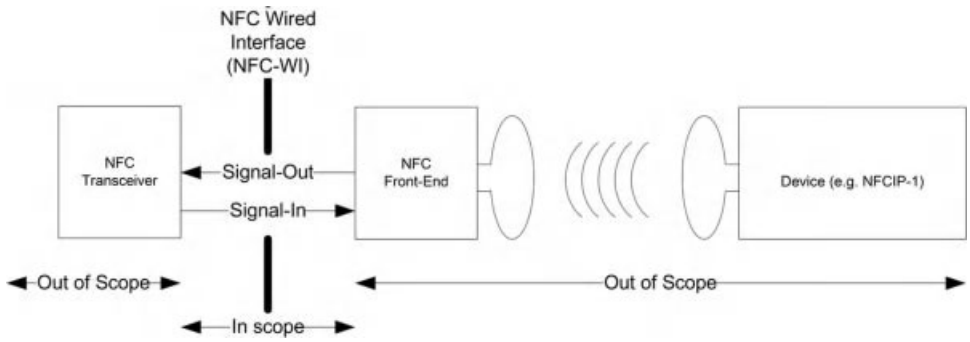

Figure 3.12 NFC-WI architecture [3].

(i) *NFC-WI*

NFC-WI (also called S2C) is a digital wire interface standardized by ECMA 373, ISO/IEC 28361 as well as ETSI TS 102 541. The SE is defined as a transceiver and the NFC controller is defined as front-end in this protocol. The SE is connected to the NFC controller via two wires [3]. NFC-WI defines the Signal-In (SIGIN) and the Signal-Out (SIGOUT) wires between the transceiver and front-end as illustrated in Figure 3.12. In the standard [3], the transceiver is the entity that drives the SIGIN wire and receives on the SIGOUT wire. The front-end is the entity that drives the SIGOUT wire and receives on the SIGIN wire.

This digital wire interface carries two binary signals which are defined as HIGH and LOW. Both of them transmit modulation signals between the NFC controller and the SE and are digitally received or sent by the RF interface. The transceiver drives the SIGIN wire with a binary signal of either HIGH or LOW. The front-end receives the binary signal that is on the SIGIN wire. The front-end drives the SIGOUT wire with a binary signal of either HIGH or LOW. The transceiver receives the binary signal that is on the SIGOUT wire.

Three transmission rates supported by NFC-WI are 106, 212 and 424 kbps. At 106 kbps (see Figure 3.13), the data stream from the NFC controller to the transceiver (SIGIN) shall carry the AND combination of the Modified Miller bit encoded data with 13.56 MHz. In the opposite direction (SIGIN) the data stream is Manchester encoded and then inverted by a logical OR operation with 848 kHz. At 212 and 424 kbps, the data stream from the NFC controller for transceiver (SIGIN) is Manchester encoded and then inverted by a logical XOR operation with 13.56 MHz. This corresponds to a PSK (Phase Shift Keying) modulation of the clock signal. In the opposite direction (SIGIN), the data stream is again Manchester encoded.

NFC-WI is fully compliant and directly coupled with all modes, types and data rates of ISO/IEC 18092 and ISO/IEC 14443, and no additional adaptation and no protocol conversion is required. It is a reliable concept which is feasible for immediate implementation as well.

(ii) *SWP*

The next physical interface option is the SWP which defines a single-wire connection between the SE and the NFC controller in the mobile phone in contrast to the NFC-WI

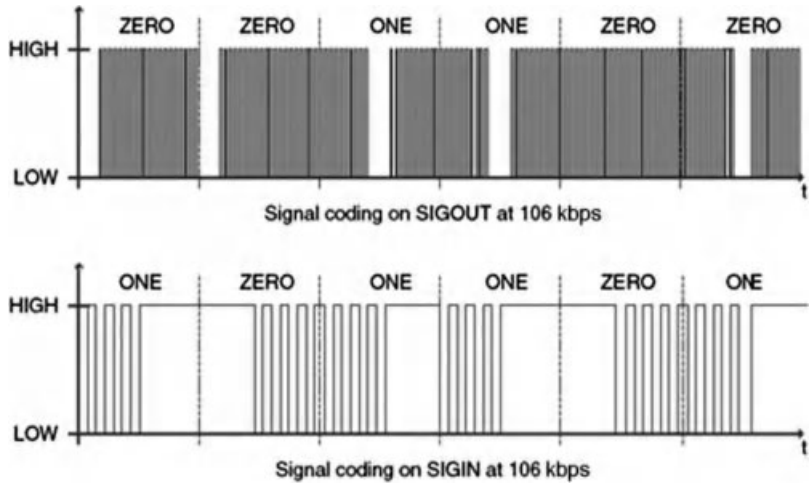

Figure 3.13 Transmission of NFC controller's modulation signals at 106 kbps [2].

double wire connection. SWP is standardized by ETSI TS 102 613. SWP is a digital full duplex protocol [4]. The data rate is scalable from 212 kbps to 1.6 Mbps for a distance that is less than 10 cm. The SWP interface is a bit oriented and point-to-point communication protocol between an SE and an NFC controller as shown in Figure 3.14. The working principle is similar to that of master and slave; the NFC controller is comparable with the master and the SE is comparable with the slave.

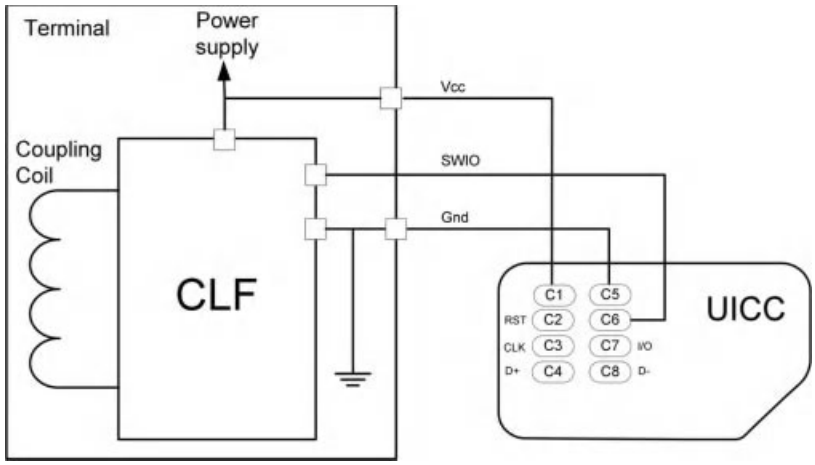

Figure 3.14 CLF-UICC physical link (SWP Architecture). © European Telecommunications Standards Institute 2008. Further use, modification, redistribution is strictly prohibited. ETSI standards are available from http://pda.etsi.org/pda/.

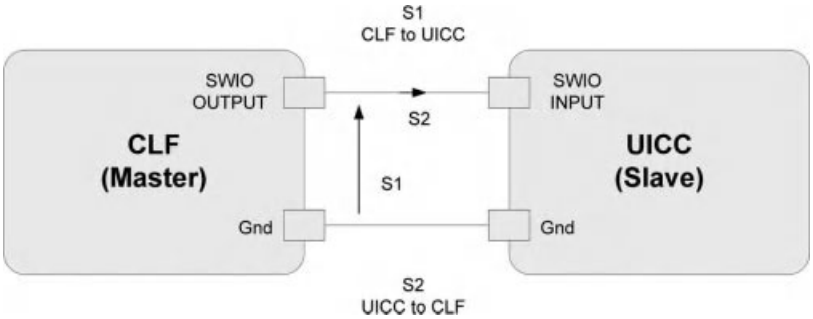

Figure 3.15 SWP data transmission. © European Telecommunications Standards Institute 2008. Further use, modification, redistribution is strictly prohibited. ETSI standards are available from http://pda.etsi.org/pda/.

The SWP is mainly intended to be used by UICC cards in mobile phones since only one of the standard eight contact paths is available for the SWP function. A special case occurs here as shown in Figure 3.14, so that the voltage (Vcc) of the UICC card is not directly supplied by the mobile phone, but supplied through the NFC interface instead. This is necessary for contactless data transmission with SEs even when the battery is exhausted. If the NFC interface is close to an NFC reader, the reader field supplies energy to the SE through the NFC interface. Remember that the NFC mobile operates in the passive mode in this case.

This way the NFC controller and the SE can be used in card emulation mode. Thus card emulation mode applications which have a high operational security and contactless functionality requirement no longer rely on the battery's charging state.

The data to be transmitted are represented by the binary states of voltage (S1) and current (S2) on the single wire (see Figure 3.15). The data transmission from the NFC interface to the SE is carried out by modulating signal S1. In the reverse direction, the data are transmitted by modulating signal S2.

On top of the physical layer, a bit oriented Medium Access and Control (MAC) layer based HDLC (High-Level Data Link Control) is implemented. The HDLC protocol is used for controlling data transmission between the NFC interface and the SE. The HDLC protocol is standardized as ISO/IEC 13239 which is one of the oldest communication protocols. It provides efficient error detection and correction, sign synchronization, and flow control.

SWP carries short packets (payload less than 30 bytes) to the application layer and allows the routing of messages to different components within the mobile. Using short packets and pipelining allow communication with low latency between the SE and the NFC interface. It uses a tunneling technique, so that any frame can be encapsulated in a SWP frame from/to the SE [5].

3.3.4 Host Controller and HCI

The HCI is a logical interface which allows an NFC interface to communicate directly with an application processor and multiple SEs. The HCI may be used in various electronic devices

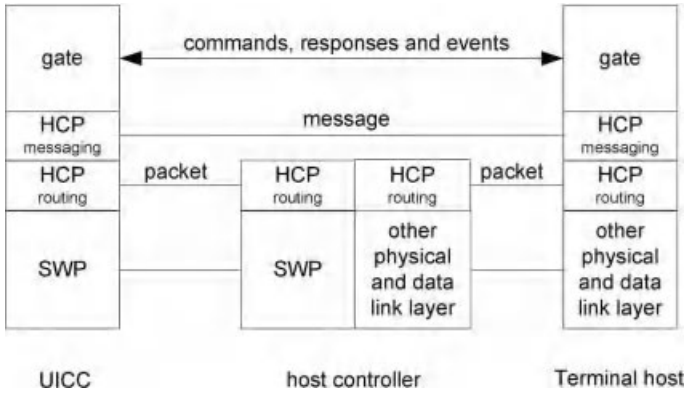

Figure 3.16 HCP Stack in a host network. © European Telecommunications Standards Institute 2008. Further use, modification, redistribution is strictly prohibited. ETSI standards are available from http://pda.etsi.org/pda/. Note: For clarity, only two gates are shown. Host controller has also gates to connect via HCP to other hosts.

such as mobile devices, PDAs and PC peripherals. For NFC enabled mobile phones, it enables faster integration of NFC functionality. The HCI is standardized in ETSI TS 102 622 [6].

The HCI defines the interface between logical entities called *hosts* that operate one or more service(s). According to the ETSI terminology, a network of two or more hosts is called a *host network*; and one of the hosts that is also responsible for managing a host network is called a *host controller*. In a host network which has a star topology, all hosts are connected to the host controller. The HCI has three components: a collection of gates that exchange commands, responses, and events; a Host Controller Protocol (HCP) messaging mechanism; and an HCP routing mechanism that may optionally segment messages when required (see Figure 3.16).

Data link layers of the HCP need to be error free so that the order of sent and received data can be trusted. The data link layer should also enable data flow control, fragment the upper layer's packets to a maximum size, and report each received packet's size to its upper layer.

(i) *Gates*

A gate provides an entry point for the services operating in a host. HCP enables gates from several hosts to exchange messages. There are two types of gates: management gates that host network management, and generic gates.

Each gate type has a gate identifier which is either unique (values "10" to "FF") or not (values "00" to "0F"). Each host must have several pre-defined gates, including administration, identity management, link management, and loop back gates.

(ii) *Pipes*

Gates communicate with each other through logical communication channels called pipes. There are two types of pipes: static pipes and dynamic pipes. Static pipes do not need to be created and cannot be deleted; however, dynamic pipes can be created and deleted. The state of a pipe can be either opened or closed. The state of the pipe

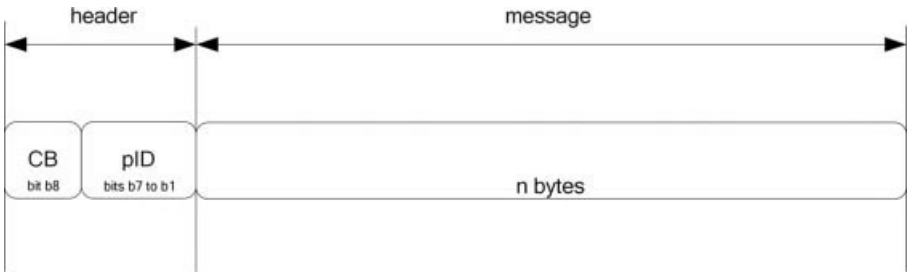

Figure 3.17 HCP packets. © European Telecommunications Standards Institute 2008. Further use, modification, redistribution is strictly prohibited. ETSI standards are available from http://pda.etsi.org/pda/.

remains persistent even if the host is powered down and up or a host is removed from the network.

The length of the pipe identifier (pID) is 7 bits. It is used in the header of HCP packets for routing information. Pipe identifiers of dynamic pipes are dynamically defined by the host controller, whereas pipe identifiers of static pipes are pre-defined.

(iii) *HCP packets*

The HCP packets are exchanged between the hosts and the host controller (see Figure 3.17); and it contains the following segments:

- *CB* is the chaining value which takes value "1" for the last packet of a fragmented message or value "0" for a packet that belongs to a fragmented message.
- *pID* is the pipe identifier.
- *Message* carries one instruction and optional data as depicted in Figure 3.18. TYPE identifies the type of instruction. INSTRUCTION can be a command (TYPE = 0), an event (TYPE = 1) or a command response (TYPE = 2).

(iv) *Registries*

Registries are 1 byte long identifiers and are used to define unique parameters related to every gate. The host is responsible for management of its registries. For every pipe, a new registry instance is created and registry parameters are set. When a pipe is removed from the network, its registry instance is removed too.

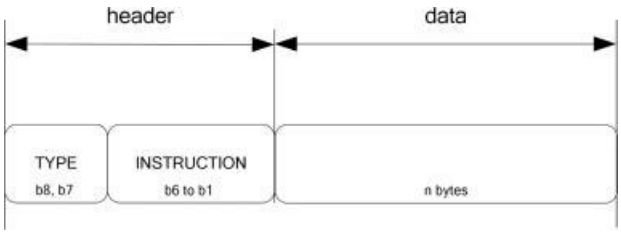

Figure 3.18 HCP message structure. © European Telecommunications Standards Institute 2008. Further use, modification, redistribution is strictly prohibited. ETSI standards are available from http://pda.etsi.org/pda/.

(v) *HCI procedures*
The following procedures are defined in ETSI TS 102 622:
- *Pipe creation* which describes how a host requests dynamic pipe creation between one of its gates and a gate in another host.
- *Registry access* which defines how a host can read/write parameters in the registry of another host.
- *Host and gate discovery* which defines how a host discovers other hosts in a host network as well as the gates.
- *Session initialization* which defines how a host can detect changes in recovery mechanisms.
- *Loop back testing* which defines how a host can verify the pipe connectivity to another host.

3.4 Physical Layer of NFC

NFC technology is based on RFID technology in a proximity range at 13.56 MHz. NFC transfers data at up to 424 kbps. The communication between two NFC devices is standardized in ISO/IEC 18092 standard as NFCIP-1. This standard defines only device-to-device communication for both active and passive communication modes. However, the RF layer of NFC is a super set of the standard protocols which is also compatible with the ISO/IEC 14443 standard (i.e., contactless proximity smart card standard) and JIS X 6319 standard as FeliCa (i.e., another contactless proximity smart card standard by Sony) as well as ISO/IEC 15693 standard (i.e., contactless vicinity smart card standard). These smart card interfaces similarly operate at 13.56 MHz from card reader to smart card with distinct data rates and communication ranges. Table 3.5 gives a short summary and comparison of ISO/IEC 14443, ISO/IEC 15693, and ISO/IEC 18092 communication interfaces. In this section, background knowledge about the proximity range communication interfaces used by NFC technology is given and then data transmission features of the RF layer are explained.

3.4.1 ISO/IEC 14443 – Proximity Contactless Smart Card Standard

As described in ISO/IEC 14443, proximity transactions are based on an electromagnetic coupling between a proximity card and RFID reader which uses an embedded microcontroller (including its own processor and one of several types of memory) and a magnetic loop antenna that operates at 13.56 MHz. ISO/IEC 14443 enables contactless transactions between a reader device and a proximity card used for identification. Usually this proximity card uses the

Table 3.5 Summary of communication interface standards

Parameters	ISO/IEC 18092	ISO/IEC 14443	ISO/IEC 15693
Operating Mode	Peer-to-peer	Reader-to-card	Reader-to-card
Communication Mode	Active and passive	Passive	Passive
Range	Proximity	Proximity	Vicinity
Data Rate	106, 212, 424 kbps	106 kbps	$\leq$26 kbps

IPR2025-01238
Apple EX1026 Page 18

Table 3.6 Parts of ISO/IEC 14443 standard

Part Name	Content
Part 1- Physical Characteristics of Contactless Smart Cards (PICC)	Defines physical characteristics of a contactless smart card, lists several requirements and tests that need to be performed at card level for construction of the card and antenna design and so on.
Part 2 - RF Power and Signal Interface	Defines the RF power and signal interface, Type A and Type B signaling schemes, and also determines how the card is powered by RF field and so on.
Part 3 – Initialization and Anti-collision	Defines the initialization and anti-collision protocols for Type A and Type B, as well as anti-collision commands, responses, data frame and timing
Part 4 – Transmission Protocol	Determines the high-level data transmission protocols for Type A and Type B which are optional protocols, thus proximity cards may be designed with or without support for Part 4 protocols

standard credit card form factor defined by ISO/IEC 7810 ID-1, but other form factors – such as tokens or key fobs – are also possible. ISO/IEC 14443 uses the terms PICC (Proximity Integrated Circuit Card) and PCD (Proximity Coupling Device) to describe the components taking part in a transaction. PCD refers to a proximity card reader whereas PICC refers to a proximity card.

The ISO/IEC 14443 standard contains four major parts (see Table 3.6): the physical characteristics are explained in the first part, RF power and signal interface are explained in the second part, initialization and anti-collision protocols constitute the third part, and the transmission protocol is defined in the fourth part [2]. It also defines two major contactless cards, namely Type A and Type B.

3.4.1.1 Major Operating Principles of ISO/IEC 14443

Contactless proximity smart cards operating at 13.56 MHz are powered by and communicate with the reader via inductive coupling of the reader antenna to the card antenna. An alternating magnetic field is produced by sinusoidal current flowing through the reader antenna loop. When a card enters the alternating magnetic field generated by a reader, an alternating current (AC) is induced in the card loop antenna. The PICC IC contains a rectifier and powers the regulator to convert the AC to direct current (DC) to power the IC. The reader amplitude modulates the RF field to send information to the card. The IC contains a demodulator to convert the amplitude modulation to digital signals. The IC also contains a clock extraction circuit that produces a 13.56 MHz digital clock signal for use within the IC. The data from the reader are clocked in, decoded, and processed by the IC. The IC communicates with the reader by modulating the load on the card antenna and the load on the reader antenna. ISO/IEC 14443 PICC uses a 847.5 kHz subcarrier for load modulation which allows the reader to filter the subcarrier frequency off the reader antenna and decode the data.

3.4.1.2 Major Proximity Contactless Smart Card Technologies

Up to now, various proximity coupling smart card technologies have emerged; however only a few of them are compatible with ISO/IEC 14443 standard. Currently, the most famous and competing contactless smart cards are MIFARE, Calypso, and FeliCa:

(i) *MIFARE*
MIFARE is a well-known and widely used 13.56 MHz contactless proximity smart card system that is being developed and is owned by NXP semiconductors which is a spin-off company of Philips Semiconductors. MIFARE is ISO/IEC 14443 Type A standard. As of 2011, MIFARE is used in more than 80% of all contactless smart cards in the world. The MIFARE family contains different types of cards such as Ultralight, Standard, Desfire, Classic, Plus, and SmartMX [7]. MIFARE Classic cards have varying memory sizes. MIFARE based smart cards are being used in an increasingly broad range of applications mostly in public transport ticketing and also for access management, e-payment, road tolling, and loyalty applications.

(ii) *FeliCa*
FeliCa is a 13.56 MHz contactless proximity high speed smart card system from Sony and is primarily used in electronic money cards [8]. The name FeliCa comes from the word "felicity," suggesting that the technology will make our daily lives more convenient and enjoyable. Sony applied for standardizing FeliCa into ISO/IEC 14443 as Type C standard, but failed. FeliCa eventually did not become an ISO/IEC standard. FeliCa currently only complies with Japanese Industrial Standard (JIS) X 6319 Part 4 which defines high speed proximity cards.

(iii) *Calypso*
Calypso is another example of a contactless proximity smart card which is also international public transportation standard [9]. It was originally designed by a group of European transit operators from Belgium, Germany, France, Italy, and Portugal. It enables interoperability between several transport operators in the same area. Calypso was created in 1993 by a partnership between transit operator RATP and Innovatron Group. The creation of this technology was patented to allow enforcement of a technical interoperability and to finance the developments through an open license scheme. Both the ISO/IEC 14443 Type B standard and the European standard EN 1545 which defines the ticketing data for smart cards are direct results of this work.

3.4.2 Near Field Communication Interface and Protocol (NFCIP)

NFCIP is standardized in two forms as NFCIP-1which defines the NFC communication modes on the RF layer and other technical features of the RF layer; and NFCIP-2 which supports mode switching by detecting and selecting one of the communication modes.

3.4.2.1 NFCIP-1

NFCIP-1 is standardized in ISO/IEC 18092, ECMA 340, and ETSI TS 102 190. This standard defines two communication modes as active and passive. It also defines the RF field, RF communication signal interface and general protocol flow, initialization conditions for the

IPR2025-01238
Apple EX1026 Page 20

supported data rates of 106, 212, and 424 kbps in detail. Moreover, it defines transport protocol including protocol activation, data exchange protocol with frame architecture and error detecting code calculation (CRC for both communication mode at each data rate), and protocol deactivation methods [10].

The carrier frequency of the RF field is 13.56 MHz. The minimum unmodulated RF field is denoted by H_{min} and has a value of 1.5 A/m rms. The maximum unmodulated RF field is denoted by H_{max} and has a value of 7.5 A/m rms. This RF field needs to be modulated during communication.

As mentioned before for the active communication mode, both the initiator and target use their own RF field to enable communication. The initiator starts the NFCIP-1 communication whereas the target responds to an initiator command in the active communication mode using self-generated modulation of the self-generated RF field. The target is powered by inductive coupling and is able to send and receive data. In the passive communication mode, the initiator generates the RF field and starts the communication. The target responds to an initiator command in the passive communication mode using a load modulation scheme as described in Chapter 2.

The communication scheme over the RF interface in active and passive communication modes includes modulation schemes, transfer speed and bit coding. Additionally it includes start of communication, end of communication, bit and byte representation, framing and error detection, single device detection, protocol and parameter selection, data exchange and de-selection of NFCIP-1 devices.

All NFCIP-1 devices have communication capability on 106, 212, or 424 kbps and may switch to another transfer speed or stay on the same transfer speed. The transfer speed of the initiator to target and the transfer speed of the target to the initiator do not need to be kept the same during a transaction. The change of transfer speed during a transaction session may be performed by a parameter change procedure. The mode (active or passive) cannot be changed within one transaction session. The transaction is started by device initialization and terminated by device de-selection (or equivalent).

3.4.2.2 NFCIP-2

NFCIP-2 is a standard specified in ISO/IEC 21481, ECMA 352 and ETSI TS 102 312. The standard specifies the communication mode selection mechanism and is designed not to disturb any ongoing communication at 13.56 MHz for devices implementing ISO/IEC 18092 (i.e., NFCIP-1), ISO/IEC 14443 (e.g., MIFARE) or ISO/IEC 15693 (e.g., long range-vicinity communication, RFID tags) [11]. Although all of the ISO/IEC 18092, ISO/IEC 14443 and ISO/IEC 15693 standards specify 13.56 MHz as their working frequency, they may specify distinct communication modes. These are defined as NFC, PCD, PICC and VCD communication modes. This is achieved using Carrier Sense Multiple Access (CSMA), hence an NFCIP-2 device will not activate its RF field when it detects an external RF that exceeds a certain threshold [11].

Devices following NFCIP-2 need to implement the functions of the proximity coupling device (ISO/IEC 14443), vicinity coupling device (ISO/IEC 15693) and the initiator and the target functions defined in ECMA-340. This makes NFC devices compatible with existing commercially deployed FeliCa and MIFARE systems. However, compatibility is not achieved

IPR2025-01238
Apple EX1026 Page 21

on the smart card emulation side for the standards ISO/IEC 14443 Type B and ISO/IEC 15936, although read-out and editing is possible [5].

3.4.3 Data Transmission on RF Layer

The reader/writer mode allows data connection only at 106 kbps and relies on the RF interface that is compliant with the ISO/IEC 14443 (Type A, Type B) and FeliCa schemes. In peer-to-peer mode, the RF interface that allows all data connections such as 106, 212, and 424 kbps is based on the ISO/IEC 18092 (NFCIP-1) standard. In card emulation mode, the RF interface is based on the ISO/IEC 14443 (Type A, Type B) standard and FeliCa. The Type B is especially used for highly secure transactions such as contactless mobile payments and ticketing. In this section the modulation and coding techniques used by NFC are explained.

(i) *Modulation*

Like the RFID standards 14443 and FeliCa, NFC uses inductive coupling. The operating frequency is 13.56 MHz, and commonly a bit rate of 106 kbps (partly also 212 kbps and 424 kbps) is used. Modulation schemes used by NFC are ASK (Amplitude Shift Keying) with different modulation depth (100% or 10%) and load modulation:

- In the case of data transmission *from the initiator to the target* such as an NFC enabled mobile phone in card emulation mode, the target device uses 13.56 MHz carrier signal of the initiator device as energy source. The modulation scheme of the initiator device is ASK modulation. In peer-to-peer mode, both directions are modulated and coded like an initiator device. However, less power is required because both active NFC devices use their own power supply, generate their own RF field, and the carrier signal is switched off at the end of transmission.
- In the case of data transmission *from the target to the initiator,* due to the coupling of the coils of initiator and target devices, the passive target device also affects the active initiator device. A variation in the impedance of the target device causes amplitude or phase changes on the antenna voltage of the initiator device, which is detected by the initiator device. This technique is called load modulation. Load modulation is carried out in listening mode using an auxiliary carrier at 848 kHz which is modulated by the baseband and varies the impedance of the target device.

(ii) *Coding*

NFC employs three different coding techniques to transfer data: *NRZ-L, Manchester*, and *Modified Miller coding* (see Figure 3.19):

- In NRZ-L coding: a high state during one bit duration refers to logic 1 and a low state refers to logic 0.
- In Manchester coding: at logic 1, the first half of a bit is set to high state, and the second half of that bit is set to low state. At logic 0, the first half of a bit is set to low state and the second half is set to high state.
- In Modified Miller coding: at logic 1, a low pulse occurs after half of the bit duration. At logic 0, a low pulse occurs at the beginning of a bit. If logic 0 comes after logic 1, no pulse occurs at logic 0, hence the signal remains high.

In Manchester and Modified Miller coding schemes a single data bit is sent in a fixed time slot. This time slot is divided into two halves, called half bits. In Miller coding a 0 is encoded

IPR2025-01238
Apple EX1026 Page 22