



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 33746.1-2017

**Technical specification of NFC security -- Part 1: NFCIP-1
security services and protocol**

Issued on: September 7, 2017

Implemented on: April 1, 2018

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China, Standardization
Administration of the People's Republic of China**

Table of Contents

Foreword

1 Scope

2 Normative references

3 Terms and definitions

Foreword

GB/T 33746 "Near Field Communication (NFC) safety technology requirements" is divided into the following two parts.

--- Part 1. NFCIP-1 security services and protocols;

--- Part 2. Safety requirements.

This section GB/T 33746 Part 1.

This section drafted in accordance with GB/T 1.1-2009 given rules.

This section uses redrafted law revision using ISO /IEC 13157-1.2010 "Information technology systems for communication and information exchange

NFC Security Part 1. NFC Security NFCIP-1 Security Services and Protocols. "

This part of ISO /IEC 13157-1.2010 technical differences and the reasons are as follows.

--- The original standard normative references in the ISO standard changed to the corresponding national standard;

--- Removed the two national standards not used in terms of LSB and MSB;

--- In Chapter 7, "The cryptographic algorithms involved in this section should follow the relevant provisions of the national commercial password.";

--- In order to avoid the suspension section of the adjustment of Chapter 8,9,10,11 chapter number;

--- Appendices in accordance with the requirements of the national standard, the original ISO standard Appendix A and Appendix B, according to the order mentioned, into the Department

Sub-Appendix B and Appendix A.

This part of the National Information Security Standardization Technical Committee (SAC/TC260) and focal point.

This part of the drafting unit. Ministry of Industry and Information Technology
Telecommunications Research Institute, Xi'an Jietong Wireless Network Communications
Co., Ltd., China Pu

Day Information Industry Co., Ltd., China Article Coding Center, the National Radio
Frequency Identification Product Quality Supervision and Inspection Center.

1 Scope

GB/T 33746 provisions of this part of the NFCIP-1 NFC-SEC security channel services and
shared secret services, as well as the corresponding service

Use the PDU and protocol.

This section covers the requirements for NFCIP-1 security services and protocols.

Note 1. NFC-SEC is designed for data exchange protocols as specified in ISO /IEC 18092.

Note 2. This section does not propose specific application-related security mechanisms (for
example, the smart card application case proposed in the ISO /IEC 7816 series of
standards requires security

Full mechanism). NFC-SEC complements the application security mechanisms in ISO /IEC
7816.

2 Normative references

The following documents for the application of this document is essential. For dated
references, only the dated version applies to this article

Pieces. For undated references, the latest edition (including all amendments) applies to this
document.

GB/T 9387.1-1998 Information technology - Open Systems Interconnection basic reference
model Part 1. Basic model

(ISO /IEC 7498-1.1994, IDT)

GB/T 17967-2000 Information Technology Open Systems Interconnection Basic Reference
Model OSI Service Definition Conventions

(ISO /IEC 10731.1994, IDT)

Information technology - Security terminology

Safety of near field communication (NFC) - Technical requirements - Part 2. Requirements
for safety mechanisms (ISO /IEC 13157-2..2003)

2010, MOD)

ISO /IEC 18092.2004 Information technology - Telecommunications and information exchange between systems - Near-field communication interfaces and protocols NFCIP-1

[Information technology-Telecommunications and information exchange between systems-Near

Field Communication-Interface and Protocol (NFCIP-1)]

3 Terms and definitions

GB/T 17967-2000, GB/T 25069-2010 and ISO /IEC 18092.2004 as defined by the following terms and definitions suitable

Used in this document.

3.1

Linkkey linkkey

Key to secure channel security.

3.2

NFC-SEC user NFC-SECuser

Entity using the NFC-SEC service.

3.3

Receiver recipient

NFC-SEC entity receiving ACT-REQ command.