

ICS 35.040
CCS L 80



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

GB/T 33746.2-2017

**Technical specification of NFC security -- Part 2: Security
mechanism requirements
(English Translation)**

Issued on: September 7, 2017

Implemented on: January 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

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 conventions and notations

4.1 level even

4.2 hexadecimal digits

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 2.

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

This section uses the redrafted law to amend the use of ISO /IEC 13157-2.2010 "Information technology systems for communication and information exchange

NFC Security Part 2. Security Mechanism Requirements, Cryptographic Criteria Using ECDH and AES. "

This part of ISO /IEC 13157-2.2010 technical differences and the reasons are as follows.

--- Standard English name changed to Technical specification of NFC security-Part 2. Security mechanism

requirements

--- Increased 3 normative references;

--- Added 5 abbreviations;

--- Delete the original data Appendix C, an increase of 2 normative Appendix C and Appendix D;

--- Replace AES with a password algorithm that complies with the national password

management rules.

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., the national radio

Frequency Identification Product Quality Supervision and Inspection Center, China Article Coding Center.

Introduction

This part of the user is the communications industry manufacturing enterprises, testing agencies and technology agencies.

The issuing authority of this document draws attention to the fact that statements that conform to this document may relate to Appendix C and "An Entity Bidirectional Identification Method"

D and the use of "a method based on symmetric cryptographic algorithms and authentication methods and systems" and other related patents.

The issuing authority of this document has no position regarding the authenticity, validity and scope of the above patents.

The patentee has assured the issuing authority of this document that he is willing to work with any applicant on terms and conditions reasonably non-discriminatory

Patent licensing negotiations. The patent holder's statement has been filed with the issuing authority of this document. Related information is available through the following link

Department obtained.

Patentee Xi'an Xi Jie Jietong Wireless Network Communications Co., Ltd

Address. 68 # Science and Technology Road, Xi'an High-tech Zone, Xi'an Software Park, Qin Feng Club A201

Contact. Liu Changchun

Postal code .710075

Email .ipri @ iwncomm.com

Phone .029-87607836

Fax .029-87607829

Please note that in addition to the above patents, some of the contents of this document

may involve patents. The issuing authority of this document does not undertake to identify these patents

Responsibility.

Near Field Communication (NFC) security technology requirements

Part 2. Requirements for safety mechanisms

1 Scope

GB/T 33746 provisions of this part of the agreement identifier PID 01 message content and encryption methods. This section of the password mechanism

Is using the SM2 key exchange protocol as the key agreement protocol and the SM4 block cipher algorithm for data encryption and integrity protection.

This section applies to the security mechanism in the establishment of NFC security services requirements.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version applies to this document. For undated references, the latest edition (including all amendments) applies to this document.

Information security technology block cipher algorithm working mode

GB/T 28455-2012 Information security technology to introduce trusted third-party entity authentication and access architecture specification

GB/T 33746.1-2017 Near Field Communication (NFC) security technology requirements
Part 1. NFCIP-1 Security Services and Protocols

(ISO /IEC 13157-1.2010, MOD)

GM/T 0002-2012 SM4 Block Cipher Algorithm

GM/T 0003-2012 SM2 Elliptic Curve Public Key Crypto Algorithm

ISO /IEC 9798-3.1998/Amd.1.2010 Information technology - Security technology - Entity identification - Part 3. Use of digital signatures

Technical Mechanisms Supplement 1

(Information technology - Security techniques - Entity authentication - Part 3.

Mechanisms using digit signature techniques - Amendment 1)

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)]

ISO /IEC .20009-2.2013 Information technology - Security technology Anonymous entity authentication Part 2. Group public key technology

Mechanism

(Information technology-Security techniques-Anonymous entity authentication-Part 2.Mechanisms based on signatures using a group public key)

3 Terms and definitions

GB/T 33746.1-2017 defined terms and definitions apply to this document.

4.2 hexadecimal digits

(XY) Represents the XY hexadecimal number (that is, in base 16), each pair of characters is encoded as a single byte.