Chinastandards.org

ICS 35.040
CCS L 80

GM

GM/T 0101-2020

Test specification for cryptography and security protocol of near field communication

近场通信密码安全协议检测规范

(English Translation)

Issued on: December 28, 2020 **Implemented on: July 1, 2021**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0101-2020

Chinastandards.org

Table of Contents

Requirements for the consistency and interoperability of NEAU protocol 1
Test method for the correctness of symmetric cryptographic algorithm 2
Test method for the correctness of digital signature algorithm engineering 3
Test method for the correctness of key exchange protocol engineering 4
Test method for the conformance and interoperability of NEAU protocol 5
Receiver (B) test method 6

5.2 Requirements for the consistency and interoperability of NEAU protocol

implementation... 8

5.3 Other requirements... 8

6 Test topology... 8

6.1 Sender (A) test topology... 8

6.2 Receiver (B) test topology... 9

7 Test methods for the cryptographic algorithm performance and the correctness of engineering implementation... 10

7.1 Test method for the cryptographic algorithm performance... 10

7.2 Test method for the correctness of symmetric cryptographic algorithm

engineering implementation... 11

7.3 Test method for the correctness of digital signature algorithm engineering

implementation... 11

7.4 Test method for the correctness of key exchange protocol engineering

implementation... 12

7.5 Random number test method... 13

8 Test method for the conformance and interoperability of NEAU protocol

implementation... 13

Preview: page 2 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0101-2020

Chinastandards.org

8.1
NEAU-A test method... 13

8.2
NEAU-S test method... 15 Test specification for cryptography and security protocol of near field communication

1 Scope

This document specifies the detection methods for cryptographic algorithm and NFC security protocol (NEAU) of Near Field Communication (NFC) devices that comply with the GB/T 33746 series of standards, including the following:

a) The detection methods and requirements of the performance of the cryptographic algorithm and the correctness of the engineering implementation;

b) The detection methods and requirements of the consistency and interoperability of NEAU protocol implementation.

This document applies to NFC devices that comply with the GB/T 33746 series of standards, and is used to detect whether the cryptographic algorithm and the NEAU security protocol implementation meet the requirements.

2 Normative references the contents of the following documents constitute the indispensable clauses of this document through normative references in the text. For dated references, only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document.

GB/T 32907, Information security technology - SM4 block cipher algorithm GB/T 32915, Information security technology - Binary sequence randomness detection method GB/T 32918.2, Elliptic Curve Public-Key Cryptography - Part 2: Digital Signature Algorithm GB/T 32918.3, Information security techniques - Elliptic Curve public-key cryptography - Part 3: Key exchange protocol GB/T 33746.1, Technical specification of NFC security - Part 1: NFCIP-1 security services and protocol the special standard equipment that provides data for auxiliary testing, other than the NEAU protocol interaction, to the test platform; the equipment is usually provided by the testing organization.

4 Abbreviations

The following abbreviations apply to this document.

CBC Cipher Block Chaining CTR Counter Operation Mode NEAU NFC Entity Authentication NEAU-A NFC Entity Authentication using Asymmetric cryptography NEAU-S NFC Entity Authentication using Symmetric cryptography NFC Near Field Communication TePA Tri-element Peer Architecture TTP Trusted Third Party

Preview: page 3 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0101-2020

Chinastandards.org

5 General requirements

5.1 Requirements for the cryptographic algorithm performance and the correctness of engineering implementation Products that comply with the NEAU protocol that is specified in GB/T 33746.2-2017 shall support the cryptographic algorithm that is approved by the national cryptographic authority.

The implementation of the cryptographic algorithm shall satisfy:

a) Cryptographic algorithm performance requirements in the NEAU protocol the cryptographic algorithm performance that is used in the NEAU protocol shall meet the specific scenario requirements of the product application.

b) Requirements for the correctness of symmetric cryptographic algorithm engineering implementation in the NEAU protocol for the symmetric cryptographic algorithm that is used in the NEAU protocol, and its operation modes (CTR and CBC), the operation result shall be consistent with the operation result that is provided by the corresponding algorithm that is specified in the national standard of cryptographic algorithm, including encryption and decryption.

c) Requirements for the correctness of asymmetric cryptographic algorithm engineering implementation in the NEAU protocol for the asymmetric cryptographic algorithm that is used in the NEAU protocol, the operation result shall be consistent with the operation result that is provided by the corresponding algorithm that is specified in the national standard of cryptographic algorithms, including key exchange, signature and signature verification.

5.2 Requirements for the consistency and interoperability of NEAU protocol implementation the near field communication NEAU security protocol shall comply with GB/T 33746.2-2017; the involved entities are mainly sender (A), receiver (B) and TTP.

NEAU includes NEAU-A mechanism and NEAU-S mechanism, among which NEAU-A mechanism is based on the Tri-element Peer Architecture (TePA).

5.3 Other requirements.

The product shall consider self-inspection, and the reliability and stability of the product shall meet the needs of specific scenarios of the product application.

According to the implementation of the protocol in the product, the correctness self-inspection of the cryptographic algorithm and the description of the random number self-inspection can be provided. A random bit generator that conforms to the approval of the national cryptographic management authority shall be adopted for the product.

The security requirements of the cryptographic module in the product shall meet GB/T 37092.

6 Test topology

Preview: page 4 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0101-2020

Chinastandards.org

6.1 Sender (A) test topology the sender (A) test is divided into two situations: TTP is supported and TTP is not supported. Among them, the tested equipment is the sender (A), and the standard equipment is the receiver (B).

The tested equipment (A) is connected to the standard equipment (B); the test platform obtains the NEAU protocol interaction data that is sent and received by the tested equipment. The way to obtain test data: the test platform actively obtains the test data through packet capture, or the tested equipment (A) actively provides the NEAU protocol interaction data sent and received to the

Figure 4; the tested equipment, the standard equipment and the support

equipment implement the NEAU protocol interaction.

b) The test platform obtains relevant data of cryptographic algorithm performance testing, including data length, cryptographic operations, number of repetitions, statistical completion time and other data.

Cryptographic operations include: SM4 encryption/decryption, SM2 signature/verification.

c) The test platform uses the obtained data to calculate the performance of the corresponding cryptographic algorithm.

7.2 Test method for the correctness of symmetric cryptographic algorithm engineering implementation the test method is as follows:

a) According to the test requirements, if the tested equipment is the sender, build the test network according to Figure 1 or Figure 2; if the tested equipment is the receiver, build the test network according to Figure 3 or

Figure 4; the tested equipment, the standard equipment and the support

equipment implement the NEAU protocol interaction. Among them, the standard equipment shall interact with the tested equipment in accordance with the operation examples that are given in GB/T 32907.

b) The test platform obtains symmetric cryptographic algorithm test related data, including the corresponding algorithm working mode, key, initialization vector, plaintext, cyphertext and other data, which is involved when the tested equipment and standard equipment implement the NEAU-S protocol in Appendix D.3 of GB/T 33746.2-2017. It is recommended to collect 3 sets of data.

c) The test platform uses such data to carry out the correctness test of the symmetric cryptographic algorithm engineering implementation, and specifically follows the algorithm working mode that is specified in GB/T 32907 and GB/T 33746.2-2017, to detect the correctness of the operation results. It is suggested that the test is judged as passed when all the 3 sets of data are correct; otherwise, it is judged as failed.

Preview: page 5 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0101-2020