

ICS 35.040

GM

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

GM/T 0064-2018

**Cryptography test requirements for range controlled
communication (RCC)**

限域通信(RCC)密码检测要求
(English Translation)

Issued on: August 20, 2018

Implemented on: August 20, 2018

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
RCC initiator product	3
RCC target product	4
General requirements	5
Decision criteria	6
Test requirements	7
Decision criteria	8
Test requirements	9
Decision criteria	10
Test requirements	11
Decision criteria	12

1 Scope

This Standard specifies the test contents and requirements of cryptography and security for the range controlled communication (RCC) products that use cryptographic technique. The test of other functions of RCC products are performed according to their corresponding product inspection specifications.

This Standard applies to cryptography test for range controlled communication (RCC) products.

2 Normative references

The following documents are indispensable for the application of this document.

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

GB/T 32907-2016, Information security technology. SM4 block cipher algorithm GB/T 32915-2016, Information security technology. Randomness test methods for binary sequence GB/T 33736-2017, Mobile payment. Technical requirements for contactless radio frequency interface based on 2.45 GHz range controlled communication technology GB/T 33737-2017, Mobile payment. Test methods for intelligent card based on 2.45 GHz RCC (range controlled communication) technology GB/T 33738-2017, Mobile payment. Technical requirements for intelligent card based on 2.45 GHz RCC (range controlled communication)

technology GB/T 33740-2017, Mobile payment. Test methods of contactless radio frequency interface based on 2.45 GHz range controlled communication technology GB/T 33741-2017, Mobile payment. Technical requirements for contactless reader terminal based on 2.45 GHz range controlled communication technology RCC, range controlled communication SD, secure digital memory card SIM, subscriber identity module UID, unique identifier

5.1 RCC initiator product

The RCC initiator product refers to a product that supports the RCC communication protocol and acts as the product of the initiator in the RCC communication session, including an RCC reader module, a POS terminal device that supports RCC, and the like. The RCC initiator product function implementation complies with the requirements of GB/T 33741-2017. The RCC initiator product function test complies with the requirements of GB/T 34096-2017. For the test system and environment, refer to Appendix A of this Standard.

If the RCC initiator product provides cryptographic services for upper-layer applications, refer to Appendix B for its application key management and security requirements.

5.2 RCC target product

The RCC target product refers to a product that supports the RCC communication protocol and acts as the product of the target in the RCC communication session, including smart cards such as RCC-SIM card and RCC-SD card. The RCC target product function implementation complies with the requirements of GB/T 33738-2017. The RCC target product function test complies with the requirements of GB/T 33737-2017. For the test system and environment, refer to Appendix A of this Standard. If the RCC target product provides cryptographic services for upper-layer applications, refer to Appendix B for its application key management and security requirements.

6.1 General requirements

This Standard mainly tests the random number that is realized in RCC products, the RCC communication link data encryption algorithm, the RCC product cryptography service and the product cryptography operation performance.

The RCC product uses the SM4 cryptographic algorithm to encrypt and protect the APDU data packets that are transmitted by the radio-frequency channel link layer; its transmission confidentiality protection shall be correct and valid.

6.3.1.2 Decision criteria

The APDU data that is transmitted by the radio-frequency channel can be protected by the SM4 cryptographic algorithm for confidentiality during the link layer transmission process.

6.3.2.1 Test requirements

If RCC products use their own hardware cryptographic resources to provide other cryptographic services such as data encryption and decryption services for upper-layer applications, they shall provide corresponding API interfaces for upper-layer applications.

6.3.2.2 Decision criteria

The RCC data encryption and decryption services function that is provided by the RCC product that is called through the API interface shall make the obtained operation result correct and valid.

6.4.1 Test requirements

Test the speed at which the RCC product encrypts and decrypts the transmitted APDU data packets at the link layer.

6.4.2 Decision criteria

The RCC product link encryption and decryption functions shall meet the requirements on data transmission efficiency of the RCC application.

6.5.1 Test requirements

RCC products use magnetic channels to transmit sensitive information; the transmission distance of magnetic channel data signals shall be strictly controlled within a safe distance.

6.5.2 Decision criteria

The card swipe distance of RCC product is not more than 10 cm.

Appendix B

(Informative)

RCC product application key management and security requirements B.1 RCC product application key management B.1.1 Application key generation the application key data that is used by the RCC product can be generated by a real random number that is generated by the security chip or be externally imported.

B.1.2 Application key storage If the RCC product needs to store the application key, it shall be able to store the application key correctly and validly in a secure area within the security

chip.

The application key cannot be read by the attacker and shall meet the requirements of the relevant application standards for key storage.

B.1.3 Application key usage the RCC product shall be able to use the application key correctly and validly in the security chip according to the type of the key and the occasion of use, and shall meet the requirements of the relevant application standards for the key usage.

B.1.4 Application key update If the RCC product has the application key update function, it shall be able to update the application key correctly and validly in the security chip.

B.1.5 Application key import If the RCC product has the application key import function, it shall be able to import the application key correctly and validly into the security chip.

B.1.6 Application key removal RCC products shall be able to correctly and validly remove application keys that are stored in the security chip according to application needs.

B.2 RCC product safety guarantee B.2.1 Document management