Chinastandards.org

ICS 35.040

GM

GM/T 0075-2019

Cryptograhy technical requirements for credit banking information systems

银行信贷信息系统密码应用技术要求

(English Translation)

Issued on: July 12, 2019 **Implemented on: July 12, 2019**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 50 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0075-2019

Chinastandards.org

Table of Contents

Secondary requirements for security protection of cryptography of credit 1
Level three requirements of the cryptography security protection of the credit 2
General 3
Communication security 4
Identity authentication 5
Verification code and dynamic password 6
Data storage 7
Key distribution 8
Key use 9

7 Secondary requirements for security protection of cryptography of credit

banking information system... 10

8 Level three requirements of the cryptography security protection of the credit

banking information system... 26 Annex A (normative) Security requirements comparison table... 48 Bibliography... 50 Cryptography technical requirements for credit banking information systems

1 Scope

This Standard, on the basis of GM/T 0054-2018, JR/T 007-2012 and other standards, combining the characteristics of credit banking system and the application needs of cryptography in the level of protection of such information system, from three aspects of cryptology security technical requirements, key security and management requirements, and security management requirements, PUTS FORWARD specific requirements for the application of cryptology in credit banking information system with different security protection levels.

This Standard is applicable to guide, standardize and evaluate commercial cipher application in credit information system.

2 Normative references the following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any

Preview: page 2 of 5 shown, 50 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0075-2019

amendments) applies.

GB/T 20547.2-2006, Banking - Secure cryptographic devices (retail) - Part 2:

Security compliance checklists for devices used in financial transactions GB/T 21078.1-2007, Banking - Personal Authentication Number management and security - Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems GB/T 21079.1, Banking - Secure cryptographic devices (retail) - Part 1:

Concepts, requirements and evaluation methods GM/T 0024, SSL VPN specification GM/T 0028-2014, Security Requirements for Cryptographic Modules GM/T 0036-2014, Technical guidance of cryptographic application for access control systems based on contactless smart card

6 Basic requirements for cipher application and functional requirements for cipher application the basic requirements for cipher application and functional requirements for cipher application of the credit banking information system shall comply with the requirements in Clause 5, Clause 6 of GM/T 0054-2018.

7 Secondary requirements 1 for security protection of cryptography of credit banking information system

7.1 Basic requirements Meet the requirements for level two indicators in GM/T 0054-2018.

7.2 Security requirements for cryptography

7.2.1 Physical and environmental security

7.2.1.1 General

Refer to general principles for the application of physical and environmental security cipher in GM/T 0054-2018.

7.2.1.2 Cipher hardware security "Cipher hardware security", "physical environment security" and "electronic access control system" are parts of the "physical and environmental security" of the credit banking information system. In the level two requirements of the cryptography security protection of the credit banking information system, the following requirements are made for the indicators of "physical and environmental security - cipher hardware security":

a) The dedicated hardware or firmware of the system and cryptographic equipment shall have effective physical security protection measures;

NOTE: "Effective measures" in this Standard refer to means that can meet the requirements of "guarantee items" or methods that can achieve the security goals set by the system. The following notes are the same.

b) The dedicated hardware or firmware of the system and cryptographic equipment shall meet the reliability requirements of the operating

Preview: page 3 of 5 shown, 50 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0075-2019

1 For comparison of all security requirements of this level with other levels, please refer to Annex A Security Requirements Comparison Table, the same below.

"network and communication security - communication security":

a) In order to prevent the access communication data from being tampered, intercepted, counterfeit and reused, it is advisable to use the integrity service, confidentiality service and authenticity service of cryptography to protect the network boundary and system resource access control information;

b) During data transmission, cryptography such as digital certificates, encryption and decryption shall be used to establish a secure transport layer session channel.

7.2.2.3 Identity authentication "Communication security" and "authentication" are parts of the "network and communication security" of the credit banking information system. In the level two requirements of the cryptography security protection of the credit banking information system, the following requirements are made for the indicators of "network and communication security - identity authentication":

a) When authenticating user who logs in to network devices, in order to prevent the authentication information from being reused and counterfeited, it is advisable to use the authenticity service of cryptography to protect the authentication information against reuse and counterfeiting.

Its cipher function shall ensure correct and effective;

b) Network equipment system management of user authentication shall not be easily fraudulently used. The static cipher of key network equipment shall be at least 6 digits. It is composed of a mixture of letters, numbers, symbols and so on and shall be regularly replaced;

c) When performing remote network management, in order to prevent the authentication information from being leaked during transmission, it is advisable to use the confidentiality service of cryptography to protect the confidentiality of the authentication information. Its cipher function shall ensure correct and effective;

d) The information system shall use cryptography to generate unique random identifiers for entities that have passed identity authentication and ensure that the function is correct and effective.

7.2.3 Equipment and computing security

7.2.3.1 General

Refer to general rules for the application of security cipher for devices and computing in GM/T 0054-2018.

password. Then enter the identity authentication module. The hash function shall be correct

Preview: page 4 of 5 shown, 50 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0075-2019

and valid;

c) When conducting key business processes, such as transfers, transactions, and modification of information, it is advisable to use a variety of cryptographies to ensure the authenticity and validity of user identity;

d) Operating system and database system management of user identification shall not be easily fraudulently used. The static password of the key system shall be more than 6 digits. It is composed of a mixture of letters, numbers, symbols and so on and shall be regularly replaced.

7.2.3.5 Verification code and dynamic password "Audit records", "access control", "identity authentication", "verification code and dynamic cipher " and "cryptographic module " are parts of the "equipment and computing security" of credit banking information system. In the level two requirements of the cryptography security protection of the credit banking information system, the following requirements are made for the indicators of "equipment and computing security - verification code and dynamic password":

a) When using SMS or other channels to send the verification code, the correct cryptography shall be used to ensure that the dynamic password sent is completely random and unpredictable;

b) When using SMS or other channels to send the verification code, ensure that the content of the verification code is not disclosed;

c) If OTP tokens are used for identity verification, use correct cryptography to ensure that OTP is completely random and unpredictable.

7.2.3.6 Cryptographic module "Audit records", "access control", "identity authentication", "verification code and dynamic cipher " and "cryptographic module " are parts of the "equipment and computing security" of credit banking information system. In the level two requirements of the cryptography security protection of the credit banking information system, the following requirements are made for the indicators of "equipment and computing security - cryptographic module":

It shall use the cryptographic module that complies with level two and more in GM/T 0028-2014 or hardware password products approved by the national cipher management department to realize cryptographic operations and key management:

a) The dedicated hardware or firmware of the system and the cryptographic equipment shall implement security functions such as authorization "application and data security" of the credit banking information system. In the level two requirements of the cryptography security protection of the credit banking information system, the following requirements are made for the indicators of "application and data security - data storage":

In terms of data storage security, the integrity service of cryptography can be used to detect

Preview: page 5 of 5 shown, 50 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0075-2019