Chinastandards.org

ICS 35.040

GM

GM/T 0077-2019

Cryptography tecyhnical requirements for core banking systems

银行核心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, 60 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0077-2019

Chinastandards.org

Table of Contents

Basic Requirements and Functional Requirements for Cryptographic 1
Level-3 Requirements for Cryptographic Technical Security Protection of Core 2
General rules 3
Cryptographic hardware security 4
Physical environmental security 5
Electronic access control system 6
Audit record 7
General rules 8
Audit record 9
Access control 10
Cryptographic module 11
Cryptographic algorithm allocation 12
Cryptographic protocol application 13
Cryptographic device application 14
Key import and export 15
Key usage and replacement 16
Key archive and destruction 17
Requirements for cryptography-using business terminal 18
Electronic access control system 19
Identity authentication 20

6 Basic Requirements and Functional Requirements for Cryptographic

Application... 11

7 Level-3 Requirements for Cryptographic Technical Security Protection of Core

Banking Information System... 11

8 Four-level Requirements for Cryptographic Technical Security Protection of Core Banking Information System... 33 Appendix A (normative) Security Requirements Comparison Table... 58 Bibliography... 60 Cryptography Technical Requirements for Core Banking

Preview: page 2 of 5 shown, 60 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0077-2019

Systems

1 Scope

On the basis of GM/T 0054-2018 and JR/T 007-2012 (TRANSLATOR NOTE: it should be JR/T 0071-2012), this Standard integrates the characteristics of the core systems of banking financial institutions and the application demands of cryptographic technique in the security construction of this type of classified information system protection. From three perspectives, namely, cryptographic security technical requirements, key security and management requirements, security management requirements, specific requirements are put forward for the application of cryptographic technique in the core systems with different security protection levels.

This Standard is applicable to the guidance, standardization and evaluation of the core information systems of banks and financial institutions.

2 Normative References the following documents are indispensable to the application of this document. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

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 Banking - Personal Identification 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 Security Requirements for Cryptographic Modules GM/T 0036-2014 Technical Guidance of Cryptographic Application for Access Control Systems Based on Contactless Smart Card GM/T 0054-2018 General Requirements for Information System Cryptography Application

7.2.1.1 General rules

Take the general rules of cryptographic application in physical and environmental security in GM/T 0054-2018 as a reference.

7.2.1.2 Cryptographic hardware security

"Cryptographic hardware security", "physical environmental security" and "electronic access control system" are the constituent parts of "physical and environmental security" of the core banking system. In Level-3 requirements of cryptographic technical security protection of the core banking information system, the following requirements are made for the "physical and environmental security - cryptographic hardware security" indicator:

a) The system's dedicated hardware or firmware and cryptographic device shall have

Preview: page 3 of 5 shown, 60 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0077-2019

effective physical security protection measures;

NOTE: in this Standard, "effective measures" refer to the means that can meet the requirements of the "ensured items" or the method that can achieve the security goals set by the system, the same below.

b) The system's dedicated hardware or firmware and cryptographic device shall satisfy operating environment reliability requirements.

7.2.1.3 Physical environmental security

"Cryptographic hardware security", "physical environmental security" and "electronic access control system" are the constituent parts of "physical and environmental security" of the core banking system. In Level-3 requirements of cryptographic technical security protection of the core banking information system, the following requirements are made for the "physical and environmental security - physical environmental security" indicator:

The authenticity function of cryptographic technique shall be used to protect the identity authentication information of physical access control and ensure the authenticity of the identity of personnel entering important areas.

7.2.1.4 Electronic access control system

"Cryptographic hardware security", "physical environmental security" and "electronic access control system" are the constituent parts of "physical and environmental security" of the core banking system. In Level-3 requirements of cryptographic technical security protection of the core banking information system, the following

e) Cryptographic technique shall be adopted to establish a secure information transmission channel, so as to perform centralized management of the security device or security components in the network.

7.2.2.5 Audit record

"Communication security", "identity authentication", "secure access path" and "audit record" are the constituent parts of "network and communication security" of the core banking system. In Level-3 requirements of cryptographic technical security protection of the core banking information system, the following requirements are made for the "network and communication security - audit record" indicator:

The integrity service of cryptographic technique shall be adopted to protect the integrity of audit record. It shall be ensured that its cryptographic function is correct and effective.

Preview: page 4 of 5 shown, 60 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0077-2019

7.2.3.1 General rules

Take the general rules of cryptographic application in device and computational security in GM/T 0054-2018 as a reference.

7.2.3.2 Audit record

"Audit record", "identity authentication", "access control" and "cryptographic module" are the constituent parts of "device and computational security" of the core banking system. In Level-3 requirements of cryptographic technical security protection of the core banking information system, the following requirements are made for the "device and computational security - audit record" indicator:

a) The scope of audit shall cover every operating system user and database user on the server and important client-sides;

b) The integrity service of cryptographic technique shall be adopted to implement the integrity verification of audit records; it shall be ensured that its cryptographic function is correct and effective;

c) The integrity function of cryptographic technique shall be adopted to protect the integrity of log records;

d) Audit content shall include important security-related events in the system, such as: important user behavior, abnormal use of system resources, and the use of important system commands, etc.;

e) Audit record shall include date and time, type, subject identification, object identification and event result, etc.

7.2.3.4 Access control

"Audit record", "identity authentication", "access control" and "cryptographic module" are the constituent parts of "device and computational security" of the core banking system. In Level-3 requirements of cryptographic technical security protection of the core banking information system, the following requirements are made for the "device and computational security - access control" indicator:

a) From the perspective of access control mechanism, in order to prevent system resource access control information from being tampered with, the integrity service of cryptographic technique shall be adopted to implement the integrity protection of system resource access control information and sensitive marks; it shall be ensured that its cryptographic function is correct and effective;

b) In accordance with the role assignment permissions of user being managed, implement the separation of permissions of the user being managed, and merely grant the minimum

Preview: page 5 of 5 shown, 60 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0077-2019