Chinastandards.org

ICS 35.040

GM

GM/T 0076-2019

Cryptography technical requirements for banking card information systems

银行卡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, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0076-2019

Chinastandards.org

Table of Contents

Basic requirements for cryptographic applications and functional 1
Level 2 requirements for the security protection of cryptographic technology 2
Basic requirements 3
Cryptographic hardware security 4
Electronic access control system 5
General 6
Identity authentication 7
Data storage 8
Cryptographic algorithm configuration 9
Use of cryptographic protocol 10
Generation of application ciphertext 11
Key storage 12
Key distribution 13
Basic requirements 14
Physical environment security 15
Electronic access control system 16
General 17
Communication security 18
Identity authentication 19
Audit records 20
General 21
Audit records 22
Identity authentication 23
General 24
Overview 25
Basic requirements 26
General 27
Physical environment security 28
General 29
Communication security 30
Identity authentication 31
Basic requirements 32

Preview: page 2 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0076-2019

General 33
Physical environment security 34
General 35
Communication security 36
Identity authentication 37

6 Basic requirements for cryptographic applications and functional

requirements for cryptographic applications... 11

7 Level 2 requirements for the security protection of cryptographic technology

of bank card information system)... 11

8 Three-level requirements of cryptographic technology security protection of bank card information system... 30

9 Level-4 requirements for security protection of cryptographic technology of bank card information system... 53 Appendix A (Normative) Comparison of security requirements... 81 References... 83

1 Scope

This standard is based on GM/T 0054-2018, JR/T 007-2012 and other standards, combined with the characteristics of the banking card system of banking financial institutions and the application needs of cryptographic technology in the classified protection of this type of information system, from three aspects of cryptographic security technical requirements, key security and management requirements, security management requirements, proposing specific requirements for the application of cryptographic technology in banking card systems with different security protection levels.

This standard is applicable to the guidance, standardization and evaluation of commercial cryptographic applications in banking card information systems.

2 Normative references the following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

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

Preview: page 3 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0076-2019

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

3 Terms and definitions the terms and definitions as defined in GM/Z 4001-2013 as well as the following terms and definitions apply to this document.

Authentication/entity authentication the process of confirming the claimed identity of an entity.

Event

Processes that conflict with information system security policies.

Key encryption key; KEK the key used to encrypt or decrypt the key.

Cryptographic protocol A series of steps taken to achieve a specific purpose for two or more participants using the cryptographic algorithms in accordance with agreed rules.

Command

A message sent by the terminal to the IC card, which initiates an operation or requests a response.

4 Abbreviations

The following abbreviations apply to this document.

AC. Application Cryptogram DOL. Data Authentication Data Object List IC. Integrated Circuit KEK. Key Encryption Key

5 Bank card information system model A typical bank card information system consists of a bank card operation terminal and a bank card information processing server, as shown in Figure 1.

6 Basic requirements for cryptographic applications and functional requirements for cryptographic applications the basic requirements of the cryptographic application and the function requirements of the cryptographic application of the mobile banking information system comply with the requirements of Chapter 5 and Chapter 6 of GM/T 0054-2018.

7 Level 2 requirements for the security protection of cryptographic technology of bank card information system1)

Preview: page 4 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0076-2019

7.1 Basic requirements

It shall comply with the requirements for the level 2 indicators in GM/T 0054-2018.

7.2.1.2 Cryptographic hardware security

"Cryptographic hardware security", "physical environment security", "electronic access control system" are part of the "physical and environmental security" of the bank card information system. In the level 2 requirements for the security protection of cryptographic technology of bank card information systems, the following requirements are made for the indicators of "physical and environmental security-cryptographic hardware security".

7.2.1.4 Electronic access control system

"Cryptographic hardware security", "physical environment security", "electronic access control system" are part of the "physical and environmental security" of the bank card information system. In the level 2 requirements for the security protection of the cryptographic technology of the bank card information system, the following requirements are made for the indicators of "physical and environmental security-electronic access control system".

7.2.3.1 General

Refer to GM/T 0054-2018 General requirements for information system cryptography application.

7.2.3.4 Identity authentication

"Audit records", "access control", "identity authentication", "verification code and dynamic password", "cryptographic module" are part of the "device and computing security" of the bank card information system. In the level 2 requirements of the cryptographic technology security protection of the bank card information system, the following requirements are made for the indicators of "device and computing security-identity authentication".

7.2.4.3 Data storage

"Data transmission", "data storage", "terminal application" are part of the "application and data security" of the bank card information system. In the level 2 requirements for the security protection of cryptographic technology for bank card information system, the following requirements are made for the indicators of "application and data security-data storage".

Preview: page 5 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0076-2019