Chinastandards.org

ICS 35.040

GM

GM/T 0073-2019

Cryptography technical requirements for mobile banking information systems

手机银行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-0073-2019

Chinastandards.org

Table of Contents

Level 2 requirements for the cryptography security protection of mobile 1
Level 3 requirements for the cryptography security protection of mobile 2
General 3
Communication security 4
General 5
Data transmission 6
Cryptographic algorithm allocation 7
Cryptographic protocol use 8

7 Level 2 requirements for the cryptography security protection of mobile

banking information systems... 11

7.1
Basic technical requirements... 11

7.2
Cryptography security requirements... 11

7.2.1
Physical and environmental security... 11

7.2.2
Network and communication security... 13

7.2.3
Device and computing security... 14

7.2.4
Application and data security... 16

7.2.5
Cryptography allocation policy requirements... 17

7.3
Key security and management requirements... 18

Preview: page 2 of 5 shown, 50 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0073-2019

Chinastandards.org

7.3.1
General... 18

7.3.2
Key security... 19

7.3.3
Key management... 20

7.4
Security management requirements... 24

7.4.1
Overview... 24

7.4.2
Security management system... 25

7.4.3
Personnel management requirements... 25

7.4.4
Cryptographic device management... 26

7.4.5
Password-using service terminal requirements... 26

8 Level 3 requirements for the cryptography security protection of mobile

banking information systems... 27

8.1
Basic requirements... 27

8.2
Cryptography security requirements... 27

8.2.1
Physical and environmental security... 27

8.2.2
Network and communication security... 29

Preview: page 3 of 5 shown, 50 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0073-2019

Chinastandards.org

8.2.3
Device and computing security... 31

8.2.4
Application and data security... 33

8.2.5
Cryptography allocation policy requirements... 35

8.3
Key security and management requirements... 36

8.3.1
General... 36

8.3.2
Key security... 36

8.3.3
Key management... 38

8.4
Security management requirements... 44

8.4.1
Overview... 44

8.4.2
Security management system... 44

8.4.3
Personnel management requirements... 45

8.4.4
Cryptographic device management... 46

8.4.5
Password-using service terminal requirements... 46 Appendix A (Normative) Table of comparison of security requirements... 48 Bibliography... 50 Cryptography technical requirements for mobile banking information systems

1 Scope

On the basis of standards such as GM/T 0054-2018 and JR/T 007-2012;

combined with the characteristics of mobile banking information systems, and the

Preview: page 4 of 5 shown, 50 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0073-2019

application needs of cryptography in the security construction of classified protection of this type of information system; in terms of cryptographic security technical requirements, key security and management requirements, and security management requirements; this Standard puts forward specific requirements for the cryptography in mobile banking information systems with different security protection classes.

This Standard applies to the guidance, standardization and evaluation of commercial cryptographic applications in mobile banking information systems.

2 Normative references the following documents are indispensable for the application of this document.

For the dated references, only the editions with the dates indicated are applicable to this document. For the undated references, the latest edition (including all the amendments) are 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 21078.1-2007 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 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 GM/T 0054-2018 General requirements for information system cryptography application Mobile banking mobile client: It refers to the mobile application client program of mobile banking, which can provide users with local electronic banking services.

Mobile banking server: It refers to the server that can provide targeted services, corresponding to the mobile client of mobile banking. The server specified in this Standard includes software programs, as well as hardware devices that carry and run programs.

Boundary: It refers to the boundary of interconnection between subjects, including interaction boundary, network boundary, physical boundary, etc.

6 Basic requirements and functional requirements for cryptography application the basic requirements and functional requirements for cryptography application of mobile banking information systems shall comply with the requirements of Clause 5 and Clause 6 of GM/T 0054-2018.

7 Level 2 requirements for the cryptography security protection of mobile banking information systems1)

7.1 Basic technical requirements it shall be in accordance with the requirements of the level 2 indicators in GM/T 0054-2018.

Preview: page 5 of 5 shown, 50 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0073-2019