Chinastandards.org

ICS 35.040

GM

GM/T 0054-2018

General requirements for information system cryptography application

信息系统密码应用基本要求

(English Translation)

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0054-2018

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 General requirements
5.1 Cryptographic algorithm
5.2 Cryptography
5.3 Cryptographic products
5.4 Cryptographic service
6 Functional requirements for cryptography
6.1 Confidentiality
6.2 Data integrity
6.3 Authenticity
6.4 Non-repudiation
7 Requirements for cryptography application
7.1 Physical and environmental security
7.1.1 General principles
7.1.2 Information system of classified protection Grade I
7.1.3 Information system of classified protection Grade II
7.1.4 Information system of classified protection Grade III
7.1.5 Information system of classified protection Grade IV
7.2 Network and communication security
7.2.1 General principles
7.2.2 Information system of classified protection Grade I
7.2.3 Information system of classified protection Grade II
7.2.4 Information system of classified protection Grade III
7.2.5 Information system of classified protection Grade IV
7.3 Equipment and computational security
7.3.1 General principles
7.3.2 Information system of classified protection Grade I
7.3.3 Information system of classified protection Grade II
7.3.4 Information system of classified protection Grade III

Preview: page 2 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0054-2018

Chinastandards.org

7.3.5 Information system of classified protection Grade IV
7.4 Application and data security
7.4.1 General principles
7.4.2 Information system of classified protection Grade I
7.4.3 Information system of classified protection Grade II
7.4.4 Information system of classified protection Grade III
7.4.5 Information system of classified protection Grade IV
8 Key management
8.1 General principles
8.2 Information system of classified protection Grade I
8.3 Information system of classified protection Grade II
8.4 Information system of classified protection Grade III
8.5 Information system of classified protection Grade IV
9 Security management
9.1 System
9.1.1 Information system of classified protection Grade I
9.1.2 Information system of classified protection Grade II
9.1.3 Information system of classified protection Grade III
9.1.4 Information system of classified protection Grade IV
9.2 Personnel
9.2.1 Information system of classified protection Grade I
9.2.2 Information system of classified protection Grade II
9.2.3 Information system of classified protection Grade III
9.2.4 Information system of classified protection Grade IV
9.3 Implementation
9.3.1 Planning
9.3.2 Construction
9.3.3 Operation
9.4 Emergency
9.4.1 Information system of classified protection Grade I
9.4.2 Information system of classified protection Grade II
9.4.3 Information system of classified protection Grade III
9.4.4 Information system of classified protection Grade IV

Preview: page 3 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0054-2018

1 Foreword

GM/T 0054-2018 was issued by State Administration of Cryptography on 8 February 2018.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing body of this document shall not be held responsible for identifying any or all such patent rights.

This standard was proposed by and is under the jurisdiction of the Cryptography Standardization Technical Committee.

All the contents of this standard in connection with cryptographic algorithm shall be implemented in accordance with the relevant regulations of China.

Drafting organizations of this standard: Beijing Certificate Authority, Commercial Cryptography Testing Center of State Cryptography Administration, Westone Information Industry INC., Jilin University Information Technologies Co., Ltd., China Financial Computerization Corp., Shanghai Jiao Tong University, and Changsha Yinhe Network Co., Ltd.

Drafters of this standard: Zhan Banghua, Deng Kaiyong, Fu Dapeng, Zhong Bo, Yan Shijie, Fu Yong, Yan Xiaqiang, Gao Zhenpeng, Hu Jianxun, Huang Yifei, Zhang Zhong, Yin Ying, Zhou Zhihong, Li Jihong, and Dong Guizhai.

2 Introduction

As the fundamental core technology of network security, cryptography is the foundation of information protection and network trust system construction, and the key technology to ensure cyberspace security.

This standard mainly puts forward the requirements for cryptography application for different grades of classified protection in terms of physical and environmental security, network and communication security, equipment and computational security, application and data security of the information system, and specifies the requirements for key management and security management of different grades of classified protection.

In this standard, " cryptography " refers to "commercial cryptography".

In the text of this standard, "may", which means it is allowed and permitted, is a declarative description indicating the clauses permitted within the scope of the standard; "should", which means it is recommended and suggested, is a recommendatory description indicating that this clause is preferred but not required; "shall", which means it is obligatory and required, is a mandatory description indicating the requirements to be met for compliance with the standard.

Preview: page 4 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0054-2018

3 Scope Preview

This standard specifies the basic requirements for the cryptography application in information system. This standard is applicable to guiding, regulating and evaluating the cryptography application in information system.

GM/T 0054-2018 falls under ICS 35.040, in the field of information technology.

This catalogue holds 105 other GM/T standards in that field.

In this catalogue, GM/T standards carry edition years from 2012 to 2024.

4 Normative references

GM/T 0005 - Randomness test specification

GM/T 0028 - Specification for security technology for cryptographic modules

GM/T 0036 - Technical guidance of cryptographic application for access control system based on contactless smart card

GM/Z 4001-2013 - Cryptology terminology

5 About this standard

Issued by: State Administration of Cryptography

English translation: about 40 pages

6 Classification and status

International classification (ICS): 35.040

Chinese Standard Classification (CCS): L 80

Prefix GM/T: recommended standard.

Preview: page 5 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0054-2018