Chinastandards.org

GM

GM/T 0134-2024

Cryptographic Module Security Design Guidelines

密码模块安全设计指南

(English Translation)

Issued on: December 27, 2024 **Implemented on: July 1, 2025**

Issued by: State Administration of Cryptography

Preview: page 1 of 4 shown, 25 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0134-2024

Chinastandards.org

Table of Contents

[Preview only]
1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
4.1 Algorithm requirements
4.2 Key types
5 Algorithm identifier and data structure
5.1 General
5.2 General framework
5.3 Sketch of basic authentication principle
5.4 Management function requirements
5.5 Hardware requirements
5.6 Parameter configurable capability requirements
5.7 Process protection
6 Overview of certificate application integrated service interface
6.1 General requirements
6.2 Instructions for algorithm use
6.3 Truncation algorithm
6.4 Management function inspection
6.5 Hardware inspection
6.6 Parameter configurable capability inspection
6.7 Process protection inspection
6.8 Non-invasive security. 119
6.9 Sensitive security parameter management. 121
7 Definition of function of certificate application integrated service interface. 8
7.1 Requirements for password token hardware
7.2 Password token security characteristics
7.3 Interfaces of cryptographic modules. 34
7.4 Roles, services, and authentication
7.5 Software/firmware security. 43
7.6 Operational environment. 45

Preview: page 2 of 4 shown, 25 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0134-2024

7.7 Physical security
7.8 Non-invasive security. 62
7.9 Management of sensitive security parameters
8 Authentication system
8.1 System description
8.2 Services of authentication system
8.3 Management functions of authentication system
8.4 Security requirements
8.5 Key agreement
8.6 Service request
8.7 Disconnection
9 Key management system
9.1 Overview
9.2 System architecture
9.3 Function requirements
9.4 System security design
9.5 Instructions for interfaces of hardware encryption device
9.6 Authentication method based on the digital certificate

1 Foreword

GM/T 0134-2024 was issued by State Administration of Cryptography on 27 December 2024 and has been in force since 1 July 2025.

The GM/T prefix marks a recommended standard. It is not law in itself: it becomes binding when a contract names it, when a regulation or a mandatory standard refers to it, or when a producer declares conformity with it.

The document runs to 25 pages in English translation.

2 Scope Preview

GM/T 0134-2024 carries no ICS number and no Chinese Standard Classification code.

This catalogue holds 160 other GM/T standards.

Of the 108 GM/T standards that do carry an ICS number, 106 (98%) fall under ICS 35, in the field of information technology.

Preview: page 3 of 4 shown, 25 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0134-2024

3 About this standard

Issued by: State Administration of Cryptography

English translation: about 25 pages

Chinese original: about 38,398 characters

4 Related standards

Standards on related subjects:

GM/T 0133-2024 - Requirements for the application of cryptography in critical information infrastructure

GM/T 0135-2024 - Multi-party secure computing technology framework

5 Classification and status

Prefix GM/T: recommended standard.

Preview: page 4 of 4 shown, 25 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0134-2024