Chinastandards.org

GM

GM/T 0127-2023

Mobile terminal cryptographic module application interface specification

移动终端密码模块应用接口规范

(English Translation)

Issued on: December 4, 2023 **Implemented on: June 1, 2024**

Issued by: State Administration of Cryptography

Preview: page 1 of 4 shown, 31 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0127-2023

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Structural model
5.1 Hierarchy
5.2 Application structure of the module
6 Definitions of data types
6.1 Definition description of the algorithm identifier and data type
6.2 Definitions of basic data types
6.3 Definitions of composite data types
7 Mobile terminal cryptographic module application interface
7.1 General
7.2 Cryptographic algorithm implementation requirements
7.3 Definition of the cryptographic application package
7.4 Definition of the cryptographic application interface
7.5 Cryptographic module class
7.6 Module connection interface
7.7 Module interface
7.8 Application interface
7.9 Container interface
7.10 Session key interface
7.11 Cryptographic hash interface
7.12 Message authentication code interface
7.13 Keyed-hash message authentication code interface
8 Safety requirements
8.1 Module usage phase
8.2 Right management
8.3 Other security requirements

Preview: page 2 of 4 shown, 31 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0127-2023

1 Foreword

GM/T 0127-2023 was issued by State Administration of Cryptography on 4 December 2023 and has been in force since 1 June 2024.

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 31 pages in English translation.

2 Scope Preview

This document specifies the structure model, data type definition, application interface, and security requirements of mobile terminal cryptographic modules. This document is applicable to the development and use of mobile terminal cryptographic module products, as well as the application development and detection based on such cryptographic products.

GM/T 0127-2023 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.

3 Normative references

GB/T 15852.1 - Information technology - Security techniques - Message authentication codes - Part 1: Mechanisms using a block cipher

GB/T 32905 - Information security techniques - SM3 cryptographic hash algorithm

GB/T 32907 - Information security technology - SM4 block cipher algorithm

GB/T 32918 (all parts) - Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves

GB/T 33560 - Information security technology - Cryptographic application identifier criterion specification

GB/T 35276 - Information security technology - SM2 cryptographic algorithm usage specification

GB/T 37092 - Information security technology - Security requirements for cryptographic modules

GM/T 0017-2023 - Smart token cryptography application interface data format specification

Preview: page 3 of 4 shown, 31 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0127-2023

GM/Z 4001 - Cryptology terminology

4 About this standard

Issued by: State Administration of Cryptography

English translation: about 31 pages

Chinese original: about 46,410 characters

5 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

6 Classification and status

Chinese Standard Classification (CCS): L 80

Prefix GM/T: recommended standard.

Preview: page 4 of 4 shown, 31 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0127-2023