Chinastandards.org

GM

GM/T 0128-2023

Datagram transport layer cryptographic protocol specification

数据报传输层密码协议规范

(English Translation)

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

Issued by: State Administration of Cryptography

Preview: page 1 of 3 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0128-2023

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Cryptographic algorithms and key types
5.1 General
5.2 Cryptographic algorithm
5.2.1 Asymmetric cryptographic algorithm
5.2.2 Block cipher algorithm
5.2.3 Cryptographic hash algorithm
5.2.4 Data expansion function P_hash
5.2.5 Pseudo-random function (PRF)
5.3 Key types
6 Protocols
6.1 General
6.2 Definition of data type
6.3 Record layer protocol
6.4 Handshake protocol suite
6.5 Key computation

1 Foreword

GM/T 0128-2023 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 13 pages in English translation.

2 Scope Preview

This document specifies datagram transport layer cryptography protocol, including record layer protocols, handshake protocol suite, and key computation. This document is

Preview: page 2 of 3 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0128-2023

applicable to the development, testing, management and use of datagram transport layer cryptography protocol related products (such as gateways, terminals, etc.).

GM/T 0128-2023 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 38636-2020 - Information security technology - Transport layer cryptography protocol (TLCP)

GM/Z 4001 - Cryptology terminology

4 About this standard

Issued by: State Administration of Cryptography

English translation: about 13 pages

Chinese original: about 19,168 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 3 of 3 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0128-2023