Chinastandards.org

GM

GM/T 0129-2023

SSH password protocol specification

SSH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 4 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0129-2023

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Protocol framework
5.1 General
5.2 Transport layer protocol
5.3 Authentication protocol
5.4 Connection protocol
6 Cryptographic algorithms and key types
6.1 Cryptographic algorithm
6.2 Key types
7 Definitions of data types
7.1 Algorithm identifier
7.2 Basic data types
8 Transport layer protocol
8.1 General
8.2 Protocol flow
8.3 Protocol version
8.4 Packet
8.5 Key agreement
8.6 Service request
8.7 Disconnection
9 Authentication protocol
9.1 General
9.2 Protocol flow
9.3 Packet
9.4 Password-based authentication method
9.5 Authentication method based on the asymmetric key
9.6 Authentication method based on the digital certificate

Preview: page 2 of 4 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0129-2023

1 Foreword

GM/T 0129-2023 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 16 pages in English translation.

2 Scope Preview

This document specifies the secure shell cryptography protocol, the encrypted transport protocol, the authentication protocol, the connection protocol of the interactive tunnel, and the usage method of the cryptographic algorithm in the protocol. This document is applicable to the development and testing of SSH server and SSH client products.

GM/T 0129-2023 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 15852.2 - Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function

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

GB/T 35275 - Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification

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

GM/T 0015 - Digital certificate format based on SM2 algorithm

GM/Z 4001 - Cryptology terminology

Preview: page 3 of 4 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0129-2023

4 About this standard

Issued by: State Administration of Cryptography

English translation: about 16 pages

Chinese original: about 24,265 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, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0129-2023