Chinastandards.org

ICS 35.040
CCS L 80

GM

GM/T 0086-2020

Specification of key management system based on SM9 identity cryptography algorithm

基于SM9标识密码算法的密钥管理系统技术规范

(English Translation)

Issued on: December 28, 2020 **Implemented on: July 1, 2021**

Issued by: State Administration of Cryptography

Preview: page 1 of 4 shown, 23 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0086-2020

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Basic feature description
6 Logo Key Management System Architecture
7 Composition and function of identification key management system
7.1 Private key generation system
7.2 Registration Service System
7.3 Public parameter service system
7.4 End entity
7.5 Local Agent
8 Basic requirements for key management
8.1 Key application login authentication
8.2 Key generation
8.3 Key Transmission
8.4 Key storage
8.5 Key update
8.6 Key cancellation
8.7 Key Backup
8.8 Key Recovery
8.9 System Master Key Management
9 Identification key management system password usage
9.1 Use of cryptographic algorithms
9.2 Password device

1 Foreword

GM/T 0086-2020 was issued by State Administration of Cryptography on 28 December 2020 and has been in force since 1 July 2021.

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

Preview: page 2 of 4 shown, 23 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0086-2020

producer declares conformity with it.

The document runs to 23 pages in English translation.

2 Scope Preview

GM/T 0086-2020 - 2 Normative references 1 3 Terms and definitions 1 4 Abbreviations 3 5 Basic feature description 3 6 Logo Key Management System Architecture 3 7 Composition and function of identification key management system 4 7.1 Private key generation system 4 7.2 Registration Service System 5 7.3 Public parameter service system 6 7.4 End entity 7 7.5 Local Agent 7 8 Basic requirements for key management 7 8.1 Key application login authentication 7 8.2 Key generation 7 8.3 Key Transmission 8 8.4 Key storage 8 8.5 Key update 8 8.6 Key cancellation 8 8.7 Key Backup 8 8.8 Key Recovery 8 8.9 System Master Key Management 9 9 Identification key management system password usage 9 9.1 Use of cryptographic algorithms 9 9.2 Password device 9 10 Key Management Security Operation Process 10 10.1 System initialization process 10 10.2 Key carrier initialization 10 10.3 User key generation process 10 10.4 Identification status release process 11 10.5 Update user identification key status process 12 10.6 Process of restoring user identification key status 12 10.7 User information status query and response process 12 10.8 Master key update process 13 11 Construction and security protection of identification key management system 13 11.1 System construction 13 11.2 Security protection settings 13 12 Safety management requirements 15 12.1 Security management mechanism 15 12.2 Personnel Management 15 12.3 Management System 16 12.4 Audit Management 16 12.5 Management Platform 16 13 Identify the key management system hierarchy 16 13.1 Identifying the type of key management system 16 13.2 Distinguish the logo of KMS 17 13.3 Registering a lower-level KMS 17 13.4 Lower-level KMS master key generation process 17 13.5 Issuing the lower-level KMS master key 18

GM/T 0086-2020 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.

3 About this standard

Issued by: State Administration of Cryptography

English translation: about 23 pages

Chinese original: about 28,224 characters

Preview: page 3 of 4 shown, 23 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0086-2020

4 Related standards

Standards on related subjects:

GM/T 0085-2020 - Identity-based cryptographic algorithm SM9 based on technology system framework

GB/T 15843.1-2017 - Information technology -- Security techniques -- Entity authentication -- Part 1: General

GA/T 1389-2017 - Information Security Technology - Guidelines for Grading of Classified Protection of Cyber Security

GM/T 0080-2020 - SM9 cryptographic algorithm application specification

GM/T 0079-2020 - Direct anonymous attestation specification for trusted computing platform

GM/T 0078-2020 - The design guidelines for cryptographic random number generation module

5 Classification and status

International classification (ICS): 35.040

Chinese Standard Classification (CCS): L 80

Prefix GM/T: recommended standard.

Preview: page 4 of 4 shown, 23 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0086-2020