Chinastandards.org

CCS L 80

GM

GM/T 0082-2020

Trusted cryptography module protection profile

可信密码模块保护轮廓

(English Translation)

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

Issued by: State Administration of Cryptography

Preview: page 1 of 4 shown, 21 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0082-2020

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, 21 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0082-2020

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 0082-2020 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 producer declares conformity with it.

The document runs to 21 pages in English translation.

2 Scope Preview

GM/T 0082-2020 is filed under Chinese Standard Classification L 80, in the field of electronic components and information technology.

This catalogue holds 52 other GM/T standards without an ICS number.

In this catalogue, GM/T standards carry edition years from 2012 to 2024.

Preview: page 3 of 4 shown, 21 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0082-2020

3 About this standard

Issued by: State Administration of Cryptography

English translation: about 21 pages

Chinese original: about 32,396 characters

4 Related standards

Standards on related subjects:

GM/T 0081-2020 - SM9 cryptographic algorithm encryption and signature message syntax specification

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

Chinese Standard Classification (CCS): L 80

Prefix GM/T: recommended standard.

Preview: page 4 of 4 shown, 21 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0082-2020