Chinastandards.org

ICS 35.040
CCS L 80

GM

GM/T 0087-2020

Browser cryptography API specification

浏览器密码应用接口规范

(English Translation)

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

Issued by: State Administration of Cryptography

Preview: page 1 of 4 shown, 22 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0087-2020

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms, definitions and abbreviations
3.1 Terms and definitions
3.2 Abbreviations
4 Overview
5 Data structure
5.1 Large integer
5.2 Key pair dictionary
5.3 JsonWebKey dictionary
5.4 Algorithm
5.5 Password interface Crypto
5.6 Key Algorithm KeyAlgorithm
5.7 Key Interface CryptoKey
6 Password interface
6.1 Interface definition
6.2 Encryption method
6.3 Decryption method
6.4 Signature method
6.5 Method of verifying signature
6.6 Hashing method
6.7 Method of generating key
6.8 Method of Deriving Key
6.9 Derived bit method
6.10 Import key method
6.11 Export key method
6.12 Encapsulation key method
6.13 Decapsulation key method
6.14 Exception
7 Algorithm flow
7.1 SM3 Algorithm
7.2 SM2 encryption algorithm

Preview: page 2 of 4 shown, 22 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0087-2020

7.3 SM2 signature algorithm

7.4 SM4 Algorithm

7.5 SM4-ECB Algorithm

1 Foreword

GM/T 0087-2020 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 22 pages in English translation.

2 Scope Preview

GM/T 0087-2020 - 2 Normative references 1 3 Terms, definitions and abbreviations 1 3.1 Terms and definitions 1 3.2 Abbreviations 1 4 Overview 1 5 Data structure 2 5.1 Large integer 2 5.2 Key pair dictionary 2 5.3 JsonWebKey dictionary 2 5.4 Algorithm 3 5.5 Password interface Crypto 3 5.6 Key Algorithm KeyAlgorithm 4 5.7 Key Interface CryptoKey 4 6 Password interface 5 6.1 Interface definition 5 6.2 Encryption method 6 6.3 Decryption method 6 6.4 Signature method 7 6.5 Method of verifying signature 7 6.6 Hashing method 7 6.7 Method of generating key 8 6.8 Method of Deriving Key 8 6.9 Derived bit method 9 6.10 Import key method 9 6.11 Export key method 10 6.12 Encapsulation key method 10 6.13 Decapsulation key method 11 6.14 Exception 12 7 Algorithm flow 12 7.1 SM3 Algorithm 12 7.2 SM2 encryption algorithm 13 7.3 SM2 signature algorithm 16 7.4 SM4 Algorithm 20

GM/T 0087-2020 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 22 pages

Chinese original: about 27,293 characters

Preview: page 3 of 4 shown, 22 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0087-2020

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, 22 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0087-2020