Chinastandards.org

ICS 35.040

GM

# GM/T 0003.5-2012

## Public Key Cryptographic Algorithm SM2 Baded on Elliptic Curves - Part 5: Parameter Definition

SM2椭圆曲线公钥密码算法 第5部分：参数定义

**(English Translation)**

**Issued by: State Administration of Cryptography**

Preview: page 1 of 3 shown, 14 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0003-5-2012

Chinastandards.org

# Table of Contents

[Preview only]
1 Scope
2 Normative References
2.1 Terms
3 Terms and Definitions
4 Abbreviations

## 1 Foreword

GM/T 0003.5-2012 was issued by State Administration of Cryptography on 21 March 2012.

It is one of 5 parts of the GM/T 0003 series.

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.

## 2 Scope Preview

This part of GM/T 0003 specifies the curve parameters of the public key cryptographic algorithm SM2 based on elliptic curves, and gives the examples of digital signature and verification, key exchange and verification, and message encryption and decryption.

GM/T 0003.5-2012 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 14 pages

## 4 Related standards

Other parts of this standard:

GM/T 0003.1-2012 - Based on Elliptic Curves - Part 1: General

GM/T 0003.2-2012 - Part 2: Digital Signature Algorithm



Preview: page 2 of 3 shown, 14 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0003-5-2012

Chinastandards.org

GM/T 0003.3-2012 - Based on Elliptic Curves - Part 3: Key Exchange Protocol

GM/T 0003.4-2012 - Based on Elliptic Curves - Part 4: Public Key Encryption Algorithm

## 5 Classification and status

International classification (ICS): 35.040

Chinese Standard Classification (CCS): L 80

Prefix GM/T: recommended standard.



Preview: page 3 of 3 shown, 14 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0003-5-2012