

ICS 35.030
CCS L 80

GM

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GM/T 0130-2023

**Certificateless and implicit-certificate-based public key
mechanisms based on the SM2 algorithms**

基于SM2算法的无证书及隐式证书公钥机制

(English Translation)

Issued on: December 4, 2023

Implemented on: June 1, 2024

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Abbreviations	3
Overview	4
Elliptic curve system parameters	5
User identification information	6
Master key generation mechanism	7
User key pair generation mechanism	8
Digital signature generation mechanism	9
Verification mechanism of digital signature	10
Encryption mechanism	11
Encryption mechanism	12

1 Scope

This document specifies the certificateless and implicit certificate public key mechanism based on the SM2 algorithm, including key generation and verification mechanism, digital signature mechanism, public key encryption mechanism.

The digital signature mechanism specified in this document is applicable to digital signatures and verification in commercial cryptographic applications; the encryption mechanism is applicable to message encryption and decryption in commercial cryptographic applications. The mechanism specified in this document is particularly suitable for application environments with limited bandwidth and computing resources.

2 Normative references

The contents of the following documents constitute the essential terms of this document through normative references in the text. Among them, for dated references, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies to this document.

GB/T 32918.1-2016 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 1: General
GB/T 32918.2-2016 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 2: Digital signature algorithm
GB/T 32918.4-2016 Information security technology - Public key

cryptographic algorithm SM2 based on elliptic curves - Part 4: Public key encryption algorithm GB/T 32918.5-2017 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 5: Parameter definition GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm GB/T 32915 Information security technology - Randomness test methods for binary sequence

4.2 Abbreviations

The following abbreviations apply to this document.

CA. Certificate Authority

5.1 Overview

The public key mechanism specified in this document includes key generation and verification mechanism, digital signature mechanism, public key encryption mechanism. Among them, the key generation and verification mechanism includes the generation mechanism of the master key and the generation and verification mechanism and process of the user key pair.

5.2 Elliptic curve system parameters

The elliptic curve system parameters include the scale q of the finite field F_q (when $q =$

5.4 User identification information

User A has an identification IDA of length entlen_A bits, where ENTLA is two bytes converted from the integer entlen_A . The KGC of the key generation mechanism specified in this document, the signer and verifier of the digital signature mechanism,

6.1 Master key generation mechanism

KGC uses the random number ms in $[1, n - 1]$ as the system master private key, to calculate the system master public key $P_{\text{pub}} = [ms]G$.

6.2 User key pair generation mechanism

User A and KGC work together to generate the user's key pair. User private key d_A and declaration public key W_A . Both shall implement the following operation steps.

7.1 Digital signature generation mechanism

Let the message to be signed be M . In order to obtain the digital signature (r, s) of message M , user A as the signer shall implement the following operation steps.

7.2 Verification mechanism of digital signature

In order to verify the received message M' and its digital signature ($r's'$), user B as the verifier shall implement the following operation steps.

8.1 Encryption mechanism

Let the message to be sent be a bit string M . In order to encrypt the plaintext M and GM/T 0130-2023 GM CRYPTOGRAPHIC INDUSTRY STANDARD ICS 35.030 CCS L 80 Certificateless and implicit-certificate-based public key mechanisms based on the SM2 algorithms Issued on. DECEMBER 04, 2023 Implemented on. JUNE 01, 2024 Issued by. State Cryptography Administration

Table of Contents

Foreword... 3

Introduction... 4

1 Scope... 5

2 Normative references... 5

3 Terms and definitions... 6

4 Symbols and abbreviations... 7

4.1 Symbols... 7

4.2 Abbreviations... 9

5 Mechanism parameters and auxiliary functions... 10

5.1 Overview... 10

5.2 Elliptic curve system parameters... 10

5.3 Auxiliary functions... 11

5.4 User identification information... 12

6 Key generation mechanism and process... 12

6.1 Master key generation mechanism... 12

6.2 User key pair generation mechanism... 12

6.3 User key pair generation process... 13

6.4 User key pair verification mechanism... 14

6.5 User key pair verification process... 15

7 Digital signature mechanism... 16

7.1 Digital signature generation mechanism... 16

7.2 Verification mechanism of digital signature... 16

8 Public key encryption mechanism... 16

8.1

Encryption mechanism... 16

8.2 Decryption mechanism... 17 Appendix A (Informative) Mechanism data example... 18

Appendix B (Informative) Application example of mechanism in implicit certificate application... 26 Appendix C (Informative) Application example of the mechanism in the industrial Internet identity resolution system... 31 Appendix D (Informative) Deterministic generation method of user key of key generation center... 35 References... 36

Certificateless and implicit-certificate-based public key mechanisms based on the SM2 algorithms

1 Scope

This document specifies the certificateless and implicit certificate public key mechanism based on the SM2 algorithm, including key generation and verification mechanism, digital signature mechanism, public key encryption mechanism.

The digital signature mechanism specified in this document is applicable to digital signatures and verification in commercial cryptographic applications; the encryption mechanism is applicable to message encryption and decryption in commercial cryptographic applications. The mechanism specified in this document is particularly suitable for application environments with limited bandwidth and computing resources.

2 Normative references the contents of the following documents constitute the essential terms of this document through normative references in the text. Among them, for dated references, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies to this document.

GB/T 32918.1-2016 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 1: General GB/T 32918.2-2016 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 2: Digital signature algorithm GB/T 32918.4-2016 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 4: Public key encryption algorithm GB/T 32918.5-2017 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves - Part 5: Parameter definition GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm GB/T 32915 Information security technology - Randomness test methods for binary sequence

4.2 Abbreviations