

ICS 35.040
CCS L 80



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

GB/T 17901.3-2021

**Information technology - Security techniques - Key
management - Part 3: Mechanisms using asymmetric
techniques**

信息技术 安全技术 密钥管理 第3部分：采用非对称技术的机制

(English Translation)

Issued on: March 9, 2021

Implemented on: October 1, 2021

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Symbols and abbreviations	
5 Requirements	
6 Key Derivation Function	
7 Remainder multiplication	
8 Key Commitment	
9 Key confirmation	
10 Key Management Framework	
10.1 Summary	
10.2 Key agreement between two parties	
10.3 Three-party key agreement	
10.4 Secret key transmission	
10.5 Public key transmission	
11 Key Agreement	
11.1 Key agreement mechanism 1	
11.2 Key agreement mechanism 2	
11.3 Key agreement mechanism 3	
11.4 Key agreement mechanism 4	
11.5 Key agreement mechanism 5	
11.6 Key agreement mechanism 6	
11.7 Key agreement mechanism 7	
11.8 Key agreement mechanism 8	
11.9 Key agreement mechanism 9	
11.10 Key agreement mechanism 10	
11.11 Key agreement mechanism 11	
11.12 Key agreement mechanism 12	
12 Key transfer	
12.1 Key delivery mechanism 1	
12.2 Key delivery mechanism 2	

12.3 Key delivery mechanism 3

12.4 Key delivery mechanism 4

12.5 Key delivery mechanism 5

12.6 Key delivery mechanism 6

13 Public key transfer

13.1 Public key delivery mechanism 1

13.2 Public key delivery mechanism 2

13.3 Public key delivery mechanism 3

Appendix A (Normative Appendix) Object Identifier

Appendix B (informative appendix) Key establishment mechanism features

Appendix C (informative appendix) Examples of key derivation functions

Appendix D (informative appendix) Examples of function F, sets S1 and S2

Appendix E (informative appendix) Example of key establishment mechanism based on elliptic curve

Appendix F (informative appendix) Patent information related to the adopted international standards

Reference

1 Scope

This part of GB/T 17901 defines the requirements of a key management mechanism based on asymmetric cryptography, key derivation functions, and remainder formulas.

Multiplication, key commitment, key confirmation, key management framework, key agreement, key transfer, public key transfer. This part intends to achieve the following objectives.

- a) Establish a shared key through key agreement for symmetric encryption between entity A and entity B. In the key agreement mechanism, The key is calculated from the data exchanged between entity A and entity B, and no entity can determine the value of the shared key in advance.
- b) Establish a shared key through key transfer, which is used for symmetric encryption between entity A and entity B. In the key delivery mechanism, The key is selected by entity A, and passed to entity B using asymmetric password protection technology.
- c) Pass the public key of entity A to other entities through key transfer. In the public key delivery mechanism, the public key of entity A is authenticated and then transmitted To other entities, but without confidentiality.

Some mechanisms defined in this section are based on the authentication mechanism

corresponding to GB/T 15843.3-2016. This section does not include the following key management content.

- a) Key lifetime management;
- b) The mechanism for generating or determining asymmetric key pairs;
- c) Key storage, archiving, and deletion mechanisms.

This section applies to the development of systems that use asymmetric technology to achieve key management, and can also guide the detection of such systems.

Note: The mechanism defined in this section does not involve the distribution of the entity's private key, and the key exchange message is signed by the public key signature system.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this article. For undated reference documents, the latest version (including all amendments) is applicable to this document.

GB/T 15843.3-2016 Information Technology Security Technology Entity Authentication Part 3: Mechanisms Using Digital Signature Technology

GB/T 17901.1-2020 Information Technology Security Technology Key Management Part 1: Framework

GB/T 25069 Information Security Technical Terms

GB/T 32905 Information Security Technology

SM3 Cipher Hash Algorithm

GB/T 32918.1 Information Security Technology

SM2 Elliptic Curve Public Key Cryptography Algorithm Part 1: General Principles

GB/T 32918.2 Information Security Technology

SM2 Elliptic Curve Public Key Cryptography Algorithm Part 2: Digital Signature Algorithm

GB/T 32918.3-2016 Information Security Technology

SM2 Elliptic Curve Public Key Cryptography Algorithm Part 3: Key Exchange Protocol

GB/T 32918.4 Information Security Technology

SM2 Elliptic Curve Public Key Cryptographic Algorithm Part 4: Public Key Cryptographic Algorithm

3 Terms and definitions

The following terms and definitions defined in GB/T 17901.1-2020 and GB/T 25069 apply to this document.

3.1 Elliptic curve cryptographic algorithm

The rational points on the elliptic curve are used to form a public key cryptographic algorithm that is difficult to calculate the discrete logarithm of the ellipse on the Abel additive group.

3.2 Token

A message composed of data fields related to a specific communication contains information transformed using cryptographic techniques.

3.3 Key commitment

The process of confirming one's own public key or key token to the other party.

3.4 Key confirmation

The process by which an entity is convinced that another identified entity has the correct key.

4.1 Symbols

The following symbols apply to this document.

A, B, C. the identification of entities A, B, and

C. BE. Encrypted data block. BS. signed data block with signed data block. CertA. Entity A's public key certificate.

DA(). The private decryption transformation function of entity A. dA. Entity A's private decryption key.

E. Elliptic curve, given the equation $Y^2 = X^3 + aX + b$ in the domain $GF(pm)$, when $p > 3$ and m is a positive integer, given in the domain The equation $Y^2 + XY = X^3 + aX^2 + b$ on $GF(2m)$, or the equation $Y^2 = X^3 + aX^2 + b$ on the field $GF(3m)$, there is an additional The reference point OE is called the point of infinity, which is recorded as $E/GF(pm)$, $E/GF(2m)$, or $E/GF(3m)$.

EA(). The public encryption transformation function of entity

A. eA. The public encryption key of entity

A. F(). Key agreement function. FP(). Pair-based key agreement function.