

ICS 35.040
CCS L 80

GM

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

GM/T 0095-2020

**Technical requirements for applications of cryptography in
electronic bidding**

电子招投标密码应用技术要求
(English Translation)

Issued on: December 28, 2020

Implemented on: July 1, 2021

Issued by: State Administration of Cryptography

Table of Contents

Foreword	1
Scope	2
Normative references	3
Terms and definitions	4
Asymmetric cryptographic algorithm	5
Digital certificate	6
Certificate authority; CA	7
Confidentiality	8
Data integrity	9
Abbreviations	10
Reference model	11
User registration	12
Bidding plan	13
Tender invitation	14
Bid issuing	15
Bid evaluation	16
Bid awarding	17
Objection	18
Algorithm requirements	19
Overview	20
Server cryptographic device	21
Identity authentication technical requirements	22
Data encryption technology requirements	23
Technical requirements for electronic signature	24
Electronic seal	25
Key management requirements	26
Foreword	27
Algorithm requirements	28
Overview	29
Server cryptographic device	30
Identity authentication technical requirements	31
Data encryption technology requirements	32

Technical requirements for electronic signature	33
Electronic seal	34

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2020 "Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents".

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. The issuing authority shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of Cryptographic Industry Standardization Technical Committee.

1 Scope

This document specifies the technical requirements for the application of cryptographic technology in electronic bidding, including in the electronic bidding process, the technical requirements for the use of cryptographic algorithms and cryptographic products.

This document is applicable to guiding the design, implementation and use of the cryptographic subsystem in the electronic bidding system. The test and management of the cryptographic subsystem in the electronic bidding system can use it as reference.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 20518, Information security technology - Public key infrastructure -Digital certificate format
 GB/T 32905, Information security technology SM3 cryptographic hash algorithm
 GB/T 32907, Information security technology - SM4 block cipher algorithm
 GB/T 32918 (all parts), Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves
 GB/T 35275, Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification
 GB/T 35276, Information security technology - SM2 cryptography algorithm usage specification
 GM/T 0031, Secure electronic seal cryptography technical specification
 GM/T 0054, General requirements for information system cryptography application
 GM/Z 4001-2013, Cryptographic terms

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GM/Z 4001-2013 as well as the followings apply.

3.1 Asymmetric cryptographic algorithm

a cryptographic algorithm that encryption and decryption use different keys; one of the keys (public key) can be made public, and the other key (private key) must be kept secret; it is computationally infeasible to solve the private key from the public key

3.2 Digital certificate

a data structure signed by a certificate authority (CA) that contains public key owner information, public key, issuer information, validity period, and extended information

3.3 Certificate authority; CA

an entity that manages the entire life cycle of digital certificate

3.4 Confidentiality

the nature of ensuring that information is not leaked to unauthorized individuals, processes and other entities

3.5 Data integrity

the characteristic that the data has not been altered or destroyed in an unauthorized manner

4 Abbreviations

The following abbreviations apply to this document.

CRL. Certificate Revocation List IC. Integrated Circuit

5 Reference model

The electronic bidding system uses various security technologies including ciphers to ensure the security of bidding operations.

6.1 User registration

During the registration process, the important sensitive information of the bidder, tendering agency, and tenderer involved in the process is encrypted and protected during the transmission process.

6.2 Bidding plan

In the bidding plan stage, the documents issued by the tenderer in the name of the organization, including bidding commission contract and bidding project documents, shall use the digital certificate of the tenderer or agency for electronic signature.

6.3 Tender invitation

In the tender invitation stage, the electronic bidding system shall use the digital certificate of the tenderer or agency to conduct electronic signature to documents such as procurement bidding announcements, prequalification announcements and tender invitations. It shall be time stamped at the same time. It is advisable to use electronic signature at the same time.

6.4 Bid issuing

During the bid issuing, the tenderer shall conduct electronic signature and time stamp to the published documents. It is advisable to use electronic seal at the same time. The bidding documents can include bidding announcements,

6.7 Bid evaluation

During the bid evaluation, the electronic bidding system shall authenticate the identity of bid evaluation experts. Identity authentication shall meet the requirements of 7.3.

6.8 Bid awarding

During the bid awarding process, the tenderer shall be able to electronically sign the announced announcement of successful bid candidates, the announcement of the winning bid result, the bid winning notice/prequalification result/tender result notice. Electronic signature shall be used. Time stamp can be sealed.

6.9 Objection

When the bidder raises objections to the prequalification documents, bidding documents, bid opening process, prequalification results, and bid evaluation results, the content of the objection submitted shall be electronically signed.

The tenderer shall electronically sign the content of the objection and stamp it with a time stamp. Electronic signature and verification shall meet the requirements of 7.5.

7.1 Algorithm requirements

The cryptographic algorithms that the electronic bidding system shall use include SM3 cryptographic hash algorithm, SM4 block cryptographic algorithm, SM2 elliptic curve public key cryptographic algorithm.