

ICS 35.030
CCS L 80

GM

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

GM/T 0109-2021

**Technical requirements for electronic signature service based
on cloud computing**

基于云计算的电子签名服务技术要求
(English Translation)

Issued on: October 18, 2021

Implemented on: May 1, 2022

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative References	2
Service mode	3
Technical Requirements for Relying Parties	4
General requirements	5
Local data protection	6
Identity authentication	7
Communication data protection	8
Key management	9
Confirmation and control of electronic signatures	10
Requirements for electronic signature format	11
Requirements for digital certificate	12
User registration	13
User review	14
User activation	15
User information maintenance	16
User logout	17
Overview	18
Key generation	19
Key backup and recovery	20
Key destruction	21
Overview	22
Identification of signature requests	23
Requirements for the electronic signature process	24
Security control of the signature process	25
Data security requirements	26
Access identity authentication	27
Access control	28
Data transmission requirements	29
Request processing and response	30
Security operation requirements	31

1 Scope

This Document describes the cryptographic technology requirements for electronic signature services based on cloud computing, and proposes the cryptographic technology requirements for electronic signature services based on cloud computing using digital certificates and digital signature technologies.

This Document is applicable to guiding the construction, management, detection and application of electronic signature services based on cloud computing.

2 Normative References

The provisions in following documents become the essential provisions of this Document through reference in this Document. For the dated documents, only the versions with the dates indicated are applicable to this Document; for the undated documents, only the latest version (including all the amendments) is applicable to this Document.

GB/T 15843 Information technology - Security techniques - Entity authentication
GB/T 20518 Information security technology - Public key infrastructure - Digital certificate format
GB/T 22239 Information security technology - Baseline for classified protection of cybersecurity
GB/T 25056 Information security technology - Specifications of cryptograph and related security technology for certificate authentication system
GB/T 25064 Information security technology - Public key infrastructure - Electronic signature formats specification
GB/T 31168-2014 Information Security Technology - Security Capability Requirements of Cloud Computing Services
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

--- In the cloud-based electronic signature activity, the signer entrusts the electronic signature function or part of the electronic signature function to the cloud-base signing service; and the signer uses the terminal, application program or application system to control and confirm the process of making electronic signature;

--- The relying party performs subsequent business operations by judging the validity of the electronic signature and related data provided by the signer or cloud-base signing service;

--- The cloud-base signing service provides electronic signature services and related user management, key management and other services; and shall provide operation support for the cloud-base signing service. The cloud-base signing service is provided in the form of cloud service; and has the characteristics of on-demand cloud service, ubiquitous access, resource pooling, rapid scalability, and service measurability.

5.2 Service mode

Depending on the business scenario, the cloud-base signing service can provide services to the outside in different modes. Common service modes are as follows.

--- Collaborative signature mode: refers to the signer and the cloud-base signing server-side each saving a part of the key component, and generating the final signature result through cryptographic protocol interaction. See A.1 for details.

--- Proxy signature mode: refers to the signer hosting the key on the cloud-base signing server-side, and authorizing the cloud-base signing server-side to complete the signing operation for it when an electronic signature is required. See A.2 for details.

6 Technical Requirements for Relying Parties

The relying party shall use the cryptographic module to complete the cryptographic functions related to the electronic signature process based on cloud computing and the verification signature process. The cryptographic module shall pass the commercial cryptographic testing and certification and meet the requirements of the security level matching the business in GB/T 37092. The cryptographic module shall support the relying party to verify the electronic signature function; and the verification electronic signature process shall meet the requirements of GB/T 25064. If the electronic signature function needs to be initiated by the relying party, the cryptographic module shall provide the cryptographic function required for the cloud-base signing service access function.

7.1 General requirements

Signers can use cryptographic modules to complete the cryptographic functions required for electronic signatures based on cloud computing. If a cryptographic module is used, the module shall pass the commercial cryptographic test and certification, meet the requirements of the security level matching the business in GB/T 37092; and support the requirements of 7.2~7.6.

7.2 Local data protection

Signers shall protect the integrity and confidentiality of local key configuration data and sensitive data.

7.3 Identity authentication

When the signer communicates with the cloud-base signing service, it shall support the authentication of the cloud-base signing service identity and declare its own identity in accordance with the access requirements of the cloud-base signing service.

7.4 Communication data protection

When the signer communicates with the cloud-base signing service, it shall protect the communication data in accordance with the access requirements of the cloud-base signing service.

7.5 Key management

When using the collaborative signature mode for electronic signature, the signers shall support the generation of the client component of the signature key within the cryptographic module, and support the storage and secure use of the key component.

7.6 Confirmation and control of electronic signatures

During the electronic signature process, the signer shall confirm the relevant data of the electronic signature and control the signing process through interaction. If the content confirmation and signature interaction adopt the cryptographic module, the following requirements shall be met:

- a) It shall support the identification of the source of the received electronic signature request and the confirmation of the integrity of the electronic signature message content;
- b) When the collaborative signature mode is adopted, it shall ensure that the customer end signature behavior matches the server-side signature behavior; for example, by verifying the signature to confirm whether the collaborative process is completed normally.
- a) The digital signature algorithm shall adopt the SM2 elliptic curve public key cryptographic algorithm, which meets the requirements of GB/T 32918 and GB/T 35276;
- b) The data integrity protection during the electronic signature process shall adopt the SM3 cryptographic hash algorithm specified in GB/T 32905;
- c) The data confidentiality protection during the electronic signature process shall adopt the SM4 block cipher algorithm specified in GB/T 32907.

8.3.1.2 Requirements for electronic signature format

The electronic signature data generated by the cloud-base signing service shall meet the requirements of GB/T 25064 or GB/T 35275. For electronic signatures that need to be stored for a long time, the electronic signature shall contain the timestamp and certificate status information at the time of signing, such as CRL, OCSP response information, etc.

8.3.1.3 Requirements for digital certificate

If the electronic signature requires third-party authentication, the electronic signature service based on cloud computing shall use a digital certificate issued by a legitimate