

ICS 35.040

GM

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

GM/T 0071-2019

Guidance of cryptographic application for electronic records

电子文件密码应用指南

(English Translation)

Issued on: July 12, 2019

Implemented on: July 12, 2019

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Application system	3
Data user	4
Electronic records	5
Universal cryptography service	6
Typical cryptography service	7
Key	8
Confidentiality of record attribute	9
Integrity of record attribute	10
Non-repudiation	11
Storage security	12
Exchange classification	13
Internal exchange of business system	14
Exchange between business systems	15

1 Scope

This Standard proposes the technical framework and security goals of the cryptographic application for electronic records, and describes the method of performing cryptographic operations for electronic records and the method of using cryptographic technique in the application system of electronic records.

This Standard applies to the development and use of application system of electronic records.

2 Normative references

The following documents are indispensable for the application of this document.

For dated references, only the dated version applies to this document. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 20518, Information security technology - Public key infrastructure -Digital certificate format
 GB/T 25069-2010, Information security technology glossary
 GB/T 31913-2015, General functional requirements for administrative electronic records creation and

transaction system GB/T 32905, Information security techniques - SM3 cryptographic hash algorithm GB/T 32907, Information security technology - SM4 block cipher algorithm GB/T 32918, 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 GM/T 0019, Universal cryptography service interface specification GM/T 0031, Secure electronic seal cryptography technical specification GM/T 0033, Interface specifications of time stamp in order to achieve the security goal of electronic record management, cryptographic technology shall be used to ensure the security of the entire life cycle of electronic records. That is, ensure that the formation process of electronic records is true and reliable; ensure that electronic records are not tampered during transmission (exchange), reception and storage; ensure that electronic records are not leaked to unauthorized visitors; ensure that operators of electronic records cannot deny their operating behaviors and processing results.

The security of electronic records is guaranteed by the security of record content and the security of record attributes.

5.3 Application system

Follow GB/T 31913-2015; in the whole life cycle of electronic records, three types of systems are generally experienced, namely business system, electronic records management system, and electronic records long-term preservation system.

The business system is also called the electronic records creation and transaction system, which mainly provides business functions that are involved in the process from creation to transaction for electronic records, and provides the data interface that is connected to other systems. The electronic records management system is responsible for capturing electronic records from the business system, maintaining various associations between records, record and business, supporting inquiry and utilization, and disposing them in an orderly, systematic, and auditable manner. The electronic records long-term preservation system maintains and provides use of electronic records in a correct and long-term effective way.

5.4 Data user

The user is the operator of the application system, including the business operator of the electronic records and the system manager of the application system.

Business operators refer to the personnel who performs specific operations such as creation, modification, authorization, reading, signing, stamping, printing, circulation, archiving and destruction of electronic records in the business system, electronic records management system and electronic records long-term preservation system.

System managers refer to the personnel who manages and maintains the application system, including system manager, audit manager and confidentiality manager.

5.5 Electronic records

The cryptographic operation of electronic records requires the use of symmetric, asymmetric, and hash algorithms. According to the scenario, use GB/T 32918, GB/T 32905, GB/T 32907, or a cryptographic algorithm that is recognized by the national cryptographic management authority.

The symmetric algorithm is used to encrypt and decrypt record content and record attributes. The asymmetric algorithm is used to encrypt and decrypt symmetric keys, and perform digital signatures and signature verification. The hash algorithm is used for integrity calculation and verification. The symmetric algorithm can adopt multiple modes such as CBC, OFB, CFB, CTR. When using OFB and CFB modes, the application system shall set the number of feedback bits.

The call to the cryptographic algorithm is completed through the identifier of the cryptographic algorithm.

5.6.2 Universal cryptography service

Universal cryptography services include digital certificate service, encryption/decryption services, signature/verification services, hash computing service. Universal cryptography services are provided by cryptographic infrastructure such as certificate authentication systems, cryptographic devices/components, and are implemented by calling related service interfaces.

Certificate authentication systems and cryptographic devices/components that provide cryptographic services shall comply with relevant national standards and industry standards, and be certified and approved by the national cryptographic management authority. The cryptographic service interface shall follow GM/T 0019. The digital certificate format shall follow GB/T 20518. The signature syntax shall follow GB/T 35275.

5.6.3 Typical cryptography service

Typical cryptography service includes authentication service, digital stamp service, time stamp service:

- The authentication service is used to realize user authentication that is based on digital certificates;
- The digital stamp service is used to stamp, verify and read the stamp of electronic records. The digital stamp service interface shall follow GM/T 0031;
- The time stamp service is used to provide time information for digital signatures and digital stamps. The time stamp service interface shall follow GM/T 0033.

5.6.4 Key

When the record attributes are maintained by the application system, the application system shall directly perform encryption and decryption of the specified record content. The symmetric key for encryption shall be randomly generated; one cypher for one record shall be ensured; and the application system cannot obtain a clear symmetric key.

The record content encryption method is as follows:

- a) Obtain the symmetric algorithm and asymmetric algorithm identifiers;
- b) Call the universal cryptography service to generate a symmetric key;
- c) Call the symmetric encryption service and use the symmetric key to encrypt the record content;
- d) Call the asymmetric encryption service and use the public key for encryption of the electronic record receiver or the application system to encrypt the symmetric key;
- e) Package the encrypted symmetric key and the record content that is encrypted by the symmetric key in a digital envelope format, to form the encrypted record content; if there are multiple receivers of the electronic records, respectively use public key for encryption of each receiver to encrypt the symmetric key, and package the encrypted symmetric key of all receivers and the record content that is encrypted by the symmetric key in the header of the digital envelope;
- f) Store the algorithm identifier, algorithm mode, and number of feedback bits in the security attribute.

The record content decryption method is as follows:

- a) Obtain the symmetric algorithm and asymmetric algorithm identifiers of encrypted electronic records from the security attribute;
- b) Call the asymmetric decryption service according to the asymmetric algorithm identifier; use the private key for decryption to decrypt the encrypted symmetric key, to obtain the symmetric key;
- c) Call the symmetric decryption service according to the symmetric algorithm identifier; use the symmetric key to decrypt the record content.

6.2.2 Confidentiality of record attribute

According to the needs, use digital envelope to encrypt the metadata attribute, seal attribute, watermark attribute, permission attribute and other attribute

- c) Call the signature verification service according to the signature algorithm identifier; use the public key for signature and digest value to verify the signature value of the record