GM

CRYPTOGRAPHY INDUSTRYSTANDARD

OFTHEPEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L80

File No.: 44632-2014

GM/T0031-2014

Secure electronic seal cryptography technical specification

安全电子签章密码技术规范

Issued on: February 13, 2014 **Implemented on: February 13, 2014**

Issued by: State Cryptography Administration

Table of Contents

Secure electronic seal

cryptography technical specification

1 Scope

This standard specifies data structure and cipher processing procedure of electronic stamp and electronic seal.

This standard applies to the development and use of electronic stamp system.

2 Normative references

The following documents are essential 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.

GM/T 0003 SM3 cryptographic hash algorithm

GM/T 0006 Cryptographic application identification specification

GM/T 0009 SM2 cryptographic algorithm specification

PKCS # 1: RSA Cryptography Standard

3 Terms and definitions

The following terms and definitions apply to this document.

3.1

Electronic stamp

It is a type of data which is signed by makers, including holder information and graphical content; it can be used to sign electronic documents.

3.2

Electronic seal

It is the process of using electronic stamp to sign electronic documents.

4 Symbols and abbreviations

The following abbreviations apply to this document:

BMP: Bitmap

GIF: Graphics Interchange Format

JPG: Joint Photographic Experts Group

OID: Object Identifier

PKI: Public Key Infrastructure

5 Cipher application security mechanism of electronic seal

Electronic seal is a combination of traditional seal and electronic signature technology. By using component technology, PKI technology, image-processing technology and cryptography, digital signature and seal are performed for electronic documents in electronic form according to public key cryptography standard system, so as to ensure the authenticity of document source and the integrity of documents, to prevent unauthorized tampering for the documents, and to ensure the non-repudiation of signature behavior.

To ensure the integrity and the unforgeability of electronic stamp, and the usage for legitimate users, a secure electronic stamp data format needs to be defined. Through digital signature, bind securely stamp image data and seal users and stamp property, in order to form secure electronic stamp. In the process of using stamp, it is also convenient to verify the security of electronic stamp.

In the process of using electronic stamp to perform electronic seal on various documents, electronic seal signer signs the document data through digital signature, so as to achieve the same visual effects as traditional paper document stamping operation; at the same time, use digital signature technology to guarantee the authenticity and integrity of the document data and the non-repudiation of the signer's behavior.

6 Cipher application protocol of electronic seal

6.1 Electronic stamp

6.1.1 Data format

```
SES_SignInfo:: = SEQUENCE{
    cert                    OCTET STRING,          -- Signature certificate of electronic stamp maker
    signatureAlgorithm      OBJECT IDENTIFIER,     -- Signature algorithm identifier
    signData                BIT STRING             -- Signature-value of electronic stamp maker

}
```

cert: It represents the certificate of electronic stamp maker who signs the electronic stamp data;

signatureAlgorithm: It represents the signature algorithm OID identifier and follows GM/T 0006. For example, the OID of using SM2 to sign is 1.2.156.10197.1.501;

signData: It represents the digital signature of information content which is composed of the seal information SES_SealInfo, the certificate of electronic stamp maker, signature algorithm identifier in electronic stamp format by electronic stamp maker in the form of SEQUENCE.

If signature algorithm uses SM2, follow GM/T 0009; if signature algorithm uses RSA, follow PKCS # 1.

6.1.2 Verification process of electronic stamp

Verification process of electronic stamp is as follows:

a) Verify the compliance of electronic stamp data format:

In accordance with electronic stamp format, analyze electronic stamp to verify whether it is in line with normative electronic stamp format;

If electronic stamp data format is not compliant, the verification fails; return the reason for the failure and exit the verification process.

b) Verify whether the signature-value of electronic stamp is correct:

According to stamp information data, certificate of electronic stamp maker and signature algorithm identifier, verify whether the signature-value of electronic stamp signature information is correct;

If the signature verification of electronic stamp fails, return the reason for the failure and exit the verification process.

c) Verify the validity of electronic stamp maker's certificate:

Analyze electronic seal data according to electronic seal format specification. If the data format of electronic seal or electronic stamp is not compliant, the verification fails, exit the verification process.

b) Verify whether electronic seal signature-value is correct:

Obtain the data to be verified from electronic seal data format; the data to be verified includes: version number, electronic stamp, time information, original hash-value, original property information, electronic seal signer's certificate, signature algorithm identifier; verify whether electronic seal signature-value is correct.

If the signature-value verification is incorrect, the verification fails; return the failure reason to the upper application and exit the verification process.

c) Verify the validation of digital certificate of electronic seal signer:

Obtain the digital certificate of electronic seal signer from electronic seal data and verify the validity of the signer's certificate; the verification-items include at least: the verification of certificate trust-chain, the verification of certificate validity-period, whether the certificate is revoked, and whether the key usage is correct.

If the verification of certificate trust-chain or incorrect key usage leads to the failure of the validity verification of electronic seal signer's certificate, return the reason for the failure and exit the verification process.

If certificate validity-period or revoked status of certificate leads to the failure of the validity verification of electronic seal signer's certificate, it is necessary to make further comprehensive determination combining with signature time.

d) Verify the validity of signature time:

Through comparing the validity-period of digital certificate of electronic seal signer with the time information of electronic seal, determine the validity of signature time:

1) If the signature time is within the validity-period of the signer's digital certificate, and the certificate is valid, further verification is required.

2) If the signature time is not within the validity-period of the signer's digital certificate, the signature is invalid, the verification fails; return the reason for the failure and exit the verification process.

3) If the signature time is within the validity-period of the signer's digital certificate, but the certificate has been revoked before the seal is signed,

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------