GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

GB/T 25064-2010

Information security technology - Public key infrastructure - Electronic signature formats specification

信息安全技术 公钥基础设施 电子签名格式规范

Issued on: September 02, 2010 **Implemented on: February 01, 2011**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine of the PRC;

Standardization Administration of the PRC.

Table of Contents

Foreword 3

Introduction 4

1 Scope 5

2 Normative references 5

3 Terms and definitions 6

4 Abbreviations 6

5 Composition of electronic signature 7

5.1 Main parties to electronic signature 7

5.2 Types of electronic signature 8

5.3 Validation of electronic signature 15

6 Data formats of electronic signature 20

6.1 Basic data formats 20

6.2 Validation data formats 28

6.3 Signature policy requirements 34

Appendix A (Normative) Abstract Syntax Notation One (ASN.1) representation of electronic signature formats 47

Appendix B (Normative) Abstract Syntax Notation One (ASN.1) representation of signature policy 55

Bibliography 61

Information security technology - Public key infrastructure - Electronic signature formats specification

1 Scope

This Standard, for the electronic signature of digital signature type generated based on public key cryptography, defines the main parties to electronic signature and validation, the types of electronic signature, validation and arbitration requirements. This Standard also standardizes the data formats of electronic signature, including basic data formats, validation data formats, and signature policy formats, etc.

This Standard applies to the design and implementation of electronic signature products. The testing, evaluation, and purchase of related products can also refer to it.

2 Normative references

The following documents contain provisions which, through reference in this Standard, constitute provisions of this Standard. For the dated references, their subsequent amendments (excluding corrections) or revisions do not apply to this Standard. However, the parties who enter into agreement based on this Standard are encouraged to investigate whether the latest editions of these documents are applicable. For undated reference documents, the latest editions apply to this Standard.

GB/T 16264.8-2005 Information technology - Open systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks (ISO/IEC 9594-8:2001, IDT)

GB/T 16262.1-2006 Information technology - Abstract Syntax Notation One (ASN.1) - Part 1: Specification of basic notation (ISO/IEC 8824-1:2002, IDT)

GB/T 19713-2005 Information technology - Security techniques - Public key infrastructure - Online certificate status protocol

GB/T 20518-2006 Information security technology - Public key infrastructure - Digital certificate format

certificate revocation lists, online certificate queries, etc. The following lists some of the main TSPs:

1) Certification authority (CA), which provides users with a public key certificate;

2) Registration authority (RA), which authenticates and registers the user before the CA issues the certificate to the user;

3) Time stamp authority (TSA), which proves that data is generated before a certain time;

d) Arbitrator. An arbitrator is an entity which makes a ruling when there is a dispute between the signer and the verifier.

5.2 Types of electronic signature

5.2.1 Basis electronic signature (BES)

The basis electronic signature (BES) refers to the electronic signature including the basic data information of signature. The basic data information mainly includes the following 3 items:

a) Signature policy. The signature policy defines the technological and procedural requirements in the process of electronic signature generation and validation, to meet the needs of a particular situation. Parties to electronic signature shall identify the policy and meet the requirements of the policy.

b) Digital signature. The digital signature is a digital signature by the signer on the comprehensive data of the following information. The information mainly includes: hash value of the signed data; signature policy identifier; and other signature attributes.

c) Other signature attributes provided by the signer. Other signature attributes are other attribute information which the signer provides to meet the signature policy requirements or standard requirements.

The basic composition structure of BES is shown in Figure 1:

c) ES with complete validation data (ES-C). Such electronic signatures, based on ES-T, add a complete set of data for verifying electronic signatures, such as certificate revocation reference information, etc. But it may include some reference information, such as a URL, that requires the verifier to go to the URL to get specific data.

d) ES with extended validation data (ES-X). Such electronic signatures, based on ES-C, add some additional data, to accommodate some special cases.

e) ES with archive timestamp (ES-A). Such electronic signatures are formed on the basis of the above various electronic signatures, mainly for storing electronic signatures for long-term archiving, so time stamps are added to the entire electronic signature, to ensure long-term security.

The signer, when submitting an electronic signature, shall at least give a signature in BES format. In some cases, it can be decided whether or not to provide an electronic signature in ES-T format. In some extreme cases, an electronic signature in ES-C format can be provided. If the signer does not provide an ES-T, the verifier can, when it receives the electronic signature, immediately create an ES-T on its own, or keep a secure record of the time receiving the signature. Both of the verifier's methods provide an independent evidence of validation time. The validation time shall actually be close to the creation time of electronic signature, so that it can have sufficient evidence to prevent denial of the signature. If the signer does not provide ES-C, the verifier can, on the basis of BES, create an ES-C on its own, provided that it can obtain the appropriate validation data. In addition to these three, ES-X and ES-A are optional supported formats.

5.2.3.2 ES with timestamp (ES-T)

The time recorded by the time stamp in the ES-T shall be as close as possible to the actual creation time of the BES, to provide maximum security protection.

If the signer does not provide an ES-T, the verifier can, when it receives the electronic signature, immediately create an ES-T on its own.

The basic composition structure of ES-T is shown in Figure 2:

c) The various cryptographic technologies used in the creation of ES-C, during arbitration, are still secure.

If condition a) is not met, the prosecution needs to provide an ES-X0 electronic signature.

If condition b) is not met, the prosecution needs to provide an ES-X1 or ES-X2 electronic signature.

If condition c) is not met, the prosecution needs to provide an ES-A electronic signature.

6 Data formats of electronic signature

6.1 Basic data formats

The data format and syntactic structure in this Standard are described by ASN.1 as specified in GB/T 16262.1-2006. The definition of data format in this subclause is based on the cryptographic message syntax (CMS) defined in RFC2630 and the enhanced security services (ESS) defined in RFC2634. For the syntactic structures already defined in RFC2630 and RFC2634, this Standard refers directly and no longer gives a specific definition.

6.1.1 Overall syntactic structure

The overall syntactic structure of an electronic signature is defined in RFC2630.

6.1.2 Data content type

The syntactic structure and requirements for data content types in electronic signature are given in RFC2630.

6.1.3 Signed data content type

The syntactic structure and requirements for signed data content types in electronic signature are given in RFC2630.

In order to ensure that the signature verifier can correctly use the signer's public key for validation, this Standard specifies that the signed attribute shall contain the hash value of the signer's signing certificate. The definition of the signed attribute is given in RFC2634.

6.1.4 Signed data type

The syntactic structure and requirements of signed data type in the electronic signature, in addition to complying with the requirements of RFC2630, shall meet the following 3 points:

a) Content-type attribute. Its syntactic structure is defined in RFC2630;

b) Message-digest attribute. Its syntactic structure is defined in RFC2630;

c) Signing-time attribute. Its syntactic structure is defined in RFC2630. The time value in this attribute shall be the time the signer claims to have completed the signature process. The recommended time format in this Standard is the Generalized Time type.

6.1.8 Alternative signed attributes

6.1.8.1 Selection criteria of signed attribute

An electronic signature conforming to this Standard shall, in the signed data, include one of the following two optional signed attributes and contain only one. The basis for the selection is that: When the hash function used is SHA-1, the ESS signed attribute is used; when using other hash functions, other signed attributes are used.

6.1.8.2 ESS signed attribute

The syntactic structure definitions and requirements for ESS signed attribute are given in RFC2634. The meaning and usage of each field, in addition to those specified in RFC2634, must meet the following points:

a) The ESS signed attribute must be a signed attribute and cannot be empty. The identifier of the certificate used to verify the signature must be included in this attribute.

b) The coding of the ESSCertID field in the ESS signed attribute corresponding to the certificate used to verify the signature shall contain the issureSerial field. The contents of the issureSerial field shall match the contents of the issuerAndSerialNumber field in SignerInfo. In the signature validation process, it shall check whether the hash value of the validation certificate used is consistent with the corresponding content in the above fields. If not, the signature shall be deemed invalid.

6.1.8.3 Other signed attributes

The structure of this attribute is the same as that of ESS signed attribute. But this attribute can be used if the hash function is not SHA-1. The requirements for the use of ESS signed attribute also apply to this attribute.

The object identifier (OID) of this attribute is as follows:

id-aa-ets-otherSigCert OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs9(9)smime(16) id-aa(2) 19 }

to the value of electronic signature. The complete validation data contains the time stamp of signature value, all certificates and revocation information for complete validation of electronic signature.

This subclause also specifies extended formats of validation data. The time stamp contains the time stamp of the ES-C. The extended time stamp contains time stamps which validation path references and revocation information references to support ES-C. The extended long validation data contains the complete validation data and the actual values of all certificates and revocation information used in the ES-C. The extended timestamp long validation data contains a time stamp or extended time stamp, and the actual values of all certificates and revocation information used in the ES-C.

This subclause also specifies the data formats of archive validation data. Archive validation data includes complete validation data, certificate and revocation information, extended timestamp, signature user data, and archive timestamps for all of this data. The archive timestamp can be re-applied after a long period of time, to maintain validity when the electronic signature and timestamp algorithms are weakened.

All data defined under this subclause is an unsigned type.

6.2.2 Electronic signature time stamp

An electronic signature can, from different time stamp authorities, obtain multiple electronic signature time stamp instances. The following object identifier identifies the signature time stamp attribute:

```
id-aa-signatureTimeStampToken OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 14}
```

The ASN.1 syntax of signature time stamp attribute value is:

```
SignatureTimeStampToken ::= TimeStampToken
```

The value of the messageImprint field in the TimeStampToken shall be the hash value of the signature field value in SignerInfo used to time-stamp the signedData.

6.2.3 Complete validation data

6.2.3.1 Complete validation data content

Complete validation data shall include at least signature time stamp attribute, complete certificate reference, and complete revocation reference.

6.2.3.2 Complete certificate reference attribute

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

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