GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 20520-2006

Information security technology - Public key infrastructure - Time stamp specification

信息安全技术 公钥基础设施

时间戳规范

Issued on: August 30, 2006 **Implemented on: February 01, 2007**

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

Standardization Administration of the People's Republic of China.

Table of Contents

Information security technology - Public key infrastructure - Time stamp specification

1 Scope

This Standard specifies the requirements for time stamp system component composition, time stamp management, time stamp format, and time stamp system security management.

This Standard is applicable to the design and implementation of time stamp systems. The testing of time stamp system and product procurement can also be used as reference.

2 Normative references

The provisions in following documents become the provisions of this Standard through reference in this Standard. For dated references, the subsequent amendments (excluding corrigendum) or revisions do not apply to this Standard, however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest edition of the referenced document applies.

GB 17859-1999, *Classified criteria for security protection of computer information system*

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

GB/T 20273-2006, *Information security technology - Security techniques requirement for database management system*

GB/T 20271-2006, *Information security technology - Common security techniques requirement for information system*

RFC 2630, *Cryptographic Message Syntax*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

6 Generation and issuance of time stamp

6.1 Application and issuance method

The TSA can receive time stamp requests and issue time stamp in different ways. But at least one of the following four ways shall be supported:

a) Application by email. The user sends a time stamp request to the email address specified by TSA. The TSA also returns the time stamp issued to the user via email. The MIME objects used for application and issuance are described in clause 8.

b) Application by file transfer. The user stores the code of the application message in a file. After the file is transferred to the TSA, the TSA also saves the generated time stamp in a file and sends it to the user. File transfer can use any trusted method, such as using the FTP protocol.

c) Application through Socket. The TSA listens for request from user on a port on the computer. After the user establishes a secure socket connection with this port of the TSA computer, the user sends an application message to TSA. Finally, TSA also sends the generated time stamp to the user on this connection.

d) Apply via HTTP. After the user connects to the TSA application page, the application message is generated by using the webpage. The application message is then sent to TSA via the HTTP protocol. The TSA then sends back the time stamp via the HTTP protocol.

6.2 Generation method for trusted time

The original source of trusted time shall come from the national authoritative time department (such as the National Time Service Center). Or the time obtained by using hardware and methods approved by the national authoritative time department.

Use one or more of the following methods to obtain time.

a) Use some kind of wireless receiving device to obtain the time release of the national authoritative time department by wireless means, such as long wave signal, satellite signal, etc.

b) Obtain time from a specified network address by using some sort of time synchronization protocol. The time of the network address release and the time synchronization protocol used shall be credible and approved by the national authority time department.

synchronization. Alerts the administrator and writes to the audit log.

6.4 Application and issuance process

Regardless of which method is used in the TSA operation, the entire application and time stamping process shall at least include the following basic processes.

a) The user submits an application request to TSA through one of the methods described in 6.1. The format of the request message shall conform to the provisions of clause 8.

b) After receiving the application request, the TSA's signature system checks the validity of the request message according to the description of the time stamp format in clause 8.

c) If the request message is not valid or the TSA cannot issue this time stamp for some internal reason, the TSA shall generate a time stamp failure response. The format shall also follow the provisions of clause 8. The TSA shall fill in the reason the application is rejected in detail.

d) If the request message is valid and the system is functioning properly, the TSA signature system shall fill in the normal time stamp and sign it according to the time stamp format described in clause 8.

e) The TSA signature system sends the newly generated time stamp to the time stamp database through the trusted channel. Save it by the time stamp database. The time stamp failure response due to the rejection of the application shall be determined by the TSA's own policy to save it. This standard does not make mandatory provisions.

f) The TSA adopts the method of issuance corresponding to the user application method. Send the newly generated time stamp to the user.

g) After receiving the time stamp, the user shall use the TSA certificate to verify the validity of the time stamp. And check the time stamp content for errors. If the time stamp is illegal or has an error, the user shall immediately report the exception to the TSA manager. TSA agency shall provide a user feedback channel. Notify administrator via this channel when users find anomalies. If the time stamp is normal, the user can save this time stamp for later use.

h) If the administrator receives an exception report from the user, he shall immediately check the audit log and time stamp database to find out the cause of the error. The TSA shall prepare a complete processing plan for this situation.

d) The backup data shall be stored in a convenient way.

e) The access to backup data shall be done when an administrator is present.

f) The backup data does not necessarily need to be encrypted or signed. However, if used, the selected algorithm shall comply with the relevant regulations of the national cryptography management department.

7.3 Time stamp retrieval

The TSA shall provide the user with an environment that can easily retrieve time stamps so that users can retrieve and obtain time stamps via the network or face to face.

The time stamp that the TSA provides to the user for retrieval shall be more than just the time stamp stored in the time stamp database. It shall also include the time stamp of the previous backup.

The TSA shall at least support retrieval of time stamps through the following three types of information.

a) Retrieve according to the time of time stamp storage. Allow multiple results to be retrieved. Then allow user to select by himself.

b) Retrieve based on the serial number of the time stamp. Since the serial number is unique, such retrieval shall have only one result.

c) Retrieve according to the complete encoding of time stamp. Such retrieval shall also have only one result.

The retrieval result of the time stamp can be sent to the user through the 6.1 issuance method. It can also let the user take it back by another reliable method, such as using an IC card, CD, etc.

7.4 Time stamp deletion and destruction

7.4.1 Deletion of time stamp

When the TSA system generates an incorrect time stamp due to an internal error or an external attack, it shall be allowed to delete the erroneous data in the time stamp database.

All time stamps deleted from the time stamp database shall be backed up for later auditing. This backup data shall be distinguished from normal backup data and stored separately. But also need to meet the requirements for backup in 7.2.

All deleted time stamps shall be published in the public channel at the first time,

8 Time stamp format

8.1 Requirements for TSA

To complete a complete time stamp, the TSA system shall meet the following conditions.

a) Have a reliable time source that shall meet the requirements of 9.2.2. The generation of trusted time must meet the requirements of 6.2.

b) Include a trusted time value in each time stamp.

c) Include a one-time random integer (nonce field) in each newly generated time stamp.

d) Whenever possible, when a legitimate request is received from a requester, a time stamp is generated based on the request.

e) When the time stamp is generated, include a unique identifier within it. This identifier indicates the security policy when the time stamp is generated.

f) Only stamp the time stamp on the hash value of the data. The hash function has a unique object identifier (OID).

g) To be able to check the identifier of a one-way hash function. And verify that the hash length of the data matches the result length of the hash function.

h) Except for the check of the length of the hash value required in g), no other checks are performed on the entered hash value data.

i) Do not contain any requestor's identity within the time stamp.

j) Sign the time stamp with a special key. This purpose of the key shall be stated in the certificate corresponding to the key.

k) If the requester makes some additional requirements in the extension field of the application message and the TSA supports these extensions, the TSA shall include the corresponding additional information in the time stamp. Conversely, if the TSA does not support these extensions, it shall return an error message.

8.2 Key identification

The TSA shall have a special key to sign the time stamp message. But a TSA can have many different private keys to suit different requirements, for example,

local clock. nonce is a large random number and is not repeated with a very high probability (for example: a 64-bit integer). In this case, the nonce shall be included in the response message, otherwise the response message shall be rejected.

e) If there is a certReq field in the request message and is set as true, the TSA shall give its public key certificate in its response message. The certificate is indicated by the ESSCertID of the SigningCertificate attribute in the response message, and the certificate itself is stored in the Certificates field of the SighedData [Translator note: should be SignedData] structure in the response message. This domain can also contain other certificates. If the certReq field is not given in the request message or the certReq field is set to false, the above certificate is not necessary in the response message.

f) The extensions field is a way to add additional information to the application message in the future. Extensions are defined in GB/T 20518-2006. For an extension, whether or not it is a critical extension, as long as it appears in the request message and cannot be recognized by the TSA, the TSA shall not generate a time slice and return a failure message (unacceptedExtension).

The time stamp request message does not need to give the identity of the requester because the TSA does not verify this information (see 8.1). If in some cases the TSA needs to verify the identity of the requesting party, then two-way authentication shall be performed.

8.4.2 Response message format

After receiving the application message, the TSA sends a response message to the requester whether the application succeeds or fails. The response message is either the correct time stamp or a time stamp containing the failure information. The specific format of the time stamp response message is as follows:

```
TimeStampResp ::= SEQUENCE  {
        status                  PKIStatusInfo,
        timeStampToken          TimeStampToken          OPTIONAL  }
```

The status of the response message is defined as follows:

```
PKIStatusInfo ::= SEQUENCE {
        status          PKIStatus,
        statusString    PKIFreeText     OPTIONAL,
```

- The validity of the time stamp log so that it can be verified later that the time stamp is authentic.

c) messageImprint shall have the same value as a similar field in TimeStampReq. The premise is that the length of the hash value is the same as the expected length of the hashAlgorithm tag algorithm.

d) The serialNumber field is an integer assigned by the TSA to each time stamp. It shall be unique for each time stamp issued by a given TSA (i.e., the TSA name and serial number can identify a time stamp flag). It shall be noted that this feature shall be retained even after experiencing a possible service interruption (such as a crash).

e) genTime is the time when the TSA creates a time stamp. It is expressed in UTC time to reduce confusion caused by the use of local time zone usage. The specific format of time shall comply with the provisions of 8.3.

f) accuracy represents the maximum error that may occur in time. genTime plus the value of accuracy, the time limit for TSA can be obtained to create this time stamp. Similarly, subtracting the value of accuracy is the lower time limit for TSA to create a time stamp. The specific definition is as follows:

```
Accuracy ::= SEQUENCE {
    seconds     INTEGER                OPTIONAL,--s
    millis      INTEGER (1..999)       OPTIONAL,--ms
    micros      [1] INTEGER (1..999)   OPTIONAL--μs }
```

If seconds, millis, or micros do not appear, the values of these fields that do not appear shall be assigned as 0.

When the accuracy option does not appear, the accuracy can be obtained from other sources, such as TSAPolicyId.

g) ordering indicates time stamp sorting conditions. If the ordering field does not appear, or the ordering field appears but is set as false, then the genTime field only indicates the time when the TSA creates the time stamp. In this case, the difference between the genTime of the first of the two time stamps and the genTime of the second is greater than the sum of the precisions of the two genTime, time stamp flags issued by the same TSA or different TSAs are possible to sort. If the ordering field appears and is set as true, each time stamp sent by the same TSA can be sorted according to genTime, regardless of genTime accuracy.

h) If the nonce field appears in TimeStampReq, it shall also appear here, and the value shall be equal to the value in TimeStampReq.

9 Security of time stamp system

9.1 Physical security

The physical security requirements of the time stamp system shall comply with the relevant requirements of 4.1 of GB/T 20271-2006. Secure the environment, equipment and recording media.

9.2 Software security

9.2.1 Operating environment

The computer environment in which all components of the TSA operate, i.e. the computer information system, shall have a security level that meets or exceeds the requirements of the second level of "system audit protection level" specified in GB 17859-1999.

All components of the TSA shall have a complete anti-virus, firewall solution. Programs and services not related to TSA operation shall not be running in the system. Personnel who can operate TSA component computers shall be strictly controlled. The password for accessing the TSA component computer shall also be strictly controlled to ensure that only authorized personnel know.

9.2.2 Trusted time source

The time source of the TSA shall be the national standard time. It is either the time published by the national authority time department or the time obtained by the hardware and method approved by the national authoritative time department.

Regardless of the method used to obtain the trusted time, strict measures shall be taken to ensure the integrity of the time information from the time source of the trusted time source to the signature system to ensure that it has not been tampered with by anyone. Even if someone invades the time information in the middle, the signature system shall have the ability to discover that the time information has been modified. Alert to TSA managers at the same time.

Software used to receive time from a time source shall also check the continuity and integrity of time to ensure that it is true and effective.

9.2.3 Signature system

All use of the key by the signature system shall be performed in accordance with the relevant regulations of the National Cryptographic Authority.

The access to the signature system shall have strict access control, including

Input, deletion and storage of trusted public key	All changes to the trusted public key (e.g. addition, deletion)	Including public key and information related to the public key
Private key and symmetric key output	Output of private and symmetric keys (including one-time session keys)	
Time stamp application	All time stamp request requests	If the application is successful, save the application request and a copy of the generated time stamp in the log; If the application fails, save the reason for the failure and the generated time stamp failure response in the log
Component configuration	All security related configurations	
Trusted time acquisition and synchronization	Synchronization time based on trusted time source	Including that if the trusted time and local time do not match, change the local time according to the trusted time, and all errors that occur during the synchronization process

For each event in Table 1, the audit record shall include: the date and time of the event, the user, the type of event, whether the event is successful, and what is required in the additional information column of the table.

Private keys, asymmetric keys, and other security-related parameters in clear text must not appear in the log record.

The audit feature component shall be able to associate an auditable event with the identity of the system user who initiates the event.

9.2.5.2 Audit review

The audit feature component shall provide the auditor with the ability to view all information about the log.

The audit feature component shall provide the log information to the reader in a manner suitable for reading and interpretation.

9.2.5.3 Audit event storage

Audit feature component shall have the following capabilities.

a) The protected audit trail storage requires audit trail storage to be protected

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

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