

ICS 35.040

CCS L 80



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

GB/T 20520-2006

**Information security technology - Public key infrastructure -
Time stamp specification
(English Translation)**

Issued on: August 30, 2006

Implemented on: February 1, 2007

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

Table of Contents

Foreword...	3
Introduction...	4
1 Scope...	5
2 Normative references...	5
3 Terms and definitions...	5
4 Abbreviation...	6
5 Composition of time stamp system...	7
6 Generation and issuance of time stamp...	8
6.1 Application and issuance method...	8
6.2 Generation method for trusted time...	8
6.3 Time synchronization...	9
6.4 Application and issuance process...	10
7 Time stamp management...	11
7.1 Storage of time stamp...	11
7.2 Time stamp backup...	11
7.3 Time stamp retrieval...	12
7.4 Time stamp deletion and destruction...	12
7.5 Check and verification of time stamp...	13
8 Time stamp format...	14
8.1 Requirements for TSA...	14
8.2 Key identification...	14
8.3 Representation format of time...	15
8.4 Time stamp application and response message format...	16
8.5 Document storage...	21
8.6 MIME object definition used...	21
8.7 Security considerations for time stamp format...	22
9 Security of time stamp system...	23
9.1 Physical security...	23
9.2 Software security...	23
Bibliography...	27

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.

6.1 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.