Time Authentication Infrastructure Guideline

(Digest Edition)

September 2003

Time Business Forum

Foreword

In our modern clock-ruled culture, it is not too much to say that no society can exist unless based on “time”. Computers, which are the key device of an information society, are equipped with high precision clocks to synchronize their entire circuit function. In an electronic environment or digital society built on computers, recordkeeping relates inevitably to the time that is ticked away by the clocks embedded in the computers.

Time is thus the infrastructure of this information society. However, the importance of securing evidential authority of electronically determined time, and synchronizing clocks of multiple computers working in cooperation are not recognized enough.

To save the situation, a notion of time for the digital society should be properly defined and popularized, specifying the way and conditions of using it safely. Time Business Forum was established to diffuse the time notion for the digital society. As part of Technology Committee of the Forum, the Guideline Subcommittee is responsible for presenting a guideline on this issue to users and providers.

The scope of discussion here focuses on some specific industries and applications for time-stamping technologies. Also, emphasis is put on releasing this guideline as quickly as possible to the public. We focused mainly on time-stamp use by national and local governments to produce a general guideline for both users and providers. The guideline will be further refined step by step as their validity is verified in actual use. Meanwhile, we are planning to work on guidelines for standard time distribution, which is as important as time-stamp to time business.

We hope that our effort to prepare the guideline for time-stamp use, application and provision will expand introduction of time-related technology and enhance relevant regulatory reforms, and contribute to building reliable infrastructure of electronic society through establishing such time businesses as standard time distribution and time authentication.

March 2003

Time Business Forum

CONTENTS

Chapter 1. Outline

1.1 Background and Objective

(1) Importance of Digital Trace of Time

In transactions, applications, personal promises or whatever we experience daily, notion of time is of the essence, whether or not we are aware of it. And physicochemically or socially obtained trace of time is recorded on paper. In other words, we are recording analog trace of time in terms of media, methods and forms.

Recent progress of information technology has rapidly promoted document digitization. Unfortunately, digital data or documents, unlike paper documents, are essentially impossible to distinguish a copy from the original. This raises problems such as securing originality and preventing alteration of information. Securing authenticity of trace of time is also one of the biggest problems.

To activities in the society, completing digital data in an electronic environment means that digital trace of time independent of any medium must be realized. This means that trace of time must be a piece of digital data that is digitally documented. Technical methods for this have been proposed and applied to practical tools, with some of them introduced into actual operation. However, the electronic trace of time has not yet obtained a high standing as the traditional one, which is supported by the time-honored custom and rules rooted deeply and widely in the society.

(2) Objective of the Guideline

To become widely approved in society, the time notion for an electronic environment needs to win public awareness, trust and daily opportunity as well as technical support. Given that the modern world is based on “time”, an electronic/digital world can be based on an integral structure that authorizes “digital trace of time”. We call the whole such structure as “time authentication infrastructure”, establishment of which is the objective of this guideline.

Through describing the feature, importance and effects of time-stamp as a trace of time given to digital documents/data stored for future use, we will provide users with a time-stamp user guideline and providers with time-stamp offer guideline. Consequently, time-stamp users will know business application standards for appropriate time, documents/data and trace of time, while providers will be suggested service quality standards such as type and reliability of time-stamp they offer.

1.2 Policies of Guideline Study

We studied the guideline, keeping the following in mind.

(a) Placing importance on time-stamp use and application

As a group of “time” specialists, we particularly tried to ensure the security aspect of our guideline for users' trust. Technical studies of time-stamp have been actively carried out by many domestic and foreign organizations concerned. However, like other technologies, time-stamp needs clear definition of its use and application in order to be fully utilized. Therefore, we took up a use-and-application point of view instead of the technology itself, so that our guideline could be helpful to both users and providers.

(b) Placing importance on practical use

Time-stamp technology standardization is being pushed forward by IETF and ISO/IEC. And as for digital documents (digital documents), time-stamping policy is defined in XML, the key standards for digital document exchange. At present, these standards are open to further improvement, as they are inadequately applied to practical tools or too specialized in certain types of business. While primarily based on domestic and international technical standards now existing, we designed this guideline to be practical taking into consideration the state of tools and services currently offered.

(c) Being neutral

Time-stamping system types will be discussed along with relevant systems whose standard requisites to fulfill are clarified. As detailed in later discussion, there are several types of time-stamping systems. It is difficult at this moment to select one from those with different characteristics. This guideline for users, therefore, focuses on the conditions necessary for using time-stamp service, not depending on or emphasizing any specific system. Similarly, this guideline for providers is designed exclusively to identify appropriate service operation, carefully avoiding inclination to any specific business type.

(d) Versatility and generality

Most technologies are developed for general uses, and introduced to practical use by defining the purpose and range of their application. This guideline defines individual business application purpose and range of the time-stamping technology. However, the more precise the definition is, the more exclusive the guideline may become, leaving out many businesses as irrelevant. On the other hand, if extremely generalized, the guideline may not be more helpful than a technical explanatory. We carefully made our guideline balanced between the individualization and generalization of the technology use.

(e) Start from electronic government services

Among many government services in which time-stamp may be effective, we selected e-application and e-tender to deal with in our guideline. Both have a pressing need of time-stamp introduction, as these new services will be instituted on a full scale under the e-Japan project. With workflows different from each other, the two services will be dealt with separately when pairing user's guideline and provider's guideline.

1.3 Guideline Composition

This guideline is composed mainly of three parts: Explanatory in Chap. 2-4, User Guideline in Chap. 5, and Provider Guideline in Chap. 6.

(1) Explanatory

In the explanatory part, problems peculiar to digital documents, time-stamp as a solution to the problems, and time authentication infrastructure to realize time-stamping system will be explained, thus clarifying the importance and effects of time-stamp introduction, which is one of the guideline's purposes.

In Chapter 2, "Digital Information Problems", the reason for time authentication's importance will be discussed. Digital documents are essentially impossible to be distinguished between originals and copies. This provides opportunities for alteration, spoofing and other document authenticity problems, causing troubles such as contract rupture by repudiation. Digital signature system is not perfect in terms of proving the existence, integrity and sequentiality of digital documents.

The technology to solve these problems is time-stamp, whose importance, requirements, and technological types and trends will be also described in the explanatory part for better understanding of the guideline parts.

In Chapter 4, named "Mechanism of Time Authentication Infrastructure", the importance of time authentication will be stressed, referring to structure and reliability of the system. Time authentication business players and their roles, flow of time-stamp issuance and verification, and time traceability will be also discussed in the chapter.

(2) User Guideline

This is a time-stamping guideline for client service providers and local public service authorities. The guideline will be specified on tender service and application service to be provided under the electronic government ("e-government"). General guideline shared among various services will be left out here except for its basic idea and framework.

The guideline will clarify the workflow first, and then, based on it, identify the documents and timing that need time-stamping. It will also clarify the reason or purpose of time-stamp

use, in order to help users decide what they need for their time-stamping system. As time-stamp requirements differ by service type, requirements for the period of validity, time precision, and verification will be defined for each service type.

The guideline will cover handling and verifying acquired time-stamps, as time-stamp acquisition may not necessarily guarantee the authenticity of digital documents.

(3) Provider Guideline

This is a guideline for time-stamp-related service providers. It will define technical and operational standards of different service types: standard time distribution, time-stamp issuance, and time-stamp verification. It will also include the standards of facility, network and server, which are common to the three service types. Time-stamp issuance is roughly divided into two systems distinct from each other: Simple Protocol and Linking Protocol. Each service type will be described based on the two systems.

1.4 Instructions for Guideline Use [Deleted]

Chapter 2. Digital Information Problems

Importance of digital information in the advanced network society is steadily growing. Information network infrastructure that guarantees security of transaction is vital to the growing opportunity of e-commerce. Secrecy of channel, authentication of document correspondent, and authenticity of exchanged documents are indispensable to security of transaction. Especially, securing digital documents' authenticity is a serious agenda, as they are distributed easily and rapidly, and copied without difficulty.

2.1 Possible Threats

The following threats are possible in digital information distribution:

① Spoofing

This means an act done by some ill-intentioned person in the disguise of the right person. On e-commerce network, one may incur damage from some unknown transaction unless personal identification is strictly conducted. This can be avoided by digital signature that secures personal authenticity.

② Alteration

Some ill-intentioned person may alter important information in a digital document. If the alteration is easy to make but hard to detect, one may incur damage from false information in, for instance, an electronic application form. Alteration can be detected through securing document authenticity with digital signature.

③ Repudiation

This means that someone denies or contradicts the fact of having done something. This can be a denial of the fact of having received or submitted an electronic application form, or a contradiction of the fact of having signed a contract. It is likely that these will happen frequently in network activities unless evidence of certain facts is recorded. Repudiation can be avoided by digital signature that secures personal authenticity.

2.2 Digital Signature Technology

(1) Authenticity of Digital document

In traditional paper society, a document is regarded to be "an authentically produced document" or "an authentic document"[1] when it has been produced truly by the one

[1] Takahito Natsui: *The Digital Signature Law*. Ric Telecom.

presenting him/herself as the author. In addition, a document with the professed author's seal allows a presumption of the contents' authenticity. Enforced in 2001, the Digital Signature Law (the Law concerning Digital Signature and Certification Services) gave digital documents (electromagnetic records) the effect of presumptive authenticity of private documents, which is provided in 228-4 of the Civil Proceedings Act. Since then, digital document authenticity can be legally recognized if signed with a key secured under a Public Key Certificate, which is issued from a well-trusted Certification Authority based on the Public Key technology (or PKI: Public Key Infrastructure). The Digital Signature Law also defines the service requirements for trusted Certification Authorities.

(2) Digital Signature Technology

Digital signature is a technology to secure authenticity of digital document author and contents. PKI enables identification of a digital document's signer, producer, and risk of having been altered, by using Public Key Certificate information issued by a trusted Certification Authority.

Figure 2-1 outlines PKI-based digital signature system. In traditional paper society, authenticity of a sealed document is verified by identifying the imprint of a registered seal, which can be generated only by its genuine owner. An interested party in a transaction examines the identity of the other's seal imprint on the document with that on a registered seal certificate issued from a municipal office. In PKI-based digital signature system, in contrast, a trusted Certification Authority issues a public key certificate to the key pair (public key and private key) after implementing a strict personal verification of its owner. An interested party in a transaction uses the private key of its exclusive possession when generating its digital signature, and can view digital document contents only by using the public key that matches the private key.

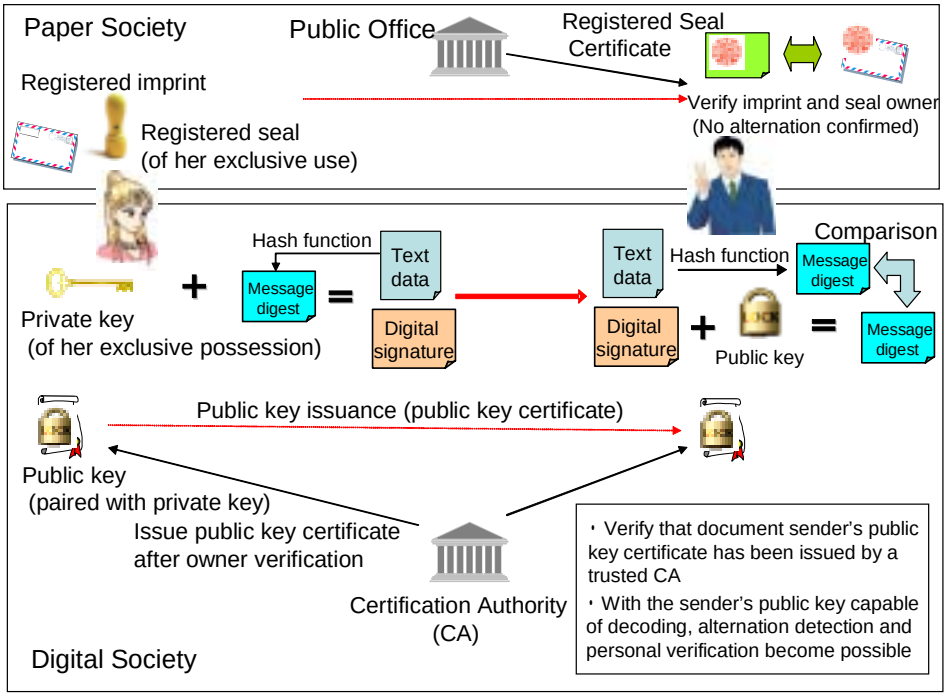


Figure 2-1 PKI Structure

In the digital signature system to secure digital document authenticity, a digital document producer degenerates the document to a message digest by hash function, and encodes it with the private key unique to him/her. The recipient of a digitally signed document acquires both the document producer's public key certificate and Certification Authority's public key certificate in order to verify that the certificate has been validly issued by a trusted CA. Then, using the producer's public key, the recipient verifies authenticity of the received electrically signed document. Damage from transmission to or alteration of the one-directional message digest can be detected during the digital signature verification.

(3) Limitations of Digital Signature

Digital signature has been adopted by national and local e-government infrastructure as a technology to verify authenticity of documents, which is essential for Internet uses such as electronic application. However, documents with digital signature based on PKI have the following limitations.

- With an absence of time-related information in itself, digital signature does not provide evidence that a document existed at the time when it is supposed to have. (Accuracy of the time axis of Figure 2-2 cannot be verified.)
- A PKI-based CA's guarantee for a digitally signed document does not last beyond the public key certificate's period of validity, which represents the period that the relevant

private key is valid. In the case that the certificate's validity is lost before the period is over, the guarantee expires when the revocation notice has been accepted and settled by the CA. (Figure 2-2)

- PKI-based digital signature system to secure document authenticity can eliminate alteration by third parties, but it cannot prevent mala fide alteration by the document producer in person.

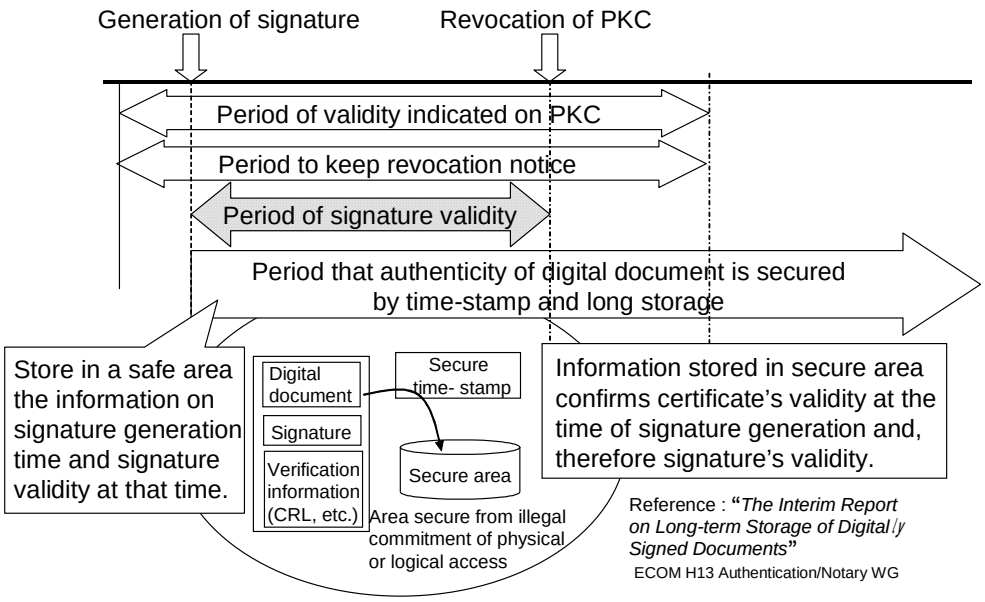


Figure 2-2 Period that Authenticity of Document is Guaranteed

To solve these problems, existence of a digital document at a specific point of time must be proved by time-stamp. This is the time-stamping technology, which realizes existential evidence of digital information.

2.3 Time-stamp

As already mentioned, digital signature is a means to enable personal verification and content authenticity of digital documents, which are involved in transactions and procedures to be secured. For security of transactions and procedures taking place on the digital network, evidence of the existence of relevant facts and proof of document delivery are also

necessary. Therefore, along with digital signature, time-stamp is essential to authenticate (guarantee) that a digital document existed at a certain time.

It is expected that time-stamp will be effective in the following functions and services:

- Evidence of the existence

To guarantee that a digital document existed at a certain point of time.

- Proof of delivery

To prove that a transmitted document has reached the recipient, as well as that the recipient have received the document. Also known as “delivery evidence” which is equivalent to delivery certificate used in existing postal service. This contributes to avoiding repudiation threat.

- Long storage of electrically signed documents

To secure authenticity of a digital document over time by providing existential evidence. The proper time of document verification information is authenticated in order to cope with digital documents exceeding the PKC validity period or key algorithm compromised.

Chapter 3. Role of Time-stamp

While contributing to securing digital document authenticity, digital signature technology has the following problems as mentioned in Chapter 2. To solve these problems, there needs to be a service to prove existence of digital information at a certain point of time.

Time of digital signature generation is left unproved

Digital signature verifies the person who produced a document and that the contents are just as they were at the time the document was signed. However, it does not verify *when* the document was produced.

Authenticity of a digitally signed document is not secured after expiration or revocation of PKC.

To secure authenticity of a digitally signed document after validity period or revocation of PKC, the following are necessary: proof that PKC, revocation information, etc. did exist at a certain point of time; and evidence that the digitally signed document really exists.

The person who digitally signed a digital document can alter it by him/herself.

If there is a third party who guarantees that a digitally signed document existed at a certain point of time, an attempt of alteration made later by the document author him/herself will never succeed.

In addition, time-stamp is indispensable for establishing evidence of the existence of digital facts, proof of digital document delivery, etc. This chapter will discuss models, technological trends, standardization and structure of time-stamping service.

3.1 Time-stamping Service Model

(1) Functions Required of Time-stamping Service

Time-stamping service provides a proof that a certain piece of digital information existed at a specific point of time. The service must satisfy the following two essential requirements.

- Existential evidence of a certain piece of digital information at a specific point of time must be supported by a technically traceable connection between time information and digital information.
- The service will have no concern with digital information contents.

The first requirement includes the use of cryptographic technology, which essentially needs security management requirements.

(2) Time-stamping Service Component

A Time-stamp Authority (TSA) provides the service as in the model case that Figure 3-1 illustrates.

- NTA

  National Time Authority to generate, maintain and distribute national standard time. It distributes national standard time to TA or TSA. Some NTAs periodically audit the time managed at TAs.

- TA

  Time Authority to distribute standard time to TSA. TAs periodically audit the time managed at TSAs. TA is a trusted third party.

- TSA

  Time-Stamping Authority to produce and issue time-stamp token (TST) for digital data submitted from users. A TSA may also act as a TST verification player, which will be described later, depending on time-stamping system adopted. TSA is a trusted third party.

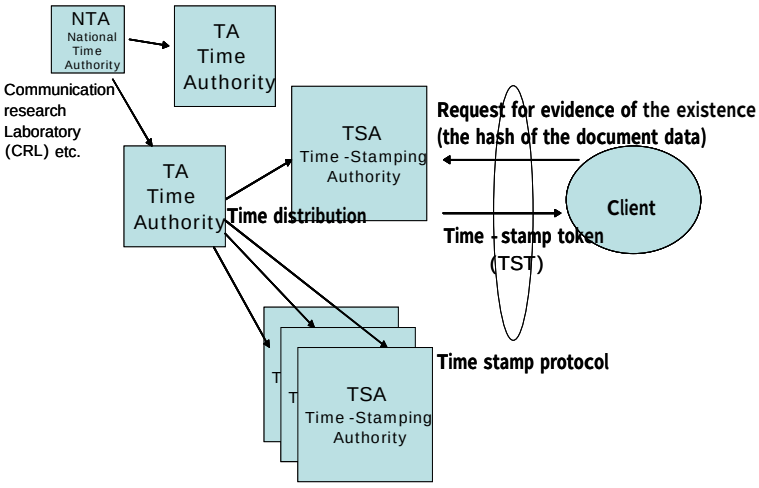


Figure 3-1 Time-stamping Service Model

3.2 Technological Trends

Time-stamping technology is controlled by the following standards:

(1) International Standards

ISO/IEC 18014-1 Information technology – Security techniques – Time-stamping services

- Part 1: Framework

  Provides frameworks for requirements, scope, and components/functions of time-stamping services. It also outlines Independent Token and Linked Token, the two different token systems to support authenticity of time-stamp.

- Part 2: Mechanisms producing independent tokens

  Defines three different mechanisms of independent token system: digital signature-based token (RFC3161 compatible), Message Authentication Code (MAC) -based token, and archive-based token.

- Part 3: Mechanisms producing linked tokens

  Defines two mechanisms of linked token system: digital signature-based token and digital signature-free token.

(2) Internet Standards (IETF: Internet Engineering Task Force)

- RFC3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

  One of the standards groups for PKI use on the Internet, defining protocols and time-stamp tokens which represent procedures and formats of time-stamping models.

- IETF Policy Requirements for Time-Stamping Authorities (draft – ietf – pkix – pr – tsa-00.txt) (2002-03)

  Provides requirements on TSA operational policies.

(3) European Standards

- ETSI TS 101 861v1.2.2 Time-stamping Profile

  Specifications based on RFC3161. Defines requirements that time-stamp clients and servers should fulfill.

3.3 Time-stamping Systems

ISO18014 defines two time-stamping systems with different time-stamp token types, which are called independent token and linked token. Typical examples of the two systems are as follows.

(1) Independent Token System

Independent token system (a.k.a. Simple Protocol) is represented by PKI-based time-stamp, which provides clients with a third-party guaranty by giving TSA's digital signature to the time information. A client sends TSA a time-stamp request in a prescribed

format along with a hash value (a message digest) of the document to be time-stamped. TSA produces a time-stamp token (TST) with the received message digest, a digital certificate of the time of acceptance and TSA's digital signature included in a prescribed format (TST type), and sends it back to the client. The client receives and stores the TST, so that the original document's existence at the time of the TST issuance can be verified by using TSA's public key certificate (PKC), when necessary in the future.

This system is characterized by simplicity of TST validation, which requires only the PKC for the public key cryptograph used to produce TST and its certificate. For effective performance of the system, the TSA here needs to be a Trusted Third Party (TTP).

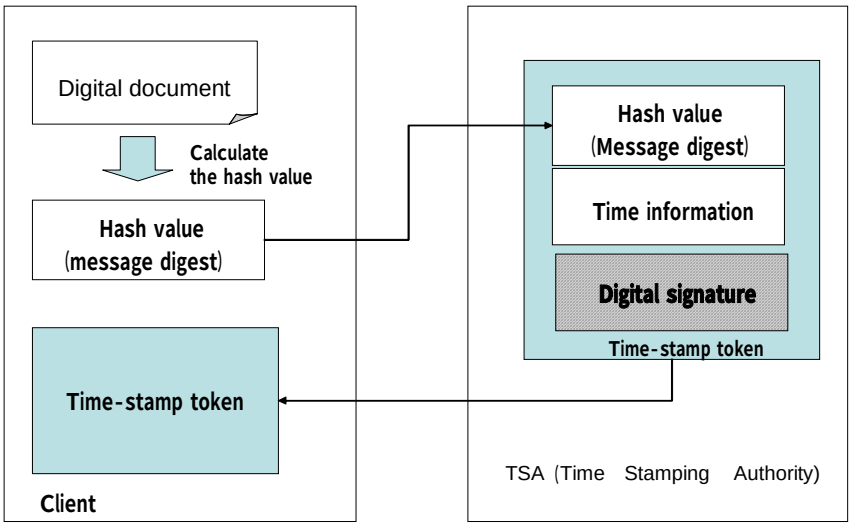


Figure 3-2 Time-stamp by Independent Token System (digital signature-based)

Independent token system also includes MAC-based time-stamp and archive-based time-stamp.

(2) Linked Token System

Linking Protocol is a system depending on security of hashing algorithm. Having received a digital document's hash value from a client, TSA sends back a linked token to use as evidence. Also, it periodically reports in the papers a total of hash values to provide a chronological linkage of the tokens.

Figure 3-3 shows a system, where TSA issues a client with a time certificate in linkage

with the message digest and hash function of another time-stamp request, which has been accepted just or shortly before. In this system, a newly issued time-stamp token is consequently linked to all those issued in the past. Therefore, no forgery of time-stamp token is possible unless coordinated with all the previous ones. In addition, with periodical publication of the linking information in papers, forgery becomes even more difficult while the linkage has to be verified only during the regular publication period.

This system always needs TSA for verification of a time-stamp token.

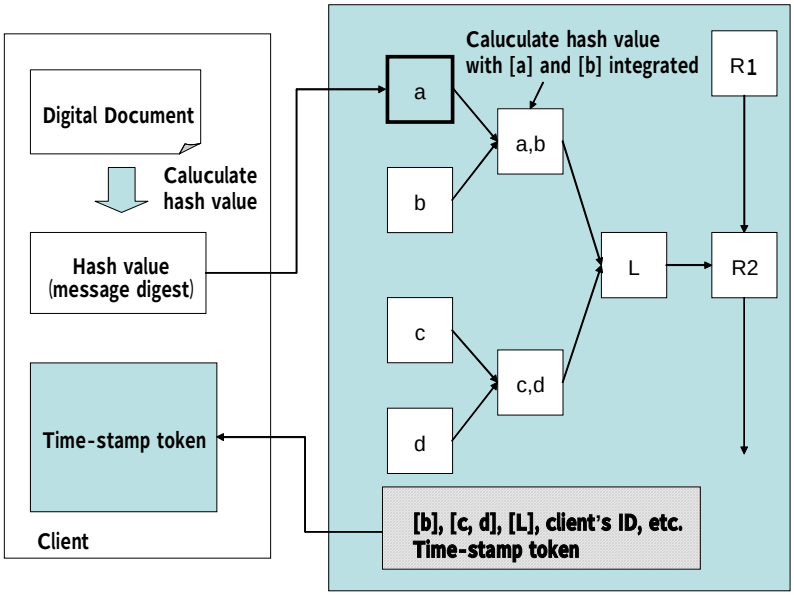


Figure 3-3 Linked Token System

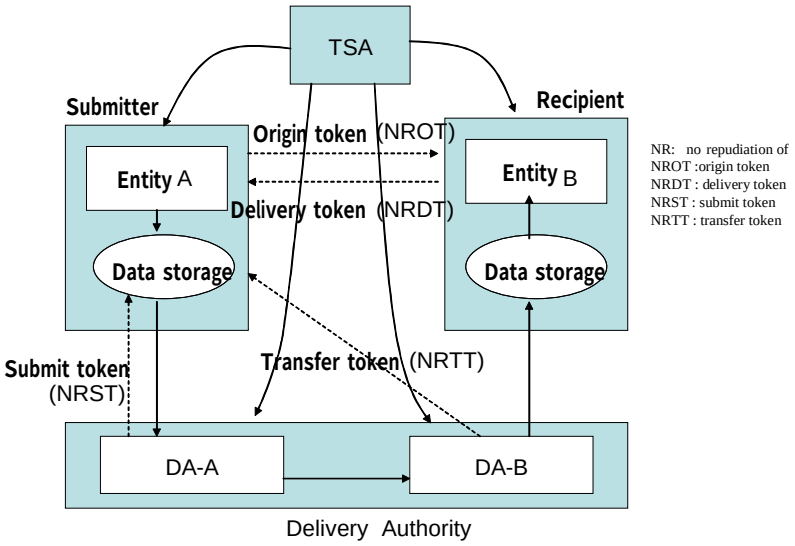
3.4 Standardization of Time-stamp Protocol [Deleted]

3.5 Non-repudiation System

Time-stamp, which provides evidence of the existence of digital documents, is effective in preventing repudiations. ISO/IEC 10181-4 and 13888 standardize the framework and technology of non-repudiation services.

Figure 3-4 shows a typical non-repudiation service, illustrating the players and systems concerned to data transmission, non-repudiation service provided, and the technologies used in the service provision.

The facts of data submission, receipt and transfer are stored respectively in the form of token. The tokens, with time-stamping and digital signature technologies applied to, verify



that the data have been properly received.

Figure 3-4 Non-repudiation Service Model

Chapter 4. Mechanism of Time Authentication Infrastructure

Time authentication infrastructure can be technically defined as a system infrastructure for providing standard time distribution, time-stamping, and other related services. The standard time distribution service is conducted by Time Authorities (TAs) in place of National Time Authority (NTA), while the time-stamping service provides evidence that a data item existed before a certain point in time, based on the time source distributed from NTA or TAs.

This chapter describes the mechanism of time authentication infrastructure, which supports time-stamping services. Time-stamping service systems (i.e. time-stamp token issuance and validation systems) described here are based primarily on the international standards such as RFC 3161 and ISO/IEC 18014.

4.1 Time Authentication Service Model

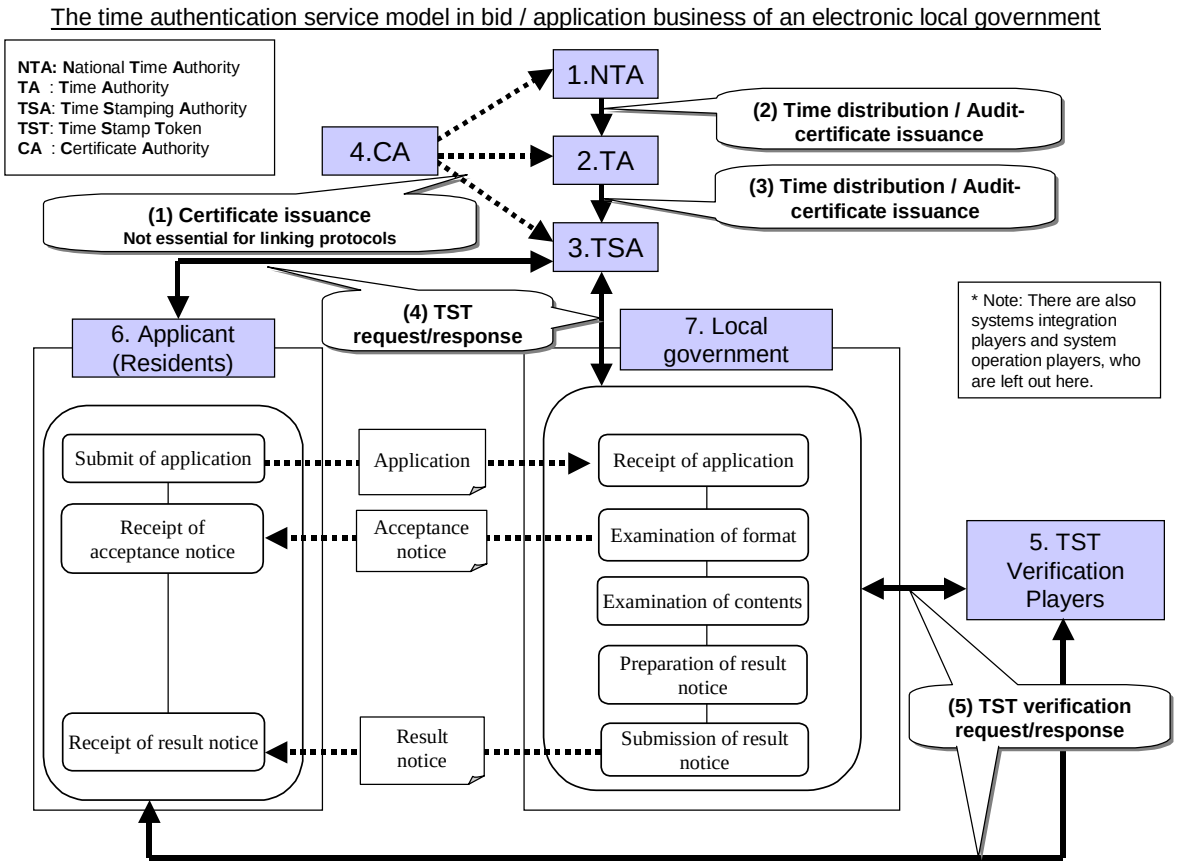


Figure 4-1 Time Authentication Service Model for E-application Transaction

The following paragraphs outline a time authentication service model applied to e-application system of a local e-government. Players in this model are defined as follows, except for NTA, TA and TSA, which have been already defined in 3.1 (2).

・CA

Certification Authority, which issues NTA, TA and TSA with appropriate certificates or PKCs for digital signatures. Some time-stamping systems do not involve this player.

・TST verification player

Verifies the validity of time-stamp tokens. The entity of this role can be different depending on time-stamping system. TSTs based on simple protocol system can be verified on PKI by clients themselves. In the case of the TSTs based on linking protocol system, TSA, who issues the tokens, or some other third party becomes the player.

・Applicant (resident)

Local residents making applications, or the residents' software and tools. They follow application formalities in communication with the application acceptance system of the local government. They can make a request to TSA for time-stamps to prove their applications' existence. In the case of some trouble, they verify the validity of TSTs issued from the local government, by using the TST verification player.

・Local government

Local government providing application services for residents, or the application system itself. Based on time-stamping services provided by TSA, the local government gives time-stamps to application forms from applicants, acceptance notice, result notice and other documents produced during the application transaction. In the case of trouble, it verifies the validity of TSTs it has issued, by using the TST verification player.

4.2 Flow of Time-stamp Token Issuance

A client acquires time-stamps for their digital data, following the basic procedure as shown below (Figure 4-2).

- Submit time-stamp request to TSA

  A time-stamp request has to include at least the hash value of digital data to be time-stamped, as well as a descriptor to indicate a hashing algorithm.

- Generate time-stamp token

  TSA generates a time-stamp token and return the response including the TST to the client.
- Receive time-stamp response from TSA

  The response carries the requested TST, which shall be stored by the client.

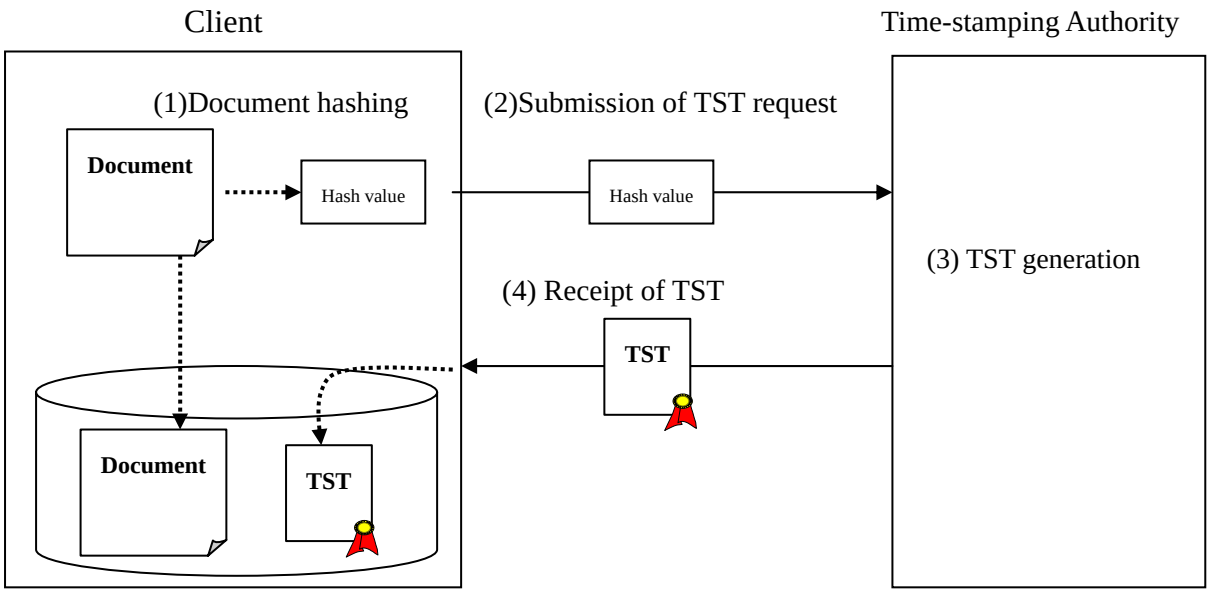


Figure 4-2 Flow of Time-stamp Token Issuance

4.3 Flow of TST Verification

Procedure of verification of the validity of a time-stamp token differs by time-stamping system.

4.3.1 Verification of Simple Protocol TST

TSTs based on simple protocol system can be verified on PKI by clients themselves. The basic procedure is as follows (See (1) in Figure 4-3).

- Examine if the TST is syntactically well-formed.
- Examine if the hash value of digital data to be verified is identical to the equivalent hash value in the TST.
- Verify TSA's signatures found in the TST.

Examine the validity of TSA's PKC. Then, using the public key in the PKC, verify the signatures in the TST.

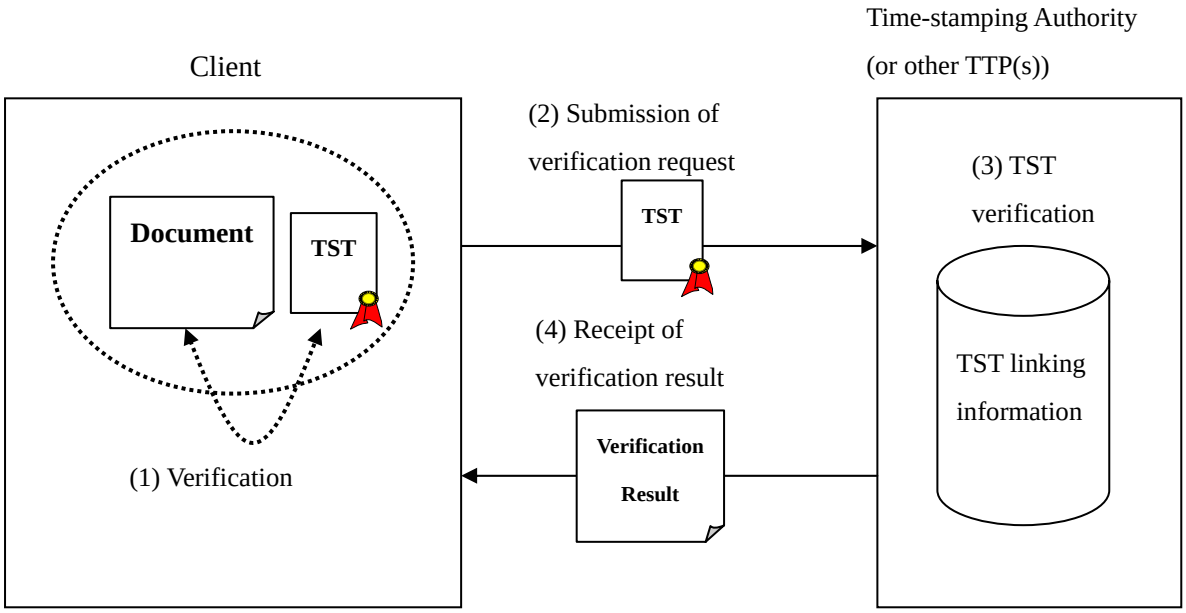


Figure 4-3 Flow of TST Verification

Alternately, clients may ask a trusted third party to carry out the verification for them.

4.3.2 Verification of Linking Protocol TST

Verification of TST based on linking protocol system needs to involve players who possess the linking information necessary for the verification. Specifically, TSA who has issued the TST or other trusted third party should take part. The basic procedure is as follows (See (1), (2) and (3) in Figure 4-3).

- Examine if the TST is syntactically well-formed.
- Examine if the hash value of digital data to be verified is identical to the equivalent hash value in the TST.
- Submit the request for verification of the TST' validity to TSA who has issued the TST or other trusted third party that has access to the issuing TSA's linking information (i.e. TSA's summary links).
- Receive the validation result from the TST or other entrusted third party.

4.4 Traceability of Time Authentication

Traceability of time authentication means the traceability of time information included in time-stamp tokens. The followings are the requirements for the traceability of time:

- It is provable that the time source of time-stamp token issued by a TSA has a logical connection with that of a TA or, if possible, NTA.
- It is provable that the difference between the time used by a TSA for time-stamp token issuance and the national standard time is within a prescribed permissible range.

Traceability of time authentication can be realized by the following methods:

- Include traceability information within time-stamp tokens.
- TSAs produce evidence of undergoing periodical time audit by a TA or NTA.

Chapter 5. Time-stamp User Guideline

5.1 Framework

This chapter will introduce time-stamp user guideline for e-bidding, which is one of the primary targets of the e-Japan Project efforts being made by local governments. The guideline will specify the cases where time-stamps should be used within business applications, as well as the proper way to use them. To begin with, time-stamp information common to different work types is provided in this section.

(1) Structure of the Guideline

Occasions demanding time-stamps and action taken on such occasions are almost the same in any work type, even if the causes and processes differ. Although detailed elements of time-stamps and time-stamping are specific to each work type, they can be integrated into a common concept of framework. Based on the common framework described below, we define the elements for each work type: documents, timing, purpose and recommendation rating to acquire time-stamps, as well as time-stamp requirements/handling/validation.

First, the timing for getting time-stamps is pointed out in workflows of different work types, with each workflow clarifying the correlation between documents and work type.

Documents given in the workflow is then listed with signs indicating recommendation rating in relation with time-stamping purposes, which are detailed in the next section. The recommendation rating is on three levels: “strongly recommended”, “recommended” and “preferable”

Requirements for time-stamps are numerically specified about performance and validity period according to purpose.

A time-stamp will not work effectively by merely acquiring it. It must be properly verified in relation with the lifecycle of a document it has been given to. In this guideline, verification necessary for the time of acquiring a time-stamp on a document, receiving the time-stamped document, storing the time-stamped document is detailed.

For the purpose of document delivery/receipt certification, delivery and receipt shall be time-stamped on every individual act, partly overlapping with system logging, or a log file of such acts shall be time-stamped for non-alteration and non-repudiation, while improving the log file clock accuracy over the standard.

(2) Purpose of Time-stamp in E-bidding

To e-bidding explained here, time-stamps are important not only to verify the past status of a certain piece of information, but also to certify its existence in order to avoid the risk of alteration, spoofing or repudiation potential in the course of transaction. To avoid troubles from the above-mentioned risk, status of information must be confirmed at each transaction

step after its submission to the local government, specifically: (1) what it was like initially, (2) how it changed in the course of transaction, (3) what it was like when it reached the final step of transaction, (4) what notice it resulted in. At the same time, it is necessary to ensure that the information exchanged between the applicant and the local government is verified at every transaction step, and that the information exchange is mutually recognized by both parties. The former is a time-stamp purpose to verify information handled at different points of time, which is called **Document Existence Verification**, while the latter is to confirm the document delivery/receipt, which is called **Delivery/Receipt Verification**.

Separate from the above, by giving time-stamp to digitally signed documents, the limited validity period of PKI-based digital signature is extended, securing document validity for a longer period of time. This is another time-stamp purpose called **Long-term Storage Verification**, which enables long retroactive verification that the document has been non-altered, and that digital signature and digital certificate were valid at the time of issuance.

Table 5-1 [Deleted]

5.2 Guideline for Use in E-bidding

In this section, timing, purposes, and their relevant requirements for time-stamp use in e-bidding transaction of local governments will be explained.

5.2.1 Timing and Purposes

Purposes, timing and documents to use time-stamp in e-bidding transaction will be shown in the workflows below, based on the time-stamp purposes presented in the previous section.

The purposes are:

- ✓ Delivery/Receipt Verification: Giving time-stamp to certificates of receipt, notices, etc. to enable after-the-fact verification of delivery and receipt of bid sheets, notices, etc., thus certifying non-alteration and non-repudiation.
  Ex.: certificates of receipt, notices, etc.

- ✓ Document Existence Verification: Giving time-stamp to documents requiring chronological sequentiality of existence and execution, such as registration of expected price information, execution of bid opening, etc. as well as to documents whose existence at certain point of time (e.g. submission deadline) may be critical, in order to certify non-alteration and non-repudiation.
  Ex.: expected price registration, execution of bid opening, etc.

- ✓ Long-term Storage Verification: Giving time-stamp to digitally signed documents, virtually extending the limited validity period of digital signature, in order that non-alteration of the document and certificate's validity at the time of issuance can be retroactively verified by long-stored verification results.
  Ex.: bid sheets, notices, etc.

Timing of acquiring time-stamps and related purposes is explained by using the general competitive bidding system, which represents the typical example of tender transaction process defined in the basic design for "Electronic Procurement System" released from Ministry of Land, Infrastructure and Transport in November 2001.

(1) Construction Procurement (by general competitive bidding system)

(a) Workflow

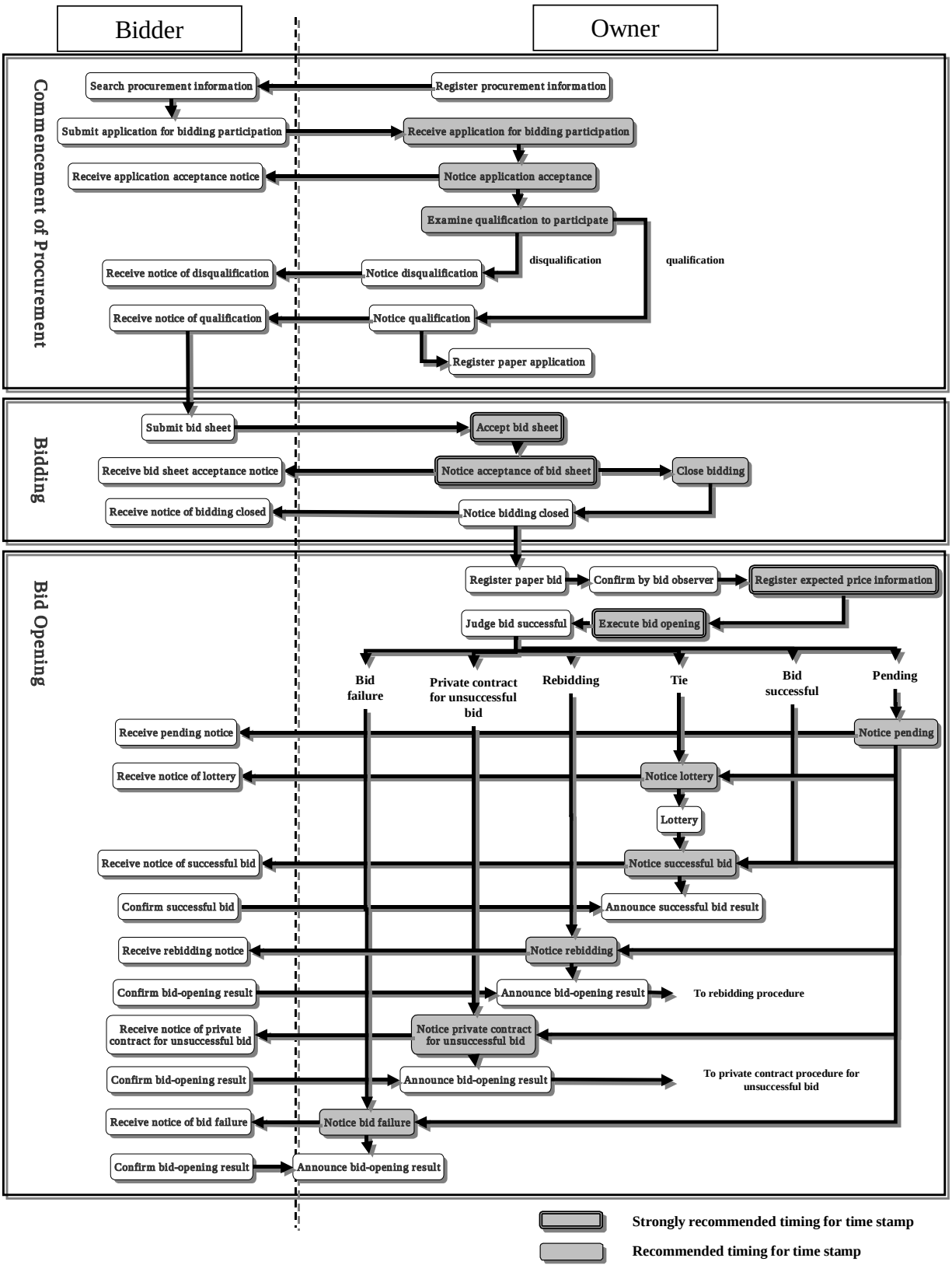


Figure 5-1 Construction Bidding Workflow and Timing for Time-stamps

Figure 5-2 [Deleted]

(b) Purpose of Time-stamp and Recommendation Rating

Table 5-2 details the purpose and recommendation rating of each time-stamp pointed out with timing in the workflow above.

Table 5-2 Timing and Purpose of Time-stamp

Work types	Job names	Target document	Purpose/Rating D/R	Exst	L-trm	Explanation
Commencement of Procurement	Receipt of application for bidding	Application for bidding qualification		○	○	・ Time-stamping the application for bidding qualification on receipt by owner enables future verification of the document and time of its receipt as well as validity of digital signature/digital certificate on it. ・ For time-stamp on log, see 5.4 Time-stamp Acquisition for Internal Log
	Acceptance notice of application for bidding	Acceptance card of application for bidding qualification	○			・ Time-stamping the acceptance card of application for bidding qualification on transmission by owner enables verification of fact and time of the document transmission.
	Examination of qualification			○	○	・ Time-stamping the result of examination of qualification by owner enables future verification of examination details and time as well as validity of digital signature/digital certificate on it.
	Notice of disqualification	Bidding qualification notice	△			・ Time-stamping the bidding qualification notice (disqualification) on transmission by owner enables verification of fact and time of the document transmission.
	Notice of qualification	Bidding qualification notice	△			・ Time-stamping the bidding qualification notice (qualification) on transmission by owner enables verification of fact and time of the document transmission.

Work types	Job names	Target document	Purpose/Rating D/R	Exst	L-trm	Explanation
Bidding	Acceptance of bid sheet	Bid sheet		◎	◎	・ Time-stamping the bid sheet on transmission by bidder enables verification of fact and time of the document transmission. ・ Time-stamping the bid sheet on acceptance by owner enables future verification of the document and time of its acceptance as well as validity of digital signature/digital certificate on it. ・ For time-stamp on log, see 5.4 Time-stamp Acquisition for Internal Log
	Notice of bid sheet acceptance	Bid sheet acceptance card	◎			・ Time-stamping the bid sheet acceptance card on transmission by owner enables verification of fact and time of the document transmission.
	Bid closing			○	○	・ Time-stamping the bid closing result by owner enables future verification of bid closing details and time as well as validity of digital signature/digital certificate on it.
	Bid closing notice	Bid closing notice	△			・ Time-stamping the bid closing notice on transmission by owner enables verification of fact and time of the document transmission.
Bid Opening	Expected price information registration			◎	◎	・ Time-stamping the registration result of expected price by owner enables future verification of expected price input details and time as well as validity of digital signature/digital certificate on it
	Bid opening execution			◎	◎	・ Time-stamping the bid opening result by owner enables future verification of bid opening details and time as well as validity of digital signature/digital certificate on it.
	Pending notice	Pending notice	○	○	○	・ Time-stamping the pending notice on transmission by owner enables verification of fact and time of the document transmission. ・ Time-stamping the pending notice on production by owner enables future verification of the produced document and time of its acceptance as well as validity of digital signature/digital certificate on it.

Work types	Job names	Target document	Purpose/Rating D/R	Exst	L-trm	Explanation
	Lottery notice	Lottery notice	○	○	○	・ Time-stamping the lottery notice on transmission by owner enables verification of fact and time of the document transmission. ・ Time-stamping the lottery notice on production by owner enables future verification of the produced document and time of its acceptance as well as validity of digital signature/digital certificate on it.
	Notice of successful bid	Notice to successful bidder	○	○	○	・ Time-stamping the notice to successful bidder on transmission by owner enables verification of fact and time of the document transmission. ・ Time-stamping the notice to successful bidder on production by owner enables future verification of the produced document and time as well as validity of digital signature/digital certificate on it.
	Rebidding notice	Rebidding notice	○	○	○	・ Time-stamping the rebidding notice on transmission by owner enables verification of fact and time of the document transmission. ・ Time-stamping the rebidding notice on production by owner enables future verification of the produced document and time as well as validity of digital signature/digital certificate on it.
	Notice of private contract for unsuccessful bid	Notice of private contract to unsuccessful bidder	○	○	○	・ Time-stamping the notice of private contract to unsuccessful bidder on transmission by owner enables verification of fact and time of the document transmission. ・ Time-stamping the notice of private contract to unsuccessful bidder on production by owner enables future verification of the produced document and time as well as validity of digital signature/digital certificate on it.
	Notice of bid failure	Call-off notice of bidding	○	○	○	・ Time-stamping the call-off notice on transmission by owner enables verification of fact and time of the document transmission. ・ Time-stamping the call-off notice on production by owner enables future verification of the produced document and time of its acceptance as well as validity of digital signature/digital certificate on it.

◎…Strongly recommended　　D/R…Delivery/Receipt verification
○…Recommended　　Exst…Document existence verification
△…Preferrable　　L-trm…Long-term storage verification

(c) Time-stamp Recommendation Rating

Meaning of recommendation ratings applied in Table 5-2 can be summarized for each time-stamp purpose as follows.

- Delivery/Receipt Verification purpose

◎ In the bidding transaction, verification of time is considered to be of essential for acceptance of bid sheets, rebidding sheets and price estimates. Therefore, time-stamping at the point of acceptance of these documents is strongly recommended.

○ Time-stamping is recommended at the point of transmission of important notices where owners need prevention against after-the-fact repudiation.

△ For delivery and receipt of documents not referred in the above, time-stamp is preferable where appropriate.

- Document Existence Verification purpose

◎ Where the sequential order of existence or occurrence in the bidding procedure is important, time-stamp is strongly recommended at the point of document production or job execution.

○ Time-stamp is recommended at the point of production of various notices to bidders.

- Long-term Storage Verification purpose

◎ In the bidding transaction, verification of contents is considered to be of essential for bid sheets, rebidding sheets and price estimates. Time-stamping at the point of acceptance or unsealing of these documents is strongly recommended for the purpose of long-term storage verification of contents, time and digital signature.

◎ The results of manual input or visual judgment at the point of paper bid registration, expected price information registration, and bid opening execution are strongly recommended to be time-stamped for the purpose of long-term storage verification of contents, time and digital signature.

○ Time-stamp is recommended at the point of production of various notices to bidders for the purpose of long-term storage verification of contents, time and digital signature.

Figure 5-3, 4, 5 [Deleted]
Table 5-3 [Deleted]

5.2.2 Requirements for Time-stamp

(1) Performance

Time-stamp must fulfill the performance requirements indicated in Table 5-4. The range required by bidding procedure shall be calculated based on each bid owner's peak cases (e.g. number of cases/day) with prescribed number of time-stamps and assumed portion of online processing taken into consideration.

Table 5-4 Performance Requirements for Time-stamp

Requirements	Delivery/Receipt Verification	Document Existence Verification	Long-term Storage Verification
Time accuracy provided by time-stamp	Within ±3 sec.	Within ±3 sec.	Within ±3 sec.
Capability of time-stamping within the range required by bidding transaction	○	○	○

※ Time accuracy indicated in the table represents the accuracy provided by TSA on time-stamping, with no consideration of time difference between the e-bidding system and TSA network.

(2) Period of Validity

Validity period requirements defined in Table 5-5 must be fulfilled. Time-stamps with different validity periods can be used where appropriate.

Table 5-5 Validity Period Requirements for Time-stamp

Requirements	Delivery/Receipt Verification	Document Existence Verification	Long-term Storage Verification
Validity period of time-stamp	3 years and longer	5 years and longer	10 years and longer

The validity periods indicated above are the minimum necessity assumed for general bidding transactions. Where there are document management rules on the owner's side defining longer periods for storing any document with time-stamp need, validity period of time-stamp should be subject to such storage periods. Where storage periods are defined according to the amount of procurement fund, the longest validity period among them should be applied, instead of using different periods by the fund amount.

Table 5-6 [Deleted]

When time-stamp dissatisfying the validity period requirements above has to be used, newly issued time-stamp may extend the original period, provided that the bid owner has a structure and system to ensure the period extension.

To be free of such complicated transactions as validity period extension, as well as to avoid the risk of extension failure, it is preferable that time-stamp which can technically guaranty a validity period of 10 years and longer is adopted. If the technology does not allow this, a reliable structure and system must be prepared for proper implementation of validity period extension.

(3) Verification

Bidding transactions should adopt time-stamping services that are available for verification at any time and in any way necessary, with both owner and bidder undergoing the verification. It is preferable that the services adopted can provide the two parties with an environment for easy and economical verification.

(4) Services to Use

Time-stamp services to use must fulfill the requirements in Table 5-5. However, it is more desirable to use services provided by trusted third parties.

Table 5-7 Time-stamp Service Requirements

Requirements	Delivery/Receipt Verification	Document Existence Verification	Long-term Storage Verification
Satisfying technical and operational standards for time-stamp issuance service defined in this guideline	○	○	○
Satisfying technical and operational standards for time-stamp verification service defined in this guideline	○	○	○

For the technical and operational standards defined in this guideline, see 'Simple Protocol' and 'Linking Protocol' explanatory in 6.2 Time-stamp Issuance Service and 6.3 Time-stamp Verification Service.

5.2.3 Management and Verification of Acquired Time-stamp

Time-stamps for bidding-related documents will not be sufficient for verification of documents with different purposes if they are merely acquired. They must be properly verified in relation with the lifecycle of documents they have been given to, in order for positive verification of documents' delivery/receipt, existence and long-term storage.

Timing for time-stamp verification in bidding transaction will be presented below.

However, as the timing presented here are of the minimum necessity, practical frequency should be well considered according to actual business importance, system load and cost.

(1) Verification on Time-stamp Acquisition

Time-stamp token, digital signature and digital certificate (if the time-stamp is based on PKI) should be verified immediately after acquisition of time-stamp.

Verification of the TST must include validation of the time when it was produced and verification if time-stamp policy and other time-stamp information (TSTInfo) are compliant with the document contents applied for time-stamp.

(2) Verification on Receipt of Time-stamped Document

When receiving a time-stamped document whose time information is needed in the subsequent procedures, the time-stamp should be verified in advance.

If the time-stamp is on a digitally signed document, the digital signature and digital certificate should be verified at the same time.

(3) Verification on Storing Time-stamped Document

Before storing a time-stamped document its time-stamp should be verified.

The time-stamped document should be stored in a form that clarifies the relation between the document and the time-stamp, and in a secure environment with little chance for the document alteration.

5. 3 Guideline for Use in E-application [Deleted]

5.3.1 Timing and Purposes [Deleted]

5.3.2 Requirements for Time-stamp [Deleted]

5.3.3 Management and Verification of Acquired Time-stamp [Deleted]

5. 4 Time-stamp Acquisition for Internal Log

Information system for time authentication infrastructure should ensure its security and reliability through proper acquisition, maintenance and periodical audit of log information.

(1) Information to Enter into Logs

The system log and the access log should be recorded as important information of security-related events, securing them with requirements as an audit log.

The audit log requirements include the following:

(a) Type of event

(b) Date and time of occurrence of event

(c) Process results
(d) Information to identify event origin (operator, system, etc.)
(e) Time and authenticity verification by time-stamp

The audit log is acquired and maintained by files.

(2) Log Protection

Real-time log alteration detective and preventive measures should be taken. Measures against log file deletion also should be taken.

(3) Time-stamp Acquisition for Logs

Log files should be provided with simple protocol or linking protocol time-stamp issued by a trusted third party for time and authenticity verification.

Time-stamp acquisition is recommended on the following occasions in order to verify that no loss, alteration nor alteration of information has taken place in the maintenance routine.

(a) Log file rotation
(b) Transfer of log files to a loghost machine or any other machine
(c) Archiving log files on external media or in storage
(d) Log analysis, audit on time-stamp verification

(4) Log collection

Log collection should be practiced as an integral part of the system function, covering the whole operational history of a day.

(5) Period of Log Storage

Log file time-stamp should be stored and kept valid as long as the bidding and application documents may be regulated or even longer where appropriate. If the log storage period is provided in system maintenance rules, time-stamp should be kept valid and stored accordingly.

(6) Log Analysis

It is recommended that log output, acquisition, information will be analyzed daily or weekly, in order to ensure that the service system is properly working.

(7) Log Audit

Log audit should be conducted periodically on log acquisition manners and maintenance condition, as well as on the audit log contents. Log audit is preferable to be conducted monthly, without prior notice to the operator who generates events.

Chapter 6. Time-stamp Provider Guideline

This chapter will present a guideline for providing time-stamping and related services.

6.1 Technical Guidelines

This section will detail the technical guidelines applied to time distribution service, time-stamping service and time-stamp verification service.

6.1.1 Standard Time Distribution Service

Standard time distribution is a service conducted by Time Authorities (TAs) in place of NTA. This guideline will focus on the standard time distribution service for time-stamping authorities (TSAs), clarifying the technical measures that Time Authorities are required.

(a) Time Authority's clock

Time authority is required to distribute time with adequate accuracy.

- Target accuracy of distributed time: approx. ±300 ms
- To realize this accuracy, Time Authority must use a clock with necessary and sufficient accuracy for its service.
- Time authority must provide itself with means to synchronize the clock for its service with UTC, which is distributed by NTA, with necessary and sufficient accuracy.
- Time authority must provide itself with means to properly manage leap seconds synchronized with UTC.

(b) Time Audit by NTA

Time authority is required to undergo time audit by NTA or its substitute auditor on the clock for its service.

- Target accuracy required for time audit: approx. ±30 ms (between NTA and TA)
- Time audit by NTA must be conducted in the way that necessary and sufficient audit accuracy will be secured for time distribution service.
- Time authority is required to be with a system to receive from NTA a digital certificate of time audit fact and results.
- It is preferable that Time Authority has a system to protect the time audit

certificate issued by NTA from illegal alteration and deletion over a necessary period of storage.

(c) Integrity of Time

Time authority must guaranty that the time it distributes retains accuracy within a prescribed range from UTC.

- Time authority must have a mechanism to detect any departure of its time from the rated accuracy.
- Time authority must have a system for recording its operational efforts to maintain integrity of time.

(d) Identifying (authenticating) TSA

Time authority must identify and authenticate time-stamp server, whom it is going to distribute time or time-audit.

- Time authority must provide itself with means to identify time-stamp server used by TSA whom it distributes time, in order to avoid the risk of spoofing in communication with time-stamp server.
- It is recommendable for Time Authority to introduce the PKI-based mutual authentication system as a way of identifying time-stamp server.

(e) Time Distribution to TSA

Time authority must provide the time to a time-stamp server, which is used by TSA, with accurate time in a secure way.

- Time distribution to time-stamp server must be in a communication method that can prevent or detect time alteration.
- Time distribution to time-stamp server must be provided with a means to synchronize the time-stamp server's clock with UTC with accuracy required by TSA.

(f) Time Audit of TSA

Time authority must audit operation of the time that it distributes to time-stamp server.

- Time authority must provide itself with a means of auditing the time of time-stamp server's clock with necessary and sufficient accuracy.
- Time audit must take place at least once a day.
- Audit results are important evidence of time operation by time-stamp server. Time authority must store audit results for future, keeping them verifiable and available for TSA.
- Time authority must provide itself with means of audit result storage that can prevent or detect time alteration.

- Time audit of time-stamp server must be provided with a function to inhibit or detect TSA's altering the time it has been distributed.

(g) Controlling TSA Time Error

Time authority must support a function to notify TSA of detection that the time distributed to time-stamp server's clock has departed the rated accuracy.

- It is recommended that Time Authority should support a function to suppress time-stamping when detecting that time-stamp server's clock time has departed the rated accuracy.

6.1.2 Time-stamping Service

Time-stamping service is to issue secure time-stamp tokens to clients on request. The agent of time-stamping service is called Time-stamp Authority (TSA). Typical methods to generate secure time-stamp tokens are Simple Protocol system and Linking Protocol system. In this section, technical guidelines for Time-stamp Authority to provide time-stamping services will be detailed for each system.

(1) Simple Protocol

Technical guidelines for a simple protocol-based Time-stamp Authority are as follows.

(a) Time source

Time-stamp server's time source (clock) to generate time-stamps and time distributing agent should be clarified.

- Time distribution and synchronizing systems must be clarified by specifying TA, GPS, standard radio wave, and NTP.
- Time synchronization must use secure and reliable system.

(b) Accuracy

Time-stamp server's time source must be synchronized sufficiently with Japan Standard Time.

- Target accuracy required: approx. ±30 ms

(c) Accuracy verification

It is preferable that Time-stamp Authority has means to verify accuracy of time-stamp server's time source.

- It is preferable that time-stamp includes audit certificates and audit records issued

by TA, verifying the facts of time synchronization with TA, time audit, time authentication, etc., so that such information is always available for reference.

- It is preferable that the certificates and audit records include specific information about time/result/auditor in charge of implementation in order to detect fact of having been altered.

(d) Time-stamp policy

Time-stamp Authority must clarify time-stamp issuance policy (time-stamp policy).

- Time-stamp must include information by which one can instantly identify time-stamp policy such as time-stamp policy identifier, references, hash, etc.
- Time-stamp policy contents must be always available for reference.
- It is preferable that time-stamp policy is available for verification of its non-alteration.

(e) Time-stamp data type

Data type of time-stamp must be clearly defined, preventing misreading of time indication.

(f) Issuer information

Time-stamp must include information to identify time-stamp issuer and time-stamp server.

(g) Client information

Time-stamp must not include any information about the client demanding the time-stamp.

(h) Serial number

It is preferable that every time-stamp has its own unique identifier.

- The identifier is preferred to be with a serial number to indicate the order of issuance.
- Whether serial number is used or not must be clarified in time-stamp policy.

(i) Ordering

Whether or not guaranteeing sequential relevancy between serial number and issuance time, and coverage of the guaranty (‘guaranteed’, ‘guaranteed to the range of seconds’, etc.) must be clearly presented in time-stamp or time-stamp policy.

(j) Representation of original data

Time-stamp must include hash value representing original data, so that identification to original data will be possible. The representation of original data must be illegible to

time-stamp issuer by digesting or encoding.

(k) Non-alteration (integrity) verification

Time-stamp must include MAC, signature or other means to verify its non-alteration.

(l) Hash algorithm, signature algorithm and key length

Time-stamp or time-stamp policy must include identifier of algorithm to calculate hash value for document to be time-stamped, time-stamp signature algorithm, and key length (where signature is used).

- Hash algorithm in the cryptography list that is recommended by e-government (SHA-1, SHA256, SHA384, SHA512, and RIPEMD-160) must be supported.
- Signature algorithm in the cryptography list that e-government recommends (RSASSA-PKCS1-v1_5, RSA-PSS, DSA and ECDSA) must be supported.
- Key length equivalence of RSA 1024 bit must be supported, while key length equivalent to RSA 2048 bit should be supported.

(m) Signature key

When signature is used, signature key must be protected with HSM.

- HSM is preferred to be certified level 3, FIPS140-2 or higher.
- Signature key is to be with a structure disabling any backup.

(n) Certificate and revocation information

When signature is used, certificate and revocation information must be properly managed or distributed.

- When requested by client, public key certificate or its identifier must be included in time-stamp token for verification of time-stamp.
- Certificate must be of exclusively issued for time-stamp use.
- Certificate path and revocation information must be available for time-stamp verifier.
- Particularly for time-stamp for long-term storage, certificate and revocation information must be kept available for a sufficiently long period of time.

(o) Validity period

Validity period of time-stamp, based on public key certificate's validity period and hash's fragility, must be clarified in time-stamp policy. Validity period is preferred to be sufficiently long (e.g. by renewing a 5-year valid certificate every year).

(p) Measures against compromisation

The algorithms of hash and signature must be proved to be secure at the time of time-stamping. When fragility is pointed out, immediate replacement with another algorithm with proved security is preferred.

(q) Transfer protocol

Time-stamp request and response must be transferable with at least HTTP or HTTPS.

(r) Replay attack protection

Supporting NONCE or other measures must be taken against replay attack.

(2) Linking Protocol

Technical standards required of linking protocol-based time-stamp are as follows.

(a) Data type of time-stamp record

Data type of time-stamp record must include the following information to avoid misreading of time indication.

- Version No.
- Message imprint・・・information bound to TSA time (e.g. hash value)
- Serial No.・・・exclusive number issued to timestamp record
- Time-stamp・・・required to include information capable of representing UTC according to ISO8601

(b) Certification period

Period of non-alteration verification and guaranty of time given by time-stamp record must be as long as storage period of digital document to be time-stamped. Although digital document storage period differs by document type and client type, it generally must fulfill the following requirements in order to provide sufficient certification period for clients.

Hash value length・・・160 bit and longer

Hash algorithm・・・RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512

Note: MD5 is not included in the cryptography list recommended by e-government, so at this moment it should not be used independently in time-stamp service. However, together with any of the above hash algorithm, MD5 use in time-stamp service will be regarded as fulfilling the required technical standards.

(c) Measures against algorithm compromisation

Linking protocol-based time-stamp service is recommended to prepare for compromisation of hash algorithm, by supporting ExRenewal extension defined in ISO/IEC 18014-3

(Mechanisms producing linked tokens). Client can extend time-stamp lifecycle by using ExRenewal extension when its time-stamped digital document must be stored beyond the expected time of TSA's algorithm compromisation.

(d) Operation

Linking protocol-based time-stamp service must be supporting the following operations defined in ISO/IEC 18014-3.

- Linking
  Information bound with time under management by TSA (e.g. hash value) must be in calculative link with that generated in the past.
- Integration
  Plural requests at a certain point of time must be operated at a time through a demand integration function.
- Publication
  Linking information managed by TSA must be periodically made open to wide public.

6.1.3 Time-stamp Verification Service

(1) Simple Protocol

(a) Secure communication route

It is preferable that verification protocol between time-stamp verification services and their users is implemented on a communication route where security measures (against spoofing, alteration, wiretapping) have been taken.

(b) Verification request data

- Verification request data must include time-stamp token to be verified.
- Verification request data may include original data of time-stamp.

(c) Verification process

- Examine the format of verification request data transmitted from client.
- Examine validity of time-stamp token transmitted from client.
- Return error messages in the case of inadequacy of verification request data format or verification failure. The message must include the reason of the error.
- In the case of successful verification, the verification result data must be returned to client.

(d) Validity of time-stamp token

- When time-stamp token includes public key certificate, examine if the certificate is still valid at the time of verification.
- When time-stamp token includes public key certificate, it is preferable to examine the certificate's validity at the time of time-stamp token issuance.
- Examine validity of digital signature included in time-stamp token by using validated public key certificate.
- Other verification method may be adopted instead of based on PKI technology. For example, comparison may be possible between time-stamp token to be verified and time-stamp token information securely stored within TST verification player.

(e) Verification result data

- Verification result data must include time-stamp token in client's verification request data
- Verification result data may include digital signature of TST verification player.

(2) Linking Protocol

The same standards as those mentioned in 6.1.2 (2) are required of Time-stamp Authority.

Time-stamp record issued by linking protocol-based TSA can be verified only by TSA who possesses the linking information generated at the time of issuance. Therefore, the standards required of verification demand accepter are the same as those required of issuance demand accepter.

6.2 Operational Guidelines

6.2.1 Common Items

(a) Obligations

① Securing reliability and security of Time-stamp Authority itself

Time-stamp Authority is obliged to continue appropriate operation based on process and procedures necessary implement services appropriate for a reliable and secure TSA.

② Appropriate information to clients and dependents of the clients

Time-stamp Authority is obliged to make clients and dependents of the clients understand their obligations well. At the same, time it is also obliged to provide them at appropriate points of time with information necessary for them to implement their obligations.

(b) Responsibilities

① Time-stamp Authority must define its own obligation, as well as define and disclose its essential policies related to responsibility and guaranty.

② On disclosing its policies, Time-stamp Authority must also disclose its operation rules and rules for service users, as well as outlines of other important information, in order that clients can evaluate the Time-stamp Authority's reliability and better understand client's obligations and Time-stamp Authority's obligations.

③ Responsibility and compensation must be defined for the case where Time-stamp Authority has caused damage or loss to client by breach of operation rules.

(c) Organization and personnel management

① Independence and neutrality

For constant and long-continued security and reliability, Time-stamp Authority is recommended to be independent as much as possible from short-term strategic influence of any specific corporation, agent or organization, and to stay neutral and fair.

② Professionalism

Time-stamp Authority is preferred to be with professional staff of information security and system audit, in order to realize constant operation with high security and reliability, appropriate and sufficient adaptability to advanced technologies, and quick response to problems.

③ Organization

An organization of Time-stamp Authority needs to meet the following requirements:

- Department possible to deal with critical data is organizationally isolated.
- Each department has function of internal restraint in order to prevent accidents.
- Restraining functions such as audit by external organizations are properly performed.
- Cause of accident can be identified.

(d) Financial basis

A financial collapse of the business means a crisis of secret key management, which is the reliability basis of the issued time-stamp tokens. Therefore, Time-stamp Authority must be operated and retained on a financial basis sufficient enough to afford positive reliability by: secure equipment and facilities; professionals and experts of time-stamp, cryptography, computer and law; development and operation of sophisticated and secure time-stamp system; and compensation for damages.

(e) Disclosure

For better trust by clients, Time-stamp Authority must positively disclose or make public its management, technical and operational information within a range that security is not affected. Disclosure system for emergency case should be also necessary.

The following information must be disclosed.

① Management information

Management information including financial status must be disclosed or made open to public for clients' conviction.

② Technical information

Technical information must be disclosed or made public as possible for clients' conviction of Time-stamp Authority's security and reliability. Technical information disclosure of time-stamp tokens before expiration of verifiable period should include technologies used in the past.

③ Security measures enforcement information

Periodical audit results on security management (measures against unlawful operation, authority dispersion, education of staff, etc.) must be disclosed or made public for clients' conviction of Time-stamp Authority's operational security.

④ Operation rules

Operation rules based on this guideline must be open to public.

⑤ Rules for service users

Rules for service users defining service contents and damage compensation policies must be made public.

(f) Confidentiality

Information that may affect Time-stamp Authority's security and reliability must be properly managed with information system's instant and wide accessibility in mind.

① Confidentiality of security-related information

Such confidential information as operator identification, operational system, machine room plan, audit information, and equipment and system security must be handled according to carefully defined rules, observation of which is appropriately reviewed.

② Confidentiality of client information

To prevent inappropriate use and leak, client information must be handled according to its secrecy rules, observation of which is appropriately reviewed.

(g) Service suspension and discontinuation

Suspension or discontinuation of service must be publicly informed or notified to clients with a defined schedule and rule.

No suspension must be without prior notice to clients, except for emergency halt by an

unexpected interruption.

(h) Client's personal information

① Information use

Time-stamp Authority must not use personal information supplied by clients beyond necessity of service provision.

② Disclosure of purpose

The purpose of personal information use must be defined in operation rules and made public.

③ Disclosure of personal information

Time-stamp Authority must not disclose personal information about clients, except for the cases that:

- Client or its representative demands disclosure of the client's registered personal information. Time-stamp Authority must prepare personal verification rules, which must be implemented before the disclosure in such cases.
- Disclosure of personal information is demanded by statute, or client agrees to the disclosure within a legal extent.

④ Access control

Access to clients' secret information must be limited to authorized personnel in order to maintain secrecy.

⑤ Storage

- Time-stamp Authority must provide itself with a system to secure safe storage and use of clients' secret information, in order to prevent alteration, deletion, leak, etc.
- It is recommended that clients' secret information should be backed up for prevention of loss in fire, etc.

(i) Audit

Time-stamp Authority must record service operation information, auditing it periodically in order to maintain system security and reliability.

① Definition of audit information

Audit information is the information needed in audit of operation rules, rules for service use, technical information, security measures, system event record, etc. The following are the details of audit information.

- Time source accuracy record and time audit record
- Record of the entire service process from distribution of service use rules to commencement of service, service contract termination or expiration
- Record of entrance to and exit from facilities and relevant admission record
- System operation record

- System performance record
- Account book access and disposal records

② Storage of audit information

Audit information must be protected against alteration, deletion, leak, etc. with clearly defined access authority, and stored to be available during a proper period of time where necessary. It is preferable that audit information should be backed up periodically and preserved in a remote storage.

③ Audit frequency

Audit must be conducted at least once a year.

④ Audit information storage period

Audit information must be stored for at least 10 years.

⑤ Disclosure of audit results and necessary action

Audit results must be disclosed as soon as it finishes. To defects and failures pointed out the following actions must be taken:

- Temporary measures until the defects are corrected (e.g. suspension of operation, adequate information to clients, etc.)
- Rectification of the defects

⑥ Storage of audit information and results

Audit information and audit results must be stored for a prescribed period of time with appropriate and reasonable measures against alteration, alteration, deletion, etc. by illegal access.

(j) Restoration from system trouble, compromisation or disaster

Unexpected interruption of time-stamp service may cause serious damage to clients. Therefore, actions in such events must be clearly prearranged for quick restoration.

① When accuracy of the time-stamp system has departed from the rated range, which shall be regarded as a system trouble, time-stamp server must be urgently stopped for restoration.

② Measures against destruction of hardware, software or data

Start restoration quickly using backup systems.

③ Equipment management in disasters

When equipment and facilities are damaged in disasters, operation must continue on spare equipment and backup data.

(k) Time source management and traceability

① Synchronization with standard time

The clock of time-stamp system must be synchronized with UTC.

② Time accuracy at Time-stamp Authority

Time used by all of Time-stamp Authority's systems must not depart more than 3 seconds from UTC.

③ Time accuracy at time-stamp server

Time at time-stamp server used by Time-stamp Authority's systems must not depart more than 3 seconds from UTC.

④ Time traceability

Time used by Time-stamp Authority for time-stamping must be kept traceable on UTC, by retaining time audit record conducted by TA or NTA.

6.2.2 Simple Protocol

(a) Key management at Time-stamp Authority[2]

Time-stamp Authority must securely and reliably manage the signature key pair for time-stamp token and encryption key in communication for their entire lifecycle.

① Key generation

- Key pair and public key must be generated by a reliable key generation system. It is preferable that the key generation system is installed within hardware security module.
- More than one manager must control generation of key pair and public key.

② Key storage

- Once generated, a key must be stored with its information elements separated from each other in order that any element can provide, by itself, no secret of the whole key, or it must be stored as a whole within hardware security module,
- When stored as separate information elements, each element must be preserved by an authorized individual.
- When stored as a whole within hardware security module, plural individuals must be authorized to preserve the key in order that it cannot be taken out by any single individual.

③ Use of key

- Public key and secret key must be kept within hardware security module when used for digital signature or decryption. When stored as separate information elements, the element loading to hardware security module must be operated in front of plural observers.

---

[2] Reference: *Certification Authority Guidelines* (V1.0), Authentication/Notary Working Group, Electronic Commerce Promotion Council of Japan, March 1998.

"http://www2.ecom.jp/report/pdf/H09/h9_cert2.pdf"

- When connecting hardware security module to time-stamp token generation system or preparing the key within the module for use, plural individuals must observe the operation.

④ Key preservation

- Public key in Time-stamp Authority must be preserved and protected from alteration, as it needs to be kept useable after its validity expiration.

⑤ Key disposal

- Secret key with expired validity and other keys over storage period must be disposed of to prevent illegal use.
- The disposal must take place in front of plural observers, making sure that one iota of secret information is not left legible.

⑥ Regular renewal of key

- A key must be given its validity period, which must be renewed regularly. The validity period is determined based on the policy of Time-stamp Authority.

⑦ Restoration of key compromisation and disaster

- Time-stamp Authority must provide itself with measures against the cases where secret key was leaked by illegal operation or deciphered by a third party, or damaged from disaster.
- When secret key has been or will be compromised, Time-stamp Authority must immediately revoke the key in question and start a procedure for the key made anew.
- When secret key has been compromised, time-stamp tokens generated with the key must be revoked all together.
- When secret key has been compromised, revocation of the key must be notified to clients or made public.

(b) Restoration of system trouble, compromisation and disaster

Unexpected interruption of time-stamp service may cause serious damage to clients. Therefore, actions in such events must be clearly prearranged for quick restoration.

① Measures to take when private key of time-stamp system has been compromised.

When invalidating time-stamp token, time-stamp tokens generated with the key must be revoked all together.

6.2.3 Linking Protocol

The following are operational standards for linking protocol-based time-stamp issuance service. (See 6.2.1 for operational standards not based on linking protocol.)

(a) Linking information management by TSA

- Generation of linking information

TSA must guarantee that TSA is generated in a secure management environment as mentioned in 6.2.1.

Linking information is the information generated by the following procedures:

A time-stamp user sends hash values to TSA.

The TSA receives the hash values for certain period of time and then integrates the hash values to generate new single hash value which represents all hash values from the time-stamp user(s). TSA calculates a linking information(t) utilizing the nearest previous linking information(t-1) and the newly generated single hash value. It is a hash value in relation with time, which can be used as data for future verification.

- Commencement of linking information generation

Linking information generation must be started in a physically secure environment as mentioned in 6.3, under twofold control by a TSA system administrator and a TSA management officer. The generation must take place in a reliable system whose security standards are guaranteed.

- Preservation of linking information

TSA must guarantee the integrity of linking information as long as its service is provided, by preserving it with a reliable system whose security standards are guaranteed. Accessing linking information needs agreement between the TSA staff member in charge and the TSA manager.

- Disclosure of linking information

TSA must disclose linking information periodically in order to prove its legitimacy. How and whom are of TSA's option provided that the following requirements are fulfilled.

✓ Requirement for acquiring linking information

Acquisition of linking information requires agreement between the TSA staff member in charge and the TSA manager.

✓ Requirement for disclosing linking information

To make it a well-known fact in public and unfalsifiable, linking information must be open to public in newspapers for at least one week. Drafts transacted with publishing companies must be kept secret from outside and preserved as long as the service period for them lasts.

- Audit of linking information

When implementing the audit defined in 6.2.1, relevancy of relation between the linking information disclosed and the linking information actually managed by TSA must be included in the audit information.

(b) Time-stamp record

TSA must guarantee that time-stamp record is securely issued with accurate time.

- Time-stamp record to issue must be given exclusive descriptor.
- Time value used for time-stamp record must be based on at least JST (Japan Standard Time) or UTC (Coordinated Universal Time).
- The time included in time-stamp record must synchronize with UTC with an accuracy range defined by TSA's policy. However, if the time-stamp record defines a time accuracy range of its own, the synchronization with UTC must be accurate within such a range.
- Time-stamp record must include data representation (e.g. hash value) to which time-stamp was given as instructed by the time-stamp demander.
- Time-stamp record must include data necessary for verification (linking information, intermediate hash value necessary to generate root hash value).

6.3 Infrastructure

6.3.1 Facility

Table 6-1 indicates the standards for facility where system for time business service is installed.

As the system for time business needs particularly strict management in terms of reliability, security and integrity, this guideline has applied the standards based on iDC use.

Table 6-1 Facility Standards

Category	Item	Achievement target	
(1) Building	Aseismatic (earthquake-resistant) standards	Fulfill standards for a building	Essential
	Base isolation	Earthquake-resistance, if seismic isolator adopted	Recommended
	Interior material	Non combustible Static electricity-proof	Essential
	Noise, EMC	EMC shield, etc.	Recommended
(2) Electric equipment	Redundancy	Double redundancy from intake to distribution/power panels Power-source inspection without power supply interruption	Recommended
	Emergency power generator	Secure redundancy larger than server area capacity (N+1) by gas turbine generator	Recommended
	Oil reservoir for generator	Capacity larger than refillable interval. Supply-control tank. Reserve capacity of more than 24h use.	Recommended
	Uninterrupted power supply system	Including 1 spare system for each group.	Recommended
	Fire alarm system	High sensitivity fire detection system.	Recommended
	Central monitor system	Covering all machines and equipment's operational condition. 24 h monitor available.	Recommended
	Grounding system	Integrated grounding system	Recommended
	Entrance/exit control	Combine IC card gate system and biometric system	Recommended
	Server room control	ITV monitor camera. No blind corner.	Recommended
(3) Air conditioning	Type	Blow low, draw high	Recommended
	Capacity	N+1以上 Over N+1 for every server area	Recommended
	Operation time	24 h continuous	Recommended
	Water leak detection system	Install in air conditioner's drainage area	Recommended
	Temperature/humidity adjustment	Temp：22～24℃±2℃Humid：50%±20%	Recommended
(4)Installation location	Rack	EIA standard 19 in. rack with locks on front and back.	Recommended
	Mount base	Fixed earthquake-proof or 2D or 3D base isolated mount base preferable	Recommended
	Installation location	Not in space shared with other system. Install in another room or enclose in a cage	Essential
	Double power source	Supporting 2-system distribution panel	Recommended
	Flooring material	Static electricity-proof	Recommended

(Reference: iDC Utility Guidelines,iDC Initiative)

6.3.2 Network

Table 6-2 indicates the standards required of network system for time business service. These standards simply indicate requirements for the network as an element of the system to provide time business services, not defining individual installation, hardware or software.

These standards are applied to both TSA and TST verification player.

Table 6-2 Network Standards

Category	Item	Achievement target	
(1)Connection with external network	Illegal access prevention	System to detect or protect from illegal access and attack from external network (e.g. Firewall). Measures against such attacks as service interruption, secret information theft, certification information theft, alteration, virus, etc.	Essential
	Server certification	Prove legitimacy by server certification. Provide clients with function to prevent wiretapping , alteration, etc.	Essential
	Time information acquisition	Use line service with constant quality without delay and not affected by other traffic.	Essential
	Connection with other networks	When connecting with plural networks outside, no IP reachability from one network to another allowable.	Essential
	Reliability	Redundancy is needed to line to connect to TA, and such devices as hub/switch, firewall, router This is not essential if the system as a whole secures the business continuity by, for instance, having a backup center separately.	Essential
	Measures against high load	Concentration of service and high traffic (massive service demands) cause no interruption of service provision except for permissive delay (e.g. load balancer).	Recommended
(2)Internal network (LAN)	Architecture	With servers and other equipment located in appropriate segment by service or by function, needless communications between segments can be blocked. Digital signature-related server and server storing time-authenticated information are installed in secure segments, with direct access from outside restricted.	Essential
	Reliability	System configuration (hub/switch, firewall, router, etc.) and LAN are redundancy-structured.	Essential
	Measures against high load	High traffic causes no interruption of service provision except for permissive delay (e.g. load balancer).	Recommended

6.3.3 Server Storage

Table 6-3 indicates the standards required of system for time business service.

These standards simply indicate requirements for the system to provide time business services, not defining individual installation, hardware or software.

Table 6-3 Server Storage Standards

Category	Item	Achievement target	
(1) System design	Extendibility	Front server is parallel-extendible, and capacity of time certification server and database server is extendible for future needs.	Recommended
	Function Division	NTP, time-stamp issuance, and verification service work on separate systems. Each system divides server by application.	Recommended
	Reliability	System redundancy, double power source, hot swap, UPS are introduced for higher reliability.	Recommended
	Availability	Measures for service continuity is taken using such technologies as load sharing, hot stand-by, clustering.	Essential
	Backup/restoration	Measures to ensure backup/restoration of system data and log data is taken using mirroring, clustering, and backup on movable media.	Essential
(2) Security	Access control	Refusal of needless access, needless application deletion, and needless port use cutoff are implemented to improve the server strength itself.	Essential
	Security control	Well-tested security patch adaptation, verification of file coordination, and system log recording are implemented for server's own security control.	Essential
(3) Quality control	Service quality	Servers for time business service are synchronized with UTC by using NTP, etc.	Essential
	System monitoring	Prepare a system monitoring system to watch CPU load, memory consumption, HDD resource and I/O use rate. The monitoring system is preferred to be equipped with function to monitor hardware defects and hardware interior temperature.	Recommended
	Defect control	Test environment, spare parts, etc. are prepared for response to unexpected events.	Recommended

Appendix 1 Terminology [Deleted]

Appendix 2 References [Deleted]

The Guideline Subcommittee Members

Chairman: Masahiro Honda

Keisuke Ichikawa	AMANO Corporation
Masahiro Honda	Asian Business Exchange Consortium (ABEC)
Yoshiyuki Kobayashi	NTT Communications Corporation
Takanori Fujiu	NTT Communications Corporation
Toru Sakurai	NTT DATA Corporation
Nobuyuki Mitani	NTT DATA Corporation
Kiichi Yamato	GOTDATE Co., Ltd.
Toshiaki Kojima	Kyokuto Boeki Kaisha, Ltd.
Satoshi Murayama	Sun Microsystems, K.K.
Toru Mukai	Seer Insight Security Inc.
Masakazu Uehata	Seiko Instruments Inc.
Koichi Shibata	Seiko Instruments Inc.
Keiji Shimano	Seiko Instruments Inc.
Tsukasa Iwama	Communications Research Laboratory
Yoshinori Onuki	Telecom Engineering Center
Ayako Komatsu	NEC Corporation
Yoshinobu Tanigawa	Hitachi, Ltd.
Toshiaki Shirakami	Marubun Corporation
Kazuya Miyazaki	Mitsubishi Electric Corporation

(In no particular order)

【Contact】

Time Business Forum (TBF) Secretariat

in

Support Center for Advanced Telecommunications Technology Research

Koike Bldg., 1-20-2, Shinjuku

Shinjuku-ku, Tokyo 160-0022

Tel +81-3-3351-8423

Fax +81-3-3351-6690

URL：http://www.scat.or.jp/time/