2-6 Trend of Time Business in Japan

IWAMA Tsukasa, SAITO Haruo, MACHIZAWA Akihiko, and TORIYAMA Hiroshi

Time Business in Japan started from the report of Ministry of Internal Affairs and Telecommunications of January, 2002. NICT participated in Time business from the beginning. In this paper, we describe the trend of Time business in Japan, research and development and standardization activity of NICT.

Keywords
Time business, Time stamping, Accreditation program for time-stamping services, International Telecommunications Union (ITU)

1 Introduction

Time business in Japan commenced with the "Study Meeting on Research and Development of Standard Time Distribution and Time Authentication Service Forum (commonly known as "Time Business Study Meetings")" held by the Ministry of Internal Affairs and Communications (hereinafter referred to as MIC) in January 2002. Held five times over January to June 2002, these Time Business Meetings developed a future image of the Japanese time business and methods to realize it[1].

Later in June 2002, the Time Business Forum was established in a joint effort by industry, academic associations and government, and from fiscal 2003 to 2005, MIC consigned NICT to conduct the "Research and Development of Time-Stamping Platform Techniques"[2][3]. Then in November 2004, MIC announced the "Guidelines Concerning Time Business; for the Safe Use of Networks and Secure Long-Term Electronic Data Storage"[4] based on the results of this research. As a result of this policy, the "Accreditation Program for Time-Stamping Services" was established in February 2005 in order to create a framework for a time-stamping system in Japan. In June 2006, the Time Business Forum concluded its activities after putting together the guidelines and systems for launching the time business. Consequently, the present Time Business Forum was established for the purpose of spreading awareness and developing time business.

Although NICT does not have a direct point of contact with users, it has been closely involved with the time business as the National Time Authority in Japan from the beginning. The activities of NICT mainly involve the participation in MIC policies and the International Telecommunications Union (ITU). One of the main activities regarding MIC is the above motioned "Research and Development of Time-Stamping Platform Techniques". This is not conducted merely to formulate policies for MIC and the "Accreditation Program for Time-Stamping Services," it also provides great support creating an actual time business foundation for actual services and partnerships with companies.

The activities regarding ITU commence with making proposals concerning research on how to ensure reliable time utilizing the Time Stamp Authority to the ITU-R SG7 WP7A meeting in 2000 as a Question from Japan. After being modified, this Question was adopted as "Question ITU-R 238/7 Trusted Time Source for Time Stamp Authority". Furthermore, in

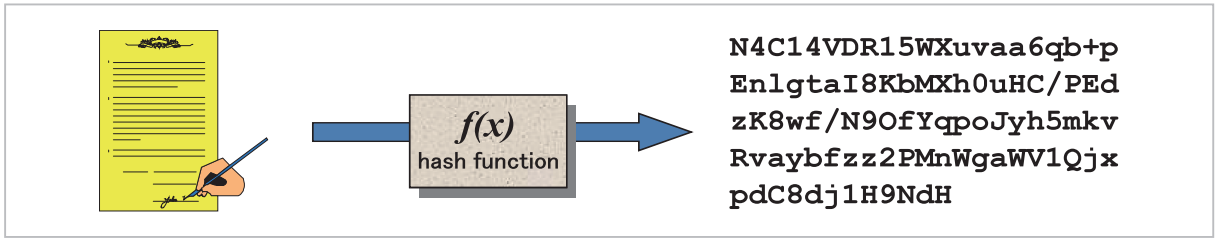

Fig.1 *Hashing of electronic documents*

September 2009, NICT submitted a recommendation proposal to the ITU-R SG7 WP7A meeting regarding the above time stamping system and after some reviews of the wording, it was sent to SG7. At the September SG7 meeting, it was determined that procedures for the adoption of this recommendation proposal in document form be conducted by all participating member states and it was adopted by SG7 in January 2010. Consequently, the ITU-R immediately commenced approval procedures and the recommendation proposal was approved as Recommendation ITU-R TF. 1876 in April 2010.

Since NICT submitted the Question to ITU ten years ago and the passing of eight years or so since the Time Business Forum, time business in Japan is now beginning to develop strong roots in Japanese society as a business. In this paper, we will examine the past ten years of the time business in Japan and its direction in the future.

2 The time-stamping structure

2.1 Threat in electronic documents

Prior to discussing time business, we will provide an outline of time stamping, the central technology of time business.

Electronic documents which have been created using PCs and digitized paper documents using scanners, etc., can be duplicated (copied) several times without losing quality, and such documents have the benefit of being capable of being reproduced by anyone who has the right software (hereinafter such documents are collectively referred to as "electronic documents," unless specified otherwise). However, on the other hand, third parties can easily alter and fake such electronic documents.

The altering and faking of such documents is a large threat to the networks of an information distribution society and in order to prevent these acts, electronic signatures and time stamps have proved to be effective.

2.2 Electronic signatures and time stamps

Electronic signatures and time stamps are used in both Japan and around the world. They are a type of technology that evidences the originality of electronic documents by cryptographic technology.

As shown in Fig. 1, electronic signatures initially randomly convert electronic documents into fixed data of a certain length using one way hash function (hash value). This converted hash value is known as message digest. Message digests are then encrypted with a secret key generated for the author of the relevant electronic document. Encryption using the secret key of the author is called a signature act and the encrypted message digest is called an electronic signature.

As shown in Fig. 2, electronic signatures can evidence the "who" and "what" by using cryptographic technology that evidences safety for the generation process and encryption of

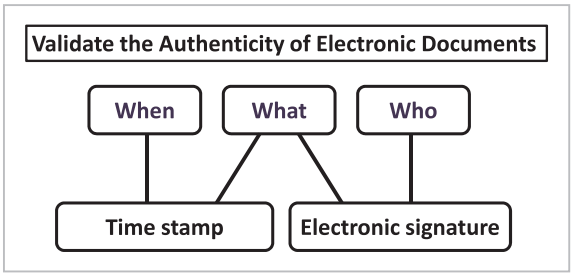

Fig.2 *Authenticity of electronic documents*

the message digest.

On the other hand, for time stamps, although the initial random electronic document message digests are generated in the same manner, these message digests are sent to the Time Stamping Authority (TSA) to generate time stamps. The TSA then adds time information to the digest messages and issues time stamps. These time stamps can evidence "what" was created in the same way as electronic signatures. However, as opposed to electronic signature, time stamps evidence "when" electronic documents were created, not "who" created the electronic documents. The organization for time stamps is shown in Fig. 3.

As shown in Fig. 2, by combining electronic signatures and time stamps, the "when", "who" and "what" can all be evidenced. This evidences the "authenticity" of electronic documents or in other words, it evidences that "the author, creation time and created electronic document or paper document is the same as the digitalized document and not a fabrication".

It is in this way that electronic signatures and time stamps technologies ensure the safety of electronic documents based on cryptographic technology. However, on the reverse side, there is a large impact if any vulnerabilities occur in the cryptographic technology. An actual example of this impact is discussed in the "Time Business Accreditation Center".

3 The commencement and expansion of time business

Here we will discuss the transformation of time business in Japan from its commencement until the present focusing on the role played by each of the related associations. The activities relating to time business can be broadly classified into the commencement stage from 2002 until 2006 and the expansion stage from 2006 until the present.

2006 was the year that the new "Time Business Forum" took over from the industry association, the old "Time Business Forum". It is from this that the position of the relevant organizations can be understood.

3.1 Commencement stage

3.1.1 Time business study meetings

The relationship between the organizations during the commencement period is summarized in Fig. 4. Although services such as time stamps existed before 2002, the unified time business in Japan commenced with the "Study

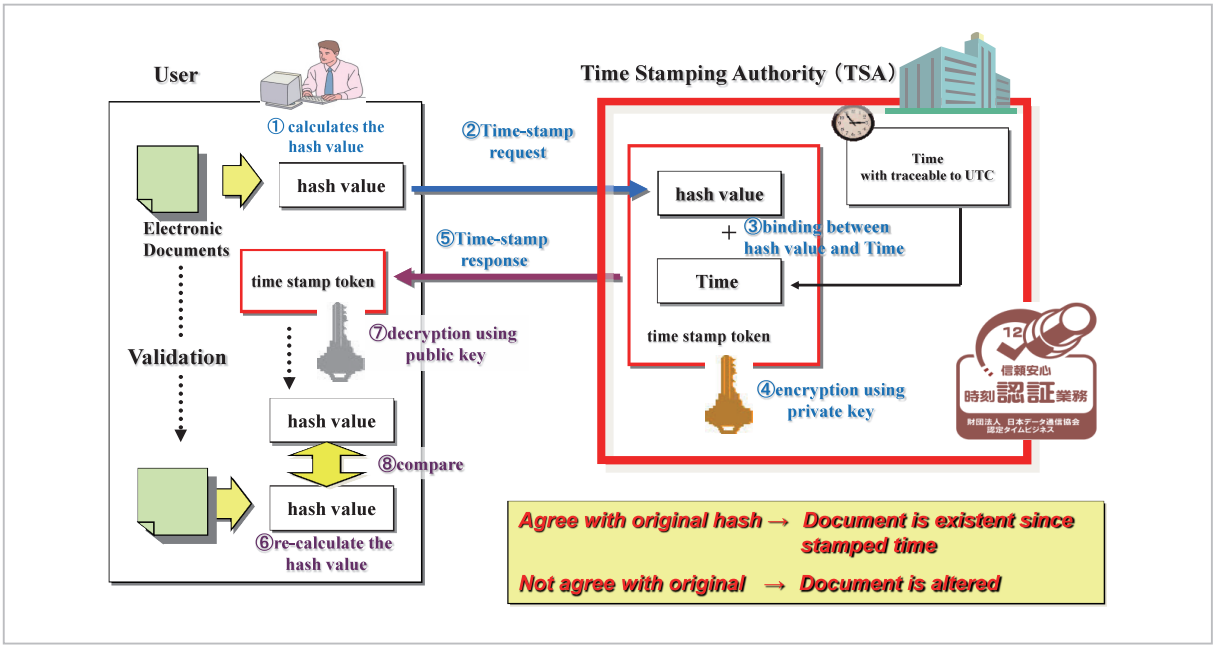

Fig.3 *Time-stamping structure*

Meeting on the Research and Development of the Standard Time Distribution and Time Authentication Service (commonly known as "Time Business Study Meetings")" held by MIC in January 2002.

The Time Business Study Meetings were held a total of five times during the period from January to June in order to build an information communications foundation for practical use in the IT society in view of "time business", and Mr. Shiomi from NICT participated as the director of the Time Business Study Meetings.

The Study Meetings actively discussed and prepared a report covering the following is-

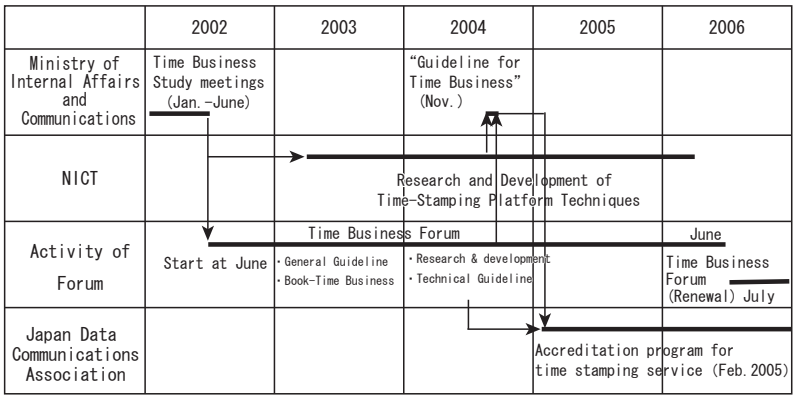

Fig.4 *Relationship between organizations on the commencement stage*

Fig.5 *A future image of time business*

(An excerpt from the report by "Study Meeting on the Research and Development of the Standard Time Distribution and Time Authentication Service")

sues.

- What is time business?
- What is the future of time business?
- The social and economical effects of time business
- Time business research and development issues and time business standardization issues
- Time business comprehensive promotion policies

The largest achievements of the Time Business Study Meetings were the establishment of time business as "business regarding 'time distribution' and 'time authentication'", and a future image of time business and the procedures to achieve this was clarified as shown in Fig. 5. The future direction of time business developed by the Time Business Study Meetings formed the basis of the time business in Japan.

At this time, "time distribution" was handled in the same manner as "time authentication (time stamps)". However, time distribution gradually became separated from the business side and time stamps became the main focus of activities.

3.1.2 The Time Business Forum

The Time Business Forum (hereinafter, "Forum") was established in June 2002 as a joint industry and academic association in order to develop time business for practical use in line with the direction formulated by the Time Business Study Meetings.

As shown in Fig. 6, the main structure of the Forum was divided into the two committees, namely the Technology Committee and the Planning Committee, and two working groups established under each of these committees. In addition, working groups were also created when necessary.

NICT held the position of general manager of the Demonstration WG established under the Technology Committee and performed based on it the research and development, etc., consigned by MIC discussed in **4**.

The Forum conducted activities for four years until June 2006. The main results of these activities are details as follows.

Publications

- *Time Business* (NTT Publishing: 2003)
- *Commentary "e-Document law"* (NTT Publishing: 2005)

Guidelines

- Time Authentication Infrastructure Guidelines (2003, English Language Edition 2003, 2nd Edition 2004)
- Time Stamp Operation Guidelines for "e-Document law" (2005)
- Time Stamp Long-Term Guarantee

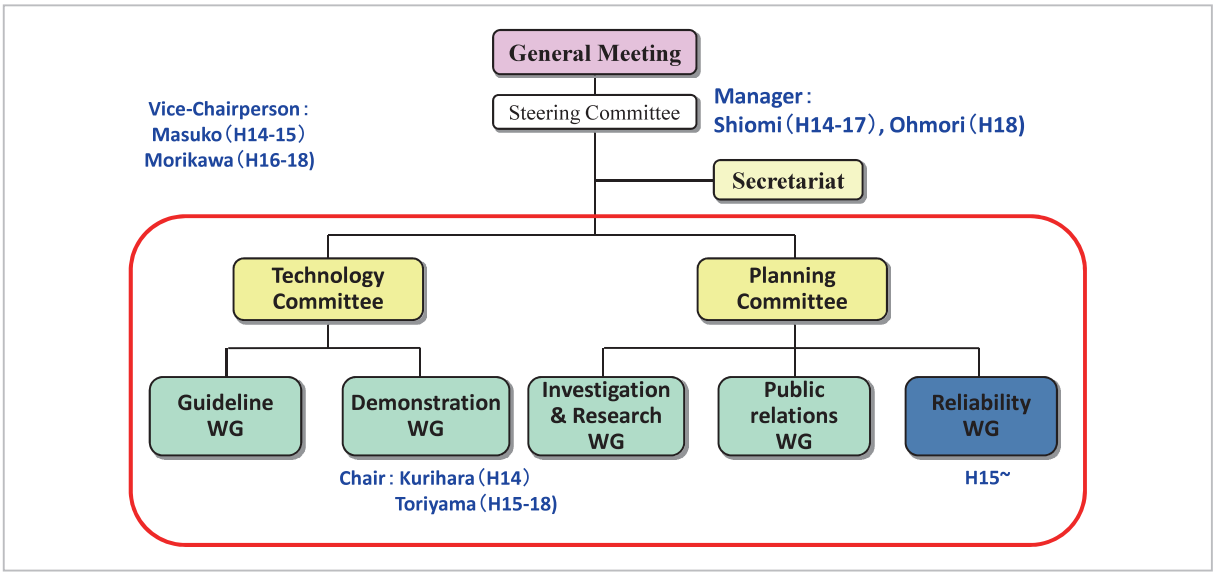

Fig.6 *Organization chart for the old time business forum*

Guidelines (2005)
- Technology and Operational Standard Guidelines for Reliable Time Authentication Infrastructure (2005)

Demonstration Reports (2005, 2006)

Investigation Reports
- Domestic Trends (2004)
- Germany (2004)
- Domestic and overseas (2005)
- United Kingdom, Hungry, Slovakia (2006)

Reports other than these can be still obtained from the Time Business Forum website[5].

In particular, the creation of the "Time Authentication Infrastructure Guidelines" was the first project performed by the Forum which provided the initial specific model for time business in Japan. The allocation of NICT (CRL at the time) to be the main provider of time distributions established it as the National Time Authority for time business in Japan.

The demonstration reports were the result of verifying the results of the "Research and Development of Time-Stamp Platform Techniques" conducted by NICT through the eyes of other members.

In November 2004, MIC released the "Guidelines Concerning Time Business; for the Safe Use of Networks and Secure Long-Term Electronic Data Storage"[4] based on the demonstration results, "Time Authentication Infrastructure Guidelines" and the results of domestic and overseas investigation reports.

The "Accreditation Program for Time-Stamping Services" was launched after the technical and operating standards were determined based on the "Guidelines Concerning Time Business" and "Technology and Operational Standard Guidelines for a Reliable Time Authentication Infrastructure".

Another major achievement of the Forum was the formulation and implementation of the "Utilization of Telecommunications Technology in Document Preservation, etc., Conducted by Private Business Operators, etc., Act" (general rules) and "Act for Revising, etc., the Relevant Acts Associated with the Enforcement of the Utilization of Telecommunications Technology in Document Preservation, etc., Conducted by Private Business Operators, etc., Act" (commonly known as "e-Document law")[5].

The "e-Document law" is a law that was enacted to enable private companies to digitalize documents and ledgers with obligations to prepare and preserve attached.

The "e-Document law" requires the "authenticity" of digitalized documents to be guaranteed. As discussed in **2**, electronic signatures and stamps can be used to provide such guarantees.

The Forum actively approached the relevant government departments and agencies in relation to the introduction of the time stamps in the "e-Document law". As a result, some documents such as national tax related documents, local government tax related documents and medical documents which are required to be preserved can now be electronically preserved using digital signatures and time stamps.

In June 2006 the Forum concluded its activities, leaving behind the legacy of the commencing of the "Accreditation Program for Time-Stamping Services" and the handling of the "e-Document law" and greatly contributing to the launch of time business and its initial expansion and awareness. From the following month, a new Time Business Forum was established and time business entered into its expansion stage.

3.2 Expansion stage

3.2.1 The Time Business Accreditation Center

Although electronic documents can now be preserved using time stamps pursuant to the "e-Document law," this does not mean that any time stamps can be used. According to the Ordinance Relating to National Government Tax Ledgers and Document Concerning the Medical Field[6] among individual laws enacted pursuant to the "e-Document law" (revision law), "time stamps relating to business accredited by

the Japan Data Communications Association" are required to be used.

This refers to "Accreditation Program for Time-Stamping Services" operated by the Time Business Accreditation Center of the Japan Data Communications Association.

As stated above, the "Time Stamp Accreditation System" was launched at the end of the commencement stage in February 2005. Since the Accreditation System maintains a fair screening function as an organization, it has established a System Consultation Committee (to evaluate and review the system) and an Accreditation Examination Committee (to examine the application conditions that are difficult for the Association to determine alone). Members of NICT have also been selected as committee members of these committees.

Examinations are conducted according to the following standards.

- Technical standards
- Operational standards
- Facility standards
- System safety standards
- Instructions to service participants and those relating to service participants

The technical and operation standards have been improved for practical use based on the Technology and Operational Standard Guidelines for Reliable Time Authentication Infrastructure created by the Forum discussed in the preceding Section. Normally, these standards would take the form of fundamental standards. However, although there are international standards for individual conditions such as the RFC3628 for the TSA policy conditions and ISO/IEC17025 for the granting of time stamps, there are no international standards for the distribution and monitoring of time. This will be further discussed in **4** but currently, the infrastructure for domestic and overseas standards is being promoted by NICT.

In addition, as discussed in **2**, since time stamping technology guarantees safety based on cryptographic technology, its vulnerability could be linked to the vulnerability of the accreditation system. Since the commencement of the accreditation system in fiscal 2005 until fiscal 2010, there have been two examinations conducted in regard to the vulnerability of encryption.

The first examination was conducted immediately after the commencement of the accreditation system in October 2005 until January 2006. This examined measures to address the problem of "SHA-1 collision difficulty vulnerability". As a result, from April 2006, "hash functions with a bit length of SHA-246 or more must be used" when hashing electronic documents were added to the standards.

The second vulnerability concerns the "SHA-1 and RSA1024 encryption algorithm vulnerability" issue which is still being conducted at the time of writing this paper in 2010. Although, in regard to these vulnerabilities, the Cabinet Secretariat Security Center, etc., are currently formulating a transition schedule for electronic signatures aimed at completing creation by the end of fiscal 2014, the transitional schedule for time stamps has been brought forward to the end of fiscal 2013 and transition preparations have already commenced.

While the "Accreditation Program for Time-Stamping Services" is a private sector accreditation system, it is currently a systematic time stamping system which forms the core of time business.

3.2.2 Time Business Forum (TBF)

Following the disbandment of the Forum, the new Time Business Forum (hereinafter, "TBF") was established in July 2006 in the aim of developing a user-friendly reliable time business, and promoting its expansion time throughout society in a transparent manner by building on the achievements of the Forum.

The structure of the TBF is shown in Fig. 7(a). This shows that the initial structure places importance on conducting examinations of the field of use in the aim of expanding practical use.

In addition to the April 2005 "e-Document law," each government department incorporated time stamps in their digitalization initiatives. For example, in March 2005, the Ministry of Health, Labour and Welfare released the "Security Guidelines for Health Information Sys-

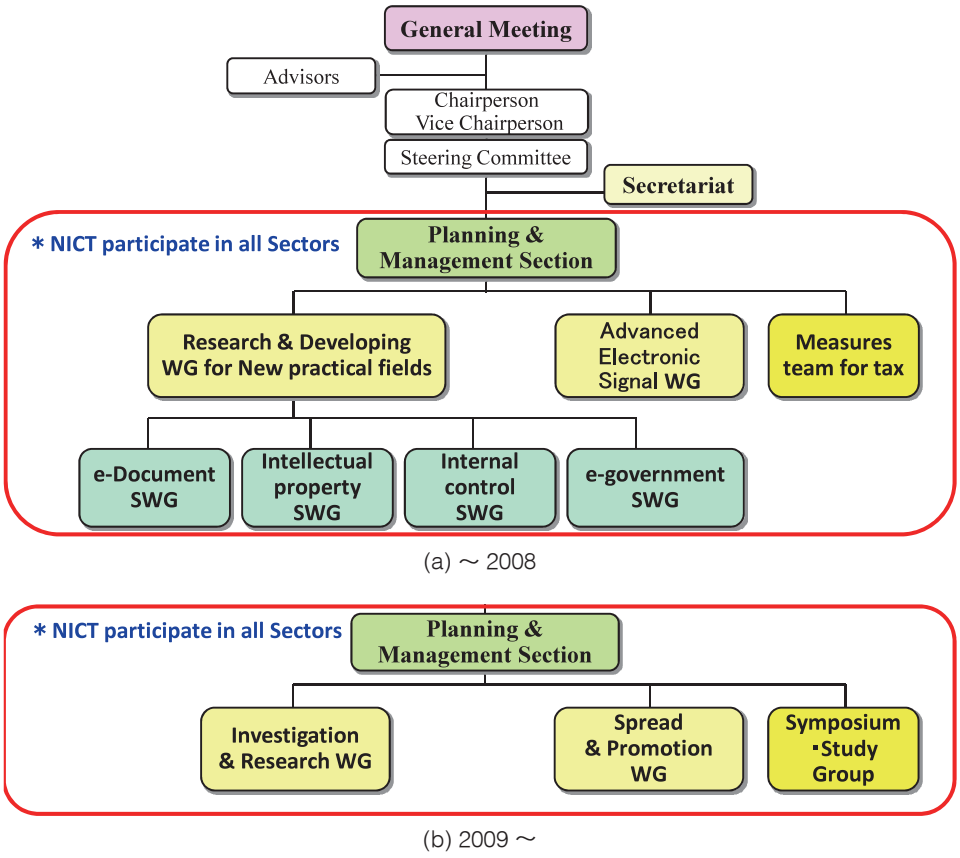

Fig.7 *Organization chart for the TBF*

tems" and in June 2006, the Patent Office released "On Guidelines for Prior User Rights System (Case Report) 'Towards Smooth Use of Prior User Rights System; for Strategic Know-How Management'".

However, the expansion of time stamping is not only attributable to the guidelines formulated by governmental departments and agencies, but is also a result of the efforts made by the corporate world represented by TBF. For example, as stated in the "2006 'e-Document law' Working Group Annual Report," the results of market research were analyzed and policies were created in the aim of furthering expansion. In addition, not only guidelines targeted at providers have been created as a policy to expand the utilization of time stamps. Numerous guides in form of cartoons, such as the "Time Stamp Utilization Guide for Intellectual Property" created in 2007, and easy to understand pamphlets aimed at users have also been created.

Even though the economy slowed down as a result of the Lehman shock in the second half of 2008, as shown in the "Time Stamp Utilization Examples[7]" published in 2010, the number of companies that have started to use time stamps has increased from 2008 as a result of these policies.

After the Forum became the TBF, the relationship with NICT also changed. At the time of the Forum, NICT held the position of Committee Vice-Chairperson and WG Director and an almost managerial position due to its relationship with MIC. However, after becoming the TBF, the Forum has become an almost private sector organization and NICT has been performing activities as a participant.

Regardless of this, from fiscal 2007 until fiscal 2008, NICT submitted a research proposal to the TBF in regard to the possibility of realizing the "Managed Time-Stamping Service

(MTS)" in order to create a client-side time authentication system for clients, and following a joint examination at the working group level, NICT and the TBF have conducted joint activities such as making proposals to the Time Business Accreditation Center.

Since it is difficult to link the activities of the TBF with profitable activities for companies and as a result of the downturn in the economy, the activities of the TBF underwent a major review in fiscal 2010. Consequently, the TBF is scheduled to re-commence its activities with a more streamlined structure in fiscal 2011 as all the participating companies have approved the significance of the organization's activities.

4 NICT activities

4.1 MIC sponsored research

In response to the direction specified by the Time Business Study Meetings and the fact that the necessity of ensuring the safety and reliability of information communications systems has been particularly mentioned in the information communications field that is one of the four important areas of the "Fund Allocation Policy for Budgets and Human Resources, etc., regarding Scientific Technology in Fiscal 2003" formulated by the Council for Science and Technology Policy, NICT was commissioned by MIC to conduct the "Research and Development of Time-Stamping Platform Techniques" in Spring 2003 as research and development that contributes to ensuring safety and reliability, and the Time Application Group has taken the initiative on research and development..

NICT raised the following three technical issues and performed system development in order to establish the "Time-Stamping Platform Techniques".

- Research and Development of highly accurate time distribution technology
- Research and Development of highly reliable time authentication technology
- Research and Development of high speed time authentication technology

Since this system is not technology containing independent elements but functions working together, as shown in Fig. 8, the time stamp platform system was developed and the functions verified.

Furthermore, security guidelines for time stamping were created and the security of the whole time stamp platform system was evaluated in order to evaluate the system with various information security issues.

The research results are briefly summarized below.

4.1.1 Research and development of highly accurate time transmission technology

Due to the different time authentication protocols formulated for the research and development of the highly reliable time authentication technology discussed in ***4.1.2***, the time stamp platform system contains two types of time distribution and authentication formats, namely the "linked authentication format" generated from the Nation Time Authority NTAI, Time Authority TA1, Time Stamping Authority TSA1 and TSA 2 and the "time link format" generated from the NTP (Network Time Protocol) server as shown in Fig. 8. Although the opposite side authentication and monitoring formats are different, both formats utilize NTP in the time distribution protocols.

The "linked authentication format" consists of NTA 1 in Koganei City, Tokyo, TA1 and TA2 in Chiba City (Makuhari), Chiba Prefecture, and TSA1 Tsukiji, Chuo Ward, Tokyo and each station is connected by ISDN 64 kbps. Although the ratio for the time difference that exceeds ± 1 millisecond within a one week measurement period in time distribution between NTA1/TA1 was approximately 4%, this is considered to be sporadic interruption handling within the used equipment. In addition, ±10 milliseconds was not exceeded in time distribution from NTA1 to TSA1 and TSA2.

The "time link format" consists of NTA2 and TA2 in Koganei City, Tokyo and the NTP server in Shinbashi, Minato Ward, Tokyo and these are connected by an up and down symmetric internet connection. Since this utilizes

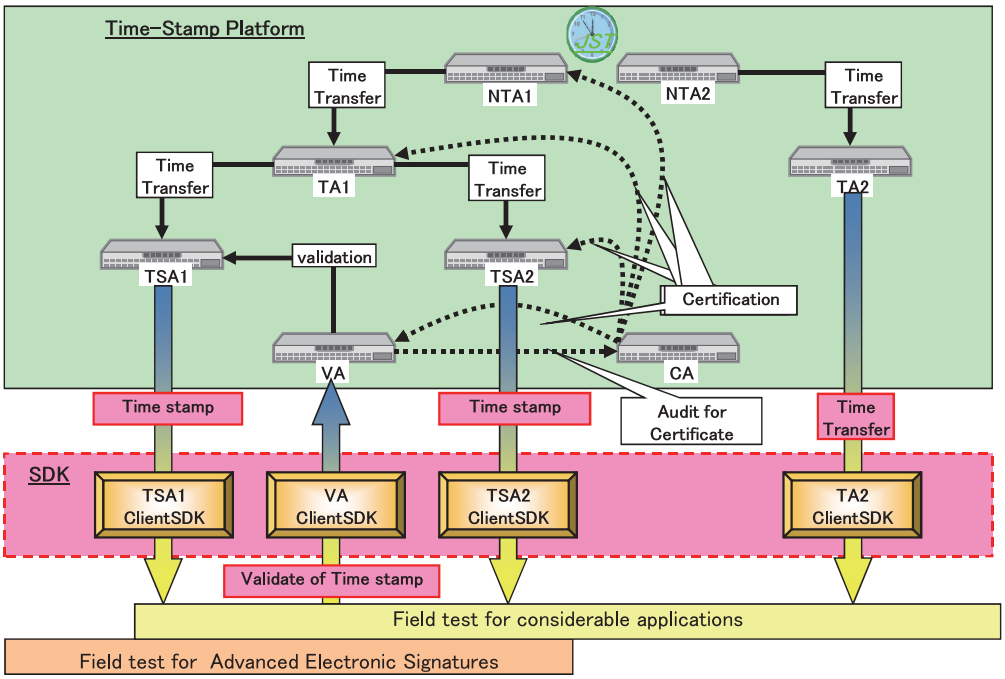

Fig.8 *Structure chart for the time-stamping platform system*

an internet connection, it may be affected by the volume of traffic but this was kept within approximately 1 millisecond. In addition, even when 1 millisecond was exceeded using a direct 10 Mbps local connection, this was mainly caused by interruption handling. Furthermore, as expected, the time difference between NTA2 and the NTA server did not exceed ±10 milliseconds.

These results show that the time difference did not exceed ±10 milliseconds from NTA to TSA in either format. Furthermore, the measurement results show that the cause of the degradation of time accuracy is caused mainly by unnecessary traffic on the network and interruption handling from other programs in the devices.

4.1.2 Research and development of highly reliable time authentication technology

The time stamp platform system adopted the "linked authentication format" and the "time link format" for the time distribution and authentication formats due to the different time authentication protocols. The "linked authentication format" issues both archive type time stamps utilizing linked information using TSA1 and PKI type time stamps using TSA2. PKI type time stamps verify the transmission route and time differences at the time of verification by sequentially granting time stamp tokens as a time audit certificate including time information in each station. Furthermore, in regard to archive type time stamps, the transmission route and time difference can be verified by viewing the time audit report publicly disclosed by the TSA at the time of verification.

In addition, a time stamp verification authority (VA: Verification Authority) has been established as a means for users to conduct time stamp verifications without being aware of the differences in these time stamp formats. Regardless of the differences in the above time stamp formats, the transmission route and time differences can be verified in line at the time stamps are verified by utilizing VA.

Incidentally, NTT Data Corporation currently utilizes archive type time stamps as accreditation time stamps. Furthermore, Seiko Instruments, Inc. has improved time audit cer-

tificates that include time information developed using PKI type time stamps and utilizes this as accreditation time transmission format.

The "time link format" generates time differences, generating institutional information and previous electronic time evidence hash values, etc., at the time of receiving transmissions in addition to the time information contained in time evidence utilizing time verification, and these are transmitted with the time evidence in the NTP packets. Hash links are generated in each station using the time evidence hash values generated at each station and the time evidence hash values sent from each station. These hash links can detect any alterations made to time evidence since they contain time evidence sent from each connected station. The "time link format" enables time evidence to be entered in to logs of the NTP server, etc., and time differences, generating institutional information and transmission route information can be verified in addition to the detection of alterations through later information containing time evidence.

Although the "time link format" was developed through research on the mail relay server in fiscal 2006, it has not yet been put into practical use.

Both the "linked authentication format" and the "time link format" contain technology that evidences the time such as transmission routes and time differences generated on the NTA. In addition, the creation of VA enabled time stamp verification regardless of the differences in the time stamp formats and provided the function that extends effective terms on the occasion of impending expiration of time stamps, which established the system for boosting convenience for users.

4.1.3 Research and development of high speed time authentication technology

TSA2 was developed for the time stamp platform system. This issues TSA1 and PKI type time stamps which issue archive type time stamps utilizing linked information.

Since TSA1 cleared the bottleneck caused by large amounts of transactions being processed, it became apparent that the communication overheads between the processes in the server were a major cause of disruption. Consequently, a maximum of 70,000 time stamps can now be processed each second due to revisions made to these processes. However, through security improvements such as doubling hash functions and adopting HTTPS communications based on the ***4.1.4*** "Time Stamp Platform Security Evaluation" and through the processing emphasizing reliability such as recording the issuance of each time stamp in the database, approximately eighty time stamps can be processed every second. These security improvements to the system and processes that emphasize reliability are overly exaggerated specifications and in regard to safe processing, there is more room to improve speed by increasing the speed of the DB devices, etc.

Since TSA2 cleared the bottleneck caused by large amounts of transactions being processed, it became apparent that the increase of processing speed in the HSM (Hardware Security Module) was a major cause of disruption. Consequently, by improving the algorithms to process the areas that were not found to be problematic during the ***4.1.4*** "Time Stamp Platform Security Evaluation" at high speed, 130 time stamps could be processed every second when eventually using 1024 bit signature keys and 26 time stamps could be processed every second using 2048 bit signature keys in order to increase the safety of time stamps. Furthermore, since the HSM processing capability has increased ten times or more, 500 or more time stamps can be processed every second using 1024 bit signature keys and 100 time stamps can be processed using 2048 bit signature keys in order to increase the safety of time stamps when converting the TSA2 processing capability to the performance of HSM currently available on the market.

Although these speeds could be considered quite low according to current standards, they are approximately ten times faster than the speeds at the time the commissioned research commenced.

4.1.4 Time stamp platform security evaluation

This item is a research and development item quickly established based on the instructions of the evaluation committee at the time of the mid-term evaluations.

Here NICT conducted a security evaluation based on the concepts of the international standards ISO/IEC 15408 regarding the security evaluation of the time stamp platform system. The TOE (Target of Evaluation) for each subsystem of the time stamp system was clarified according to the "Comprehensive Platform Security Evaluation Guidelines" formulated by NICT and a security evaluation of the TOE was conducted.

The main TOE items are specified below.

- Encryption components
- Time information
- Unauthorized internal access
- The threat of being unable to verify time stamps in the future.

The first two items can be addressed with technology but the last two items need to be addressed with technology and operations.

Although the authentication speed (***4.1.3***) decreased as a result of the evaluation, system safety was enhanced. However, since the evaluation was a system that attached overriding importance on safety, safety, performance and economic factors need to be considered for the actual creation of the system. Furthermore, some of the guidelines for this security evaluation have been incorporated in assessments of the current accreditation system.

4.1.5 Time stamp platform experiments

As shown in Fig. 9, experiments utilizing the time stamp platform system involved the system being placed over a wide area, the use of applications in various fields and the clarification of issues such as the evaluation of practical use from the user's perspective, and the required technology and operation. In addition, these experiments involved verifications of the technical and operational policies regarding the long-term guarantees of the effectiveness of time stamps prior to the expiration of the effective terms of the relevant time stamps and prior to the relevant time stamps becoming vulnerable.

The main experiment items are specified below.

- Electronic contract experiments
- Log server experiments

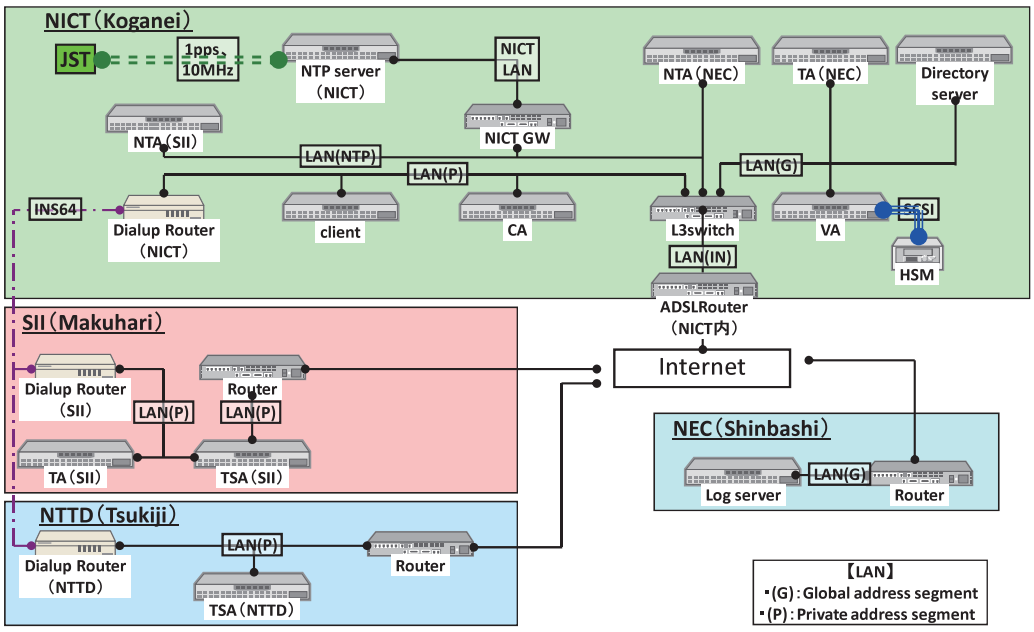

Fig.9 *Schematic for the time-stamping platform system*

- Long-term guarantee experiments utilizing archive type time stamps using link information
- Long-term guarantee experiments using VA

Please refer to the Forum demonstration report mentioned in ***3.1.2*** for the details of the results of these experiments.

Apart from VA, most of the experiment results have been put into practical use. In addition, as an extension of the VA experiment results, MIC has commissioned the TBF to conduct examinations on verification tools that can uniformly verify the various types of time stamps.

As shown in Fig. 4, the research and development of the time stamp platform technology not only contributed to the launch of the Accreditation Program for the Time Stamping Service, but also greatly contributed to the practical use of many technical elements and the launch of the time business in Japan.

4.2 Time business and standardization

4.2.1 Standardization by the International Telecommunication Union (ITU)

In September 2000, NICT (CLR at the time) submitted a Question to ITU-R SG7 WP7A Meeting (prior to the Time Business Research Forum) of the International Telecommunication Union (ITU) for standardizing time stamps. The ITU-R is the Radiocommunications Sector of the ITU, SG7 means Study Group 7 (for science services) and WP7A means Working Party 7 (for time signals and frequency standard emissions).

As stated above, since the granting and verification of time stamps involves cryptographic technology, standardization has been formulated by the RFC (Request For Comments) of the IETF (Internet Engineering Task Force), etc., in the internet industry, and some standardization has been formulated by the ISO (International Organization for Standardization) and the JIS (Japan Industrial Standards). However, definite standards for another important factor of time stamps, namely the reliability of time stamp time, have not yet been formulated.

Consequently, in 2000, the ITU-R SG7 WP7A Meeting received a research question from Japan regarding research of how to ensure the reliability of time used by Time Stamping Authorities. After some modifications, the Question was adopted and research was commenced under to heading “Question ITU-R 238/7 Trusted Source for Time Stamp Authority”.

Following this, in September 2002, NICT, as the National Time Agency, reported the structure of time stamp services in Japan as a standard for time to the ITU-R SG7 WP7A Conference, a matter that was discussed at the Time Business Study Meetings. Although this received strong interest from the participating countries, in particular European countries, no other countries submitted any subsequent reports.

Normally, although the ITU-R reviews questions approximately every four years and there was an opportunity to review this question in 2003 and 2007, several European countries have submitted proposals to continue this research.

As shown in Fig. 10, NICT submitted a recommendation proposal to the ITU-R SG7 WP7A Meeting in regard to the structure of the responsibility of TAs in Japan to transmit and audit time. Although this recommendation proposal was favorably received by each country and expressions were modified, such as changing the name of TA to Time Assessment Authority, almost the entire Japanese proposal was sent to SG7 and after being accepted by SG7 and completing the approval procedures of ITU-R, it was approved as Suggestion ITU-R TF. 1876 in April 2010[8].

The main arguments of the recommendation proposal are specified below.

- Each Standards Authority in the world must provide their UTC (UTC (k)) to the TSA with the required accuracy.
- The traceability UTC (k) time from TSA must be evidenced by continuous monitoring by TAA (Time Assessment Authority)

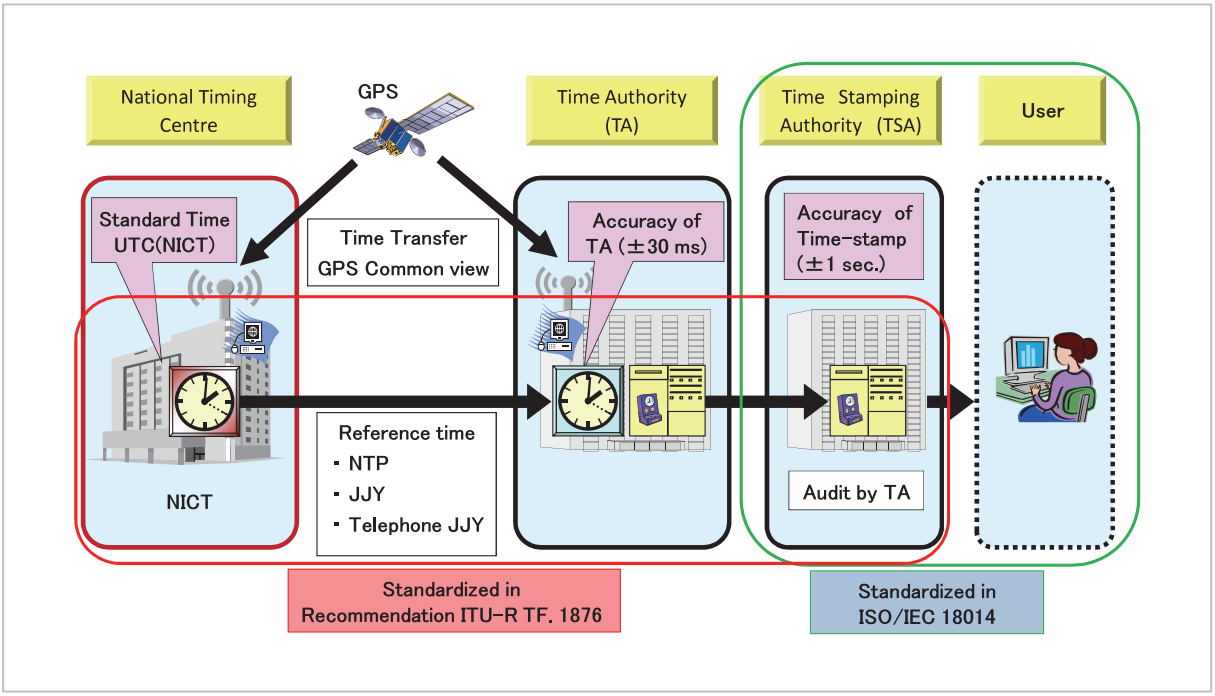

Fig.10 *Applicable scope for recommendation ITU-R TF. 1876*

- TAA should have the function to assess whether or not the required accuracy of the time used by TSA is being maintained.
- TAA is the function to be executed by National Time Authorities or Trusted Third Parties (TTP).

This is where the function of TA is defined. This is a function that encompasses the previous definition of an institution as a TA and is a more generalized concept. The introduction of the TAA concept laid the foundation of exporting the accurate Japanese style time stamps overseas. Of course, since this recommendation proposal only defines the function of TAA, it should be further enhanced in the future.

4.2.2 Standardization

Along with the standardization of the TAA function at ITU-R, from fiscal 2009, NICT commenced the formulation of the technical requirements regarding TAA as JIS in conjunction with the Japan Data Communications Association that operates the "Accreditation Program for Time Stamping Services".

Since internationalization was considered in the recommendation proposals of ITU-R, TSA does not need to use time provided by TAA. However, since TSA is obliged to use the time provide by TAA under the accreditation system in Japan, it is necessary to establish standards in line with the Japanese accreditation system. Furthermore, although it is noted in JIS, NICT is positioned as an institution which provides the standard time for Japan.

For JIS formulating work, the JIS Drafting WG drafted an original proposal, which was determined to be applied as a JIS draft version in consultation with the JIS Drafting Committee composed of experts. Thus, at the end of fiscal 2009, a JIS draft version was created and applied to the Ministry of Economy, Trade and Industry in charge of JIS as Application No. 12, the Industrial Standardization Act.

At the end of August 2010, the Planning Adjustment Working Group held a hearing in regard to the establishment of JIS and modifications were made based on the comments of the committee members and the matter was resubmitted. However, as of September 2010 (current), there have not been any major issues raised and it is anticipated that it would be standardized as JIS in the near future.

Furthermore, in order to provide the Japan time stamp structure overseas, international

standardization is required. Consequently, work to formulate it as ISO based on the current JIS proposal has commenced from the latter half of 2010.

5 Conclusion

Time business is a very new field that is barely ten years old. However, as a result of the rapid development of the high-speed information communications society and network environments, it is becoming an essential part of modern society. NICT has had a deep involvement and contributed to the development of time business from the beginning as the institution responsible for Japan Standard Time.

The safety of electronic documents has become an issue due to information leaks and alteration incidents in recent years. Furthermore, due to the clouding of networks, how to protect the security of electronic information remains a large issue. In view of this social situation, this area is predicted to grow even more both in Japan and overseas. As the National Time Authority in Japan, NICT needs to continue its efforts in the future in order to fulfill its responsibilities.

References

1 MIC, "Report of Research and Development of Standard Time Distribution and Time Authentication Service Forum (commonly known as "Time Business Study Meetings") —for the wide spreading of the Time Business—," Sep. 2002.

2 Time Business Forum, "Experimental report of the time stamp platform," May 2005.

3 Time Business Forum, "Experimental report of the time stamp platform," May 2006.

4 Reference; http://www.dekyo.or.jp/tb/summary/data/MICguideline041105.pdf

5 Reference web-site; http://www.dekyo.or.jp/tbf/seika/

6 Reference web-site; http://www.dekyo.or.jp/tb/

7 Time Business Forum, "Utilized examples of Time stamp," Journal of Japan Data Communications Association, No. 176, pp. 11–25, Nov. 2010.

8 ITU-R Recommendation TF. 1876, "Trusted Time Source for Time Stamp Authority," Apr. 2010.

(Accepted Oct. 28, 2010)

IWAMA Tsukasa, *Ph.D.*

Research Manager, Space-Time Standards Group, New Generation Network Research Center

Secure Time Stamping, Time Dissemination & Synchronization

SAITO Haruo

Expert, Space-Time Standards Group, New Generation Network Research Center

Time and Frequency Measurement

MACHIZAWA Akihiko

Team Leader, Information Systems Team, Information Management Office

Picture Coding, Visual Information Processing, Network Measurement, Time Synchronization

TORIYAMA Hiroshi, *Ph.D.*

Director, Information Management Office

Information Theory, Network Applications, Secure Time-Stamping