5-5 Development of the Trusted Time Stamping System

IWAMA Tsukasa, KURIHARA Noriyuki, IMAE Michito, IMAMURA Kuniyasu, KOTAKE Noboru, GOTOH Tadahiro, SUZUYAMA Tomonari, and MORIKAWA Takao

IT social infrastructures based on the "e-Japan Strategy" and the development of e-commerce are rapidly increasing. According to this trend, documents are changing from paper-based to digital data. If we use only digital-signature techniques for digital data, it is difficult to guard against fraudulent practices. We have found that time stamping techniques, which, when combined with digital signatures, provides an effective solution to this problem. In this paper, we present the results of our basic time-transfer measurements and future plans, which are needed by the National Time Authority.

Keywords
National time authority, Time authority, Time stamping authority

1 Introduction

The trend toward converting paper-based information into digital data is gaining momentum with the development of electronic commerce and progress toward an advanced information society, in line with the "e-Japan Strategy." When handling digitized information, we are faced with problems such as spoofing, alteration, and repudiation (a phenomenon in which the existence of an event is denied after the fact, as the name implies). Electronic signature technology alone, which has been intensively investigated, cannot solve such problems. To cite a few examples, it is difficult without accurate time data to prove the occurrence of an event such as issuance and reception; tampering by a third party may be prevented but the sender can modify the description; and the limitations to the effective term of the public key make it difficult to protect documents for long-term storage. These problems can only be solved by adding an accurate, accredited time to the signature. Proven time-stamping technology provides such accurate, accredited time.

As the organization responsible for the national time and frequency standards, the Communications Research Laboratory (CRL) has maintained Japan Standard Time, which is traceable to Coordinated Universal Time (UTC). However, the CRL has only provided accurate time; it has not accredited the time it provides.

A time-stamping system has already been shown to be commercially workable; however, such a system relies on GPS or the like as a time source. It is becoming increasingly necessary to use Japan Standard Time in place of such sources. CRL is now expected to serve as a national time authority (NTA), one that will not only supply traceable Japan Standard Time to the UTC but will also accredit—i.e., attest to the integrity of—the time it provides.

This paper describes the development of a time-stamping system that will be required for the CRL to serve as an NTA, and discusses the future challenges we will face.

2 Outline of the time-stamping system [1]

Fig.1 shows a conceptual diagram of the CRL time-stamping system. In this figure, the time authority (TA) and time-stamping authority (TSA) represent third parties that can be trusted (a "trusted third party," or TTP). Distinguishing itself from conventional time-distribution services, an NTA not only distributes time to TA and TSA but also audits the time, issuing a corresponding certificate. The NTA's roles in terms of these functions are summarized in Fig.2. The portion marked with a red arrow represents the new responsibilities accompanying the execution of a trusted time-stamping service. As an NTA developing such a service, the CRL must consider how it will assume these responsibilities. Accordingly, three major challenges must be addressed:

- Ensuring security,
- Ensuring time accuracy, and
- Issuing a certificate and storing the log.

We modified a system currently available on the market and conducted basic time-distribution experiments. Following are the details of these experiments.

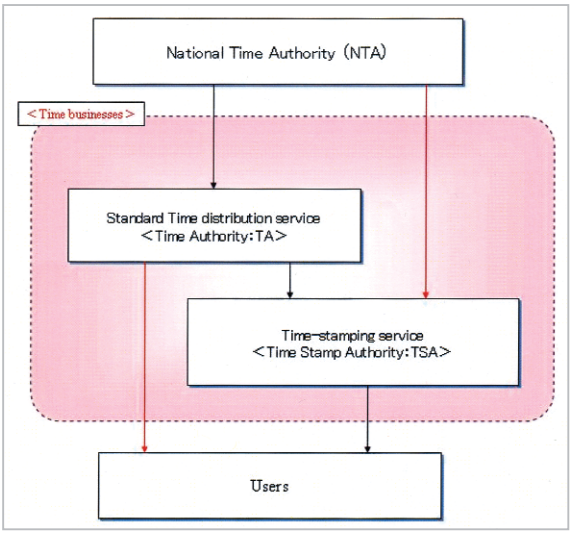


Fig.1 *Conceptual diagram of the electronic time-stamping system*

3 Basic experiment to evaluate standard time distribution[2]

Fig.3 illustrates the configuration of the basic experiment conducted to evaluate standard time distribution. The NMI server and TMC server employed were those used in the

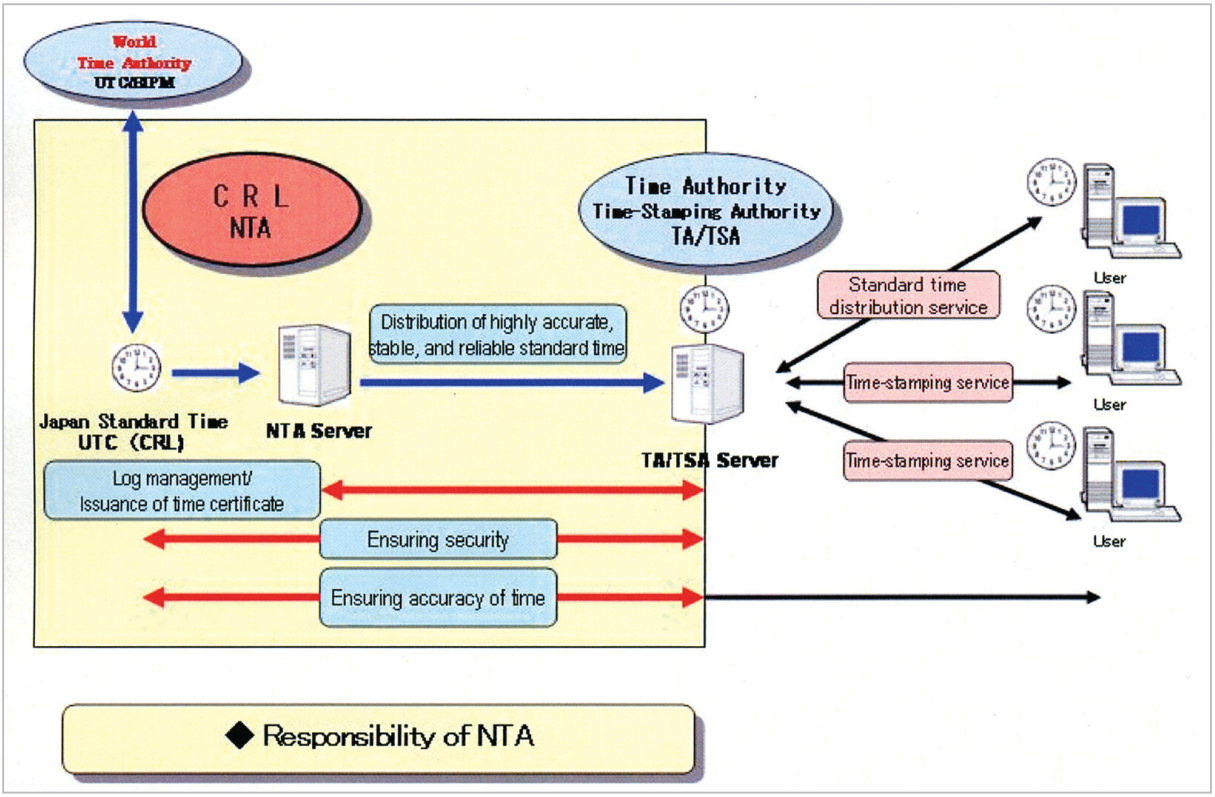


Fig.2 *Responsibility of NTA*

Datum (now Symmetricom) trusted time system. These servers feature a Rb oscillator as the internal clock. The NMI server is synchronized with UTC(CRL) and the TMC server is synchronized with the NMI server via telephone line using a clock relying on GPS.

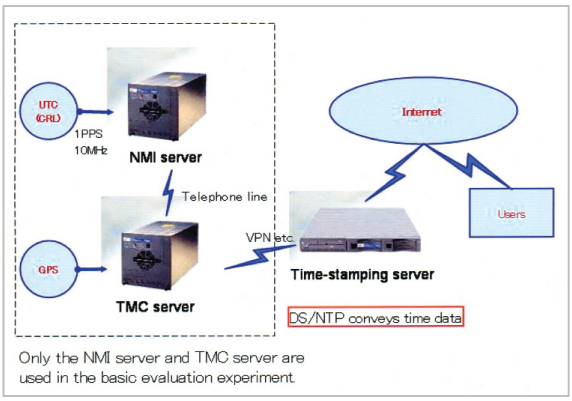


Fig.3 *Experimental system for the evaluation of standard time distribution*

The most common tool used for time synchronization among computers is NTP (Network Time Protocol). In the basic evaluation experiment we employed the secure time transmission protocol developed by Datum known as DS/NTP. The security of this protocol was enhanced through the use of a telephone-based public key infrastructure (PKI) as the basis of accreditation.

Fig.4 shows an example of measurement results obtained in a time-distribution experiment using the basic evaluation system. In this experiment, UTL(CRL) was linked directly to the NMI server, and the NMI server was connected to the TMC server through a telephone line via a circuit simulator. The time difference between the NMI server and the TMC server is indicated in yellow in Fig.4. The nominal specification for time synchronization in the TMC server is ≤10ms. Fig.4 shows a measured time difference of 0.1 ms, well within this specification.

To evaluate system error in the time-distribution experiment, we modified the delay time with the simulator and performed measurement using an NTT telephone line. No significant resulting difference was seen in the measurement results; we found that the basic experimental system could distribute time with an accuracy of 10 ms or less. Note that this experiment was to evaluate the accuracy of time distribution, not to assess the validity of time accreditation.

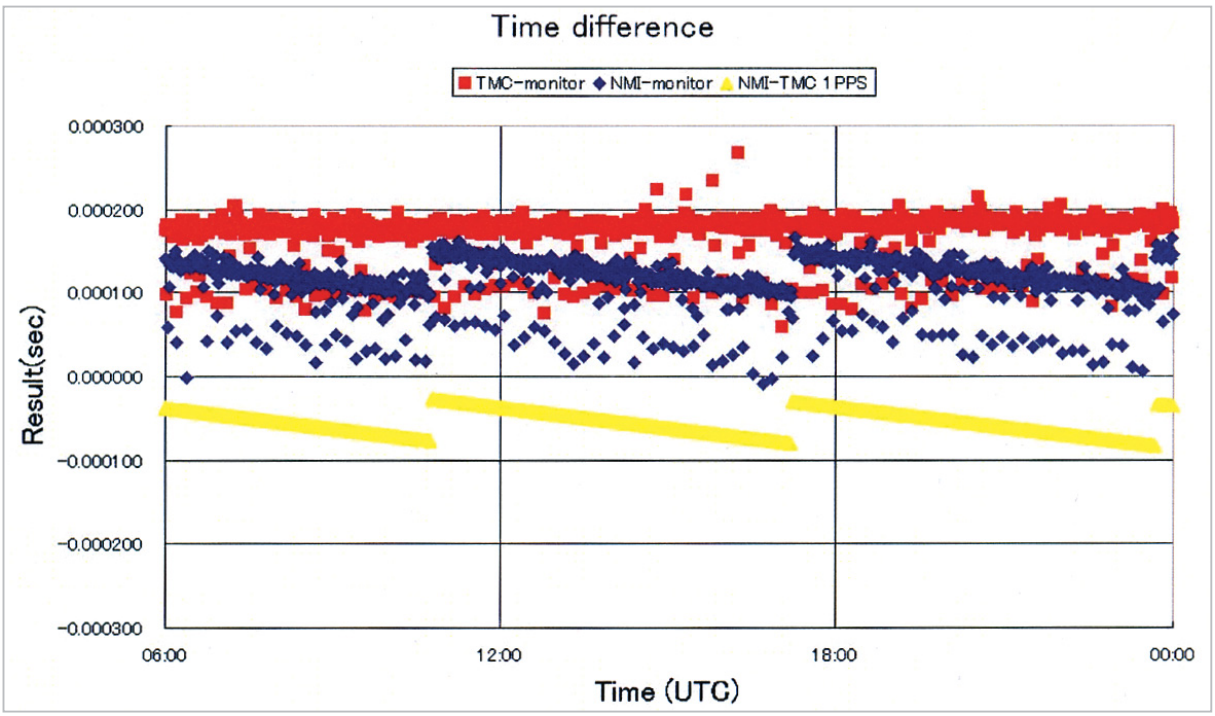


Fig.4 *Time-distribution experimental results*

4 Future challenges

Section **3** described an experiment relating to secure time distribution. This experiment established a method to ensure security and time accuracy, in accordance with the challenges listed in Section 2. However, if we are to provide commercial services as an NTA, we must examine delivered time further.

The remote calibration system investigated in **5-4-2** is useful in the assessment of delivered time. Using the remote calibration system, we will be able to examine the accuracy of time delivered to a TA/TSA and to conduct time accreditation, thus addressing the third challenge mentioned above: issuance of a certificate and storage of a log. Accordingly, we must consider the following items in the commercialization of a time-stamping system.

- Method of time evaluation using a remote calibration system
- Frequency of time stamping
- Ways of issuing a certificate
- Handling of the log

We intend to discuss such issues with TAs/TSAs, both in the Time Business Forum and at other opportunities.

The technique under investigation in the current study represents only one of various methods of time distribution; needless to say, it will be necessary to examine and develop alternative methods.

5 Conclusions

This paper has presented an overview of our trusted time-stamping system, addressing three specific challenges as well as additional issues to be addressed. We will continue discussions [3] with TAs/TSAs in connection with the Time Business Forum and on other occasions, to determine how we are to resolve outstanding problems and how we will share required information with TAs/TSAs as well as with public users.

We evaluated one method of time distribution; however, we did not investigate time accreditation. We intend to make progress on this and other issues through joint work with the Field Test Group of the Time Business Forum.

Development of the trusted time-stamping system is not proceeding as rapidly as expected. However, our goal is to commercialize the system, in cooperation with the Ministry of Public Management, Home Affairs, Posts and Telecommunications and the Time Business Forum.

References

1 Study Group on R&D of Time Validation and Time-stamping Services, "Towards the spread of time business—Report of Study Group on R&D of Time Validation and Time-stamping Services—", Jun. 2002. (in Japanese)

2 Imamura K., Gotoh T., Kurihara N., Imae M., and Iwama T., "Distribution of Japan Standard Time and Basic Experimental Results Using the Time-Stamp Infrastructure", Proc. of the 2003 IEICE general conf., D-9-5, 2003. (in Japanese)

3 Time Business Forum, "Time Authentication Infrastructure Guideline", Mar. 2003 (in Japanese). [Digest Edition were published in English at Sept. 2003]

The follow is also considered as reference.

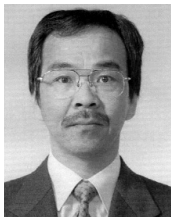
· Time Business Forum Homepage: http://www.scat.or.jp/time/index.html

IWAMA Tsukasa

Senior Researcher, Time Stamp Platform Group, Applied Research and Standards Division

Time and Frequency Standards, Mobile Communication

E-mail; iwama@crl.go.jp

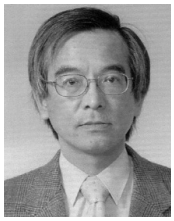


KURIHARA Noriyuki

Leader, Japan Standard Time Group, Applied Research and Standards Division

Time and Frequency Standards, Space Measurement

E-mail; kurihara@crl.go.jp



IMAE Michito

Leader, Time and Frequency Measurements Group, Applied Research and Standards Division

Frequency Standards

E-mail; imae@crl.go.jp

IMAMURA Kuniyasu

Senior Researcher, Japan Standard Time Group, Applied Research and Standards Division

Time and Frequency Standards

KOTAKE Noboru

Researcher, Japan Standard Time Group, Applied Research and Standards Division

Time and Frequency Standard

E-mail; kotake@crl.go.jp

GOTOH Tadahiro

Reseacher, Time and Frequency Measurement Group, Applied Research and Standards Division

GPS Time Transfar

***SUZUYAMA Tomonari**, Ph. D.*

Researcher, Japan Standard Time Group, Applied Research and Standards Division

Time and Frequency Measurement

E-mail; suzuyama@crl.go.jp

MORIKAWA Takao

Research Supervisor, Applied Research and Standards Division

E-mail; tak@crl.go.jp