The Leap Second's Effect on Society

Sep 19th, 2013

Japan Data Communications Association
Time Business Forum
Steering Committee Chair Koichi Shibata
AGENDA

- The importance of TrustedTime to the ICT
- Japan’s Time Business
- Accidents caused by the “Leap Second” in Japan
- The “Leap Second” in Time Business
- Review

With "Time Business", your information will be protected

~ Trustworthy Information is Essential ~
Scope: ICT infrastructure for secure information society

- e-Record Management
- Authentication infrastructure
- Digital certificate infrastructure
- Signature infrastructure
- Time Stamping infrastructure
- Public Key Infrastructure
- Trust Framework
- Trusted Time
- Time Synchronization
Information = the past phenomenon


“When”?

Can’t share unless be there

We must Record it!

Civilization of Info Recording ⇒ Writing, Printing, Microphone, Camera

Is it Correct?

Culture of Info Management ⇒ Signatures, Stamps, Seals, Archives, Memorandum, Contracts
The **Risks** and **Fixes** to Info Management

As Time Flows

Create  Register  Update  Verify  Finalize  Store  Use  Discard

Explosive Increase in Information
Involvement of Stakeholders
Absence of Authors
Secondary, Tertiary use
Is it all accurate?

Fraud
Aging
Error
Tampering

Coat information with the universal measure, Trusted Time = Time Stamping

Decay/Destruction
Loss of Legibility
Leakage/Misplacement
Searching Difficulties
Accidental Deletes

Copyright Time Business Forum, 2013
Time Stamp: Digital can Prove the "When"

Verifies that an digital document...

① Has existed before the stamped time
② Has not been modified after the stamped time

① Existed Before  →  ② Not Modified After

Combine Hashing & Trusted Time, create Time Stamp Token, attach to document

Dec 3rd 2006
Time Stamping at this time

March 19th 2012
Accurate

Backdating Not Allowed

Time Stamping protects the integrity of digital documents using the trustworthy resource, Trusted Time
Market Trend in Japan

- An increase in digital evidence
  Transition of trust from paper to digital

1998
  • Electronic account ledgers archive law

2000
  • Basic IT law

2002
  • **Digital signature law**
  • IT documents omnibus law
  • Private Information Protection Law

2005
  • **e-Documents law**

2006
  • Digital signature law (revised)

2008
  • Digital signature law (revised)

2010

2012
  Guideline for safe control of Medical information
  (Health, Labour and Welfare Ministry) Ver4.1

- E-signature formats for long term e-signatures based on RFC3126 has been enacted as JIS. CAdES, XAdES
- The intellectual property right: Patent Office guideline “to smooth use of the use right system ahead”.
- Scanner data allowed by time stamp and e-signature
- EDI: require time stamp & e-signature
- The guideline for safe control of Medical information provides for the method of fixing “When” “Who” and “What”
- CAdES:ISO 14533-1  XAdES:ISO 14533-2

Copyright Time Business Forum, 2013
February 2005, the Nippon Information Communications Association (NIC) established the voluntary accreditation program for time-stamping services. The program is based on the guideline of “time business” issued by MIC (Ministry of Internal Affairs and Communications) in November 2004, and is to approve if the services of a TA (Time Authority) and a TSA (Time Stamping Authority) meet the required criterions of the program. The criterions cover five fields, (1) technology, (2) operation, (3) facilities, (4) network security and (5) information obligations. Requirements for accreditation are: (1) Accredited TA & TSA must have business footholds and facilities & equipments for time business within JAPAN. (2) Accreditation is valid for 2 years and accredited TA & TSA must submit an application to NIC for the renewal. 

To enhance levels of time-stamping service provision and to contribute to the technical infrastructure of IT societies.
Trusted Time Traceability

Time Assessment Authority

Time Stamping Authority

Time Stamping Unit

Gate

USER

Internet

Time Stamp

TSR

ISDN

GPS Common View

National Time Authority

Telephone JJY

Time Check w/Gate Close

Time Check w/o Gate Close

Time Distribute w/Authentication
**Time Stamp Token (RFC3161/ISO18014/JISX5063)**

### Time Stamp Request
- version
- hashAlgorithm
- hashedMessage
- reqPolicy
- nonce
- certReq
- extensions

### Time Stamp Response
- status
- statusString
- failInfo
- timeStampToken

### Time Stamp Token
- contentType
- version
- digestAlgorithms
- eContentType
- eContent (= TSTInfo)
- certificates
- crls
- signerInfos

### SignerInfos
- version
- sid
- digestAlgorithm
- signedAttrs
  - ContentType
  - messageDigest
  - SigningCertificate
  - ESSCertID
  - ESSCertID
- signatureAlgorithm
- signature
- unsignedAttrs

### Certificate
- version
- sid
- digestAlgorithm
- signedAttrs
  - ContentType
  - messageDigest
  - SigningCertificate
  - ESSCertID
  - ESSCertID
- signatureAlgorithm
- signature
- unsignedAttrs

### Trusted Time

---

Copyright Time Business Forum, 2013
Standardize the traceability of trusted time

Trusted time source for Time Stamping Authority : **TAA (Time Assessment Authority)** has been defined as the international recommendation.

In April 2010, recommendation from Japan has been authorized as ITU-R **TF.1876** by ITU-R (International Telecommunication Union Radiocommunication Sector) SG7(Business Science).

**JIS X 5094:2011**…Technical requirements for TAA to certify TSA clocks of UTC-traceability

**ISO/IEC 18014-4** …Information technology - Security techniques - Time-stamping services - Traceability of time sources
- STATUS: Under development
- Stage: 40.00 (2013-06-13)
- TC/SC : JTC 1/SC 27 WG2
Law and Guideline included timestamping in Japan

National Tax Agency
The amended Electronic Storage Act in the 2005 tax reform bill

Ministry of Health, Labour and Welfare
Guideline: Safe management of medical information system

Japan Patent Office
Guideline: Effective use of prior use rights system

Ministry of Education, Culture, Sports, Science and Technology
Guidelines: Digitization of education records

Building Contractors Society
Guideline: Digitization of documents and drawings and archive about building work

Ministry of the Environment / Minister of Economy, Trade and Industry
Guideline: Information security measures for ASP/SaaS

Minister of Economy, Trade and Industry
Guideline: Pollution prevention for operators

Cabinet Secretariat
Guideline: Risk assessment and Electronic signatures and authentication for online procedure system

The Japanese Institute of Certified Public Accountants
Guideline: Confirmation by electronic media or route in audit

Law and Guideline included timestamping in Japan
Case Summary

Time Stamps are used in various fields in Japan.

Users’ needs are:

- non-Repudiation
- Right of Prior Use
- Accountability
- Misappropriated application
- Electronic document by scanner
- Record Authenticity
- Paperless
- Lawsuit Aversion
## Example of Timestamping Application (1)

### Transaction Doc, e-commerce

<table>
<thead>
<tr>
<th>User name</th>
<th>Purpose</th>
<th>Target data</th>
<th>Format</th>
<th>Commencing Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>JTB Corp.</td>
<td>Speedup operation and Operational efficiency</td>
<td>Written estimate</td>
<td>PDF</td>
<td>2005~</td>
</tr>
<tr>
<td>Murata Manufacturing Co., Ltd.</td>
<td>Speedup operation and Operational efficiency</td>
<td>From for foreign trade</td>
<td>PDF</td>
<td>2011~</td>
</tr>
<tr>
<td>AICHI Bank</td>
<td>Compliance for e-Doc law</td>
<td>Image Scanned….Request for account transfer, various notification, identification</td>
<td>PDF</td>
<td>2011~</td>
</tr>
<tr>
<td>NISHIJIN Hospital</td>
<td>Compliance for e-Doc law</td>
<td>Image Scanned….Receipt, agreement, written consent</td>
<td>PDF</td>
<td>2012~</td>
</tr>
</tbody>
</table>

### e-contract

<table>
<thead>
<tr>
<th>Username</th>
<th>Purpose</th>
<th>Target data</th>
<th>Format</th>
<th>Commencing Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS Solutions Corp.</td>
<td>Electric contract service</td>
<td>Contract</td>
<td>PDF</td>
<td>2010~</td>
</tr>
<tr>
<td>Toho Co., Ltd</td>
<td>Operational efficiency</td>
<td>Contract for movie contents</td>
<td>PDF</td>
<td>2011~</td>
</tr>
<tr>
<td>Edison Co., Ltd</td>
<td>Web Service of management for industrial wastewater</td>
<td>Contract for outsourcing of industrial wastewater treatment</td>
<td>PDF</td>
<td>2011~</td>
</tr>
<tr>
<td>Communication Plan</td>
<td>Electric contract service</td>
<td>Contract</td>
<td>PDF</td>
<td>2012~</td>
</tr>
</tbody>
</table>
**Example of Timestamping Application (2)**

**>> Medical Information**

<table>
<thead>
<tr>
<th>User Name</th>
<th>Purpose</th>
<th>Target data</th>
<th>Format</th>
<th>Commencing Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teikyo Univ. Hospital</td>
<td>Compliance for e-Doc Law</td>
<td>Medical record(Scanned images….surgical consent form, letter of introduction)</td>
<td>PDF</td>
<td>2009~</td>
</tr>
<tr>
<td>Osaka Univ. Hospital</td>
<td></td>
<td>Medical Record (Scanned images)</td>
<td>PDF, XDW</td>
<td>2010~</td>
</tr>
<tr>
<td>Toyama Univ. Hospital</td>
<td></td>
<td>Medical Record</td>
<td>PDF</td>
<td>2011~</td>
</tr>
<tr>
<td>Japanese Red Cross Shizuoka</td>
<td></td>
<td>Medical Record (Letter of introduction medical certificate)</td>
<td>PDF</td>
<td>2011~</td>
</tr>
<tr>
<td>Hospital</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Institute Chukyo Hospital</td>
<td></td>
<td>Consent form, Letter of introduction, Interview sheet, Medical certificate</td>
<td>PDF, XDW</td>
<td>2011~</td>
</tr>
<tr>
<td>Daido Hospital</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NISHIJIN Hospital</td>
<td></td>
<td>Scanned images(Receipt, agreement, written consent)</td>
<td>PDF</td>
<td>2012~</td>
</tr>
<tr>
<td>Keio Univ. Hospital</td>
<td></td>
<td>Letter of introduction, Medical certificate</td>
<td>TIFF</td>
<td>2012~</td>
</tr>
<tr>
<td>Takara pharmacy</td>
<td></td>
<td>Prescription, Dispensing record</td>
<td>JPEG</td>
<td>2012~</td>
</tr>
<tr>
<td>St. Luke’s International Hospital</td>
<td></td>
<td>Letter of introduction, Medical certificate</td>
<td>PDF</td>
<td>2012~</td>
</tr>
<tr>
<td>Nagoya Memorial Hospital</td>
<td></td>
<td>Consent form, Letter of introduction, Interview sheet, Medical certificate</td>
<td>PDF, XDW</td>
<td>2012~</td>
</tr>
<tr>
<td>Takeda General Hospital</td>
<td></td>
<td></td>
<td>XDW</td>
<td>2012~</td>
</tr>
</tbody>
</table>
# Example of Timestamping Application (3)

## Intellectual Property

<table>
<thead>
<tr>
<th>User name</th>
<th>Purpose</th>
<th>Target data</th>
<th>Format</th>
<th>Commencing Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Printing Bureau.</td>
<td>Responsibility of giving trusted information as national authority</td>
<td>Official Gazette</td>
<td>PDF, XDW</td>
<td>2003～</td>
</tr>
<tr>
<td>Japan Data Communications Association</td>
<td>Ensure the integrity</td>
<td>Privacy Mark certification</td>
<td>PDF</td>
<td>2007～</td>
</tr>
<tr>
<td>Ministry of Finance Japan</td>
<td>Ensure the integrity</td>
<td>IOU for Fiscal Loan Fund, Certificate for money on deposit</td>
<td>XML</td>
<td>2009～</td>
</tr>
<tr>
<td>UBE-NITTO KASEI Co.,Ltd</td>
<td>Prior use right, Rights reserved in joint study or development</td>
<td>Document and report and experiment data generated in study or development</td>
<td>PDF</td>
<td>2006～</td>
</tr>
<tr>
<td>Nippon Soda Co., Ltd</td>
<td></td>
<td></td>
<td>PDF</td>
<td>2006～</td>
</tr>
<tr>
<td>OMRON Corp.</td>
<td></td>
<td></td>
<td>PDF</td>
<td>2009～</td>
</tr>
<tr>
<td>NIPRO Corp.</td>
<td></td>
<td></td>
<td>PDF</td>
<td>2010～</td>
</tr>
</tbody>
</table>
Incidents in Japan

■ TAA
  - trouble after leap second pushed
    • Jan 2\(^{nd}\) 2006: More Leap second pushed at 24hour after
    • July 1\(^{st}\) 2012: Former i-Rig device‘s output time was 1second late

■ Cybouz: Groupware Software Vender
  - trouble before leap second
    • A bug in the central server‘s OS prevented access to Cybouz.com
    • June 30\(^{th}\) 2012  09:25am ~ 10:41pm

■ Mixi: SNS site
  - trouble 4hours
    • July 1\(^{st}\) 2012
    • Server slowed down, users could not login, or sometimes lost response.
Japan’s Timezone Situation
TimeSchedule on July 1st 2012
Review

- Time is a crucial measurement to the ICT Society.
- Irregular actions done with time causes confusion to the ICT Society.
- It is thought to be impossible to adjust every time label in the system by $\pm 1$ second at once.
- The side-effects to this problem cannot be predicted.
- Should we not prevent the possibility of confusion happening as much as we can?
Thank you.