Internet Trust from the Perspective of Time Stamp

2017.7.4

The Chair of Steering Committee of Time Business Forum
Koichi Shibata
AGENDA

- Time Business Forum (TBF)
- What is internet trust?
- Environment which has been developed
- Trust service in its practical stage
- Declaration of e-Trust Japan
Time Business Study Group  JAN 2002

- “Meeting on the Research and Development of the Standard Time Distribution and Time Authentication Service” (Time Business Study Group) Held by Ministry of Internal Affairs and Communications (MIC)
  It was held for six months and had been examined needs and future of the time business

Time Business Promotion Forum  JUN 2002

- Established to develop more specific promotions in response to the achievement of the Time Business Study Group.
  • Developed the following guidelines:
    Guideline for implementing time stamps in accordance with e-Document Law (2005), etc.
  • Demonstration tests
    Identified technical and operational problems, and verified the new possible field of application.
- The forum was closed by accomplishing the original goals in June 2006.

Time Business Forum  JUL 2006

- Established through the meeting of promoters and the general meeting.
  With the purpose to develop and promote the use of time business to enlarge its demand.
- Announced the “Declaration of e-Trust Japan!” (provisional) in September 2016
  Started making efforts to establish trust service promotion forum (provisional)
Time Business Forum Framework (Fiscal year of 2017)

Supreme Advisor: Masakazu Ohashi, Professor, Chuo University Dept of Policy Sciences
Advisor: Osamu Sudoh, Professor, The University of Tokyo, Interfaculty Initiative in Information Studies, Graduate School of Interdisciplinary Information Studies

Chairman: Takaaki Yamamoto, Chairman, Seiko Solutions Inc.
Vice-chairman: Kazuya Miyazaki, Mitsubishi Electronic Corp.

Chairman: Koichi Shibata (Seiko Solutions Inc.)
Vice Chairman: Keisuke Ichikawa (Amano Business Solutions Corporation)

Investigation Research WG
- Project Mgr. Kazuya Miyazaki (Mitsubishi Electronic Corporation)
- Fixed investigation of technology trends in securing originality to ensure traceability of digital information

Promotion WG
- Project Mgr. Keisuke Ichikawa (Amano Business Solutions Corporation)
- Planning and promotion of time stamp use

Elec. certification infrastructure review WG
- Project Mgr. Koichi Shibata (Seiko Solutions Inc.)
- Discussion on digital evidence provision and verification infrastructure
Time Business Forum List of Members (July 2017)

Executive Chairman
Seiko Solution Inc.
Chairman Takaaki Yamamoto
Vice-chairman
Mitsubishi Electric Corporation
Kazuya Miyazaki

Supreme Advisor
Chuo University
Faculty of Policy Studies
Professor Masakazu Ohashi
Advisor
The University of Tokyo,
Interfaculty Initiative in Information Studies, Graduate School of Interdisciplinary Information Studies
Professor Osamu Sudoh

Executive Members (9 companies)
• Amano Business Solutions Corporation
• NTT Data Corporation
• Cosmos Corporation
• CYBERLINKS CO., LTD.
• Seiko Solution Inc.
• Secom Trust Systems CO., LTD.
• TKC Corporation
• Warehouse TERADA
• Mitsubishi Electric Corporation

Executive Members (9 companies)
• Amano Business Solutions Corporation
• NTT Data Corporation
• Cosmos Corporation
• CYBERLINKS CO., LTD.
• Seiko Solution Inc.
• Secom Trust Systems CO., LTD.
• TKC Corporation
• Warehouse TERADA
• Mitsubishi Electric Corporation

Supporting Member
• OMC, Inc.
• GMO Global Sign K.K.
• JEF Systems, Inc.
• SKY Perfect JSAT Corporation
• SECOM Co., Ltd.
• HyperGEAR. Inc
• PFU Limited
• Hitachi Ltd.
• Hokkaido Telecommunication Network Co., Inc.
• RICOH JAPAN Corp.

Supporting Member
• OMC, Inc.
• GMO Global Sign K.K.
• JEF Systems, Inc.
• SKY Perfect JSAT Corporation
• SECOM Co., Ltd.
• HyperGEAR. Inc
• PFU Limited
• Hitachi Ltd.
• Hokkaido Telecommunication Network Co., Inc.
• RICOH JAPAN Corp.

TBF Partner
(Academic)
• Satoru Tezuka (Keio University)
• Tsuneharu Yonemaru (Senshu University)
• Nakamura Motonori (National Institute of Informatics)

(Legal)
• Jiro Makino (MAKINO Legal Professional Corporation)
• Hiroshi Miyauchi (Miyauchi Mizumachi IT Legal Professional Corporation)

(Tax practices)
• Kikuzo Sodeyama (SKJ General Certified Tax Accountant Office)

(Intellectual Properties)
• Kazuo Seki (Daiichi International Patent Office)
• Koji Kitamura (Seiju IP Firm)
• Hajime Shimoide (Sapientist Inc.)

(Business organizations, Individuals)
• Japan Network Security Association (JNSA)
• JIPDEC
• Certification Authority Conference (CAC)
• Kieichi Mitani (NTT Data Institute of Management Consulting, Inc.)
AGENDA

- Time Business Forum
- What is Internet Trust?
- Development of environment
- Trust service in its practical stage
- Declaration of e-Trust Japan
What is Internet Trust?

✓ What is TRUST?
✓ Judgment of trustworthiness
✓ What are the criteria?
✓ Until now
✓ Space (face-to-face): trustworthy person?
✓ Time (in writing): trustworthy information?
✓ What about the trust in the internet environment through the time and space?
Trust in the internet community
(judge to trust based on the information from the past)

Exchange of information

Original site

False site

User

Authentication of user

Space

Correct info. management

Time

Origin and development of information

Time Flow

Create  Register  Renew  Approval  Finalize  Preserve  Utilize  Dispose

Info. Explosion
Alter. stakeholders
Absence of interested parties
2nd use? 3rd use?
What is right?

Spoofing
Reduction of info. freshness
Reduction of info. accuracy

Falsification

Forgery
Deterioration and destruction
Loss of readability
Leak and loss
Difficult to retrieve
Erroneous disposal

In order to ensure that it is correct information, provide universal scale of events “Time of Trust”

All Rights Reserved. Copyright ©2017 Time Business Forum
Information is event in the past


“When”

You cannot share the information unless you are there at the certain point of time

Must be kept!

Culture of record (a repository of great innovations!)
⇒ characters, print technology, gramophone, camera

Are they correct?

Culture of record management
⇒ signature, seal, sealed document, archive, request for approval, contract
AGENDA

- Time Business Forum
- What is internet trust?
- Development of environment (technology, legislation)
- Trust service in its practical stage
- e-Trust Japan
Electronic authentication, time stamp, and electronic signature

Electronic Signature Act: 2001
Became JIS: 2008
e-Documentation Law: 2005

Electronic application
S/MIME
~approx. 5 years
Certificate
Site validation
Authentication

Electronic signature
Who?
Electronic contract
Medical information
Meeting minutes

Time stamp
When?
Electronic alibi
Copyright
National tax related doc.

~10 years~
Proof of existence
Subsequent validation
Objectivity

Signature
Subsequent validation

Authentication of User
Space

Correct info. management
Time

All Rights Reserved. Copyright ©2017 Time Business Forum
Characteristics of time stamp

- **Fundamental technique to prove that an electronic document**
  1. existed before a certain point of time
  2. has not been altered since that time

- **Put time stamp to a document with hash value and time information**
  (Time stamp token)

- **Cannot be backdated**

- **Time stamp is a fundamental technique to ensure the evidentiality of electronic documents using Trustworthy Time.**

- **Aug 31, 2016**
  Time stamp at this point of time

- **Oct 1, 2020**
  Has not been altered
Accreditation Scheme for Trustworthiness of Time Business

It is an accreditation scheme to ensure that TSA and TAA operations are properly implemented by technologies, systems, operational structures meeting the standards specified by JADAC. Established in Feb 2005

<http://www.dekyo.or.jp/tb>

Accreditation criteria for time
- TSA shall use time distribution services provided by accredited TAA.
- TAA shall compare and store time as designated by NTA

Trustworthy Time of TAA • TSA

- JISX5094: May 20, 2011
- ISO18014-4: April 15, 2015 Published
Hash value can be thought as "fingerprint" of electronic data. A hash value is a value of fixed length which computed from the original data with certain process and used to identify the original data.

<table>
<thead>
<tr>
<th>Input string</th>
<th>SHA-256 (32 byte)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I have a pen</td>
<td>2FCF9FE9BA147AB1C36377DE3CC4AC860E9EB76C8F392773252BF34D34F4BE</td>
</tr>
<tr>
<td>I have a pin</td>
<td>0F4691B1B50477BE56F3DFE4984322803DD49636AE5140FE2D891C9525872BB6</td>
</tr>
<tr>
<td>I have a pan</td>
<td>54C1A05B8D63F4F957454B10293FB2E6B0CDCE220FF46191E260FBBCE3EA0B3</td>
</tr>
<tr>
<td>I have a pineapple</td>
<td>F97DEDAE1909206E5260ECF859B97B783A2BC5ED628B538268AC2035D5EDA44</td>
</tr>
</tbody>
</table>
Standardization of Long-term Signature Profile

PDF Electronic Signature (PAdES) : ISO/PRF 14533-3 (Stage50.00 Apr 2017)

【Point】
・Secure evidentiality of signed time by Signature Time Stamp (STS)
・Secure continuity of certificate validation by storing revocation information and certificates in signature data.
・Protect signature data and revocation information, etc. by using crypto algorithm of archive time stamp (ATS)
<table>
<thead>
<tr>
<th>Markets</th>
<th>Goals</th>
<th>Grounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Information</td>
<td>Disposal of paper-based original doc.</td>
<td>Ministry of Health Labor and Welfare “Guidelines on secure management of medical information system” Ver.5 (May 2017)</td>
</tr>
<tr>
<td></td>
<td>BCP</td>
<td>Ministry of Economy, Trade and Industry “Guidelines on medical information management for Information processing service operators” (Oct 2012)</td>
</tr>
<tr>
<td></td>
<td>Dispute resolution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protection of personal information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Abusive application resolution</td>
<td>Open &amp; Close Strategy</td>
</tr>
<tr>
<td></td>
<td>BCP</td>
<td>INPIT Time Stamp Preservation Service (started in Mar 2017)</td>
</tr>
<tr>
<td></td>
<td>Protection of trade secrets</td>
<td></td>
</tr>
<tr>
<td>The ordinances on storage of electronic account books</td>
<td>Disposal of paper-based original doc.</td>
<td>The ordinances on storage of electronic account books Art. 4: preservation of national tax related documents in electronic form (Apr 2005)</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td>Revision of its implementing Rules Art. 3 (Mar 2015, Mar 2016)</td>
</tr>
<tr>
<td>Certificate distribution</td>
<td>Improvement of operational efficiency</td>
<td>Implementing Rules Art. 8 Revision (Mar 2015)</td>
</tr>
<tr>
<td></td>
<td>Reduction of printing cost</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Improvement of operational efficiency</td>
<td>Notification No. 394 (Building Standards Law: May 2014)</td>
</tr>
</tbody>
</table>
AGENDA

- Time Business Forum
- Internet Trust
- Development of environment
- Trust service in its practical stage
- e-Trust Japan
Number of TSA validated time stamps issued (Company S)

The ordinances on storage of electronic account books, Amended in 2015

ISO18014-4

The ordinances on storage of electronic account books, Amended 2016

Patent Office GL Ver.2

INPIT start service

Ministry of Health, Labor and Welfare Medical Information GL V5

JISX5094

e-Document Law 2005

Ministry of Economy, Trade and Industry METI Medical Information GL V4.2

Ministry of Land, Infrastructure, Transport and Tourism MLIT Notification No. 394
**Protection of trade secret: Efforts of Patent Office**

**Time Stamp Storage Service**: To protect technical know-how by complementing original proofing

Users use time stamps provided by private companies and public sectors to store those time stamps, which allows stable long-term evidence to be secured.

(From Industrial Structure Council, Intellectual Property Subcommittee, Subcommittee on protection and utilization of trade secret, 2nd meeting (Oct 31, 2014) Material 6)

**INPIT Time Stamp Storage System**

http://www.inpit.go.jp/katsuyo/tradesecret/ts.html
A “Contract” is “evidence” that is prepared by parties concerned in order to voluntarily hedge a risk in the contract “identical declarations of intent to offer and to accept.”
AGENDA

- Time Business Forum
- Internet Trust
- Development of environment
- Trust service in its practical stage
- e-Trust Japan
Announced the “Declaration of e-Trust Japan!” September 2016

~It has been published on several news papers. Trust Service Promotion Forum is currently being prepared to start.

Declaration of e-Trust Japan!

Areas where time stamp usages are growing
National taxes, intellectual properties, medical, electronic contracts

Social issues, unsolved data
Piling, fuel consumption, copper wire strength, chemical liquid injection volume, airbag exhaust gas concentration, seismic base isolation…

Future efforts
• Establish Trust service Promotion Forum (provisional)
• Discuss on ideal states, propose systems
• Respond to technical challenges, new technologies, standardization
• Promotion

TBF launched

Y2006
Y2016
Y2026

IoT → Big data with time information

Trust service
Time stamp, electronic signature, electronic Delivery, Electronic authentication, electronic contract, document preservation…

Electronic Certification Infrastructure

IoT → Big data with time information

It has been published on several news papers. Trust Service Promotion Forum is currently being prepared to start.
Trust Service Infrastructure (Proposal)

- Agriculture, forestry and fisheries industry
- Construction industry
- Manufacturing industry
- Transport and postal industry
- Wholesaling and retailing industry
- Accommodation and food services industry
- Finance and insurance industry
- Information and communications industry
- Electricity, gas, water supply industry
- Real estate industry, Goods rental business
- Medical and welfare service industry
- Life services and entertainment industry
- Scientific research, professional and technical services industry
- Education, Study support

Trust Service Infrastructure

Trust service

Electronic Authentication Infrastructure

- CA
- RA
- VA
- TSA
- TAA
- Remote Sig.
- Accreditation Scheme
- Accreditation Body

Trust list
Overview of Registration Scheme using Accredited Time Stamp

All business operators using accredited time stamps are covered!

- Official name: Registration scheme for business operators who use accredited time stamps
- Subject to Registration: Services or operations using accredited time stamps
- Use of registration mark: available on website and printed materials, etc.
- Registration period: registration per fiscal year (April to the next March) Automatically renewed
- Registration fee: 1st service or operation 50,000 yen (tax not included), 2nd case～30,000 yen (tax not included)
- Publication: published on the website
- Provision of information: Information is provided to the Japan Patent Office and the National Tax Administration Agency
- Management body: Japan Data Communications Association

Actual cases

✓ When we assessed by using accounting ASP for scanner storage of national tax related documents, it was not easy to select one because we were not sure if they used accredited time stamps.
✓ We wished to make an appeal about our use of “accredited time stamps” for providing electronic contract services. However, it was out of the scope of the TSA accredited mark.
✓ The storage service we use is time stamped. However, we were not sure if we could use INPIT time stamp preservation service.

Advantages of registration (assumption)

✓ You will be able to make an appeal about your use of “accredited time stamps” for accounting services operated as ASP, which will increase then number of inquiries you receive.
✓ The electronic contract service you considered to introduce is adopting long-term signature format using accredited time stamp, and this allows you to chose it with confidence.
✓ Using accredited time stamps for storage service operations allows clear indication of covering INPIT time stamp preservation service.

※Accredited time stamp means a time stamp issued by accredited time stamping authority in line with the guidance on Time Business (Nov 5, 2004, MIC ).
※Date and time indicated by an accredited time stamp is able to prove the certain point of time, since its traceability with the standard time supplied by NICT is secured.
It is Digital that allows secured integrity, authenticity, and accountability of information.