

# Internet Trust from the Perspective of Time Stamp

2017.7.4

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

- 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

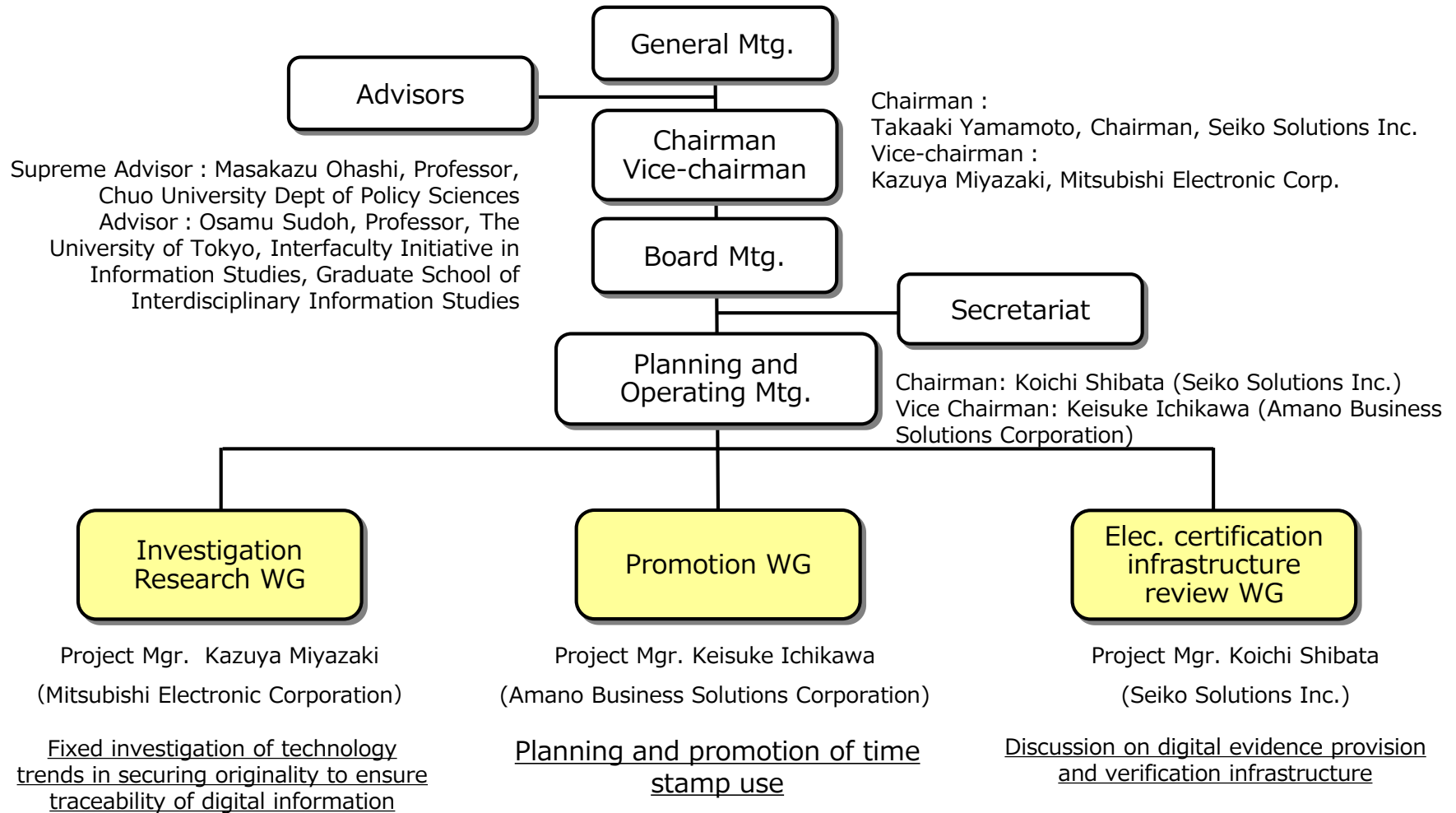
Secretariat: SCAT

- Established to develop more specific promotions in response to the achievement of the Time Business Study Group.
  - Developed the following guidelines:
    - Time Authentication Infrastructure Guideline (2004)
    - 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

Secretariat: JADAC

- 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)



## ■ 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

## ■ 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.)

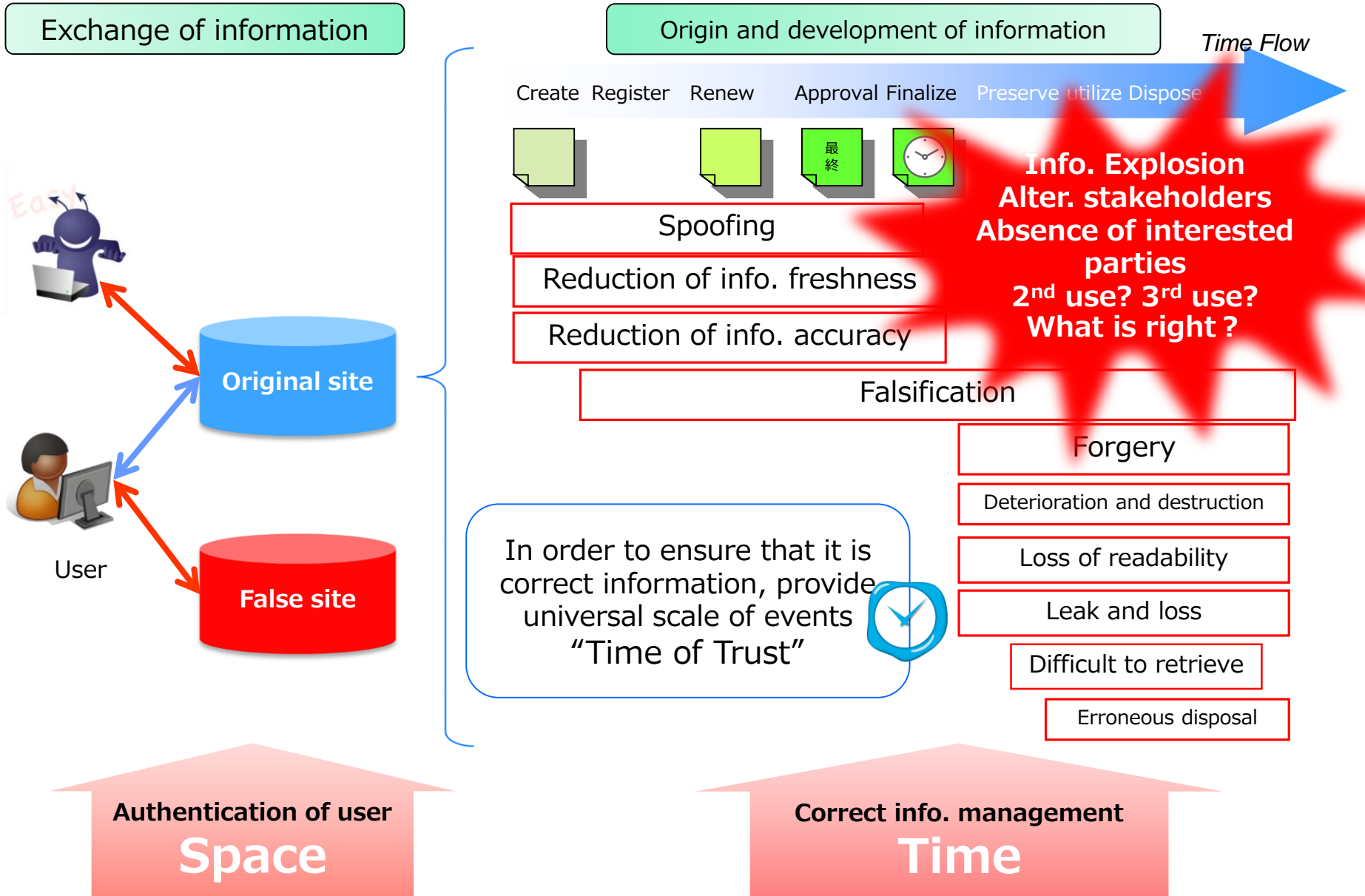
### (Business organizations, Individuals)

- Japan Network Security Association (JNSA)
- JIPDEC
- Certification Authority Conference (CAC)
- Keiichiro Mitani (NTT Data Institute of Management Consulting, Inc.)

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

- ✓ 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)





“Who”

“What”

“Why”

“Where”

“How”

“When”  
“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

- Time Business Forum
- What is internet trust?
- Development of environment (technology, legislation)
- Trust service in its practical stage
- e-Trust Japan

Electronic Signature Act: 2001

Became JIS: 2008

e-Documentation Law: 2005



Electronic application  
S/MIME

Electronic signature  
Who?

Time stamp  
When?

~approx. 5 years

Electronic contract  
Medical information  
Meeting minutes

Protection of IP  
Electronic alibi  
Copyright  
National tax related doc.  
10 years~

Certificate  
Site validation  
Authentication

Signature  
Subsequent validation

Proof of existence  
Subsequent validation  
Objectivity

Authentication of User  
**Space**

Correct info. management  
**Time**

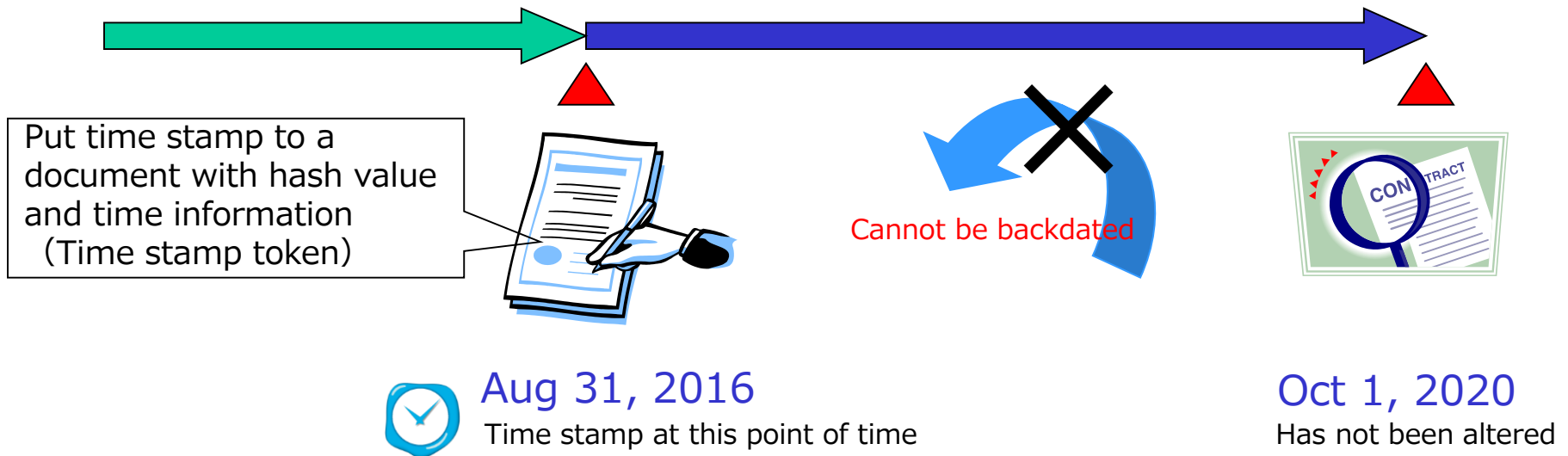
# Characteristics of time stamp

Fundamental technique to prove that an electronic document

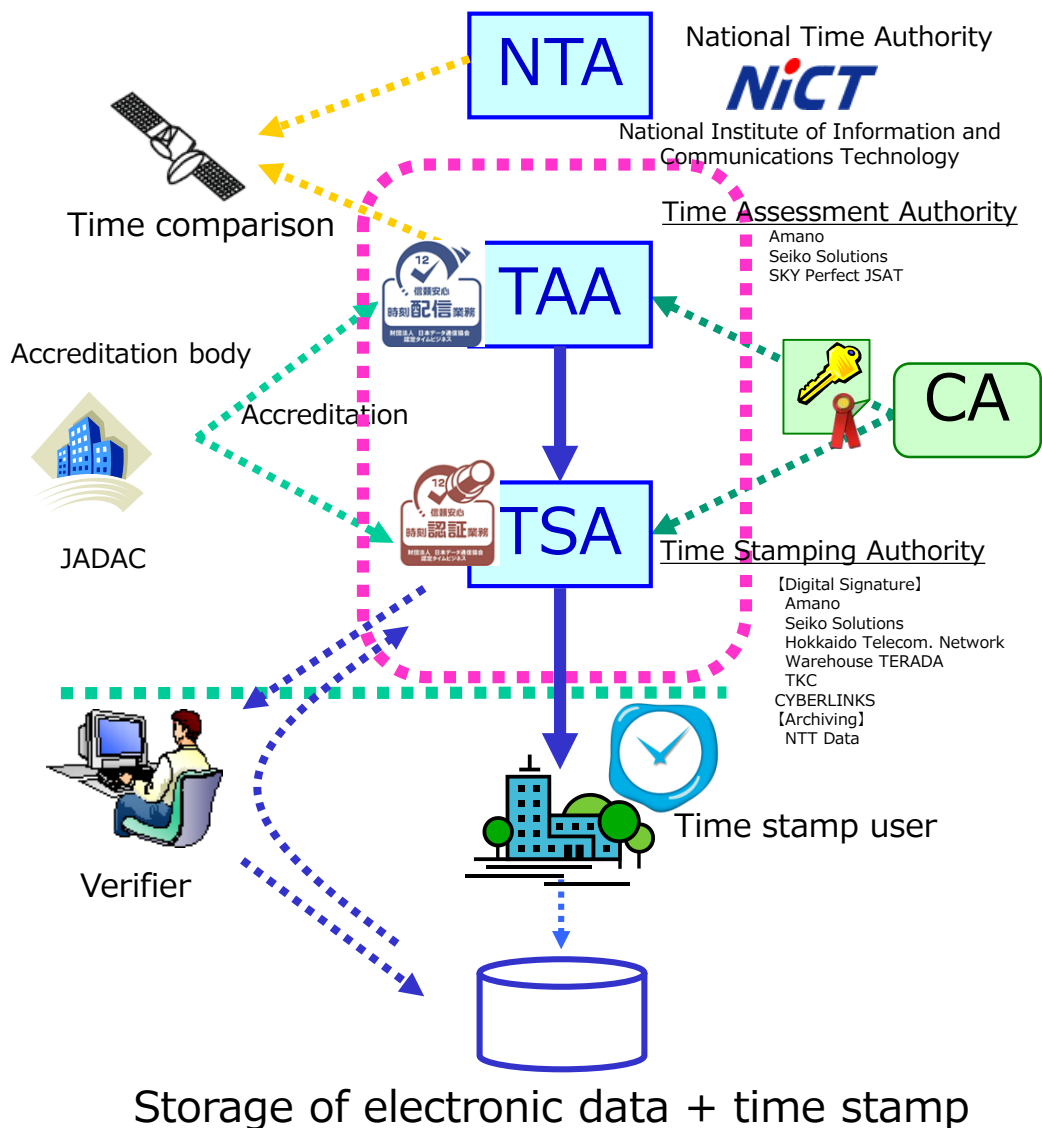
- ① existed before a certain point of time
- ② has not been altered since that time

① existed before a certain point of time

② has not been altered since that time



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



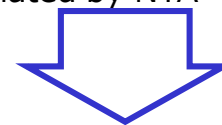
“Guidelines on Time Business ~ for secure use of network and secure long-term preservation of electronic data” (Ministry of Internal Affairs and Communications)

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>>

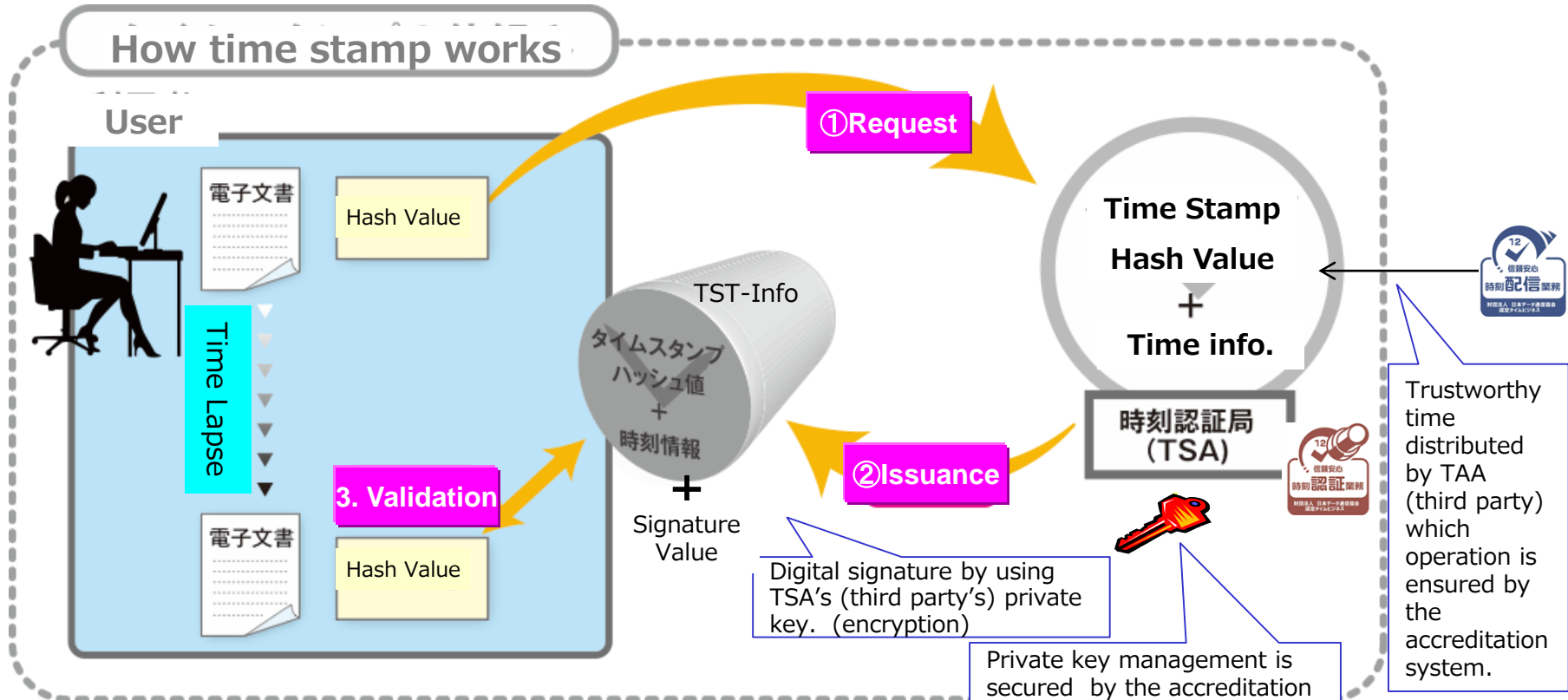
### Accreditation criteria for time

- 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.

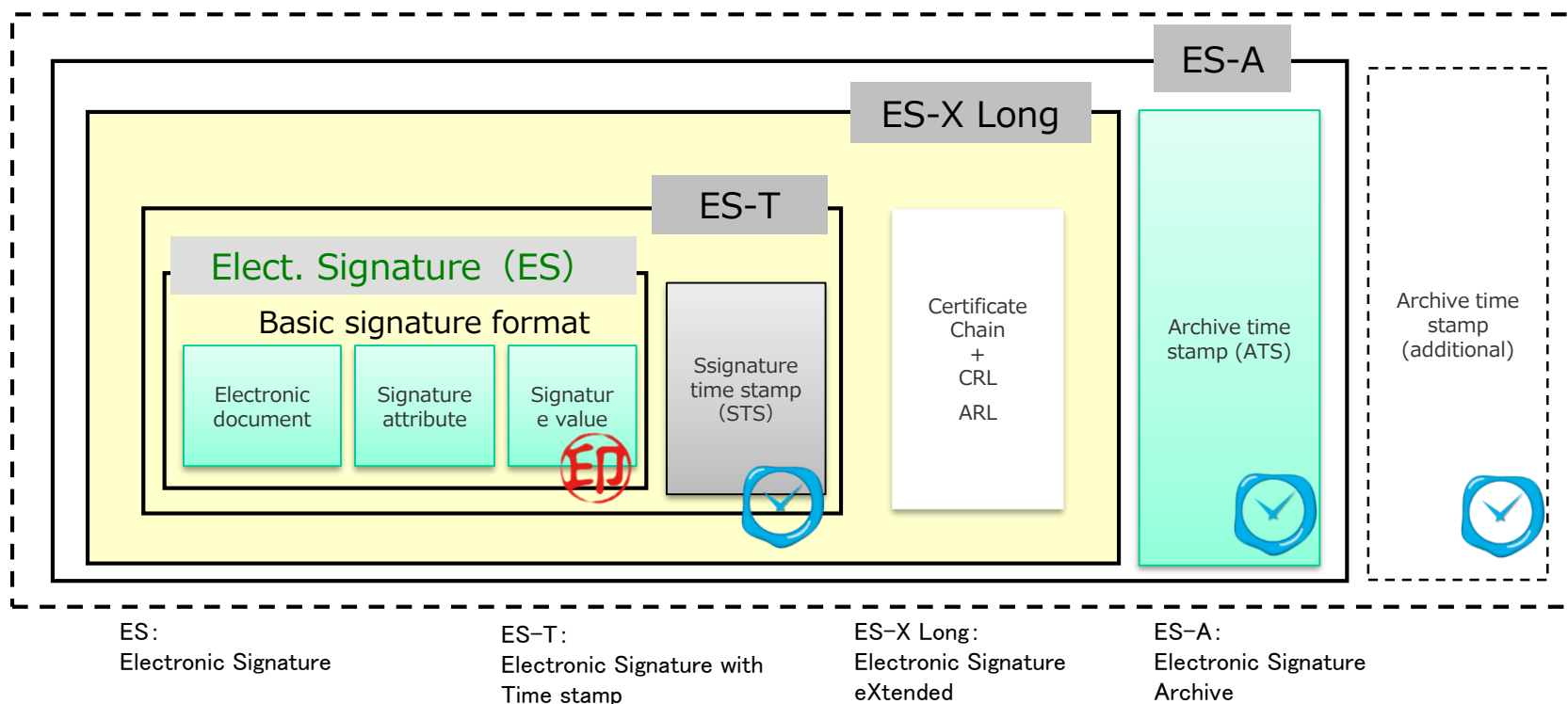
Input string	SHA-256 (32 byte)
I have a pen	2FCF9FE9BA147AB1C36377DE3CC4AC860E9EAB76C8F3922773252BF34D34F4BE
I have a pin	0F4691B1B50477BE56F3DFE4984322803DD49636AE5140FE2D891C9525872BB6
I have a pan	54C1A05B8D63F4F957454B10293FB2E6B0CDCE220FF46191E260FBBC0E3EA0B3
I have a pineapple	F97DEDAE1909206E5260ECFE859B97B783A2BC5ED628B538268AC2035D5EDA44

# Standardization of Long-term Signature Profile

CMS Electronic Signature (CAAdES) : JIS-X5092 (2008) 、ISO14533-1 (2014)  
 XML Electronic Signature (XAdES) : JIS-X5093 (2008) 、ISO14533-2 (2012)  
 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 algorism of archive time stamp (ATS)



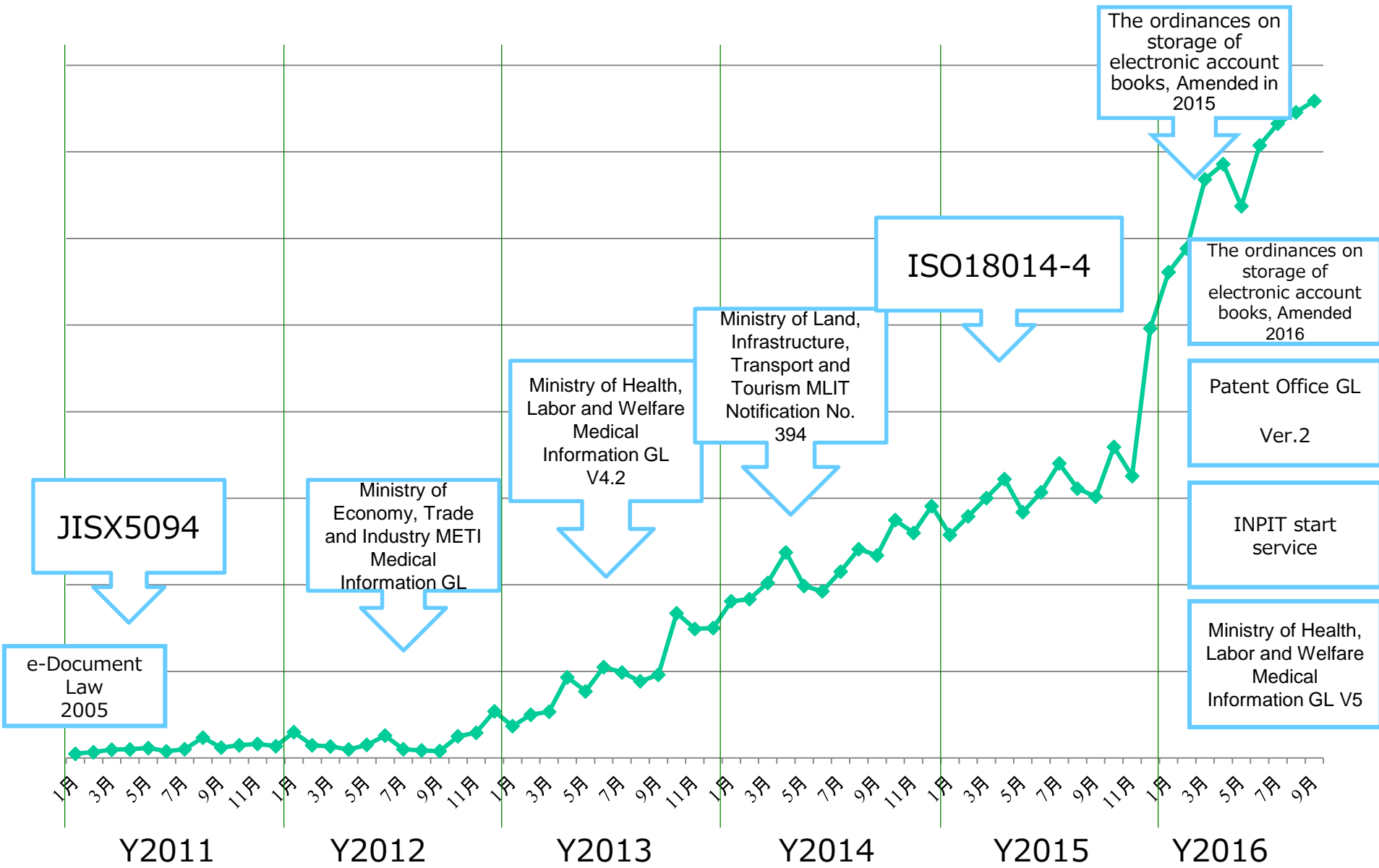
# Key Markets Where Time Stamps Are Used

Markets	Goals	Grounds
Medical Information	Disposal of paper-based original doc. BCP Dispute resolution Protection of personal information	Ministry of Health Labor and Welfare "Guidelines on secure management of medical information system" Ver.5 (May 2017) Ministry of Economy, Trade and Industry "Guidelines on medical information management for Information processing service operators" (Oct 2012)
IP Protection	Dispute resolution Abusive application resolution BCP Protection of trade secrets	Japan Patent Office "Guidelines for the Prior User's Rights Systems" (Ver.1 Jun 2006, Ver.2 May 2016) Open & Close Strategy INPIT Time Stamp Preservation Service (started in Mar 2017)
The ordinances on storage of electronic account books	Disposal of paper-based original doc. Compliance	The ordinances on storage of electronic account books Art. 4: preservation of national tax related documents in electronic form (Apr 2005) Revision of its implementing Rules Art. 3 (Mar 2015, Mar 2016)
Electronic contract Electronic commerce Certificate distribution	Reduction of stamp tax Reduction of postal cost Improvement of operational efficiency Reduction of printing cost	Tax Office Tax Answer, e-Document Law (Apr 2015) Electronic bookentry Law Art. 10: Electronic preservation of electronic commerce information (Apr 2005) Implementing Rules Art. 8 Revision (Mar 2015)
Construction related books	Disposal of paper-based original doc. BCP Improvement of operational efficiency	e-Document Law: Building Standard Law, Act on Architects and Building Engineers (Apr 2005) Ministry of Land, Infrastructure, Transport and Tourism: Notification No. 177 (Construction Business Act: Oct 2008) Notification No. 394 (Building Standards Law: May 2014)

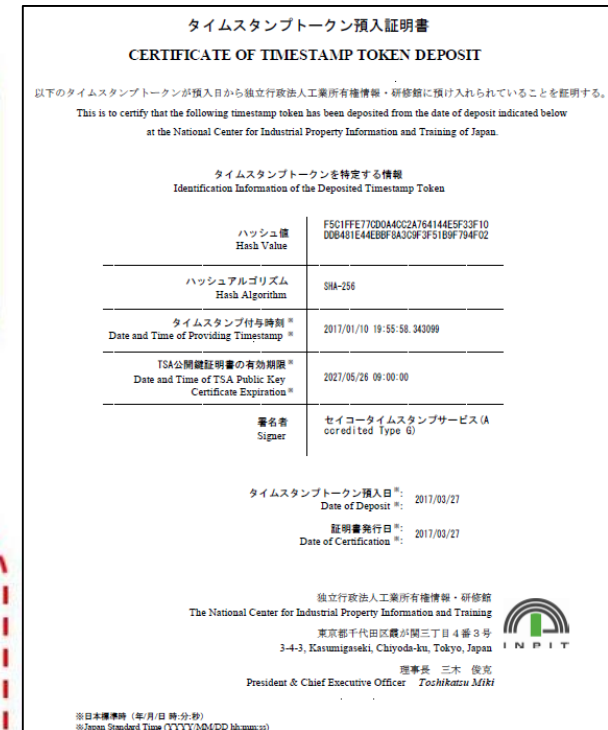
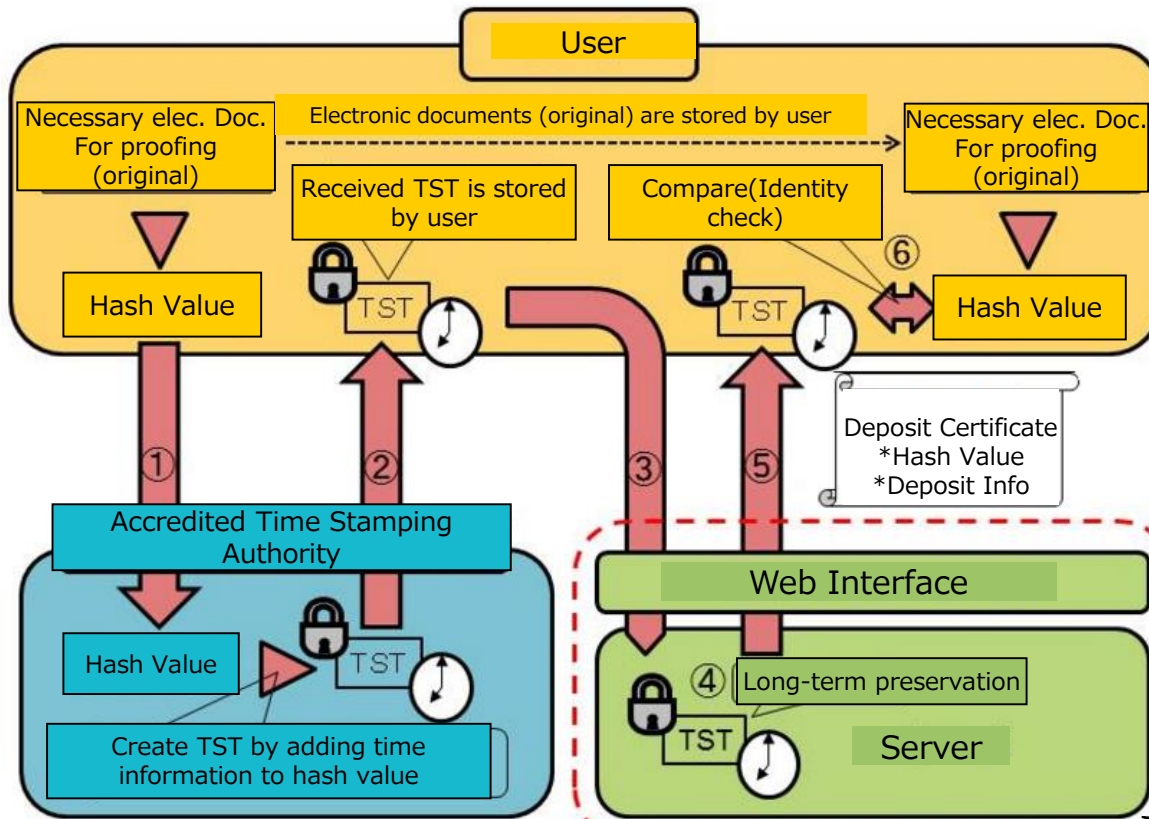


- Time Business Forum
- Internet Trust
- Development of environment
- Trust service in its practical stage
- e-Trust Japan

# Number of TSA validated time stamps issued (Company S)



**Time Stamp Storage Service** : To protect technical know-how by complementing original proofing  
 Users use time stamps provided by private companies and public sectors 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)



Started on  
 March 27, 2017

<http://www.inpit.go.jp/katsuyo/tradeseecret/ts.html>

- Housing loan electronic contract system is planned to be introduced  
Scheduled to start in summer 2017; Mizuho Bank, Ltd.
- Paperless lease termination procedure by using “simple electronic contract”  
April 19, 2017; Fuyo General Lease Co., Ltd.
- The industry’s first introduction of paperless system for construction contracts  
March 31, 2017, Leoplace 21 Corporation
- Banking industry’s first introduction of electronic mortgage contract system using “my number card” ~Reduction of customers’ administrative burden by the cooperation of banks and real estate agencies~ March 21, 2017 ; The Bank of Tokyo-Mitsubishi UFJ, Ltd.
- The first electronic contract for housing loan in Japan  
July 12, 2016; The Mortgage Corporation of Japan, Limited)
- Construction contracts for newly opened convenience stores  
February 29, 2016; FamilyMart Co., Ltd.
- Introduction of “electronic contracts” to loan agreements  
October 13, 2015; Sumitomo Mitsui Banking Corporation
- Realization of electronic contract system using tablet which concludes necessary procedures including contract and bank transfer at visited places. – Bears, house-keeping, house-cleaning services. June 9, 2015; Bears Co., Ltd.



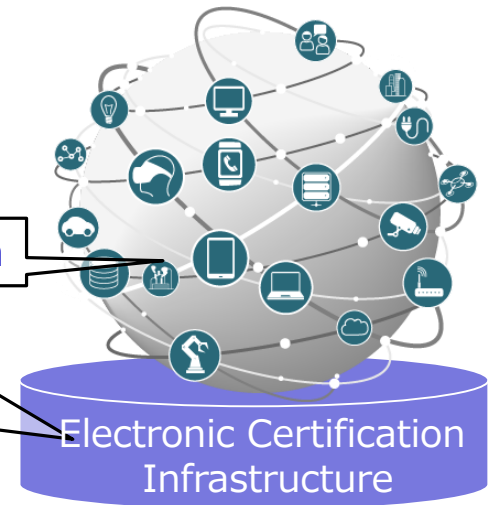
TBFの調査

A “Contract” is “[evidence](#)” that is prepared by parties concerned in order to voluntarily hedge a risk in the contract “[identinal declarations of intent to offer and to accept](#)”

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

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

# Declaration of e-Trust Japan!



IoT → Big data with time information

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

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

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

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

Present

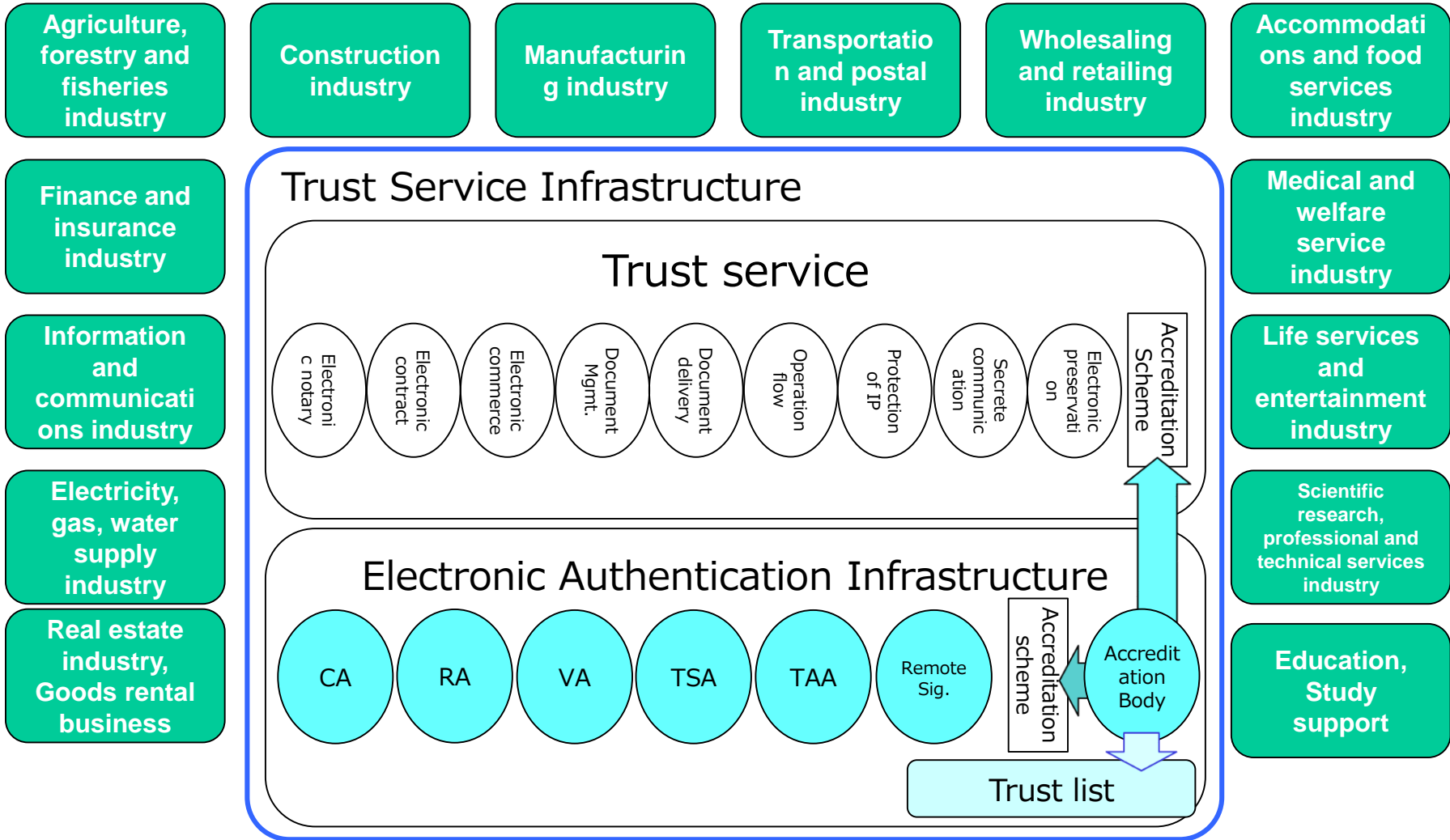
TBF launched

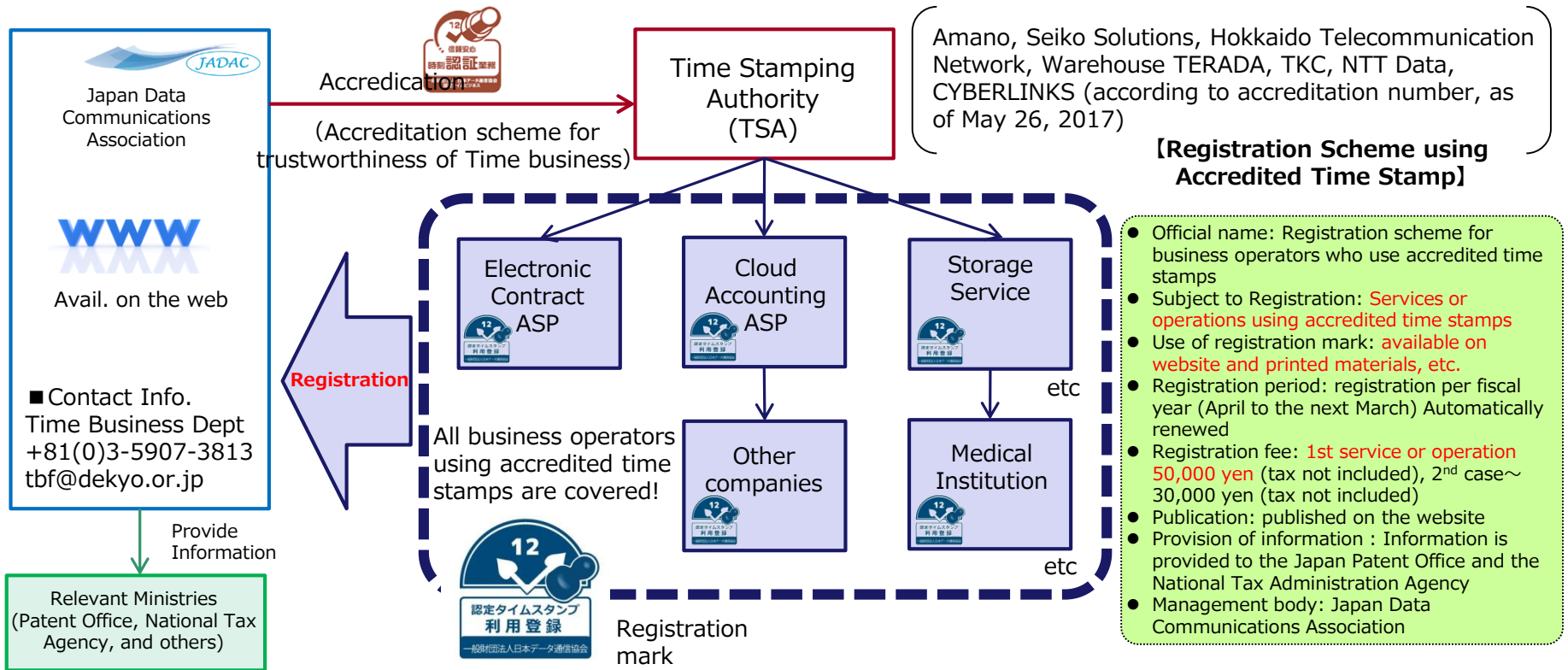
Y2006

Y2016

Y2026

# Trust Service Infrastructure (Proposal)





## 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.





Trusted Time

It is Digital that allows secured integrity, authenticity, and accountability of information

