Japanese trust services
and
International Mutual Recognition
-Technical WG (IMRT-WG)

September 3, 2019

Keio University
Satoru Tezuka
1. Japanese Trust Services

2. International Mutual Recognition -Technical WG
e-Signature Act and Act on JPKI Services

● e-Signature Act
  • Act on Electronic Signatures and Certification Business
  • Code of Civil Procedure Article 228.1
    Private documents shall prove its creation to be authenticate.

Electronic Signature
Certification Business
Specific and Accredited Certification Business

● Act on Japanese Public Key Infrastructure Services
  • Laws for authentication service of local public bodies for electronic signature and electronic authentication (Act on Japanese Public Key Infrastructure)
  • The function to ensure that there is no spoofing in application and falsification of electronic data during communication, which is to implement safe and secure administrative procedures through internet
Overview of Japanese PKI

- Private CA
- Foreign CA
- Commercial registration CA

GPKI
- BCA
- Government post CA
- Gov post

Interconnection
- LGPKI
- BCA
- Organizational CA

Personal authentication
- BCA
- Prefecture CA
- Prefecture A
- Municipal office
- Resident

Electronic application / filing

BCA: Bridge CA

47 CA
# Overview of Japanese PKI

<table>
<thead>
<tr>
<th>Name of certification infrastructure</th>
<th>Issuer</th>
<th>User</th>
<th>Law</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPKI</td>
<td>Each ministry or agency</td>
<td>Government positions</td>
<td>G/G, B, C</td>
<td></td>
</tr>
<tr>
<td>LGPKI</td>
<td>Accreditation authority of each prefecture</td>
<td>Local government positions</td>
<td>G/G, B, C</td>
<td></td>
</tr>
<tr>
<td>Ministry of Justice Commercial Register</td>
<td>Ministry of Justice</td>
<td>Representative of a corporation</td>
<td>B/G, B, C</td>
<td></td>
</tr>
<tr>
<td>Japanese Public Key Infrastructure Service (JPKI)</td>
<td>Governors of each prefecture</td>
<td>Residents</td>
<td>C/G</td>
<td></td>
</tr>
<tr>
<td>HPKI</td>
<td>HPKI CA accredited by the Ministry of Health, Labor and Welfare</td>
<td>Healthcare professionals</td>
<td>B/B, C</td>
<td></td>
</tr>
<tr>
<td>Specific CA</td>
<td>Private business operators</td>
<td>Natural person</td>
<td>C/G, B, C</td>
<td></td>
</tr>
<tr>
<td>Other CA</td>
<td>Private business operators, etc.</td>
<td>People, things, addresses, etc.</td>
<td>B, C/B, C</td>
<td></td>
</tr>
</tbody>
</table>

G: Public organizations  B: Private businesses  C: Citizens
Electronic Power of Attorney

● Basic Act on the Advancement of Public and Private Sector Data Utilization (December 2016)
  • Article 10(3) The State is to implement legislative and other necessary measures to ensure that a person that was delegated with mandate by a representative of a corporation is able to implement an offer of a contract or any other procedure by exclusively using an electronic data processing system.

● Act on Promotion of Dissemination of Electronic Power of Attorney (January 2018)
  • Basic guidelines for promoting the dissemination of electronic power of attorney and accreditation system for handling electronic power of attorney has been established.
Electronic Power of Attorney

1. Delegation of authority of representation (delegation to employee)
2. Registration of electronic power of attorney
3. Storage of electronic power of attorney
4. Browsing electronic power of attorney
5. Receipt of electronic power of attorney
   - Confirm Company A’s delegation of authority of representation
6. Conclusion of contracts, etc.

Source of reference: Partially revised the 2nd system review WG
Study Group on Trust Services

Key Issues

(1) Present condition analysis of Trust Service and examination of challenges
(2) Issues concerning the ideal state of Japan’s Trust Services and measures to secure interoperability with overseas countries from the viewpoint of promoting smooth data distribution utilizing online platform services in Japan and overseas countries

Key Issues

(1) 13 People
(2) Chair : Prof. Satoru Tezuka (Professor, Faculty of Environment and Information Studies)
(3) Other members : TSPs, Lawyers, and so on

Key Issues

(1) 9 meeting held since January 2019
(2) Timestamp, Remote Signature, eSeal, eDelivery and Web Authentication have been discussed so far

Interim report from the study group on trust services

- Remote Signature
  - Necessity of standards related to Specified/Accredited Certification Business for Remote Signature
  - Necessity of organizing the remote signature on e-Signature Act

- eSeal
  - Expected to promote digitization
  - More study on reliable environment for eSeal incl. systematization

- Website Authentication
  - Strategic participation to CA/B forum
  - Japanese Trusted List

- Timestamp
  - Further study on required system to promote the use of timestamp
  - Global interoperability

- eDelivery
  - Less Needs
  - Need to study more use cases and needs

122 comments received
- Most of them are positive comments
1. Japanese Trust Services

2. International Mutual Recognition -Technical WG
Concept of mutual recognition

- Concept of trust services by international collaboration

**US**
- GSA
  - FBCA
- CBCA
- SAFE

**Japan**
- Government CIO / NISC / MIC / METI
  - Cross Certification (CC)
  - JBCA
- JPKI BCA
- LGPKI BCA
  - CA for public sector
- Commercial BCA
  - Aerospace Industry BCA
  - Power Industry BCA
  - Automotive Industry BCA
  - CA for private sector (Bridge-Type)
- T-RCA
  - Trust List
  - CA for private sector (Trust-List-Type)

**EU**
- DG CONNECT
  - EULoTL
- F-TL
- G-TL
International Mutual Recognition Technical WG (IMRT-WG)

A Technical Working Group (WG) for international mutual recognition is to be formed by Keio University. The WG will consist of three technical experts each from US, EU, and Japan, and also one technical expert each from the CA/B Forum.

• Chair  Satoru Tezuka (Keio University)

• US (3 people)
  Judith Spencer (CertiPath), Kyle Neuman (SafeBioPharma), Patrick Patterson (A4A, Carillon)

• EU (3 people)
  Nick Pope (Security and Standards Associates), Arno Fiedler (Nimbus), Olivier Delos (Sealed)

• Japan (3 people)
  Soshi Hamaguchi (Keio University), Kazuo Noguchi (Keio University), Atsushi Inaba (GMO Global Sign)

• Others
  Kirk Hall (CA/B Forum, Entrust Data Card)
## Outcome of IMRT-WG

<table>
<thead>
<tr>
<th>ETSI “Pillar”</th>
<th>ETSI for PTC</th>
<th>WebTrust for PTC</th>
<th>ETSI for eIDAS</th>
<th>FPKI</th>
<th>Japanese electronic Signature Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law</td>
<td>CA/Application agreement</td>
<td>CA/Application agreement</td>
<td>eIDAS Regulation</td>
<td>E-Government Act of 2002</td>
<td>Act on Electronic Signatures and Certification Business</td>
</tr>
<tr>
<td>Objective</td>
<td>Acceptance by application root store</td>
<td>Acceptance by application root store</td>
<td>Legal recognition of trust services,</td>
<td>Identity management and trust across organizational, operational, physical and network boundaries.</td>
<td>To promote the distribution of e-document through ensuring the smooth use of e-Signatures.</td>
</tr>
</tbody>
</table>

### Legal context

<table>
<thead>
<tr>
<th>Application</th>
<th>Web Servers</th>
<th>Web Servers</th>
<th>Signature, ERDS, Timestamp, e-Seal, Website (server) authentication</th>
<th>Authentication (Personal ID and Device ID) Signature Encryption</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community</td>
<td>Global Public</td>
<td>Global Public</td>
<td>EU public, business and government</td>
<td>US Public, Business and Government</td>
<td>JP Public, business and government</td>
</tr>
<tr>
<td>Harmonization Body/CA/Browser forum</td>
<td>CA/Browser forum</td>
<td>EU Commission</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Certification Body</td>
<td>Conformity Assessment Body (Accredited by NAB)</td>
<td>Licensed Practitioners</td>
<td>N/A</td>
<td>FPKI Policy Authority</td>
<td>Same as above</td>
</tr>
<tr>
<td>Conformity Assessment Body</td>
<td>Conformity Assessment Body (Accredited by NAB)</td>
<td>Same as above</td>
<td>Conformity Assessment Body</td>
<td>FPKI Certification Policy Working Group</td>
<td>Designated Investigation Organization</td>
</tr>
<tr>
<td>Harmonized standards</td>
<td>RFC5280</td>
<td>RFC5280</td>
<td>RFC5280</td>
<td>RFC5280</td>
<td>RFC5280</td>
</tr>
<tr>
<td>Supporting Technical Documents</td>
<td>ETSI Standards</td>
<td>WebTrust Criteria</td>
<td>ETSI Standards</td>
<td>NIST SPs, FIPS 201, FPKIPA Documents</td>
<td>Accreditation Criteria</td>
</tr>
<tr>
<td>Assurance to be achieved</td>
<td>Technical Compliance</td>
<td>Technical Compliance</td>
<td>Legal admissibility + Technical Compliance</td>
<td>Technical Compliance, Interoperability with Federal PKI system</td>
<td>Legal admissibility + Technical Compliance</td>
</tr>
<tr>
<td>Trust representation</td>
<td>Browsers/OSs</td>
<td>Browsers/OSs</td>
<td>Trusted List</td>
<td>Federal Bridge CA</td>
<td>Official Journal and Websites</td>
</tr>
</tbody>
</table>
IMRT-WG event

- Workshop Style Seminar International Data Free Flow with Trust: Trusted Services and International Mutual Recognition

Agenda

Wednesday, September 4, 2019, 11:30 – 17:30 (Lunch provided)
Hitachi America, Ltd., 101 Park Avenue, 10F, New York, NY 10178

12:30 – 13:30: EU status and direction on Mutual Recognition: Nick Pope, Arno Fiedler, Olivier Delos, experts with ETSI (European Telecommunications Standards Institute), etc.

13:30 – 14:15: US industry and technical view of the Trusted Services and Mutual Recognition: Judith Spencer, CertiPath

14:15 – 15:00: NIST perspective and progress of Trust Services (Tentative – please propose the title): David Temoshok, NIST

15:00 – 15:30: Japan’s perspective and progress of Trust Services: Satoru Tezuka, Keio University

Japanese Language Seminar and Q&A

16:00 – 17:30 Japanese language presentation and Q&A

+++++

For registration, please send your full-name, title, and affiliation to: kazuo.noguchi@hal.hitachi.com. The registration will be closed when we reached maximum of 55 people.