Comparison of Electronic Signature between Europe and Japan: Possibiltiy of Mutual Recognition

[1]Soshi Hamaguchi, [1]Toshiyuki Kinoshita, [2]Satoru Tezuka
[1]Tokyo University of Technology, Tokyo, Japan, [2]Keio University, Kanagawa, Japan

Abstract

electronic signature is one of the most used trust services and should be mutual recognized. This study compares legal framework, audit scheme and audit criteria of electronic signature between Europe and Japan and identified deviations to examine the possibility of mutual recognition. Also, definition of trust services usually includes other than electronic signature such as timestamps and electronic deliveries but because electronic signature is only one trust service which legal admissibility is defined by law in Japan, the paper is focused on electronic signatures.

1. Introduction

Businesses and societies are increasingly global and are more and more based on electronic transactions. There are a lot of security measures developed to protect the electronic transaction securely, but businesses and citizens hesitate to carry out transactions electronically and adopt new services due to the lack of legal certainly and trust. In Europe, uniform requirements, definitions and legal values are set for several trust services, such as electronic signature, electronic seal and electronic time stamp, by eIDAS regulation [1], in order to establish the trust among electronic transaction within Europe. On the other hand, in Japan, legal value of electronic signature is also defined by electronic signature act [2] and this study examined the gaps between them from not only the legal aspect but also audit scheme and technical standards point of view and seek the possibility of mutual recognition of electronic signature.

2. Related Works

Our previous study identified differences between ETSI certification and WebTrust for CA from both scheme and technical requirement point of view and examined the possibility of reuse of certification result [3]. We also conducted study about different trust models of Public Key Infrastructure [4].

Kirc Hall introduced different standards and regulations applicable to CAs in his white paper "Standards and Industry Regulations Applicable to Certification Authorities [5]". Kirc Hall summarized in the paper that the CAs today are subjected considerable common security standards and industry regulations, imposed on CAs by the CAs themselves and by the browsers and applications as condition to be included in trusted root stores [5].

Thijs R. Timmerman compared the requirements in ETSI TS 102 042 and WebTrust for CAs and identified the differences in his thesis "Certificate Authority Criteria in User Perspective [6]" in 2014. His study identifies some gaps between two criteria and shortcomings of both criteria. In order to examine the possibility of reducing the burden of assessment, the identified gaps are referred in this paper.

3. Legal Framework

This chapter describes the definitions and the requirements of electronic signatures defined in both European and Japanese law.

3.1. eIDAS Regulation

In eIDAS regulation, three different electronic signatures were defined, simple electronic signature, advanced electronic signature and qualified electronic signature. Simple electronic signature is any sort of electronic signature which data in electronic form is and associated with other data in electronic form and is used by the signatory to sign. Advanced electronic signature has more strict requirements than the simple electronic signatures which is uniquely linked to the signatory, capable of identifying the signatory and created using electronic signature creation data that the signatory can with a high level of confidence, use under his sole control. Only electronic signature based public key infrastructure fulfills these requirements as advanced electronic signature. Qualified electronic signature is defined as which legal value is as same as handwritten signature and is advanced signature created by qualified electronic signature creation device, such as secure IC card and based on qualified electronic certificate.

3.2. Act on Electronic Signatures and Certification Business

Japanese electronic signature act has different approach than in Europe based on Japanese seal culture. In Japan, a personal seal is often used instead of signature as official verification especially for important documents. Therefore, Japanese electronic signature act is more focused on electronic certificate and certification service provider. So, instead defining three different type of electronic signature like Europe, three different certification services (certification "business" as original text of the law), simple certification service, specified certification service and accredited certification service, are specified. Simple certification service is a service that, in response to either the request of the signatory with respect to the electronic signature that the signatory performs or the request of relying party, certifies that the electronic signature performed is done by the signatory. Specified certification service is the certification service which is based on PKI and accredited certification service is PKI based certification service and accredited by the competent minister. Legal value of the electronic signature based on electronic certificate issued by accredited certification service is presumed as valid.

The below figure 1 shows comparison of definitions and requirements of electronic signatures between Europe and Japan.

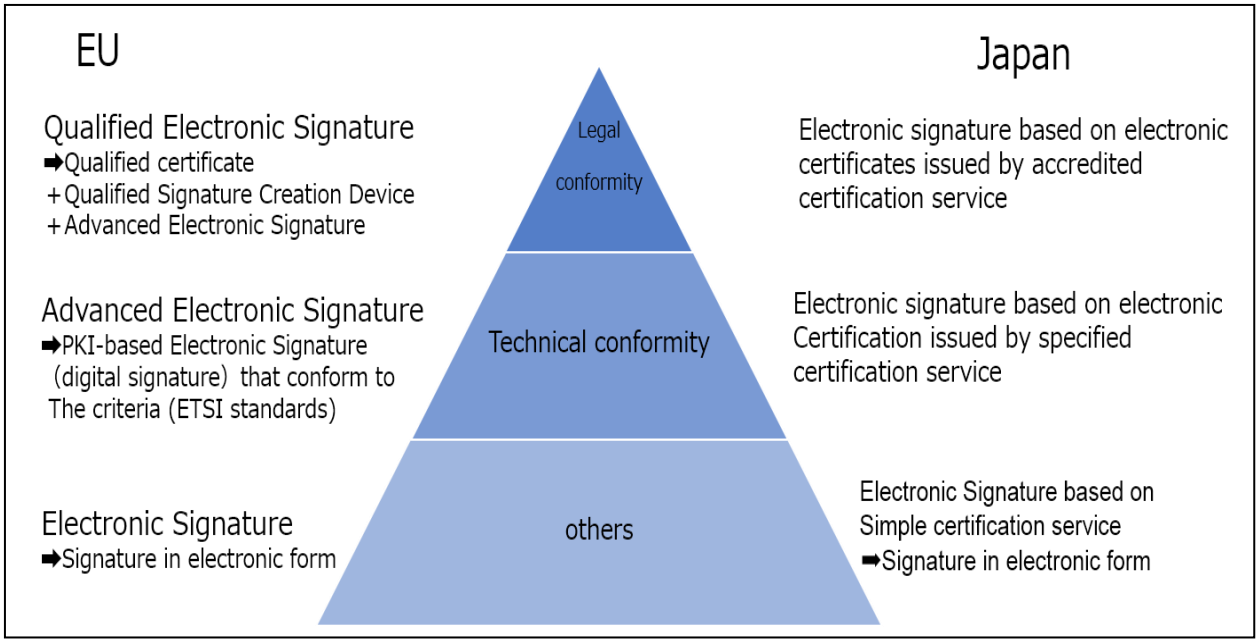

Figure 1. definitions of electronic signature

Although Japanese e-signature law is focusing on how certification business (CAs), both scheme defined 3 different levels. In both scheme, any form of electronic signatures are not denied its legal admissibility by the reason that it is electronic form. Next level of electronic signatures are technically compliant signatures often called as digital signature. Electronic signatures based on public key infrastructure and fulfilling specific algorithm requirements are recognized as digital signature currently in EU and Japan. Highest level is technical conformity plus law conformity and regarded as same as handwritten signature. In both European and Japanese legal framework, only the electronic signature which are categorized as legal conformity, the top part of the triangle in Figure 1, are explicitly recognized its legal value as equal to handwritten signature. Legal value of other electronic signature such as advanced electronic signature and simple electronic signature are not denied but shall be examined at the court in case of conflict. The biggest difference here is the requirements of qualified signature creation device. According to Japanese electronic signature act, it is signatory's responsibility to securely manage the private key therefore, the use of IC card is not mandated. So far, gap regarding the use of hardware token is identified as significant difference between EU and Japan, we recognized this as only one major gap between EU and Japan to be fulfilled in order to mutual recognition possible.

Table 1 provides mapping of electronic signature framework between eIDAS regulation and Japanese e-Signature Act.

Table 1. Mapping of Electronic Signature Framework

	eIDAS	**Japanese e-Signature Act**
Law	eIDAS regulation	Act on Electronic Signatures and Certification Business
Objective	Legal recognition of trust services,	To promote the distribution of e-document through ensuring the smooth use of e-Signatures.
Governor	EU Committee	Ministry of Economy, Trade and Industry. Ministry of Internal Affairs and Communications. Ministry of Justice.
Harmonization Body	EA	N/A
Accreditation body	Member states	Ministry of Economy, Trade and Industry. Ministry of Internal Affairs and Communications. Ministry of Justice.
Certification Body	Supervisory Body	Same as above
Conformity Assessment Body	Conformity Assessment Body	Designated Investigation Organization
Supporting Technical Standards	ETSI Standards, CEN Standards	Accreditation Criteria
Assurance to be achieved	Legal admissibility + Technical Compliance	Legal admissibility + Technical Compliance

4. Audit Scheme of Certification Service Provider

Trust is established by not only the security requirements but also the trust framework. This chapter compares audit the audit scheme between eIDAS regulation and Japanese electronic signature act.

4.1. Audit scheme of eIDAS regulation

In Europe, issuer of qualified certificate shall go through the conformity assessment and certified as qualified trust service provider. Conformity assessment of eIDAS regulation is performed by Conformity Assessment Body accredited by National Accreditation Body and harmonization of accreditation processes among accreditation bodies is ensured by European Co-operation for Accreditation. Below Figure 2 shows typical audit scheme of eIDAS regulation. Successful assessment report is sent to Trust Service Status Notification Body from Conformity Assessment Body and Trust Service Status list will be updated and certification service provider is listed as qualified trust service provider. This list is maintained by each EU member states individually and checked if the certificate used for the electronic signature is issued by one of the certification service provider listed. Audit cycle of conformity assessment is two years, but between two years, a surveillance audit is required.

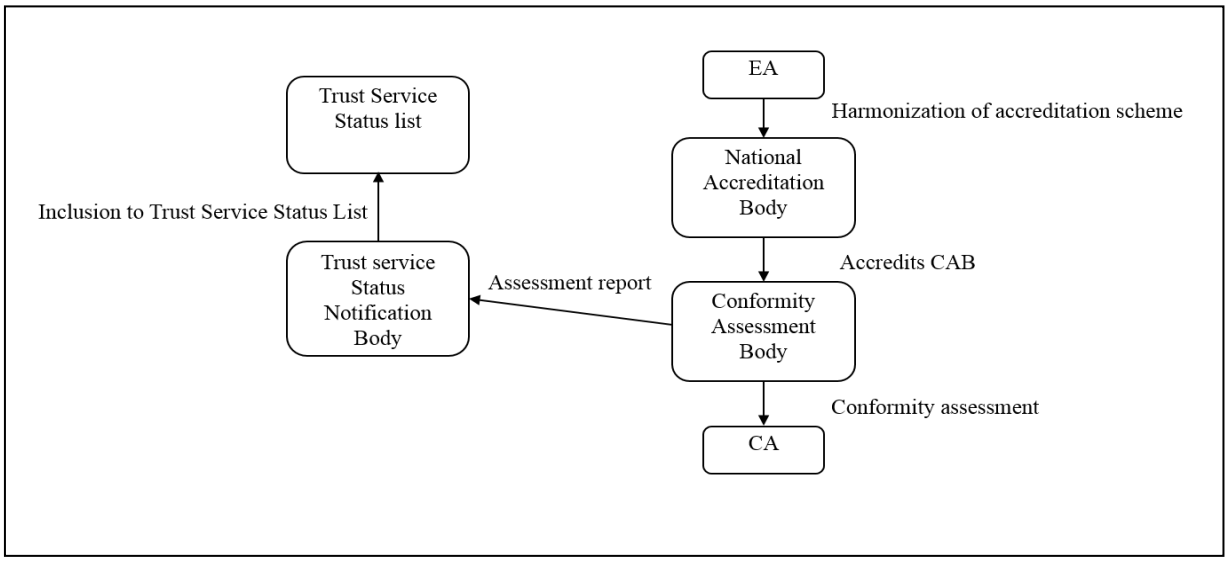

Figure 2. Audit scheme for eIDAS regulation

4.2. Audit scheme of Japanese electronic signature act

Competent Ministers, Minister of Internal Affairs and Communications, Minister of Justice and Minister of Economy, Trade Industry, designated an investigative organization which investigates the conformance of applied certification service. Accreditation status to the applied certification service is granted by Competent Minster when successful investigation is received from the designated investigative organization. Electronic signature based on the certificate issued by accredited certification business is regarded as legally effective signature.

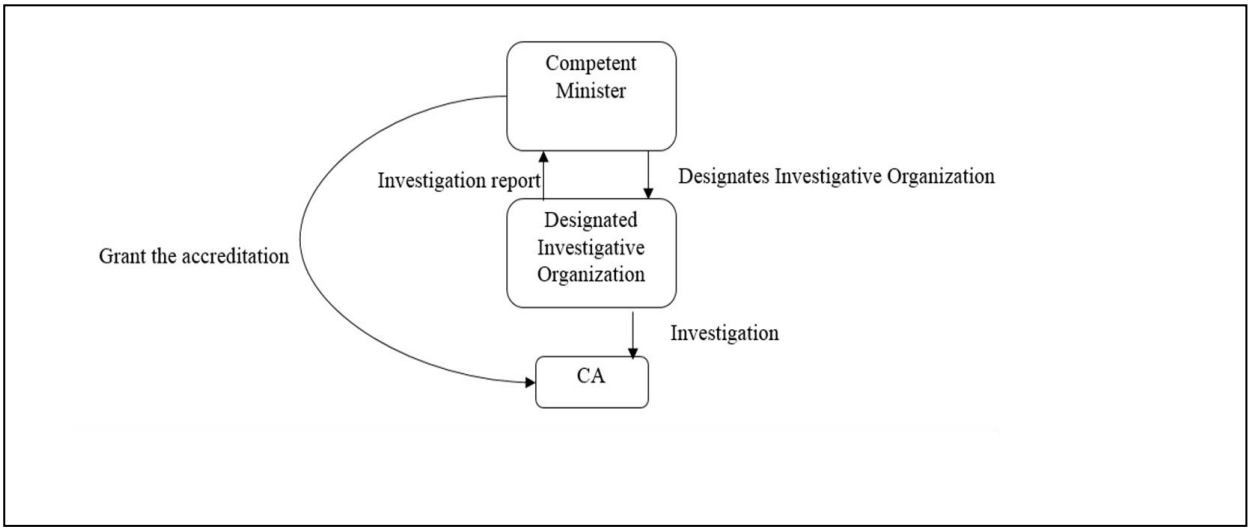

Figure 3. Audit scheme for Japanese electronic signature act

Audit cycle in this scheme is annual and full audit is required annually.

Following deviations are found by comparing the two audit schemes.

- Absence of Trust service status list in Japanese audit scheme
- Absence of the harmonization body for accreditation

Absence of the harmonization body is foreseen as no multiple accreditation body exist in Japanese audit scheme. However, lack trust service status list could be problem for mutual recognition. The role of trust service status list is a trust anchor and without this list, the signature validation software could not automatically check if the certificate used for the

signature is issued by qualified/accredited certification service provider or not.

5. Audit Criteria

5.1. ETSI EN standards

Three set of technical criteria are used as audit criteria in eIDAS compliance audit. EN 319 401 describes general requirements for trust service provider [7], and EN 319 411-1 describes more specific requirement for certification service provider [8] and EN 319 411-2 describes additional requirements for certification service provider issuing qualified certificate [9]. Relation of each standards are illustrated in Figure 4.

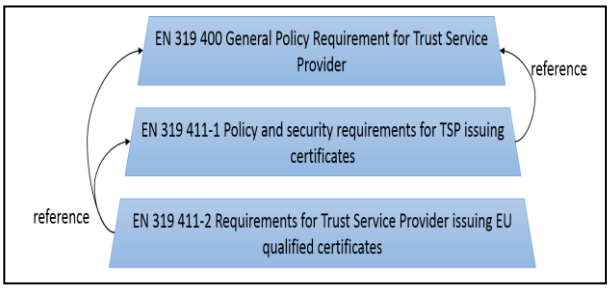

Figure 4. relation among ETSI EN standards

A lot of reference to EN 319 411-1 and EN 319 400 are given in EN 319 411-2, thus the certification service provider issuing qualified certificate shall fulfill the requirements from all three standards.

5.2. Implementing regulation and guidelines for Japanese electronic signature act

Instead of technical standards, implementing regulation and guideline are prepared as a criteria for the audit of certification service provider in Japan. Also, the questionnaire consists of requirements from implementing regulation and guideline together with examples of conformance is prepared. Therefore, to compare with ETSI EN standards, Japanese requirements are more explicit and less freedom for the auditor. Furthermore, Japanese audit criteria has so called sample check system which requires to check actual records of certain amount of issued certificate. The number of samples is determined based on the number of certificates issued by the certification service provider. By comparing the audit criteria for certification service provider between Europe and Japan, following deviations are found.

- ETSI EN standards have more strict requirements for financial aspect
- ETSI EN standards require back ground checks of the personnel which is very uncommon in Japanese culture
- ETSI EN standards have requirements for the termination of the service which enable relying party to verify the electronic signature even after the certification service provider terminates its certification service
- ETSI EN standards include requirements of CA/Browser forum
- Japanese audit criteria have sample check system
- Japanese audit criteria have examples of conformance for each requirement

6. Delviations

6.1. Legal Framework

Japanese electronic signature act does not require the use of signature creation device, i.e. IC card. This is the biggest gap between Europe and Japan. The role of signature creation device is to securely maintain the private key under sole control of the signatory.

6.2. Audit scheme

Although the audit scheme for eIDAS regulation looks more sophisticated, it is due the fact that EU is consist of multiple member states. Except the harmonization body for accreditation, both scheme have same three-layer, applicant (Certification service provider), assessment body and accreditation body. And also, the accreditation body is the governmental organization for both schemes. Lack of trust service status list is the problem when verifying the electronic signature. Also list of accredited certification service providers are published on the governmental web site in Japan, the list is neither machine readable nor securely protected.

6.3. Audit Criteira

ETSI EN standards have more coverage than the Japanese audit criteria and more freedom to the auditor. However, because Japanese audit criteria has examples of conformance for each requirement, the requirements are more explicit in Japan.

7. Mutual Recognition

e-Signature Law in Japan has very simple three-layer model, competent ministers as certification body, designated investigation body as conformity assessment body and CA. At the same time, this is also a part of a common hierarchy structure compared to the eIDAS

model. In order to realize mutual recognition technically, Japanese scheme should have trust status information service such as Trust Service Status List which is currently not available at Japanese scheme.

Below figure 5 shows proposed mutual recognition model between EU and Japan.

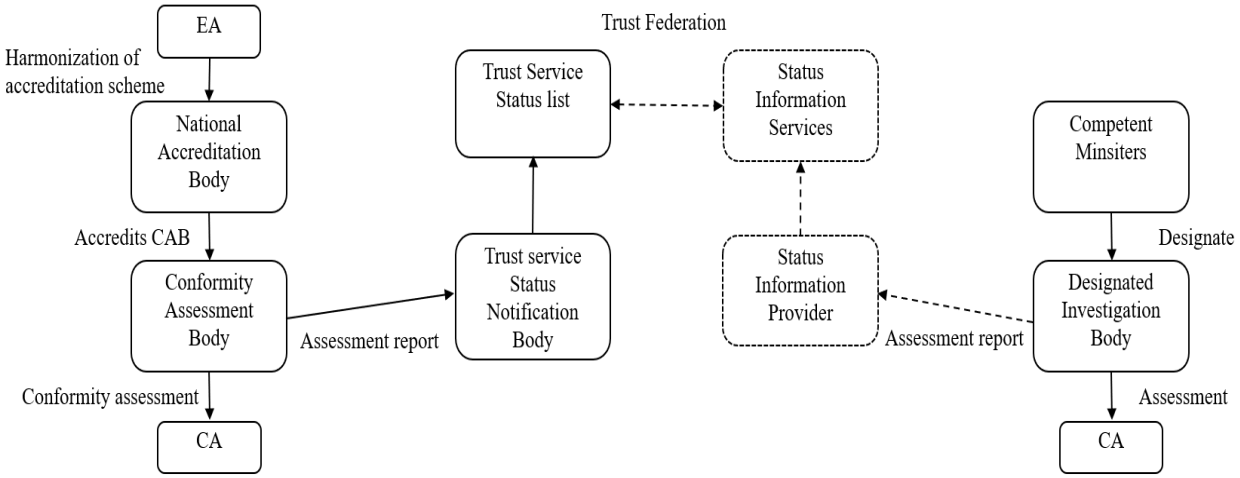

Figure 5. Mutual recognition model

Left side of Figure 5 is the audit scheme of eIDAS regulation represented by Figure 2 and another side is the audit scheme of Japanese e-Signature law with additional dialog drawn with dot line.

What is important in mutual recognition is to make mutual services verifiable. In Europe, trust service status list is used and a list of qualified trust services for each member states. In the mutual recognition model shown in Figure 5, the status information service cooperates to make mutual services verifiable, but since Japan does not have its own status information service, adopting trusted list method (same as EU) is the best solution to realize the technical interoperability.

8. Conclusion

Mutual recognition of electronic signature between Europe and Japan may give the huge positive impact for global industries. Regarding electronic signatures, Japan and Europe have the same three-step definition. However, there are many deviations shall have acknowledged each other. This study identified the deviations from the aspect of legal framework, audit scheme and audit criteria. We have also proposed the mutual recognition model between EU and Japan represented by Figure 5. The biggest deviation is the requirements about signature creation device. Currently no use of secure signature creation device is required in Japanese law and it is up to signatory responsibility to securely manage the private key to be used for electronic signature. Among the legal requirements of electronic signatures of Japan and Europe, it became clear that there is a difference in the handling of hardware tokens. In Europe, it is required by law to store a private key in a security token that has been subjected to security evaluation and generate a signature inside this token, but in Japan there is no legally required use of a hardware token, and even in the present situation, in many cases, private keys are managed on PC. A remote signature is a means to solve this difference. The remote signature is a method of managing the private key of the signer with the cryptographic module on the server side, and the signer performs user authentication to the remote signature server, and as a result, the signer's private key is activated on the server side, and signature generation is performed. According to the eIDAS regulation, even if it is as a remote signature, if it meets certain requirements, it is stipulated that it can be accepted as a qualified electronic signature. In Japan, if the requirements for remote signature in developed the same way as in Europe are, it is not only safer and simpler, but also eliminates the gap related use of hardware token and enables electronic signatures mutually recognizable. So, we suggest when discussing the mutual recognition of electronic signature between Europe and Japan, remote signature could be a good starting point.

We hope our study help to obtain appropriate understanding about the electronic signature between Europe and Japan and give the reference when discussing the mutual recognition of electronic signature.

9. References

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[2] Act on Electronic Signature and Certification Business, Act No. 102 of May 31, 2000, Japan.

[3] Soshi Hamaguchi, Toshiyuki Kinoshita and Satoru Tezuka, "Examination on Possibility on Reuse of Certification Result between Different Assessment Scheme for Certification Authority", The 15th International Conference on Security and Management, Las Vegas Nevada, USA 2016.

[4] Soshi Hamaguchi, Toshiyuki Kinosita and Satrou Tezuka, "An Analysis of Trust Models of Public Key Infrastructure" International Jounal of Control Theory and Application 2016, p. 395-402.

[5] Standards and Industry Regulations Applicable to Certification Authorities, Kirk Hall, Trend Micro, Inc

[6] Certification Authority Criteria in User Perspective, Thijs R. Timmerman, August 2014.

[7] European Telecommunication Standards Institute, ETSI EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, February 2016.

[8] European Telecommunication Standards Institute, ETSI EN 319 411-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements , February 2016.

[9] European Telecommunication Standards Institute, ETSI EN 319 411-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, February 2016.

