

Comparison Report of International Mutual Recognition for Trust Services Infrastructure



Click here for the comparison report
<https://d-trust.sfc.wide.ad.jp/>

Keio University
October 30, 2024

Contributors

Japan	Satoru Tezuka (Project Professor, Keio University Global Research Institute, Keio University)
	Satoshi Kai (Senior Researcher, Keio Research Institute at SFC, Keio University)
	Akira Nishiyama (Senior Researcher, Keio Research Institute at SFC, Keio University)
	Takahiro Fujishiro (Senior Director, Hitachi, Ltd.)
	Akira Sakaino (NTT Communications)
	Hiroshi Nakatake (Managing Director, Representative of the Japan Office, GLEIF)
	Naohiko Sagara (General Manager, Trust Service Sales Dept., SECOM Trust Systems Co., Ltd.)
	Fumiaki Ono (SECOM Trust Systems Co., Ltd.)
	Akihiro Odajima (TEIKOKU DATABANK, LTD.)
	Katsumi Nakamura (Mitsubishi Electric Information Network Corporation)
	Kenji Urushima (GMO GlobalSign K.K.)
	Satoshi Arai (NTT Business Solutions Corporation)
	Miki Okumura (NTT Business Solutions Corporation)
	Saori Matsui (NTT Business Solutions Corporation)
	Masahiro Shikutani (Cybertrust Japan Co., Ltd.)
	Mitsuyoshi Tamura (Cybertrust Japan Co., Ltd.)
	Maiko Ishibashi (Cybertrust Japan Co., Ltd.)
Yasuhiko Yamamoto (Cybertrust Japan Co., Ltd.)	
Europe	Vicente ANDREU NAVARRO (EU Commission, DG CNECT)
	Apostolos Tolis Apladas (EU Commission, DG DIGIT)
	Jean-Emmanuel Perez Hernandez (External Subject Matter Expert, European Commission)
India	Arvind Kumar (Controller of Certifying Authorities (CCA) Ministry of Electronics & Information Tech, New Delhi)
	Aashish Banati (Deputy Controller Ministry of Electronics & Information Technology, New Delhi)
	Vijayakumar Manjunatha (Secretary General, Asia PKI Consortium, Bengaluru, India)
	Vikas Panwar (Country Business Manager for India, GLEIF)

1. Scope and Objectives

To achieve international safe and secure data distribution in cyberspace, International mutual authentication of trust services is necessary. Electronic authentication is designed to prevent spoofing of senders and receivers. Especially in digital trade, it is intended to prevent the spoofing of person, organization, thing, process and product. Electronic signature is used to prevent data tampering. The bilateral infrastructure with electronic authentication and electronic signature is called a Trust Service Infrastructure.

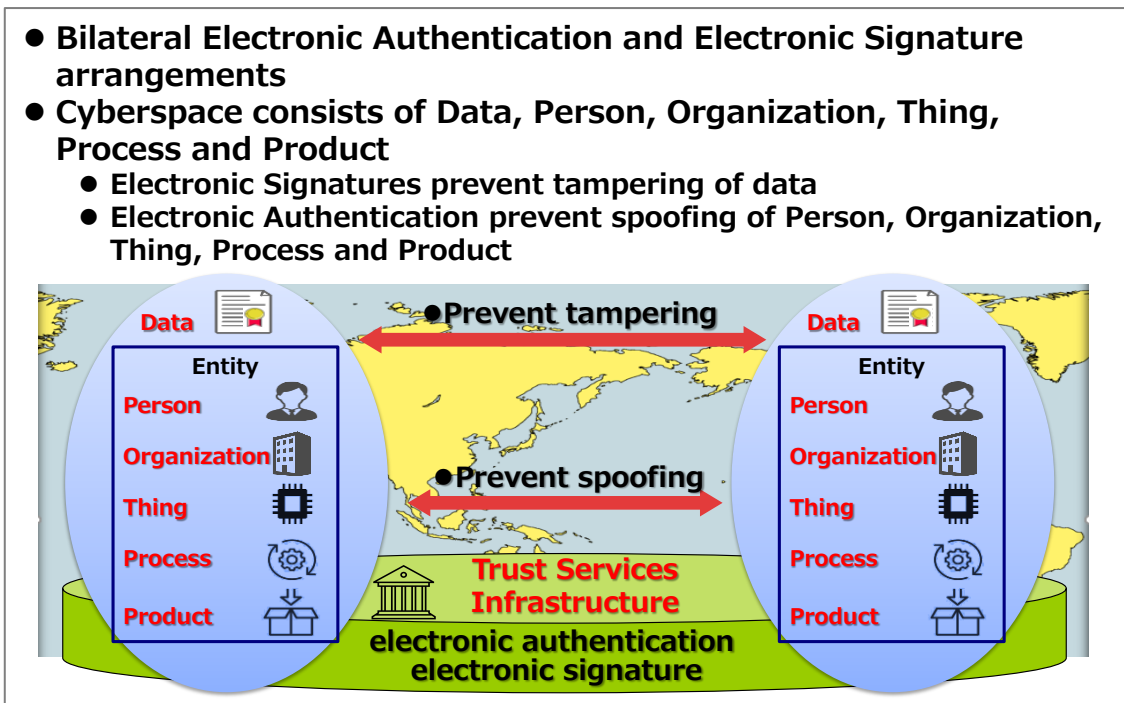


Diagram 1-1: Bilateral Electronic Authentication and Electronic Signature

The DFFT realization is easier to understand if it is organized in three layers. The upper level is the Trust Application Service layer, which performs data input/output and data usage. The middle layer, the Data Distribution Layer, performs secure data exchange between entities. The lower Trust Service Infrastructure layer provides trust to prevent spoofing and tampering.

It can be regarded as the global interoperability of the Trust Service Infrastructure layer is essential to realize DFFT. Therefore, we should achieve international mutual recognition of Trust Service Infrastructure.

● **DFFT is realized with Three-Layered Architecture**

- Trust Application Service Layer: Input/Output of data and use of data
 - Trust Data Distribution Layer: Securely exchange data with entities
 - Trust Service Layer: Trust by preventing tampering and spoofing
- **International mutual recognition of trust service infrastructures is essential.**

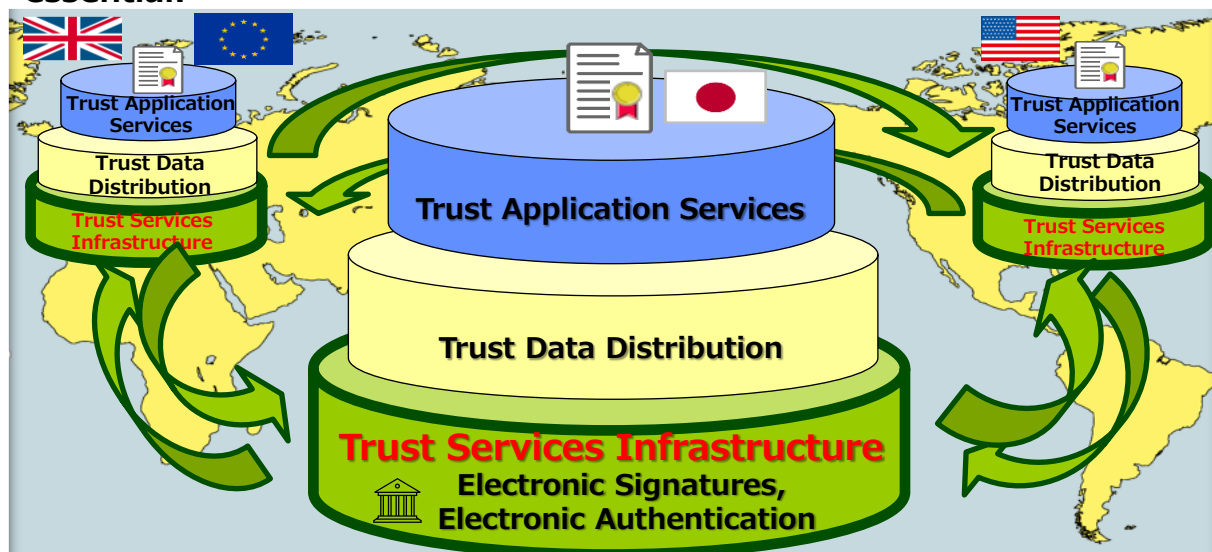


Diagram 1-5: International Mutual Recognition of Trust Services Infrastructure

For the equal footing of the Trust Service Infrastructure, it is best to organize it in four categories. They are (Pillar 1) Legal Context / Legislation, (Pillar 2) Supervision and Auditing System / Accreditation, (Pillar 3) Best Practice / Technology Standard, and (Pillar 4) Trust Representation / Trust Anchor*1 Chain. A comparison of the countries is shown in the table. In this comparison report, (Pillar 3) Technology Standard and (Pillar 4) Trust Anchor Chain are discussed.

*1 RFC 6024 describes "A trust anchor is a public key and associated data used by a relying party to validate a signature on a signed object". In this paper, "A trust anchor is a set of public keys and associated data used by a relying party to validate the legitimacy of trust services and a signature on a signed object" is defined.

- **Realization of International Mutual Recognition**
- Confirmation of the legitimacy of Data, People, Organization, and Things internationally, including the G20 host country, India






	Pillar	EU 	UK 	US 	Japan 	India 
1	Legal context / Legislation	eIDAS	UK-eIDAS	Executive Order 13526.	Public Certification Service for Individuals law Commercial Registration Law Electronic Signature Act	Information Technology Act
2	Supervision and auditing systems / Accreditation	Two steps of EU Commission, Member States	National body	Federal government	National body	National Regulator - Controller of Certifying Authorities (CCA)
3	Best Practice / Technology Standard	ISO, ETSI	ISO	ISO, NIST	ISO, JIS	CCA / WebTrust
4	Trust Representation / Trust Anchor Chain	LoTL, MS TL	UK TL	FBCA	Government BCA	Root Certificate Authority of India (RCAI)

Diagram 1-2: Equal Footing for International Mutual Recognition

2. Comparison Method

2.1 (Pillar 3) Best Practice / Technology Standard

The scope of the technical assessment is not limited to Policy and security requirements for CA alone, but should also consider the all aspect of following

- (1) Policy and Security requirements for CA issuing QC
- (2) Certificate profiles (X.509 items)
- (3) Qualified Signature Creation Device (QSCD)
- (4) Signature format (CADES, XAdES, PAdES, JAdES)

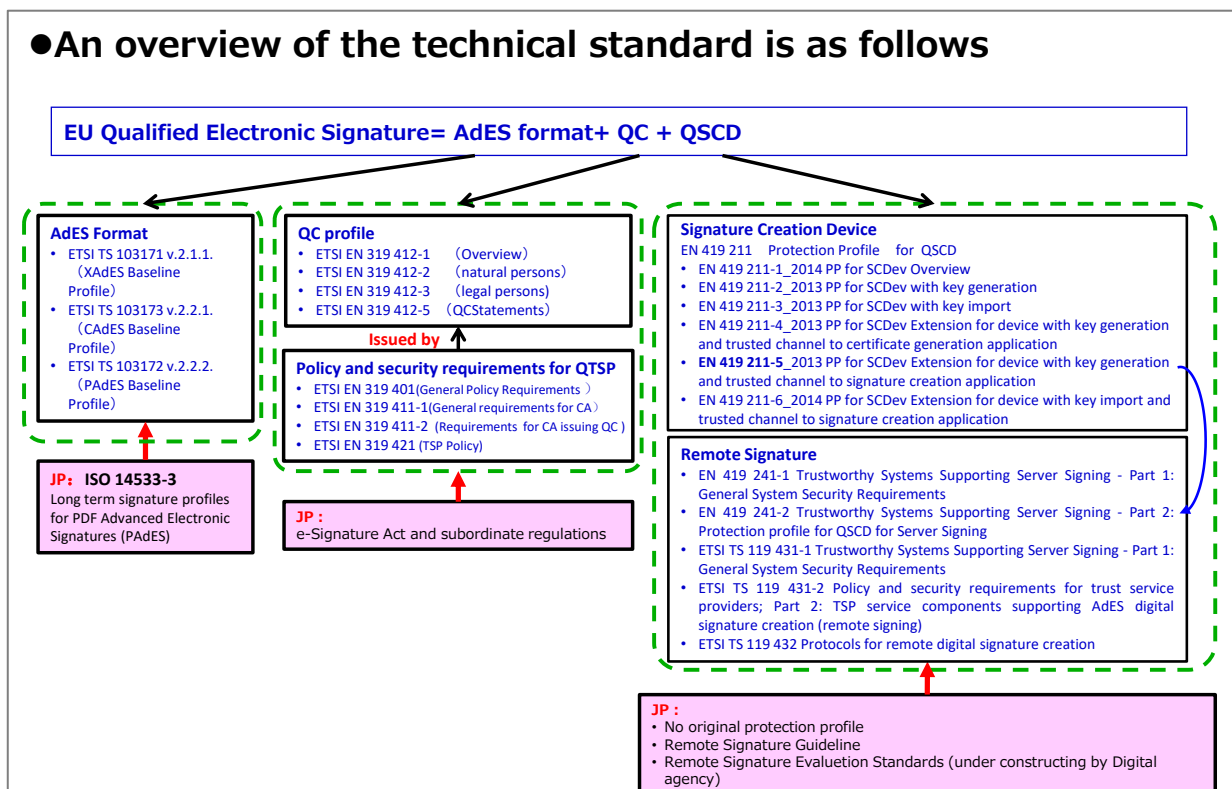


Diagram 2-1: Overview of Policy and Technical Standards for QES

● Major checkpoints should not be limited to the scope of RFC3647, but should be assessed more broadly technically

EU Qualified Electronic Signature= AdES format+ QC + QSCD

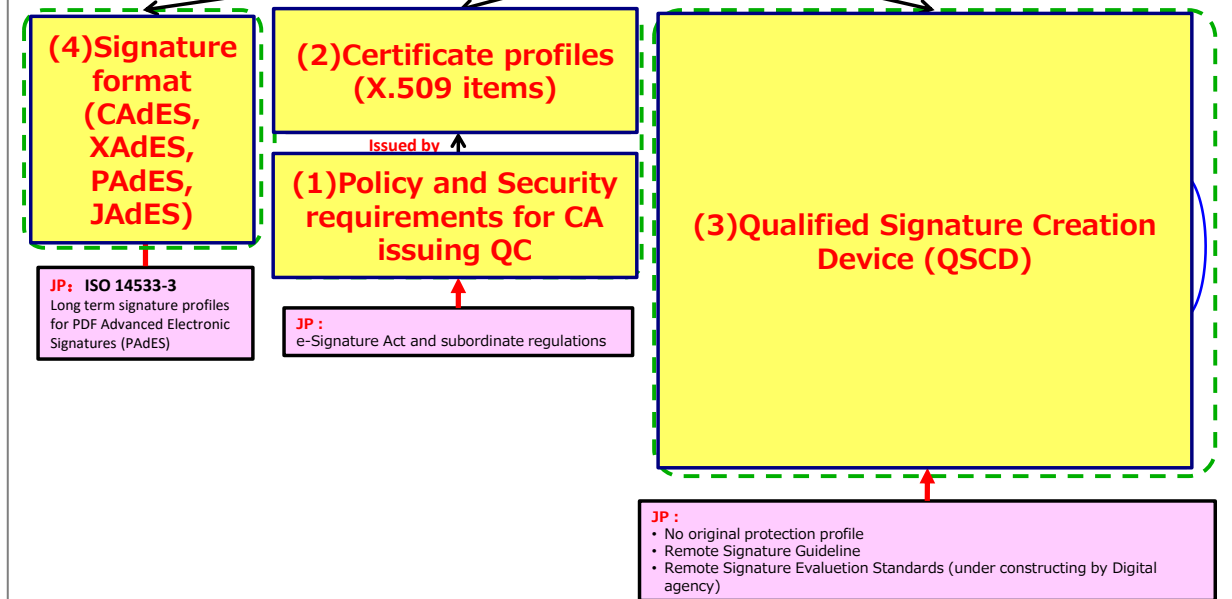


Diagram 2-2: Overview of Major Check Points (1)-(4)

Major Check Points;

(1) Policy and Security requirements for CA issuing QC

We have incorporated the proposed revision at the medium classification level of "the Revised Standard (Draft) for accredited CAs," which we introduced at the last meeting in the modernization of the e-Signature Act. In the coming year, the critical issue will be to position the level of specific evaluation criteria in the e Signature law.

We didn't map the CA Policy of Public Certification Service for Individuals to ETSI standards. This may be out of scope for current work.

(2) Certificate profiles (X.509 items)

This year, the Ministry of Internal Affairs and Communications (MIC) held a study group on e-seals and is discussing establishing an accreditation system for certification authorities that issue certificates for legal persons. The final report will be issued at the end of March.

The next step will be to reflect the policy OIDs and QC statements in the certificate profiles for natural persons in the Signature Act accreditation criteria.

(3) Qualified Signature Creation Device (QSCD)

In the research project of a Digital agency, we are making Evaluation Criteria for Remote Signatures.

We have developed criteria harmonized with ETSI to allow mutual recognition in principle. However, we have added a Japan-specific extension that generates key pairs at the CA and sends them to the RSSP (this is not subject to mutual recognition).

We didn't make the original Japanese protection profile for QSCD but referred to ETSI standards.

(4) Signature format (CAAdES, XAdES, PAdES, JAdES)

Most signature formats used in Japan are long-term signature formats. We refer to ISO and ETSI AdES formats; some long-term signature formats, such as PAdES, are created as JIS standards (Japanese Industrial Standards).

2.2 (Pillar 4) Trust Representation / Trust Anchor Chain

The following are the assumptions for discussing trust anchor chains.

Each country has an official gazette to be established under law, and the Official Journal shall establish a Trusted List Scheme or a Bridge Scheme. This technical report describes the Trusted List Scheme. In the future, when connecting to a country with a bridge system, the legal basis should be traced back to the Official Journal.

In addition, while it is a matter of course to have a Domestic Trusted List, this technical report assumes an International Trusted List for the future. International Trusted Lists are to be utilized for connection with other countries.

- **Structure of Trust Anchor**
 - In the official journal, the country/region will specify the Trusted List system, the Bridge CA system, or both

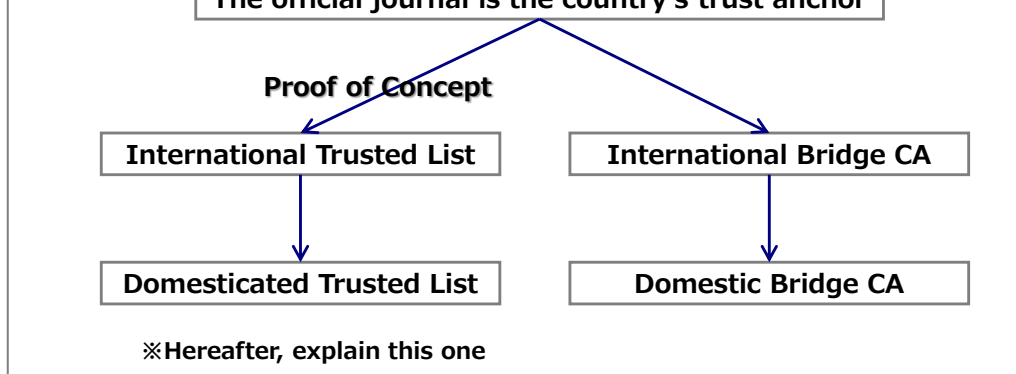


Diagram 2-3: Structure of Trust Anchor

We organize the relationship between the Official Journal and the Trusted Lists into four types.

Method 1 is that each country's Trusted List points to another country's Domestic Trusted List without pointing to another country's Official Journal.

Method 2 is that each country's Trusted List points to another country's International Trusted List without pointing to another country's Official Journal.

Method 3 is that each country's Trusted List points to the Official Journal of the other country and points to the Domestic Trusted List of the other country.

Method 4 is that each country's Trusted List points to the Official Journal of the other country and points to the International Trusted List of the other country.

- **Structure of Trust Anchor**
 - International TLs in each country are classified into 4 methods based on where they point to in other countries

Table: Classification of pointing method from own International TL

	Pointing to existing Domestic TL	Pointing to newly created International TL
Pointing without Official Journal	Method 1	Method 2
Pointing with Official Journal	Method 3 PoC assumption In India-EU-JP	Method 4

Diagram 2-4: Classification of Pointing Method

A comparison of the four methods is described. In outbound from an own country to another country, the point of passing through the own country's International Trusted List is common. On the other hand, inbound from other countries to the own country, Method 1 points directly to the Domestic Trusted List of the other country, Method 2 points to the International Trusted List of the other country, Method 3 points to the Official Journal of the other country, and Method 4 points to the International Trusted List of the other country.

● Comparison of Method 1 to 4

Items		Method 1	Method 2	Method 3	Method 4
Connect	Out-bound	International-TL	International-TL	International-TL	International-TL
	In-bound	Direct access to Domestic-TL (same as access for people in own country)	International-TL -> Domestic-TL	-> Official Journal -> Domestic-TL	International-TL -> Official Journal -> Domestic-TL
Disconnect	Out-bound	International-TL	International-TL	International-TL	International-TL
	In-bound	Disconnect Domestic-TL (Change the pointer of the TL -> affects own country as well)	International-TL (remove from table)	International-TL (remove from table)	International-TL (remove from table)
Selected Result				PoC	

Diagram 2-5: Comparison of Pointing Method

The above discussion has discussed the possibilities of a Trusted List. By the way, looking around each country, some countries (e.g., Indonesia) do not seem to have an Official Journal, and although Method 3 was constructed based on the assumption of an Office Journal, we believe that Method 2 should also remain a possibility, considering its use in a wider range of countries.

3. Comparison Results

3.1 (Pillar 3) Best Practice / Technology Standard

For detailed comparative results, see Annex. In this section, a summary of the results is presented.

(1) Policy and Security requirements for CA issuing QC

In order to compare policy and security requirements between Japan and Europe, RFC3647 was adopted as a common axis for both sides. The policy and security requirements between Japan and Europe were compared for each item in RFC3647, and the results were summarized into the following five categories.

A Equal or Higher

Equal level of Japanese and foreign standards, some Japanese standards in here may be contain more strict requirement.

B Implemented

Not described in the current Japanese standards, but each CA has already implemented this standard. Items that should be added to the Japanese standard (RFC3647 compliant, RFC5280 compliant, etc.)

C Minor differences

Not listed in current Japanese standards and not implemented by accredited CAs. But minor enough to be added as a new Japanese standard, some wording may be changed as needed.

D1. Explanation required

- Items that are unique to Japan and require explanation (certificate of residence, certificate of seal impression, identification by the Individual Number Card (My Number Card) , etc.)

D2. Adjustments required

- Items that are not included in the current Japanese standards and are not fully implemented by CA, but need to be adjusted when adding them as new Japanese standards (e.g., disaster recovery sites, ISMS).

The meanings of A to D2 and the corresponding actions are shown in the diagram.

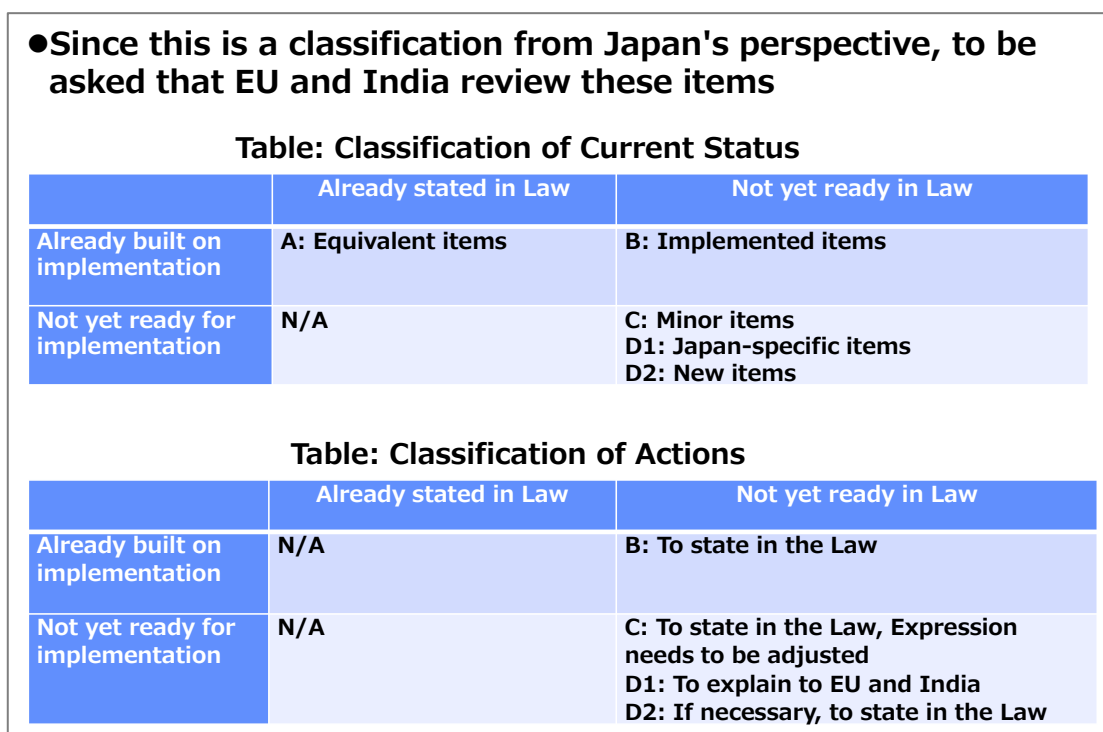
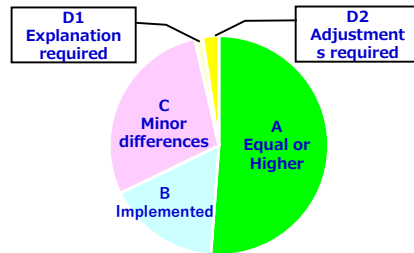


Diagram 3-1: Classification of Current Status and Actions

The results of the comparison are shown below. Results A to C account for 96% of the total.

Classification	# of Items	Rate
A Equal or Higher	43	51.2%
B Implemented	14	16.7%
C Minor differences	24	28.6%
D1 Explanation required	1	1.2%
D2 Adjustments required	2	2.4%
Total	84	100.00%



<Explanation of Classification> ←we have described more precisely

A Equal or Higher

Equal level of Japanese and foreign standards, some Japanese standards in here may be contain more strict requirement.

B Implemented

Not described in the current Japanese standards, but each CA has already implemented this standard. Items that should be added to the Japanese standard (RFC3647 compliant, RFC5280 compliant, etc.)

C Minor differences

Not listed in current Japanese standards and not implemented by accredited CAs. But minor enough to be added as a new Japanese standard, some wording may be changed as needed.

D1. Explanation required ⇒ (See "2b_Flow for Issuance of Digital Certificate.pptx")

- Items that are unique to Japan and require explanation (certificate of residence, certificate of seal impression, identification by the Individual Number Card (My Number Card) , etc.)

D2. Adjustments required

- Items that are not included in the current Japanese standards and are not fully implemented by CA, but need to be adjusted when adding them as new Japanese standards (e.g., disaster recovery sites, ISMS).

Diagram 3-2: Classification Result in new Revised Standard

(2) Certificate profiles (X.509 items)

The ICA Profile, EE Profile, CRL Profile and OCSP Response Profile were compared between Japan and the EU. The results were mostly A, with only a few D1 results.

(3) Qualified Signature Creation Device (QSCD)

There are no QSCD requirements in Japan, so it was not possible to make a comparison.

(4) Signature format (CAAdES, XAdES, PAdES, JAdES)

When the standards between Japan and Europe were compared, they were found to be almost equivalent.

If Japan's Digital Signature Law Modernisation is achieved, the differences between the EU and Japan are small. The assurance level of international mutual recognition can be considered equal and can proceed.

3.2 (Pillar 4) Trust Representation / Trust Anchor Chain

For detailed comparative results, see Annex. In this section, a summary of the results is presented.

First, we will show an image of Japan's domestic mutual recognition. The Japanese official journal is at the top, and international TL and domestic TL are pointed out.

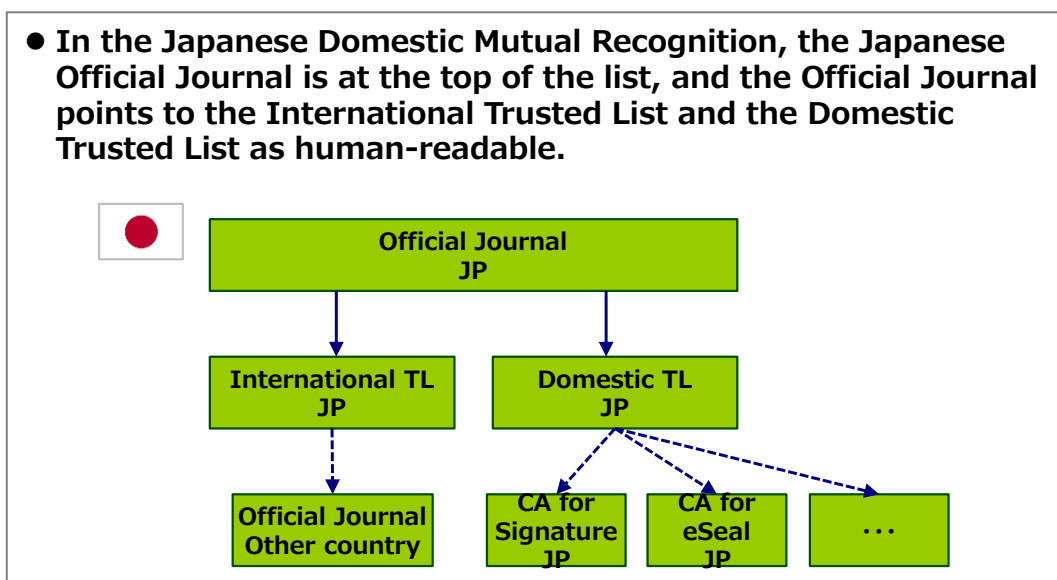


Diagram 3-3: Domestic Mutual Recognition

The following is a diagram showing the image of international mutual recognition. Each country's official gazette will mutually recognize each other based on the agreement. The official journal is the same as domestic mutual recognition, but the response differs for each country.

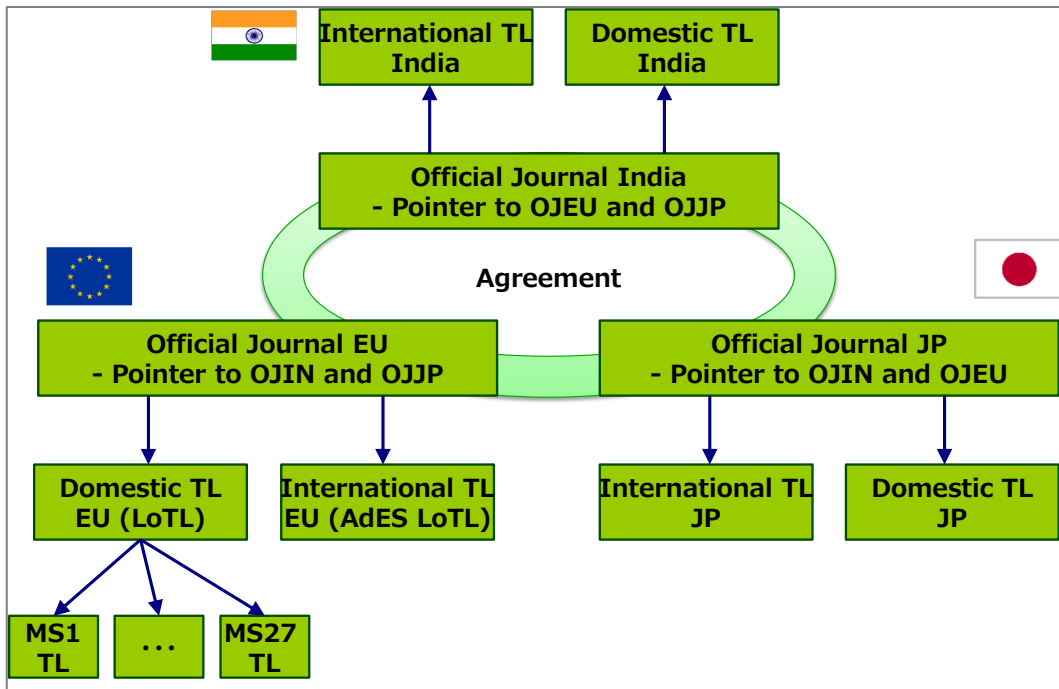


Diagram 3-4: International Mutual Recognition

In some countries, there may be no official gazette. In such cases, a system that points to the International TL rather than the official journal could be considered.

Trusted list mechanism/method for International Mutual Recognition established. That was confirmed by PoC.

4. Proposal

4.1 Proposal from EU

The technical comparison for pillar 4 yielded positive result, with the pilot project demonstrating the suitability and feasibility of using the trusted list mechanism as an interoperability tool for multilateral recognition of trust.

This is a particularly welcome result from the EU perspective confirming and aligning with EU law Regulation (EU) 910/2014 as amended by Regulation (EU) 2024/1183 Art.14.2 which requires that mutual recognition agreement on qualified trust service providers and the qualified trust service they provide ensure that the third parties establish, maintain and publish a trusted list.

On pillar 3, the technical comparison led to further alignment between EU standards and the JP "Revised Standard (Draft) for accredited CAs" with the JP team implementing all suggestion from EU side made over the course of the technical assessment.

The implementation of EU comments set the JP draft standard on a level that can be considered as technically equivalent for the purpose of technical interoperability, with the minor differences remaining considered as not of a nature that would prevent the technical interoperability.

For ensuring continuous maintenance of the technical equivalence over time, considering the frequency of update to EU standards, it is recommended to establish a joint work committee for managing a coordinated strategy to standards update.

Finally, for further progress, as the technical assessment assumed the establishment of a national trusted list and considering that the pilot demonstrated the suitability and feasibility of trusted lists in multilateral recognition of trust services, considering also the current lack of a trusted list in Japan and India, the establishment of a national trusted list at least as a technical interoperability tool (i.e. not necessarily as a constitutive legal instrument as in the EU) in countries looking for multilateral recognition of trust services is highly recommended.

It is also expected that provided trust lists are established in Japan and India, the current achievements will facilitate further progress to the TC AdES LOTL programme of the Commission with inscription of the national trusted lists in the TC AdES LOTL, in parallel to the discussions that will happen at the OECD level in the IAP working group.

4.2 Proposal from JP

In October 2024, Japan's Keidanren (Japan Business Federation) published a proposal "Toward the Establishment of an Industrial Data Space". According to this proposal, one of the actions to be taken by the public and private sectors is the development of a trust infrastructure, indicating its importance.

Excerpts from "Actions to be Taken by the Public and Private Sectors

(2) Development of Trust Infrastructure

Based on the above strategy and timetable, the Digital Agency will systematically develop the necessary environment to establish a Trust Infrastructure (including corporate information (base registry), which is the basic premise for trust and interoperability of the industrial data space, as well as establish operating rules for the industry to properly enjoy the public interest and trustworthiness, and steadily implement them. At the same time, it is necessary to formulate and steadily implement operational rules for the industry to properly enjoy the public interest and reliability.

Source: <https://www.keidanren.or.jp/policy/2024/073.html>

Furthermore, in October 2024, the Digital Policy Forum formulated and published "Proposal: Promoting a Data Governance Strategy. According to this recommendation, one of the specific measures is to improve the environment for Trust Services, and its importance can be seen.

Excerpts from "Specific Measures

(3) Environmental Improvement for Trust Services

The Internet is anonymous by nature, and as the Internet becomes a social infrastructure, it is extremely important to have a mechanism ("Trust Service") to realize trustworthy data distribution. In order to realize Trust Service, it is necessary to have a person's declaration of intention based on the Electronic Signature Act, e-seals to prove the origin or origin of data, and time stamps to prove the existence and integrity of the data.

In particular, it is necessary to clarify the policy on the division of roles between the public and private sectors with regard to Trust Service, which is the basis of data federation infrastructure, and to create an environment to motivate the private sector to invest in the competitive area.

Source: <https://prtimes.jp/main/html/rd/p/000000009.000131931.html>

In Japan, the importance of establishing a Trust Service Infrastructure is being emphasized more strongly from various quarters.

The technical aspects of the PoC have been identified, as described in this comparison report. The next step is to translate this into a system.

Modernization of the electronic signature law must be achieved, implementation of e-seal must be realized, Trust Lists must be established, and international mutual recognition must be ensured.

By meeting these requirements, the differences from the Electronic Signature Act of 20 years ago will be clearly demonstrated, and we will be able to ensure consistency with the legal framework without hindering our equal relationship with the EU.

Change log

Date	Part	Change details
2024/08/23	Whole	Draft version of the report
2024/09/12	Whole	Review and update
2024/10/30	Whole	World Premiere