International Mutual Recognition
A description of trust services in US, UK, EU and JP and the Testbed "Hakoniwa"

Satoshi KAI[1], Takao KONDO[1], Naghmeh Karimi[2], Konstantinos Mersinas[3], Marc Sel[3], Roberto Yus[2], and Satoru TEZUKA[1]

[1]*Keio University, Tezuka-Laboratory, 5322 Endo, Fujisawa, Kanagawa, 252-0882 Japan*

[2]*University of Maryland, Baltimore County, US*

[3]*Royal Holloway, University of London, Department of Information Security, UK*

Keywords: mutual recognition, digital trust, signatures, tampering, impersonation, testbed

Abstract: With the proliferation of digital transactions, trust is becoming increasingly important, as exemplified by the World Economic Forum's Data Free Flow with Trust. Digital signatures are utilized to establish trust to prevent spoofing and unauthorized modification of transmitted digital data. However, the extent of trust is limited by jurisdictions, trusted lists and bridge certificate authorities, and does not have international coverage. For this reason, mutual recognition is needed, i.e. trust relationships established across countries. Establishing mutual recognition is complex and time-demanding due to the legislations, systems, and technologies involved. In parallel, electronic signatures consist of complex systems and structures and, thus, focusing on the technical requirements and solutions can enhance mutual recognition processes. The purpose of our approach is to develop a testbed that can verify technical aspects of mutual recognition. This paper describes the concept of the testbed "Hakoniwa" which includes analyzing the requirements, simulating and testing mutual recognition trust services across US, UK, EU and JP.

1 INTRODUCTION

The Internet of Things (IoT) is generating, collecting, and storing large amounts of digital data as more and more information from the real world can be collected in cyberspace. The IoT enables us to collect more information and reproduce real-world situation in cyberspace in greater detail. This will enable us to understand complex causes, predict future phenomena and consider optimal countermeasures and plans, which were more difficult to achieve before.

On the other hand, digital data has become an object of interest to malicious actors, and it has been subject to the threat of tampering and spoofing. Especially when business applications become highly dependent on digital data, tampering or impersonation of digital data can lead to significant business damages. A typical example includes business email fraud.

Under these circumstances, different countries and organizations are designing measures to protect international digital commerce. For instance, Japan proposed the concept of Data Free Flow with Trust (DFFT) (Digital Agency, 2019) in 2019. DFFT aims to promote the free flow of data internationally, where data useful for business and social issues can freely come and go without regard to national borders, while ensuring trust in privacy, security, and intellectual property.

However, in order for data to be transferred freely without national borders obstacles, it is increasingly necessary to conduct research that includes different perspectives, including legal, technological and societal ones. The authors are conducting research on international mutual recognition in three groups under the international research framework INCS-CoE (INCS-CoE, 2022) project.

- Technical group;
- Human group;
- Ontologies group.

In this paper we present the work of the technical group which develops a testbed for international mutual recognition with the aim of promoting research in this field. In the following sections, we describe the basic concept of the testbed and the selected use cases under consideration.

2 OVERVIEW OF EACH COUNTRY'S TRUST SERVICES

Countries have developed an infrastructure called trust services for the creation, verification, and validation of electronic signatures, electronic seals or time stamps, and their associated certificates (EUR-Lex, 2014), as a mechanism to prevent digital data from being tampered with or spoofed. This chapter describes the status of trust services in each country as shown in Table 1.

Items	EU	UK	US	JP
Legal	eIDAS	UK eIDAS	FICAM program	Electronic Signature Act
Trust service representation	Trusted List		Bridge	

Table 1: Country comparison of trust services.

2.1 European Union

In 1999, a Directive of the European Parliament on a Community framework for electronic signatures was enacted. According to this Directive, an electronic signature is considered equivalent to a handwritten signature. The eIDAS Regulation (EUR-Lex, 2014) is a groundbreaking direct law that ensures a certain level of trust in the data in circulation to allow for secure electronic transactions across different countries within the EU. The eIDAS Regulation has been enforced since 2016 and it gives legal effect to trust services.

Article 3 of the regulation provides a definition of trust services which shows digital signature, e-seal and timestamp etc. Furthermore, it is stated that each trust service "shall not be denied legal effect or admissibility as evidence in legal proceedings solely because it is in electronic form" (EUR-Lex, 2014).

The regulation specifies that a National Supervisory Body (Supervisory Body) is to be established in each EU member state and a Conformity Assessment Body is to be designated to assess the conformity of Qualified Trust Service Providers.

It stipulates that a Trusted List (TL) of qualified trust service providers and services be compiled for each member state, managed and published in a uniform format, and that the information in the list be machine-readable with an electronic signature or e-seal. It also stipulates that the EU will make these national lists publicly available.

As of November 2022, there are 222 qualified trust service providers. A list of these Qualified Trust Services is published in each of the EU Member States in a machine-readable format called a Trusted List (TL). In addition, a List of Trusted Lists (LoTL) (eIDAS, 2022) links all Trusted Lists of the EU member states.

2.2 United Kingdom

The UK eIDAS Regulation (ICO, 2022a) provides the legal framework for the use of electronic trust services offered within the UK and identifies equivalent services offered in the EU. Electronic trust services can be used in a number of ways to provide security for electronic documents, communications and transactions, e.g. to help ensure that documents sent electronically have not been altered in any way and that the sender can be easily authenticated. Electronic trust services allow for such security properties to be applied and then validated and thus help ensure confidence in the electronic transfer of information.

While being a member of EU, UK's trust services were listed on the UK TL (ICO, 2022b), which is linked from the EU LoTL. After leaving the EU, UK maintains its own UK TL according to UK eIDAS[1].

2.3 United States

The United States (US) consider threats on its digital information and communications infrastructure as a significant security challenge. In order for the federal government to address these threats, the security control measures necessary to prevent and detect unauthorized access to federal information technology networks, systems, and data are critical. The Federal Identity, Credential, and Access Management (FICAM) (FICAM, 2022) initiative is a means for addressing the nation's cybersecurity needs. FICAM's recommendations include increasing the authentication strength of individuals and devices, using privacy-enhancing technologies, and expanding the availability of identity management capabilities to address cyber threats.

If the functions of Identity, Credential, and Access Management (ICAM) for each agency run independently, users are forced to deal with multiple incompatible credential, authentication, and access control functions. In addition, each ICAM function has a separate administrative interface used for

[1] https://tl.ico.org.uk/uktrustedlist/UKTL.xml

registration and authorization management, which would result in redundancy and inefficiency if left to each agency. Therefore, when establishing functions for use across federal applications, users needed to re-establish credentials by providing identity proof in each system across the federal government. For that reason, the Federal PKI Trust Architecture (GSA, 2022)] was developed and consists of the Federal Bridge Certification Authority (FBCA) and the Federal Common Policy Certification Authority (FCPCA).

2.4 Japan

The Electronic Signature Act of 2001 (Ministry of Justice, 2022) establishes a legal foundation for electronic signatures that is of equal validity to handwritten signatures and seals. The Act states the presumption that an electromagnetic record (e.g., an electronic document) is authentic when it is signed by a certain electronic signature of the person in question.

The structure of the Japanese Certification Authorities is based on the Government Bridge CA (GPKI, 2022) as its core, which is interconnected with the GPKI (Government PKI), the LGPKI (Local Government PKI), the Commercial Registration CA, and the JPKI (Japanese PKI). In addition, private accredited certification authorities (JIPDEC, 2022) are connected to the Government Bridge CA under the Electronic Signature Act.

3 BASIC CONCEPT

There exist trust services which work in one country or one region, but trust services amongst countries or regions can be challenging. One solution for global trust services is having a centralized trust service as shown in Figure 1(a). Although there are some example of centralized trust services (Adobe, 2023), such a solution has significant political, technical and ethical considerations. Another solution is a mechanism called mutual recognition according to which what is recognized as a trustworthy entity in one country or region is also recognized as trustworthy in another country or region. In this fashion, trust services are connected to each other in a decentralized manner as shown in Figure 1(b).

Without mutual recognition, trust services need to conform to the norms of the country or region where they are accepted. On the other hand, if mutual recognition is in place, then a country's own national customs become trust for other countries and regions. Especially since digital trade is becoming commonplace, if following a country's or region's trust services style becomes a trustworthy entity for another country or region, the cost-effectiveness of trust verification can be improved. Such cost-effectiveness can be achieved by the following means:

- Scope increase for trust service verification, via mutual recognition;
- Equal footing with one's own country or region.

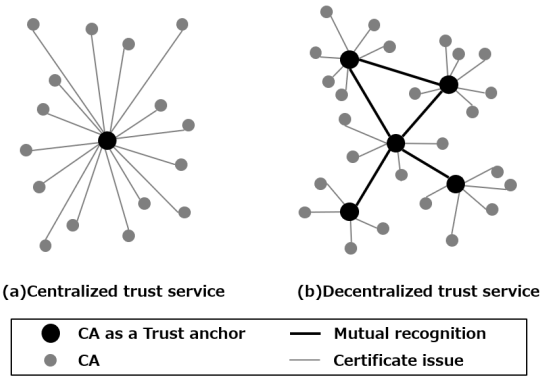

Figure 1: Centralized versus Decentralized Trust Services (adapted and modified from (Baran, P. , 1964)).

Focusing on mutual recognition, we identify two practical models for connecting domains of trust: one based on the Trusted Lists and the other based on the Bridge (or Bridge CA) type, as shown in Figure 2. Both these models require, for the sake of simplicity, one Bridge CA or TL which cross-certifies each CA in its domain (e.g. in one country) in a connected certification fashion. Then, there is cross-certification of the corresponding entities (Bridge CAs or TLs) across countries via mutual recognition. We do not consider certification hierarchies here, as having a single Root CA at international level is more challenging than establishing the pair-wise mutual recognition. We also do not consider certificate chains since, at governmental, country level, a connected certification model reduces the complexity of the verification process. In verifying certificates issued by the trust service, path finding, path verification, and equal footing are common to both types. For this purpose, it is necessary for a country or region to support both the Trusted List type and the Bridge type. In this study, we proceeded under the assumption that Japan supports both types.

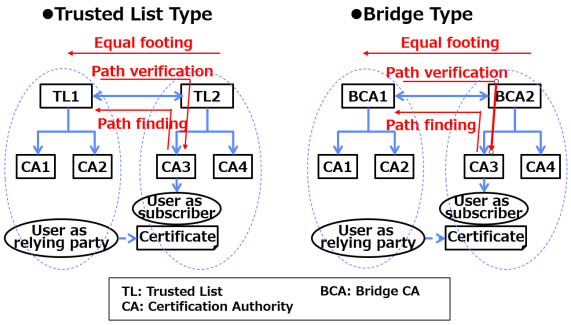

Figure 2: Two types of mutual recognition.

4 MUTUAL RECOGNITION TESTBED "Hakoniwa"

Mutual recognition takes time to be established because of the variety of laws, systems, and technologies involved. On the other hand, since digital signatures consist of complex systems, exploring possible technical solutions can enhance mutual recognition processes. A trust service infrastructure based on international mutual recognition is built at Keio University so that it can be easily accessible. This section describes the testbed requirements for mutual recognition.

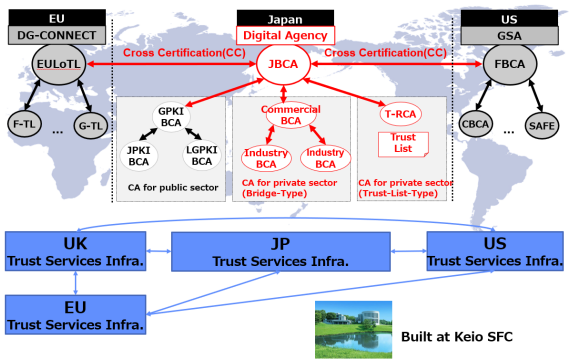

Figure 3: Overall picture of testbed.

4.1 Trust service verification in each country or region

The testbed enables us to simulate the verification of trust services in each country and region. All trust services include servers for signature and certificate verification, as shown in Table 2.

- The EU trust service infrastructure includes EU LoTL and MS TL.
- The UK trust service infrastructure includes the UK TL.
- The US trust service infrastructure is equipped with the FBCA (Federal Bridge CA).
- The JP trust service infrastructure includes a tentative JP TL and JBCA hypothetically.

Items	EU	UK	US	JP
Trusted List representation	EU LoTL MS TL	UK TL	N/A	(New) JP TL
Bridge representation	N/A	N/A	FBCA	(New) JBCA

Table 2: "Hakoniwa" trust service design.

4.2 Trust service verification according to mutual recognition

The testbed enables to simulate technical part of mutual recognition between countries.

- Tentative mutual recognition between Trusted Lists.
- Tentative mutual recognition of Bridge CAs.

Mutual recognition between the Trusted List type and the Bridge type will be achieved through Japan by having Japan support both types of representation.

4.3 Provides an easy-to-use API from the application

The testbed enables us to verify both the signature and certificate issued by the trust service. For the purposes of usability, the testbed provides two types of interfaces:

- A Web interface for direct human operation; and
- REST API for machine-readable.

REST API is for IoT devices that supports communication between web applications. In most cases, JSON is used over HTTP for data transfer.

5 TESTBED "Hakoniwa" BASIC DESIGN

The trust service infrastructure was configured as virtual machines and virtual networks. This section provides an overview of these. The trust service infrastructure in each country will enable the verification of Qualified Services for each country.

5.1 Countries' network and server designs

The virtual network for "Hakoniwa" is shown in Figure 4. The virtual network was configured by

dividing it into segments that simulated the networks of different countries. From the management network, each country's network can be accessed. The networks in each country are also mutually accessible.

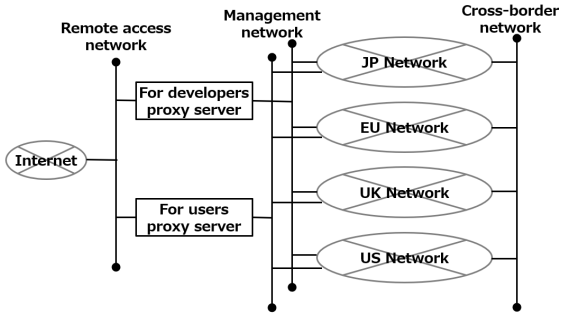

Figure 4: Virtual network configuration.

Figure 5 shows the server configuration within the JP network. The server configuration consists of (a) certificate issuing, (b) signature generation, and (c) signature verification and certificate validation. One feature of the Japanese network is hypothetically that it is equipped with both Trusted List type verification and Bridge type verification. This server configuration enables path finding, path verification, and equal footing for both types.

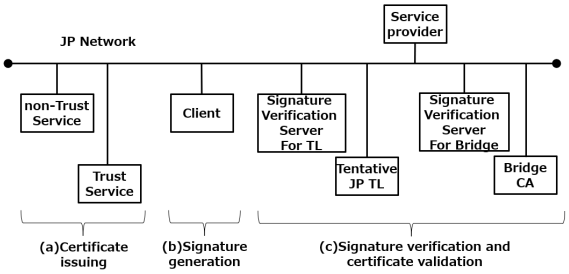

Figure 5: JP server configuration

The server configuration of the EU network is shown in Figure 6. As in the Japanese case, it consists of (a) certificate issuing, (b) signature generation, and (c) signature verification and certificate validation. One additional feature is that the Trusted List type consists of two levels, i.e., a Trusted List for EU member states and a List of Trusted Lists for the EU as a whole.

The server structure of the US network is shown in Figure 7 and it consists of (a) certificate issuing, (b) signature generation, and (c) signature verification and certificate validation, as in JP (Figure 5) and the EU (Figure 6). One feature of US is that bridge CAs are multi-tiered.

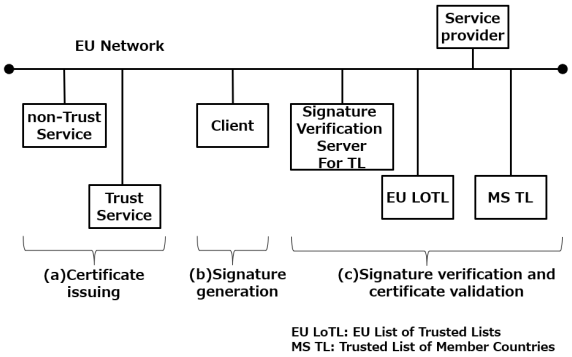

Figure 6: EU server configuration.

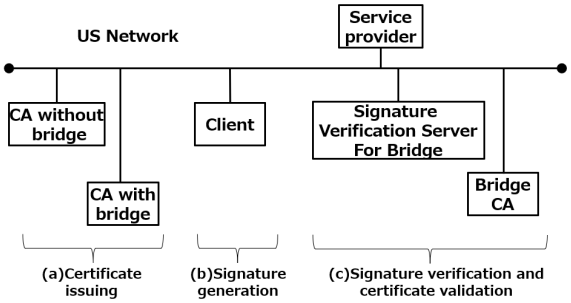

Figure 7: US server configuration.

5.2 Mutual recognition between countries

This section describes the logical connection between Trusted Lists and Bridges, respectively, in order to technically realize mutual recognition. This mutual recognition allows verification across countries, unlike trust services that are confined in each country.

5.2.1 Trusted List type

In our approach, it is assumed that JP TL and EU LoTL are equivalent and mutually recognized by JP and EU LoTL for path construction, path verification and equal footing. Their relationship is shown in Figure 8. The JP TL points to the EU LoTL by URI (Uniform Resource Identifier) and includes a public key certificate to verify the digital signature of the EU LoTL. Conversely, the EU LoTL includes a public key certificate to verify the digital signature of the JP TL, along with a URI to point to the JP TL.

As shown by the real line, when signing in the EU and verifying in JP, the path is traced from the JP TL to the EU LoTL and then to the MS TL. Conversely, as shown by the dotted line, in the case of signing in JP and verifying in the EU, the path starts from the EU LoTL and ends at the JP TL.

The information for equal footing is shared between LoTL and JP TL in the same sense of qualification. LoTL specifies JP TL's qualified

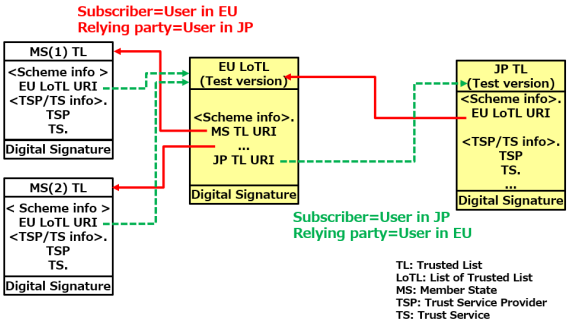

Figure 8: Trusted list type mutual recognition.

digital signature (a digital signature that conforming to hypothetical Japanese law), e-seal (an electronic signature that authenticates that the document was issued by a legal entity), and time stamp as EU-equivalent qualified services, respectively, while JP TL does the same. and EU's qualified digital signature, e-seal, and timestamp are each designated as a qualified service equivalent to JP. The information for this equal footing i.e. equivalent meaning of each trust services, is outside the scope of this study, although it is important to highlight that there are legal challenges for mutual recognition, beyond the technical ones.

The specification of such equivalent meaning is addressed by the ontology team. Two approaches are followed. The first approach consists in the creation of a new ontology by integration of existing relevant ontologies. The second approach makes use of enterprise data created and made public under controlled conditions to add instance data to a knowledge graph. The trustworthiness evaluation policy is extended to make use of this additional information during evaluation. The enterprise data from GLEIF[2] is used as instance data. The $\mathcal{TE}$ (Trustworthy Ecosystem) ontology proposed by Sel (Sel and Mitchell, 2021) is used to build the knowledge graph. Querying the graph allows a trustor to interpret information about a potential trustee according to a trustworthiness policy with semantics that are formally specified in OWL Description Logic.

5.2.2 Bridge type

Japan already has a government Bridge CA, but its purpose is to verify LGPKI and JPKI, not a Bridge CA to connect to other countries. Since the FBCA is originally intended for Bridge certification with legacy CAs and CAs in other countries, it was assumed that existing FBCAs would be connected to the JBCA. A diagram of the relationship between Bridge CAs is shown in Figure 9.

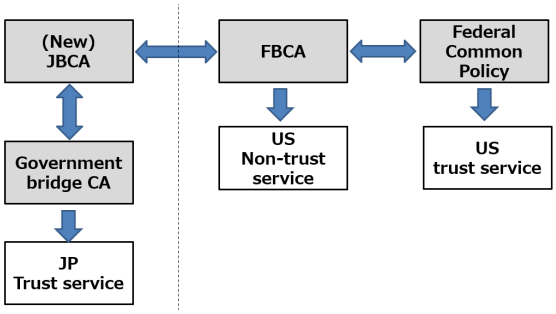

Figure 9: Bridge type mutual recognition.

Information for equal footing is shared in the JBCA and FBCA mutual authentication certificates. In certificates issued by the JBCA to the FBCA, the certificate policies defined in the CP/CPS of the FBCA will be mapped to the JP's certificate policies. For certificates issued by the FBCA to the JBCA, the certificate policy defined in the CP/CPS of the JBCA will be mapped to the US certificate policy. These mappings are expressed as correspondence between the OIDs of the certificate policies.

5.3 Digital signature and verification flow

The flow of signature creation in EU and signature verification in JP is shown in Figure 10. In the figure, the upper part in white is the application and the lower part in blue shading is the trust service infrastructure.

(a) The EU client generates a key pair, and the EU trust service grants a certificate to the public key.

(b) The EU client signs the document with its own private key. The client passes the three sets (document, signature, and public key certificate) to JP.

(c) Upon receiving the three-piece set, the JP client verifies the signature and the certificate using the trust service infrastructure. Those results are output as a verification report.

The flow of signature generation by JP and signature verification by EU is shown in Figure 11. Verification is the reverse process to the explanation shown in Figure 10, from EU to JP.

In both cases, the common point is that the relying party verifies the signatures created in other countries using its own trust service infrastructure and the relationship this infrastructure established with the other trust service infrastructure.

[2]publicly published daily, available at https://data.world/gleif

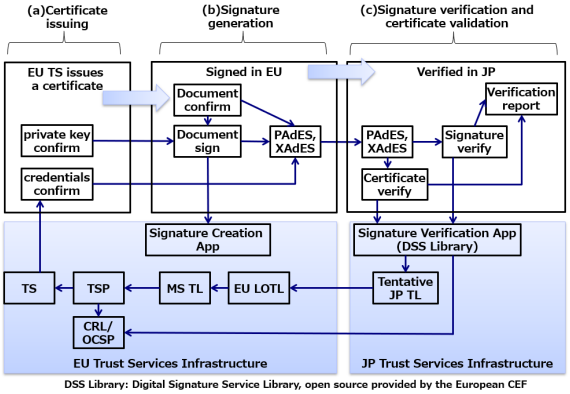

Figure 10: Verification flow when EU entity is as subscriber; JP as relying party.

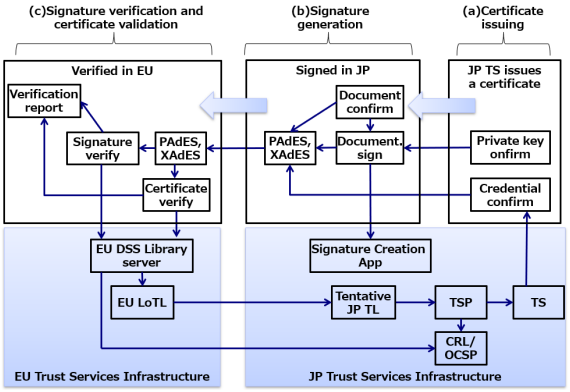

Figure 11: Verification flow when JP entity is as subscriber, EU entity as relying party.

6 FUTURE RESEARCH AND USE CASE

A use case to demonstrate mutual recognition considering invoices across countries is work in progress, as shown in Figure 12.

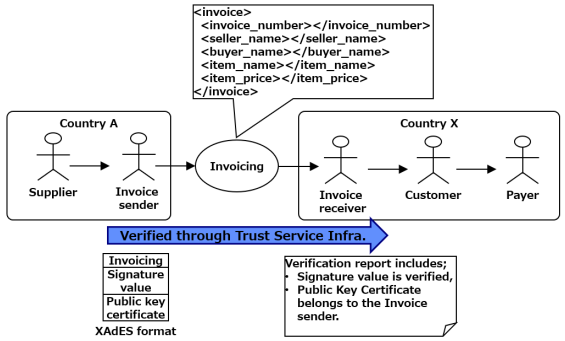

Figure 12: Sample showcase of invoicing.

The scenario is as follows: a supplier in country A sends goods or services to another country X, and issues an invoice. The sender in country A signs the invoice with his/her private key and sends the three variables (invoice, signature value, and public key certificate, these are all included in XML Advanced Electronic Signature, XAdES format) to another country X. In another country X, the recipient verifies the above 3-variable set with its own trust service infrastructure. At this point, the mutual recognition mechanism (path finding, path verification and equal footing) verifies the validity of the certificate of one country A. In country X, after the verification of the invoice validity, the amount of goods is be paid.

Indicatively, from the standpoint of Japan, the Bridge CA method can be utilized, but Trusted Lists are not an available option yet. Table 3 depicts the envisioned items to be verified.

No.	Item	Description
1	Verification of List of Trusted Lists	Verify the authenticity and integrity of the List of Trusted Lists (XML).
2	Verification of Trusted Lists for each country	Verify the authenticity and completeness of the Trusted List (XML). Do this for the number of countries included in the List of Trusted Lists.
3	Retrieval of listed trust services that match the certificate	Use the Trusted List to obtain information on trust services that match the certificate at a specific date and time.
4	Determination of Qualified Certificates	The Trusted List is used to determine which type of qualified certificate matches at a particular date and time. Type of qualified certificate is one of qualified digital certificate, qualified e-seal, qualified website authentication certificate
5	Determination of Qualified Signature/e-Seal Generating Device (QCSD)	Using the Trusted List, determine that the private key corresponding to a qualifying certificate is present in the QCSD at a particular date and time.
6	Determination of Qualified Time Stamp	Use the Trusted List to determine that the timestamp token was a qualified timestamp at the time it was generated.

Table 3: Verification item for trusted list type.

Future research tasks include:

- The creation of the aforementioned use case;
- An analysis of the requirements for consistency of trust services components for equal footing, and
- The mapping of these requirements against legal interpretations.

7 CONCLUSION

There is a mutual recognition mechanism for trust services which are recognized as qualified in one

country to be also recognized as qualified in another. It will take a considerable amount of time for mutual recognition to become operational. In this study, we present a testbed to try out mutual recognition from a technical perspective. The testbed simulates the trust service infrastructure of the EU, UK, US, and Japan, and examines both the Trusted List and Bridge CAs methods of mutual recognition across countries to be tested. Future research involves the expansion of these methods into semantic representations to allow for the internalisation of trust services.

Acknowledgements

This research was partially supported by grants from the International Cyber Security Center of Excellence (INCS-CoE). We would also like to thank Prof Niki Panteli, from Royal Holloway, University of London, for her support and contribution.

REFERENCES

Adobe (2023). Adobe Approved Trust List. https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html, accessed 2023-2.

Baran, P. (1964). On Distributed Communications. Memorandum RM-3420-PR.

Digital Agency (2019). Data Free Flow with Trust. https://www.digital.go.jp/policies/dfft/, (in Japanese), accessed 2022-11.

eIDAS (2022). Trusted List Browser. https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home, accessed 2022-11.

EUR-Lex (2014). EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG, accessed 2022-11.

FICAM (2022). Federal Identity, Credential, and Access Management (FICAM). https://playbooks.idmanagement.gov/arch/, accessed 2022-11.

GPKI (2022). Government Certificate Infrastructure (GPKI), Government Authentication Infrastructure. https://www.gpki.go.jp/(inJapanese),accessed2022-11.

GSA (2022). Trust Services. https://www.idmanagement.gov/buy/trust-services/, accessed 2022-11.

ICO (2022a). Information Commissioner's Office, Guide to eIDAS. https://ico.org.uk/for-organisations/guide-to-eidas/, accessed 2022-11.

ICO (2022b). Information Commissioner's Office, UK Trusted List. https://ico.org.uk/for-organisations/guide-to-eidas/uk-trusted-list/, accessed 2022-12.

INCS-CoE (2022). International Cyber Security Center of Excellence (INCS-CoE). https://incs-coe.org/, accessed 2022-11.

JIPDEC (2022). Japan Information Economy and Society Promotion Association, List of Accredited Certification Services. https://www.jipdec.or.jp/project/designated-investigative-organization/accredited-ca-list.html,accessed2022-11.

Ministry of Justice (2022). Overview of the Electronic Signature Act. https://www.moj.go.jp/MINJI/minji32-1.html(inJapanese),accessed2022-11.

Sel, M. and Mitchell, C. J. (2021). Automating the evaluation of trustworthiness. In Fischer-Hübner, S., Lambrinoudakis, C., Kotsis, G., Tjoa, A. M., and Khalil, I., editors, *Trust, Privacy and Security in Digital Business - 18th International Conference, TrustBus 2021, Virtual Event, September 27-30, 2021, Proceedings*, volume 12927 of *Lecture Notes in Computer Science*, pages 18–31. Springer.

Appendix

Abbreviations

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DSS	Digital Signature Service
EC	European Commission
EU	European Union
EUMS	European Union Member States
FBCA	Federal Bridge CA
GPKI	Government PKI
JBCA	Japanese Bridge CA
JP	Japan
JPKI	Japanese PKI
LGPKI	Local Government PKI
LOTL	List Of Trusted Lists
MS	Member State
OCSP	Online Certificate Status Protocol
PKC	Public Key Certificate
PKI	Public Key Infrastructure
OID	Object Identifier
QC	Qualified Certificate
QSCD	Qualified Signature/e-Seal Creation Device
TL	Trusted List
TSA	Time-Stamping Authority
TSL	Trust-service Status list
TSP	Trust Service Provider
TST	Time-Stamp Token
XAdES	XML Advanced Electronic Signature