Lessons from existing practices of cross-border mutual recognition mechanism

Sung Heun Ha

Note

This study report is prepared by the author for contribution to discussion on mutual recognition mechanism for trade related data and documents in electronic form. This is a draft for review in the 8th Meeting of the Legal and Technical Working Groups on Cross-border Paperless Trade facilitation, not for circulation or citation. After incorporating comments received from review, it will be published as an ASIA-PACIFIC RESEARCH AND TRAINING NETWORK ON TRADE (ARTNeT) working paper.
# Contents

1. **Introduction** ............................................................................................................................. 1

2. **Cross-border Mutual Recognition cases of non-electronic transactions** ........................................ 2

   2.1 **Authorized Economic Operator** ......................................................................................... 2

   2.1.1 Elements of AEO MRA ......................................................................................................... 3

   2.1.2 Challenges in AOE MRA ......................................................................................................... 4

   2.1.3 Summary and implications ...................................................................................................... 6

   2.2 **APEC TEL MRA** .................................................................................................................. 7

   2.2.1 Summary and implications ...................................................................................................... 11

   2.3 **ILAC MRAs** ........................................................................................................................... 12

   2.3.1 Summary and implications ...................................................................................................... 14

3. **Cross-border Mutual Recognition cases of electronic transactions** .................................................. 15

   3.1 **eIDAS** .................................................................................................................................... 15

   3.1.1 Requirements for mutual recognition ...................................................................................... 18

   3.1.2 Control of a mutual recognition scheme .................................................................................. 22

   3.1.3 Challenges and lessons from the eIDAS experience ................................................................ 25

   3.1.4 Summary and implications ...................................................................................................... 27

   3.2 **PAA PKI Mutual Recognition Framework** ............................................................................... 28

   3.2.1 Stakeholders ............................................................................................................................ 29

   3.2.2 Inputs and tools ....................................................................................................................... 29

   3.2.3 How the PAA PKI recognition framework operates .............................................................. 30

   3.2.4 Challenges and lessons from the PAA Mutual Recognition scheme set-up experience .......... 33

   3.2.5 Summary and implications ...................................................................................................... 33

4. **Attributes that form cross-border recognition schemes** .................................................................... 34

   4.1 **Key stakeholder group** ......................................................................................................... 37

   4.2 **Legal group** ............................................................................................................................ 37

   4.3 **Operational group** .................................................................................................................. 37

5. **Conclusion** ....................................................................................................................................... 38
List of tables

Table 1. APEC TEL MRA participating member economies .................................. 10
Table 2. Common key attributes for establishing and operating cross-border mutual recognition schemes ................................................................. 35
Table 3. Three groups of MRA attributes ........................................................... 36

List of figures

Figure 1. General multilateral recognition arrangement of conformity assessment ........................................................................................................ 2
Figure 2. Relationships among entities under an MRA ........................................ 9
Figure 3. ILAC Organization Chart ................................................................. 14
Figure 4. The e-Transaction workflow of eIDAS ............................................. 17
Figure 5. Scope of eIDAS ............................................................................. 18
Figure 6. European Interoperability Framework ............................................. 20
Figure 7. Electronic identification, authentication and trust services architecture ............................................................................................................. 21
Figure 8. PAA PKI Mutual Recognition Framework ...................................... 31
Figure 9. PAA Transaction Services operation model ..................................... 32
1. Introduction

The Mutual Recognition Arrangement (MRA) has been introduced as a tool for facilitating trade, increasing market accessibility and eliminating or reducing Non-Tariff Barriers (NTBs). However, the MRA is often misinterpreted that it may require unified standards or technical regulations. Understanding how the MRA works may help preventing such misinterpretation. In MRA, a designated agency of an exporting country accredits or appoints a conformity assessment institute (testing agency or certification agency) that can conduct the conformity assessment pursuant to the importing country's technical regulations. In certain countries’ cases, a designated agency may appoint an agency to conduct accreditation of a conformity assessment institute on behalf of it. When a designated agency provides an importing country with a list of accreditation agencies and the conformity assessment agencies, the importing country decides approval of the listed agencies after assessment.

The most important thing in establishing and maintaining the mutual recognition scheme is how to manage the trust in the MRA. The best-known worldwide mutual recognition scheme is the Multi-lateral Recognition Arrangement (MLA) of the International Accreditation Forum (IAF). The IAF is the world association of Conformity Assessment Accreditation Bodies. Its primary function is to develop a single worldwide programme of conformity assessment which reduces the risks for businesses and their customers by assuring them that accredited certificates may be relied upon. The IAF ensures that Accredited Bodies follow the framework of accreditation and its rules to maintain a consistent level of deliverables (accredited certificates).

The basic scheme in maintaining the minimum level of credibility is the use of peer evaluation in accordance with ISO/IEC 17011: 2004 (General Requirements for Accreditation Bodies and Accreditating Conformity Assessment Bodies) on Accreditation Bodies, and ISO/IEC Guide 65 or ISO 17021-1 2015 (conformity assessment – requirements for bodies providing audit and certification of management systems) on Certification Bodies that are accredited by Accreditation Bodies. Figure 1 illustrates how the multilateral recognition scheme works in conformity assessment across the borders.
2. Cross-border Mutual Recognition cases of non-electronic transactions

2.1 Authorized Economic Operator

An Authorized Economic Operator (AEO) Mutual Recognition Agreement refers to the signing of a formal document between two or more customs administrations outlining the circumstances and conditions in which AEOs are recognized and accepted between the signing parties. The MRA sets out the process to implement, evaluate, monitor and maintain mutual recognition. Also, the MRA defines the benefits mutually provided by the participating Customs administrations and lays down the practical arrangements enabling the participating Customs administrations to provide those benefits.

---

1 Certification and Accreditation Framework, Global Food Safety Initiative.
2 “Each Contracting Party shall grant the status of “authorized economic operator” to the economic operator established in its customs territory. An authorized economic operator shall benefit from facilitations with regard to security-related customs control (Guidelines for Developing a Mutual Recognition Arrangement/Agreement, WCO Safe package, 2011).
The objective of Mutual Recognition of AEOs is that one Customs administration recognizes the validation findings and AEO authorizations by the other Customs administration issued under the other programme and agrees to provide substantial, comparable and – where possible – reciprocal benefits/facilitation to the mutually recognised AEOs. This recognition is generally premised on the existence (or creation) of both relevant legislation (where applicable) and operational compatibility of both or more programmes. The MRA should, to the extent possible, be published as a matter of public record.

2.1.1 Elements of AEO MRA

The guidelines of AEO MRA5 state the eight elements of AEO MRA – responsible entities, compatibility, mutual recognition, information exchange and participant communication, future endeavours, modification and consultation, status of arrangement/agreement, and commencement and discontinuation/termination. The elements of a Mutual Recognition Arrangement/Agreement of AEO can be summarised as follows:

- **Element 1 (responsible entities).** The agreement shall specify two customs administrations that are engaging in the arrangement/agreement. Customs can delegate the AEO certification process or parts/sections thereof to a designated third party;
- **Element 2 (compatibility).** Any standards put forward in the arrangement/agreement shall remain compatible with regard to the application process for AEO certification, assessment of AEO applications, approval and monitoring of AEO status, etc.;
- **Element 3 (mutual recognition).** There shall be provisions requiring that the participants accept the validation and approval status of their counterpart's AEO programmes while reserving the right to conduct risk assessment once the consignment is under their control;
- **Element 4 (information exchange and participant communication).** The arrangement/agreement shall include sharing relevant information with the

---


5 AEO Mutual Recognition Strategy Guide, WCO.
counterpart on changes or evolution within their AEO programme, or any changes of AEO status such as suspensions and revocations;

- Element 5 (future endeavours). It is necessary to focus on items that may be future endeavours for mutual cooperation as well as a reference to potential future benefits of the MRA that are currently unavailable, but which may become so in the event of future expansion of the programme;
- Element 6 (modification and consultation). Reference should be made that the MRA may be modified with the consent of both participants;
- Element 7 (status of arrangement/agreement). The MRA shall clarify legally binding and non-binding commitments, obligations under international or national law, and rights or privileges for particular parties. However, the MRA shall not limit cooperation and assistance related to other international provisions, agreements, treaties, and domestic laws and practices;
- Element 8 (commencement and discontinuation/termination). When the MRA is to take effect, and what is the process for the suspension, discontinuation or termination of the MRA, shall be clarified in the arrangement/agreement.

Excluding the common elements of international agreements or arrangements from the eight elements of the AEO MRA, distinctive elements that can be applied to the mutual recognition scheme can be extracted. The remaining elements, i.e., compatibility, mutual recognition, and information exchange and participant communication, could be interpreted as core elements that characterize the cross-border AEO recognition scheme. These three elements are a critical part of a cross-border mutual recognition scheme for maintaining trust among participants by keeping reciprocal compatible standards, accepting the validation and approval status of their counterpart’s AEO Programmes, and sharing up-to-date information with counterparts.

2.1.2 Challenges in AOE MRA

Mutual recognition of AEO Programmes may ultimately lead to the globalization of supply chain security and compliance standards and is therefore of great importance for those companies seeking true global supply chain security and compliance benefits. Companies participating in mutual recognition of AEO Programmes will have confidence that their standing in such programmes will be made available, if they choose this, to other Customs administrations with which an MRA has been signed.
Additionally, Customs administrations will be able to factor this information into their risk determinations, which may lead to more focused validations and other compliance benefits. However, because of the nature of AEO MRA, challenges exist in AEO MRA:6

- Lack of standard process for negotiating MRAs. No standardised templates for scope, format, or provisions/clauses that should be included;
- The focus (e.g., security and/or compliance issues), level of development and implementation of AEO programmes around the world are often different, including the ways in which these programmes are managed and organised. However, at the regional, subregional, multilateral or bilateral level in the region, it may be easier to achieve because of the similarity in procedures;
- Priorities and level of support of each customs administration to engage in MRA negotiations vary. Both sides must be fully committed to the level of time and resources necessary to see the endeavour finalised;
- Each programme has its own terminology;
- There are limitations on information sharing due to partner countries’ different laws and regulations. Consent to share information is not always provided by companies in each programme;
- Differing benefits extended through the AEO programmes in each country can make it difficult to establish reciprocity;
- There is no global trader identification number (e.g., TIN) for companies to be identified by the MRA partner to ensure that benefits are delivered to the AEOs;
- Many countries use incompatible technologies (e.g., differences in capabilities of Customs IT systems);
- The costs and investments required to develop new technologies are extensive;
- Storage of each other's AEO details in databases needs to be reconciled with data protection and data security concerns;
- Adapting customs declaration systems to capture and validate the parties in the supply chain that could be an AEO;

---
Adapting risk management engines to take into account the status of AEO favourably in risk management;

There are different ways of identifying AEO companies from MRA partners;

AEO programmes of partner countries sometimes target different parties in the supply chain (e.g., some do not cover the importer; others do not cover the exporter);

The absence of any technique or mechanism for dealing with the supply chain as a whole. Even with MRAs in place, logistical entities involved in the supply chain are excluded, and only importers and exporters are concerned;

Differentiated benefits established in different programmes.

2.1.3 Summary and implications

The AEO Cross-Border Mutual Recognition scheme, which has been adopted by many countries, was initiated and is managed by the international body, World Customs Organization. There is no Convention governing or supporting the AEO MRAs, but there is a WCO SAFE framework of standards as guidelines, which is implemented by customs authorities of MRA partner countries. It is worth noting that what is recognized through an AEO MRA is the AEO programme of a partner country, not the AEOs themselves. AEO partners have the ownership of AEO mutual recognition requirements, giving more flexibility in establishing and entering into an MRA as well as the legitimate authority to conduct the validation of entities that are AEOs of the other MRA partner’s customs. However, such an approach also reduces possibility of interoperability among existing AEO MRAs, while it allows flexibility.

The standards compatibility mechanism is used to establish a recognition scheme, including the “application process for membership, assessment of membership applications and approval of membership. To maintain trust, WCO recommends engaging in mutually beneficial information exchange regarding supply chain security, AEO members of the programme and updates on their own programme’s operation.

(Key words and phrases: WCO SAFE framework of standards as a guideline; implemented by customs of MRA partner countries; AEO MRA recognises an AEO

---

7 WCO Mutual Recognition Arrangement/Agreement Strategy Guide.
programme; ownership of mutual recognition requirements; standards compatibility mechanism; and mutually beneficial information exchange.)

2.2 APEC TEL MRA

In June 1998, the APEC Telecommunications and Information Ministers agreed to streamline APEC-wide processes for the testing and type-approval of telecommunications equipment. This landmark arrangement, the Mutual Recognition Arrangement for Conformity Assessment of Telecommunications Equipment (APEC TEL MRA), was the first multilateral agreement of its type in the world. It was supposed to remove a significant barrier to what is projected to be a US$60 billion industry. Its scope includes all equipment that is subject to telecommunication regulations, including wireline and wireless, and terrestrial and satellite equipment. For such equipment, the MRA covers electromagnetic compatibility (EMC) and electrical safety aspects as well as purely telecommunications aspects of the conformity assessment requirements.

This arrangement is intended to streamline the Conformity Assessment Procedures for a wide range of telecommunications and telecommunications-related equipment, thereby facilitating trade among the Parties concerned. It provides for mutual recognition by the importing Parties of Conformity Assessment Bodies as well as mutual acceptance of the results of testing and equipment certification procedures undertaken by those bodies in assessing the conformity of equipment to the importing Parties’ own Technical Regulations.

APEC TEL MRA is open not only to its member economies to enter the arrangement, but also to the regional institutions such as ASEAN, and even to some national institutions such as United States NIST and FCC (table 1). To operate the APEC TEL MRA, the main responsible APEC fora, the APEC Telecommunications Working Group, has created a designated Conformance Assessment and Mutual Recognition Arrangement Task Force under its Liberalisation Steering Group subgroup.

---

The MRA does not undermine Regulatory Authority within member Economies. Certain procedures need to be followed to implement this MRA. These apply to distinct bodies identified in the MRA as:

- **Party** – an APEC member economy that agrees to participate in the arrangement;
- **Joint Committee** – a committee of the APEC Telecommunications Mutual Recognition Arrangement Taskforce established for the purpose of managing the implementation of the MRA;
- **Regulatory Authority** – a government entity responsible for telecommunications requirements within an economy;
- **Designating Authority** – a government authority appointed by a Party for the purpose of designating a Conformity Assessment Body to perform Conformity Assessment Procedures under the MRA;
- **Accreditation Body** – a body that is responsible for assessing and recognizing the specific competencies of testing laboratories and/or certification bodies (Conformity Assessment Body) in accordance with international standards;
- **Conformity Assessment Body** – a body, which may include a third party or a supplier's testing laboratory or a certification body, which is designated to perform conformity assessment of an importing Party's Technical Regulations under the arrangement.

Certain functions such as designation, accreditation and recognition are defined in the text of the MRA. They are typically carried out by one or more organizations within an economy. Figure 2 shows the possible relationships between various entities that may have a role in MRA implementation within an economy. It is the Party to the arrangement that has the final responsibility for the implementation as well as the key role in supervising or delegating tasks to other groups.
Figure 2. Relationships among entities under an MRA

**Economy A**  
RA  
DA  
AB  
CAB

**Economy B**  
RA  
DA  
AB  
CAB

**Economy C**  
RA  
DA  
AB  
CAB

**Economy D**  
RA  
DA  
AB  
CAB

RA = Regulatory Authority  
DA = Designating Authority  
AB = Accrediting Body  
CAB = Conformity Assessment Body
<table>
<thead>
<tr>
<th></th>
<th>Australia</th>
<th>Canada</th>
<th>Chile</th>
<th>Taiwan Province of China</th>
<th>Hong Kong, China</th>
<th>Japan</th>
<th>New Zealand</th>
<th>Republic of Korea</th>
<th>Singapore</th>
<th>United States</th>
<th>Viet Nam</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>○</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(99.7)</td>
<td>(99.7)</td>
<td>(02.6)</td>
</tr>
<tr>
<td>Canada</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(99.7)</td>
<td>(99.7)</td>
<td>(99.7)</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>(99.7)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(02.3)</td>
<td>(97.1)</td>
<td>(01.3)</td>
</tr>
<tr>
<td>Chile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td></td>
<td>(08.6)</td>
<td></td>
</tr>
<tr>
<td>Taiwan Province of China</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(99.7)</td>
<td>(99.7)</td>
<td>(99.3)</td>
</tr>
<tr>
<td>Hong Kong, China</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(99.7)</td>
<td>(99.7)</td>
<td>(05.4)</td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td></td>
<td>(02.1)</td>
<td>(07.2)</td>
</tr>
<tr>
<td>New Zealand</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Republic of Korea</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(97.1)</td>
<td>(08.6)</td>
<td>(06.1)</td>
</tr>
<tr>
<td>Singapore</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(99.7)</td>
<td>(99.7)</td>
<td>(03.10)</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>(99.7)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(99.7)</td>
<td>(99.7)</td>
<td>(03.10)</td>
</tr>
<tr>
<td>United States</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(02.1)</td>
<td>(05.4)</td>
<td>(07.2)</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>(01.3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td>(99.5)</td>
<td>(07.2)</td>
<td>(03.10)</td>
</tr>
<tr>
<td>Viet Nam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td></td>
<td>(06.1)</td>
<td></td>
</tr>
</tbody>
</table>

**Source:** Author’s calculation, 2020.

**Note:** The numbers indicate the effective year and month of the bilateral APEC TEL MRA.

*Note: one small circle means it is in the first phase of APEC MRA and double circle means it is in the second phase*
APEC TEL MRA emphasizes the importance of an importing Party's confidence in the competence of Conformity Assessment Bodies of another Party to test or assess conformity with the importing Party's requirements. To facilitate confidence building, APEC TEL MRA recommends technical cooperation and assistance, which can help to develop institutional structures on measurement, testing and other conformity assessment skills, and by means of courses, seminars, personnel exchanges, inter-comparisons, joint audits and similar approaches in order to develop a greater familiarity with other Parties' requirements and a greater commonality of approach.

2.2.1 Summary and implications

As one of the first multilateral MRA schemes in the world, it was initiated by the international body, Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Ministers, and it led more than 10 member economies entering into cross-border MRAs. APEC provides the Mutual Recognition Arrangement which is intended to streamline procedures of the conformity assessment for telecommunications and telecommunications-related equipment. However, this arrangement has no legally binding effect, and members need to enter into legally binding obligations between or among themselves through an individual MRA incorporating this arrangement as they deem necessary. The central weight of recognition requirements lies with importing countries because the acceptance of certification of equipment means that equipment is in conformity with the importing countries' technical regulations. The regulatory authority of the importing economy is responsible for telecommunications requirements within an economy.

Designation and accreditation are used as the main tools for the recognition scheme. The Designating Authority and/or Accreditation Body are in charge of the recognition of the Conformity Assessment Body. In this arrangement, the target object of recognition is not the conformity assessment procedure results but the designated or accredited Conformity Assessment Bodies. It means that the result of conformity assessment procedures performed by those bodies is accepted by participating members because it is issued by recognised Conformity Assessment Bodies. As the APEC TEL MRA does not have strong enforcement mechanism to impose on the participating MRAs, the confidence building as a best endeavour measure is recommended for promoting and maintaining the MRA scheme.
(Key words and phrases: APEC, Mutual Recognition Arrangement; individual Mutual Recognition Agreement; the Regulatory Authority of importing economy is responsible for requirements; and Designating Authority and/or Accreditation Body are in charge of the recognition; object of recognition is the designated or accredited conformity assessment bodies; designation and accreditation; and confidence building measures.)

2.3 ILAC MRAs

Historically, the International Laboratory Accreditation Cooperation (ILAC) started as a conference. It was held to develop international cooperation in facilitating trade by promotion of the acceptance of accredited test and calibration results. In 1996, ILAC became a formal cooperation organization with a charter for establishing a network of MRAs among accreditation bodies.

In 2000, the 36 ILAC Full Members – comprising laboratory accreditation bodies from 28 economies worldwide – signed the ILAC Mutual Recognition Arrangement (ILAC MRA) in Washington, D.C. to promote the acceptance of technical test and calibration data for exported goods. The ILAC MRA for calibration and testing laboratories came into effect on 31 January 2001. It was then extended in October 2012 to include the accreditation of inspection bodies.

Currently, ILAC is the international organization for accreditation bodies operating in accordance with ISO/IEC 17011 (general requirements for bodies providing assessment and accreditation of conformity assessment bodies and additional requirements) and is involved in the accreditation of conformity assessment bodies (CAB), including: (a) calibration and testing laboratories (using ISO/IEC 17025; (b) general requirements for the competence of testing and calibration laboratories); (c) medical testing laboratories (using ISO 15189, requirements for quality and competence); and (d) and inspection bodies (using ISO/IEC 17020, requirements for the operation of various types of bodies performing inspection).

9 See http://ilac.org/ilac-mra-and-signatories/.
The incorporation of a proposed accreditation body into the ILAC MRA will be evaluated by peers from other accreditation bodies in accordance with the relevant ILAC rules and procedures. ILAC has published two types of rules and procedural documents.

Being a signatory to ILAC MRA, an Accreditation body shall maintain conformity with the latest version of ISO/IEC 17011 and ensure that all laboratories and inspection bodies that are accredited comply with appropriate laboratory and inspection bodies standards. Accreditation bodies are established in many economies with the primary purpose of ensuring that conformity assessment bodies are subject to oversight by an authoritative body. Accreditation bodies that have been peer-evaluated as competent, sign regional and international arrangements to demonstrate their competence. These accreditation bodies then assess and accredit conformity assessment bodies to the relevant standards. In the end, the signatory to the ILAC MRA (or a recognised accreditation body) accredits facilities that issue test result, inspection result and calibration certificates. These issued result or certificates are to be accepted by the other signatory to the ILAC MRA in other regions as well as other government regulatory bodies.

Three recognized regional bodies represent (a) Europe – the European Cooperation for Accreditation (EA), (b) Asia and the Pacific – the Asia-Pacific Laboratory Accreditation Cooperation (APLAC); and (c) America – the Inter-American Accreditation Cooperation (IAAC). The mutual recognition arrangements and evaluation procedures of EA, APLAC and IAAC have been peer-evaluated by ILAC and have demonstrated competence in maintaining and managing an MRA. Signatories to the EA, APLAC and IAAC MRAs, who are also members of ILAC, are entitled to become signatories (full members) of the ILAC Arrangement. ILAC relies on the evaluation of the ILAC members in their respective regions. ILAC undertakes the evaluation of the regional representatives as well as the unaffiliated accreditation bodies that do not belong to a specific regional representative. These recognized regional cooperation bodies are re-evaluated every four years. The other cooperation bodies – the Southern African Development Community in Accreditation (SADCA), the Arab Accreditation Cooperation (ARAC) and the African Accreditation Cooperation (AFRAC) – are in the process of developing their respective MRAs and their associated evaluation procedures before seeking recognition by ILAC.
The General Assembly is the primary body and ensures that ILAC tasks are in alignment with the objectives of ILAC (figure 3). All members are eligible for providing a representative to the General Assembly. The Arrangement Council is the mutual recognition decision-making body for determining signatory and recognition status under the ILAC Arrangement.

**Figure 3. ILAC Organization Chart**

![ILAC Organization Chart](https://ilac.org/about-ilac/structure/organisation-chart/)

### 2.3.1 Summary and implications

ILAC is a network of MRAs among accreditation bodies, eliminating testing as a technical barrier to trade through recognition of competence between accreditation bodies. In the scheme of the ILAC MRA, there is the ILAC MRA, which is a private agreement. And unlike other cases, the ILAC MRA takes the technical and standards requirements from the international standard body, ISO. The ILAC Arrangement Council is responsible for the recognition under ILAC arrangement.

---

10 See [https://ilac.org/about-ilac/structure/organisation-chart/](https://ilac.org/about-ilac/structure/organisation-chart/).
The recognised objective is an accreditation body, and the cross-border acceptance is given to the test result, inspection result and certifications issued by facilities accredited by an accreditation body. Also, a peer review is a basic evaluation method for an accreditation body, while ILAC supports and leads overall coordination of the mutual recognition scheme. While not having any supporting international legal framework, the role of ILAC remains as a coordinator of a mutual recognition scheme.

(Key words and phrases: ILAC; ILAC Mutual Recognition Arrangement; coordinator of a mutual recognition scheme; technical and standards requirements of the international standard body; recognised objective is an accreditation body; and peer review.)

3. Cross-border Mutual Recognition cases of electronic transactions

3.1 eIDAS

In the European Union (EU), the certification services have recently been expanded to provide a variety of trust services other than digital signature certification. The European Union enacted EU Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation, 2014\textsuperscript{12}), which has replaced the EU Digital Signature Directive.\textsuperscript{13}

The eIDAS Regulation is aimed at enhancing trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the European Union. In other words, electronic identification and

\textsuperscript{11} eIDAS stands for electronic IDentification and Authentication Services.


electronic trust services are keys for ensuring secure cross-border electronic transactions and for building a single European digital market.

The old Digital Signature Directive came into force on 19 January 2000. And the member States were required to comply with their national legislation as the European Union member States must have implemented the content of this Directive by their national law as of 19 July 2001, 18 months from the date of entry into force. However, as eIDAS went into effect on 1 July 2016, the Directive has been abolished, and countries are in the process of reforming the relevant legislation as they have direct effect as a digital signature law for European Union member States.

The Digital Signature Directive recommended that each member State should establish digital signature legislation based on this Directive since its legislative form is a Directive. The eIDAS Regulation, on the other hand, differs in that the legislative form is a Regulation, which means that it has a legal effect directly as national law in a member State without enacting a separate national law.

Member States that have enacted digital signature legislation, in accordance with the European Union Digital Signature Directive, differ from country to country with regard to the interpretation of the electronic signature guidelines. This has resulted in differences in the details of domestic legislation. Also, there was a problem that the supervisory system of certification service providers (certification bodies) varied between them. As a result, discrepancy between the member States has arisen. Also, since the format of the trust list of the certification provider was not uniform among the member States, it was difficult to verify the digital signatures of other countries automatically. These problems had been barriers to the formation of a single digital market in the European Union region. The eIDAS Regulations, therefore, were established to eliminate these obstacles and form a regional digital single market (figure 4).
The eIDAS Regulation (figure 5) does not impose obligations on the use of electronic certification services in the European Union member States. In other words, the mandatory mutual recognition in the region is provided only in the public service area, and it is left to the individual members to decide on whether to adopt this regulation in the private area.

The structure of the eIDAS Regulation consists of six chapters and 52 articles (with three annexes). Chapter 2, Electronic Identification, provides for mutual recognition, eligibility for notification of electronic identification systems, level of assurance, notification, security violations, liability, cooperation and interoperability. Interoperability is "to build coherent services for users, from components that are technically different and managed by different organizations". Chapter 3, Trust Services, regulates matters concerning the supervisory body, security requirements of trust service providers, qualified trust services, electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, website authentication etc. Chapter 4 sets out the legal effect of electronic documents while Chapter 5 concerns delegation of power and implementing provisions. Chapter 6 has additional provisions. The key parts of the text are Chapters 2 and 3, which define the

---

requirements and effects of various certification services, such as the supervision and management system of such services and electronic signature, electronic seal and website certification.

Figure 5. Scope of eIDAS

3.1.1 Requirements for mutual recognition

Electronic identification means the process of using a person’s identification data in electronic form, thereby uniquely representing either a natural or legal person or a natural person representing a legal person. This electronic identification is used for authentication when using the online service through electronic identification means such as e-ID cards or tokens issued through certain procedures in the individual member States.

Such mutual recognition of electronic identification requires a certain trust system. Article 6 of the Regulation states that “when an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one member State, the electronic identification means issued in another member State

---

15 The definition is from eIDAS Regulation Article 3.
shall be recognised by the first member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met":

(a) The electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission;
(b) The assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;
(c) The relevant public sector body uses the assurance level substantial or high in accessing that service online.

Article 9 of the Regulation, as a prerequisite for the mutual recognition of electronic means of identification, sets out the information to be submitted and the relevant procedures when individual member States notify their electronic identity systems. It comprises the electronic identification scheme, the applicable supervisory regime, roles and responsibilities of the Party issuing the electronic identification means, the party operating the authentication procedure, the authority or authorities responsible for the electronic identification scheme etc.

With regard to cooperation and interoperability among the member States, Article 12 sets out the European Interoperability Framework (EIF) criteria and components (figure 6). In eIDAS, the interoperability framework aims at being technology-neutral and does not discriminate between any specific national technical solutions for electronic identification. It follows European Union and international standards, facilitates the implementation of the principle of privacy by design and ensures that personal data are processed in accordance with the Data Protection Directive (95/46/EC). The interoperability framework components include a reference to minimum technical requirements for the assurance levels, interoperability and common operational security standards, mapping of national assurance levels of notified electronic identification schemes to the assurance levels of eIDAS, a reference to a minimum set of personal identification data uniquely representing a natural or legal person, and rules of procedure and arrangements for dispute resolution.
The eIDAS Cooperation Network (see below) has published eIDAS Interoperability Architecture that specifies the interoperability components of the eIDAS-Network, i.e., the components necessary to achieve interoperability of notified eID schemes according to the eIDAS Regulation. This specification is based on the requirements laid down in the Implementing Act.

Interoperability between different member States’ eID schemes is achieved via defining the technical interfaces between eIDAS Connectors and eIDAS Services – collectively, eIDAS-Nodes. The interfaces between the eIDAS Connectors and relying parties, and between the eIDAS Services and the eID scheme are part of the national system of the receiving member State and the sending member State, respectively. Therefore, it is not covered by the eIDAS Interoperability Architecture.

The eIDAS Node is an operational entity involved in cross-border authentication of persons. A Node can have different roles, which are distinguished in this specification (eIDAS Connector/eIDAS Service). The eIDAS Connector is an eIDAS Node requesting a cross-border authentication. The eIDAS Service is an eIDAS Node, which provides cross-border authentication, and is divided into two categories – eIDAS Proxy Service and eIDAS Middleware Service. The eIDAS Proxy Service is an eIDAS Service operated by the sending member State that provides personal identification data of the
The eIDAS Middleware Service is an eIDAS Service running middleware provided by the sending member State and operated by the receiving member State that provides personal identification data of the sending member States. The eIDAS Nodes use OASIS Security Assertion Markup Language for communication. For more information, read eIDAS Interoperability Architecture.

Figure 7. Electronic identification, authentication and trust services architecture

An electronic identification sending member State can have two integration scenarios for the eID-scheme: Proxy-based and middleware-based scenarios (figure 7). The sending member State operates an eIDAS Proxy Service, relaying authentication requests and authentication assertions between an eIDAS Connector operated by the receiving member State and the eID scheme of the sending member State. In the middleware-based scenario, the sending member State provides a middleware to the other receiving member State, which is operated by the operator(s) of the eIDAS Connector(s) of the receiving member State. Each receiving member State must operate one (or more) eIDAS Connector(s). Connectors can be operated by public or private relying parties established in the receiving member State. The Centralised model operates only one Connector in the Member State while the Decentralised model operates several Connectors. An eIDAS-Connector is operated together with eIDAS-Middleware-Services for communication with middleware-based eID schemes.
3.1.2 Control of a mutual recognition scheme

The eIDAS provides a mechanism for mutual recognition of identification means of a member State on public online services of all other member States. The eIDAS requires the member States to maintain a certain level of procedure and assurance in order to maintain trust among them. However, eIDAS does not define the technical electronic identification means to achieve interoperability for electronic identification and electronic trust services. Instead, eIDAS defines the levels of assurance for trust service implementation. Mutual recognition of electronic identification means has been mandatory since 2018. An identification means must have:

(a) Been issued following an electronic identification scheme notified by the member States concerned, and appear on the list published by the Commission. Since September 2015, member States have been able to notify electronic identification schemes;
(b) An assurance level equal or superior to the one required by the public authority concerned in order to access this online service, provided that the level is substantial or high. This mutual recognition only concerns public authorities that require the implementation of a notified electronic identification means in order to access one of their online services.

The Commission Implementing Regulation (EU) 2015/1502 provides details of the requirements applicable to the different assurance levels. The levels are granted by the compliance level with specifications, norms and minimal procedures. There are three assurance levels:

(a) Low. At this level, the purpose is simply to reduce the risk of identity misuse or alteration;
(b) Substantial. At this level, the purpose is to substantially reduce the risk of identity misuse or alteration;
(c) High. At this level, the purpose is to prevent identity misuse or alteration.

Commission implementation regulation (EU) 2015/1502 sets out minimum technical specifications and procedures for assurance levels of electronic identification means according to Article 8(3) of eIDAS Regulation. The assurance level of the
electronic identification means issued under a notified electronic identification scheme is determined by the reliability and quality of the four elements of enrolment, electronic identification means management, authentication, and management and organisation.\textsuperscript{16}

Commission Implementation Decision (EU) 2015/296 establishes procedural arrangements for cooperation between the member States on electronic identification. The core of Decision 2015/296 is a “peer-reviewing process” and “the Cooperation Network”.

In the Decision 2015/296, peer review is defined as "a mechanism for cooperation between the member States designed to ensure interoperability and security of notified electronic identification schemes". Peer reviewing includes the following arrangements: (a) the assessment of relevant documentation; (b) examination of processes; (c) technical seminars and (d) consideration of independent third-party assessment. The peer review process can be initiated on request by a member State to be peer-reviewed or by a member States expressing the wish to peer review the eID scheme of another member State. Such a request must indicate the reasons for wishing to conduct the peer review and must explain how the peer review would contribute to the interoperability or security of that member State’s electronic identification scheme. All the requests for peer reviewing will be announced by the Cooperation Network.

The Cooperation Network was created and mandated to facilitate procedural arrangements for achieving the objectives of eIDAS regulation.\textsuperscript{17} The Cooperation Network includes all the member States and engage them in a formalised manner in order to cooperate vis-à-vis the practicalities of maintenance of the interoperability framework. The Cooperation Network should examine draft notification forms provided by the member States under the eIDAS Regulation, and issue opinions providing indications as to the compliance of the national electronic identification schemes with the requirements and the implementation Decision. The notifying member States must

\begin{footnotesize}
\begin{itemize}
  \item[16] For details of the low, substantial and high assurance level criteria, refer to the Commission implementation regulation (EU) 2015/1502.
  \item[17] Member States must cooperate with regard to the interoperability and the security of e-ID scheme. The cooperation consists of the exchange of information, experience and good practices, and a peer review of electronic identification schemes.
\end{itemize}
\end{footnotesize}
refer to the opinions of the Cooperation Network and describe how the notified electronic identification scheme meets the requirements of eIDAS interoperability.

Unlike the Digital Signature Directive, under the eIDAS Regulation, each member State must designate a supervisory body to oversee the certification work in that country and notify the European Commission of the results. The role of the supervisory body will depend on whether the trust service provider is “qualified” or not. First, in the case of a qualified trust service provider (QTSP), the supervisory body will conduct ex-ante and ex-post supervision\textsuperscript{18} on whether the accredited certification body and the accredited certification services they provide meet the requirements set out in this regulation. In contrast, the supervisory body will only perform ex-post supervisory activities for non-qualified trust service providers if they are informed that the trust service provider or their certification services do not meet the requirements set out in this regulation.

For the supervision of QTSP, the regulation requires QTSP to be audited at their own expense at least once every 24 months by a conformity assessment body (ex-post supervision). The purpose of the audit is to confirm that qualified trust service providers and the qualified trust services provided by them fulfill the requirements laid down in the Regulation. The qualified trust service providers must submit the resulting conformity assessment report to the supervisory body within three working days after receiving it. In addition, the supervisory body may at any time audit or request a conformity assessment body to perform an assessment of the qualified trust service providers, at the expense of those trust service providers, in order to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in the Regulation.

Article 14 sets out the principle of the recognition of third countries’ trust service providers. Trust services provided by trust service providers established in a third country will be recognised as being legally equivalent to services provided by qualified trust service providers established in the European Union where the former are recognised under an agreement concluded between the European Union Commission.

\textsuperscript{18} Ex-ante is Latin terminology meaning “before the event”, while ex-post means “after the event”. In eIDAS, ex-ante supervision is an evaluation of whether an applicant to become a trust service provider can be certified by qualifying the minimum requirements of eIDAS. Ex-post supervision is auditing the quality of a trust service provider at least once every 24 months.
and the third country. The vice versa also applies according to the principle of reciprocity.

**Mutual recognition and subsidiarity as a general principle of EU law**

Subsidiarity is defined as “the principle that a central authority should have a subsidiary function, performing only those tasks which cannot be performed at a more local level” (Oxford English Dictionary). Among others, the European Court of Justice has recognised the fundamental rights, proportionality, legal certainty, equality before the law and subsidiarity as general principles of European Union law (J.H. Jans, 2007, *Europeanisation of Public Law* (first edition), p. 418, Europa Law Publishing).

Under the principle of subsidiarity, in areas that do not fall within its exclusive competence, the European Union will act only if, and in so far as the objectives of the proposed action cannot be sufficiently achieved by the member States, either at the central level or at a regional and local level, but which can, by reason of the scale or effects of the proposed action, be better achieved at the European Union level.

It can be assumed that eIDAS Regulation conforms to the principle of subsidiarity. Accordingly, the revision of the Digital Signature Directive into eIDAS Regulation implies that the European Commission considers that cross-border mutual recognition of e-ID and e-transactions requires stronger enforcement than the guideline for measures of individual member States.

3.1.3 Challenges and lessons from the eIDAS experience

The challenges are that:

(a) The eIDAS claims for technology neutrality. However, during the implementation of the eIDAS Interoperability Framework, specification adopted specific technology, and its principle of technology neutrality was questioned;

(b) The readiness and capacity of each member State for eIDAS are different. That difference must be addressed.
The lessons learnt are that:

(a) Before the design of the EIF model, eIDAS e-Transaction workflows were carefully considered. By going through the possible work scenario, the process of modelling a mutual recognition scheme could be much simpler and efficient;

(b) eIDAS is designed to enhance trust in electronic transactions in the internal market of the European Union; however, it also applies the principle of reciprocity to other markets. The mutual recognition scheme of the Framework Agreement follows the same direction, by allowing non-member States to join the scheme;

(c) eIDAS has learnt from the European Union Digital Signature Directive experience, and it has strengthened legal enforcement. Strong governance of the cross-border mutual recognition scheme helps to improve compliance and efficiency while restricting policy space of the member States;

(d) Mandatory mutual recognition in the region is provided only in the public service area, and it is left to autonomous decision whether to adopt this regulation in the private area. In a business with rapid technological change, the risk of regulatory error is high, making non-technologically neutral regulation risky. Yet, technology neutrality will be critical to encouraging innovation and efficiency in the private sector. The same principle could apply to the Framework Agreement;

(e) A peer review mechanism has been introduced to ensure interoperability and security of notified electronic identification schemes;

(f) To establish a comparative level of trustworthiness and keep it sustainable, it is necessary to hold a periodical requirements compliance audit procedure.

3.1.4 Summary and implications

The European Union enacted the eIDAS Regulation, which abolishes and replaces the EU Digital Signature Directive. The old Directive recommended that each member State should establish digital signature legislation, but inequality of legislation between the member States became a barrier to the formation of a single digital market. The eIDAS has a direct legal effect as national law in the member States in order to eliminate these obstacles and form a regional digital single market.

The object of recognition is electronic identification, which is used for authentication when using the online service through electronic identification means issued through certain procedures in the individual member States. Mutual recognition of electronic identification requires a certain trust system and eIDAS stipulates that identification means must be issued under the eIDAS electronic identification scheme with an assurance level equal to, or higher than the assurance level required. The mandatory mutual recognition in the region is provided only in the public service area, and it is left to autonomous decision whether to adopt this regulation in the private sector.

The Cooperation Network was established under the European Commission to facilitate cooperation for the maintenance of the EIF by engaging them in a formalized manner. A peer review mechanism is applied to ensure interoperability and security of notified electronic identification schemes of the member States.

The EIF was designed for the establishment of the single digital market by fostering cross-border and cross-sectoral interoperability among European public services. The eIDAS interoperability framework aims to be technology-neutral and does not discriminate between any specific national technical solutions for electronic identification. It follows European and international standards, facilitates the implementation of the principle of privacy by design, and ensures that personal data are processed in accordance with the Data Protection Directive of the European Union.

Under the eIDAS Regulation, each member State must designate a supervisory body to oversee the national certification work and notify the body to the European Commission. The supervisory body will conduct ex-ante and ex-post supervision over trust service providers.
3.2 PAA PKI Mutual Recognition Framework

PAA is an alliance of paperless trade service providers in Asia. PAA comprises 11 members from: the Republic of Korea; China; Japan; Hong Kong, China; Taiwan Province of China; Macau, China; Thailand; the Philippines; Singapore; Indonesia; and Malaysia.\(^{20}\) PAA aims to provide seamless cross-border transaction services through a robust legal and technical cross-border electronic message exchange framework. For this purpose, PAA has established a Public Key Infrastructure (PKI) Mutual Recognition Framework to establish a comparable level of trustworthiness. Authentication of the identity of individuals or organizations is required in order to establish non-repudiation for cross-border exchange of electronic messages.

A PKI relies on public key cryptography technology. The basic concept is that the secret private key of each entity is only known by that entity and is used for digital signing. The public key is derived from a private key, and a public key is used for verifying signatures signed by the paired private key. A public key cannot be used to sign and it is made available to anyone, and is typically included in the certificate document. A PKI is an operational system that employs cryptography, IT, business rules and legal matters. A PKI supports the secure electronic transfer of information for a range of network activities such as e-commerce, payment and secure email.

A properly managed PKI requires all of these disciplines – legal, business, technology and cryptography – in order to function effectively; the lack of one or more of these disciplines can undermine the effectiveness and efficiency of PKI.\(^{21}\) The PKI began with the establishment of the X.509 certificate standard in 1993, with

\(^{20}\) As of May 2020, there were two associate members from India and Sweden.

the establishment of Request for Comments (RFC) 142. The X.509 defines a framework for the provision of authentication services. In 1995, a PKIX workgroup was established to support public key infrastructures based on X.509 on the Internet. The PKIX has produced many RFC, and these are often referred to as "PKIX standards". In X.509, the term "Certification Authority" is defined as "an authority trusted by one or more users to create and assign certificates." A Certification Practice Statement (CPS) is a statement of the practices that a CA employs in managing digital certificates that it issues.

3.2.1 Stakeholders

The PAA PKI Mutual Recognition Framework has four stakeholder groups – the PAA Certificate Policy Authority (CPA) under PAA, (accredited or applying) Certificate Authority(s), and PAA members and users (trading companies or trade-related service providers).

3.2.2 Inputs and tools

Tools exist that define the relationship, role and responsibility of stakeholders in this recognition framework. These inputs and tools are the PAA Club Agreement, CPA Terms of Reference, PAA Certificate Policy, CA Recognition Agreement, CA (and CPS) Recognition Procedure, PAA Interconnection Agreement (with Service Level Agreement) and PAA Subscriber Agreement.

The PAA Club Agreement is a rulebook that governs the whole recognition and cross-border transaction service framework by defining the roles, responsibilities, relationship, and definitions of stakeholders and tools for the framework. By signing the subscriber agreements, users agree to the terms and conditions of the PAA Club Agreement, PAA PKI Mutual Recognition Framework and cross-border transaction service scheme.

The Certificate Policy (CP) prepared by the PAA Certificate Policy Authority contains the set of rules that govern the issuance and use of digital certificates, and indicates the applicability of the certificates to the communities within PAA. It specifies

---

22 RFC is the standard protocol of the Internet Architecture Board (IAB) that requests discussion and suggestions for improvements.
23 Internet Engineering Task Force.
the audit procedure, revocation, records archive, and Certificate and CRL (Certificate Revocation List) profiles among others. PAA CP is the basis of the Mutual Recognition of Public Key Infrastructure that forms a part of the conditions for periodical assessment of (accredited) CA; each CA will need to ensure that their CPS complies with this Certificate Policy.

The CA Recognition Agreement is an agreement between the PAA Certificate Policy Authority and each Certificate Authority contracted by the PAA Service Provider in each economy. Under the CA Recognition Agreement, the Certificate Policy Authority recognizes that the applicant CA is a conforming or accredited CA of PAA.

The CA and CPS (Certification Practice Statement) Recognition Procedure defines the procedure to be used by the PAA Certificate Policy Authority to give recognition to the individual Certification Practice Statement and Certificate.

3.2.3 How the PAA PKI recognition framework operates

The PAA CPA was established in 2001. Its main purpose is to set criteria for PAA CA and CPS recognition (figure 8).

The CPA Terms of Reference define a common PAA CP, a procedure for the recognition of CA’s CPS against this CP, a procedure for the management change and the recognition procedure, and it also administers the recognition and changes to the management procedure.

The PAA CP defines a set of rules as a minimum and common recognition criterion for use within the PAA domain and is trusted by the PAA members. The CPS of a CA seeking recognition by PAA is assessed against this PAA CP. The PAA CP governs a CPS that covers different aspects (policy, legal, operational and technical).

Recognition procedures of the PAA CP cover initial recognition as well as renewal and revocation of recognition. The initial recognition follows the following procedure:

(i) The applying CA submits supporting documents (e.g., a sponsor letter from a PAA member who is the user/relying party of the certificate, CPS, external assessment report, test report etc.) to the Certificate Policy Authority;

(ii) The PAA PKI experts review the submitted documents against the CP and other requirements;
(iii) The PAA PKI experts produce a recommendation report;

(iv) If accepted, the PAA will sign the recognition agreement with the CA, publish the CA information on the Authority’s official website and add the CA to the Certificate Trust List (CTL) to be distributed to PAA members.

Figure 8. PAA PKI Mutual Recognition Framework

The procedure for applying the PAA PKI Mutual Recognition Framework to actual recognition of cross-border exchanges of electronic messages is as follows (figure 9):

(i) Trading company A signs the User Subscription Agreement with the PAA service provider A in the trading company's domain economy. Trading company B will proceed in the same way. Service providers A and B exchange registered information of trading companies A and B;

(ii) Trading company A creates an electronic message, using an in-house system or service provider A's web system), signs it with a private key of trading company A (optional, depending on the arrangement between trading company A and service provider A) and dispatches the electronic message to service provider A;

(iii) Service provider A verifies the received electronic message and reformats it into the PAA standard format;
(iv) Service provider A creates an ebXML (OASIS e-commerce messaging standard) envelope, signs the PAA standard format message, identifies the receiving party and dispatches it to the receiving service provider B;

(v) Service provider B verifies the received message, signature and certificate of service provider A. Service provider B reformats the message into a national or proprietary standard of trading company B and signs the message with an electronic certificate of service provider B, based on the arrangement with trading company B, and dispatches the message to the trading company B;

(vi) Service provider B returns the delivery notification to service provider A. Service provider A returns the delivery notification to trading company A;

(vii) Trading company B receives the message either via an in-house system or the web application of service provider B;

(viii) If message acceptance notification is required, trading company B creates and dispatches the acceptance notification back to trading company A through service providers B and A.

Figure 9. PAA Transaction Services operation model
3.2.4 Challenges and lessons from the PAA Mutual Recognition scheme set-up experience

(i) Challenges

- Because the PAA Mutual Recognition scheme is based on a private agreement, PAA transactions and electronic messages are not recognised by most receiving economy authorities. Even if it is recognized, acceptance is limited to a specific authority.
- Not every member economy of PAA has a legal framework for certified CA and the use of electronic certificates (there is no digital signature law or electronic transaction or electronic document related laws). This gap among the participants can be addressed in the Framework Agreement to realize cross-border mutual recognition of electronic messages.

(ii) Lessons

- Governance structure and recognition policy are the most important aspects of a cross-border mutual recognition scheme.
- To establish a comparative level of trustworthiness and keep it sustainable, it is necessary to make a periodical compliance audit procedure on requirements.
- It is important to have authentication of the identity of individuals or organizations to establish non-repudiation of cross-border trade and adherence to "good practice" while being flexible to allow for local requirements or variations.

3.2.5 Summary and implications

PAA aims to provide seamless cross-border transaction services, and for this purpose it has established a PKI Mutual Recognition Framework to provide a comparable level of trustworthiness. PAA uses PKI for the identity authentication in establishing non-repudiation of cross-border exchange of electronic messages.

In this PAA recognition framework, seven tools define the relations among, role and responsibility of stakeholders. These tools are the PAA Club Agreement, Certificate Policy Authority Terms of Reference, PAA Certificate Policy, Certification
Authority Recognition Agreement, CA Recognition Procedure, PAA Interconnection Agreement and PAA Subscriber Agreement. The PAA Club Agreement is a rulebook that governs the whole recognition and cross-border transaction service framework by defining the roles, responsibilities, relationship, and stakeholders, and tools for the framework.

The Certificate Policy prepared by the PAA CPA stipulates the set of rules that govern the issuance and use of digital certificates. PAA CP is the basis of the Mutual Recognition of Public Key Infrastructure that requests a periodical assessment of accredited CAs. The object of recognition is a Certification Authority. Under the CA Recognition Agreement, PAA CPA recognizes that the applicant CA is an accredited CA of PAA.

Challenges arise due to the limited acceptance of PAA electronic transactions by public institutions as well as the capacity gap between PAA members. Only some PAA member economies have a legal background on the use of accredited CAs and electronic certificates.

(Keywords: PAA, PAA Club Agreement, PAA CPA, accredited CAs, periodical assessment, object of recognition is CAs, CPS covers policy, legal, operational and technical aspects, limited acceptance of electronic transactions of PAA by public institutions, and ebXML and proprietary PAA standard message format.)

4. Attributes that form cross-border recognition schemes

In the previous section, cross-border mutual recognition establishment and operational characteristics were identified through case analysis. Keywords and phrases of cross-border mutual recognition extracted from individual cases were mutually reviewed, and similar keywords and phrases have been grouped. The result shows that there are common key attributes for establishing and operating cross-border mutual recognition schemes (table 2).
Table 2. Common key attributes for establishing and operating cross-border mutual recognition schemes

<table>
<thead>
<tr>
<th>WCO AEO MRA</th>
<th>APEC MRA</th>
<th>ILAC MRA</th>
<th>EU eIDAS</th>
<th>PAA PKI MRA</th>
<th>Key attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCO</td>
<td>APEC</td>
<td>ILAC</td>
<td>EU</td>
<td>PAA Steering Committee</td>
<td>Mutual recognition scheme and governing body</td>
</tr>
<tr>
<td>Customs of MRA partner countries</td>
<td>Designating Authority or Accreditation Body</td>
<td>ILAC Arrangement Council</td>
<td>Cooperation Network and Supervisory body of Member States</td>
<td>PAA CPA</td>
<td>Implementation body</td>
</tr>
<tr>
<td>Customs of MRA partner countries</td>
<td>Regulatory Authority is responsible for telecommunications requirements</td>
<td>Technical and standards requirements are from the international standard body</td>
<td>EU Commission</td>
<td>PAA Steering Committee</td>
<td>Owner of recognition requirements</td>
</tr>
<tr>
<td>SAFE framework of standards</td>
<td>APEC Mutual Recognition Arrangement</td>
<td>ILAC Mutual Recognition Arrangement</td>
<td>eIDAS Regulation</td>
<td>PAA Club Agreement</td>
<td>Major legal instruments or governance rules set by the governing body</td>
</tr>
<tr>
<td>AEO programme</td>
<td>Conformity Assessment Bodies</td>
<td>Accreditation Bodies</td>
<td>Electronic Identification scheme</td>
<td>Certification Authorities</td>
<td>Target object being recognised</td>
</tr>
<tr>
<td>Standards compatibility mechanism</td>
<td>Designation or Accreditation</td>
<td>Accreditation</td>
<td>Peer review for eID scheme and Ex-ante supervision for QTSP</td>
<td>Accreditation</td>
<td>Actualization methods for recognition</td>
</tr>
<tr>
<td>Information exchange</td>
<td>Confidence building measures</td>
<td>Periodical peer-review</td>
<td>Notification of eID scheme changes, and ex-post supervision for QTSP</td>
<td>Periodical assessment</td>
<td>Trust mechanism</td>
</tr>
<tr>
<td>Public service area</td>
<td>Public service and private service areas</td>
<td>Private service area</td>
<td>Mostly in the public service area</td>
<td>Mostly for private transactions and limited acceptance of electronic transactions by public institutions</td>
<td>Application coverage of recognition</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>European Union Interoperability Framework</td>
<td>ebXML and proprietary PAA technical standards</td>
<td>Interoperability guidelines</td>
</tr>
</tbody>
</table>
This report categorizes the nine common elements into three groups (table 3). They are: (1) an international or regional body that governs the rule or provides principles for cross-border mutual recognition schemes; (2) implementation bodies implementing such schemes or guidelines; and (3) owner of recognition requirements. These three elements represent key stakeholders in the cross-border mutual recognition scheme. Another group includes: (5) target object being recognized; (6) execution method for recognition; (7) trust mechanism; (8) application coverage of recognition; and (9) interoperability guidelines. These five elements comprise the operational aspect of cross-border mutual recognition scheme. An element of (4) legal group, is a major legal instrument or governance rules set by the governing body or agreed upon by participants, which is a legal basis of a cross-border mutual recognition scheme.

**Table 3. Three groups of MRA attributes**

<table>
<thead>
<tr>
<th>Key stakeholder group</th>
<th>Legal group</th>
<th>Operational group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 International or regional body that governs the rule or provides principles for cross-border mutual recognition scheme.</td>
<td>4 Legal instrument or governance rules set by the governing body or agreed upon by participants.</td>
<td>5 Target object being recognised.</td>
</tr>
<tr>
<td>2 Implementation bodies implementing such a scheme or guideline.</td>
<td></td>
<td>6 Execution method for recognition.</td>
</tr>
<tr>
<td>3 Owner of recognition requirements.</td>
<td></td>
<td>7 Trust mechanism.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 Application coverage of recognition.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 Interoperability guidelines</td>
</tr>
</tbody>
</table>
4.1 Key stakeholder group

- An international or regional body that governs the rule or provides principles for cross-border mutual recognition schemes (or a scheme owner). In all the multilateral recognition schemes, there is an international or regional governing body that is responsible for developing and maintaining recognition principals. However, their role and responsibility are case-specific. Some international organizations control the detailed specifications of recognition implementation, including the execution method and trust mechanism, while some international organizations merely provide guidelines and principles only for participating members.

- Implementation bodies implementing such a scheme or guidelines. Implementation bodies are stakeholders that supervise the implementation of the mutual recognition process and system by the agreement or guidelines. The implementation body could be the owner of recognition requirements.

- An owner of recognition requirements (or a decision-maker of recognition specification). An owner is a stakeholder who sets specific mutual recognition criteria and requirements (such as the specific competencies or conformity to security or quality requirements). A specification owner does not have to be a stakeholder governing a cross-border recognition scheme nor an implementing body.

4.2 Legal group

- A legal instrument or governance rules that are set by the governing body or agreed upon by participants.

- Most mutual recognition schemes have an international, regional or bilateral agreement, a set of guidelines or agreed upon by the governing body(s).

4.3 Operational group

- The target object being recognized. Mutual recognition can be achieved through direct or indirect recognition methods. For example, notarization is one method of direct recognition on a document. In the case of APEC TEL MRA, it is a testing laboratory and certification body, not the test result report nor a Certificate. In the case of eIDAS, the target object is a qualified trust service
provider. By recognizing the trusted issuing body, the documents are indirectly recognised (or accepted) in the other receiving MRA country(s).

- An execution (or actualization) method for recognition. Recognition can be actualized by different methods. Designation and accreditation are common methods for the actualization of recognition.

- Trust mechanism is about how the mutual recognition arrangement maintains trust after an actualization of mutual recognition. Operating and maintaining trust under the mutual recognition arrangement is a challenging issue. In most cases, an actualization and a trust mechanism are shown together in the "compliance" form (i.e., APEC TEL MRA or PAA MRA).

- Application coverage (scope) of recognition. Application coverage is about whether the recognition scheme is designed to cover regulatory control or public service areas, or private business transactions.

- Interoperability guideline: Whether cross-border mutual recognition arrangement (of electronic transactions) provides any technical interoperability guidelines for the interconnection between the participants’ scheme.

5. Conclusion

Cross-border paperless trade requires a certain degree of trust. Some countries have national infrastructures to provide trusted paperless interaction in different spheres, such as tendering, customs declaration, Single Window among others. All these infrastructures are usually based on national legislation and may apply different technologies. Consequently, economic operators face obstacles when they engage in paperless trade across borders.

The Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific, adopted by the ESCAP member States, is aimed at "promoting cross-border paperless trade by enabling the exchange and mutual recognition of trade-related data and documents in electronic form, and by facilitating interoperability among national and subregional Single Windows and/or other paperless trade

---

24 When the overseeing structure is weak and governance power is decentralized, this form of dispute resolution is commonly accepted by the member States.
systems, for the purpose of making international trade transactions more efficient and transparent while improving regulatory compliance.\textsuperscript{25}

The aim of this study is to (a) provide an overview of existing practices in deploying international initiatives of cross-border mutual recognition and (b) help the members of the Framework Agreement to gain a better understanding of how the cross-border mutual recognition schemes are structured and how they work. Through the five cases analysed, nine attributes in three groups of key stakeholders, legal and operation for forming the mutual recognition arrangement was identified. These attributes interact with each other and constitute the characteristics of the mutual recognition scheme. As such, representative models of the cross-border mutual recognition scheme can be constructed by reflecting different values for the attributes.

Two other key findings are characteristic of an object of mutual recognition scheme as well as the importance of recognition of e-ID for cross-border electronic transactions. In the cross-border mutual recognition arrangement cases, the mutual recognition object is often not the last material that crosses borders. In the five cases, the recognized objects are Certification Authorities (PAA), electronic Identification Schemes (eIDAS), Conformity Assessment Bodies (APEC), Accreditation Bodies (ILAC) and the AEO Programme (WCO). Thus, in all five cases, the object of mutual recognition is an organization that produces (electronic) certification documents or authenticates the human/entity that is being exchanged across borders with trading partners, or programmes or processes operated by such organizations.

Individual objects of mutual recognition cannot be incorporated into the mutual recognition scheme until the organization, or its programme, has been evaluated through peer review or audit by a superior organization for relevant management norms, rules and technical competencies required to meet the minimum requirements for mutual recognition. This is an important lesson for the members of the Framework Agreement with regard to designing the mutual recognition scheme.

\textsuperscript{25} See https://treaties.un.org/doc/Treaties/2016/05/20160519%2012-16%20PM/Ch_X-20.pdf.
Cases of cross-border mutual recognition for the facilitation of electronic transactions similar to the Framework Agreement are e-IDAS and PAA. The mutual recognition objectives of these two schemes – a Certification Authority and an electronic identification scheme – are common in terms of authenticity. Both objects aim to provide a digital solution for proof of the identity of citizens or organizations. According to the World Bank,26 two-thirds of the high-income countries have already adopted digital IDs, and low-income countries are building digital ID systems, leapfrogging the more traditional physically-based system.

Most developing countries have a digital ID scheme tied to specific functions and serving a subset of the population. The findings from the target object of MRAs show that it might be necessary to consider including the mutual recognition of the electronic identity or authentication scheme as part of the Framework Agreement’s mutual recognition arrangement to achieve the goal of promoting cross-border paperless trade under the Framework Agreement.

For future research, it would be worthwhile reviewing other theoretical studies on mutual recognition arrangements and comparing the structure and components of the results of this report’s case studies.

---