ESCAP
Economic and Social Commission for Asia and the Pacific

Document title: Legal Implementation Guide for Cross-border Paperless Trade

Version: 23 May 2024

Third session of the Standing Committee, 3-5 June 2024
Agenda item 2c

DRAFT

This background document is prepared to facilitate discussion of the Standing Committee Agenda item 2c on reviewing the draft legal guide on engaging in a cross-border exchange of trade-related data and documents in electronic form consistent with regional and international laws and regulations and best practices.[1]

[1] The draft guide was prepared by Mr John Gregory. The concept note as well as earlier draft was reviewed by the UNNExT Expert Group Meetings on Developing a Legal Guide for Cross-border Paperless Trade. Experts provided verbal and written comments as well as inputs to the draft guide. All experts participated and provided feedback on their individual capacities. Participation and contributions from these experts are well appreciated: Aleksei Bondarenko, Luca Castellani, Nikolay Dmitrik, Runqiu Du, Maksim Egorov, Leonila Guglya, Sergey Kiryushkin, Alexander Plakhov, Tamara Shashikhina, Nina Solovyanenko, Tianmi STILPHEN, Bryan Tan, Oleg Vinichenko and Hong Xue.

Table of Contents

Contents

I. Introduction 3

I.A. Context 3

I.B. Objective 4

II. Harmonization of laws 4

II. A. Introduction 4

II. B. Principles 5

II. B. 1. Functional equivalence 5

II. B. 2. Non-discrimination 6

II. B. 3. Technology neutrality 6

II. B. 4. Interoperability 7

II. C. International instruments: standards and laws 7

II.C.1. Validating e-communications generally 8

II.C.2. Making international financing documents work 9

II.C.3. Supporting digital transport documents 9

II. D. Trade agreements 10

III. Mutual Recognition 12

IV. Platforms 14

V. International and domestic laws 17

V. A. Impact of international laws and regulations on domestic laws 17

V. B. Aligning the domestic framework with selected international frameworks 17

VI. Conclusion 20

APPENDICES 21

Appendix A: Representative international agreements and standards affecting cross-border paperless trade 21

Appendix B: Standards 23

Appendix C: 24

Paperless trade commitments in trade agreements involving more than three ESCAP member States and the CPTA Parties 24

Appendix D: The need for global trusted environment to support cross-border paperless Trade (Including mutual recognition of digital data and documents) 27

Appendix E: Discussion paper: Basic elements of legal recognition of electronic data and documents in paperless trade facilitation 29

DRAFT

LEGAL IMPLEMENTATION GUIDE FOR CROSS-BORDER PAPERLESS TRADE

A legal guide to engaging in cross-border paperless trade taking into account regional and international laws and regulations and best practices

DRAFT

I. Introduction

I.A. Context

The potential advantages of advancing cross-border paperless trade are evident, presenting an opportunity to counteract the rising trajectory of trade costs through enhanced efficiency achieved by streamlined and digital processes. The latest report jointly conducted by the Asian Development Bank (ADB) and the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) emphasizes that further acceleration of digital trade facilitation implementation could result in a noteworthy reduction of average trade costs in the region, estimated at approximately 11%.[2]

For our purposes, the focus remains in facilitating the movement of goods through the use of commercial or regulatory documents or data in support of transactions involving those goods, not on production of goods. The proper documents are needed to ensure both that any transaction is permitted (i.e. it is not an offence, and it complies with applicable regulations) and that it is legally effective (i.e. it is valid and enforceable in commercial practice – the parties know what they have to do - and in the event of a dispute.)

Again, our concern here is not about the substance of what is allowed or what is required. It is about demonstrating compliance with the law, the ability of transacting parties to create effective legal relationships and to support those relationships wherever required. The demonstration, the creation of relationships and their support all depend on documents, or at least data, generated in or relating to the transactions.

While this kind of analysis is needed even for domestic commerce, it becomes more complex when the goods and supporting documents cross borders. Are the same documents needed in another country, and are goods originating in another country properly supported when they come to this country?

Such questions have been asked for a long time in cross-border trade, and there are widely accepted answers, which the Guide will mention. The novelty arises when the supporting documents become electronic. Is a collection of electrons a document at all? How does one decide to trust it? How does it fit into one's legal and regulatory system? Should one focus on 'data' rather than 'documents', and what difference would that make? The Guide will attempt to address these questions.

[2] ADB and ESCAP (2024). Asia-Pacific trade facilitation Report 2024: promoting sustainability and resilience in global value chains. Available at https://www.unescap.org/kp/2024/asia-pacific-trade-facilitation-report-2024-promoting-sustainability-and-resilience-global

I.B. Objective

This document will serve as a guide to the legal issues arising in cross-border paperless trade, indicate the most commonly accepted solutions to those issues, and suggest approaches for countries to implement or adapt those solutions to facilitate their participation in that trade. It will do so with particular reference to the United Nations treaty, the Framework Agreement on the Facilitation of Cross-Border Paperless Trade in Asia and the Pacific (hereafter referred as "the CPTA").

At the domestic level, in most countries today, parties to most commercial transactions have very broad autonomy to make the deals that suit them for business purposes. The law does not restrict them from taking on whatever obligations they choose. Recourse to "law" to decide the content or even performance of contracts is not common, except at the enforcement stage.

But there are specialist areas of the law like transport and financing documents where legal effect and enforceability depend on careful compliance with applicable legislation. Specialized instruments can also be needed in areas of regulated economic activity where the regulations require them.

Likewise, it is often helpful to ensure by legislation the effectiveness of electronic documents of all kinds, aside from their substance: (i) are they valid if electronic? (one of the earliest questions to be disposed of domestically as well as internationally); and (ii) how can one reproduce electronically some key features of paper documents e.g. originality, uniqueness, controllability?

Most countries in the world have made some legal accommodation with electronic communications. Some e-transactions are legally effective just about everywhere. Considering cross-border trade, however, raises the question whether domestic accommodation is good enough.

II. Harmonization of laws

II. A. Introduction

Referring to an issue that this Guide will come back to: should the law on the domestic use of e-communications be consistent with, or even modeled on, the law on such communications in cross-border trade?

The short answer is that it would be helpful if countries gave legal effect to e-documents at home and abroad on consistent principles. One of the principal methods of ensuring legally effective use of documents and data across borders is the harmonization of the legal regimes that apply to them. The more the law of country A and the law of country B about any topic are similar, the fewer legal problems will arise dealing with that topic across their borders. This is true of rules about form as well as rules about function.

Harmonization is a guiding theme of the CPTA. The CPTA puts great emphasis on harmonization of a Party's law with international precedents and standards, and by implication, with the laws of states with which one trades that are also based on those instruments. Several articles promote the concept:

- Article 5 sets out principles for Parties' approach to paperless trade. Most of them are recognizable statements from international organizations that have developed models for harmonization, notably UNCITRAL, the United Nations Commission on International Trade Law.

DRAFT

- Article 6 requires Parties to endeavour to establish a national policy framework and enabling legislation for paperless trade, 'taking into consideration international standards and best practices.'

- Article 9 asks Parties 'to apply international standards and guidelines to ensure interoperability in paperless trade', as well as to 'endeavour to become involved in the development of international standards and best practices.'

- Article 10 allows Parties to 'adopt relevant international legal instruments concluded by the United Nations and other international organizations.' They are also to endeavour to ensure that 'exchange of trade-related data and documents in electronic form is consistent with international law as well as regional and international regulations and best practices.'

II. B. Principles

The first four principles of article 5 provide a good foundation for establishing, or reforming, legal frameworks conducive to cross-border paperless trade. They are functional equivalence, non-discrimination, technological neutrality and interoperability.

II. B. 1. Functional equivalence

DEFINITION: Functional equivalence means that data or a document in electronic form are treated as having the same legal and policy function as their paper-based equivalent. One does not have a separate or parallel legal world of digital documents; one has a uniform world of documentary policy. One does not have to redraft the substantive rules for the transactions or relationships that are becoming digital.

IMPLEMENTATION STRATEGY: How does one implement this principle? One can analyse one's own legislation to see why it says what it does. It may be easier, these days, to consider the analysis already done elsewhere and reflected in international instruments.

Legislation – based on a convention or implementing a model law – should spell out what features of a digital document will fulfil the legal policy functions of the digital one. For example, a digital document can be the functional equivalent of a written document – so if the law requires writing, the digital functional equivalent will satisfy that requirement. To do that, the UNCITRAL Model Law on Electronic Commerce and the United Nations Electronic Communications Convention (ECC) require that the digital document be "accessible so as to be usable for subsequent reference". In essence, the function of a writing requirement is to make the contents of the writing available later, to have them serve as memory. The functional equivalent of writing on paper is digital text accessible for subsequent reference.

Likewise, the functional equivalent of a signature on paper is a digital method associating a legal person with a text and indicating the person's intention with respect to the text (often stated as 'approval' of the text.) Sometimes, when the signature or the association of the person with the text is particularly important, the law may require more detail about the method of signing, to make it more reliable.

GOOD PRACTICES: The UNCITRAL Model Law on Electronic Signatures, followed by the ECC, gives more detail for such cases about the connection between the signatory and the signature and about the signature and the signed text.

DRAFT

Similar language is found in the annex to the CMR Convention on Road Transport about the authentication of electronic consignment notes. This is just one demonstration that the principles set out in the CPTA are broadly accepted in operating legal regimes.

II. B. 2. Non-discrimination

DEFINITION: This principle protects the legal effectiveness of electronic data, by ensuring that its effectiveness is not prejudiced, or discriminated against, solely because it is in electronic form.

IMPLEMENTATION STRATEGY: In general, an express legislative statement of the principle will satisfy the principle. The 'double negative' formulation (legal effect shall **not** be **denied** solely because..) is needed because the legislation should not positively grant legal effect to any electronic data. There may be many reasons why electronic data should not be legally effective in particular cases. This provision ensures that its electronic form alone is not one of them.

GOOD PRACTICES: Most implementations of the UNCITRAL Model Law on Electronic Commerce have been built on this principle.

II. B. 3. Technology neutrality

DEFINITION: This principle means that laws on digital documents should not specify what technology or procedures must be used to create the documents. Transacting parties can decide how to achieve the results specified in the law.

IMPLEMENTATION STRATEGY: Countries can implement this principle simply by not attaching specific technologies to permission to use e-communications.

Though most international instruments promote technology neutrality, they also accept that in some cases and for some purposes, the law may need to be more precise about the technological results to be achieved and sometimes about the technology to be used. High security or reliability demands lead to higher precision about the technology needed to meet them.

Consultation with businesses and regulators may disclose instances where more assurances are needed that would require specifying the technology to be used. It is important, however, not to be any more technology-specific than circumstances require, since prescribing technology has disadvantages (cost, inflexibility) as well as benefits.

GOOD PRACTICES: Many international precedents have been enacted in the past thirty years. Most implementations of the UNCITRAL Model Law on Electronic Commerce have been largely or wholly technology neutral.

However, many countries insist that for an e-signature to be functionally equivalent to a handwritten signature, the e-signature must be created using public key cryptography with a certificate from a national authority – conditions that can be onerous and that a foreign signature provider can probably not satisfy. This risk standing in the way of innovative methods of authentication and recognition, such as blockchain-based e-signing.

DRAFT

II. B. 4. Interoperability

DEFINITION: This principle refers to the ability of documents to be effective in any medium – on paper or digital, mainly – and to move from one medium to the other as required, and from one type of use, say commercial, to another, say regulatory. "Data is interoperable if information from one platform can be interpreted unambiguously by another platform."[3] It is "essential for both government and industry to enable documents to flow between systems in digital form. Siloed approaches will create inefficiencies and undermine the benefits of paperless trade."4

It can also refer to the ability of documents to be effective under different legal regimes, such as across borders. They work at both ends of a trade, or along a trading corridor.

IMPLEMENTATION STRATEGY: Domestic interoperability can be achieved by using consistent language in enabling legislation. References to technical standards for compliance should be consistent as well, and common data structures. Technology neutrality helps in this. International interoperability is more likely to flow from co-ordinated legal rules, bilateral or multilateral agreements, or appropriate harmonization of legal rules and technical and organizational standards.

II. C. International instruments: standards and laws

Several of the articles listed above advocate conformity with international standards and laws, and "best practices". "Standards" in these provisions refer not only to technical standards but also to accepted methods of expressing policy, independent of the legal vehicle used to convey them. The proper mix of technical and legal provisions in harmonizing rules for electronic communications is often hard to determine, and sometimes controversial.

Many of them are expressed in some or all of the instruments listed in Appendix A to this Guide. The reason for the references, to all the instruments and the UN documents in particular, is to promote harmonization of law on paperless trade. Here we look briefly at how that can work in practice.

A number of the documents listed fall into the class of "United Nations documents" referred to in article 10 of the CPTA. They can be guides for any Party to the CPTA. Before any laws are changed, lawmakers should hold careful discussions with potential creators and users of the data and documents that will be affected. The capacity of such Parties to apply reliable practices needs to be verified and perhaps developed first. Capacity building is possible through membership in the CPTA, through working groups and the like.

It may be noted that many ESCAP member States have not acceded to the main international documents on electronic commerce and electronic signature. Adhesion may be relevant, among other things, in giving effect to article 8 of the CTPA on mutual recognition, discussed below.

One should note that foreign instruments may in some cases reflect different principles or rules of law about the underlying transactions. It is not just a one-to-one comparison of the text of the documents themselves. Much of this level of analysis has already been done in the development of the United Nations documents (and other instruments), and newcomers to the discussion can usually trust the analysis reflected in the guides to enactment or reports on the development of the instruments, to govern their own implementation.

---

[3] Wirjo, Bayhaqi, Oh, "Digitalizing Trade: The Role of Paperless Platforms", APEC Policy Brief (March 2024), p.6. Online: CITE

[4] International Chamber of Commerce, "Creating a Modern Digital Trade Ecosystem", 2021, page 11. https://www.dsi.iccwbo.org/_files/ugd/0b6be5_0934506fada643a197d5f727413c4389.pdf?index=true

DRAFT

It should be noted that international rules to be harmonized may be in the form of technical standards governing types of trade or governing methods for making electronic communications more reliable and trustworthy among trading partners. The International Standards Organization is one noted source of such standards.[5] The United Nations Economic Commission for Europe (UNECE) has published many standards through the Centre for Trade Facilitation and E-business, UN/CEFACT.[6] The G7 has been managing a project called Data Free Flow and Trust (DFFT) that is developing criteria for the trust needed to support the free flow of data. Regional bodies like the European Union or respected national bodies like the United States National Institute for Science and Technology (NIST) may also be influential. Private bodies like the International Chamber of Commerce (ICC) are also active – its Digital Standards Initiative has been very active in developing rules for trusted networks.[7] There is no shortage of models. A recent APEC study said that according to the WTO and ICC, 'close to 100 standards and initiatives are used in international trade today.' [8] Evaluating which are the most promising, or which are becoming the basis for international consensus, can be a challenge. (See Appendix B for more on Standards.)

And knowing how and when to combine them with legal rules, and the extent to which legal rules should depend on the application of technical standards, is very challenging – especially when trying to be "technology neutral".

Consider as case studies, as it were, three classes of international documents mentioned in Appendix A to see how they support cross-border paperless trade. This is not an exhaustive list. One could consider identity management and trust services, or electronic invoicing, or many other points of concern.

1. Validating e-communications generally: Model Law on Electronic Commerce (MLEC), Model Law on Electronic Signatures (MLES), Electronic Communication Convention (ECC), Model Law on Identity Management and Trust Services (MLIT)
2. Making international financing documents work: Model Law on Electronic Transferable Records (MLETR)
3. Supporting digital transport and shipping documents: eCMR

II.C.1. Validating e-communications generally

The UNCITRAL Model Laws will apply mainly at the domestic level, but their principles are very widely adopted in the world and will assist in harmonization with many nations. While the language of the Model Laws and the ECC is on its face commercial, their principles can often be applied throughout a country's legislation, to resolve issues of the medium of other kinds of communication as well. Governments need not prescribe in detail how private parties should act to take advantage of the permissions given by the Model Laws. Flexibility is an advantage. Governments can indicate the existence of guides or supporting texts internationally.

Implementing legislation for the Model Laws and the Convention should not require more security or special technology than necessary. They are all built on the principle of technology neutrality. Countries should consider international best practices and solutions adopted by their trading partners. Some adopters of these instruments will need to build more capacity than others, as will some industries or commercial

[5] More information available at https://www.iso.org/
[6] More information available at https://unece.org/trade/uncefact
[7] More information available at https://www.dsi.iccwbo.org/
[8] Wirjo et al, above, fn 3, p. 7.

DRAFT

sectors. Some parts of the economy may be able to move forward under a new legal regime more quickly than others.

While this Guide principally addresses questions of law, the state of the available technology is also critical. The basic state of technology is an adequate physical infrastructure – telecommunications, computers, connectivity. Beyond that, permissive law may inspire the development of capable technology, but that may not be enough. Consider the Readiness Checklists on Cross-border Paperless Trade, both for legal and technical aspects , and the Readiness Assessment Guide for Cross-border Paperless Trade .[9] International sources of support and expertise in relevant technology have been mentioned above. See also Appendix B.

II.C.2. Making international financing documents work

A special class of document essential to trade, especially cross-border trade, is transferable records. They are 'transferable' because the holder of the document owns the goods or money described in the document and can require their delivery. One can change the ownership by transferring (selling) the paper. A bill of lading is an example; the holder of the B/L can demand delivery of the goods it described. Likewise, a warehouse receipt shows ownership of the goods in the warehouse.

They are often used as a means of payment or their delivery a condition of payment. They are often a kind of financing document. A promissory note or bill of exchange is also a transferable record in this sense. It is important that such transferable records should be authoritative, i.e. there should be only one valid document at a time – so competing claims are not made on the goods.

The UNCITRAL Model Law on Transferable Electronic Records (MLETR) sets out the rules for doing this electronically. (MLETR has other uses than in finance as well.) The key element is the use of a "reliable method" to show that a document is *the* document with the rights attached, that is has not been altered and that its ownership is accurately stated. Just adopting the words of the MLETR is unlikely to be satisfactory. Practical rules describing the reliable methods will be needed to give businesses the confidence to accept the records in electronic form. The Model Law sets out criteria for judging reliability, though they are relatively abstract.

MLETR's implementation in significant trading nations is quite recent, unlike that of the MLEC, MLES and ECC mentioned above. Countries contemplating adoption should pay close attention to how it is being done there. Many people are confident that MLETR represents the future of many trade documents. MLIT is too recent to have had much impact on international developments, but a number of its principles on trust services will probably be relevant to resolving issues mentioned in this Guide.

II.C.3. Supporting digital transport documents

Transport documents may be considered a separate class of document, particularly focused on cross-border trade. There are many forms, though bills of lading and consignment notes are important among them. They accompany goods across borders and through Customs.

Many have standard forms on paper, under conventions developed over the decades. More recently, most or all of the main paper forms have, by convention, been given electronic versions. However, the validity

[9] The Interim Intergovernmental Steering Group on Cross-border Paperless Trade Facilitation and its Legal and Technical Working Groups have developed the Checklists. ESCAP, along with partners including EIF and UNCITRAL, has further developed the Readiness Assessment Guide. Further information and details available at https://readiness.digitalizetrade.org/

DRAFT

in law of these digital documents in the countries other than where they are made is still open to question. Work continues internationally on supporting their use.

Special attention to supporting the cross-border legal validity of electronic transport documents under the most recent version of the main transport conventions would be a valuable contribution to cross-border paperless trade. Doing so in a way consistent with neighbouring countries and trading partners would be best.[10]

II. D. Trade agreements

A relatively recent, but already widespread, way to harmonize the law on digital data and documents among nations is to make such harmonization an obligation in a bilateral or multilateral agreement on trade relations generally. The class used to be known as 'free trade agreements' (FTAs), but the 'freedom' provided by the reduction or abolition of tariffs has given way to farther-reaching attempts to promote trade among the parties. In essence, these developments acknowledge that facilitating trade today involves ensuring that trade can be done digitally.

When e-commerce provisions were first introduced into FTAs, some concerns were expressed whether they were the right vehicle. FTAs tended to be subject to broad economic forces and negotiations involving geopolitical trade-offs, whereas e-commerce instruments were more usually technical documents debated by commercial law experts.[11]

However, it appears to be generally accepted that FTAs tend to have better political momentum than technical commercial law reform, and their multi-state character gives them a harmonization power – because the agreements will actually be adopted and implemented - that e-commerce instruments on their own simply do not have. In essence, they recognize that facilitating trade today involves ensuring that trade can be done digitally. The parties have to remove barriers to digital trade, and in newer versions, actively promote it,[12] including through interoperability of solutions used and mutual recognition of their outcomes.

An 'early' version of these trade agreements with provisions enabling e-commerce is the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (2016). It requires parties to recognize electronic signatures on terms similar to those in UNCITRAL texts. The Canada-Mexico-United States Trade Agreement (2018) required to harmonize their laws governing electronic transactions to implement either the MLEC or the ECC. In addition, parties must have rules on e-signatures consistent with the MLES or ECC.[13] It is worth noting that the FTAs do not attempt to renegotiate the e-commerce instruments; they merely attempt to get them onto the agenda for adoption.

DRAFT

[10] UNECE has a working group to operationalize the digital records annex to the CMR convention on carriage of goods by road. It is far from finished its work.

[11] See for example J.D.Gregory, "Trade Agreements to promote E-commerce", 216, https://www.slaw.ca/2016/11/08/trade-agreements-to-promote-electronic-commerce/

[12] ESCAP has helped develop a website analysing a large number of trade agreements from different aspects. The texts of agreements can be searched for key terms. See "Legal TINA" – the legal version of Trade Intelligence and Negotiation Advisor, online: https://legal.tina.trade/app/start.

[13] An analysis of the CTTPP and the Canada/US/Mexico agreement is online: "Trade Agreements to promote e-Commerce II", (2018) https://www.slaw.ca/2018/11/08/trade-agreements-to-promote-electronic-commerce-ii/.

Additional requirements touch on consumer protection, privacy and cross-border enforcement. A country becoming a party to such an agreement needs to enact appropriate legislation. Models for it are not hard to find.

A more 'modern' or advanced trade agreement is the Digital Economy Partnership Agreement (DEPA) among Singapore, New Zealand and Chile (2021). In the words of a Canadian government analysis,

> It builds upon the digital trade or e-commerce chapters of existing free trade agreements, such as the CPTPP, adding enhanced commitments on facilitating digital trade and multi-party cooperation on a range of advanced technologies.[14]
>
> It addresses a range of emerging digital economy issues including:
>
> - artificial intelligence
> - digital identities
> - digital inclusion

The portfolio of the rules addressed in e-commerce and digital economy agreements ranges over 50 topics combined. Many of them are of key or at least some relevance to paperless trade.

It must be said, however, that the actual laws that a member must adopt to comply with the DEPA are not spelled out in detail. The Agreement requires some action but does not give specific direction on its content. It does, however, promote the World Trade Organization's Trade Facilitation Agreement (TFA), which contains obligations about what services and activities its members must provide digitally. See the chart in Appendix C for examples of provisions on digital economies found in recent trade agreements.

While the provisions of the e-commerce/digital economy instruments are, typically, broadly phrased, some of them are accompanied by more precise secondary acts of binding (annexes) or non-binding nature, such as MoUs, action plans, or implementation guidelines, clarifying the understanding of the rules agreed on by the parties and/or setting the implementation benchmarks.

The most representative (in the terms of membership) of such agreements, still in the making, is the future E-commerce Agreement to be concluded under the auspices of the WTO Joint Statement Initiative on Electronic Commerce (the WTO JSI), in which 90 WTO Members are participating.

In short, these agreements recognize the value of digital communications across the economy and push the parties to develop state-of-the-art provisions in all of them. There are a few reservations or exceptions on points of sensitive public policy, but generally subject to limits of reasonableness. While it would be premature for countries in the early stages of their digital trade policy to expect to join these agreements in the short term, the agreements may serve as a focus of ambition, as to where they might like to get to in the next few years.

The key feature of both agreements is their comprehensive concept of the digital economy. It is not enough simply to authorize electronic forms of 'writing' or 'signature', though doing so is necessary. The principles of the CPTA are capable of taking Parties much further. However, agreement on recognition of authentication methods may be more difficult when the states involved do not use the same underlying cryptographic algorithms for authentication. It is more difficult to give legal effect to a document when exchanging electronic documents from different jurisdictions based on different cryptographic standards.

[14] https://www.international.gc.ca/trade-commerce/consultations/depa-apen/background-information.aspx?lang=eng

DRAFT

The DEPA is a first of its kind digital economy agreements It has two components. The first is a restatement of principles in existing treaties and agreements. As DEPA parties are signatories to these treaties and agreements, this is not controversial for economies with a digital outlook.The second is an aspirational call to certain areas (such as e-invoicing and artificial intelligence) and principles. There are non-prescriptive or have weak standards. This again should be non-controversial for economies with a digital outlook.

DEPA contains many references to the WTO – including WTO agreements and dispute resolution mechanisms). This is because the DEPA is only open to WTO members. Also, the DEPA was formed to allow WTO members who had a digital outlook to form common ground while waiting for the general body of the WTO to agree on a digital economy agreement. Progress is being made on the JSI (Joint Standards Initiative) that has ambitious paperless trade rules.

DEPA is designed as an open agreement welcoming other economies to join to join, which means it has the potential to expand to a multilateral agreement. The Republic of Korea has acceded to DEPA in May 2024. China, Canada, Costa Rica and Peru have submitted formal requests to accede. Moreover, DEPA provide a flexible mechanism for future participants, which allows them to select only elements ('modulars') and to take different levels of commitment that best suit the particular circumstances of members. Even governments that intend to carry on with unilateral decisions could choose to align domestic rules with aspects of the DEPA.[15]

III. Mutual Recognition

The other important rule of the CPTA affecting its international impact is article 8, which requires Parties to "provide for mutual recognition of trade-related data and documents in electronic form originating from other Parties on the basis of a substantially equivalent level of reliability."

The second paragraph of the article acknowledges that Parties will have to make agreements on the rules or conditions for mutual recognition in practice, and these agreements can involve some complicated technology. There is no off-the-shelf system for mutual recognition.

To a large extent, mutual recognition depends on the comfort and confidence of the Parties – public or private – in relying on the documents and data to be exchanged between the Parties. Different Parties may have different degrees of comfort and confidence with the same technology, so arriving at generally acceptable rules has been difficult.

Comfort levels and practices and responsible officials, and even the reliability of trading partners, may change over time. "Trusted trade environments" may evolve.

Parties may need to be satisfied with adequate reliability – reliability that is 'appropriate in the circumstances', in the words of the Model Law on Electronic Commerce. There will be no universal solution more precise than that, though agreements among particular Parties about particular transactions using particular documents or data may be drafted in more detail.

[15] https://asiantradecentre.org/talkingtrade/designing-next-generation-trade-agreements-for-the-digital-economy.

DRAFT

Substitutes for technical reliability may be satisfactory to some transacting parties, such as a general trust in the integrity of the source of the data or documents.[16]

However, if agreements to "operationalize" mutual recognition are to be made formal, they should have some substantive technology rules behind them. In 2014, the Netherlands and the Republic of Korea made an agreement to mutually recognize certain plant quality certificates ("e-Phyto" certificates).[17] The agreement contained recitals that the two countries had exchanged documents on point and had not had any problems with them. It went on to agree that such documents could continue to be used with legal effect in each country.

What the agreement lacked was any description of how the documents had been produced or communicated. There were no 'safety standards' or rules for creating a reliable document. There was nothing that one party could verify about an incoming document to see that it continued to deserve to be trusted and thus given legal effect (be recognized) where it was received. On a technical reading of paragraph 8(3) of the CPTA, that provision was not satisfied because it was not possible to know that the agreement was 'consistent with the principles of the transboundary trust environment and all the other general principles' described there.

The challenge is that ultimately, one cannot require trust without justifying it, and justifying trust is very complex. Deciding what is 'consistent with the principles of the transboundary trust environment' is technical and legal and financial and personal all at once. The MLES and MLETR and now the MLIT all have considerations about trustworthiness, all consistent, gradually becoming more specific over the more than 20 years between the oldest and newest of these instruments.[18] No factor is definitive and there is no body with complete authority to adopt standards or to ensure compliance with them.

States will find it hard, perhaps impossible, to agree to give a body that authority without being quite specific about what the standards will be. National legislatures undertake this kind of activity – decide on laws and enforce them. But no global legislature exists with the legitimacy to make rules for everybody, and no one has adequate enforcement powers for prescribed standards. (See the earlier discussion of international standards … and the bodies, public, quasi-public and private, that are trying to fill the gap.)

It may be necessary to create such a legal and technological regime voluntarily – by international convention - to form the foundation of an acceptable trusted trade environment. Elements of such a proposal are set out in Appendix D. Policymakers may have to decide whether having such a regime is necessary before progress can be made on other matters. Probably a definitive global plan for substantially equivalent reliability of all digital documents and trade data will depend on some blend of legal and technical provisions like what is in the appendix, possibly with features from proposals mentioned in Appendix B.

That said, it is not necessary to solve all the problems before solving any of them. Some current initiatives are promising and partial solutions are worth pursuing. Deciding how far to go along the road to a reliability in which we have confidence is still difficult.

IMPLEMENTATION STRATEGY: Adopt the principles of MLES article 13 and CPTA article 8, if not already enacted: give legal effect to foreign-sourced data and documents if their authentication is as reliable

---

[16] Some of the issues and the workarounds to explain why cross-border paperless trade occurs despite lack of widely-accepted rules on mutual recognition are dealt with in J.D. Gregory, "Mutual Recognition of Methods of Authentication", online: https://www.slaw.ca/2020/05/19/mutual-recognition-of-methods-of-authentication/

[17] The agreement is described, with some supporting documents, online: https://www.digitalizetrade.org/projects/korea-netherlands-e-phyto-certificate-project

[18] MLES article 10; MLETR article X; MLIT article(s) Y.

DRAFT

as one's own. Consider the supports for that authentication. Consult with interests, national and otherwise, that may be affected by that legal effect to understand the risks and limits of the policy. Different countries will come to different conclusions about similar systems.

See Appendix E for further useful perspectives on the options and challenges of mutual recognition.

IV. Platforms

Another method for dealing with cross-border paperless trade could be seen as a mechanism that relies on or promotes both of the 'traditional' approaches just discussed: harmonization and mutual recognition. There is also an element of 'choice of law', by which parties choose the law that they will be subject to (to the extent that this is allowed under the law applicable to them). That method is reliance on e-commerce or trading platforms.

A platform in this sense is an online 'place' created by software (though probably residing on particular hardware) that allows participants in the platform to load data and to interact with other participants. There are many examples of public commercial platforms, such as Alibaba.com or Amazon.com. Other designs are possible, though. A business could use a platform to share data or documents with its customers (e.g. DHL.com or other courier services), other businesses or with regulators of the business, or all of these classes. A business could share evidence of compliance with legal requirements – such as the possession of a transit carnet, or a certificate of origin of goods.

So long as access to the platform was carefully managed and data or documents shared on it were of known origin and secure against tampering, it could be a productive way to make information usable across borders and in several legal systems. One would not need to invent new forms of document or new purposes for data, but just have a method of sharing those that one is already familiar with. Distributed ledger technologies (blockchains) could be one of possibilities for secure management of documents that would need to be further discussed and investigated.[19]

Commercial parties might choose the platform for safe communications, assuming that the 'law of the platform' could accommodate all of them (and, as mentioned, assuming that the law governing their operations permitted such a choice of law. How much 'party autonomy' do they have?) And the platforms could be designed to satisfy the legal requirements of any state it operated in or in which users originated. Users of the platform would agree on becoming members to accept the legal consequences of joining, e.g. accepting the reliability of data posted to the platform and agreeing to give legal effect to them as required.

Systems set up under conventions for the exchange or communication of digital documents, such as that contemplated in the e-TIR convention and other transport-related instruments, would in effect operate as platforms, and the law of platforms could be broadly enough drafted to apply to them.

Platforms for these purposes could be established and run by government agencies if they were widely trusted in matters of information security and data governance (a 'top down', G2B system), or they could be private enterprises, subject to the same need to earn and keep the trust of potential users (a 'bottom up',

[19] At this stage the Guide is canvassing potential supports for cross-border paperless trade. Blockchains – or distributed ledger technologies – often rely for their credibility on the use of digital signatures, which in turn need a trusted public key infrastructure: reliable certification service providers, secure technology – that do not now exist across borders in much of the world. Deciding how to support wide use of blockchains to build trust is beyond the scope of this Guide.

DRAFT

B2B system) as any other commercial enterprise. They may also be subject to law in places where they operate to ensure their reliability, accessibility and fair treatment of all interests engaging with them. Article 6 of the Law about Electronic Commerce of the Kyrgyzstan is only one example.[20]

There could also be G2G platforms where government compliance with standards or conventions from one country to the next is being asserted or measured. A platform for communicating official phytosanitary certificates under plant safety conventions might be a G2G operation, for example.

Considerable questions of data security and data confidentiality need to be resolved, but in principle they should be manageable. A trusted platform could be very useful to many interests, state and private. Participating on such a platform might give one an 'ex ante' reliability[21]: just being there shows that one is reliable (but someone would have to enforce the criteria for participation, unless the technology required to participate was secure enough to avoid doubt on that question.) And the people in charge, and thus the perceived reliability of the system, may change over time.

Whether one could overlay the platform concept with some of the other concepts here, like harmonization or mutual recognition, remains to be seen. The 'choice of law' could be reflected in the decision of private actors/businesspeople to use the platform at all, and which platform they chose. It would be an expression of 'party autonomy' that is protected by many e-communications texts. Whose platform, under whose legislated or contractual rules, is the most credible as the 'place' for cross-border transactions? A government could presumably impose the use of a platform it considered to be trustworthy, at least on entities within its sovereignty – but not beyond.

Some questions of operational trust are worth noting, as well. Governments and private platform operators may both be tempted to take advantage of their central position to make the platform that they establish serve their own priorities, or to extract commercially useful data from other platform users, or otherwise not be a neutral administrator. Recently a much-publicized commercial shipping platform, TradeLens, failed despite being proposed and operated by Maersk, a very large shipping company, and Microsoft. TradeLens was to operate on the blockchain, which some people found cumbersome despite its theoretical security. An important reason for its failure to attract enough other traders to be commercially viable was a lack of trust that Maersk would not abuse its position as the organizer of the platform, in handling the data of competitors.

Likewise, not all governments may trust all other governments, if a platform were to be run by one of them. Nations compete as well as co-operate, and trade is one of the areas of competition. In theory, everyone using the same platform would operate under its rules, which would harmonize the legal relations effectively. It is worth developing the concept and operation of platforms. If their challenges can be resolved, they offer a number of attractive solutions to other problems. At present, however, there does not seem to be an operating platform that meets all these requirements.

IMPLEMENTATION STRATEGY: Develop or encourage the development of a national platform for cross-border trade of all kinds. Allow participation by foreign interests to the extent that the authentication of their data meets national standards of reliability. Be open to reciprocal agreements with trading partners on such recognition. Ensure by law the fair operation of the platform for all users, pubic and private, domestic and foreign.

---

[20] Kyrgyzstan, Law about Electronic Commerce, online: https://cis-legislation.com/document.fwx?rgn=136937

[21] "Ex ante" standards are applied before the use of a document or an authentication method in a transaction, often by compliance with an established rule or by certification by an established authority. "Ex post" standards are applied after use, in the event of a dispute over compliance or over authentication, for example.

DRAFT

Although some of platforms may be an effective place for exchanging legal documents, some experts doubt that such a mechanism is well suited for G2G or G2B exchanges of electronic documents. Others would argue that governments can bind themselves to participate fairly and effectively in platforms according to platform rules if they choose to do so. In any event, governance and governments are key challenges for platforms that would resolve data conflicts.

It may be helpful to reflect on the role of national single window (NSW) facilities in the context of platforms. A national single window is involved in imports and exports. Can a single window be compatible with platforms? Is a Single Window a kind of platform for this purpose? (By definition a national single window is not a cross-border platform, but its function is to facilitate cross-border trade. It is a repository of and way-station for documents/data crossing a border.) A platform would not normally 'compete' with a single window, since the SW has a governmental and regulatory role that a general trade platform does not.

To date, the ability of national single windows to harmonize electronically with other national single windows has been limited, even between states with advanced technology. Is that a cautionary lesson for platforms' ambitions, on the limits of international digital trust? Or are NSWs trying to do something different from what platforms would be expecting?

One may consider the EU experience of integrating national single window environments through a certificates exchange system (Regulation 2022/2399 of 23.11.2022). How much authority must a regional or transnational body have over its members to enforce consistency? How common is that in the world? Perhaps a transnational network of single windows could be a kind of platform.

According to an APEC Policy Brief published in 2024, four areas of deficiency hold back the development of trading platforms: a lack of:

- acceptance and enforceability of electronic documents (key element: MLETR)
- appropriate interoperability standards and practices (data interoperability and technical interoperability)
- commercial viability (mainly for private platforms) (cost of meeting standards of multiple platforms, cost of using blockchain for data security can keep number of members of the platform too low to survive.)
- digital skills and infrastructure (personal skills and broadband capacity).[22]

The remedies the document suggests are:

- law reform consistent with MLETR and in the meantime, possibly rely on private rule-books for members of the platforms, such as the Bolero Rulebook for electronic bills of lading in that system.
- Adopt UN model laws and applicable standards from toolkits, trade associations for inter-industry cooperation. Technology neutrality is crucial. Reconsider use of (expensive) blockchain technology. Do not multiply platforms, which are costly to build and run. Attract diverse customers.
- Work on several fronts: skills, upgrade infrastructure, harmonize laws.

[22] Wirjo, Bayhaqi, Oh, "Digitalizing Trade: The Role of Paperless Platforms", APEC Policy Brief 59 (March 2024), online:

DRAFT

V. International and domestic laws

V. A. Impact of international laws and regulations on domestic laws

It is clear that the CPTA aims at integrating Parties into the international commercial legal order, one might say, "from both sides": countries must be aware of the international legal environment in which they are operating, but they must also "endeavour" to take steps to adopt legislation and otherwise harmonize their legal systems with relevant international regimes.

Normally rules of international law would not affect a state unless it consented in some way, at some level, to be affected. We will look in a moment at the ways it can consent.

It may be possible, however, for a private party to opt into an international legal regime by choosing another country's law to apply to its own transaction. If that other country is a party to a convention, or has implemented a model law, or conforms to practices under bilateral agreements, then the rules of those instruments will apply to the party choosing that law. In some instances, traditional acceptance of parties' "choice of law" would allow such result, without having to refer to a convention.

A state that has implemented the UNCITRAL Model Law on Electronic Signatures will probably have provided that it will recognize foreign electronic signatures if they are created in a way substantially as reliable as its own. In this way, such a foreign signature or foreign documents generally could be given legal effect without any express agreement between the two countries and without any special legislation.

There may be ways in which adopting an international legal regime – whether by ratifying a convention, implementing a model law or just changing one's own legislation to match the foreign regime – will affect other domestic laws or relationships in unanticipated ways. Such effects are a matter for the next section of this guide, and in any event suggest broader and more careful policy analysis before adopting the international regime. Unintended effects are hard to avoid but not usually desirable.

An arguable exception to that principle is the rule in the UN Electronic Communications Convention (article 20) that its principles of validating electronic documents and signatures should be read as applying not just to international contracts but to contracts subject to any other convention to which the member is a party. This offers an excellent opportunity to expand the validity of digital documents in a legally consistent way, with little risk. (Studies of the potential impact of such wholesale extensions of legal permissions show almost no drawbacks to making them. The ECC permits parties to adjust the application of its rules over time.)

V. B. Aligning the domestic framework with selected international frameworks

There is no single way in which an international legal rule may apply to a state that seeks its application. Sometimes, in some places, just acceding to a convention will make that convention legally effective. At other times or in other places, a convention will also need to be implemented by some legal process – legislation, a regulation, a decree. Moreover, some conventions or other instruments may apply on their face only to international transactions or international relations, while others will have domestic effect. In many cases, "adding" a domestic effect requires its own decision and legislation.

For example, it is clear that the Convention on the International Sale of Goods (CISG) allows for contracts made via electronic communications (since nothing in its text restricts such contracts to those made on paper.) A member state of the CISG will – by the terms of the convention – apply that law to all contracts

DRAFT

between parties in contracting states (and others in some cases), unless the transacting parties opt out of the convention. Therefore, a transacting party in a state that has no law allowing e-contracts can nonetheless make such contracts with foreign trading partners in CISG-member countries.

A state that becomes a party to the ECC will by that fact authorize international e-contracts as well, with more information than in the CISG about how they are to be made. Depending on the state, acceding to the ECC may change the law on such contracts without domestic implementing legislation. A few states have expressly made the ECC their domestic law as well as their law for international contracts. Singapore amended its Electronic Transactions Act to that effect in 2010.[23]

In another example, the protocol to the CMR Convention on road transport provides criteria for valid electronic signatures and documents, and they may have effect even in the absence of positive confirmation in states party to the convention. Other transport conventions may need domestic legislation to ensure cross-border recognition of the signatures that they require or of the prescribed consignment certificates in general.

The Revised Kyoto Convention on Customs Procedures is similar – it requires member states to permit the filing of goods declarations and supporting documents by electronic means. (On the other hand, it may simply require that domestic legislation be enacted to have that effect.) The WTO Trade Facilitation Agreement is similar: member states must adopt measures to deal with commercial documents electronically, though less developed countries have a more forgiving timetable for such measures.

Each state will have to decide on its own priorities. Becoming a member of the CPTA obliges a state to "endeavour" to align its laws with international standards and adopt international texts, but choosing how to do that, and where to start, still requires analysis. In part, the exercise will depend on the current state of domestic laws – do they adequately support digital documents? Are they already based on international models, e.g. MLEC, MLES? The basic UNCITRAL legal framework? The WTO?

The Legal and Technical Readiness Checklists on Cross-border Paperless Trade will enable countries to conduct assessments of legal and technical readiness, leading to recommendations and individual actions plans. They could assist countries in assessing the current situation in this regard. [24] The resource also includes a Legal Guide, to understand the principles and the legislative options.[25]

Some of the questions include how well established these laws are. What are the expectations of businesses and regulators? Is there already a national single window in place? Is it based on international standards like the UN/CEFACT Recommendations or the ASEAN model[26]? Alignment of priorities will also depend on the current state of international laws. One needs to look at specific international rules – this is not a generic question, one size does not fit all.

One approach is to ask whether international permissions for digital communications in general, or in particular instruments, are consistent with domestic law. Amendments to implement international rules may be less disruptive or difficult if there are few differences in outcome. And international good practices may influence more paper-based domestic customs, if an international regime is adopted for cross-border trade.

[23] Most Australian states did likewise, though Australia has not yet acceded to the ECC itself. Canada has uniform legislation for this purpose as well, but to date it has been implemented in only two provinces.
[24] Information about the readiness assessments is avaialbe at : https://readiness.digitalizetrade.org/
[25] https://readiness.digitalizetrade.org/legal-guide
[26] ASEAN Single Window, online: https://asean.org/our-communities/economic-community/asean-single-window/

DRAFT

Another 'test' is the state of international or digital commerce laws in a country's principal trading partners. It would be a fair method of setting priorities to harmonize with the legal regimes that will have the strongest impact on one's own trade. Which borders most need to be opened, and which will best be opened by increasing the ability to do paperless trade?

In any event, it is worth trying to make domestic law conform to international good practices unless there is a good local public policy reason not to do so. What might some of those reasons be?

- It is possible that businesses or other potentially affected actors may not be technologically ready to operate in a digital world, or with digital competition from abroad.

- Moreover, perhaps potential users of electronic documents, or transacting parties, or regulators will not be comfortable evaluating the reliability of e-documents or of methods to achieve reliability. They may need their state to develop assistive regulations or standards to help them know what to trust and for suppliers, how to create the trusted document or system.

- In short, capacity building may be needed for any or all of the technical, legal and business practice elements of the economy.

While it is possible to ask whether a country should "start" by reforming domestic laws to enable paperless commerce or by harmonizing with international regimes, this question arguably comes too late. Almost all countries have some law by now to permit some e-commerce, and almost all have some way of effectively doing some trading across borders without paper. Nobody is just "starting".

A more subtle analysis is needed, to start with the reforms with the greatest impact – which could mean the fastest to be implemented or the ones with the greatest financial benefit. The results of such an analysis may be different in different countries.

One could also choose the international instruments or regimes that are the most widely adopted, globally or regionally, or the ones with the least controversy over how to implement them. These would likely be the ones with the most documentation about how to implement them and expertise on resolving challenges in implementation. (Many, including especially UNCITRAL instruments, are accompanied by official guides to enactment or explanatory notes. Analytical literature is also widely available on the best-established regimes.)

Four sources of guidance should be noted as particularly valuable, in their commitment to maximizing digitalization of trade and in the thoroughness of their analysis of business and legal considerations.

1. WTO/ESCAP/UNCITRAL, "Cross-border Paperless Trade Toolkit" (2022) notably chapter 2, "Enabling a conducive legal framework".[27]
2. International Chamber of Commerce, "Digital Standards Initiative." This is an online suite of resources and considerations of business and regulatory issues to be dealt with in promoting cross-border paperless trade. It contains much valuable material to help governments and businesses prepare for paperless trade.[28]

[27] Available at: https://www.wto.org/english/res_e/booksp_e/02_paperlesst_2_enabling_a_conducive_legal_framework_e.pdf

[28] Available at: https://www.dsi.iccwbo.org/our-work .

DRAFT

3. UNECE/Centre for Trade Facilitation and e-Business (CEFACT). This body has been the source of practical recommendations and standards for paperless trade for many years.[29]
4. WTO Joint Standards Initiative unites 90 countries in the search for acceptable standards for reliable, trustworthy cross-border trade. Much of the work is now complete.[30]

VI. Conclusion

Creating the legal foundation for cross-border paperless trade involves attention to one's domestic framework – is paperless trade properly supported in law at home? The UNCITRAL Model Laws mentioned in this Guide are a very firm foundation for that. Good practice is to give the maximum flexibility to private parties to use the technology they are comfortable with, i.e. that they trust, to make valid and binding agreements. Just how much flexibility may depend on how knowledgeable businesses are about information technology, including estimates of security and reliability. It is common for countries to require more demanding security for digital communications with state authorities, since the consequences of mistake or fraud may be greater.

For this purpose, provisions about acceptable technology may come into consideration.

When one crosses national borders, similar factors need to be considered. How confident can a business or a government be in the reliability of digital data from outside the country? The answer is both legal and technological. The UNCITRAL principle is sound, of giving legal effect to data produced by methods as reliable as those one accepts at home. Deciding what methods are similarly reliable may require describing in detail the technology used to carry them out.

There are many sources of legal rules for cross-border paperless trade, and the CPTA contemplates reference to them, as described in this Guide. The legal rules must rest on technology in which one has confidence. Many standards exist or are in development for such technology.

Some day there may be a thorough international agreement describing reliable digital technology and how to use it. Pending such an agreement, countries may find legal security through other forms of agreement:

- trade agreements that provide trade facilitation, sometimes based on technical standards;
- mutual recognition agreements with operational details of supportive technology;
- standards for membership in trade platforms that require participants to be technologically secure and commercially honorable as well.

Countries new to cross-border paperless trade will probably choose to focus their legal efforts, and their analysis of the relevant technology, in priority on the places across their border where they have the greatest economic benefit from increasing trade – possibly with considerations of cultural, political and social ties as well.

There are no perfect answers. No one has cross-border paperless trade at 100%. Laws are still being developed – the MLIT was adopted in 2024 – and standards are being formulated all the time. Still, it is hoped that the Guide could help countries head in the right direction for their participation in digital trade.

[29] Available at: https://unece.org/trade/uncefact and https://unece.org/trade/uncefact/tf_recommendations

[30] Joint Statement Initiative on e-commerce (December 2023): https://www.meti.go.jp/english/press/2023/1220_001.html

DRAFT

APPENDICES

Appendix A: Representative international agreements and standards affecting cross-border paperless trade

(i) Instruments about electronic communications

a. Conventions
   i. UN Convention on the Use of Electronic Documents in International Contracts (Electronic Communications Convention) (ECC)
   ii. UN Convention of the Facilitation of Cross-Border Paperless Trade in Asia and the Pacific (CPTA)
   iii. World Trade Organization Trade Facilitation Agreement (TFA)
   iv. World Customs Organization Revised Kyoto Convention on Customs Procedures
   v. International Convention on the Harmonization of Frontier Controls of Goods
   vi. Council of Europe (Budapest) Cybercrime Convention
   vii. Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data

b. Model Laws
   i. UNCITRAL Model Law on Electronic Commerce (MLEC)
   ii. UNCITRAL Model Law on Electronic Signatures (MLES)
   iii. UNCITRAL Model Law on Electronic Transferable Records (MLETR)
   iv. UNCITRAL Model Law on Identity Management and Trust Services (MLIT)

c. Standards
   i. From public bodies
      1. UN/CEFACT – Legal Framework for international trade single window, Recommendation 35
      2. UN/CEFACT – Authentication of Trade Documents, Recommendation 14
      3. UN/CEFACT – Single Window, Recommendation 33
      4. UN/CEFACT – Single Window Interoperability, Recommendation 36
      5. World Trade Organization – Joint Standards Initiative (forthcoming)
      6. ASEAN - Protocol on the ASEAN Single Window
   ii. From private bodies
      1. International Chamber of Commerce, Uniform Customs and Practice (UCP)
      2. International Standards Organisation (ISO), computer security standards (and many others)
         a. For example, ISO/IEC TR 14516, ITU-T recommendation X.842 Information Technology – Security techniques – Guidelines for the use and management of trusted third party services

(ii) Instruments about sectors of the economy

a. Conventions
   i. Convention on the International Sale of Goods (CISG)
   ii. Convention on the contract for the international carriage of goods by road with protocol on electronic certificates (CMR Convention)
   iii. Convention on Air Transport – Montreal Convention – IATA – air waybills
   iv. Convention on Rail Transport (CIM/SGMS) – eCIM consignment certificates

DRAFT

v. Convention on Facilitation of International Maritime Traffic (annex)
vi. Customs Convention on the International Transport of Goods under Cover of TIR Carnets (TIR) – eTIR rules
vii. Convention on the Carriage of goods by Sea (Rotterdam Rules)(Hamburg Rules)
viii. Convention on the Facilitation of International Maritime Traffic, 1965, as amended (the FAL Convention).
ix. International Plant Protection Convention (IPPC - Phytosanitary measures)
x. Convention on the International Trade in Endangered Species (CITES Convention)

b. Standards and guidelines [*see Appendix B, below*]
   i. UN Guideline on Consumer Protection
   ii. Organization on Economic Cooperation and Development (OECD): Guidelines on the Protection of Privacy and Transborder Data Flows
   iii. Trade standards of various sorts prepared by ICC and WTO: https://www.dsi.iccwbo.org/our-work and https://www.dsi.iccwbo.org/_files/ugd/8e49a6_2d93b2f219cf404ab91bafd028e31fcc.pdf Key Trade Documents and Data Elements: Digital Standards Analysis and Recommendations (2023)

(iii) Trade Agreements

i. Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)
ii. Digital Economy Partnership Agreement (DEPA)
iii. Regional Comprehensive Economic Partnership (RCEP)
iv. Japan-UK agreement, Japan-US agreement focusing (in part) on Data Free Flow & Trust ideas

ESCAP data base of trade agreements – Legal TINA – Trade Information and Negotiation Advisor, online: https://legal.tina.trade/app/start.

DRAFT

Appendix B: Standards

There needs to be mention, possibly in detail, of the active discussion of reliance on international standards, either existing or to be developed, as a kind of international legal regime that trading partners would adhere to (more or less voluntarily, or perhaps national laws would require it.) Among the sources of such discussions going on now – documents from 2023, 2024 - are:

- The G7/OECD/WEF work on Data Free Flow & Trust
    - Many business interests writing on this topic focus on data localization rules more than the present project needs to worry about.
    - The project touches mainly on commercial data.
- The WTO joint digital statement initiative (JSI)
- International Chamber of Commerce Digital Standards Initiative, Industry Advisory Board (publications of trade document standards)
    - WTO & ICC "Standards Toolkit for Cross-border Paperless Trade: Accelerating Trade Digitalization through the Use of Standards" (2022)
- The World Bank advocacy for a 'platform of platforms' approach
- UN/ECE/CEFACT standards for digital trade data (often mentioned)
- The WCO (World Customs Organization) Data Model
- ESCAP technology readiness checklist and guide and country reports and action plans

Singapore Infocomm Media Development Authority, TradeTrust program. Many of these documents suggest that there is currently no consensus on the content of such standards, except in a general way, and that more work is needed. This suggests that the present Guide may not be able to be definitive in its recommendations!

Many of the documents raise privacy and confidentiality issues as important and unresolved.

Few if any of these 'trust' and 'data free flow' discussions talk about computer security, e.g. authentication, digital signatures, and the like. Sometimes they seem to take for granted that some such system will be needed, and other times they seem to think that authentication will not be an issue.

Many of the standards proposed to harmonize the international flow of data appear to be technical rather than legal. For example, the ESCAP working paper from 2023 by Aleksei Bondarenko on 'advancing the digitalization of trade supporting documents in the EAEU' proposes several possible models of authenticating documents, but usually says 'legal base needs to be adjusted' – meaning that the legal status of any of them remains to be determined.

However, it is difficult to frame a law to validate them without knowing clearly what they are and how they work – unless compliance is entirely a decision of parties to a transaction. If there is a public policy element to them, then a legal basis must be precise and detailed.

An argument can be made that such standards would apply well to platforms and could be adopted voluntarily by users of the platform (or imposed on the users of the platform by the owners/operators of the platform.)

DRAFT

Appendix C: Paperless trade commitments in trade agreements involving more than three ESCAP member States and the CPTA Parties[31]

DRAFT

[31] This appendix is prepared by Runqiu Du, consultant, ESCAP.

Commitments on cross-border paperless trade	ASW Agreement (2005)	WTO TFA (2017)	PACER PLUS (2017)	CPTPP (2018)	RCEP (2020)	DEPA (2020)	CPTA (2016)
Making trade administration documents available to the public in electronic form	NA	shall endeavour	NA	shall endeavour	shall endeavour	mandatory	NA
Acceptance of trade-related data and documents in electronic form	mandatory	shall endeavour	NA*	shall endeavour	shall endeavour	mandatory	shall endeavour
Enabling domestic legal environment for paperless trade	NA	NA	NA	NA	NA	NA	shall endeavour
Developing systems for submission/ exchange of trade-related data and documents in electronic form	mandatory	NA	Should	mandatory	NA	shall endeavour	shall endeavour
Allowing cross-border transfer of information by electronic means	NA	NA	NA	mandatory	mandatory**	mandatory*	NA
Mutual recognition of trade-related data and documents in electronic form	NA	NA	NA	NA	NA	NA	mandatory*#
Harmonization of standards for trade-related data and documents in electronic form	mandatory	encouraged	NA	shall endeavour	encouraged	encouraged	shall endeavour
Increasing interoperability of data/document exchange systems	mandatory	NA	NA	NA	NA	shall endeavour	encouraged
Development of national single-window systems	mandatory	shall endeavour	NA	shall endeavour	NA	mandatory	encouraged
Development of integrated regional single-window systems	mandatory	NA	NA	NA	NA	NA	NA

DRAFT

'Should' and 'Shall endeavour' are not binding language in trade agreements but usually indicating stronger commitment than encouragement.
*PECAR PLUS only requires the acceptance of electronic documents covering all goods contained in a shipment to expedite the clearance.

**RCEP and DEPA provide carve-out to the obligation.
*#CPTA only requires mutual recognition of documents of "substantially equivalent level of reliability", which has to be separately negotiated and determined; actual operationalization exchange of documents is subject to separate bilateral/multilateral arrangements

KEY: *WTO Agreement on Trade Facilitation (TFA), Comprehensive and Progressive Agreement for Trans-Pacific Partnership Agreement (CPTPP) and the Regional Comprehensive Economic Partnership Agreement (RCEP), Digital Economy Partnership Agreement (DEPA), Agreement to Establish and Implement the ASEAN Single Window (ASW Agreement), the Pacific Agreement on Closer Economic Relations Plus (PACER PLUS)*
Source: ESCAP, UNNExT Working paper No.09, 2024

DRAFT

Appendix D: The need for global trusted environment to support cross-border paperless Trade (Including mutual recognition of digital data and documents) [32]

It can be argued that a key legal obstacle that hinders cross-border exchange of electronic documents and data in the context of trade is the lack of international legal frameworks that address the problem of legal recognition of electronic documents and data produced in one State oin the territory of another State. This problem has arguably been solved for public documents on paper, by the Hague Apostille Convention 1961. However, there is no international agreement which recognizes the legal validity of electronic documents and data at the international level rather than national or regional levels. The eIDAS regulation within the European Union goes furthest in this direction.

The legal problem of cross-border mutual recognition of electronic documents and data is closely connected with the technical problem of applying certain technological standards (including cryptographic algorithms and features of the implementation of the national public key infrastructure). In order for States to apply their applicable technological standards in the process of cross-border electronic interaction, they need an international legal framework securing the right of each State to apply such technological standards that allow them to preserve their digital sovereignty, i.e to build an international trust space, allowing States to apply different crypto-mechanisms, so long as they are similarly reliable. In order to ensure effective cross-border electronic interaction within the trusted trade environment (TTE), States should **establish** special legal entities – Trusted Third Parties (TTP). A TTP is, in fact, an operator in one State who interacts with similar operators in other States ensuring cross-border legalization for electronic documents and data. (A TTP is a 'third party', i.e. not the signer or authenticator of the data or document in question and not the reader/addressee/relying party. The TTP is independent of both of these.) At the same time, the procedure for governmental or intergovernmental accreditation of TTPs should be defined within their own jurisdiction or country to allow TTPs to obtain official status and make TTPs' activities controlled by a governmental or intergovernmental regulatory body.[33]

Technical conditions for the TTE functioning include technological and organizational requirements for certain aspects of cross-border exchange of electronic documents and data which are aimed to harmonize national TTE segments. The technical conditions may be adopted by an advisory body which Parties may wish to establish on a parity basis. Who appoints such a body and who constitutes it is beyond the scope of this discussion. It has been suggested that appointments are on a 'parity basis', so all participating countries would have equal representation. (While the body may be 'advisory', its advice will need to be given international legal effect to resolve questions of harmonization and mutual recognition and to secure the TTE.)

Moreover, in order to build transboundary trust space between different actors, normally in different countries, an agreement should be adopted to regulate relations between national TTPs in the process of cross-border exchange of electronic documents and data. Such an agreement, or possibly a network of interlocking agreements, may cover, among other issues, 'private law' matters like the basis and limits of mutual liability of TTPs for improper performance of verifying the authenticity of electronic documents

[32] This text is adapted from contributions from Sergei Kiryushkin, Alexander Plakhov, T. Shashikhina, O. Al.Vinichenko, and A.A. Dukarev

[33] Technical standards for TTPs are set out by the International Telecommunications Union (ITU) in its standard X.842, online: https://www.itu.int/rec/T-REC-X.842-200010-I

DRAFT

and the standards of reliable provision of trust services in cross-border electronic interaction, as well as the procedure for resolving disputes or differences in interpretation between TTPs.

….

Adoption of such an international treaty within ESCAP member States would allow parties to define: a) basic principles of cross-border electronic interaction within the TTE; b) legal status of TTPs, including basis and limits of their liability for damage caused to third parties as a result of improper performance of verifying the authenticity of electronic documents; c) requirements for an equivalent level of reliability (levels of assurance).; d) provisions on compliance with international information security standards, including with regard to protection of personal data and trade secrets based on current national and international legal instruments ; e) the legal status and requirements for a certification authority (in some formulations, a root certification authority) which is designated to issue electronic signature certificates to TTPs to ensure the interaction of TTPs with each other and with their customers/subscribers.

Experts noted that technical conditions for the TTE functioning may be adopted by an advisory body and then made law by the usual methods of international rule-making.

……

In order to create a trusted system, States should be sure that there is a reason to believe that (1) means of communication used by participants in the process of cross-border exchange of electronic documents and data are consistent with a "substantially equivalent level of reliability" (based on the terminology of the UNCITRAL Model Law on Electronic Signatures and CPTA), (2) these means are used by participants in good faith, (3) and participants counteract the unfair use of these means. (Standards of conduct for TTPs are outlined in MLES articles 6, 9 and 10.) The technical conditions for the TTE functioning should **include** ensuring an equivalent level of reliability in the process of cross-border exchanges of electronic documents and data as specified in Article 8 of CPTA.

The organizational conditions for the TTE functioning may include the establishment of national TTPs in each State and, if needed, a parity-based "advisory" body which is authorized 1) to make decisions aimed at ensuring the TTE functioning; and 2) to audit the achievement of an equivalent level of reliability of national TTE segments.

The legal conditions for the TTE functioning may include articulation of a system of legal relations arising in the process of cross-border electronic interaction between its participants. These legal relations may consist of mutual rights and obligations of the participants which are aimed at organizing reliable and secure exchange of electronic documents and data at all stages of interaction. The legal conditions may be enshrined in an international agreement.

The proposed trust system does not imply the creation of uniform technological rules for everyone. The trust system is built on the principle of digital sovereignty. No one evaluates the technological standards of states; the parties only conduct an audit of existing standards to understand how the state will participate in the cross-border space of trust.

There is no need to build a space of trust if any uniform technological standards are adopted.

DRAFT

Appendix E: Discussion paper: Basic elements of legal recognition of electronic data and documents in paperless trade facilitation[34]

1. Background

The purpose of this paper is to provide a basis for validation of legal recognition mechanisms to implement article 8 of the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (CPTA).

> *Original reproduces Article 8, CPTA, and the full Explanatory Note for the article.*

2. The scope of article 8 CPTA

Under its terms, article 8 CPTA foresees a specific mechanism for cross-border legal recognition of trade-related electronic documents and data. The mechanism is based on the conclusion of agreements between States parties to the CPTA that establish legal recognition across borders based on the notion of "substantially equivalent level of reliability". The agreements are negotiated in the framework of the institutional arrangements provided for in the CPTA. It is assumed that the legal recognition should be mutual.

The core content of the agreements is the identification of the standards under which reliability may be considered "substantially equivalent". While the article refers to "trade-related data and documents", the arrangement must deal with the level of reliability of the data contained in a document or otherwise exchanged. **The assurance of a certain level of reliability of data quality presupposes the use of trust services.**

It is therefore not surprising that the explanatory note would refer to the use of a typical trust service, i.e., an electronic signature based on PKI certificate (also known as a "digital signature"), as an example of mutual recognition. For example, two States that wish to exchange electronically trade-related data and documents may decide to rely on the use of PKI certificates to do so for assuring origin and integrity of the information. This could be done in the framework of the CPTA, namely as an implementing activity. The parties would map the respective PKI standards to establish their substantively equivalent level of reliability, be it in absolute terms or with reference to a common global standard (e.g., X.509, or NIST or ETSI reference documents).

Moreover, article 8 CPTA is based on the general principles underpinning the Agreement and listed in article 5 CPTA, namely, legal recognition of the use of electronic means, technology neutrality and functional equivalence – taken from UNCITRAL texts – and promotion of interoperability as well as improving transboundary trust environment. This means that **arrangements implementing article 8 CPTA should not violate those principles.**

[34] This discussion paper is written by Luca Castellani, Legal Officer, UNCITRAL.

DRAFT

In addition, article 8 CPTA does not limit other manners for States parties to the CPTA to give legal recognition to trade-related data and documents through other venues, including in accordance with other international agreements.

All mechanisms for cross-border legal recognition of foreign trade-related data and documents are relevant for the digital trade ecosystem and contribute to its functioning. Hence, **this note provides information on different options for States to engage in cross-border legal recognition and their relevance for CPTA implementation.**

3. Introduction: declarations and the law

Declarations or statements may have legal effects under different branches of the law. For instance, certain statements may be offensive and expose to criminal sanctions. In an opposite scenario, it is necessary to indicate consent to marriage to start a new family. Intentional statements (called communications) are of great importance also in commercial law.

Communications that intentionally triggers legal effects should be explicit and recognisable. However, communications in commercial law may be made in different manners: orally, in writing, electronically, or – under certain conditions – also factually. These are the forms in which a contract may be concluded and performed. In practice, it is desirable to record the communications for future reference, including as evidence in case of dispute. For this reason, important communications are recorded on paper or another durable medium. The information contained in those communications is often structured as a document for easier readability. Sometimes, the intervention of a trusted third party, such as a notary public, gives additional assurance of certain qualities of the paper-based document such as time of creation and subscription, and integrity.

The diffusion of electronic means has enabled fast transmission of information and its analysis and reuse. **It is however also important to maintain the qualities of paper-based documents**, such as providing at least equal assurance of origin and integrity of information. This can be achieved by using trust services, which are defined as "electronic services that provide assurance of data quality".[35]

4. What is legal recognition?

Facts, acts, statements, and documents may have legal consequences. This means that they are legally valid, and have legal effect.

In each jurisdiction, different rules apply to different legal fields. In commercial law, documents may need to contain certain information and to meet certain form requirements to have legal effect. For instance, a cheque should contain the word "cheque" to be legally valid, and a contract for the transfer of interests in real estate usually needs to be drafted in writing, and often with the assistance of a public notary.

Usually, parties to a commercial contract intend to exchange valid documents. In case of dispute on the legal effect of those documents, it is necessary to ask a third party, such as a judge or an arbitrator, to give legal recognition to these documents through a formal declaration of validity.

[35] UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (hereinafter, "MLIT"), article 1(l).

DRAFT

In the field of electronic transactions law, **legal recognition has also a specific meaning as a principle underpinning UNCITRAL texts. That principle indicates that electronic communications may not be denied legal validity or effect only because of their electronic form,** and for that reason it is also known as "principle of non-discrimination against the use of electronic means". This means that electronic transactions have legal validity and effect. Reference to this principle may be found in article 5 CPTA.

5. What is cross-border legal recognition?

Since the requirements for the legal validity of commercial documents may change in each jurisdiction, **it is necessary to find criteria so that documents will have legal effect regardless of the jurisdiction where recognition is sought.** Different techniques are used for paper-based documents.

Some are based on recognising freedom of choice of applicable law. This means that the jurisdiction where recognition is sought will allow the parties to choose the law applicable to the document. The applicable law will determine also the form requirements.

For instance, freedom of choice is common with regard to bills of lading. In the electronic field, ICE Cargo Docs e-bills of lading may be issued under the law of any jurisdiction that enacts the UNCITRAL Model Law on Electronic Transferable Records.[36]

This solution is very convenient as it gives flexibility to the parties at limited or no cost. However, additional legal requirements of mandatory application ("ordre public") may effectively hinder legal recognition: for instance, certain countries require that the bill of lading is drafted in the local language. If the local language is not available, recognition may not be granted.[37]

Another approach to cross-border legal recognition **relies on third parties providing assurance of the existence of certain conditions (e.g., apostille and legalisation)**.[38] In this case, an institutional mechanism often based on a dedicated international agreement (treaty) is set up. However, this solution may be costly and requires each State's specific adhesion, which may be time-consuming.

6. How is the notion of legal recognition relevant to paperless trade facilitation?

Trade facilitation is about sharing information about trade to make trade more efficient. Efficiency may be measured against different standards: time needed for clearance; ability to track the goods during their carriage; reduction of costs; reduction of data input; increased control of the goods traded; reduced environmental impact, etc.

Traditionally, trade-related information has been provided on paper. However, paper-based information-sharing processes are time and resource consuming. Hence, the strong global drive towards paperless trade.

However, paper documents have been used for centuries – they even predate the notion of State. As mentioned, mechanisms have been set up to give legal validity and recognition to documents in the jurisdiction of origin, and to extend their validity abroad. In a nutshell, it may be said that, as far as private

[36] See https://www.essdocs.com/press-room/ice-digital-trade-announces-igpandi-approval-local-law-ebl-solution.
[37] See Jacqueline Tan, Legal Article: Contracts in Indonesia, available at https://www.ukpandi.com/news-and-resources/articles/2018/legal-article-contracts-in-indonesia/
[38] See HCCH, Apostille Convention, at https://www.hcch.net/en/instruments/conventions/specialised-sections/apostille

DRAFT

commercial relations are concerned, parties are free to agree on the law applicable to the document, and on the related requirement, within the limits of mandatory law. However, when it comes to interaction with public entities, usually it is necessary to comply with domestic legal and technical requirements, and to rely on a local physical or legal person to submit the relevant information. This explains historically the rise of service providers such as freight forwarders, customs agents and – more recently – advanced economic operators.

Similarly, online ethe recognition of the legal effects of data and documents may take place at the national or at the international level.

At the national level, a law (no matter how called: law, decree, regulation) usually exists and applies to all kind of data messages, including those relating to trade. The law may contain a statement of the principle of legal recognition (or non-discrimination) similar to that contained in UNCITRAL texts.

However, **legal recognition may also not be granted on a technology neutral basis, but subject to the fulfilment of technical and other requirements.** For instance, certain electronic transactions and signatures law require the use of a national PKI standard for giving legal recognition. This technology-specific solution restricts the types of data messages that may be used. It also poses an obstacle to cross-border recognition.

7. Elements relevant for cross-border legal recognition

Cross-border legal recognition is not an end in itself, but a means to an end, i.e., facilitating electronic transactions across borders. This may explain why **there is no single solution to legal recognition, but a variety of mechanisms are used. These mechanisms often build on practical needs, rather than on legal theory,** and reflect different approaches and priorities.

However, document- and country-specific solutions should not hinder broader recognition of dataflows involving more types of documents and additional countries. In short, **the cross-border legal recognition mechanism should not create data silos or technology-specific requirements.** Each country should therefore find the appropriate solution bearing in mind the desirability of avoiding data silos and workflow fragmentation.

The following overview of elements will help to classify a recognition mechanism. Each element has an option. Each element can be combined with each of the others in both ways, depending on the recognition scheme.

Type of information: may be data or document

Reciprocal recognition: may be unilateral, bilateral, multilateral

Type of transaction: may be B2B or G2G/B2G (sometimes called B/A ‘administration’ i.e. regulators)

Assessment mechanism: may be ex ante – officially approved before its use, either by centralized or decentralized process – or ex post – subject to legal confirmation of its effectiveness after its use.

Legal basis: may be statutory or voluntary

Technology neutrality: may be neutral or technology specific

Legal effect: may be a matter of national law or foreign law.

DRAFT

These terms and distinctions are explained in more detail in what follows.

Type of information

The type of information object of the legal recognition may be data or documents. Documents are made of data organised in a manner to be easily readable by humans.

For the purposes of paperless trade, data refers to computer data and documents refers to commercial or trade-related documents.

Article 2(a) of the UNCITRAL Model Law on Electronic Commerce defines "Data message" as follows:

> *"Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;*

Moreover, article 1(l) of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT) defines "Trust service" as follows;

> *"Trust service" means an electronic service that provides* ***assurance of certain qualities of a data message*** *and includes the methods for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services;*

By using trust services, it is therefore possible to provide assurance of qualities of data messages such as origin and integrity. The MLIT offers a legal blueprint for the recognition of the effects of trust services both at the national and at the international level. In short, by adopting that Model Law it is possible to give legal effect to foreign trust services and, ultimately, legal recognition to the data messages to which those foreign trust services are applied.

Alternatively, it is possible to give legal recognition to foreign documents, i.e., a document that has been issued abroad, or under a foreign law, or that has any other significant foreign element that entails legal consequences.

A document may be issued abroad under a common or uniform legal regime. For instance, a bill of lading may be issued under English law and the Hague-Visby Rules. As noted, the applicable law will normally determine the form requirements. Moreover, a document may be recognised in a jurisdiction other than that of origin provided it does not violate any mandatory rule ("ordre public").

Dedicated legal texts may be set up to facilitate legal recognition of electronic documents. For instance, the e-CMR Protocol has been adopted to give legal recognition to consignment notes in electronic form issued under the CMR treaty. It contains rules to facilitate automatic legal recognition among e-CMR States parties.

The advantage of focusing on documents is easier implementation in a defined community and higher level of legal predictability if a treaty is available. The disadvantage is the possible creation of data silos by adopting industry-specific standards and solutions.

One possible solution is to adopt both approaches. This means relying on recognition of documents whenever the legal context is favourable and at the same time develop a general mechanism for cross-border recognition of trust services. Such general mechanism is a fundamental element of the broader trade ecosystem.

DRAFT

Reciprocity

Article 8 CPTA refers to "mutual recognition". This means that the parties to a cross-border legal recognition arrangement will grant reciprocally legal recognition. The arrangement itself may be bilateral or plurilateral, i.e., involving two or more States. The EU eIDAS Regulation provides an example of plurilateral mechanism for the recognition of foreign data.

Bilateral and multilateral agreements may be negotiated ad hoc. For that reason, it may be expected that they will contain mutual recognition mechanisms.

Certain treaties relevant for legal recognition are open to participation of all States. In that case, legal recognition is based on a multilateral mechanism.

Another option, often adopted in UNCITRAL texts, is to grant unilateral legal recognition. Under this approach, the State sets requirements for the legal recognition of foreign data and documents regardless of whether the State of origin does the same. Such provisions are often contained in national law.

Article 12 of the UNCITRAL Model Law on Electronic Signatures offers an example of unilateral mechanism for the recognition of foreign certificates and electronic signatures that may be included in national law. It reads as follows:

> *1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:*
>
> > *(a) To the geographic location where the certificate is issued or the electronic signature created or used; or*
> >
> > *(b) To the geographic location of the place of business of the issuer or signatory.*
>
> *2. A certificate issued outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate issued in [the enacting State] if it offers a substantially equivalent level of reliability.*
>
> *3. An electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as an electronic signature created or used in [the enacting State] if it offers a substantially equivalent level of reliability.*
>
> *4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.*
>
> *5. Where, notwithstanding paragraphs 2, 3 and 4,* ***parties agree, as between themselves****, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.*

The effect of the above article is to place on the same plane national and foreign electronic signatures and certificates when it comes to assessing their reliability. The treatment of foreign electronic signatures and certificates as national ones effectively gives them legal recognition.

Type of transaction

DRAFT

As mentioned, the type of transaction – or, better said, the type of actor involved – may have a significant impact on legal recognition.

Professional traders may decide the law applicable to their electronic exchanges (B2B), including when it comes to cross-border transactions.

However, when a public entity is involved (B2G and G2G exchanges), special rules may apply. This may happen due to the need to use dedicated facilities that meet higher security standards. Moreover, there may be a desire to reproduce the business processes applicable to paper, including related safeguards. However, this may hinder data submission, force to double data input with increased costs and errors, and ultimately discourage from using the single window facility.

A typical example of B2G transaction is provided by submissions to the single window for customs operations. Data submission may require the use of dedicated software and prior registration, which presupposes a presence in the country where the single window is used. However, it is possible to envisage data transmission between single windows based on common technical standards. It is also possible to envisage data submission validated with the use of a foreign trust services whose effects are recognised in the relevant jurisdiction.

Assessment mechanism

The legal recognition mechanism may rely on an **assessment of equivalence** that takes place before (ex-ante) or after (ex-post) the document or data exchange.

A mechanism ex-ante will recognise all data and documents that meet certain conditions. For instance, under the EU eIDAS Regulation all data that is validated with the use of qualified trust service provider has legal recognition across the European Union and enjoys certain legal presumption.

The ex-ante recognition mechanism may be centralized, i.e., managed by a single central entity. However, it may also be decentralised, i.e., left to various entities. One example of decentralised mechanism is the cross-certification of PKI certificates, which may be carried out by individual certification service providers provided legal requirements are met.

A mechanism ex-post will rely on the decision of a court or of another adjudicating body to confirm that the requirements for legal recognition are met.

Article 12 of the UNCITRAL Model Law on Electronic Signatures (see above) provides an example of ex-post mechanisms by requiring courts to give legal effect to foreign electronic signatures and certificates regardless of their origin.

Moreover, paragraph 5 of that article provides an example of decentralised recognition mechanism by allowing parties to an electronic transaction to agree on the use and legal effect of foreign electronic signatures and certificates.

As usual, ex-ante and ex-post recognition mechanisms may operate jointly under the so-called “two tier” approach. The UNCITRAL MLIT adopts a two-tier approach to legal recognition across borders of trust services (among others).

Legal basis

The legal basis for legal recognition of foreign data and documents may be found in a statute (law or regulation).

DRAFT

Alternatively, the legal basis may be found in the will of the parties, based on the general principle of party autonomy. That principle is limited by the application of mandatory rules.

As mentioned, **a statutory basis is common for transactions involving public entities, while party autonomy may suffice for transactions involving only commercial parties**.

Technology neutrality

The legal recognition mechanism should be technology neutral, in line with the general recommendation for electronic transactions law.

In practice, existing mechanisms may focus on specific documents and technologies, thus violating technology neutrality. This may however hinder dataflows in the broader digital trade ecosystem.

Legal effect

Legal recognition mechanisms may give foreign data and documents the same legal status as national data and documents. This would apply also where the mechanism sets up a specific status for the recognised data and documents (e.g., legal presumptions under the EU eIDAS Regulation).

Alternatively, legal recognition mechanisms may recognise the legal effect that the law of the jurisdiction of origin gives to data and documents.

In that regard, **it may be useful to separate the legal issues related to the electronic nature of the data and documents, and the substantive issues applicable to the document itself. It may be possible that the law of the recognising jurisdictions applies to the former, and the law of the jurisdiction of origin applies to the latter.**

DRAFT