

National Center for Asia Pacific Economic Cooperation  
Working Group on E-Signatures

# **ADVANCING DIGITAL TRANSACTIONS IN APEC: ENHANCING E-SIGNATURES AND DIGITAL SIGNATURES**

---

March 2022



# CONTENTS

ACKNOWLEDGEMENTS.....	3
FOREWORD.....	4
EXECUTIVE SUMMARY.....	5
I. E-SIGNATURES AND DIGITAL SIGNATURES IN APEC: FOUNDATIONS.....	9
II. LEGAL AND REGULATORY FRAMEWORKS IN APEC MEMBER ECONOMIES.....	20
III. BARRIERS TO EFFECTIVE ADOPTION AND USE.....	46
IV. IMPACTS OF COVID-19 AND RESPONSES.....	50
V. RECOMMENDATIONS.....	54
FOOTNOTES.....	61
REFERENCES.....	71





## ACKNOWLEDGEMENTS

The National Center for Asia Pacific Economic Cooperation (NCAPEC) Working Group on E-Signatures would like to thank the following member companies and individuals for their support:

### **Report Sponsors**

AIG

Citi

PayPal

### **Report Authors**

Douglas Arner, Ph.D.

*Kerry Holdings Professor, University of Hong Kong*

Alessandro Di Lullo

*Ph.D. Candidate, University of Hong Kong*

Lucien van Romburg

*Ph.D. Candidate, University of Hong Kong*

### **NCAPEC Working Group on E-Signatures**

Kathryn Tinker

*Regional Manager, Asia Pacific Government Affairs, AIG*

Christine Tam

*Asia Head Legal, Innovation & Technology, AIG*

Richard Lomas

*Senior Vice President, Government Affairs Asia Pacific, Citi*

Steven X. Chan

*Asia-Pacific Head, Government Relations & Public Policy, PayPal*

Amrita Nair

*Government Affairs Specialist, PayPal*

Alex Parle

*Executive Vice President, NCAPEC*

Nicole Vukonich

*Policy Manager, NCAPEC*



## FOREWORD

This project was launched two years ago when the world was beginning to grapple with the uncertainties of the unprecedented COVID-19 pandemic. Business procedures and logistics made an abrupt shift to online formats in order to keep operations moving during pandemic-driven lockdowns. A swift transition to the digital economy became essential to preserving business continuity and economic vitality across the Indo-Pacific region.

Businesses specializing in finance, insurance, and logistics noted fragmented adoption across the APEC economies\* of electronic signatures (e-signatures) and digital signatures practices; the absence of accepted e-signatures/digital signatures protocols in those economies presented a barrier to onboarding new customers and maintaining operations throughout the customer lifecycle when “wet signatures” requiring in-person interactions were not possible during the pandemic.

The goals of this report are to provide an overview of the key terms and international frameworks governing e-signatures, gain a better understanding of the current landscape of e-signatures and digital signatures in APEC economies, identify what measures were adopted during the COVID-19 pandemic, examine relevant cases studies, and provide recommendations. The seven recommendations included in this report offer pragmatic solutions for economies and regulators as they make the transition to a digital economy.

The findings and recommendations of this report will serve as a springboard for advancing wider acceptance and recognition of e-signatures and digital signatures. APEC, as the premier economic and trade forum in the region is an ideal venue in which to discuss this issue. Its non-binding approach makes APEC well-placed to pilot regional recommendations. Business, finance and logistics firms depending on the digital transformation of their processes and procedures require broader acceptance of these tools to keep from being left behind.

A special thank you to U.S. National Center for APEC member companies AIG, Citi, and PayPal for their invaluable support, expertise, and guidance throughout this project. A special thank you also goes to the University of Hong Kong’s Asian Institute of International Financial Law, led by Dr. Douglas Arner, with Alessandro Di Lullo and Lucien Van Romburg. Additional thanks go to the APEC Business Advisory Council (ABAC) members and colleagues who have offered support and advice on this project.

Monica Hardy Whaley  
President  
National Center for APEC

## EXECUTIVE SUMMARY

In an increasingly digitized world, the manner in which electronic commerce (e-commerce), business and finance are conducted globally, particularly on a cross-border basis, is a major focus of attention for both the public and private sector. The COVID-19 global pandemic has dramatically emphasized the role of e-commerce, business and finance, further catalyzing the evolution of what has been described as the 'Fourth Industrial Revolution', the 'digitization of everything'.<sup>[1]</sup> Out of necessity, the COVID-19 global pandemic has, more than ever, highlighted the existing tools available to conduct, effect and process e-commerce, business and finance and ordinary commercial transactions in place of usual in-person business operations. Fundamental to e-commerce, business and finance are electronic signatures (e-signatures) and digital signatures. These are increasingly also coming together with other forms of digital identification and digital identity.

The broader use and adoption of e-signatures and digital signatures across the APEC region and its member economies have the potential to significantly improve the efficiency of both domestic and cross-border transactions. According to the United Nations Economic and Social Commission for Asia and the Pacific, paperless cross-border trade together with the implementation of the WTO Trade Facilitation Agreement could reduce trade costs by more than 25%, potentially decreasing international transaction costs in Asia and the Pacific by US\$ 0.6 trillion annually.<sup>[2]</sup>

In place of the use of traditional handwritten 'wet' signatures, e-signatures are used by parties to indicate their intention, agreement with, and acceptance of the content of an electronic record to which the e-signature is affixed. In the most common form, e-signatures are ordinarily effected through affixing a digitalized version of an individual's signature onto an electronic document. Other examples of technologies used for effecting e-signatures include biometric identification, personal identity numbers (PINs), and online 'I Accept' check boxes. This contrasts with digitized signatures, in which a document is printed, signed, scanned, and sent.

In practice, the term 'e-signature' is often used interchangeably with the term 'digital signature.' There is, however, a marked distinction between the two terms, most notably being the use of cryptography in the case of digital signatures. In the case of digital signatures, the relevant signed information is scrambled into an unreadable format and subsequently decoded for the recipient of the relevant signed information.

The distinction between these two terms is important for identifying the various strategies which have been adopted worldwide, more significantly amongst the APEC member economies, in relation to the use of e-signatures and digital signatures as well as digitized signatures in their respective jurisdictions.

The use of e-signatures and digital signatures is meant to create a number of efficiencies in the manner in which e-commerce and ordinary commercial transactions are conducted. In the first instance, their use can bolster operational efficiency by speeding up commercial processes, such as accounts receivables, accounts payable, and closing deals faster (particularly those effected on a cross-border basis) as e-signatures can be effected very quickly.[3] In addition, their use can bolster transaction transparency through their ability to provide detailed records of e-commerce transaction processes.[4]

All APEC member economies currently have an e-signature and digital signature law in effect. In fact, all APEC member economies have established a legal and regulatory framework governing the adoption, permissibility and use of e-signatures and digital signatures for the purposes of conducting commerce and effecting other legal status matters.

Nonetheless, e-signature and digital signature laws and regulations remain fragmented across APEC member economies as to the definitions of key basic terms and permitted use.

APEC member economies have taken divergent approaches to the manner in which they regulate the use and permissibility of e-signatures and digital signatures in their respective jurisdictions. For example, some have adopted a minimalist approach by giving e-signatures the same status accorded to traditional 'wet' signatures.

Others have taken a more prescriptive approach in prescribing specific methods for affixing e-signatures for them to be legally enforceable. Whilst other APEC member economies have adopted a combination of the aforementioned approaches. These divergent approaches have also influenced how APEC member economies approached defining key terms in their e-signature and digital signature legal and regulatory frameworks, in addition to prescribing specific exceptions to the use thereof based on their individual contexts.

Moreover, in spite of the COVID-19 pandemic's impact on in-person business operations, only a handful of APEC member economies have amended, with varying approaches, their digital signature laws and regulations to take this into account by relaxing their use to effect certain transactions and execute certain documents. This has resulted in further fragmentation of e-signature and digital signature laws and regulations across APEC member economies.

Even where e-signatures and digital signatures use is legally permitted, in a large number of APEC member economies, it still appears to be market practice to require 'physical attendance' and the usage of traditional 'wet signatures', chops and seals when submitting applications, forms, notices, and effect regulatory reporting to the relevant local authority or to effect transactions.

Also, we discover that established e-signing platform service providers, appear to be the favorite e-signing platforms for use to affix e-signatures, particularly to effect transactions on a cross-border basis.

Looking forward, in addition to taking efforts to develop or upgrade interoperable systems amongst APEC member economies, the development of Digital Identification Systems (DIS) would act to reduce reliance on the use of traditional 'wet' signatures and promote broader use and permissibility of e-signatures and digital signatures. DIS are usually described as systems which create and implement processes for validating, enrolling, and authenticating the attributes and credentials that uniquely identify individuals.[5]

More broadly, DIS can be utilized in APEC member economies to broaden access to the formal financial sector to assist individuals, businesses, and governments in receiving and making payments digitally, in executing remittances, and in applying for personal and business loans. DIS could possibly act to increase efficiency, enhance effectiveness, identify new ways of providing financial services, and overall would minimize the risk of false identification.[6] There are, however, several barriers to the successful implementation of DIS tools. These barriers include cost implications as DIS may require significant investment to both develop and maintain as a result of their complex and technical nature.

In spite of these potential barriers, several DIS have been developed, or are in the process of being implemented, in an increasing range of APEC member economies, including Japan, Malaysia, Singapore, and the Republic of Korea.[7] A comprehensive discussion on DIS in the APEC region requires a detailed consideration of the various factors it involves, and ultimately falls outside the specific remit of this report. However, looking forward, further discussion on the use and implementation of DIS in the APEC region offers tremendous potential particularly in conjunction with the use of e-signatures and digital signatures.

### **This report is structured as follows:**

**Section I** provides an overview of the key terms and international frameworks governing e-signatures and digital signatures.

**Section II** summarizes the legal and regulatory frameworks for e-signatures and digital signatures across the various APEC member economies as at the date of this report. In addition, it highlights the different approaches and strategies which have been taken in the regulation of e-signatures and digital signatures worldwide and among APEC member economies.



**Section III** provides a selection of case studies from APEC member economies based on interviews conducted with NCAPEC stakeholders. The selection of case studies illustrates stakeholders' experience with e-signatures and digital signatures in APEC, in particular the barriers which exist in the use and adoption of e-signatures and digital signatures and the best practices which have emerged to deal with such barriers.

**Section IV** considers the impact of COVID-19 and responses in the region.

**Section V** uses the observations gathered from the landscape overview and the selection of case studies and interviews conducted with NCAPEC stakeholders to suggest policy areas that APEC member economies should take into account to facilitate regional cooperation for the broader use and adoption of e-signatures and digital signatures. A brief set of recommendations is provided for APEC leaders and economies as suggestions to effectively adopt and use e-signatures and digital signatures throughout APEC.

# I. E-SIGNATURES AND DIGITAL SIGNATURES IN APEC: FOUNDATIONS

In an ever-increasingly digitized world, the manner in which electronic commerce (e-commerce), business and finance are conducted globally, particularly on a cross-border basis, is a major focus of attention for both the public and private sector. The COVID-19 global pandemic has dramatically emphasized the role of e-commerce, business and finance, further catalyzing the evolution into what has been described as the 'Fourth Industrial Revolution', the 'digitization of everything'.<sup>[8]</sup> Out of necessity, the COVID-19 global pandemic has, now more than ever, highlighted the existing tools available to conduct, effect and process e-commerce, business and finance and ordinary commercial transactions in place of usual in-person business operations. Fundamental to e-commerce, business and finance are electronic signatures (e-signatures) and digital signatures. These are increasingly being supported, supplemented and enabled via other systems of digital identification and digital identity for both individuals and firms.

The broader use and adoption of e-signatures and digital signatures across the APEC region and its member economies have the potential to significantly improve the efficiency of both domestic and cross-border transactions. According to the United Nations Economic and Social Commission for Asia and the Pacific, paperless cross-border trade together with the implementation of the WTO Trade Facilitation Agreement could reduce trade costs by more than 25%, potentially decreasing international transaction costs in Asia and the Pacific by US\$ 0.6 trillion annually.<sup>[9]</sup>

In place of the use of traditional handwritten 'wet' signatures, e-signatures are used by parties to indicate their intention, agreement with and acceptance of the content of an electronic record to which the e-signature is affixed. In the most commonly known form, e-signatures are ordinarily effected through affixing a digitalized version of an individual's signature onto an electronic document. Other examples of technologies used for effecting e-signatures include biometric identification, personal identity numbers (PINs), and online 'I Accept' check boxes. This contrasts with 'digitized signatures,' in which a document is printed, signed, scanned and sent.

In practice, the term 'e-signature' is often used interchangeably with the term 'digital signature' in reference to the same concept. There is, however, a marked distinction between the two terms, most notably being the use of cryptography in the case of digital signatures. In the former case, the relevant signed information is scrambled into an unreadable format and subsequently decoded for the recipient of the relevant signed information.

The distinction between these two terms is important for identifying the various strategies which have been adopted worldwide, more significantly amongst the APEC member economies, in relation to the use of e-signatures and digital signatures as well as digitized signatures in their respective jurisdictions.

The use of e-signatures and digital signatures is meant to create a number of efficiencies in the manner in which e-commerce and ordinary commercial transactions are conducted. In the first instance, their use can bolster operational efficiency by speeding up commercial processes, such as accounts receivables, accounts payable, and closing deals faster (particularly those effected on a cross-border basis) as e-signatures can be effected very quickly.[10] In addition, their use can bolster transaction transparency through their ability to provide detailed records of e-commerce transaction processes. [11]

This section provides a landscape overview of e-signature and digital signatures. The first section provides a glossary of the most commonly used terms with reference to e-signatures and digital signatures. The second section provides an overview of the international framework in place for e-commerce, including the use and permissibility of e-signatures and digital signatures.

## **Basic Concepts**

This section begins with a glossary of the commonly used terms with reference to e-signatures and digital signatures.

This definition list includes some of the most important basic concepts which appear commonly with reference to the e-signature and digital signature legal and regulatory frameworks at an international level and across APEC. The definition list, however, is not exhaustive of the terms associated with and used in reference to e-signatures and digital signatures.

### **(a) Data message**

Data messages refer to information that is generated, received, sent, or stored electronically, optically, or other similar means.[12] Examples of data messages include electronic data interchange, electronic mail, telecopy and telex, and 'voice' when it is used in an automated transaction.[13]

### **(b) Digital authentication**

Digital authentication refers to techniques, processes or systems used with the purpose of identifying persons, confirming authority or to provide surety on the integrity of data and information.[14] It can employ a number of factors including inherence (e.g., biometric information), knowledge (e.g., PINs), and ownership (e.g., possession of OTPs). [15]

**(c) Digital / electronic certificates**

Digital or electronic certificates refer to certificates that are data messages or other records which confirm the linkage between signature creation data and its signatory.[16] They are ordinarily issued by a certification authority who verifies that the public key corresponds to the specific identity and confirms that the signer holds the corresponding private key.

**(d) Digital identity**

Digital identity refers to digital or electronic information used by a computer system to confirm the identity of an agent, usually an individual, corporation or other legal entity, a machine etc.[17] The relevant electronic information operates in the same manner as printed documents such as passports and national IDs to confirm identity.

**(e) Digital signatures**

Digital signatures (advanced signatures) refer to electronic signatures which make use of cryptography to scramble signed information into an unreadable format and decode it for the recipient of the relevant signed information.[18] They are regarded as being more secure than ordinary e-signatures principally through the use of public-key cryptography. [19]

**(f) Electronic communications**

Electronic communications refer to communications (e.g., data messages) transmitted digitally through the use of technology via electric signals or electromagnetic waves.[20] Examples of electronic communications include using a computer to transmit image and sound files, send emails, and conduct video calling.

**(g) Electronic documents and records**

Electronic documents and records refer to information that is generated, received, sent, or stored electronically. Examples of electronic documents and records include email, databases, word processing and spreadsheet, documents, text messages and websites.

**(h) Electronic signatures**

Electronic signatures (standard e-signatures) refer to the process of parties indicating their intention, agreement with and acceptance of the content of an electronic record to which the electronic signature is affixed.[21] E-signatures are most commonly effected through affixing a digitalized version of an individual's signature onto an electronic document.

**(i) Public and private key infrastructure**

Public and private key infrastructure refer to the technology in which algorithmic functions are used to create two mathematically related 'keys' to effect digital signatures. [22] The public key is used to create the digital signature and scramble data into an unreadable format, while the private key verifies the digital signature and returns data into its original format.

**(j) Traditional 'wet' signatures**

Traditional 'wet' signatures (handwritten signatures) are created when individuals mark documents physically, mostly by hand. Ordinarily, this is effected by using ink or wax to write a name (or some other mark) or using a stamp (chop) on a writable surface, most commonly paper. [23] 'Wet' refers to the fact that the ink or wax requires time to dry.

**(k) Qualified electronic signatures**

Qualified electronic signatures refer to digital signatures (which rely on encryption) but also require the signer to make use of a qualified signature creation device (QSCD) which verifies signer's identity.[24] Users are only provided with a QSCD once KYC ('know your customer') processes have been completed. Examples of such devices include cloud-based trust services, smart cards, tokens, etc.

**International Legal and Regulatory Frameworks**

A framework for e-signatures and digital signatures has been developed at an international level principally through the work of the United Nations Commission of International Trade Law (UNCITRAL). Most significantly, this work is represented through the Model Law on Electronic Commerce and its subsequent iterations.[25] In addition to the Model Law on Electronic Commerce, the manner in which e-signatures and digital signatures are regulated at an international law level has been developed by a range of international trade agreements. These trade agreements typically include an e-commerce section containing provisions as to the permissibility and use of e-signatures and digital signatures governing the parties to the agreement. Trade agreements usually reflect the approach of the UNICTRAL Model Law on Electronic Commerce.

At a domestic level, e-signature and digital signature laws and regulations have been adopted throughout APEC. The wide-spread adoption has, however, varied in approach and practical application across the individual APEC member economies. While laws generally permit the use of e-signatures and/or digital signatures, specific regulations among APEC member economies appear to be inconsistent and limiting to various degrees which impacts interoperability and the operation of e-commerce on a cross-border basis.

In addition to these efforts, there have been attempts to develop a coherent and consistent framework for the Asia-Pacific region. This is particularly seen through the work of the United Nations Economic and Social Commission for Asia and the Pacific and its Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific.[26]



This section provides a brief overview of the efforts internationally to establish harmonized and internationally accepted laws and regulations governing e-commerce. These efforts have, in most instances, culminated in the establishment of model laws to assist governments in drafting their own domestic laws. These efforts have varied in their efficacy and there still appears to be varying standards and rules across jurisdictions worldwide, including amongst APEC member economies specifically.

## **International Model Laws**

### **(a) UNCITRAL Model Law on Electronic Commerce**

The Model Law on Electronic Commerce (MLEC), with the addition of Article 5 bis, was adopted in 1998 by the United Nations General Assembly with the principal purpose of facilitating e-commerce and building efficiency in international trade through the provision of a set of internationally accepted standards and rules. In particular, the MLEC established a set of standards and rules which are now widely accepted as the foundational principles for the governance of e-commerce, including:

- functional equivalence;
- non-discrimination between electronic forms of communication and paper-based communications; and
- technological neutrality.

The overall purpose of establishing and developing internationally accepted standards was to remove legal barriers and increase legal certainty for e-commerce at an international level.

A model law, by its nature, is designed to be a model for development and implementation of legislation at the domestic level. Provisions in the domestic framework in turn support both domestic as well as cross-border transactions. A model law is thus fundamentally different from a treaty, which is a form of international law governing interactions between its signatories. Model laws are suggested legal frameworks which do not in themselves have the force of law.

### **(b) UNCITRAL Model Law on Electronic Signatures**

The Model Law on Electronic Signatures (MLES)[27] was adopted in 2001 by the UN General Assembly in alignment with the same set of principles established in the MLEC. However, while the MLEC focused on establishing foundational principles for governing e-transactions internationally, the MLES' rules and standards are focused more specifically on e-signatures. In particular its purpose is the harmonization and establishment of fair legal frameworks governing the use of e-signatures to give certainty to their legal treatment.

In particular, the MLES provides model rules and standards which establish:

- technical reliability requirements for equivalence between e-signatures and traditional 'wet signatures';
- guidelines for the assessment of the duties and liabilities of signatories, relying parties and third parties involved in the signing process; and
- provisions for the recognition of foreign certificates and e-signatures.

### **(c) UNCITRAL Model Law on Electronic Transferable Records**

The Model Law on Electronic Transferable Records (MLETR)[28] was adopted in 2017 by the UN General Assembly and as with previous UNCITRAL texts, it functions to further the foundational principles for governing e-commerce as set out in the MLEC. Its primary purpose is to enable the legal use of electronic equivalents of paper-based transferable documents, both on a cross-border basis and domestically. In the usual course, these paper-based transferable documents entitle the holder thereof to claim performance of the obligations contained therein or to transfer the claim to the performance to another party.

Examples of such documents include:

- bills of exchange;
- bills of lading; and
- promissory notes.

In the context of international trade, electronic equivalents of these transferable documents are particularly important as commercial tools as they improve the speed and security of transactions, permit data reuse and automate specific transactions via 'smart contracts'.

### **(d) United Nations Convention on the Use of Electronic Communications in International Contracts**

The United Nations Convention on the Use of Electronic Communications in International Contracts (ECC)[29] was adopted in 2005 by the UN General Assembly as the first international treaty to govern technology use in e-commerce on a cross-border basis. Its primary purpose is to facilitate the use of e-communications in an international trade context by ensuring e-commerce communications and transactions are as legally enforceable as their paper-based counterparts. Most significantly, the ECC establishes the general principle that communications should not be denied legal validity simply on the ground that they were made in an electronic form.

As with the UNICTRAL texts, the ECC sets out to provide legal certainty on the use of e-communications internationally, in particular by establishing criteria for:

- functional equivalence between e-communications and paper-based documents, including e-authentication methods and handwritten signatures;
- defining the time and place of dispatch and receipt of e-communications; and
- the enforceability and use of contracts entered into by automated message systems.

As at the date of this report, only 18 states are signatories to the ECC, including the APEC member economies of China, Philippines, Republic of Korea, Russia, and Singapore. As a convention, the ECC is a treaty among the signing states, governing their transactions.

## International Trade Agreements

Trade agreements play a significant role in facilitating and furthering the use and permissibility of e-signatures, electronic transactions and electronic authentication. The World Economic Forum (WEF) has reported that more than half of the trade agreements currently in operation contain an e-commerce chapter which set out commitments to the facilitation of e-commerce. Trade agreements are also important instruments which ensure the adoption of the UNCITRAL Model Laws, whether in whole or in part, in requiring parties thereto to create legal and regulatory frameworks based thereon.

In particular, examples of how the UNCITRAL legislative texts have influenced the manner in which trade agreements govern the permissibility of use of e-signatures, e-transactions and e-authentication include trade agreements which:

- require the parties thereto to adopt domestic legislation that is based on the MLEC;
- contain directives requiring the parties thereto to take note of the MLEC's provisions or to adopt domestic legislation based thereon when practicable; and
- require the parties thereto to comply with the MLEC's foundational principles for the governance of e-commerce.

On 20 April 2021, World Trade Organization (WTO) members participating in ongoing e-commerce talks announced that a “clean” negotiating text on the issue of e-signatures and authentication has been finalized.[30] The text is derived from 11 proposals that were presented by WTO members at the start of the process. This initiative aims at ensuring the validity of e-signatures used in online transactions.

According to the OECD-WTO Global Review 2017 Aid for Trade Monitoring Exercise, e-signatures were ranked 4th among the top 10 challenges facing enterprises and consumers when accessing and using internet services.[31] The absence of mutual recognition and standards between countries can add additional costs and unpredictability that can be very challenging for small and medium-sized enterprises (SMEs).

Several WTO members have raised, in the past, the possibility of using the global trade body as an institution to advance greater interoperability of legal rules on electronic transactions and e-signatures, with the goal of boosting e-commerce. For example, in May 2017, the EU circulated a communication to members of the council that highlighted the importance of a WTO outcome on electronic transactions and trust services including e-signatures and electronic contracts.

## **Regional Legal Frameworks**

In addition to international model laws and trade agreements, there are also a range of regional frameworks for e-signatures, digital signatures and in some cases digital identification and identity more broadly.

The work of the European Union is to date the most developed example. In the Asia-Pacific region there have been concerted efforts to develop a cohesive and harmonized approach to regulating e-commerce, which includes directives on the use and permissibility of e-signatures and digital signatures.

### **(a) European Union: eIDAS Regulation**

E-signatures in European Union (EU) are regulated by the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014. This new legal framework, which came into effect in July 2016 for all the Member States, replaced the eSignature Directive of 1999 and paved the way for pan-European harmonization of e-signatures.

The eIDAS Regulation ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU Member States where eIDs are available. Moreover, it creates a European internal market for electronic trust services – namely e-signatures, electronic seals, time stamps, electronic delivery services and website authentication – by ensuring that they work on a cross-border basis and have the same legal status as traditional paper-based processes.

Specifically, when using an electronic identification means and authentication as required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognized in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:

a) the electronic identification means is issued under an eIDs that is included in the list published by the EU Commission;

- b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high; and
- c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.[32]

#### **b) Asia Pacific: Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific**

The Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (FAFCPT) is a UN treaty which was adopted in 2016 following the efforts of more than 25 Asia-Pacific countries. As with the UNCITRAL legislative texts, the FAFCPT sets out a fundamental legal and regulatory framework for facilitating cross-border paperless trade and interoperability of paperless trade systems in the Asia-Pacific region, together with providing a roadmap to achieve such aims. Unlike the UNCITRAL texts, it operates as a treaty rather than as a model for domestic legal implementation.

In particular, its primary objective is to provide generally accepted standards and rules which enable the digitization of trade processes, exchange and mutual recognition of trade-related data and documents in electronic form in the Asia-Pacific region. In setting out these objectives, the overall purpose of the FAFCPT is to increase the transparency and efficiency of international trade and to improve regulatory compliance. The FAFCPT also adopts the foundational principles for governing e-commerce as set out in the MLEC.

As at the date of this report, only 5 states are signatories to the FAFCPT, including only one APEC member economy, China. The Philippines has acceded to the treaty, which in the usual course has the same legal effect as ratification (i.e., indication of the consent to be bound to a treaty).[33]

#### **c) ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN)**

ASEAN is the first regional organization in the Asia-Pacific region to develop a harmonized e-commerce legal and regulatory framework.[34] The ASEAN Vision 2020[35] was published in 1997 with the purpose of furthering the development of science and technology in the Asia-Pacific region. These efforts have resulted largely in the development of non-binding legal and regulatory frameworks such as the e-ASEAN Reference Framework for Electronic Commerce Legal Infrastructure.[36] The purpose of this framework was to assist ASEAN member countries in developing their own e-commerce laws and to facilitate cross-border e-commerce and cross-certification of digital signatures and digital certificates. Its principal aim was to provide a template which ASEAN member countries could use to develop their own e-signature and digital signature laws and regulations.



The framework was developed based on the e-signature and digital signature laws of Singapore, Malaysia and Thailand, amongst others. These e-commerce laws were correspondingly drafted on the basis of the UNCITRAL MLEC and the MLES. The framework sets out important provisions relating to e-commerce including basic concepts and definitions; general principles; scope and legal effects; presumptions; and implementation. In addition, it briefly points out cross-border issues which should be addressed in future studies, including those related to jurisdiction and taxation obstacles.

On a broader policy level, efforts have been made to establish harmonized standards in the Asia-Pacific region, including the e-ASEAN Framework Agreement (Framework Agreement),[37] published in 2012. The purpose of the Framework Agreement was to strengthen and enhance the competitiveness of the ICT (Information. Communication and Technology) sector in ASEAN, facilitate e-commerce growth and development, and to increase investment in online products and services. More recently, the ASEAN Work Programme on Electronic Commerce 2017 – 2025 includes initiatives to modernize the e-commerce legal framework across ASEAN through voluntary peer reviews of ASEAN member countries' e-commerce laws and regulations.[38] This is in alignment with the ASEAN Economic Community Blueprint 2025 (AEC)[39] which contains directives for increased cooperation among ASEAN member countries to facilitate the development of cross-border e-commerce. The AEC Blueprint 2025 includes measures to develop “[i]nteroperable, mutually recognised, secure, reliable and user-friendly e-identification and authorisation (electronic signature) schemes”.[40]

#### **d) ASIA PACIFIC ECONOMIC COOPERATION (APEC)**

In addition to the work of ASEAN, e-commerce has been one of APEC's priorities since 2004[41] leading to a number of initiatives, including those related to the use and permissibility of e-signatures and digital signatures. An action plan in the form of the APEC Blueprint for Action on Electronic Commerce was approved in 1998.[42] Since then, initiatives have included (i) an Assessment Report on Paperless Trading in APEC Economies[43] to measure the extent of paperless trading in the APEC region, (ii) Public Key Infrastructure Guidelines: Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross-jurisdiction eCommerce,[44] and (iii) an Assessment of Best Practices on Paperless Trading to Facilitate Cross-border Trade in the APEC Region.[45] E-commerce and paperless trade have also been highlighted as significant drivers for trade and investment facilitation in terms of APEC's Trade Facilitation Action Plan[46] and its Investment Facilitation Action Plan.[47] One of the important conclusions reached by the final report of APEC's Guidance for Electronic Commerce was that an interoperable framework for e-commerce needs to be developed in partnership with public and private stakeholders, led by APEC member economy governments.[48]

(The Study on APEC Paperless Business Environment with the Focus on the Use and Archiving of e-Documents (CTI 22/2009T) led to the publication of the Guidelines for Paperless Environment in the APEC region (the Guidelines).[49] The Guidelines include an assessment of the paperless business environment in the APEC region, including electronic document usage in the public and private sectors of the 13 surveyed APEC member economies. At the time of the publication of the report in 2010, digital signature usage was reported to be significantly below 50%, with only South Korea reporting a rate of 42.7%.[50] The Guidelines also reported large differences in technical capacity and digital infrastructure amongst the surveyed APEC member economies. In 2017, APEC published its Cross-border E-commerce Facilitation Agreement[51] recognizing the importance of e-commerce for the future growth of the Asia-Pacific region (APEC Framework Agreement). The objectives of the APEC Framework Agreement included the creation of a favourable regulatory ecosystem for e-commerce and promotion of the development of ICT infrastructure to facilitate cross-border e-commerce, amongst others. More recently, one of the four priority areas for APEC Chile 2019 was advancing the use of digital signatures and electronic certification for SMEs.[52] In addition, APEC is currently in the process of implementing a project titled “Utilising Digital Technology in the Field of Trade Facilitation under the current COVID-19 Pandemic and Beyond: Best Practices Sharing Workshops” which includes the objective, amongst others, to share knowledge and experience regarding the use of digital signatures and other electronic validations.[53] The outcomes of the workshops include providing a final report which sets out policy options and good practices.

## II. LEGAL AND REGULATORY FRAMEWORKS IN APEC MEMBER ECONOMIES

The section discusses the varying approaches which have been taken worldwide, including among APEC member economies, in regulating the use of e-signatures and digital signatures. The section provides an overview of the laws and regulations which currently apply in all APEC member economies.

### A. E-signature and Digital Signature Typologies

Jurisdictions across the world, including APEC member economies, have taken varying approaches to the manner in which they regulate the use and permissibility of e-signatures and digital signatures in their respective jurisdictions. These distinguishing approaches have culminated in a typology which is briefly described below. However, the typology below should not be treated as being definitive of the manner in which approaches to the legal treatment of e-signatures and digital signatures worldwide have been characterized.

All APEC member economies, with the most recent addition of Papua New Guinea, currently have an e-signature and digital signature law in effect. In fact, all APEC member economies have established a legal and regulatory framework governing the adoption, permissibility and use of e-signatures and digital signatures for the purposes of conducting commerce and effecting other legal status matters.

Nonetheless, e-signature and digital signature laws and regulations are largely fragmented across APEC member economies as to the definitions of key basic terms and permitted use.

APEC member economies have taken divergent approaches to the manner in which they regulate the use and permissibility of e-signatures and digital signatures in their respective jurisdictions. For example, some have adopted a minimalist approach by giving e-signatures the same status accorded to traditional 'wet' signatures.

#### (a) Minimalist Approach

Jurisdictions who have adopted this approach have ordinarily based their legal and regulatory frameworks on the foundational principle of functional equivalence by giving e-signatures and digital signatures the same status as traditional 'wet' handwritten signatures.[54] The application of this principle, however, is subject to the caveat that the technology used to effect e-signatures and digital signatures is appropriate for the purpose used.

APEC member economies who have adopted this approach include Australia, Canada, New Zealand, Singapore, and the US.

### **(b) Prescriptive Approach**

Jurisdictions who have adopted this approach have ordinarily formulated their legal and regulatory frameworks to require parties to use prescribed methods, standards or technologies to effect e-signatures and digital signatures.[55] As such, legal effect and recognition are only given to documents and records which have been signed using the prescribed tools mandated by law. Often, these prescribed methods relate to origin and integrity of signed documents and records.

APEC member economies who have adopted this approach include Indonesia and Vietnam whose governments only recognize digital signatures which have been effected through digital certificate providers registered with a local authority and whose servers are located locally.

### **(c) Two-tier Approach**

Jurisdictions who have adopted this approach have ordinarily formulated their legal and regulatory frameworks to consist of a combination of the minimalist and prescriptive approaches.[56] They may permit the use of and provide legal recognition and effect to a number of methods of effecting e-signatures but may also require a greater degree of evidentiary veracity for more advanced methods of effecting e-signatures, such as digital signatures and qualified e-signatures. APEC member economies who have adopted this approach include Chile, China, and Mexico.

## **APEC MEMBER ECONOMIES: LEGAL AND REGULATORY FRAMEWORKS**

The section which follows below provides an overview of the e-signature and digital signatures legal and regulatory frameworks as they currently apply (at the date of publication of this report) in each of the jurisdictions of the APEC member economies.

### **AUSTRALIA**

The Electronic Transactions Act 1999 is 'tech neutral' and a signature is taken to have been made in relation to an electronic communication if:

- a) a method is used to identify the person and to indicate the person's intention
- b) the method used is either reliable as appropriate or proven to fulfil the functions described in paragraph (a)
- c) the method used with reference to paragraph (a) is in accordance with the IT requirements of a Commonwealth entity
- d) the method used with reference to paragraph (a) is used with the consent of a person who is not a Commonwealth entity[57]

## AUSTRALIA (continued)

Commonwealth entity' is defined to mean:

- a) a minister; or
- b) an officer or employee of the Commonwealth; or
- c) a person who holds or performs the duties of an office under a law of the Commonwealth; or
- d) an authority of the Commonwealth; or
- e) an employee of an authority of the Commonwealth.[58]

'IT requirements' is defined as including software requirements.[59]

'electronic communication' means:

- a) a communication of information in the form of data, text or images by means of guided and/or unguided electromagnetic energy; or
- b) a communication of information in the form of speech by means of guided and/or unguided electromagnetic energy, where the speech is processed at its destination by an automated voice recognition system [60].

The Electronic Transactions Act 1999 does not set out any specific technology requirements for e-signatures, nor does it provide for specific categories of e-signatures (as is the case in some other APEC member economies). As such, there are no specific requirements around the use of digital signatures. They are permitted provided their use and execution comply with all relevant legal and regulatory requirements set out under Australian law.

Examples of documents on which an e-signature may be placed include:

- Non-disclosure agreements
- Procurement documents
- Terms of sale
- Employment contracts or any other HR documents
- Sale contracts and quotes
- Real estate documents or lease agreements
- License agreements
- Offers

The Electronic Transactions Regulations 2020 set out the exemptions to the Electronic Transactions Act where use of e-signatures is not permitted. These include documents relating to:

- Migration
- Citizenship
- Bills of exchange



## AUSTRALIA (continued)

- Wills
- Powers of attorney
- Personal service
- Legal proceedings

In relation to the COVID-19 pandemic, e-signature usage was expanded to include additional use-cases on a temporary basis. For example, under the Corporations (Coronavirus Economic Response) Determination (No. 3) 2020 (Cth) (Determination 03/2020), Australian companies were permitted to make use of e-signatures to execute documents under section 127(1) of the Corporations Act 2001 (Cth). This was permitted if the relevant document(s) were signed by two company directors; or a director and the company secretary, or a sole director of a proprietary company who is also the company secretary.

In addition, each signatory to the relevant document(s) was required to:

- a) digitally paste a copy of an e-signature into the relevant document(s);
- b) e-sign using cloud-based platforms; or
- c) execute the e-signature on a laptop, smartphone or tablet using a finger or stylus.

Examples of e-signature usage referred to in Determination 03/2020 included:

- a) signing a physical copy or counterpart of the relevant document(s) where the copy or counterpart includes the entire contents of the relevant document(s); or
- b) using an appropriate and reliable method to indicate their identity and the intention to execute the relevant document(s).

In addition, Determination 03/2020 permitted companies to conduct their meetings virtually.

The exemptions created under Determination 03/2020 only applies to companies registered under the Corporations Act 2001.[61] As a result, overseas companies, incorporated associations, and registered charities could not make use of the temporary COVID-19 relief measures created.

The exemptions created under Determination 03/2020, however, expired on 21 March 2021. The Treasury Laws Amendment (2021 Measures No. 1) Bill 2021 (Cth) which was meant to extend the temporary relief granted under Determination 03/2020 came into force on 14 August 2021.[62] The new Act amends the Corporations Act 2001 and permits companies to:

- execute company documents electronically (including members' resolutions, notices of resolutions, proxy documents and minute books);

## AUSTRALIA (continued)

- conduct company meetings (including AGMs) virtually via electronic means; and
- transmit notices of company meetings to shareholders via electronic means or by providing information to shareholders to permit them to assess notices electronically.

The temporary relief to companies extended and refined by the Bill will only apply until 31 March 2022. However, in October 2020 the Australian government introduced the Corporations Amendment (Virtual Meetings and Electronic Communications) Bill 2020 (Cth) which intends to make the temporary COVID-19 relief measures introduced permanent.[63] The Bill is yet to be passed.

## BRUNEI DARUSSALAM

The Electronic Transactions Act (Cap. 196) (ETA) defines e-signature as any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record and executed or adopted with the intention of authenticating or approving the electronic record.[64]

The ETA specifically confirms that contracts cannot be denied enforceability merely because they are concluded electronically. To prove a valid contract, parties sometimes have to present evidence in court. Leading digital transaction management solutions can provide electronic records that are admissible in evidence under Sections 35A and 62 of the Evidence Act (Cap 108), to support the existence, authenticity, and valid acceptance of a contract.

Use cases where an e-signature is typically appropriate include:

- HR documents, such as employment contracts, benefits paperwork and other new employee onboarding processes
- Commercial agreements between corporate entities, including NDAs, procurement documents, sales agreements
- Consumer agreements

Secure Electronic Signatures are designed to mean that if, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that the e-signature was, at the time it was made:

- (a) unique to the person using it;
- (b) capable of identifying such person;
- (c) created in a manner or using a means under the sole control of the person using it; and
- (d) linked to the electronic record to which it relates in a manner such that if the record was changed the e-signature would be invalidated.[65]

## BRUNEI DARUSSALAM (continued)

Secure Digital Signatures are designed to mean that the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity.[66]

Traditional 'wet' signatures are still required for the documents including:

- The creation of any legal instrument or document under any written law relating to Islamic law
- Wills
- Negotiable instruments
- Indenture
- Power of attorney
- Contracts for the sale or other disposition of immovable property, or any interest in such property
- Conveyance and transfer of immovable property

## CANADA

The Personal Information and Electronic Documents Act 2000 defines 'electronic signature' to mean "a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document".[67]

'Electronic document' means "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print-out or other output of that data".[68]

'Secured electronic signature' means an e-signature that results from the application of a technology or process that is:[69]

- a) unique to the signer;
- b) under sole control of the signer;
- c) can be used to identify the signer; and
- d) linked to the electronic document in a manner which can be used to determine whether the electronic document has been changed since the e-signature was affixed

The Uniform Electronic Commerce Act 1999 defines 'electronic signature' to mean "information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document".[70]

## CANADA (continued)

Documents which require traditional 'wet' signatures include:

- Wills and codicils
- Trusts created out of wills and codicils
- Specific powers of attorney
- Divorce and adoption family law documentation
- Specific legally mandated disclosures to consumers
- Official court documents
- Specific real estate agreements
- Promissory notes

## CHILE

Law 19799 Electronic Documents, Electronic Signature and Certification Services of Such Signature defines 'electronic signature' to mean 'any sound, symbol, or electronic process that allows the recipient of an electronic document to at least formally identify its author'.[71]

'Advanced electronic signature' is defined to mean "one certified by an accredited provider, which has been created using means that the owner maintains under his exclusive control, so that it is linked only to himself and the data to which it refers, allowing the subsequent detection of any modification, verifying the identity of the owner and preventing them from ignoring the integrity of the document and its authorship".[72]

The Accrediting Entity referred to above is the Under-Secretariat of Economy, Development and Reconstruction.[73]

Electronic documents that have the quality of a public instrument must be signed by means of an advanced e-signature.[74]

Documents which require traditional 'wet' signatures include:

- Those in which the law requires a solemnity that cannot be fulfilled by electronic documents
- Those in which the law requires the personal occurrence of any of the parties
- Those related to family law

## CHINA

The Electronic Signature Law of the People's Republic of China, first enacted in 2005 ('E-signature Law') and last amended in 2019, states that contracts can be electronically signed. To prove a valid contract, parties have to present sufficient evidence in court that the contract was formed electronically. Electronic records that can be provided by e-signature platforms are admissible in evidence under Chinese law, to support the existence, authenticity, and valid acceptance of a contract.

If an e-signature concurrently meets the following conditions, it shall be deemed as a reliable e-signature:

- a) when the creation data of the e-signature used for the e-signature is belong exclusively to an electronic signatory. The creation data of an e-signature means such data as the characters and codes that are used in the course of the e-signature and that reliably connects the e-signature with the electronic signatory;
- b) when the signature is entered, its creation data are controlled only by the electronic signatory;
- c) after the signature is entered, any alteration made to the e-signature can be detected; and
- d) after the signature is entered, any alteration made to the contents and form of a data message can be detected.[75]

Use cases where an e-signature is typically appropriate include:

- HR Documents
- Most commercial agreements between businesses (NDAs, purchase orders, invoices, etc.)
- Most consumer agreements (sales and services terms, software licenses, purchase orders, order confirmations, invoices, shipment documentation, etc.)

Documents which require traditional 'wet' signatures include:

- Marriage, adoption, and succession
- Pledges and mortgages
- Corporate documents that must be registered (must be registered with an agency that only accepts handwritten signatures)
- Government-related filings, including application forms for registration or licensing and assignment of intellectual property rights
- Certain commercial contracts, including major transactions of listed companies
- Suspension of public utility services



## HONG KONG, CHINA

The Electronic Transaction Ordinance (ETO) regulates the use of e-signatures in Hong Kong. For transactions not involving any government entity, e-signatures are valid and enforceable provided they comply with the requirements under the ETO. In particular:

- a) the e-signature must be attached to, or logically associated with, the electronic message;
- b) the e-signature process must be reliable as is appropriate given the purpose for which the signature is required; and
- c) the recipient must consent to the signatory using an e-signature.[76]

Use cases where an e-signature is typically appropriate include:

- Commercial agreements between companies (NDAs, purchase orders, invoices, etc.)
- Consumer agreements (sales and services terms, software licenses, purchase orders, order confirmations, invoices, shipment documentation, etc.)
- Human resources agreements (NDAs, employee invention agreements, privacy notices, employment contracts, etc.)
- IP licenses documents (copyright, patent, and trademark)
- Intangible property transfer agreements

Documents which require traditional 'wet' signatures include:

- Wills and codicils
- Trust
- Power of attorney
- Government conditions of grant and government leases.
- Deeds and conveyance
- Statutory declarations
- Affidavits and oaths
- Warrants
- Judgments or orders of courts

## INDONESIA

Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Electronic Information and Transactions ('EIT Law') states that e-signatures are valid and acceptable. In addition, Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions ('GR 71') provides that there are two types of e-signatures: certified and uncertified.

## INDONESIA (continued)

-E-signature with certification: This type of e-signature involves the creation of a unique code that is designated for a specific legal subject (also called a digital certificate). The digital certificate, which must be issued by an Indonesian certified e-signature provider, is created based on the legal subject's identification documents.[77]

-E-signature without certification: This type of e-signature is created without involving the service of an Indonesian certified e-signature provider and may include a digitized version of an individual's handwritten signature.[78]

To be able to legally produce an e-signature with certification, an Indonesian certified e-signature provider must be registered with the Ministry of Communications and Informatics and certified by an e-signature certification agency. Any e-signature produced by a foreign e-signature provider is considered as an e-signature without certification.[79]

Under the GR 71, both types of e-signatures have the same level of enforceability and admissibility as a traditional 'wet' signature if they meet the following requirements for validity:

- a) the data is associated only with the signer;
- b) the data must be controlled solely by the signer;
- c) any alteration that occurs after the time of the signing is traceable,
- d) certain methods are adopted to identify the signer; and
- e) certain methods are adopted to demonstrate that the signer has given his or her consent to the associated electronic information.[80]

While the above is true, the use of an e-signature/e-seal with certification is preferable as it has historically been accepted more favorably as evidence before a court of law.

Use cases where an e-signature may be appropriate include:

- Commercial agreements between corporate entities, including NDAs, procurement documents, sales agreements
- Consumer agreements, including new retail account opening documents

On the other hand, there are documents which still require traditional 'wet' signatures, including:

- Contracts and deeds for the sale of immovable property or the transfer of any interest in immovable property
- Corporate documents, such as a deed of establishment, articles of association (and amendments), a deed of shareholder resolutions and shares/assets transfer documents
- An agreement of a mortgage over land or immovable property

## JAPAN

The Electronic Signatures and Certification Act No. 102 of 31 May 2000 defines 'Electronic Signature' to mean "a measure taken with respect to information that can be recorded in an electromagnetic record (a record that is prepared by an electronic form, a magnetic form or any other form not perceivable by human senses and that is used for information processing computers), and which is:

- a) a measure to indicate that such information was created by the person who has taken such measure; and
- b) a measure to confirm whether such information has been altered".[81]

An electromagnetic record will be presumed to be authentic if the e-signature is performed by the principal through appropriate management of codes and properties in relation to information recorded in an electromagnetic record in order to express the signatory's intention.[82]

Certificate based digital signatures must be issued by the Japanese Public Key Infrastructure or an Authorized Service Provider. They are primarily used for e-filing documents with government departments.

Examples of documents on which an e-signature may be placed include:

- IP transfer agreements
- Consumer agreements
- Certain HR documents
- General lease agreements
- Commercial agreements

Documents which require traditional 'wet' signatures include:

- Notarial deeds
- Testamentary documents (civil code)
- Documents required to be in writing (i.e., lease and brokerage agreements)
- Specific filings under a power of attorney

## REPUBLIC OF KOREA

Electronic signatures are governed by the Digital Signature Act and the Framework Act on Electronic Documents and Transactions of Korea. Under the Digital Signature Act, last amended on 9 June 2020, the term 'electronic signature' piece of information in electronic form that is affixed on, or logically combined with, an electronic document in order to identify the signatory and verify that the electronic document has been signed by the said signatory.[83]

## REPPUBLIC OF KOREA (continued)

Use cases where an e-signature is typically appropriate include:

- HR documents, such as employment contracts, benefits paperwork and other new employee onboarding processes
- Commercial agreements between corporate entities, including NDAs, procurement documents, sales agreements
- Certain consumer agreements, including new retail account opening documents
- Certain real estate documents, such as lease agreements
- Non-exclusive licenses of intellectual property, including patent and copyright

Documents which require traditional 'wet' signatures include:

- Real property transfer contracts and deeds (excluding lease)
- Intangible property transfers

Prior to the 2020 amendment, the ESA outlined two types of electronic signatures: (1) a certified electronic signature and (2) an uncertified electronic signature. A valid certified electronic signature needed to be based on a public key certificate.[84]

The amended ESA abolishes the concept of the certified electronic signature due to fairness and monopoly concerns. Under the amended ESA, an electronic signature will not be denied validity solely because it is in electronic form.

## MALAYSIA

The Electronic Commerce Act 2006 (ECA) specifically confirms that contracts cannot be denied enforceability merely because they are concluded electronically. To prove a valid contract, parties sometimes have to present evidence in court. Leading digital transaction management solutions can provide electronic records which may be admissible in evidence under the Evidence Act 1950, to support the existence, authenticity, and valid acceptance of a contract.

In order to be recognized under the ECA, an electronic signature must:

- be attached to or logically associated with the electronic message;
- adequately identify the signer and adequately indicate the signer's approval of the information to which the signature relates; and
- be as reliable as is appropriate for the purpose and circumstances in which the signature is required.[85]

## MALAYSIA (continued)

An electronic signature is “as reliable as is appropriate” if:

- a) the means of creating the electronic signature is linked to and under the control of only the signer;
- b) any alteration made to the electronic signature after the time of signing is detectable; and
- c) any alteration made to that document after the time of signing is detectable.[86]

Digital signatures are regulated by the Digital Signature Act (DSA) 1997. The DSA defines digital signatures as “a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer’s public key can accurately determine whether the transformation was created using the private key that corresponds to the signer’s public key, and whether the message had been altered since the transformation was made”. [87]

When the law requires a seal to be affixed to a document, a digital signature must be used in lieu of wet signature.

Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature where:

- a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;
- b) that digital signature was affixed by the signer with the intention of signing the message; and
- c) the recipient has no knowledge or notice that the signer has breached a duty as a subscriber; or does not rightfully hold the private key used to affix the digital signature. [88]

Use cases where an e-signature is typically appropriate include:

- HR documents
- Commercial agreements between corporates
- Commercial real estate documents

## MALAYSIA (continued)

Documents which require traditional 'wet' signatures include:

- Power of attorney
- Wills, codicils and trusts
- Trusts
- Bills of exchange and promissory notes
- Statutory declarations
- Bills of sale
- Money lending agreement

## MEXICO

The Code of Commerce defines simple e-signature as being the data in electronic form recorded in any technology in a data message, which indicates that the signatory approves the information contained in such data message.[89]

'Data message' is defined to mean "the information generated, sent, received or filed through optical or electronic means or through any other technology".[90]

The 'data message' containing the e-signature must be:

- a) kept in its original version;
- b) stored in its entirety and kept available for subsequent consultation; and
- c) attributable to the signers.

The most common examples of simple e-signatures include digital wet signatures, PINs and biometric factors (voice, fingerprint or facial identifiers).

The Code of Commerce defines advanced or reliable e-signatures as meeting the following requirements:

- a) the signature creation data corresponds solely to the signatory;
- b) the signature creation data, at the time of signing, is under the control of the signatory solely;
- c) it is possible to detect any alteration of the electronic signature once it has been made; and
- d) it is possible to detect any alteration of the information in a data message once it has been made.[91]

Advanced or reliable e-signatures may be issued certification service providers or authorities. They usually involve the application of a mathematical algorithm to a graphical representation of the name of the relevant signatory.

## MEXICO (continued)

Examples of these types of e-signatures include those issued to persons enrolled in the Federal Taxpayer Registry by the Tax Administration Service.[92]

Documents which require traditional 'wet' signatures include public instruments required to be legally granted before a notary public or commercial broker, including:

- Incorporation of commercial companies (General Law on Commercial Companies, Article 5) and trusts holding real estate (General Law on Negotiable Instruments and Credit Transactions, Articles 388 and 404)
- Formalization of minutes of extraordinary meetings (General Law on Commercial Companies, Article 194)
- Ratification of signatures for non-possessory pledge agreements (General Law on Negotiable Instruments and Credit Transactions, Article 365)
- Specific powers of attorney (Federal Civil Code, Article 2551)

Despite e-signatures seemingly being permitted for use on public deeds, notary publics and commercial brokers have been reluctant to allow their use.

## NEW ZEALAND

The Contract and Commercial Law Act 2017 defines 'electronic signature' to mean "in relation to information in electronic form, means a method used to identify a person and to indicate that person's approval of that information".[93]

An e-signature is valid if it:

- a) identifies the signatory and indicates the signatory's approval of the information to which the signature relates; and
- b) is reliable as is appropriate for the purpose for which it is given, and the circumstances in which, the signature is required.[94]

The presumption of reliability of an e-signature applies if:

- a) means of creating the e-signature is linked to signatory solely;
- b) means of creating the e-signature was under control of signatory solely;
- c) alterations to the e-signature after signing is detectable; and
- d) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, alteration made to that information after the time of signing is detectable.[95]



## NEW ZEALAND (continued)

Examples of documents on which an e-signature may be placed include:

- General business contracts
- Employment contracts
- Lease agreements

Documents which require traditional 'wet' signatures include:

- Documents relating to citizenship and passports
- Documents relating to elections
- Documents relating to credit contracts and consumer finance
- Notices to the public
- Powers of attorney
- Wills, codicils, or other testamentary instruments
- Negotiable instruments
- Bills of lading
- Documents relating to provisions of enactments in respect of certain courts, tribunals and other bodies

In relation to the COVID-19 pandemic, e- signatures were permitted to be used in relation to deeds which create powers of attorneys in connection with a security interest made on and from 21 March 2020 up until 6 months thereafter.[96] On 3 November 2021, the New Zealand government reinstated the temporary COVID-19 relief granted under the COVID-19 Response (Further Management Measures) Legislation Act 2020 (2020 No. 13) to apply until 30 April 2022 (unless extended otherwise).[97] In the interim, business and other organizations are thus permitted to make use of 'electronic means' even if their constitutions or rules do not permit such use. Such electronic means may only be used to the extent that the majority of the business or organization's governing body believe in good faith that it is reasonably practicable to use non-electronic means.[98]

Under the COVID-19 Response (Requirements For Entities—Modifications and Exemptions) Act 2020 (No. 14), the term 'electronic means' is used with reference to:

- having or recording information in writing;
- calling or holding meetings, including for the purpose of establishing a quorum;
- voting (though there are some matters that electronic voting can't be used for);
- giving or receiving information;
- making or keeping new records;
- providing access to records or information held by or on behalf of the entity;
- signing any instrument (document); and
- retaining any information.[99]

## PAPUA NEW GUINEA

The Electronic Transactions Act No. 38 of 2021 defines ‘electronic signature’ to mean “any symbol or other data in electronic form in, affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s intention in respect of the information contained in the data message”. [100]

‘Data message’ is defined to mean “information generated, sent, received or stored by guided or unguided electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic communication, electronic mail, telegram, telex or telecopy”. [101]

An e-signature is considered to be reliable if:

- (a) the signature creation data is within the context in which it is used, linked to the signatory and of no other person or party; and [102]
- (b) the signature creation data was, at the time of signing, under the control of the signatory and of no other person or party; and
- (c) any alteration to the electronic signature, made after the time of signing, is detectable; and [103]
- (d) the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable. [104]

Documents which require traditional ‘wet’ signatures include:

- Transactions on a regulated exchange
- Foreign exchange transactions
- Inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments
- The transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary
- Transactions and issues relation to personal law such as marriages, divorce, the creation or execution of a will or any other testamentary disposition
- A Power-of-Attorney
- A trust, excluding a constructive, implied and resulting trust
- Documents legally required to be attested before a notary public (including affidavits, statutory declarations, or other documents involving an oath or affirmation)
- Other documents or transactions exempted by special provisions of a Papua New Guinea law. [105]

## PERU

Digital Certificates and Signatures Law No 27269 defines 'electronic signature' to mean any symbol based on electronic means used or adopted by a given party with the precise intention of linking or authenticating a document so that it meets the features of a handwritten signature.[106]

'Digital signature' is defined to mean an e-signature that uses a symmetric cryptography technique, based on the use of key pair that are unique; a private key and a public key which are mathematically linked to each other, so that people who have access to the public key cannot retrieve the private key from it.[107]

Examples of documents on which an e-signature may be placed include:

- HR documents such as Employment Contracts, benefits paperwork and other new employee onboarding processes
- Commercial agreements between corporate entities including NDAs, procurement documents, sales agreements
- Consumer agreements including new retail account opening documents Certain real estate documents including Lease agreements, certain purchase and sales contracts

Documents which require traditional 'wet' signatures include:

- Specific real estate agreements such as real property transfer, donation of estate property (Peruvian Civil Code, Article 1625)
- Incorporation of civil legal entities and all acts that entail a change of company by laws (General Law of Corporations, Article 5 and Peruvian Civil Code, Articles 81 and 100)
- Specific powers of attorney (Peruvian Civil Code, Article 156)
- Mortgages (Peruvian Civil Code, Article 1098)
- Antichresis (Peruvian Civil Code, Article 1092)
- Wills, waiver of inheritance, establishment of family assets, partition of inheritance, marriage/prenuptial separation of goods (Peruvian Civil Code, Articles 675 and 496)
- Specific wills (Peruvian Civil Code. Article 696)

## PHILIPPINES

The use of e-signatures in the Philippines is governed by the Electronic Commerce Act of 2000 (ECA) and its Implementing Rules and Regulations (IRR). Alongside the Supreme Court's subsequently issued Rules on Electronic Evidence (REE), parties may generally use e-signatures to create valid private and government contracts, provided that there are no specific statutory requirements to the contrary.

## PHILIPPINES (continued)

Under the ECA, an e-signature is:

- a) any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person; and
- b) attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person.[108]

Apart from an e-signature, the Supreme Court's REE elaborates on a digital signature, which refers to an electronic signature which is asymmetrically encrypted using a hash function through private and public keys. [109]

Use cases where an e-signature is typically appropriate include:

- HR documents
- Commercial agreements between corporates
- Consumer agreements including new retail account opening documents, sales terms, service terms, software licenses, shipment documentation, user manuals and policies.
- IP licenses (excluding trademark licenses)
- Intangible property transfers

Documents which require traditional 'wet' signatures include:

- Acts and contracts for immovable property
- Special power of attorney
- Subordinated loan agreements
- Several corporate documents submitted to the SEC, including as articles of incorporation and voting trust agreements
- Tax returns

In December 2020, the Philippine Anti-Red Tape Authority (ARTA) and the Commission on Audit (COA) announced that government agencies and local government units (LGUs) can use digital signatures issued by the Department of Information and Communication Technology (DICT) through the Philippine National Public Key Infrastructure (PNPKI) for faster processing of documents. Both PNPKI digital signatures and the traditional electronic signatures will be honored by government.

## RUSSIA

Federal Law No. 63-FZ defines e-signature as a piece of information in electronic form that is attached or otherwise related to another piece of information in electronic form (information that is to be signed by e-signature) and that is used to identify a person signing such piece of information.[110]

Under Russian law, there are three types of e-signatures, including:

- a) **Simple e-signatures** – a code, log-in, password (including via sms), email or any other means that the parties may agree as to the means to confirm the fact of creation of an electronic signature of the person
- b) **Enhanced unqualified e-signature** – a piece of information that is encrypted and requires an electronic key to decode it. This is a means to confirm that a particular person has signed the document. It also serves to ensure that no change can be made in a document after it has been signed
- c) **Enhanced qualified e-signature** – requires complex encrypting through cryptographic tools certified by the licensing and certification center of the Russian Federal Security Service. An electronic key is required for decoding and is obtained by a holder of the qualified electronic signature from an entity accredited as a ‘certification center’ by the Ministry of Communications

The most common examples of e-signature use include:

- Exchange of data with state authorities (i.e., mandatory tax filings, state insurance funds or state statistical services)
- To sign accounting documents and tax returns
- In banking business
- In transactions conducted via exchanges
- Commercial agreements between corporate entities such as NDAs, procurement documents and sale agreements
- Consumer agreements such as new retail account opening document
- Short-term real estate documents such as lease agreements, purchase and sale contracts)

Documents which require traditional ‘wet’ signatures include:

- Documents requiring notarization (i.e., contracts of sale, gift, pledge of shares in the authorized capital of a company, powers of attorney)
- Promissory notes
- Documents requiring state registration, such as long-term real estate or rent agreements

## SINGAPORE

E-signatures in Singapore are regulated by Singapore's Electronic Transactions Act (ETA), which was first passed in 1998, and by the Electronic Transactions (Certification Authority) Regulations 2010.

The ETA states that an electronic record is any record that is generated, communicated, received, or stored by electronic means in an information system or for transmission from one information system to another.[111]

For an e-signature to be valid, it must meet the following conditions:

- a) there must be reliable assurance about the integrity of information in the electronic record, from the time it was first made in its final form;
- b) where the electronic record is to be provided to a person, it must be capable of being displayed to that person; and
- c) it must comply with any additional requirements relating to electronic records specified by the public agency supervising the provision or retention of such records.

[112]

Secure e-signatures are defined to mean e-signatures that, if, through the application of a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, can be verified to be, at the time it was made:

- a) unique to the person using it;
- b) capable of identifying such person;
- c) created in a manner or using a means under the sole control of the person using it; and
- d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated.[113]

Pursuant to an amendment to the ETA in 2011, for a digital signature to be accepted, it must meet the following conditions:

- a) it must have been created during the operational period of a valid certificate and could be verified by reference to the public key listed in that certificate; and
- b) the certificate is considered trustworthy because:

- (i) it was issued by an accredited certification authority operating in compliance with the regulations; or

- (ii) it was issued by a recognized certification authority; or

- (iii) it was issued by a public agency approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or

- (iv) the parties have expressly agreed between themselves (sender and recipient) to use a digital signature as a security procedure, and the digital signature was properly verified by reference to the signatory's public key.[114]

## SINGAPORE (continued)

Digital signatures backed by certificates from trusted service providers are treated as a form of secure e-signature.

Use cases where an e-signature is typically appropriate include:

- HR documents
- Commercial agreements between corporates
- Consumer agreements
- Software license agreements
- IP licenses, including patent, copyright and trademark
- Intangible property transfers (e.g., patent and copyright assignments)

Documents which require traditional 'wet' signatures include:

- Wills
- Negotiable instruments, documents of title, bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money
- Indenture
- Conveyance of or transfer of any interest in real estate property
- Trust or power of attorney
- Contracts for the sale or other disposition of immovable property (except implied, constructive and resulting trusts)

## CHINESE TAIPEI

E-signatures in Chinese Taipei are regulated by the Electronic Signatures Act (ESA) of 2001 and its Enforcement Rules.

'Electronic signature' means data attached to and associated with an electronic record and executed with the intention of identifying and verifying the identity or qualification of the signatory of the electronic record and authenticating the electronic record.[115]

'Digital signature' means an e-signature generated by the use of mathematic algorithm or other means to create a certain length of digital data encrypted by the signatory's private key, and capable of being verified by the public key.[116]



## CHINESE TAIPEI (continued)

Digital signature, supported by a certificate issued by a certification service provider whose certification practice statement is approved by the Taiwanese government, can be used in an electronic record in circumstances where law or regulation requires a handwritten signature or seal.

The most common examples of electronic signature use include:

- HR documents
- Commercial agreements between corporates
- Consumer agreements (excluding consumer loan agreements), residential and commercial lease agreements
- Software license agreements
- Copyright, patent and trademark licenses
- Transfers of intangible property (e.g., patent and copyright assignments)

Documents which require traditional 'wet' signatures include:

- Real property transfer contracts and deeds
- Contracts made for the obligations of the transferring, creation, or altering of rights over the real property
- Securities transactions and listing documents required by the Financial Supervisory Commission under Securities Transaction Act, Merger and Acquisition Act, Regulations Governing the Administration of Shareholder Services of Public Companies
- Notices of insurance contracts and evidential documents for insurance claims under the Insurance Law required by the Financial Supervisory Commission (Ruling dated March 31, 2016 No. 10502561091 by the Financial Supervisory Commission)
- Documents regarding the issuance and amendment of passport by the Ministry of Foreign Affairs

## THAILAND

E-signatures in Thailand are regulated by the Electronic Transactions Act (ETA), first passed in 2001. To prove a valid contract, parties sometimes have to present evidence in court. Electronic records are admissible in evidence under Section 11 of the ETA, to support the existence, authenticity, and valid acceptance of a contract.

The ETA defines e-signature as "letter, character, number, sound or any other symbol created in electronic form and affixed to a data message in order to establish the association between a person and a data message for the purpose of identifying the signatory who involves in such data message and showing that the signatory approves the information contained in such data message."

## THAILAND (continued)

According to the Electronic Transactions Development Agency's (ETDA) guidelines, e-signatures are categorized as follows:

a) Type 1: General e-signature (Section 9 of the ETA) - an e-signature in any form (letter, number, or any other symbol) which the method used for signing possesses the following qualifications:

- (i) capable of identifying the signatory and signatory's approval of information contained in the data message;
- (ii) being a reliable method that is appropriate to the objectives of the generation or delivery of the data message considering surrounding circumstances and relevant agreements;
- (iii) being another method that can, independently or with the presentation of related evidence, identify the signatory and signatory's approval of information contained in data messages. [117]

Examples of e-signatures include typed names at the end of an e-mail, signing with a stylus pen or through an automated workflow system and clicking on the agree checks [118]

b) Type 2: Trustworthy e-signature (Section 26 of the ETA) - must meet the following requires:

- (i) the signature creation data are only linked to the signatory and under the control of the signatory and of no other person at the time of signing;
- (ii) any alteration to the electronic signature, made after the time of signing, is detectable. [119]

Example of Trustworthy e-signature include creation of e-signature through Public Key Infrastructure (PKI).[120]

c) Type 3: Trustworthy e-signature (Section 26 of the ETA) - with a certificate issued by the Certification Authority shall meet the criteria laid out in Section 26 of the ETA for Trustworthy e-signature. Additionally, the certification service provider must comply with Section 28 of the ETA as follows:

- (i) act in accordance with the policies and practices the service providers have initially pledged;
- (ii) exercise caution to ensure the accuracy and comprehensiveness of all material represented in the certificate throughout its validity period;
- (iii) provide reasonable accessibility means which allow other disputants to verify facts shown on the certificate.[121]

## THAILAND (continued)

Use cases where an e-signature is typically appropriate include:

- HR documents
- Commercial agreements between corporates
- Consumer agreements including new retail account opening documents
- Real estate documents including lease agreements (for a period of no more than 3 years), and other related documentation for residential and commercial real estate

Documents which require traditional 'wet' signatures include:

- Contract of sale or gift of immovable property
- A hire of immovable property for more than a period of 3 years
- Mortgage contract
- Transactions relating to family law (such as contracts of succession)
- Successions

## UNITED STATES

The United States Electronic Signatures in Global and National Commerce Act defines 'electronic signature' to mean "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." [122]

An e-signature is valid and legally binding if:

- a) both users have demonstrated clear intent to sign the document;
- b) both users have demonstrated their consent to conduct business electronically;
- c) electronic signatures must be connected to the document being signed;
- d) software utilized to collect electronic signatures must indicate the signatories to the document; and
- e) electronic record must be kept of all digital transactions which is accessible to all users at any time.

States are able to adopt UETA in place of E-SIGN and modify federal requirements by indicating alternative procedures if it is aligned with E-SIGN and federal law and does not require or favor a particular technology.

UETA has been adopted in 47 states, the District of Columbia, Puerto Rico and the US Virgin Islands. State laws differ as to:

- Validation of specific types of electronic signatures
- Requiring forms of security
- Validation of digital signatures solely
- Types of transactions that are covered

## UNITED STATES (continued)

Documents which require traditional 'wet' signatures include:

- Domestic and family law (adoption and divorce) documentation
- Wills, codicils and testamentary trusts
- Court documents
- Health and life insurance cancellation notices
- Utility cancellation notices
- Housing default and foreclosure notices
- Product recall notices
- Documents relating to hazardous materials

## VIETNAM

E-signatures in Vietnam are regulated by the Law on E-Transactions, first passed in 2005. To prove a valid contract, parties sometimes have to present evidence in court. Electronic records are admissible in evidence to support the existence, authenticity and valid acceptance of a contract.

E-signatures are valid if:

- a) the method of creating the E-signature identifies the signer and indicates their approval of the contents of the data message; and
- b) such a method is sufficiently reliable and appropriate for the purpose for which the data message was created and sent.[123]

The requirements for a valid digital signature are as follows:

- a) the digital signatures are created during the valid period of the corresponding digital certificates and able to be checked by the public key recorded on such valid digital certificates;
- b) the digital signatures are created by using the private key corresponding to the public key recorded on digital certificates granted by certification authorities; and
- c) the private key is only under the control of the signer at the time of signing.[124]

Use cases where an e-signature may be appropriate include:

- HR documents
- Commercial agreements between corporates
- Consumer agreements including new retail account opening documents
- Service agreements.

Documents which require traditional 'wet' signatures include:

- Contracts related to real property transfer
- Intangible property transfers
- Transfer of movable asset

### III. BARRIERS TO EFFECTIVE ADOPTION AND USE

Even where e-signatures and digital signatures use is permitted, in a large number of APEC member economies, it still appears to be market practice to require ‘physical attendance’ and the usage of traditional ‘wet signatures’, chops and seals when submitting applications, forms, notices, and effect regulatory reporting to the relevant local authority or to effect transactions. The global e-signing platforms DocuSign and Adobe Sign appear to be the favorite e-signing platforms for use to affix e-signatures, particularly to effect transactions on a cross-border basis. In addition, e-signing platforms appear to be costly in some cases and even unaffordable for many SMEs.

This section presents a summary of some of the barriers to the effective adoption, implementation, and use of e-signatures and digital signatures.

**(1) E-signature and digital signature use are permitted (with exceptions), but physical attendance and traditional ‘wet’ signatures in hard copy format is still required as market practice.**

In this case, e-signature and digital signature use is permitted by law, but certain stakeholders (such as financial institutions and local authorities) still require physical attendance and the effecting of traditional ‘wet’ signatures in hard copy format for certain applications, notifications, transaction approval and an official chop or stamp to make amendments thereto, as market practice. For example, some banks do not accept e-signatures and digital identity verifications for KYC verification processes and still require regular notarization and legalization of documents proving identity.

For example:

- In Chinese Taipei, whilst allowing e-signatures, in the instance of travel insurance customers can request a policy when booking travel online but the policy cannot be sold until the customer returns a ‘wet’ signature on a printed copy of the policy. The return rate of the signed policies is very low, and this practice presents a significant barrier to online sales of travel insurance.
- In Hong Kong, China, the Securities and Futures Commission requires the original signed licensing application forms in order to process a licensing application. While e-signatures are currently accepted by the SFC, the original signed forms are still required to be submitted to the SFC before the SFC would approve the licensing application. Moreover, amendments to the forms typically require a physically amended page stamped with the applicant’s chop.

- In the Republic of Korea, where e-signatures are fairly common but digital account opening is limited due to regulations under the Real Name Verification Law which requires submission of hard copies of certain documents, even where previously submitted. These requirements include Identification of corporate (Corporate Registration Certificate, etc.), Identification of corporate representative or agent, Delegation document (Power of Attorney and Corporate Seal Certificate).
- In Malaysia, digital signatures are permitted and can be used to digitally open a bank account or other service contracts electronically. However, regulation still requires physical documents and in-person attendance for certain activities. For example, all contracts (with wet signatures) must be physically presented at the local tax office for document stamping. Payment of stamping fees also need to be done at the stamping office.

**(2) E-signature and digital signature use are permitted but their use is restricted to a limited classes of documents and / or in relation to specific transactions.**

In this case, e-signature and digital signature use is permitted by law, however, their use is limited by laws and regulations which required traditional 'wet' signatures to be affixed to certain classes of documents and in relation to specific transactions. Most notably, this is the case where a notary public is required to notarize specific documents or where seals and chops are required for the document to have necessary effect.

For example:

- Indonesia, Malaysia, Thailand, and Vietnam do not accept the use of e-signatures and digital signatures in relation to tax and treasury documents.
- In Thailand traditional 'wet' signatures are still required to effect new fund registrations and to amend prospectuses in spite of that it is permitted to use e-signatures and digital signatures by law.

**(3) E-signature and digital signature use are permitted (with exceptions), but the local authority needs to approve use of relevant e-signing platform or require local vendors to certify electronic signatures.**

In this case, e-signature and digital signature use is permitted by law, however, the local authority must approve the use of the specific technology (i.e., e-signing platforms such as DocuSign and Adobe Sign) which is used to effect e-signatures and digital signatures. The delays caused by having to require the approval of the relevant local authority to use e-signatures and digital signatures makes the use of the technology ineffectual and does away with the efficiencies in speed and convenience created through its use.

For example:

- In both China and Indonesia, DocuSign and Adobe Sign do not meet local regulations given the fact that a local e-signature vendor must be used in order for the document to be certified. Laws on data privacy are also strict in most cases, therefore requiring keeping data locally.
- In Chinese Taipei, during the COVID-19 pandemic multinational corporations have made use of e-signatures to effect transactions and sign documents. This, however, appears to be a temporary measure and the use of e-signature platforms to sign and transmit documents to clients (including individuals and corporations) must be approved by the Banking Bureau.

**(4) Definitions of key basic terms, such as ‘e-signature’ and ‘digital signature’, are not always clear and appear to be heterogeneous across APEC member economies, making implementation challenging for businesses.**

Bearing in mind the different approaches to the implementation and use of e-signatures and digital signatures across APEC, the definitions utilized for these terms have been inconsistent and unclear.

Specifically, it has been reported that jurisdictions such as Indonesia, Singapore, Hong Kong, and China provide a substantially clear definition of the areas where e-signatures are accepted and what the requirements are to ensure their validity. Other jurisdictions such as Vietnam, lack clear definitions of the realm of e-signatures applicability, leaving businesses in uncertainty, especially given the fact that most courts are still not familiar or comfortable with the matter.

Having a law that defines clear cases while adopting a definition that is generic enough to leave flexibility to businesses tends to be the preferred approach for most stakeholders.

Other examples:

- Jurisdictions such as Singapore, Hong Kong, Malaysia, Philippines and South Korea have stringent (outsourcing) regulatory clearance requirements, when the external service provider has access to, processes or stores bank/customer data – which external third-party electronic signature solutions often entail. Each third-party solution and its documents/use cases therefore needs to be assessed on its own facts.



If there are any cross-border elements to the documents/use cases for e-signatures, including but not limited to:

- parties in different countries of domicile;
- more than 2 parties to the transaction/agreement;
- governing law not being one that adopts a “Minimalist Approach” (eg Singapore law) and/or reliance is placed on a “neutral” country’s law governing the transaction/agreement where neither party is established there; and/or
- enforcement envisaged in another jurisdiction,

Then, each use case and its documents will also need to have:

- (a) addressed multi-jurisdictional legal considerations of validity, authority, registration formalities, enforceability and evidential requirements, amongst others, and
- (b) built-in controls to give effect to or work within the said multi-jurisdictional considerations.

#### **(5) Courts are often reluctant to accept electronically signed documents.**

Even with e-signature and digital signature laws and regulations in place, in practice courts in the APEC region have been slow in accepting the concept of electronic signatures and electronic documents and therefore admitting them in court.

For example:

- In Thailand, banks continue to require customers to sign loan agreements using a traditional ‘wet’ signature as doubt remains as to the extent to which Thai courts would be willing to accept documents signed electronically into evidence.

## IV. IMPACT OF COVID-19 AND RESPONSES

In spite of the impact of the COVID-19 pandemic on in-person business operations, only a handful of APEC member economies have amended, with different approaches, their digital signature laws and regulations to take this into account by relaxing their use to effect certain transactions and execute certain documents. This has resulted in further fragmentation of e-signature and digital signature laws and regulations across APEC member economies.

This section highlights the impact of COVID-19 on in-person business operations, together with the best practices which have been deployed.

**(1) Social distancing measures have restricted in-person business operations, accelerating the use of e-signatures and digital signatures to effect commercial and ordinary business transactions.**

As billions of people and professionals had to face lockdowns to prevent the spread of COVID-19, e-signatures and digital signatures acceptance has naturally increased. In practice, many businesses and institutions found themselves in the position of being forced to embrace the e-signatures laws and regulations that were created years before.

For example, in Japan, a country where business practices tend to be conservative, services that allow users to affix seals and conclude contracts online surged in popularity during the COVID-19 pandemic due to companies promoting remote working. Shachihata Inc., a company offering an electronic seal-stamping service via the cloud, provide an alternative to physical stamp using hanko personal seals, has reported a “drastic increase of new users” in 2020.[125]

**(2) Amendments and relaxation of e-signature and digital signature laws and regulations to create exceptions to prohibited use of e-signatures and digital signatures in place of the usually required traditional ‘wet’ signatures, chops and seals.**

The COVID-19 pandemic has forced governments to reconsider their laws and policies to incentivize business activities that have been dramatically impacted by lockdowns and other restrictions.

For example:

The Australian government has first introduced a temporary modification to the Corporations Act 2001 (Cth) (Corporations Act) through the Corporations (Coronavirus Economic Response) Determination (No. 3) 2020 (Cth) (Determination 03/2020), that presented the following changes:

- Meeting of directors and shareholders may be held in a fully online setting, while previously physical presence was required, at least partial.
- Notice of meetings may be provided and signed electronically, while previously a paper notice was required unless a shareholder had agreed explicitly otherwise.
- Minutes of the meeting may be taken and stored electronically, while previously hard copies and physical storage were required
- Documents may be signed electronically provided that certain conditions are met, while previously wet signature was required.

Conditions under which e-signature of the document is valid are:

- (a) a method is used to identify the person and to indicate the person's intention to sign a copy or counterpart of the document, for example, as the explanatory memorandum of the Bill suggests, using a stylus tool to sign a PDF or a platform such as DocuSign;
- (b) the electronic copy includes the entire contents of the document; and
- (c) the method must be as reliable as appropriate for the purposes for which the document was generated or proven in fact to have indicated the person's identity and intention.

- The Treasury Laws Amendment (2021 Measures No. 1) Act 2021 extends and refines the temporary relief granted under the Corporations (Coronavirus Economic Response) Determination (No. 3) 2020 (Cth) (Determination 03/2020) until 31 March 2022.
- In addition, the government has subsequently formulated the Corporations Amendment (Virtual Meetings and Electronic Communications) Bill 2020 (Cth) that proposes making permanent the relief to enable e- signatures for the purposes of signing documents under section 127 of the Corporations Act 2001, as well as directors' meetings and general members' minutes.

In New Zealand an amendment of the Contract and Commercial Law Act 2017 created an exception to allow the use of electronic signatures in relation to deeds which create powers of attorneys in connection with a security interest made on and from 21 March 2020 up until 6 months after the exception came into force.

- On 3 November 2021, the New Zealand government reinstated the temporary COVID-19 relief granted under the COVID-19 Response (Further Management Measures) Legislation Act 2020 (2020 No. 13) to apply until 30 April 2022 (unless extended otherwise).[126] In the interim, business and other organizations are thus permitted to make use of 'electronic means' even if their constitutions or rules do not permit such use. Such electronic means may only be used to the extent that the majority of the business or organization's governing body believe in good faith that it is not reasonably practicable to use non-electronic means.[127]

**(3) Use of a back-up solution to digitize onboarding and KYC/AML processes in APEC member economies where e-signature and digital signature laws are not working effectively.**

Financial institutions have started to work on innovating KYC and digital onboarding procedures well before the pandemic hit. Nonetheless, COVID-19 has been a natural accelerator to scaling these efforts to create a seamless and convenient digital experience for customers, which is today a reality in the majority of the APEC member economies. E-signatures are a key component of digital onboarding and KYC but as highlighted in this report, regulations in some countries are lagging.

For example:

- In China and Indonesia, institutions are prevented from relying on a unique e-signature platform due to the requirement that it must be a local platform.
- In Vietnam and Chinese Taipei, certain documents are required to be signed using the company's chop.

To overcome these challenges, financial institutions have been relying on a back-up solution in these markets. This back-up solution ('e-submit') allows customers to apply a wet signature on a printed copy of the document and upload it as the final solution.

**(4) More prevalent and increased usage of e-signing platforms, such as DocuSign and Adobe Sign, and electronic stamp sealing services to effect transactions on a cross-border basis.**

On a global level, usage of e-signature software has been sharply increasing. For example, DocuSign saw its customer base more than double over the last two years, up to more than 988,000 clients.[128] Especially for businesses with multiple international offices or with frequent cross-border activities, these platforms have also helped harmonize the different options to electronically sign documents to both clients and staff. On one hand, this is mainly aimed at minimizing cases of dispute and, on the other, to ensure a smooth execution and to standardize operations.

However, it is worth noting that the price of many e-signing online platforms remains expensive or even unaffordable for many SMEs. The accessibility of these solutions will likely be a key area of focus going forward.

**(5) Governments have launched local e-signature and digital signature solutions to support the digitalization of the economy**

Governments are working on harmonizing the use of e-signatures to support businesses and citizens.

These initiatives have the potential to both become a core component of the e-signature infrastructure as well as simplifying the relationship between the public and different government agencies.

For example:

- In Singapore, a major initiative is the 'Sign with SingPass'. The service is delivered by Assurity, a subsidiary of the Government Technology Agency, in partnership with eight third party vendors, including DocuSign, Adobe and Kofax. Using the service, Singaporeans will be able to verify their identity (via biometric features) and digitally sign contracts and documents within the app. GovTech stated that each digital signature is identifiable and cryptographically linked to the signer, while signed documents are platform agnostic and can be viewed within the user's preferred system.
- United Overseas Bank (UOB) recently announced a pilot with 'Sign with Singpass' to allow a set of retail and corporate customers to confirm transactions and product applications. If the pilot is successful, UOB aims to expand the service to markets across the region from 2022. For markets without a national digital identity platform, UOB will use electronic signatures and authenticate the customer through two-factor authentication.
- Australia has launched the new Trusted Digital Identity Bill 2021 to establish a national framework for digital identification and digital identity.

## V. RECOMMENDATIONS

The observations gathered from the landscape overview in Sections I and II and the selection of case studies and interviews conducted with key NCAPEC stakeholders in Section III and IV support a set of policy recommendations below for APEC member economies to consider in facilitating regional cooperation for the broader use and adoption of e-signatures and digital signatures in APEC.

The implementation of these policy recommendations would be best served by APEC's Digital Economy Steering Group (DESG) which was created in 2018, and the Sub-committee on Standards and Conformance.

The main objective of the DESG is to foster the development of the digital economy and the internet, which includes e-commerce and digital trade. The DESG is also responsible for implementing APEC's Internet and Digital Economy Roadmap (AIDER), a framework which sets out to provide guidance on the facilitation of technological and policy exchanges among APEC member economies, including bridging the digital gap in the APEC region. The AIDER has eleven key areas, including:

- promoting interoperability;
- developing holistic government policy frameworks for the internet and digital economy;
- promoting coherence and cooperation of regulatory approaches affecting the internet and digital economy;
- promoting innovation and adoption of enabling technologies and services;
- enhancing trust and security in the use of ICTs; and
- facilitating e-commerce and advancing cooperation on digital trade.[129]

The DESG also performs the functions of the erstwhile Electronic Steering Group (ECSG) and reports on this work, specifically its work programme on e-commerce and trade-related digital economy, to APEC's Committee on Trade and Investments.

The Sub-committee on Standards and Conformance (SCSC) was established in 1994 to assist with reducing the adverse effects which divergent standards have on investment flows and trade in the Asia-Pacific region.

The SCSC consists representatives of each of the 21 APEC member economies who are selected from domestic agencies responsible for trade policy, standards, and conformance matters. Its main objectives include, among others:

- reducing technical barriers to trade and enhance market access through standards and conformance;
- aligning each of the APEC member economy's standards with international standards;

- promoting good regulatory practices in the preparation, adoption and application of standards, technical regulations and conformity assessment procedures;
- progressing mutual recognition arrangements for conformity assessment within the region; and
- encouraging participation in standards education and awareness programs to build capacity and capability to enhance the competitiveness of businesses, including micro, small and medium enterprises.[130]

The SCSC, through its objectives, also furthers the work of APEC's Committee on Trade and Investments, particularly APEC's agenda to achieve trade liberalization and trade facilitation.

Bearing in mind the relevance of the breadth and scope of the DESG's and the SCSC's work, the implementation of the policy recommendations would fall well within their remit, particularly through joint cooperation.

Overall, the recommendations are made with the view to improve legal and regulatory coherence and regional cooperation on e-signatures and digital signatures as part of the greater APEC agenda, by focusing on:

### **1.Establishing definition and terminology consistency for key basic terms to establish legal certainty and coherence.**

While most APEC member economies have established legal and regulatory frameworks governing the adoption, permissibility and use of e-signatures and digital signatures, there is a lack of definitional consistency as to basic terminology used among APEC member economies. This lack of definitional consistency is a key attribute impeding the establishment of consistent rules on the use of e-signatures and digital signatures.

This is no more prevalent than in the varied approaches taken to define the most basic of terms, 'e-signature' and 'digital signature'. Despite there being a marked difference between the two terms, they are often used interchangeably or conflated in the definition sections of legal instruments.

For example, the Republic of Korea's Digital Signature Act defines 'digital signature' to mean information in digital form affixed on, or logically combined with, an electronic document.[131] It has been generally accepted, however, that this definition would be more appropriately applied to 'e-signatures'. Several examples of incorrect use of terminology or jargon can be found in other APEC legislative texts.



While definition and terminology consistency are not only of semantic relevance but bears effect on the ease and speed with which cross-border transactions are conducted. The successful use of interoperable systems will also require definitional and terminology consistency, particularly regarding the consistent parameters for concepts such as validity and reliability.

As ‘best practice’, a minimalist approach to regulating the use and permissibility of e-signatures and digital signatures would perhaps be recommended. As indicated previously, this approach grants e-signatures and digital signatures the same status as traditional ‘wet’ handwritten signatures. In Australia, for example, ‘e-signature’ is defined simply without the imposition of any technological requirements, prescribed methods, or standards required to give legal effect e-signatures and digital signatures (as is required with the prescriptive and two-tiered approaches in relation specifically to qualified e-signatures).

APEC member economies, particularly those who have limited access to the necessary technologies and relevant resources, would benefit from the use and permissibility of e-signatures and digital signatures which are not required to comply with specific prescribed methods or standards for them to be given legal effect. These prescribed methods or standards could possibly act as a barrier to promoting the use and permissibility of e-signatures and digital signatures more broadly.

In addition, following a minimalist approach could possibly create efficiencies in speed and convenience for the promotion of interoperability of cross-border transactions among APEC member economies. Invariably, a system in which APEC member economies prescribe differing and heterogeneous methods or standards for qualifying e-signatures and digital signatures with legal effect could possibly act as a barrier to ensuring their broader use in effecting transactions between contracting parties based in different jurisdictions.

Above all, APEC member economies should be encouraged to review and amend their e-signature legal instruments with the view to extending the use cases permitted for affixing e-signatures, the appropriate dispensing of the physical attendance requirement, and to reconsider the requirement to affix traditional wet signatures in certain cases. In addition, the rules and requirements governing local platforms should be revised appropriately to allow for the use of alternative e-signing platform service providers.

In this regard, a public-private sector expert group could be established within the APEC DESG to proffer advice to APEC member economies on the review and amendment of their preexisting e-signature legal and regulatory frameworks. Further, APEC member economy Ministers responsible for trade, should be encouraged to issue a joint statement setting out their support for extending e-signature usage capacity, and to harness cross-border trade efficiencies.

## **2. Establishing a unified APEC approach to extending temporary COVID-19 relief beyond the pandemic.**

The response to the COVID-19 pandemic has been varied amongst APEC member economies. In particular, divergent approaches have been taken regarding the use and permissibility of e-signatures and digital signatures to conduct e-commerce transactions in place of ordinary in-person business operations curtailed or prohibited by social distancing policies.

As a first response, some APEC member economies have relaxed laws and regulations prohibiting the use of e-signatures and digital signatures for certain classes of documents and transactions. This is evident in Australia and New Zealand, where exceptions to laws and regulations which prohibit the use of e-signatures and digital signatures have been created, even if just temporarily. The majority of the APEC member economies, however, appear to have made no attempts to implement such measures.

Agreement and cooperation as to temporary COVID-19 relief measures, particularly in relation to effecting and facilitating cross-border transactions, would assist with the ease and speed with which these types of transactions are conducted and would also provide the necessary legal certainty and coherence for the facilitation of trade regionally.

As ‘best practice’, and in the long-term, extending temporary COVID-19 relief measures to apply more permanently will provide further clarity on the use and permissibility of e-signatures, together with the creation of efficiencies, such as speed convenience. This approach, for example, is being taken in Australia through the Corporations Amendment (Virtual Meetings and Electronic Communications) Bill 2020 (Cth).

It is perhaps important to point out that APEC member economies should, in relaxing the laws and regulations prohibiting the use of e-signatures and digital signatures, also consider broadening the categories of entities to whom the exemptions would be applicable. For example, the temporary COVID-19 relief measures introduced in Australia only applied to companies, thus limiting the possible efficiencies created by a broader category of entities making use of e-signatures and digital signatures.

## **3. Develop or upgrade paperless trade systems to enable interoperability amongst APEC member economies.**

Interoperable systems established between APEC member economies would create efficiencies of convenience and speed and would facilitate cross-border trade. APEC member economies should therefore develop policies and strategies to ensure greater cooperation across the APEC region in developing or upgrading paperless trade systems to enable interoperability in support of cross-border transactions.

While the FAFCTP provides a roadmap for developing or upgrading interoperability of paperless trade systems in Asia and the Pacific, it only came into force in February 2021 and has a long way to go in achieving its aims. In addition, it is only open to the 53 member states in Asia and the Pacific region, and as such excludes North America.

Greater cooperation and regionally coordinated efforts among APEC member economies in developing or upgrading paperless trade systems to enable interoperability would therefore also act in support of the efforts being coordinated and executed through the FAFCTP and ASEAN.

In addition to taking efforts to develop or upgrade interoperable systems amongst APEC member economies, efforts should be expended on discussions surrounding the development, implementation and use of DIS. This is especially so as DIS would act to reduce the reliance on the use of traditional 'wet' signatures to sign documents and effect transactions and would thus encourage the broader use of e-signatures and digital signatures.

#### **4. Create and promote educational initiatives on the import and use of e-signatures and digital signatures**

The uptake of e-signatures and digital signatures is sometimes thwarted by ingrained cultural norms and perceptions prevalent in APEC member economies. These norms and perceptions may, for example, impact the manner and extent to which e-signatures and digital signatures are used by individuals and businesses alike. Of more concern, particularly with reference to Recommendation 5 below, is the extent to which local authorities, such as regulators and government agencies and departments, accept e-signatures and digital signatures.

APEC member economies should therefore be encouraged to create and promote educational initiatives which educate persons, government agencies and businesses alike on the extent to which e-signatures and digital signatures may be used, the exceptions to their use, and how they may be used practically through e-signing platforms, such as DocuSign and Adobe Sign.

#### **5. Encourage local authorities to accept electronic documents and records affixed with e-signatures and digital signatures, such as email approvals, in lieu of traditional 'wet' signatures, specifically where e-signature and digital signature use is permitted by law.**

It has been observed in a number of APEC member economies that despite the use and permissibility of e-signatures and digital signatures being mandated by law, local authorities nevertheless require physical attendance and traditional 'wet' signatures to be affixed to documents or to execute transactions as a matter of market practice.

Local authorities, such as regulators and other governmental agencies and departments, should be encouraged to accept the affixing of e-signatures and digital signatures, and should develop clear guidance on acceptance of e-signatures or be provided with the necessary tools and technologies to make this a possibility.

Such efforts would also support the development of a hybrid model which ensures that both traditional and digital forms of affixing signatures to documents and executing transactions are available. This is especially relevant to APEC member economies with low smartphone penetration and low rates of new technology adoption.

## **6. Promote and improve wider accessibility to e-signing online platforms, particularly taking into account their high costs which can act as a barrier to their use by SMEs.**

Given their more prevalent and increased use, particularly during the COVID-19 pandemic, APEC member economies should promote and improve broader accessibility to e-signing platforms and software, such as DocuSign and Adobe Sign.

The use of DocuSign and Adobe Sign has become particularly crucial for businesses who have established offices in multiple countries or who frequently enter into and execute cross-border transactions. Ultimately, these e-signing platforms assist with minimizing cases of dispute and ensure that operations are standardized and that documents are executed with ease.

However, it is worth noting NCAPEC stakeholders have indicated that online e-signing service providers are costly software platforms, which in many cases are unaffordable for SMEs. APEC member economies should therefore develop policies and strategies which focus on minimizing the costs of using such e-signing platforms or source similar software which provide the same functionality at lower cost.

## **7. Develop digital identity systems**

Looking forward, in addition to taking efforts to develop or upgrade interoperable systems amongst APEC member economies, the development of Digital Identification Systems (DIS) would act to reduce reliance on the use of traditional 'wet' signatures and promote broader use and permissibility of e-signatures and digital signatures. DIS are usually described as systems which create and implement processes for validating, enrolling, and authenticating the attributes and credentials that uniquely identify individuals.[132]

More broadly, DIS can be utilized in APEC member economies to broaden its citizens access to the formal financial sector to assist them in receiving and making payments digitally, in executing remittances, and in applying for personal and business loans.

DIS could possibly act to increase efficiency, enhance effectiveness, identify new ways of providing financial services, and overall would minimize the risk of false identification. [133]

There are, however, several barriers to the successful implementation of DIS tools. These barriers include cost implications as DIS require large amounts of investment to both develop and maintain their complex and technical nature. In spite of these potential barriers, several DIS have been developed, or are in the process of being implemented, in some APEC member economies, including Japan, Malaysia, Singapore, and the Republic of Korea.[134]

To tackle these issues, in 2021, Global Legal Entity Identifier Foundation (GLEIF) unveiled the issuance and technical infrastructure models for its verifiable LEI (vLEI) system. A vLEI is a secure digital attestation of a conventional LEI, Legal Entity Identifier

One of the examples that this innovation permits is standardizing the way in which a legal entity's LEI code could be embedded in digital certificates. Moreover, the new infrastructure ensures that all vLEIs are traceable, through a cryptographically protected chain of credentials, back to their source LEI record in the Global LEI Index. Also, in February 2022, GLEIF has published the vLEI Ecosystem Governance Framework. The Framework defines the vLEI operational model and describes how the new ecosystem's range of vLEI issuing stakeholders will qualify for and perform their roles in the Global LEI System to use digital credentials.[135]

A comprehensive discussion on DIS in the APEC region requires a detailed consideration of the various factors it involves, and ultimately falls outside the specific remit of this report. However, looking forward, further discussion on the use and implementation of DIS in the APEC region is warranted.

## FOOTNOTES

### Page 5

- [1] Klaus Schwab, *The Fourth Industrial Revolution* (Penguin UK 2017).
- [2] UNESCAP. *Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific* (2019) iv. Available at <https://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific>.

### Page 6

- [3] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 5. Available at: [http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).
- [4] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 5. Available at: [http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

### Page 7

- [5] Arab Monetary Fund: Arab Regional Fintech Working Group, 'Digital Identity and e-KYC Guidelines for the Arab Region' (2020) 8 < <https://www.amf.org.ae/sites/default/files/Files/Digital%20Identy%20Booklet.pdf>. > accessed 28 July 2021.
- [6] World Bank Group: ID4D, 'Digital ID and the Data Protection Challenge' (October 2019) 2 < <http://documents.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf> > accessed 28 July 2021).
- [7] Chris Burt, 'Digital identity systems around Asia compared as [Chinese Taipei] seeks path forward' (Biometric.com 17 February 2021) < [https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-\[chinesetaipei\]-seeks-path-forward](https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-[chinesetaipei]-seeks-path-forward) > accessed 28 July 2021. Also see UNCTAD, 'Digital identity for trade and development: TrainforTrade case studies in South East Asia' (2020) < [https://unctad.org/system/files/official-document/dtlkdb2020d1\\_en.pdf](https://unctad.org/system/files/official-document/dtlkdb2020d1_en.pdf) > accessed on 28 July 2021.

### Page 9

- [8] Klaus Schwab, *The Fourth Industrial Revolution* (Penguin UK 2017).
- [9] UNESCAP. *Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific* (2019) iv. Available at <https://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific>.

**Page 10**

[10] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 5. Available at:

[http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

[11] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 5. Available at:

[http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

[12] UNESCAP. Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (2019) iv. Available at

<https://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific>.

[13] UNCITRAL Model Law on Electronic Signatures 2001, art 2(b). Available at:

[https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic\\_signatures](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures).

[14] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 4. Available at:

[http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

[15] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 4. Available at:

[http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

**Page 11**

[16] UNCITRAL Model Law on Electronic Signatures 2001, art 2(c). Available at:

[https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic\\_signatures](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures).

[17] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 4. Available at:

[http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

[18] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 4. Available at:

[http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

[19] e-ASEAN Reference Framework for Electronic Commerce Legal Infrastructure 2001 3. Available at [https://www.asean.org/wp-](https://www.asean.org/wp-content/uploads/images/2012/Economic/TELMIN/e-Asean%20Reference%20Framework.pdf)

[content/uploads/images/2012/Economic/TELMIN/e-Asean%20Reference%20Framework.pdf](https://www.asean.org/wp-content/uploads/images/2012/Economic/TELMIN/e-Asean%20Reference%20Framework.pdf).

[20] UNESCAP. Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (2019) iv. Available at

<https://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific>.

[21] 3] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 4. Available at:

[http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf)

[22] e-ASEAN Reference Framework for Electronic Commerce Legal Infrastructure 2001 3. Available at [https://www.asean.org/wp-](https://www.asean.org/wp-content/uploads/images/2012/Economic/TELMIN/e-Asean%20Reference%20Framework.pdf)

[content/uploads/images/2012/Economic/TELMIN/e-Asean%20Reference%20Framework.pdf](https://www.asean.org/wp-content/uploads/images/2012/Economic/TELMIN/e-Asean%20Reference%20Framework.pdf).



**Page 12**

[23] See UNCITRAL. 'Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods' (2009) 2 for further discussion. Available at [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/08-55698\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/08-55698_ebook.pdf).

[24] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 4. Available at:

[http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

[25] UNCITRAL Model Law on Electronic Commerce 1996. Available at:

[https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic\\_commerce](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce).

[26] UNESCAP. Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific 2019 art 3(b). Available at

<https://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific>.

**Page 13**

[27] UNCITRAL Model Law on Electronic Signatures 2001. Available at:

[https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic\\_signatures](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures).

**Page 14**

[28] UNCITRAL Model Law on Electronic Transferable Records 2017. Available at:

[https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic\\_transferable\\_record](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_record).

[29] UN Convention on the Use of Economic Communications in International Contracts (New York, 2005). Available at:

[https://uncitral.un.org/en/texts/ecommerce/conventions/electronic\\_communications](https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications).

**Page 15**

[30] WTO. E-commerce negotiations: Members finalise "clean text" on e-signatures and authentication. Available at:

[https://www.wto.org/english/news\\_e/news21\\_e/ecom\\_20apr21\\_e.htm](https://www.wto.org/english/news_e/news21_e/ecom_20apr21_e.htm).

[31] World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) 4. Available at:

[http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

**Page 17**

[32] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, art. 6

[33] See 'What is the difference between signing, ratification, and accession of UN treaties?' < <https://ask.un.org/faq/14594> > accessed 26 July 2021.

[34] Phet Sengpunya 'ASEAN E-Commerce Legal Framework and Alignment of Lao PDR: A Review' (2019) 6(3) *Lentera Hukum* 381

[35] ASEAN Vision 2020. Available at [https://asean.org/?static\\_post=asean-vision-2020](https://asean.org/?static_post=asean-vision-2020).

[36] ASEAN. e-ASEAN Reference Framework for Electronic Commerce Legal Infrastructure 2001. Available at <https://www.asean.org/wp-content/uploads/images/2012/Economic/TELMIN/e-Asean%20Reference%20Framework.pdf>.



## Page 18

- [37] ASEAN. e-ASEAN Framework Agreement 2012. Available at [https://asean.org/?static\\_post=e-asean-framework-agreement](https://asean.org/?static_post=e-asean-framework-agreement).
- [38] ASEAN. ASEAN Work Programme on Electronic Commerce 2017 – 2025. Available at <https://asean.org/asean-economic-community/sectoral-bodies-under-the-purview-of-aem/e-commerce/#4f3ca15fff4dc1aaf>.
- [39] ASEAN. ASEAN Economic Community Blueprint 2025. Available at [https://www.asean.org/storage/2016/03/AECBP\\_2025r\\_FINAL.pdf](https://www.asean.org/storage/2016/03/AECBP_2025r_FINAL.pdf).
- [40] ASEAN. ASEAN Economic Community Blueprint 2025 24. Available at [ASEAN-2025-Forging-Ahead-Together-final.pdf](#).
- [41] APEC. APEC Guidance for Electronic Commerce (Stage 3): Lessons Learnt of Implementation of APEC Strategies and Actions toward a Cross-Border Paperless Trading Environment: Final Report 2010 6. Available at <https://www.apec.org/Publications/2010/12/APEC-Guidance-for-Electronic-Commerce-Stage-3-December-2010>.
- [42] APEC. APEC Blueprint for Action on Electronic Commerce 1998. Available at [https://www.apec.org/Meeting-Papers/Leaders-Declarations/1998/1998\\_aelm/apec\\_blueprint\\_for.aspx](https://www.apec.org/Meeting-Papers/Leaders-Declarations/1998/1998_aelm/apec_blueprint_for.aspx).
- [43] APEC. Assessment Report on Paperless Trading in APEC Economies 2005. Available at <https://www.apec.org/Publications/2005/09/Assessment-Report-on-Paperless-Trading-of-APEC-Economies>.
- [44] APEC. Public Key Infrastructure Guidelines: Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross-jurisdiction eCommerce 2005. Available at <https://www.apec.org/Publications/2005/05/Public-Key-Infrastructure-PKI-Guidelines-Guidelines-for-Schemes-to-Issue-Certificates-Capable-of-Bei>.
- [45] APEC. Best Practices on Paperless Trading to Facilitate Cross-border Trade in the APEC Region 2010. Available at <https://www.apec.org/Publications/2010/06/Assessment-and-Best-Practices-on-Paperless-Trading-to-Facilitate-Cross-Border-Trade-in-the-APEC-Regi>.
- [46] APEC. Second Trade Facilitation Action Plan 2007. Available at <https://www.apec.org/Achievements/Group/Committee-on-Trade-and-Investment-2/Sub-Committee-on-Customs-Procedures-4#:~:text=APEC's%20Second%20Trade%20Facilitation%20Action,in%20the%20period%202007%2D2010>.
- [47] APEC. Investment Facilitation Action Plan 2008. Available at <https://www.apec.org/Achievements/Group/Committee-on-Trade-and-Investment-2/Investment-Experts-Group-1>.
- [48] APEC. APEC Guidance for Electronic Commerce (Stage 3): Lessons Learnt of Implementation of APEC Strategies and Actions toward a Cross-Border Paperless Trading Environment: Final Report 2010 6. Available at <https://www.apec.org/Publications/2010/12/APEC-Guidance-for-Electronic-Commerce-Stage-3-December-2010>.
- .

**Page 19**

- [49] APEC. Guidelines for Paperless Environment in the APEC region 2010. Available at <https://www.apec.org/Publications/2010/05/Guidelines-for-Paperless-Business-Environment-in-the-APEC-Region>.
- [50] APEC. Guidelines for Paperless Environment in the APEC region 2010 10. Available at <https://www.apec.org/Publications/2010/05/Guidelines-for-Paperless-Business-Environment-in-the-APEC-Region>.
- [51] APEC. Cross-border E-commerce Facilitation Agreement 2017. Available at [https://www.apec.org/Meeting-Papers/Annual-Ministerial-Meetings/2017/2017\\_amm/Annex-A](https://www.apec.org/Meeting-Papers/Annual-Ministerial-Meetings/2017/2017_amm/Annex-A).
- [52] APEC. Priorities for APEC Chile 2019. Available at <https://www.apecchile2019.cl/apec/apec-chile/priorities-apec-2019>.
- [53] The project proposal is available at <https://aimp2.apec.org/sites/PDB/Lists/Proposals/DispForm.aspx?ID=2696>. Further proposal documents is available at <http://mddb.apec.org/Pages/search.aspx?setting=ListMeeting&DateRange=2021/05/01%2C2021/05/end&Name=Utilizing%20Digital%20Technology%20in%20the%20Field%20of%20Trade%20Facilitation%20Under%20the%20Current%20COVID-19%20Pandemic%20and%20Beyond%3A%20Best-Practices%20Sharing%20Workshop%20-%20Trade%20Facilitation%20Through%20Trade%20Platforms%202021>.

**Page 20**

- [54] Stephen Mason. Electronic Signatures in Law (4th edn, University of London: London) 119. Available at: <https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic signatures>.

**Page 21**

- [55] Stephen Mason. Electronic Signatures in Law (4th edn, University of London: London) 116. Available at: <https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic signatures>.
- [56] Stephen Mason. Electronic Signatures in Law (4th edn, University of London: London) 122. Available at: <https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic signatures>.
- [57] Electronic Transactions Act 1999, s 10.

**Page 22**

- [58] Electronic Transactions Act 1999, s 5.
- [59] Electronic Transactions Act 1999, s 5.
- [60] Electronic Transactions Act 1999, s 5.

**Page 23**

- [61] Corporations (Coronavirus Economic Response) Determination (No. 3) 2020, s 127.  
 [62] Treasury Laws Amendment (2021 Measures No. 1) Act 2021. Available at:  
<https://www.legislation.gov.au/Details/C2021A00082>.

**Page 24**

- [63] See <https://treasury.gov.au/consultation/c2020-119106> for more information.  
 [64] Electronic Transactions Act, Revised Edition 2008, art 2.  
 [65] Electronic Transactions Act, Revised Edition 2008, art 17.

**Page 25**

- [66] Electronic Transaction sAct, Revised Edition 2008, art 20.  
 [67] Personal Information and Electronic Documents Act 2000, s 31(1).  
 [68] Personal Information and Electronic Documents Act 2000, s 31(1).  
 [69] Personal Information and Electronic Documents Act 2000, s 31(1) read with s48(2).  
 [70] Uniform Electronic Commerce Act 1999, s 1(b).

**Page 26**

- [71] Law 19799 Electronic Documents, Electronic Signature and Certification Services of Such Signature, art 2(f).  
 [72] Law 19799 Electronic Documents, Electronic Signature and Certification Services of Such Signature, art 2(g).  
 [73] Law 19799 Electronic Documents, Electronic Signature and Certification Services of Such Signature, art 2(e).  
 [74] Law 19799 Electronic Documents, Electronic Signature and Certification Services of Such Signature, art 4.

**Page 27**

- [75] Electronic Signature Law of the People's Republic of China, 2004, art 13.

**Page 28**

- [76] Electronic Transactions Ordinance, ch. 533, s6.

**Page 29**

- [77] Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions  
 [78] Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions  
 [79] Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions  
 [80] Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions

**Page 30**

- [81] Electronic Signatures and Certification Act No. 102 of 31 May 2000, art 2(1).
- [82] Electronic Signatures and Certification Act No. 102 of 31 May 2000, art 3.
- [83] Digital Signature Act, Act No. 17354, 9 June 2020.

**Page 31**

- [84] Digital Signature Act, No. 14577 of 14 March 2017, art 2
- [85] Electronic Commerce Act, No. 658 of 31 August 2006, s. 9

**Page 32**

- [86] Electronic Commerce Act, No. 658 of 31 August 2006, s. 9.
- [87] Digital Signature Act, No. 562 of 30 June 1997, art 2.
- [88] Digital Signature Act, No. 562 of 30 June 1997, art 62.

**Page 33**

- [89] Code of Commerce, art 89.
- [90] Code of Commerce, title 2, ch 1.
- [91] Code of Commerce, art 97.

**Page 34**

- [92] Code of Commerce, art 98.
- [93] Contract and Commercial Law Act 2017, s 209.
- [94] Contract and Commercial Law Act 2017, s 226.
- [95] Contract and Commercial Law Act 2017, s 228.

**Page 35**

- [96] Contract and Commercial Law Act 2017, s 218 read with s 218B as inserted by s 3 of the COVID-19 Response (Further Management Measures) Legislation Act 2020 (2020 No. 13).
- [97] See COVID-19 Response (Requirements For Entities—Modifications and Exemptions) Act 2020 (No. 14) available at:  
<https://www.legislation.govt.nz/act/public/2020/0014/latest/LMS344839.html>.
- [98] COVID-19 Response (Requirements For Entities—Modifications and Exemptions) Act 2020 (No. 14), s10A(1).
- [99] COVID-19 Response (Requirements For Entities—Modifications and Exemptions) Act 2020 (No. 14), s10A(1).

**Page 36**

- [100] Electronic Transaction Act No. 38 of 2021, pt I, s 3(1).
- [101] Electronic Transaction Act No. 38 of 2021, pt I, s 3(1).
- [102] Electronic Transaction Act No. 38 of 2021, pt I, s 3(1).
- [103] Electronic Transaction Act No. 38 of 2021, pt I, s 3(1).

**Page 36 continued**

[104] Electronic Transaction Act No. 38 of 2021, pt VI, s 25(4).

[105] Electronic Transaction Act No. 38 of 2021, pt I, s 3(5).

**Page 37**

[106] Digital Certificates and Signatures Law No 27269 and APEC, 'The Peruvian Legal Framework as Support of the Paper Less Capacity Building – Successful Experiences in the Public Sector' 2007/ECSG/SYM/013. Available at [http://mddb.apec.org/documents/2007/ECSG/SYM1/07\\_ecsg\\_sym1\\_013.pdf](http://mddb.apec.org/documents/2007/ECSG/SYM1/07_ecsg_sym1_013.pdf).

[107] Digital Certificates and Signatures Law No 27269 and APEC, 'The Peruvian Legal Framework as Support of the Paper Less Capacity Building – Successful Experiences in the Public Sector' 2007/ECSG/SYM/013. Available at [http://mddb.apec.org/documents/2007/ECSG/SYM1/07\\_ecsg\\_sym1\\_013.pdf](http://mddb.apec.org/documents/2007/ECSG/SYM1/07_ecsg_sym1_013.pdf).

**Page 38**

[108] Electronic Commerce Act, No. 8792 of Jun. 14, 2000, s. 5

[109] Rules on Electronic Evidence, of Aug. 1, 2001, s. 1

**Page 39**

[110] Federal Law No. 63-FZ, art 2(1).

**Page 40**

[111] Electronic Transaction Act, Revised edition 2011, art 2.

[112] Electronic Transaction Act, Revised edition 2011, art 10.

[113] Electronic Transaction Act, Revised edition 2011, art 18

[114] Electronic Transaction Act, Revised edition 2011, third schedule

**Page 41**

[115] Electronic Signatures Act, of Nov 2001, art 2.

[116] Electronic Signatures Act, of Nov 2001, art 2.

**Page 43**

[117] Electronic Transaction Act, of December 2001, s. 9.

[118] ETDA Recommendation on ICT Standard for Electronic Transactions: Electronic Signature Guideline, of May 2020, p.4.

[119] Electronic Transaction Act, of December 2001, s. 26.

[120] ETDA Recommendation on ICT Standard for Electronic Transactions: Electronic Signature Guideline, of May 2020, p.4.

[121] Electronic Transaction Act, of December 2001, s. 28.

**Page 44**

[122] United States Electronic Signatures in Global and National Commerce Act, code § 7006(5).

**Page 45**

[123] Law on E-Transactions, No.51 of 2005, art 24.

[124] Decree No. 130/2018/ND-CP.

**Page 50**

[125] <https://www.japantimes.co.jp/news/2020/06/30/national/hanko-seal-alternatives/>

**Page 51**

[126] See COVID-19 Response (Requirements For Entities—Modifications and Exemptions) Act 2020 (No. 14) available at:

<https://www.legislation.govt.nz/act/public/2020/0014/latest/LMS344839.html>.

[127] COVID-19 Response (Requirements For Entities—Modifications and Exemptions) Act 2020 (No. 14), s10A(1)

**Page 52**

[128] DocuSign Investor Presentation Summer 2021, available at:

<https://investor.docusign.com/investors/events-and-presentations/default.aspx>

**Page 54**

[129] APEC, 'Digital Economy Steering Group' <

<https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group>> accessed 26 July 2021.

**Page 55**

[130] APEC, 'Sub-Committee on Standards and Performance' <

<https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Sub-Committee-on-Standards-and-Conformance>> accessed on 26 July 2021.

[131] Digital Signature Act, No. 14577 of Mar. 14, 2017, art 2.

**Page 59**

[132] Arab Monetary Fund: Arab Regional Fintech Working Group, 'Digital Identity and e-KYC Guidelines for the Arab Region' (2020) 8 <

<https://www.amf.org.ae/sites/default/files/Files/Digital%20Identity%20Booklet.pdf>.

> accessed 28 July 2021.

**Page 60**

[133] World Bank Group: ID4D, 'Digital ID and the Data Protection Challenge' (October 2019) 2 <

<http://documents.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf>

> accessed 28 July 2021).

[134] Chris Burt, 'Digital identity systems around Asia compared as [Chinese Taipei] seeks path forward' (Biometric.com 17 February 2021) <

[https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-\[Chinese Taipei\]-seeks-path-forward](https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-[Chinese-Taipei]-seeks-path-forward)> accessed 28 July 2021. Also see UNCTAD, 'Digital identity for trade and development: TrainforTrade case studies in South East Asia' (2020) < [https://unctad.org/system/files/official-document/dtlkdb2020d1\\_en.pdf](https://unctad.org/system/files/official-document/dtlkdb2020d1_en.pdf)> accessed on 28 July 2021.

[135] Global Legal Entity Identifier Foundation (GLEIF), 'The Birth of the vLEI: A New Dawn in Digital ID for Legal Entities Everywhere' (gleif.com February 2022) <

<https://www.gleif.org/en/newsroom/blog/the-birth-of-the-vlei-a-new-dawn-in-digital-id-for-legal-entities-everywhere> > accessed 17 February 2022.

## REFERENCES

APEC. Assessment Report on Paperless Trading in APEC Economies 2005. Available at <https://www.apec.org/Publications/2005/09/Assessment-Report-on-Paperless-Trading-of-APEC-Economies>.

APEC. Best Practices on Paperless Trading to Facilitate Cross-border Trade in the APEC Region 2010. Available at <https://www.apec.org/Publications/2010/06/Assessment-and-Best-Practices-on-Paperless-Trading-to-Facilitate-Cross-Border-Trade-in-the-APEC-Regi>.

APEC. APEC Blueprint for Action on Electronic Commerce 1998. Available at [https://www.apec.org/Meeting-Papers/Leaders-Declarations/1998/1998\\_aelm/apec\\_blueprint\\_for.aspx](https://www.apec.org/Meeting-Papers/Leaders-Declarations/1998/1998_aelm/apec_blueprint_for.aspx).

APEC. Cross-border E-commerce Facilitation Agreement 2017. Available at [https://www.apec.org/Meeting-Papers/Annual-Ministerial-Meetings/2017/2017\\_amm/Annex-A](https://www.apec.org/Meeting-Papers/Annual-Ministerial-Meetings/2017/2017_amm/Annex-A).

APEC. Digital Economy Steering Group. < <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group> > accessed 26 July 2021.

APEC. APEC Guidance for Electronic Commerce (Stage 3): Lessons Learnt of Implementation of APEC Strategies and Actions toward a Cross-Border Paperless Trading Environment: Final Report 2010 6. Available at <https://www.apec.org/Publications/2010/12/APEC-Guidance-for-Electronic-Commerce-Stage-3-December-2010>.

APEC. Guidelines for Paperless Environment in the APEC region 2010. Available at <https://www.apec.org/Publications/2010/05/Guidelines-for-Paperless-Business-Environment-in-the-APEC-Region>.

APEC. Priorities for APEC Chile 2019. Available at <https://www.apecchile2019.cl/apec/apec-chile/priorities-apec-2019>.

APEC. Public Key Infrastructure Guidelines: Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross-jurisdiction eCommerce 2005. Available at <https://www.apec.org/Publications/2005/05/Public-Key-Infrastructure-PKI-Guidelines-Guidelines-for-Schemes-to-Issue-Certificates-Capable-of-Bei>.



APEC. Second Trade Facilitation Action Plan 2007. Available at <https://www.apec.org/Achievements/Group/Committee-on-Trade-and-Investment-2/Sub-Committee-on-Customs-Procedures-4#:~:text=APEC's%20Second%20Trade%20Facilitation%20Action,in%20the%20period%202007%2D2010.>

APEC. Sub-Committee on Standards and Performance. <  
<https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Sub-Committee-on-Standards-and-Conformance>>.

Arab Monetary Fund: Arab Regional Fintech Working Group. Digital Identity and e-KYC Guidelines for the Arab Region 2020 Available at <  
<https://www.amf.org.ae/sites/default/files/Files/Digital%20Identy%20Booklet.pdf>.

ASEAN. ASEAN Economic Community Blueprint 2025. Available at  
[https://www.asean.org/storage/2016/03/AECBP\\_2025r\\_FINAL.pdf](https://www.asean.org/storage/2016/03/AECBP_2025r_FINAL.pdf).

ASEAN. ASEAN Vision 2020. Available at [https://asean.org/?static\\_post=asean-vision-2020](https://asean.org/?static_post=asean-vision-2020).

ASEAN. ASEAN Work Programme on Electronic Commerce 2017 – 2025. Available at  
<https://asean.org/asean-economic-community/sectoral-bodies-under-the-purview-of-aem/e-commerce/#4f3ca15fff4dc1aaf>.

ASEAN . e-ASEAN Framework Agreement 2012. Available at [https://asean.org/?static\\_post=e-asean-framework-agreement](https://asean.org/?static_post=e-asean-framework-agreement).

Burt C. Digital identity systems around Asia compared as Taiwan seeks path forward. (Biometric.com 17 February 2021). <<https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-taiwan-seeks-path-forward>>.

e-ASEAN Reference Framework for Electronic Commerce Legal Infrastructure 2001. Available at <https://www.asean.org/wp-content/uploads/images/2012/Economic/TELMIN/e-Asean%20Reference%20Framework.pdf>.

Global Trade Review. Analysis: The impact of the UNESCAP agreement on cross-border paperless trade (2021). Available at: <https://www.gtreview.com/news/asia/analysis-the-impact-of-the-unescap-agreement-on-cross-border-paperless-trade/>.

Mason S. Electronic Signatures in Law (4th edn, University of London: London). Available at: <https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic signatures>.

Schwab K. 'The Fourth Industrial Revolution' (Penguin UK 2017).

Phet Sengpunya 'ASEAN E-Commerce Legal Framework and Alignment of Lao PDR: A Review' (2019) 6(3) *Lentera Hukum* 375 – 396.

UN Convention on the Use of Economic Communications in International Contracts (New York, 2005). Available at: [https://uncitral.un.org/en/texts/ecommerce/conventions/electronic\\_communications](https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications).

UNCITRAL Model Law on Electronic Commerce 1996. Available at: [https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic\\_commerce](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce).

UNCITRAL Model Law on Electronic Signatures 2001. Available at: [https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic\\_signatures](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures).

UNCITRAL Model Law on Electronic Transferable Records 2017. Available at: [https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic\\_transferable\\_record](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_record).

UNESCAP. Digital trade facilitation in Asia and the Pacific. Studies in Trade, Investment and Innovation (2017), No. 87. Sales No. E.18.II.F.10. Available at: <https://www.unescap.org/publications/digital-trade-facilitationasia-and-pacific-studies-trade-investment-and-innovation-87>.

UNESCAP. Draft road map for the implementation of the substantive provisions in the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (2018). Available at [https://www.unescap.org/sites/default/files/E\\_PTA\\_IISG2018\\_CRP1E.pdf](https://www.unescap.org/sites/default/files/E_PTA_IISG2018_CRP1E.pdf).

UNESCAP. Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (2019). Available at <https://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific>.

UNESCAP. Frequently Asked Questions (FAQ) on the Framework Agreement on Facilitation of Crossborder Paperless Trade in Asia and the Pacific (2020). Available at: [https://www.unescap.org/sites/default/d8files/knowledge-products/FAQ%20on%20the%20Framework%20Agreement\\_Dec%202020.pdf](https://www.unescap.org/sites/default/d8files/knowledge-products/FAQ%20on%20the%20Framework%20Agreement_Dec%202020.pdf).

UNESCAP. Accelerating Trade Digitisation in Times of the Pandemic (2021). Available at: <https://www.unescap.org/op-ed/accelerating-trade-digitalization-times-pandemic#>.

UNCITRAL. 'Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods' (2009) 2 for further discussion. Available at [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/08-55698\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/08-55698_ebook.pdf).

UN Treaty Collection. Chapter X International Trade and Development. Available at: [https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=X-20&chapter=10&clang=\\_en](https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=X-20&chapter=10&clang=_en).

World Bank Group: ID4D. Digital ID and the Data Protection Challenge October 2019. Available at <http://documents.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf>.

World Economic Forum, 'Making deals in cyberspace: What's the problem' White Paper (2017) Available at: [http://www3.weforum.org/docs/WEF\\_White\\_Paper\\_Making\\_Deals\\_in\\_Cyberspace.pdf](http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf).

National Center for Asia Pacific Economic Cooperation  
Working Group on E-Signatures

---