WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Making Deals in Cyberspace: What's the Problem ?

October 2017

World Economic Forum®

REF 111017 - case 00036074

Table of Contents

Introduction

In an analogue world, when two parties agree to a transaction on paper, proof of mutual consent regarding its terms may be necessary or desirable. Some transactions may require a signature to be valid. Paper-based documents have been used to support commercial transactions for centuries, whether in a national or a cross-border context. While broad consensus exists on the idea of paper-based documents and handwritten signatures, countries have different rules governing commercial activities, such as regulating a contract's execution, its conditions of validity, and what makes for legally binding proof of consent. The latter can require a notary or witness to attest to the identity of the person signing a document. Some conflict may arise, but generally businesses have learned to cope in the physical "offline" world, even if requires cumbersome formalities typically amplified by variations between countries.

Once transactions move online, however, the picture becomes more complex. Three general challenges apply for both national and international transactions. First, in countries where rules for electronic transactions (e-transactions) and laws for electronic signatures (e-signatures) are not in place, waits may occur if paper documents need to be signed. Second, parties need to find ways to ensure the people signing documents are who they say they are, without necessarily seeing them in person; or, that the transaction document in question has not been tampered with, copied or otherwise changed. Parties also need to have confidence that their information will not be misappropriated or details copied. The third and associated challenge is that the technologies and methods for electronically exchanging contractual information and authenticating documents are numerous. Unlike a physical signature or a stamp (which have changed little over the years), information and communication technologies for authentication and e-signatures can evolve rapidly.

The approaches taken towards resolving these challenges will vary by country. Although information contained in electronic data messages is legally admissible in many nations, approaches can vary. Countries can put in place different types of e-transaction laws, with different requirements for the legal value of an e-signature, or require various authentication processes. At present, no universal system of standards, technologies or regulations exists for e-transactions. However, because a major benefit of the digital economy is its efficacy in spanning borders – and, in shrinking the visibility gap between producers and consumers in electronic commerce (e-commerce) – business and government alike may seek after regulatory coherence or interoperability.

Among international institutions, the United Nations Commission on International Trade Law (UNCITRAL) has taken steps to increase the uniformity of countries' legal rules governing e-transactions, e-signatures and digital authentication. These include:

- UNCITRAL Model Law on Electronic Commerce (MLEC) (1996)
- UNCITRAL Model Law on Electronic Signatures (MLES) (2001)
- United Nations Convention on the Use of Electronic Communications in International Contracts (ECC) (2005)
- UNCITRAL Model Law on Electronic Transferable Records (MLETR) (2017)

To date, over 70 states have enacted the MLEC, while more than 30 have turned to the MLES as the basis for their national legislation, and 18 states have signed (and nine have ratified) the ECC.[1]

UNCITRAL model laws, though not legally binding, are designed to guide states in drafting legislation, while the ECC, as a treaty, is "hard law" that allows for less variation on formal adoption. Not surprisingly, enactment of national and subnational laws along the lines suggested by UNCITRAL is uneven, even among countries that have committed to the model law. A government may choose to enact elements it likes, and discard the others. For instance, several states have enacted the MLES without referring to its Article 12 on cross-border recognition of e-signatures. Consequently, e-commerce businesses confront a plethora of different laws and regulations to which they must comply.

Does the lack of conformity in national laws present a problem for cross-border e-transactions? Some might argue no. After all, millions of such transactions take place

daily despite these differences. Just as businesses cope with different national laws governing the verification of consent for offline transactions, they can do the same for online transactions. Moreover, only an insignificant number of transactions are ever challenged legally, and not all e-transactions require signatures or authentication – nor should they.

However, others think that problems already exist or are looming on the horizon. Divergent domestic rules on e-transactions, e-signatures and authentication make cross-border digital activities more complex and raise the cost of doing business in multiple markets. Different legal frameworks can also lower confidence in e-commerce, since consumers may be uncertain of the relevant legal norm or standard. This is compounded by a lack of transparency in many countries on the grounds of an e-signature's acceptability for cross-border trade. Some industries have more reason than others to worry about the e-transaction regulatory landscape, notably banking, where the consequences of a fraudulent transaction, such as the unauthorized transfer of funds, are serious. Moreover, limited mutual recognition exists to date between different countries' authorities who certify e-signatures.

As more transactions move online and technology evolves, the picture is only likely to become more complex. E-commerce also holds promise for making trade more inclusive. Hence, some believe that greater cross-border cooperation must disseminate principles promoting e-transactions across borders, and increase uniformity of legal rules governing this space.

For those in the latter category, trade agreements have served as an obvious avenue for addressing the issue. A number of free trade agreements (FTAs) include provisions on e-transactions, e-signatures and authentication. Some regions, such as the European Union (EU), have advanced common e-signature regulations as part of a trade bloc. Member states of the United Nations Economic and Social Commission for Asia and the Pacific have adopted a framework agreement on paperless trade that outlines general legal principles which could help promote e-transaction interoperability. Some countries have suggested addressing e-transactions through the World Trade Organization's (WTO) ongoing work programme on e-commerce.

This White Paper aims to build the knowledge of current e-transaction and e-signature rules. It evaluates how these apply in national and international commercial contexts, and bridges perspectives from business, legal experts and trade policy-makers to deepen understanding on potential trade policy interventions that could boost regulatory coherence. The paper contributes to a World Economic Forum public-private dialogue series on best practices in e-commerce policy as part of a broader digital trade programme.

What's in a Name?

The terms "electronic signature", "digital signature", "digital authentication" and, increasingly, "digital identity" are sometimes used interchangeably; however, they do not mean the same thing. The four terms should be clarified before going further:

An electronic signature (e-signature) is a process of signalling intent, including acceptance, as to the content of an electronic record. Practically speaking, the technologies used for e-signatures include email addresses, enterprise IDs, personal ID numbers (PINs), biometric identification, social IDs, scanned copies of handwritten signatures and clickable "I accept" boxes.

A *digital signature*, or advanced e-signature, uses cryptography to scramble signed information into an unreadable format and decodes it again for the recipient (see Box 1). Specialized third parties, known as certification authorities (CAs), often provide certification services for verifying the signer's identity. In certain instances, some firms may choose to use their own systems.

Some jurisdictions, such as the EU, distinguish between digital signatures and qualified e-signatures (or qualified digital signatures). While both rely on encryption and CAs to identify the signer, the qualified e-signatures also require the signer to use a qualified signature creation device (QSCD), such as a smart card, token or cloud-based trust service. The QSCD verifies the digital identity and can only be given to users once they have passed a Know-Your-Customer (KYC) process.

Digital authentication refers variously to the techniques used to identify individuals, confirm a person's authority or prerogative, or offer assurance on the integrity of information. "Authentication" can mean different things in different national legal contexts, with the challenge of doing it remotely over networks. Digital authentication can rely on a varied set of factors, such as those concerning knowledge (e.g. passwords, answers to a pre-selected security question), ownership (e.g. possession of a one-time password) or inherence (e.g. biometric information). Depending on the level of security desired, a digital authentication system could be single-, double- or multi-factor.

Digital identity refers to a broader conception of the information used by a computer system to identify an agent, which is most frequently considered to be an individual but is also referred to as an entity, such as a corporation or a machine. Printed documents such as passports, national ID cards and driver's licences offer proof of a person's identity. Similarly, online electronic information can be linked to an individual or another entity to offer proof of identity.

Box 1: Digital Signatures and Certificates Explained

Digital signatures use public key encryption systems to encrypt and decrypt signed information. As a first step, the signer will delineate the relevant information to be signed, which then goes through the "hash function", a mathematical process that compresses the information into a unique format with its own code.

Computer software then uses the signer's "private key" – a large number produced by a formula – to create a digital signature based on the hash result. A private key is likely to be kept on a smart card or be accessible through a PIN. A "public key", mathematically related to the private key and used to unscramble the signed message, is more widely available. Moreover, if the cryptographic system is properly designed, it will be impossible to derive the private key from it.

A new hash function is computed from the signed information once it is received. The public key allows the verifier to check whether the digital signature was created using a corresponding private key. If the hash functions don't match, the document is considered to have been tampered with and the signature is invalidated.

CAs issue digital certificates verifying that a public key corresponds to a given identity, whether an individual or an organization, and attest that the prospective signer holds the corresponding private key. CAs should provide a certification practice statement (CPS) that defines how they maintain certificates within the public key infrastructure (PKI). The latter refers to the ecosystem of CAs in a given jurisdiction.

Digital certificates also play an important role in building trust in websites and online transaction platforms. Organizations will purchase a digital certificate from a trusted CA for services requiring a level of confidence, such as email, instant messaging or websites where credit card details are needed. When users go online, web browsers will detect the presence of a digital certificate and switch from an open session (http) to a secure session (https). Organizations can also purchase Extended Validation (EV) SSL certificates from CAs that add an extra layer of security by requiring a KYC check of the requestor.

Source: Authors/internal analysis

Digital identity management has become a foundational part of the digital economy. Digital identities enable remote interactions between individuals by providing key information about who they are. The term "digital identity" is broader in scope than digital authentication. Digital identity tools can be used for other purposes, such as for authorization and providing information, beyond simply authenticating a person's identity.

Interoperability is critical in managing digital identity systems; this is no different from the physical, offline world. Passports, for example, are based on standards agreed by the International Civil Aviation Organization to ensure these will be accepted worldwide.

To date, many digital identity systems rely on physical public ID systems managed by governments. In other words, they leverage existing government systems (which may be offline), but create an online digital dimension for e-transactions. The Aadhaar scheme uses unique 12-digit ID numbers issued by the Indian government to all the country's residents. IDs are associated with biometric and resident information stored on a central database. Aadhaar IDs can be used to open a bank account, for which banks use Aadhaar as part of the KYC process to identify and verify their clients' identities. Aadhaar IDs can also be used to issue e-tickets, among other exchanges requiring proof of identity.

Cross-border interoperability, however, has been a hurdle so far,[2] and not all stakeholders agree on common definitions of digital identity, let alone its governance.[3] New collaborative efforts continue to emerge, such as the World Identity Network, launched in July 2017 to catalyse the move towards universal ID and secure digital identification schemes. In addition, ID2020 is a public-private partnership committed to addressing the challenge of accelerating access to digital identity for the 1.1 billion people worldwide who lack any form of officially recognized ID. However, efforts to provide legal identity for all people, in pursuance of Sustainable Development Goal 16/Target 9, do not focus on commercial applications.

Having clarified the differences in the terms' meanings, the question of why this topic matters in the context of the current global economy can be examined.

Why this Matters: Taking stock of the e-transaction landscape

Electronic transactions have exploded over the past few decades. The United Nations Conference on Trade and Development (UNCTAD) estimates the value of business-to-business e-commerce exceeded $15 trillion in 2013, with business-to-consumer e-commerce at $1.2 trillion and expanding rapidly. The gross merchandise value of the cross-border e-commerce market was $300 billion in 2015, and is expected to grow by roughly 25% annually through 2020.[4] E-commerce can be particularly enabling for small businesses by expanding access to more customers. One study of developing-country firms found that while offline sellers mainly exported to one market, over 60% of sellers online were selling to two or more markets. New "microwork" platforms, such as Upwork and Freelancer, are also providing opportunities for entrepreneurs and businesses to sell services online.[5]

Underpinning aspects of this activity are legislative frameworks that recognize contracts or important documents can be concluded online, and that affirm the legal value of e-signatures and authentication. Ensuring that individuals can provide approval or consent online when downloading an e-book, checking out of a digital shopping cart or validating payrolls is a key commercial imperative for digital trade and exchange. E-signatures are an opportunity to speed up business processes, such as accounts receivable and accounts payable, and close deals faster by eliminating transaction barriers and invoicing issues. Signatures can be gathered in a matter of minutes,

increasing operational efficiency. According to Adobe, the office technology supplier Ricoh trimmed five days from its process for sales contracts by switching to the use of electronic and digital signatures. Further, while paper has no digital history, well-designed digital processes and e-signatures can show each action – when it was taken and by whom – thus helping to boost transparency.[6]

E-transaction and e-signature rules are also an important part of the regulatory framework for facilitating digital custom initiatives including submitting trade administration documents that are usually business-to-government. E-traders can particularly benefit where paperless trade reduces the cost and hassle of moving goods across borders. E-commerce typically involves smaller consignments with lower margins for transaction costs, and unexpected delays can leave consumers unsatisfied.[7]

Although many countries have e-transaction laws, regional disparities exist. According to UNCTAD, 145 countries have enacted such laws, of which 104 are developing or transitioning economies. Almost half, 46.3%, of African economies have adopted e-transactions laws, compared to 72% of Asian, 81.8% of Latin American and Caribbean and 97.6% of developed economies.[8] Further, some e-transaction laws only address e-signatures, without other important elements such as electronic contracting, which includes the time and place of dispatch and receipt; acknowledgement of receipt; party location and the use of automated message systems.

Box 2: Trust Challenges and Opportunities in E-Transactions

E-traders and entrepreneurs in developing countries may have difficulty fulfilling requirements for accessing a qualified e-signature from a CA in a developed country – often as a result of the investment made in due diligence processes and the associated risk. The CA will not deliver a trust product unless it can verify and document the existence of the company (for business e-signatures) and the identity and address of the e-signature holder. Companies and individuals can technically obtain a SwissSign qualified e-signature (SuisseID) through a public notary in Europe or a Swiss post office. To verify the company's existence, the Swiss CA can rely on a trustable online national company register of another EU or European Economic Association country. However, developing-country e-traders, namely those that may want to use qualified e-signatures to add security to a contract or web product, can face multiple challenges in doing so.

A complication arises when a country has no online company registry to prove the existence and beneficiaries of the company. Another complication is that the company register itself is neither secure nor authenticated (no SSL certificate, or a non-EV SSL certificate). The national registry may also be in a language other than English, making verification difficult. Similar problems may occur when verifying an individual's identity and address; national identity documents are often in the local language and difficult to verify, so holders are requested to have a valid passport. Proof of address typically must be translated into English.

All company and personal documents must then be authenticated. An entrepreneur would have to ensure the translation is done by a certified translator with accreditation that the CA can verify. Challenges can arise at this stage, too, as often no trustable online register of official translators exists. One solution is to have the documents translated by a translator known or recognized by the Swiss Embassy in that country, but this can involve additional costs and time. Once translations are acceptable, all the documents must be certified as true copies by a public notary. Again, developing countries often have no trustable online directory of public notaries. Proving the existence of a local public notary requires additional costs and, typically, a law firm's legal opinion attesting to the institution's existence in the country. An entrepreneur will usually have to find and use the services of a developed country's law firm having local representation, so that this firm's developed country office can provide a legal opinion based on the legal work forwarded to them by their branch in the entrepreneur's country.

After the verification process, international recognition of a given country's "certified true copies" may present an additional hurdle. As many developing countries are not signatories to The Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents (Apostille Convention), entrepreneurs based in these jurisdictions must "legalize" their documents, requiring the submission of copies and fees to one or more government institutions (e.g. the ministry of foreign affairs) for an additional stamp and layer of certification. Generally, whereas a qualified digital signature or EV SSL certificate may cost about $400 for a company based in a developed country, it could typically cost upwards of $2,000 (coupled with procedural delays) for an entrepreneur in a developing country. Even once the process has been followed, the relevant CA might not issue the trust product applied for, invoking a right to refuse applications in view of KYC rules.

In a bid to help ease this process, the International Trade Centre (ITC) has partnered with SwissSign to train four staff on KYC and identity verification, as well as on the technical and encryption processes for SwissSign products, as part of its e-solutions programme. The ITC is then able to verify the identity of the entrepreneurs it works with on the ground in developing countries, delivering the SuisseID to about 30 e-commerce advisers in Tunisia and Morocco who are mostly from the information and technology area and the services sector, as well as from the web agency or development companies. These individuals in turn can train more small and medium-sized enterprises on using qualified e-signatures. The programme offers a distinctive approach for bridging the gap in accessing qualified e-signatures for businesses from countries that are not part of the Organisation for Economic Co-operation and Development (OECD). The programme's main challenges were to ensure security and user identification when delivering the qualified signature creation device and pin codes. Some devices and associated SIM cards were not delivered or blocked at customs, or required documentation or duties to be imported.

Source: Contributed by the International Trade Centre based on its analysis.

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.[9] Most e-transaction laws are ill-equipped to deal with international aspects of e-commerce, such as choice of law, which can hinder the predictability of the applicable law.[10] The absence of mutual recognition and divergent rules between countries can create additional costs that may be particularly difficult for small and medium-sized enterprises (SMEs) to manage. Moreover, enabling legal frameworks may be in place in some cases, but experience in implementing among the judiciary is limited, with the overall effect of lowering confidence in the online transaction environment.

Another challenge facing all e-traders is securing consumer confidence.[11] Online trust is extremely valuable for e-commerce and contributes substantially to business success.[12] Smaller businesses in developing countries, however, may be more limited in accessing electronic trust tools and services, such as qualified digital signatures and EV SSL certificates that reassure foreign customers about a transaction's security (see Box 2). From this brief overview, the paper now looks at how countries typically approach e-transaction regulation, and then at international efforts to boost coherence, including from a trade perspective.

A Typology of National Implementation Efforts

The legal treatment of electronic and digital signatures is particularly relevant for e-commerce because it may be used as shorthand for the legal recognition of all e-transactions. In general, a state could be classified into one of three approaches regarding the laws governing e-signatures and digital authentication:

1. Minimalist (functional equivalence)
2. Prescriptive
3. Hybrid (two-tier)

Minimalist approach: States in this category give the same status to e-signatures as to handwritten ones, provided the technology used is appropriate for the purpose. An assessment of the method's reliability, based on certain pre-identified technology-neutral elements, is typically carried out only in case of dispute. Minimalist laws have been adopted in countries including the United States, Canada, New Zealand, Australia and Singapore. Often, jurisdictions adopting this approach belong to the common law tradition.

The approach offers significant benefits, such as flexibility and adaptability to technological developments and needs, and is generally business- and consumer-friendly. Minimalist laws tend to limit cross-border friction by accepting all forms of electronic or digital signatures (usually as long as parties agree on the form). Moreover, prior consent is obtained to conduct business electronically, and the signatory and their intent are clearly identifiable. Thus, an email signature may be appropriate in some circumstances; in others, it would require further evidence as support. A disadvantage of the approach, however, is that in the case of a dispute, the method selected will only be judged to be appropriate after the fact.

While minimalist laws permit the use of e-signatures for virtually all types of agreements, some countries and subregional entities do outline certain exceptions. In Australia, the law does not apply to documents related to migration and citizenship, while some regions exclude wills, powers of attorney and real estate. In Canada, some real estate agreements, wills and powers of attorney are also excluded, and some variation in restrictions exists among the provinces. United States federal law, as well as most of the country's state-level laws, exclude property transfers, wills and some legally required notices to consumers.

Prescriptive approach: Countries in this category usually require parties to employ a specific method or technology to sign documents electronically. Only records or signatures that have been created and managed using a prescribed methodology, standard or technology receive legal recognition, which often extends to attributes of the signed electronic record, such as origin and integrity. This approach is more commonly employed by countries with limited resources and/or where the government seeks to guide e-signature development in a particular direction. For example, Indonesia recognizes only digital signatures created through a digital certificate provider that is registered with the Ministry of Communication and Technology and has servers located in the country.

The prescriptive approach has the benefit of introducing maximum certainty on those methods and technologies that can be used. From a government perspective, this approach may be pursued to ensure the confidence in and security of an economy's transactions, and to increase trust in the digital economy. Depending on the formulation of the law, disadvantages include limiting recognition of emerging technologies for e-signatures and authentication methods, and dealing with cross-border recognition issues and challenges for small businesses in e-commerce; namely, SMEs not physically present in a country may find it difficult to use the country's PKI or access a national CA. One workaround is for countries to conclude bilateral mutual recognition agreements on CAs. However, this solution may be time- and resource-consuming, and few such agreements have been concluded in practice.

Hybrid (two-tier) approach: Countries in this third category use a mixed approach. They may provide legal status to all methods, such as typing the name at the bottom of an email. However, they accord greater evidentiary weight to certain methods, such as digital signatures or qualified e-signatures. This leaves users with a choice, but greater certainty if they decide to employ certain technologies.

Several variations of the hybrid approach exist. The EU established a new legal structure for electronic identification, signatures, seals and documents in July 2016, known as the regulation on electronic identification and trust services (eIDAS Regulation). The Regulation provides for three levels of signatures: basic, advanced and qualified e-signatures.

While all types of signature are legal, admissible and enforceable, only qualified e-signatures are legally identical to handwritten signatures. These are also the only types of signatures mutually recognized by all EU member states. Qualified electronic certificates must be based on qualified certificates issued by a CA accredited and supervised as designed by EU member states.

The eIDAS Regulation replaced an EU e-signature directive that had been in place since 1999 but was implemented in different ways by individual member states. In practice, many also would not recognize each other's e-signature laws.[13] The result was a complex landscape for business and consumers to work in, as e-signatures and certification tools underpinning digital signatures were not applicable across the bloc.[14]

Other countries, including Brazil, Chile, China, India, Mexico and South Africa, as well as the British overseas territory of Bermuda, enforce both simple electronic and digital signatures but only give the latter the same status as handwritten signatures. In most of these, as in the minimalist approach, e-signatures are presumed valid unless proof to the contrary is provided. In Mexico, digital signatures may be required to certify official documents and those related to tax obligations. South Africa specifies exceptions to using e-signatures in some areas, such as long-term leases and property transfers.[15] China also has exceptions for documents concerning personal relationships, termination of public service and other situations stipulated by laws and administrative regulations.[16] Brazil requires qualified e-signatures in the public sector that use public key infrastructure; these are typically used for high-value, high-volume transactions, including foreign exchange or transactions with the Brazilian government. Under Brazilian law, a written signature may not be required for a valid contract, but may be needed in case of a dispute. E-signatures may be admissible as acceptance of a contract – for instance, confirming purchase orders, invoices and sales agreements.[17]

The typology and descriptions above are designed to highlight just how varied the laws and regulations are that govern electronic and digital signatures. Countries have chosen to take different approaches; significant differences in the approach taken by governments can occur, even within a given category in the typology. Furthermore, it will likely prove to be increasingly challenging to ensure that cross-border e-transactions flow efficiently as the volume of cross-border transactions grows, new technologies emerge, and new laws and regulations are drafted in response.

UNCITRAL Model Laws and the ECC

Among international institutions, UNCITRAL has played a key role in trying to address the cross-border challenges of regulating e-transactions. Creating model legislative texts has been a crucial part of this effort. Trade agreement provisions increasingly refer to existing UNCITRAL legislative texts to promote coherence; it is thus important to understand their general contours and how they have been implemented.

UNCITRAL Model Law on Electronic Commerce (MLEC) (1996)

The MLEC provides a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for e-commerce. A major aspect is non-discrimination between paper-based and electronic forms of communication. The MLEC also promotes the principles of technological neutrality and functional equivalence. The former principle requires laws that do not insist on a specific technology for recognizing the validity of e- transactions. The latter lays out criteria under which electronic communications may be considered equivalent to paper-based notions such as "writing", "original", "signed" and "record".

While the main variation across domestic use is on e-signatures, national definitions of e-transactions determine what types of virtual exchange are recognized by law, including for cross-border use.

UNCITRAL Model Law on Electronic Signatures (MLES) (2001)

The MLES builds on the same fundamental principles of the MLEC. According to the UNCITRAL website, the MLES outlines "criteria of technical reliability for the equivalence between electronic and hand-written signatures as well as guidelines for assessing duties and liabilities for the signatory, the relying party and trusted third parties in the signature process". It also contains provisions on recognizing foreign certificates and e-signatures.

While the MLEC provides foundational notions for e-transactions, the MLES is more specific to signatures. Thus, while the MLEC contains a provision on the functional equivalence between handwritten and electronic signatures, the MLES adds to it by specifying that the e-signature method satisfying certain requirements will benefit from certain presumptions, for instance on the origin or integrity of the signed message (the two-tier approach). Moreover, the MLES contains additional articles, such as on the liability of certification service providers, that may not be relevant for all states.

United Nations Convention on the Use of Electronic Communications in International Contracts (ECC) (2005)

The ECC builds on the model laws and is the first legally binding international treaty to directly address cross-border use of digital technology in online transactions. This means it only applies at the international level; namely, the ECC comes into play when data messages are exchanged between parties whose places of business are in different countries.

Overall, the ECC aims to enhance legal certainty on the use of electronic communications by addressing a number of issues, such as determining a party's location in an electronic environment, the time and place of dispatch and receipt of electronic communications, and the use of automated message systems for contracts. By doing so, the ECC updates and complements the MLEC's provisions.

While the latter is a useful piece of legislation, updates are needed as technology evolves; for this reason, about 15 countries have incorporated provisions of the Convention into national legislation, but have not yet adopted it as a treaty.

Several factors may explain the relatively limited adoption of the ECC. First, it has not yet been fully adopted by major digital players, such as the United States, China and the EU, thus curbing its reach.[18] Second, countries may feel their cyberlegislation is already in place, and see no reason to update it. Third, UNCITRAL has limited resources for promoting its texts, which leads to lower visibility.

UNCITRAL Model Law on Electronic Transferable Records (MLETR) (2017)

UNCITRAL's most recent text aims to enable the use of electronic equivalents of paper-based transferable documents or instruments that entitle the holder to request delivery of goods or a sum of money – for example, bills of lading, promissory notes, bills of exchange and warehouse receipts. The MLETR builds on prior UNCITRAL texts, namely on the principles of functional equivalence and technological neutrality.

The MLETR may become particularly useful for facilitating paperless trade because certain transferable documents contain accurate data relevant for submission to electronic single windows for customs operations. The possibility to digitize those documents could therefore also provide a reliable electronic data source for purposes of regulatory compliance.

The Role of Trade Agreements

As noted above, solutions have been sought through trade agreements, given that some policy-makers have looked to smooth frictions caused by divergent legal frameworks on e-transactions in order to boost cross-border economic activity. Slightly more than half of all such agreements with a stand-alone e-commerce chapter contain a commitment on e-transactions, e-signatures and/or electronic authentication. An increasing number of trade agreements require a country to adopt a legal framework based on a UNCITRAL legislative text. Article 14.5 of the Trans-Pacific Partnership (TPP) mandates that parties adopt and maintain a legal framework governing e-transactions consistent with the principles of the MLEC or ECC. Other trade agreements that require domestic law to be based on the MLEC include Australia's FTAs with China, Malaysia, Singapore, South Korea and Thailand. The New-Zealand-Thailand FTA also contains a similar requirement. Some other trade agreements require governments to take note of the MLEC or adopt laws based on it as soon as is practicable; examples include the Association of Southeast Asian Nations (ASEAN)-Australia-New Zealand FTA, the Hong Kong-New Zealand Closer Economic Partnership and the Korea-Vietnam FTA.

In addition, many trade agreements elaborate specific actions that are barred. For example, in the Australia-Japan FTA, both parties commit that they will not enact "measures regulating e-transactions that (a) deny the legal effect, validity or enforceability of a transaction, including a contract solely on the grounds that it is in the form of an electronic communication, or (b) discriminate between different forms of technology".[19] This draws on the UNCITRAL principles of non-discrimination and technological neutrality.

A number of trade agreements further stipulate that a signature's legal validity cannot be denied simply because it is in electronic form, again deploying the UNCITRAL non-discrimination principle. Examples include the TPP and the China-Korea FTA.[20]

The treatment of electronic authentication is relatively diverse in FTAs, with different definitions that usually clarify the extent to which an e-signature must be combined with the means to identify the person signing the record or attesting the information's integrity. Many trade agreements mandate parties to allow participants in e-transactions to determine for themselves the appropriate authentication technology.[21] These FTAs often require that governments not limit the transactions' participants to using designated authentication technologies and implementation models.[22] In other words, these agreements encourage UNCITRAL's principle of technological neutrality. Furthermore, if challenged, the parties should be allowed to prove in court that their e-transactions comply with any legal requirement. The Agreement Establishing the ASEAN-Australia-New Zealand Free Trade Area (AANZFTA) follows this approach.[23]

Some trade agreements are silent on the issue of whether governments are allowed to take a prescriptive approach, but include the requirement for parties to demonstrate legal compliance. Examples include the Chile-Colombia FTA and Colombia's FTA with El Salvador, Guatemala and Honduras.[24] Meanwhile, some FTAs explicitly state that parties may require authentication services for certain transactions to meet performance standards or be provided by a legally established provider, approved by an authority in accordance with the domestic law.[25]

A handful of trade agreements note the importance of digital certificates or interoperability among authentication technologies, but these are often soft commitments and vary across FTAs. For example, Article 14.6 of the TPP commits countries to using interoperable electronic authentication. Other trade agreements seek to promote regulatory cooperation on this issue, including mutual recognition of digital certificates and e-signatures, usually based on internationally accepted standards issued or recognized by governments.[26] Parties to the recent Additional Protocol to the Framework Agreement of the Pacific Alliance may consider recognizing advanced or digital e-signature certificates issued by a certification service provider operating in the territory of another party.[27] The Additional Protocol also requires parties to establish mechanisms and approval criteria that promote the interoperability of electronic authentication between them, according to international standards.

Some FTAs include provisions on sharing information and experiences on laws, regulations and programmes

in e-commerce, such as those related to electronic authentication and e-signatures. All recent EU regional trade agreements require parties to maintain a dialogue on regulatory issues raised by e-commerce, addressing various issues, including the recognition of certificates of e-signatures and facilitation of cross-border certification services.[28] Uniquely, the Korea-Peru FTA commits parties to establishing cooperation mechanisms between the national accreditation and digital CAs for e-transactions.[29]

Improving Interoperability: A principles approach

In general, the three core principles advanced by UNCITRAL – non-discrimination, functional equivalence and technological neutrality – are useful guides for pursuing interoperable e-transaction and e-signature rules that support cross-border e-commerce. Technological neutrality may be particularly critical given rapid innovations, such as digital identity, and through the adoption of new tools including blockchain (see Box 3).

Several WTO members have raised the possibility of using the global trade body as an institution to advance greater interoperability of legal rules on e-transactions and e-signatures. Some have suggested adopting commitments to ensure contracts can be concluded online within individual jurisdictions and cannot be denied legal validity purely because of their being digital, mirroring commitments made in FTAs. Similar principles have also been suggested regarding e-signatures and trust services.

Some proposals would ensure that countries do not adopt measures for e-signatures and authentication that would prevent contracting parties from mutually determining the appropriate method for the transaction, or from being able to prove to a judge that the e-transaction complies with certain legal requirements. Others suggest promoting the mutual recognition of digital certificates and e-signatures. WTO members could also share domestic e-transaction or e-signature information to identify mutually acceptable global rules in these areas. Several have noted that cross-border interoperability of e-transaction and e-signature rules, among other measures, could positively impact SMEs.

Box 3: Transforming Information Dissemination

Blockchain, which is simply one form of distributed ledger technologies (DLTs), could fundamentally shifting how people share and treat verifiable information in the near future. By enabling the creation of immutable distributed databases, blockchain could be a useful tool in developing distributed, or self-sovereign, digital identity.

How is this possible? In a DLT, submitted data is woven together with other data into a cryptographically hashed and timestamped group or "block". That block is woven into the next block, and so on. Because each block is immutably timestamped, the resulting chain of blocks is very difficult to tamper with, as changes in a block will mean it no longer matches up with the code from the previous one, and so on for further blocks, denoting an alteration in the chain. Further, because the DLT is shared across an entire network, the verification process is decentralized, and any alteration is promptly detected by other nodes in the chain.

In theory, this technology could greatly ease trust and security along supply chains that require supportive documents or signed information, allowing information about digital transactions to follow the physical object in a secure way. Moreover, it opens options for trusted transactions between distant parties without the need for a third-party verifier or certification authority in the traditional sense. DLT, however, is just one breakthrough and not without questions about governance. Other breakthroughs could occur, suggesting future rules should be technology-neutral to allow for possible future developments.

Source: Contributed by Dan Puterbaugh, Legal Advocate, Adobe Systems Inc.

In light of the above, trade policy-makers and regulators may want to address the following questions as part of efforts to boost interoperable frameworks in the digital economy and e-commerce:

- What is the country's current legal framework concerning e-transactions? Does it enact any UNCITRAL text? Does it deal with cross-border aspects? If not, why? What types of changes would be required to promote mutual legal recognition? Where might points of opposition arise?
- In implementing a framework for e-transactions, what type of capacity already exists in the government? What more is needed? For example, if the country does not recognize e-signatures or other electronic authentication technologies, what limitations prevent it from doing so? Are those limitations technical or legal in nature? What additional assistance is required to establish effective cyberlaws that build trust in e-commerce?
- To what extent is the government willing to rely on the digital certification of other governments? What are the possible costs and benefits of engaging in mutual recognition agreements with other countries on this issue?
- Do relevant regional initiatives already exist to promote greater standardization or harmonization and to minimize the risks of fragmentation of the legal frameworks underlying e-transactions? Will the country's businesses likely feel the need to adjust to standards set by other regions to continue facilitating digital trade? Do regional initiatives favour or hinder e-commerce with countries outside the region?
- If a new WTO initiative would be advanced on this topic, how should it be organized? Can it serve as a stand-alone discussion point within the WTO e-commerce work programme? Or must it be bundled with other topics to be effective, and if so, which ones?

Capacity building for policy-makers and small businesses will be an important part of crafting interoperable frameworks and ensuring that the benefits from these are used. An UNCTAD survey of government representatives in 38 countries in Africa, Asia, and Latin America and the Caribbean cited the need to build knowledge in e-transactions among lawmakers and the judiciary. Nearly 80% of respondents identified a lack of skills or training for policy- or lawmakers as a challenge to enacting e-commerce legislation. Over 70% indicated a lack of skills or training for members of parliament as a hurdle.[30]

Public-private dialogue between policy-makers and the private sector could help shape frameworks fit for current growth drivers and new technological developments. Dialogue on e-transaction and e-signature rules could contribute to boosting knowledge among policy-makers on the challenges faced by business in the digital economy; in turn, it could help identify potential interventions, whether those done unilaterally or through trade agreements. To be inclusive, dialogue should involve a range of businesses, large and small, as well as civil society and consumer interest representatives.

Technical assistance from donors, international agencies and other forms of collaboration, including with the private sector, can further help to address very practical issues holding back e-traders or businesses from integrating e-transactions or tapping into online trust tools to boost competitive advantages. From this perspective, additional questions policy-makers and the wider e-commerce community should be asking that pertain to their countries include:

- To what degree do businesses, especially SMEs, face problems of interoperability with respect to digital authentication technologies when engaging in cross-border e-commerce? If these are not yet problems, what are the main overseas markets where the country's service providers will trade digitally, and is there a potential threat of conflict in the future?
- Do sector-specific working groups already exist, or should they be established within the country to help cater to the regulatory needs and business realities of that sector in facilitating e-transactions?
- Is a task force needed to think through the effects of new technologies and their deployment in business models on trade practice and policy, both in capturing advantages and reducing divergent rules that minimize potential benefits?

One practical challenge facing some developing-country entrepreneurs who seek to use trust products is that their country's CA may not be recognized on major approved trust lists. To be part of a list of trusted CAs, a CA must go through a strict application process, along with making financial deposits for each provider and software it certifies. To date, most trusted CAs are in North America, Western Europe and, more recently, in China and other advanced Asian economies. This can result in a challenging application process for developing-country entrepreneurs (see Box 2). In addition to addressing e-transaction regulations, capacity building and access to finance solutions could help to upgrade developing-country CAs so that the benefits of trust technologies can be more widely spread. Such efforts would benefit from accounting for different stakeholder perspectives – whether end-users looking for clear trust signals, entrepreneurs seeking to deploy these services, CAs not on the trust list, internationally trusted CAs and the e-security trusted list industry. Multistakeholder collaboration could develop solutions based on public-private capacity building, including assistance for CAs to join trusted lists.

In other instances, industry initiatives could help to advance interoperable standards once broader legislative frameworks are in place. For example, a reference in the EU's eIDAS Regulation on the potential use of cloud-based trust service for a QSCD prompted the set-up of a Cloud Signature Consortium. The cross-industry-backed initiative aims to create standardized specifications for cloud-based digital signatures, which would be interoperable between different service providers and clients.[31] Separately, Open Identity Exchange brings together leaders from competing business sectors to conduct research and carry out pilot projects to expand existing identity services and serve adjacent markets. OASIS is another non-profit consortium working towards developing, converging and adopting standards for the internet of things, cloud computing and content technologies, among other areas.

Conclusion

In theory, the digital economy does not recognize national borders or ministerial portfolios. However, many governments are challenged by the rapid pace of innovation and technological developments. Not surprisingly, governments have responded by imposing different laws and regulations affecting e-transactions. Streamlining these differences and enabling growth in online sales of goods and services as well as trade facilitation, if managed properly, could be a significant leveller, allowing more businesses and individuals to reap the benefits of globalization's economies of scale. While many countries already have baseline e-transaction laws in place, as has been demonstrated in this paper, divergences in details are manifest and do not always address cross-border aspects.
Similarly, while e-signatures may be useful for signalling trust in digital transactions, requirements can differ between jurisdictions and may not always be available to entrepreneurs in developing countries. Advancing knowledge among policy-makers – through conversation with business and consumers about where exactly the absence of interoperability creates challenges and holds back growth, particularly for SMEs – could eventually help shape targeted interventions, including through trade frameworks. Capacity building as well as public-private solutions could also be sought to improve the broader enabling environment, and to ensure the benefits of technological advances are widely spread.

Endnotes

[1] States party to the ECC are Cameroon, Congo, the Dominican Republic, Fiji, Honduras, Montenegro, the Russian Federation, Singapore and Sri Lanka. For the updated treaty status, see "United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)", available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html.

[2] Organisation for Economic Co-operation and Development (OECD), Digital Identity Management: Enabling Innovation and Trust in the Internet Economy, 2011. Available at http://www.oecd.org/sti/ieconomy/49338380.pdf.

[3] World Economic Forum, A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity, An Industry Project of the Financial Services Community, World Economic Forum, August 2016. Available at http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

[4] DHL Express, The 21st Century Spice Trade: A Guide to the Cross-Border E-commerce Opportunity, 2016. Available at http://www.dhl.com/content/dam/Campaigns/Express_Campaigns/Local_Campaigns/apem/express_campaign_spice_trade_apem_en.pdf.

[5] Organisation for Economic Co-operation and Development (OECD) and World Trade Organization (WTO), Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development, Chapter 10, "Public-Private Priorities for Aid for Trade in the Digital Era", 2017. Available at https://www.wto.org/english/res_e/booksp_e/aid4trade17_chap10_e.pdf.

[6] Adobe, "Electronic and Digital Signatures in Adobe Sign White Paper", September 2017. Available at https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-transform-business-processes-with-electronic-and-digital-signature-solutions.pdf.

[7] The importance of e-transaction and e-signature rules to trade facilitation and digitized customs procedures that can reduce trade costs is discussed in a World Economic Forum White Paper on paperless trade as part of a series on e-commerce best practices.

[8] United Nations Conference on Trade and Development (UNCTAD), "Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned", Note by the UNCTAD secretariat, 2015. Available at http://bit.ly/1H5zDjc.

[9] Organisation for Economic Co-operation and Development (OECD) and World Trade Organization (WTO), Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development, 2017.

[10] United Nations Conference on Trade and Development (UNCTAD), Information Economy Report 2015: Unlocking the Potential of E-commerce for Developing Countries, 2015. Available at http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf.

[11] International Centre for Trade and Sustainable Development (ICTSD), "Bridging Distance for Development: Regulatory Cooperation Applied to Consumer Rights, Parcel Delivery and Sales Tax", 10 August 2017. Available at https://www.ictsd.org/themes/global-economic-governance/research/bridging-distance-for-development-regulatory-cooperation.

[12] Howe, J., "International E-Commerce in Africa: The Way Forward", International Trade Centre, Technical Paper, 2015. Available at http://www.intracen.org/uploadedFiles/intracenorg/Content/Publications/International%20E-Commerce%20in%20Africa_Low-res.pdf.

[13] Legal IT Insider, "Understanding eIDAS – All you ever wanted to know about the new EU Electronic Signature Regulation", 1 March 2016. Available at https://www.legaltechnology.com/latest-news/understanding-eidas-all-you-ever-wanted-to-know-about-the-new-eu-electronic-signature-directive/.

[14] European Commission, Digital Single Market, "The first big step in eIDAS implementation accomplished", 9 September 2015. Available at https://ec.europa.eu/digital-single-market/en/blog/first-big-step-eidas-implementation-accomplished.

[15] Adobe, "Global Guide to Electronic Signature Law: Country by Country summaries of law and enforceability", 2017. Available at https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf.

[16] China Briefing, "Electronic Contracts in China Can Improve Efficiency with Strong Controls", 23 August 2017. Available at http://www.china-briefing.com/news/2017/08/23/electronic-contracts-china-can-improve-efficiency-strong-controls.html.

[17] DocuSign, "eSignature Legality in Brazil", 2017. Available at https://www.docusign.com/how-it-works/legality/global/brazil.

[18] In China and the United States, formal steps towards ECC adoption have been taken.

[19] Agreement between Australia and Japan for an Economic Partnership, art. 13.5.2.

[20] Trans-Pacific Partnership, art. 14.6.1; China-Korea Free Trade Agreement, art. 13.4.1.

[21] See, for example, Korea-Australia Free Trade Agreement, art. 15.5. Some agreements include this mandate expressed in a negative manner, see Free Trade and Economic Partnership Agreement between Japan and Switzerland, art. 78 ("Neither party shall adopt or maintain legislation . . . prohibit[ing] parties . . . from mutually determining the appropriate electronic signature methods.").

[22] Singapore-Australia Free Trade Agreement, art. 14.5.

[23] Agreement Establishing the ASEAN-Australia-New Zealand Free Trade Area (AANZFTA), art. 5.1.

[24] Free Trade Agreement between Chile and Colombia, art. 12.7; Colombia-Northern Triangle Free Trade Agreement, art. 14.7.

[25] United States-Korea Free Trade Agreement, art. 15.4; Free Trade and Economic Partnership Agreement between Japan and Switzerland, art. 78.

[26] See, for example, China-Australia Free Trade Agreement, art. 12.6.2; Korea-Australia Free Trade Agreement, art. 15.5.3; EU-South Korea Free Trade Agreement, art. 7.49.1.

[27] Additional Protocol to the Framework Agreement of the Pacific Alliance, art. 13.10.

[28] See, for example, Deep and Comprehensive Free Trade Area (DCFTA) of the EU-Ukraine Association Agreement, art. 140; EU-South Korea Free Trade Agreement, art. 7.49.

[29] Free Trade Agreement between the Republic of Korea and Peru, art. 14.8.

[30] United Nations Conference on Trade and Development (UNCTAD), Information Economy Report 2015: Unlocking the Potential of E-commerce for Developing Countries, 2015.

[31] Cloud Signature Consortium, "Building a standard for cloud signatures". Available at http://www.cloudsignatureconsortium.org/.

Acknowledgements

This White Paper was prepared by Luca Castellani, Secretary, UNCITRAL Working Group IV (Electronic Commerce), Mark Wu, Assistant Professor, Harvard Law School, and Kimberley Botwright, Policy Analyst, Digital Trade, World Economic Forum.

The authors are grateful for contributions by the International Trade Centre, the Universal Postal Union and Dan Puterbaugh, Legal Advocate, Adobe Systems Inc. The views expressed herein are those of the authors and do not necessarily reflect the views of their respective organizations.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org