The Commonwealth Model Law on Digital Trade and Guide to Enactment

The Commonwealth Connectivity Agenda

The Commonwealth Model Law on Digital Trade and Guide to Enactment

The Commonwealth

Wherever possible, the Commonwealth Secretariat uses paper sourced from responsible forests or from sources that minimise a destructive impact on the environment.

Published by the Commonwealth Secretariat.

Part 1
The Commonwealth Model Law on Digital Trade

Part 1 The Commonwealth Model Law on Digital Trade

Part 2 Guide to Enactment

Foreword

In an era defined by speed, innovation and digital connectivity, the way we trade must evolve as fast as the world around us. The Commonwealth, with its rich tapestry of cultures, economies and shared legal traditions, has a historic opportunity to lead this transformation. This *Commonwealth Model Law on Digital Trade* ('the Model Law') is not just a legislative tool, it is a gateway to a smarter, more inclusive and resilient global trading system.

Our member countries are navigating complex challenges, from disrupted supply chains to the urgent need to integrate small businesses into global markets. The solution lies in digitalisation and, more critically, in laws that are modern, interoperable and built for the digital economy. That is precisely what this Model Law delivers: a clear, practical and globally harmonised legal framework to empower governments, unlock growth and enable trade that is faster, cheaper and more secure.

Digital trade holds great promise to catalyse global value chains and grow trade worldwide. Within the Commonwealth, facilitating digital trade could increase intra-Commonwealth trade by approximately US$90 billion. More significantly, legal reform to support the digitalisation of trade processes could add a further US$1.1 trillion in efficiency and growth gains. Combined, these reforms could deliver nearly US$1.2 trillion in total benefits over a five-year period, underscoring the immense value of adopting paperless trade systems.

The *Model Law* offers practical legislative guidance, enabling legal recognition of electronic transactions, signatures and transferable records. It ensures national laws are interoperable, secure and business-ready, while maintaining necessary protections for data, identity and trust. Its adoption will empower governments to unlock economic opportunities, boost trade competitiveness and ensure their economies are fit for the demands of modern commerce.

I invite all Commonwealth member countries to take full advantage of this legal framework. By aligning national legislation with these principles, we can unlock the full potential of digital trade, empower our businesses, and ensure that no nation or entrepreneur is excluded from the benefits of the digital economy. The Commonwealth Secretariat stands ready to support members every step of the way.

Hon. Shirley Botchwey
Commonwealth Secretary-General

Introduction

Legal reforms are having a remarkable impact on growth and productivity. By way of example, within the UK the last 12 months, companies, large and small, have cut average trade transaction times from an average two to three months to one hour, while trade transaction costs and cross-border processing times have been reduced 80 per cent and workforce productivity has increased 60 per cent. The worldwide use of electronic bills of lading has more than doubled in 12 months since the UK Electronic Trade Documents Act (ETDA) 2023 came into force.

These are just some of the benefits being delivered to business from modernising legal infrastructure to enable the transition to technology-led trade. If implemented across the Commonwealth, the estimated economic benefit is US$1 trillion in growth and efficiency gains, including a 35 per cent efficiency gain for micro, small and medium-sized enterprises (MSMEs). The opportunity is to ensure that all businesses benefit. To achieve this, we are calling on all Commonwealth members to remove legal barriers to digitalising trade and align national laws to UN model laws to ensure legal systems are interoperable.

We recognise that limited capacity and not knowing where to start can be a real challenge for many Commonwealth members. This Model Legal Framework has been developed by the Commonwealth Secretariat in conjunction with industry as a practical guide for policy- and law-makers. The framework is intended to be a tool to help governments unlock the array of growth and productivity benefits on offer.

We hope you find this framework useful and look forward to supporting the worldwide effort to make trade cheaper, faster and simpler for all.

Teddy Soobramanien
Co-Chair, Commonwealth Connectivity Agenda B2B Cluster
(CEO, Common Market for Eastern and Southern Africa, Business Council)

Chris Southworth
Co-Chair, Commonwealth Connectivity Agenda B2B Cluster
(Secretary General, International Chamber of Commerce, United Kingdom)

Overview

The *Commonwealth Model Law on Digital Trade* ('the Model Law') offers transformative benefits for governments, businesses and consumers across member countries. By providing legal certainty for electronic communications, records, signatures and contracts, the law eliminates long-standing barriers that have limited the adoption of paperless trade. Its implementation enables faster, more efficient transactions, reducing delays and administrative burdens, and improving overall trade performance.

One of the law's most significant benefits is its ability to unlock economic opportunity by making trade systems more inclusive and accessible. It empowers micro, small and medium-sized enterprises to participate more effectively in domestic and international markets by lowering entry costs and simplifying compliance. By ensuring legal recognition of digital trade documents and platforms, the *Model Law* strengthens trust and confidence in electronic transactions, which is essential for scaling cross-border commerce.

The law also enhances resilience and adaptability in trade systems. By allowing for fully digital processes, it reduces dependence on physical documentation and manual procedures, which is a critical advantage in times of disruption, such as during pandemics or geopolitical crises. It also supports innovation by being technology-neutral, enabling member countries to adopt and integrate new digital tools without requiring continuous legislative amendments.

Another major benefit lies in harmonisation. The *Model Law* helps align national legal frameworks across the Commonwealth, creating a more predictable and interoperable environment for trade. This not only lowers legal friction for businesses operating across borders but also positions Commonwealth countries to attract investment and integrate more deeply into global value chains.

Finally, the law provides a structured, practical pathway for legal reform. It is designed to be readily adaptable to national contexts, allowing governments to modernise their trade legislation efficiently, while upholding high standards of legal integrity, data protection and public trust. Its adoption marks a decisive step toward building modern economies that are competitive, connected and digitally empowered.

An Act to authorise the legally effective use of electronic communications, to promote digital trade and to implement a number of related model laws of the United Nations Commission on International Trade Law, including the Model Law on Electronic Transferable Records.

Interpretation

a. Definitions

1. In this law, the following terms have the following meanings:

   (a) 'Automated system' means a computer system that is capable of carrying out actions without the necessary review or other intervention of a natural person.

   (b) 'Certificate' means a statement by a knowledgeable individual or body, after investigation, that certain facts or relationships exist. The certificate may be expressed to a specified degree of reliability or assurance.

   (c) 'Certification' is the process of issuing a certificate.

   (d) 'Data' includes all representations of information in any format or medium.

   (e) 'Data message' means information generated, sent, received or stored by electronic, magnetic, optical or similar means.

   (f) 'Electronic signature' is the electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document.

   (g) 'Transferable document or record' has the meaning set out in Section 34.

b. Interpretation and application

2. (1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

   (2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

   (3) This Law does not apply to [*set out exceptions]*

Electronic Form Issues

Validity

3. (1) Information shall not be denied legal effect, validity or enforcement solely because it is in electronic form.

(2) ([Nothing in this Law requires a party to use or accept information in electronic form, but a party's agreement to do so may be inferred from the party's conduct.]

Writing

4. (1) A legal requirement that information should be in writing is satisfied by information in electronic form if it is accessible so as to be usable for subsequent reference.

(2) A legal requirement that a person must provide information in writing to another person is satisfied by the provision of the information in an electronic form that is:

i. accessible by the other person so as to be usable for subsequent reference; and

ii. capable of being retained by the other person.

(3) If information is required to be provided in a specific physical form, this requirement is met if the electronic information is organised and presented in a way that is the same as, or substantially equivalent to, the required physical form.

(4) Despite subsection (3), nothing in this Law limits the operation of any provision of law that expressly authorises, prohibits or regulates the use of electronic information or electronic documents.

(5) Nothing in this Law limits the operation of a legal requirement for information to be posted or displayed in a specified manner or for any information or document to be transmitted by a specified method.

Forms

5. If a law of [enacting jurisdiction] requires a particular form, the authority responsible for the form may make an electronic form that is substantially the same as the form set out in the law and the electronic form is to be considered as the form set out in the law.

6. A provision of [enacting jurisdiction] law that authorises prescribing a form or the manner of filing a form includes the authority to prescribe an electronic form or an electronic means of filing the form, as the case may be.

Originals

7. (1) A legal requirement that an original document should be provided, retained or examined is satisfied by the provision, retention or examination of an electronic document if:

(a) there exists a reliable assurance as to the integrity of the information contained in the electronic document from the time the document to be provided, retained or examined was first created in its final form, whether as a written document or as an electronic document; and

(b) in a case where the original document is to be provided to a person, the electronic document that is provided is accessible by the person so as to be usable for subsequent reference and capable of being retained by the person.

(2) For the purposes of clause (1)(a):

(a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the introduction of any incidental changes that arise in the normal course of communication, storage and display and that do not affect the core contents of the document;

(b) whether an assurance is reliable shall be determined in light of all the circumstances, including the purpose for which the document was created.

Retention

8. A legal requirement to retain a document, whether or not originally on paper, is satisfied by the retention of an electronic document if:

(a) the electronic document is retained in the format in which it was created, sent or received, or in a format that accurately represents the information contained in the document that was originally created, sent or received;

(b) the information in the electronic document that is retained is accessible so as to be usable for subsequent reference by any person who is entitled to have access to the document that was originally created, sent or received, or who is authorised to require its production; and

(c) where the electronic document was sent or received, information, if any, that identifies its origin and destination and the date and time when it was sent or received is also retained.

Extended meaning

9. In this Law, a reference to a legal requirement includes a reference to a provision of law:

(a) that imposes consequences if writing is not used or a form is not used, a document is not signed or an original document is not provided or retained; or

(b) by virtue of which the use of writing, the presence of a signature or the provision or retention of an original document leads to a special permission or other result.

Evidence

10. In any legal proceeding, nothing in the rules of evidence applies to deny the admissibility of information in evidence:

(a) on the sole ground that it is in electronic form; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain.

Communications

Governmental use

11. (1) Governments and other public bodies may communicate among themselves and with the public by electronic means and may use electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with documents or information.

(2) These communications shall be as secure and as reliable as appropriate in the circumstances, considering their purpose, their content and their intended audience.

Time and place of sending and receipt

12. (1) Unless otherwise agreed between the originator and the addressee, the time of sending of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee.

(3) The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address.

(4) An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

(5) An electronic communication is deemed to be sent from the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business. The parties may designate other places for this purpose.

Location of parties

13. (1) This Law does not require disclosure of the location of any person or affect requirements of other law about such disclosure.

(2) For the purposes of this Law, a party's place of business is presumed to be the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.

(3) If a party has not indicated a place of business or has more than one place of business, then the place of business for the purposes of this Law is that which has the closest relationship to the relevant transaction, having regard to the circumstances known to or contemplated by the parties at any time before or at the time of the transaction.

(4) If a natural person does not have a place of business, reference is to be made to the person's habitual residence.

(5) A location is not a place of business merely because it is: (a) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or (b) where the information system may be accessed by other parties.

(6) The sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

Transactions

Contracts

14. (1) A contract is not invalid or unenforceable by reason only of being in electronic form.

(2) Automated systems may be used to form or to perform contracts, including by:

(a) generating or otherwise processing data messages that constitute an action in connection with the formation of contracts, such as an offer or acceptance of an offer;

(b) generating or otherwise processing data messages that constitute an action in connection with the performance of a contract, such as its modification or termination.

(3) An automated system may be programmed to operate in a deterministic or a non-deterministic manner.

(4) A contract may be formed by the interaction of an automated system and a natural person, or by the interaction of automated message systems.

(5) A contract formed using an automated system shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in any action carried out in connection with the formation of the contract.

(6) An action carried out by an automated system in connection with the formation or performance of a contract shall not be denied legal effect, validity or enforceability on the sole ground that no natural person reviewed or intervened in the action.

15. (1) A contract shall not be denied validity or enforceability on the sole ground that the terms of the contract are contained in data messages in the form of computer code.

(2) A contract shall not be denied validity or enforceability on the sole ground that the terms of the contract incorporate information from a data source that provides information that changes periodically or continuously.

(3) An action in connection with the formation of a contract shall not be denied legal effect, validity or enforceability on the sole ground that the action involves processing data messages containing information from a source that provides information that changes periodically or continuously.

(4) Unless otherwise agreed by the parties, where an action carried out by an automated system is attributed to a party to a contract, the other party to the contract is not entitled to rely on that action if, in the light of all the circumstances:

(a) the party to which the action is attributed could not reasonably have expected the action; and

(b) the other party knew or could reasonably be expected to have known that the party to which the action is attributed did not expect or could not reasonably have expected the action.

(c) Nothing in this section affects the application of any rule of law or agreement of the parties that may govern the legal consequences of an action carried out by an automated system.]

Attribution

16. (1) As between the parties to a contract, an action carried out by an automated system is attributed in accordance with a procedure agreed to by the parties.

(2) If subsection 1 does not apply, an action carried out by an automated system is attributed to the person who uses the system for that purpose.

(3) Attribution of an action carried out by an automated system shall not be denied on the sole ground that the outcome was unexpected.

(4) Nothing in this section affects the application of any rule of law that may govern the legal consequences of attributing an action carried out by an automated system to a person.

Invitations to make offers

17. A proposal to conclude a contract made through electronic communications which are not addressed to specific parties but are generally accessible to persons making use of information systems, is considered an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

Input errors

18. Where a natural person makes an input error in an electronic communication exchanged with the automated system of another person and the automated system does not provide the person with an opportunity to correct the error, that person has the right to withdraw the portion of the electronic communication in which the input error was made if:

(a) the person notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and

(b) the person has not used or received any material benefit or value from the goods or services, if any, received from the other party.

Signatures

Signatures

19. (1) If a rule of law requires the signature of a person, that requirement may be met by an electronic signature.

(2) Parties may agree to use a particular method of electronic signature, unless otherwise provided by law.

(3) In determining whether an electronic signature is reliable, parties may consider whether:

(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable;

(d) where a 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; and

(e) the signature method has been proven in fact to have identified the signatories and indicated their intention with respect to the information contained in the electronic communication, by itself or together with further evidence.

(4) The [regulation-making authority] may require by regulation that, for a particular category of transactions, the method of authentication or electronic signature must meet certain performance standards or must be certified by a trust service provider.

Foreign signatures and certificates

20. (1) An electronic signature or a certificate supporting the signature created, used or issued outside [the enacting state] shall have the same legal effect in [the enacting State] as an electronic signature or certificate created, used or issued in [the enacting State] if the foreign electronic signature or certificate offers a level of reliability that is substantially equivalent to that of [the enacting State].

(2) In determining whether an electronic signature or certificate offers a substantially equivalent level of reliability for the purposes of subsection (1), regard shall be had to recognised international standards and to any other relevant factors.

Identity, Trust, Reliability

Certification Services

Review and certification

21. (1) One or more public or private bodies may be authorised to review the activities of parties to electronic communications and certify the existence or reliability of certain facts about parties to commercial transactions and their activities.

(2) In certifying reliability, a body shall so far as practicable follow international standards and the provisions of this Law on what makes the activities in or the characteristics of a particular transaction reliable.

(3) An entity may be authorised, in addition or instead, to review and designate as reliable the systems and practices of bodies that themselves certify such matters about transacting parties or the use of technology in commerce.

(4) In reviewing the reliability of such bodies, the entity shall take into account all relevant circumstances, including any duties assigned to them by this Law.

(5) Any such designation creates a rebuttable presumption that the services provided by the body reviewed are reliable.

(6) An entity designating the reliability of the systems and practices of certifying bodies as contemplated in subsection (3) shall maintain a public record of the systems and practices it has designated as reliable, and their providers, in sufficient detail for users of the systems to recognise them.

Identity Management

Identification management service provider

22. (1) A body (here called an 'identity management service provider') may determine and certify the identity of legal and natural persons for purposes of their engagement in electronic communications (a process here called 'identity management').

(2) The determination consists of two phases:

(a) Identification: a process used to achieve sufficient assurance of a person's digital identity, being a set of attributes that allows a person to be uniquely distinguished within a particular context.

(b) Identity proofing: assembling evidence of the presence and strength of those attributes to ensure their appropriate reliability for the purposes for which identity is required.

Duties of an identity manager

23. An identity management service provider shall, at a minimum:

(a) Have in place operational rules, policies and practices, as appropriate to the purpose and design of the identity management system, to address requirements to:

1. enrol persons, including by:

a. registering and collecting attributes;

b. carrying out identity proofing and verification; and

c. binding the identity credentials to the person;

2. update attributes;

3. manage identity credentials, including by:

a. issuing, delivering and activating credentials;

b. suspending, revoking and reactivating credentials; and

c. renewing and replacing credentials;

4. manage the electronic identification of persons, including by:

a. a. managing electronic identification factors; and

b. b. managing electronic identification mechanisms.

(b) Act in accordance with its operational rules, policies and practices, and any representations that it makes with respect to them.

(c) Ensure the online availability and correct operation of the identity management system.

(d) Make its operational rules, policies and practices easily accessible to the clients whose identities it manages (here called 'subscribers'), relying parties and other third parties.

(e) Provide easily accessible means that enable a relying party to ascertain, where relevant:

1. any limitation on the purpose or value for which the identity management service may be used; and

2. any limitation on the scope or extent of liability stipulated by the identity management service provider.

(f) Provide and make publicly available means by which a subscriber may notify the identity management service provider of a security breach pursuant to Section 24.

Duties of subscriber to identity manager

24. The subscriber shall notify the identity management service provider, by utilising means made available by that body pursuant to clause 23(f) or by otherwise using reasonable means, if:

(a) the subscriber knows that the subscriber's identity credentials have been compromised; or

(b) the circumstances known to the subscriber give rise to a substantial risk that the subscriber's identity credentials may have been compromised.

Legal effect of electronic identification

25. (1) The result of electronic identification shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that:

(a) the identity proofing and electronic identification are in electronic form; or

(b) the identity management service is not designated pursuant to Section 21.

(2) Where the law requires the identification of a person for a particular purpose, that requirement is met with respect to identity management services if a reliable method is used for the identity proofing and electronic identification of the person for that purpose.

(3) For the purposes of Section 25(2), the method shall be:

1. as reliable as appropriate for the purpose for which the identity management service is being used; or

2. deemed to be as reliable as appropriate if proven in fact by or before a court or other competent adjudicative body to have fulfilled the function described in Section 22, by itself or together with further evidence.

Determining reliability of identification management services

26. The reliability of identification management services is determined according to the criteria set out in Section 39.

Trust Services

Trust service provider

27. (1) A service provider may offer as a trust service an electronic certification service that provides assurance of certain qualities of a data message and may include methods for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services.

(2) A trust service provider may enter into agreements with clients, here called 'subscribers', to provide one or more trust services to the subscriber, for the benefit of the subscriber or another person.

Duties of a trust service provider

28. A trust service provider shall, at a minimum:

(a) Have in place operational rules, policies and practices, including a plan to ensure continuity in case of termination of activity, as appropriate to the purpose and design of the trust service;

(b) Act in accordance with its operational rules, policies and practices, and any representations that it makes with respect to them; and

(c) Make its operational rules, policies and practices easily accessible to subscribers, relying parties and other third parties;

(d) Where the trust service is in respect of an electronic signature, ensure that its certificate enables a relying party to ascertain from the certificate:

a. the identity of the trust service provider;

b. that the signatory identified in the certificate had control of the signature creation data at the time when the certificate was issued; and

c. that the signature creation data were valid at the time when the certificate was issued.

(e) Provide and make publicly available means by which a subscriber may notify the trust service provider of a security breach pursuant to Section 30.

(f) Provide easily accessible means that enable a relying party to ascertain, where relevant:

a. the method used to identify the signatory or subscriber;

b. the validity of the signature or identity data and the absence of any compromise of them;

c. the use of a timely revocation service, if any;

d. any limitation on the purpose or value for which the trust service may be used; and

e. any limitation on the scope or extent of liability stipulated by the trust service provider.

Breach of security

29. If a breach of security or loss of integrity occurs that has a significant impact on a trust service, the trust service provider shall, in accordance with the law:

(a) take all reasonable steps to contain the breach or loss, including, where appropriate, suspending or revoking the affected service;

(b) remedy the breach or loss; and

(c) give notice of the breach or loss to subscribers and appropriate public authorities.

Duties of subscribers

30. (1) The subscriber shall exercise reasonable care to avoid unauthorised use of its signature creation data or any other data used for access to and usage of the trust service.

(2) The subscriber shall notify the trust service provider, by utilising means made available by the trust service provider pursuant to Section 28, paragraph e, or by otherwise using reasonable means, if:

(a) the subscriber knows that data or means used by the subscriber for access and usage of the trust service have been compromised; or

(b) the circumstances known to the subscriber give rise to a substantial risk that the trust service may have been compromised.

(3) Where a certificate is used to support the electronic signature, the subscriber shall exercise reasonable care to ensure the accuracy and completeness of all material representations made by the subscriber that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

Legal effect of trust services

31. The result deriving from the use of a trust service shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that:

(a) it is in electronic form; or

(b) the trust service is not designated pursuant to Section 21.

32. (1) Where the law requires that facts or relationships be documented or actions confirmed, as described in Section 27(1), the requirement for documentation or confirmation is satisfied if a trust service provider uses a reliable method to provide the documentation or confirmation in electronic form.

(2) The method shall be:

(a) as reliable as appropriate for the purpose for which the trust service is being used; or

(b) deemed to be as reliable as appropriate if proven in fact by or before a court or other competent adjudicative body to have fulfilled the function required by law, by itself or together with further evidence.

(c) A method used by a trust service provider designated pursuant to Section 21 is presumed to be reliable.

Determining reliability of trust services

33. The reliability of trust services is determined according to the criteria set out in Section 39.

Electronic Transferable Records

Definition of transferable record

34. (1) 'Transferable record' means a document, record or instrument issued on paper that entitles the holder to claim the performance of the obligation indicated in it and to transfer the right to performance of the obligation indicated in it by means of its transfer.

(2) Examples of transferable records are bills of lading, promissory notes, bills of exchange, cheques, warehouse receipts, ship's delivery orders, mate's receipts, marine insurance policies and cargo insurance policies.

(3) This Law does not apply to securities, such as shares and bonds, and other investment instruments, and to ....

Legal effect of using electronic transferable records

35. (1) An electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form.

(2) Nothing in this Law requires a person to use an electronic transferable record without that person's consent.

(d) The consent of a person to use an electronic transferable record may be inferred from the person's conduct.

Using electronic transferable records

36. If the law requires a transferable record, the requirement is met by an electronic record if:

(a) The electronic record contains the information that would be required to be contained in the transferable document, record or instrument.

(b) A reliable method is used to:

i. identify the electronic record as the record containing the information necessary to have the desired legal effect among the parties;

ii. render that record capable of being subject to control from its creation until it ceases to have any effect or validity;

iii. establish exclusive control of the electronic transferable record by a person;

iv. identify that person as the person in control;

v. ensure that upon a transfer of control, the transferee has the same capacity to exercise exclusive control, and the transferor ceases to have control;

vi. retain the integrity of that electronic record;

vii. convert an electronic transferable record to a non-electronic transferable record, and vice versa, in such a way that there is ever only a single version of the transferable record effective to convey the legal rights it describes, and that the fact of each conversion is stated in the record.

Validity of foreign electronic transferable records

37. (1) An electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it was issued or used abroad.

(2) (2) Nothing in this Law affects the application to electronic transferable records of rules of private international law governing a transferable document or instrument.

Determining reliability of electronic transferable records

38. (1) The reliability of methods to manage elements of electronic transferable records set out in Section 36 is determined according to the criteria set out in Section 39.

Reliable Services

Reliability

39. (1) In determining the reliability of the methods used to carry out the duties of identification management and trust service providers, the creation and management of electronic transferable records and the reliability of the systems within which they operate, all circumstances relevant to the uses to be made of the data may be taken into account. Without limitation, these include:

(a) Compliance by the body with its own internal rules and procedures, including those on governance, record-keeping and technical controls, in so far as they relate to assessing reliability of the record.

(b) The financial and human resources of the body, including the existence of assets.

(c) The quality, including the security, of its hardware and software systems.

(d) Any measures taken to secure the integrity of the information held on the system and to prevent unauthorised access to and use of the system.

(e) The purposes for which trust is being evaluated.

(f) The regularity and extent of an independent audit.

(g) The assessment of the reliability of the system by an entity with supervisory or regulatory functions.

(h) Any declaration by the state, an accreditation entity or the service provider itself regarding compliance with any of the foregoing criteria.

(i) The provisions of any voluntary scheme or industry standard that apply in relation to the system.

(j) Any relevant agreement between transacting parties, including any limitation on the purpose or value of the transactions for which trust, identification management or other certification services may be used.

(2) In addition to the considerations mentioned in subsection (1), in determining the reliability of certificates issued under any provision of this Law [*applicable to any question relevant to the matters dealt with in this Law*], the following factors may be taken into account:

(a) Compliance by the body whose trustworthiness is to be evaluated with the duties imposed on it by this Law and other applicable laws.

(b) Its procedures for processing certificates, applications for certificates and the retention of records.

(c) The availability of information to signatories identified in certificates and to potential relying parties.

(3) A transferable document or record in electronic form is also valid if there is proof in fact that the method or the system used to reliably support a feature set out in Section 22, subsection 25(2), Section 32 or paragraph 36(b) has fulfilled the function for which it is used, by itself or together with further evidence.

(4) In determining the reliability of the method and of the service using it, no regard shall be had to:

(a) the geographic location where the identity management or trust service is provided; or

(b) the geographic location of the place of business of the identity management or trust service provider or originator of the electronic transferable record.

(5) Despite subsection (4), the validity or effect of an electronic signature created outside the country is determined as set out in Section 20.

Other Data Protection

Duties of Data Controllers

40. (1) Holders of personal and commercial data shall ensure that the data are secure against degradation and loss, and accessible only to those with a valid reason to access such data and only to the extent of that reason.

(2) Holders of data shall ensure that the data are accessible to those persons at all times and restore access as soon as practicable in the event of any interruption to this access.

(3) (3) Persons with a valid reason to access the data may include public authorities and law enforcement authorities in cases where they have no other practicable way to obtain the data and the data are essential to their functions.

Conflicts of interest

41. Holders of data shall not disclose the data except as provided in Section 40 and shall not make use of the data for their own purposes or their own benefit except as consistent with the reasons for which they hold such data.

Closing Provisions

Power to make regulations

42. The [appropriate authority] may make regulations for the more effective implementation of any provision of this Law, and in particular may prescribe:

    a. ...

    b. ...

    c. ...

Short Title

43. This Act may be known as the 'Digital Trade Act, 2025'.

Coming into Force

44. This Law comes into force ....

    (a) [On Royal (Executive) consent]

    (b) [On proclamation]

    (c) [Part 1 on [date x], Parts 2- 4 on [date y] etc.]

Part 2
Guide to Enactment

Introduction

It is widely recognised that we are living in the information age; however, not all jurisdictions have fully addressed its legal implications. As digital technologies continue to evolve, legal frameworks must adapt accordingly, as what applied yesterday may not reflect today's commercial reality.

What was once termed 'electronic commerce' is now more commonly referred to as 'digital trade' or 'paperless trade', particularly in cross-border contexts. The term 'digital' is increasingly preferred, as it emphasises the structured and codified nature of modern data over the means of transmission. This Model Law accordingly uses the term digital trade.

Some consider 'digital' to imply more manipulable or actionable data, whereas 'electronic' may suggest only the medium.[1] The Organisation for Economic Co-operation and Development (OECD) and UN Trade and Development (UNCTAD), among others, define electronic commerce and digital trade similarly, with digital trade typically applying only to international transactions, while electronic commerce can refer to both domestic and international dealings.[2]

Further distinctions are sometimes drawn between:

- digitally ordered trade (for example, purchases made through online platforms);
- digitally delivered trade (for example, digital content such as music, software and streaming); and
- digitally facilitated trade – a broader category encompassing transactions enabled by digital infrastructure.[3]

Some definitions identify e-commerce as 'digitally enabled trade' and reserve digital trade for the exchange of purely digital assets.[4]

Electronic communications also encompass more than traditional commercial messages. Legal rules governing such communications may apply to a broader set of digital interactions with commercial significance. Determining whether a communication is trade-related can be complex; the provisions of this Model Law are therefore designed to apply to any messages that have, or could have, commercial consequences.

Commercial law often lags behind commercial practices, providing post hoc validation or correction. This is equally true for electronic commerce and digital trade: much digital trade has occurred in advance of comprehensive legal regulation, and this trend continues.

In legal terms, distinctions between e-commerce and digital trade seldom affect enforceability. However, they may influence system design and terminology in legal drafting. (See further below for the treatment of documents versus data in this context.)

1 The distinction lies in the emphasis on structured, codified content rather than the method of transmission.

2 See: OECD, Digital Trade, and UNCTAD, *E-Commerce and the Digital Economy Reports* [AQ: add URL? And/or specify year of publication, place/publisher?], online: https://unctad.org/topic/ecommerce-and-digital-economy

3 See World Trade Organization (WTO) (2023), *Handbook on Measuring Digital Trade*. [AQ: published by WTO? Geneva?] online: https://www.wto-ilibrary.org/content/books/9789287073594

4 Ibid.; see also UNCITRAL, Model Law on Electronic Commerce, and recent commentary.

To support business practices in the digital economy, legal rules generally do not need to distinguish between domestic and international transactions or focus on the nature of the goods or services involved. Nonetheless, where cross-border elements are legally significant, this *Guide to Enactment* notes them explicitly.

This Model Law uses 'electronic' in contexts more aligned with domestic retail transactions, and 'digital' for broader or more complex commercial processes. Terminological choices also reflect alignment with existing UN Commission on International Trade Law (UNCITRAL) model laws, which have only recently begun referring explicitly to digital data.

Legislative Background

The Commonwealth Model Law on Electronic Transactions (2002)[5] was developed based on early UNCITRAL texts, namely the Model Law on Electronic Commerce (1996) and the Model Law on Electronic Signatures (2001)6. Since its adoption, both technology and commercial practices have evolved significantly. In response, national and international institutions have introduced updated legal frameworks to address new realities.

Today, merchants, consumers and governments operate in a digital landscape shaped by global e-commerce platforms, data-intensive social media and the growing influence of artificial intelligence. These developments have given rise to new expectations and standards for lawful and ethical conduct online, necessitating a modernised legal approach to digital trade.

To keep pace with evolving digital trade practices, UNCITRAL has developed several new model laws addressing additional legal dimensions. Among the most significant is the Model Law on Electronic Transferable Records 2017 (MLETR),[6] which enables the legal recognition of electronic equivalents to paper-based transferable documents, such as bills of lading, promissory notes and warehouse receipts, where possession traditionally confers rights to goods or payment.

The current draft of *the Commonwealth Model Law on Digital Trade* is intended to implement the principles and mechanisms set out in MLETR, thereby facilitating the use of electronic transferable records across Commonwealth jurisdictions. UNCITRAL has also adopted the Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services 2022 (MLIT),[7] the Model Law on Automated Contracting 2024 (MLAC)[8] and most recently, the UNCITRAL – UNIDROIT Model Law on Warehouse Receipts 2024.[9]

In summary, this Model Law on Digital Trade replaces the 2002 Commonwealth Model Law on Electronic Transactions, incorporating and updating provisions that remain relevant while introducing new rules to reflect contemporary commercial practices. It also aligns and aims to support the implementation of key instruments adopted by UNCITRAL since 2002, including the MLETR and selected provisions of the United Nations Convention on the Use of Electronic Communications in International Contracts (2005)[10], commonly referred to as the 'Electronic Communications Convention' (ECC).

All these recent instruments rely on 'reliable methods' of ensuring critical characteristics of the transactions they cover. They principally seek to outline how to determine if a method is reliable. The present Model Law aims to unite these reliability

5 The Commonwealth Model Law on Electronic Transactions 2002, https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/P15370_8_ROL_Model_Bill_Electronic_Transactions_0.pdf

6 The UNCITRAL Model Law on Electronic Transferable Records 2017, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

7 The UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services 2022, https://uncitral.un.org/en/mlit

8 The UNCITRAL Model Law on Automated Contracting 2024, https://uncitral.un.org/en/mlac

9 The UNCITRAL – UNIDROIT Model Law on Warehouse Receipts 2024, https://uncitral.un.org/en/mlwr

10 The United Nations Convention on the Use of Electronic Communications in International Contracts 2005, https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications

tests, while respecting earlier criteria for reliable certification services for secure electronic signatures under the UNCITRAL Model Law on Electronic Signatures 2001(MLES).[11]

UNCITRAL's foundational requirement for digital processes is that they should be 'as reliable as appropriate in the circumstances'. While this standard remains, newer UNCITRAL texts, reflected in this Model Law, provide more detailed and practical guidance on assessing reliability, while preserving the flexibility needed to support diverse applications.

This Model Law addresses key challenges of modern digital trade, aligning with international best practices. It enables the conduct of transactions through digital means, including through automated systems and smart contracts, with suitable legal protections. It also includes provisions on data protection, intended to complement the Commonwealth Model Legal Provisions on Data Protection (2003).

This *Guide to Enactment* explains the rationale and intended operation of the Model Law's provisions, helping Commonwealth member countries understand how to adapt and apply them within their domestic legal systems. Effective implementation will strengthen national frameworks for cross-border paperless trade, both within the Commonwealth and with global partners that have adopted similar legal standards, now comprising most international trading jurisdictions.

It is also worth noting that the Commonwealth, through its ministerial forums and Heads of Government meetings, has adopted several related legal instruments impacting digital trade. Member countries undertaking law reform in this area are encouraged to consider implementing these instruments alongside the Model Law on Digital Trade. Each is supported by its own background materials and guidance, to which reference is recommended, and is listed below.

- Commonwealth Model Law on Electronic Evidence[12]
- Commonwealth Model Law on Computer and Computer-Related Crime[13]
- Commonwealth Model Law on Data Protection[14]
- Commonwealth Model Law on Virtual Assets[15]

11 The UNCITRAL Model Law on Electronic Signatures 2001, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

12 Commonwealth Model Law on Electronic Evidence 2002, www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/download/776/776/6064?inline=1

13 Commonwealth Model Law on Computer and Computer-Related Crime, https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf

14 Commonwealth Model Law on Data Protection, https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-02/ROL%20Model%20Law%20Provisions%20on%20Data%20Protection.pdf?VersionId=Fpgmtvhd6E3dm3JfQiEVp8lP0zO_mGy0

15 Commonwealth Model Law on Virtual Assets, https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2024-07/commonwealth-model-law-on-virtual-assets_d19821.pdf

Principles

This *Model Law* provides a legal framework for the use of electronic communications in commercial activities, collectively referred to as 'digital trade'. Commonwealth member Countries are encouraged to adopt the Model Law, either in full or with necessary adaptations to reflect national legal and policy contexts.

A core objective is harmonisation. Many Commonwealth countries are parties to free trade and digital economy agreements that benefit from consistent legal frameworks. Aligning national laws through this Model Law helps reduce legal uncertainty and facilitates cross-border trade.

While the provisions are suitable for domestic trade, a key goal is to support legal interoperability among jurisdictions, thereby lowering barriers to international commerce. The broader the alignment and consistency in implementing this Model Law, the more predictable and efficient digital transactions become. This, in turn, promotes investment, innovation and trust in digital markets.

The *Model Law* is grounded in four foundational legal principles, established by UNCITRAL and widely recognised in digital trade law reform.

- **Functional equivalence**. Ensuring that digital methods are legally equivalent to paper-based processes.
- **Non-discrimination**. Preventing digital communications or documents from being denied legal effect solely because of their electronic form.
- **Technological neutrality**. Avoiding preference for any specific technology or platform, allowing innovation and flexibility.
- **Interoperability**. Promoting systems and standards that enable digital trade across different legal, technical and institutional environments.

Together, these principles provide the legal certainty necessary for digital trade to flourish, both within and across Commonwealth jurisdictions and with many other nations that have also legislated according to these principles.

The **principle of functional equivalence** ensures that electronic data or documents can perform the same legal and policy roles as their paper-based counterparts. The goal is not to establish a separate legal regime for digital documents, but to uphold a uniform documentary framework, allowing existing legal rules to apply regardless of format. Substantive rules governing transactions and relationships do not need to be redrafted simply because those interactions are now conducted digitally.

Functional equivalence also serves as a means of assessing the legal validity of electronic documents. The key question is whether an electronic document is capable, both legally and practically, of fulfilling the role that a paper document would perform under existing laws. If so, it can be treated as legally equivalent.

To support this approach, legislation must generally articulate the underlying policy functions that paper-based requirements serve, such as ensuring that information is in writing, properly signed or presented in original form. The law can then clarify how digital data can meet those same functions, ensuring that digital transactions enjoy the same legal certainty and enforceability as their paper-based equivalents.

The **principle of non-discrimination** ensures that information is not denied legal effect, validity or enforceability solely because it is in electronic form. This guarantees that digital data is treated on an equal footing with paper-based records, provided it meets the substantive requirements of the law.[16]

In essence, electronic information must not be disregarded or diminished in legal value simply due to its format. Digital records can be just as valid and enforceable as their paper counterparts, reinforcing legal certainty in electronic transactions.

The **principle of technological neutrality** holds that laws governing digital data and documents should not prescribe specific technologies or processes for their creation, transmission or storage. Instead, the law should focus on the outcomes or functions to be achieved, allowing parties to choose the tools or methods best suited to their needs.[17]

This approach ensures that legislation does not inadvertently mandate or privilege specific technologies, which could distort the market by limiting compliance with particular systems or tools. Doing so can hinder innovation and competition, especially as newer, more effective solutions may emerge that are incompatible with overly prescriptive legal frameworks. Given that technology evolves more rapidly than legislation, maintaining a neutral legal framework is essential to ensuring long-term relevance, adaptability and legal certainty in the digital economy.

Interoperability refers to the capacity of data and documents to function effectively across different formats, platforms, and legal or institutional settings. This includes the ability to operate in both paper and digital forms, to transition seamlessly between media and to be used flexibly for various purposes, such as commercial, administrative or regulatory functions.

It also encompasses cross-border compatibility, enabling systems, entities and processes to function across jurisdictions regardless of their origin. This is particularly important for international trade, where legal and technical interoperability reduces friction and increases efficiency.

The Model Law has been designed with these needs in mind. It reflects international standards and best practices, drawing on global legal and policy developments to support the most effective approaches to digital trade. In doing so, it not only enhances legal coherence within the Commonwealth, but also contributes to broader international harmonisation.

Importantly, the Model Law aims to ensure reasonable legal and institutional protection for individuals engaging in digital trade.

16 See: UNCITRAL Model Law on Electronic Commerce 1996, Article 5; United Nations Convention on the Use of Electronic Communications in International Contracts 2005, Article 8.

17 See UNCITRAL Model Law on Electronic Commerce 1996, *Guide to Enactment*, para. 20; UNCITRAL Model Law on Electronic Transferable Records 2017, para. 65.

Text Analysis

Preliminary matters

'Data' and 'documents'

Recently, digital trade law has focused on the use and recognition of data as well as documents. For example, some international treaties now consistently refer to 'data and documents'.[18] The legal discussion can no longer be restricted to 'documents', a word that may refer to information in digital form as well as on paper, but with a fixed structure.

It is important to distinguish between **digitisation** and **digitalisation**. 'Digitisation' refers to converting physical documents into digital formats, such as scanning papers into PDF files. While useful for storage and sharing, such files generally do not allow for automated analysis, processing or integration.

In contrast, 'digitalisation', or comprehensive digital transformation, involves rethinking processes and systems to be data-driven, enabling dynamic use, automation and interoperability. Global trends increasingly favour data-centric approaches over static document-based models, particularly in digital trade, where efficiency, analysis and adaptability are essential.

The advantage of dealing with data is that data can be more flexible in how they are processed by computers for different purposes, while retaining the essential commercial and other information required by law (including by laws that may predate the digital era). This Guide will not explore the difference in depth, but an ability to handle both with legal effect is essential to cross-border paperless trade.[19]

Consent

The foundational UNCITRAL Model Laws and the Electronic Communications Convention were based on the principle that no party could be compelled to use or accept electronic information without explicit consent. Such consent could be inferred from conduct, such as the continued use of electronic communications or documents without objection.

This principle served a dual purpose. First, it acknowledged that some individuals were uncomfortable with intangible information and may not have had access to or familiarity with computers. Second, by preserving the right to refuse electronic communications, it allowed parties to accept them only when sufficiently secure methods were used, providing a mechanism for recipients to ensure the trustworthiness of the information received.

18 For example, both terms are consistently used in the UN Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific 2016, https://docs.un.org/en/E/ESCAP/RES/72/4

19 This note is derived from Gregory, J (2024), 'Legal Implementation Guide For Cross-border Paperless Trade', UN/ESCAP. For a detailed discussion of the implications of 'data' in trade matters, see: UNCITRAL (2023), *Taxonomy of Legal Issues related to the Digital Economy*, Part two, United Nations Publication Sales No.: E.12.V.11 ISBN 978-92-1-002939-1, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/digitaleconomytaxonomy.pdf

Since the adoption of the Electronic Communications Convention over two decades ago, the landscape of digital and mobile communications has evolved dramatically. These technologies now play a central role in trade and a wide range of other activities, making it increasingly reasonable to expect parties to engage electronically.

Security concerns are addressed through the common legal requirement that the validity of electronic communications or data messages depends on their reliability. This Guide provides a detailed analysis of what constitutes reliability and outlines the responsibilities for demonstrating its presence, or absence, within a given context.

Another important issue is the technical compatibility of digital documents with the recipient's computer systems. This is especially significant for governments and public bodies that are legally required to receive information from individuals or organisations. In such scenarios, unlike consensual commercial transactions where both parties have a shared interest in seamless functionality, submissions may be made reluctantly, and the sender may not be inclined to facilitate ease of receipt or processing.

To address this, some governments have implemented formal or administrative information technology standards that must be met for any data submitted to them. These requirements help ensure that incoming information is compatible with internal systems and does not pose a risk to public infrastructure.

While the Commonwealth Model Law does not require consent and does not explicitly authorise the imposition of information technology (IT) standards, it leaves room for such measures to be adopted where appropriate to support administrative and operational effectiveness.

Interpretation

Section 1: 20 Definitions

Several terms are defined to clarify their intended meaning within the Model Law. As a general rule, terms used in their ordinary, everyday sense are not defined.

Some definitions, such as 'data message', are adopted from existing UNCITRAL instruments. It is worth noting that the UNCITRAL Model Law on Electronic Transferable Records (MLETR) uses the term 'electronic record' in place of 'data message'. Where this Model Law addresses the same subject matter, it aligns with MLETR terminology. The relevant definition is as follows:

> *'"Electronic record" means information generated, communicated, received or stored by electronic means, including, where appropriate, all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not.'*

There is no indication that the scope of 'electronic record' differs materially from that of 'data message'. One advantage of the MLETR definition is that it expressly encompasses metadata associated with the record. While the definition of 'data message' likely covers this as well, the inclusion in the MLETR text provides additional clarity.

The United Nations Convention on the Use of Electronic Communications in International Contracts defines electronic communications as those made by means of data messages. Its definition explicitly includes, without limitation, technologies such as electronic data interchange (EDI), email, telegram, telex and telecopy (fax). States adopting this Model Law may wish to ensure that the term 'data message' is interpreted in a similarly broad and inclusive manner.

Other terms, such as 'certificate', have been specifically formulated for use within this Model Law. In contrast, terms like 'interoperability' are not defined, as they do not appear in the text of the Model Law itself.

Section 2: Interpretation and application

These provisions reflect a common feature of UNCITRAL instruments: they support the harmonisation of laws across jurisdictions by identifying shared sources and methods for interpreting comparable legal rules in countries that implement the Model Law.

The general principles referred to are those articulated earlier in this document and in the various UNCITRAL model laws previously cited. Other recognised methods of statutory interpretation may also assist in identifying and applying these principles.

In addition to UNCITRAL texts, internationally or regionally recognised legal models may also serve as sources of interpretive guidance. These may originate from intergovernmental, governmental or non-governmental organisations, as well as from international instruments such as digital economy agreements or digital trade frameworks.

---

20 Since the Model Law is intended for use in the Commonwealth, it is divided into 'sections' rather than 'articles', as in the international instruments like the UNCITRAL model laws discussed in the text.

Subsection 2(3) of the *Model Law* anticipates that implementing states may designate specific exclusions from the law's scope. Although the language of the Model Law is framed broadly, its development has been grounded in the context of commercial relations and trade, as indicated by its title. Accordingly, its provisions are most directly relevant and effective in that context.

There may also be categories of communication that are not suitable for general authorisation in electronic form, due either to the sensitive nature of the content or to the identities of the parties involved. Common exclusions include areas such as family law, estates and successions, and matters of national security. Each implementing state will determine its own list of exceptions, guided by national policy priorities and legal traditions.

At the time of adoption of the UNCITRAL *Model Law on Electronic Commerce* (1996), it was common to exclude certain instruments, such as negotiable instruments and bills of lading, whose legal operation depended on their uniqueness. However, subsequent legal developments have addressed these concerns. This Model Law incorporates the principles of the *Model Law on Electronic Transferable Records* (2017), which provides a framework for recognising such documents in electronic form.

In some cases, there has been debate over whether general authorisation for electronic communications should extend to consumer transactions. The concern has been that consumers may be less equipped to protect themselves against insecure or potentially exploitative practices in electronic environments.

This Model Law does not exclude consumer transactions from its scope. Consumers, like businesses, should have the assurance that their electronic transactions are valid and enforceable. Legal protections that apply to consumers in traditional, offline settings are equally applicable to online interactions. If additional safeguards are needed to address risks specific to electronic communications, they can be introduced through separate legislative measures. This Model Law does not seek to provide such protections, but neither does it preclude them.

Electronic Form Issues

Section 3: Validity

Subsection 3(1) articulates the core non-discrimination principle: information in electronic form should not be treated as inherently less valid than information in traditional forms such as paper.

The provision is expressed as a double negative, stating that information 'shall not be denied [...] validity', to reflect the legal reality that both electronic and paper-based information may, in certain cases, be invalid for various substantive reasons. The goal is not to elevate electronic information above other formats, but rather to ensure that its form alone is not grounds for denying legal effect or enforceability.

This approach avoids overstatement. A positive assertion that electronic information is valid in law could be too broad, potentially overriding legitimate grounds for questioning a document's validity. Instead, the Model Law ensures that the mere fact that information is in electronic form cannot, by itself, be used as a basis for denying its legal recognition.

Importantly, this principle supports the interoperability of different forms of communication. It ensures that equivalent legal outcomes can be achieved across different media, electronic or otherwise, thereby facilitating seamless legal and commercial transactions in mixed or digital environments.

Subsection 3(2) addresses the issue of consent, stating that the use of information in electronic form must occur with the express or implied consent of the parties involved. This provision is presented in square brackets to indicate that it is optional and that implementing states may choose whether to adopt it. Unlike the non-discrimination rule in subsection 3(1), this provision is not as strongly recommended.

The rationale for this more cautious endorsement is discussed in detail earlier in this document, under the section titled 'Consent'. While the Model Law does not impose a general requirement for consent, it recognises that in some circumstances, consent may still be appropriate. Where specific types of electronic communication are deemed unsuitable for compulsory use, consent requirements may be introduced in those targeted contexts.

For instance, subsection 35(2), which governs the use of electronic transferable records, includes a consent provision tailored to that specific scenario. Similar measures may be adopted elsewhere as necessary to balance flexibility with user protection.

Section 4: Writing

This section introduces the first of several provisions addressing form requirements in traditional legal systems. These are rules that mandate information to be conveyed in a particular form, medium or manner, often directly or indirectly requiring the use of paper documents.

In most Commonwealth jurisdictions, it is standard for legal frameworks to require certain types of information, such as notices or transactional documents, to be in writing. Globally, there has also been a longstanding view that electronic communications do not satisfy writing requirements. Although this perception is

gradually changing with the increasing use of digital platforms, the UNCITRAL model laws, and this Model Law, are based on the assumption that information in electronic form is not inherently equivalent to writing.

Accordingly, to enable compliance with legal form requirements through electronic means, an alternative approach must be applied. This approach, known as 'functional equivalence', is based on identifying the legal or policy function served by the original requirement and determining how that function can be achieved through electronic formats.

In the case of writing requirements, the generally accepted legal rationale is that writing serves the function of memory. It allows information, whether an agreement, a law or a declaration, to be recorded, preserved and made accessible for future reference and verification.

To reflect this purpose, UNCITRAL introduced a widely adopted standard: information in electronic form must be 'accessible so as to be usable for subsequent reference'. This formulation is used in the Model Law.

The standard does not specify the individual or entity to whom the information must be accessible, in the same way that traditional writing requirements do not indicate who must be able to read or receive the written document. The question of access is governed by other areas of law, including those related to document retention, information rights and contractual obligations between parties.

Similarly, the standard does not define the period during which information must remain accessible. Just as a requirement for writing does not ensure the document is not later lost or destroyed, the electronic form requirement does not guarantee indefinite preservation. Rules that specify minimum retention periods for records are distinct and addressed separately, in this case, under Section 8.

Section 4 addresses particular scenarios where writing requirements apply.

Subsection 4(2) deals with legal obligations to provide information in writing, such as the requirement to deliver written notices. In such cases, it is not sufficient merely to display the document to the recipient; the information must be delivered in a manner that gives the recipient control over it. The subsection captures this requirement by stating that the information must be 'capable of being retained' by the recipient. Importantly, this provision does not require the recipient to retain the information, but rather ensures they have the ability to do so. The responsibility to provide information in a retainable format lies with the sender, while the choice to retain it rests with the recipient.

Subsection 4(3) concerns instances where information must be provided in a specified form, such as a prescribed layout for applications or declarations. This subsection provides that electronic information presented substantially in the same manner as the required format satisfies the legal requirement. The intent is for the electronic version to closely replicate the structure and appearance of the authorised paper version, including elements such as layout, font and spacing, thereby preserving the functional design of the form. The determination of whether the electronic version is sufficiently similar is a matter of interpretation and may ultimately be clarified through judicial decisions. In situations where no official digital version of the form exists, this provision allows for compliance through substantial equivalence rather than strict identity.

Subsection 4(4) applies where legislation or regulations already permit or regulate the use of electronic formats. These provisions may prescribe how electronic information must be formatted, secured, transmitted or, in some cases, explicitly prohibited. This subsection clarifies that such specific legal provisions take precedence over the general permissions set out in the earlier subsections, which operate under the assumption that the governing law is silent on electronic communications. In most cases, such silence is the result of the legal text having been drafted prior to the emergence of electronic media.

Subsection 4(5) ensures that any additional legal requirements concerning the mode of display or method of delivery of information continue to apply when information is provided in electronic form. Examples include obligations to post notices in public or accessible locations or to use a delivery method that provides confirmation of receipt. While the subsection does not specify how such requirements must be fulfilled electronically, it affirms that the underlying legal obligations remain applicable regardless of the medium used.

Sections 5 and 6: Forms

Sections 5 and 6 clarify that where a statute or regulation prescribes the use of a form, the corresponding use of an electronic version of that form is permitted. Additionally, any statutory authority granted to create or prescribe forms is deemed to include the authority to prescribe those forms in electronic format.

However, these provisions are subject to the limitation set out in Section 4(4). If a law expressly requires the use of a written (that is, paper-based) form to the exclusion of electronic versions, that express requirement prevails. In such cases, the general permission to use electronic forms does not override the specific mandate for a written format.

Section 7: Originals

A number of statutes require that certain documents must be presented in original form in order to have legal effect. The underlying policy rationale for this requirement is typically to ensure the authenticity and integrity of the document – namely, that it has not been altered since taking the form intended to carry legal consequences. Drafts or earlier versions are generally excluded for this reason.

Section 7 of the Model Law addresses this issue by allowing the use of electronic versions of documents, provided there are reliable assurances that the integrity of the information has been maintained. Subsection 7(2) establishes that the integrity of an electronic document is assessed by determining whether the information has remained complete and unaltered since it was generated in electronic form, with the exception of any changes arising solely from the process of communication, storage or display.

This standard applies equally to documents that are originally created in electronic form and to those converted from paper to electronic format.

Section 7 introduces the critical concept of 'reliability', a recurring principle throughout the Model Law and a foundational element in electronic and digital legal processes. The concept is further developed in later sections, including:

- Section 20 (foreign signatures)
- Section 21 (certification)

- Section 25 (identification management services)
- Section 32 (trust services)
- Section 36 (electronic transferable records)
- Section 39 (general reliability criteria)

The Model Law adopts the UNCITRAL standard of reliability, which provides that an electronic document, communication or action must be 'as reliable as appropriate in the circumstances'. This standard is intentionally flexible, allowing it to be adapted to a wide range of use cases and technologies. However, its open-ended nature can also lead to legal uncertainty and interpretive divergence. Strategies for addressing that uncertainty are discussed in connection with the specific sections referenced above.

Section 7 specifically incorporates the reliability test developed in the UNCITRAL Model Law on Electronic Commerce 1996 (MLEC).[21] The standard is further contextualised by reference to the purpose for which the document was created. In cases where an electronic document is a reproduction of a paper document, comparison between the two formats may help establish authenticity by revealing any alterations or omissions. In addition, technical assessments, such as analysis of metadata or the integrity of the electronic recordkeeping system or register, may be used to support a finding of reliability.

It is important to note that Section 7 is not intended to support the use of electronic transferable records, where the requirement for integrity is of a higher order due to the essential role these records play in transferring rights. Support for such instruments is provided under Sections 36 and 39. Nonetheless, the standards in Section 7 are not inconsistent with those applicable to transferable records.

Finally, Section 7(1)(b) requires that electronic data purporting to serve as an original must also satisfy the conditions for written information as set out in Section 4(2) – specifically, that the data must be capable of being retained by the recipient.

Section 8: Retention

As noted previously, the requirement that information be in writing, or in an electronic form that satisfies the principle of functional equivalence, does not address the time for which the information must be preserved. That aspect is governed by Section 8, which deals specifically with record retention obligations.

Retention rules may arise in both public and private contexts. They may serve purposes such as compliance audits, evidentiary availability or the preservation of records for future reference. Examples include land title registries and public archives, where the continued accessibility of information may be critical not only to current stakeholders but to future owners or generations.

The core principle of Section 8 is that an electronic version of a record is legally sufficient if it:

i. contains all information required by law;

ii. is presented in a format that is comprehensible and usable for the relevant legal purpose; and

21 The UNCITRAL Model Law on Electronic Commerce 1996, with additional Article 5, is as adopted in 1998, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

iii. remains accessible to any person entitled by law to access it, for the duration required by law.

This requirement incorporates and extends the foundational elements introduced in earlier sections concerning writing (Section 4), forms (Sections 5 and 6), and accessibility (Section 7).

Additionally, Section 8(c) requires that the retained electronic information, where applicable, must indicate whether it was sent or received. This requirement ensures that the history and lifecycle of the record can be established, providing evidentiary value and supporting traceability within both commercial and administrative processes.

Section 9: Extended meaning

Some UNCITRAL model laws refer to legal provisions that either require a particular form or provide consequences for failure to use that form. In addition, legal frameworks may confer specific benefits upon compliance with certain formalities, even if those formalities are not explicitly mandatory. For example, a rule stating that only a signed document will be considered valid effectively creates a signature requirement, despite not using mandatory language.

Such cases do not always align neatly with the formulation that 'the requirement is met' by using an electronic version. This is because the formality may be expressed indirectly, through negative consequences for non-compliance or conditional recognition based on form, rather than through an outright requirement.

Section 9 is designed to address these scenarios. It clarifies that legal provisions that impose negative or conditional consequences for failure to meet a formality are to be deemed as imposing a requirement for the purposes of this Model Law. As a result, the provisions in earlier sections that address the satisfaction of form requirements through electronic means can be applied more consistently and comprehensively.

This approach is consistent with paragraph 67 of the UNCITRAL Guide to Enactment of the Model Law on Electronic Transferable Records (MLETR), which states that such an interpretation is implicit in the term 'requirement'. However, to ensure clarity and legal certainty, particularly for jurisdictions where this implication may be less obvious, the present Model Law includes an explicit provision to remove any ambiguity.

Section 10: Evidence

Section 10 reinforces the non-discrimination principle articulated in Section 3, specifically in the context of evidence. This applies across judicial proceedings, arbitration and any other setting in which information may be treated as evidentiary material.

In particular, Section 10 affirms that the admissibility of evidence may not be denied solely on the basis that it is in electronic form. In doing so, it also addresses a core principle of common law evidence: the 'best evidence' rule. Under this rule, documentary evidence is generally required to be presented in its original form unless a satisfactory explanation is provided for relying on a copy.

While Section 7 of the Model Law deals with the conditions under which electronic versions of original documents can be used, Section 10 complements it by ensuring that electronic documents are not unjustifiably excluded under the best evidence rule. It reinforces the idea that the form of a document, electronic or paper, should not prejudice its evidentiary admissibility.

This position is supported by a practical distinction between paper and electronic originals. Paper originals are difficult to alter without leaving visible signs of tampering, which justifies the preference for originals in evidentiary contexts. In contrast, electronic documents differ fundamentally: a properly created and stored electronic copy is typically identical to the original. Once finalised (that is, no longer in draft form), an electronic document can be replicated without any degradation or distinction, whether it is the first or the hundredth copy.

Accordingly, insisting on an 'original' in the electronic context does not contribute meaningfully to ensuring the integrity of the document. Instead, such a requirement may operate as an unnecessary barrier to the admissibility of valid and reliable electronic evidence.

UNCITRAL's Model Law on Electronic Commerce (MLEC) goes further in Article 9 by addressing the weight to be given to electronic evidence. However, in many common law jurisdictions, legislation generally does not prescribe how adjudicators should assess or weigh evidence once it is admitted. For this reason, that portion of the MLEC is not adopted in the present Model Law.

Nevertheless, the general principle of non-discrimination, as expressed in Section 3, continues to apply both to the admissibility and evidentiary weight of electronic information. It ensures that electronic evidence is treated no less favourably than traditional forms, subject always to contextual and legal standards of reliability and relevance.

Communications

Section 11: Governmental use

Section 11 affirms that governments and other public bodies may use electronic communications both for internal operations and in their interactions with the public. This includes the unilateral delivery of information as well as the exchange of correspondence and documents. The section reinforces the general non-discrimination principle set out in Section 3, ensuring that electronic formats are not treated as inherently less valid in public sector contexts.

The provision is intended to support administrative efficiency and modern service delivery, enabling the use of electronic means for communication, notice, filing and information dissemination. However, practical considerations may arise in cases where the intended recipients of such communications do not have access to or do not use electronic tools, such as computers, mobile phones or the internet. In such situations, it may be appropriate for implementing jurisdictions to limit electronic communications to recipients who have expressly or implicitly consented to receiving information in that form. While the Model Law does not currently include a general consent requirement in this section, implementing states may choose to incorporate such a safeguard to ensure inclusiveness and fairness.

Importantly, Section 11 imposes a responsibility on governments and public bodies to use secure and reliable methods of electronic communication. The provision offers a flexible standard for evaluating reliability, taking into account the purpose, content and intended audience of the communication. This allows governments to adapt communication methods to the sensitivity of the information and the expectations of the recipients.

To operationalise this responsibility, governments may wish to adopt regulations addressing the security, confidentiality and reliability of electronic communications. Such regulations can set out minimum technical standards, authentication protocols or procedural safeguards. Authority to issue these regulations is provided in Section 42 of the Model Law.

Section 12: Time and place of sending and receipt

This provision, inspired by Article 15 of UNCITRAL's Model Law on Electronic Commerce (MLEC), addresses the timing and location of sending and receiving electronic communications. It is particularly relevant in practice, as many electronic messages are not transmitted directly between the communicating parties but are instead handled by intermediaries. The rule establishes that an electronic message is considered dispatched when it leaves an information system under the control of the sender. In many cases, this occurs when the message is transferred to the sender's communications intermediary for delivery. However, if the addressee is part of the same information system as the sender, such as when both parties use the same email service provider, the message is considered dispatched when it is received by the addressee.

The provision also clarifies the time at which an electronic message is deemed received. It distinguishes between cases where the addressee has provided a specific address for receiving electronic communications and cases where no such address has been provided. If an address has been specified, the message is considered

received when it reaches that address and becomes capable of being retrieved by the addressee. This standard ensures that the legal effect of the message cannot be avoided simply because the recipient chooses not to access it. The act of making the message available in a retrievable manner at the designated address is sufficient for it to be deemed received.

In contrast, if the addressee has not designated an address for the receipt of electronic communications, the message is considered received when it becomes capable of being retrieved and when the addressee becomes aware that the message is available. In such cases, the determination of whether these conditions have been satisfied will depend on the evidence presented. The rule sets out a practical framework indicating what each party would need to prove in case of dispute. Notably, the provision includes a presumption that a message stored in an information system accessible to the addressee is capable of being retrieved. This presumption relieves the sender of the burden of proving that technical retrieval was possible.

In addition to addressing the timing of dispatch and receipt, the provision also determines the place where each action is deemed to occur. Unless the parties have agreed otherwise, the place of dispatch is deemed to be the sender's place of business, and the place of receipt is deemed to be the addressee's place of business. These presumptions serve important legal functions, such as establishing jurisdiction and applicable law. For jurisdictions that wish to legislate in greater detail, for example, in situations involving parties with multiple or no identifiable places of business, guidance may be drawn from Article 15 of UNCITRAL's MLEC, which provides a more granular framework.

Section 13: Location of parties

The Model Law does not impose any requirement that parties to electronic communications be located in specific jurisdictions, nor does it require them to disclose their physical location. Nevertheless, other applicable laws may impose such obligations and, in many legal contexts, it is important to establish the location of a party for purposes such as determining jurisdiction, applicable law or tax obligations. To support such inquiries, the Model Law provides default rules to determine a party's location.

A party to a transaction is presumed to have a place of business at a location it has designated as such. This presumption stands unless another party can demonstrate that the designated place is not, in fact, the party's actual place of business. In jurisdictions where businesses are required or permitted to register their official address, that registration may serve as evidence of a designated place of business.

Where a party has not designated a place of business, or where it has more than one, the applicable location is determined by identifying the place that has the closest relationship to the transaction giving rise to the legal inquiry. This determination depends on the information available to the other party involved in the transaction. The rule is intended to strike a balance between flexibility and legal certainty, particularly in cross-border digital transactions.

In the case of a natural person who does not operate a business or otherwise lacks a place of business, the individual's habitual residence is deemed to be the relevant location. This ensures that every party to a transaction, whether an individual or an entity, can be associated with a legally recognised location for purposes of interpretation and enforcement.

The Model Law also makes it clear that certain technological indicators are not determinative of a party's location. Specifically, the mere presence of servers, network infrastructure or information systems in a particular country does not establish that a party's place of business is located there. Similarly, the use of a domain name or email address that is associated with a particular country, such as one ending in a country code top-level domain, does not create a presumption that the party is located in that country.

These clarifications help prevent assumptions based on technical or superficial indicators and instead encourage determinations based on substantive and legally relevant connections to the transaction.

Transactions

Sections 14 and 15: Contracts

This part of the Model Law confirms that contracts may be formed and executed electronically, including through the use of automated systems. It affirms the legal validity of contracts concluded without direct human involvement, recognising that consent, the traditional foundation of contract formation, can be given in advance through the design, deployment or activation of automated processes. A contract may therefore be formed or performed entirely by systems acting autonomously, without any human reviewing the transaction in real time.

This provision serves to implement principles from the UNCITRAL Model Law on Automated Contracting (MLAC) of 2024, incorporating both longstanding and newer elements of electronic contracting. For example, the general acceptance of contract formation through electronic means, including by automated systems, has been well established in international law. As subsection (6) of this provision confirms, the same principle applies to contract performance, that is, the carrying out of contractual obligations, when executed automatically without human intervention.

More recent additions include concepts relating to deterministic and non-deterministic systems, particularly in the context of artificial intelligence (AI). These provisions recognise that when AI tools are used in contracting, the outcomes may not always align with the expectations of the party that initiated the process. Nevertheless, the contract remains valid even if the terms, results or performance conditions diverge from what the initiating party anticipated. In short, parties bear the legal consequences of using automated tools, even when outcomes are unexpected, unless other legal doctrines, such as mistake, misrepresentation or unconscionability, apply.

Importantly, the Model Law does not seek to assign liability for adverse outcomes arising from the use of automated systems. Instead, existing national legal frameworks, such as those addressing negligence, good faith or contractual fairness, will apply. However, the threshold for liability, or the standard of care, may be influenced by a party's voluntary decision to employ such automated systems, especially where foreseeable risks are not mitigated.

Expanding on these principles, the Model Law also contemplates contracts that are written in computer code, rather than natural language. These contracts, commonly referred to as 'smart contracts', may be inaccessible to non-experts but remain enforceable if they meet legal standards for intent and agreement. Additionally, smart contracts may involve systems that automatically react to incoming data or events, such as determining whether a breach has occurred and imposing automated penalties or actions in response. These features reflect the emerging reality of programmable contracts that self-execute based on external inputs or internal conditions.

While the Model Law provides for the legal effect of smart contracts, it also implicitly raises concerns about the protection of vulnerable parties, such as consumers or small businesses. Automated clauses may include onerous terms, operate too rigidly, or trigger default conditions based on flawed or incomplete data. In some cases, the automation of contract performance may override traditional legal safeguards, leading to disproportionate consequences. Implementing jurisdictions may therefore

wish to consider additional protections to ensure fairness, such as enabling review or reversal of automated outcomes in specific circumstances. Legal certainty may, at times, need to yield to reasonable fairness and procedural justice.

The Model Law includes optional provisions, reflected in subsections (4) and (5), to address situations where automation produces results that surprise one of the parties. These provisions, drawn from the square-bracketed language in the MLAC, apply when a result is one the other party knew or should have known would be unexpected. This mechanism may be particularly helpful during the early stages of market adoption of smart contracts, when many parties are still adapting to the use of code-based or AI-driven contracting mechanisms. However, even beyond the transitional period, questions of fairness and reasonable reliance will continue to arise.

It is important to note that these specific provisions do not necessarily render the entire contract void *ab initio*. Whether the affected action voids, modifies or suspends part of the contract will depend on the legal assessment of the impact and context. This approach is comparable to Article 14 of the UN Convention on the Use of Electronic Communications in International Contracts, which permits a party to withdraw a mistaken data entry but does not require the entire transaction to be annulled.

Section 16: Attribution

This provision addresses the attribution of electronic messages or actions to one of the transacting parties. The primary basis for attribution is any agreement between the parties identifying who is responsible for a particular communication or action. In the absence of such agreement, the action is attributed to the party who uses an automated system for the purpose of carrying out the relevant activity. Importantly, attribution is not negated simply because the outcome of the automated system was unexpected. This reflects the principle, developed in the previous section, that the use of non-deterministic or AI-based systems may produce unforeseen results, yet those results can still be legally attributed to the initiating party. However, this attribution rule does not override any applicable rules of law that govern the legal consequences of such attribution. Existing legal doctrines relating to liability, mistake, misrepresentation or other matters remain fully applicable and may influence how attribution affects the rights and obligations of the parties involved.

Section 17: Invitations to make offers

This provision, which mirrors Article 12 of the UN Convention on the Use of Electronic Communications in International Contracts, addresses the legal status of statements directed to the public at large that appear to be offers. It clarifies that such public statements, such as online advertisements, automated listings or digital announcements, are not to be treated as binding offers capable of being accepted unilaterally to form a contract. This safeguard is particularly important in electronic environments, where a single public statement might generate an unmanageable number of acceptances, far beyond the capacity of the publisher to fulfil. Instead, such communications are treated under common law as invitations to treat, and in international legal terminology, as invitations to make offers. The publisher of the original message retains the discretion to accept or reject responses, thereby controlling the formation of contractual obligations in accordance with available capacity and business considerations.

Section 18: Input errors

Section 18, drawing on Article 14 of the United Nations Convention on the Use of Electronic Communications in International Contracts 2005,[22] provides a limited remedy for individuals who make input errors when transacting with automated systems, such as online ordering platforms. Many e-commerce systems offer users an opportunity to verify their orders before submission, typically through a confirmation message such as 'You have ordered X items for [price]. Is this correct?' This verification step serves to reduce the risk of unintentional commitments. However, in the absence of such a prompt, a user may inadvertently submit an incorrect order and find themselves immediately bound by its terms, even though the error was unintended.

To address this risk, Section 18 allows a person who has made an input error when dealing with an automated system to withdraw the erroneous message, provided that two conditions are met: the withdrawal must be communicated promptly, and the user must not have used or obtained any material benefit from goods or services received as a result of the mistaken communication. This provision introduces a practical safeguard for electronic transactions by allowing for limited error correction, without undermining the reliability and enforceability of digital commerce.

22 The United Nations Convention on the Use of Electronic Communications in International Contracts 2005, New York, https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications

Signatures

Section 19: Signatures

The requirement to sign a document, such as a contract, represents another formality or 'form requirement', akin to the requirement that certain information be in writing, as discussed in relation to Section 4. While traditional common law generally does not mandate that a contract be signed in order to be valid, signatures are customary in most transactional contexts. However, specific statutes, such as Statutes of Frauds, may expressly require a signature and, in some cases, other methods of authenticating a document may suffice. Section 19 of the Model Law applies only where a rule of law requires a signature.

A strong argument exists that electronic signatures already meet the legal definition of a signature: they are marks or symbols affixed to a document to associate the signatory with its content and to indicate the signatory's intent. The Law Commission of England and Wales, in reports issued in both 2000 and 2018, recommended against enacting special legislation for electronic signatures, on the grounds that they were already valid as signatures under existing law. Nonetheless, most jurisdictions, both common law and civil law, have chosen to legislate expressly on electronic signatures to provide greater legal certainty.

Subsection 19(1) permits legal signature requirements to be satisfied by an electronic signature, which is defined in Section 1 as 'electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document'. The relevant intent is the intention to sign the document, aligning the legal function of the electronic signature with that of a traditional handwritten signature. The legal relationship between the signatory and the signed text remains unchanged, regardless of whether the signature is handwritten or electronic. The signatory's mental state, intention, consent and approval, retain the same significance. That intention may serve various purposes: to confirm agreement to a contract, to witness another's signature, to acknowledge receipt of a document and so on. In this context, the medium does not alter the message.

Subsection 19(2) allows parties to agree on any form of electronic signature, without mandating that a specific level of reliability be met. This diverges from the UNCITRAL Model Law on Electronic Commerce (MLEC), which includes a reliability test. The Model Law deliberately avoids imposing mandatory reliability requirements for ordinary electronic signatures, as such requirements can be overly restrictive and technologically burdensome. Imposing technical standards could potentially invalidate genuine signatures based on theoretical deficiencies in reliability. Subsection 19(3)(e) is included specifically to prevent such outcomes.

It is generally unlikely that a transacting party who has used an electronic signature would later challenge its validity on grounds of reliability. A more realistic concern arises from third parties, such as tax authorities, creditors or former spouses, who may have an incentive to question or invalidate a transaction based on the electronic signature. For these reasons, the Model Law does not include the general UNCITRAL reliability test for e-signatures. However, subsection 19(3) incorporates the presumed reliability criteria drawn from the UNCITRAL Model Law on Electronic Signatures (MLES). These criteria are not mandatory but serve as useful guidance

for parties assessing whether to accept or rely on a particular electronic signature. They reflect widely accepted international standards and offer a benchmark for good practice.

To provide flexibility, subsection 19(4) authorises enacting jurisdictions to issue regulations requiring the use of particular types of electronic signatures or setting specific reliability thresholds for designated purposes. These regulations may incorporate the standard UNCITRAL test of reliability, namely, whether the method used is 'as reliable as appropriate in the circumstances'. This test also appears elsewhere in the Model Law, including in provisions governing electronic transferable records (see Section 39).

It is important to note that the Model Law uses the term 'electronic signature' rather than 'digital signature'. The term digital signature refers to a specific form of electronic signature, typically created using public-key cryptography (also known as dual-key encryption). Digital signatures are often supported by digital certificates that verify the identity of the signatory and are governed by a framework of legal and technical agreements known as a Public Key Infrastructure (PKI).[23] PKI arrangements involve contracts between the certification service provider (CSP) and the signatory, who receives and uses private signing keys issued by the CSP. These digital signature mechanisms are further addressed in Sections 21, 27 through 33, and 39 of the Model Law.

Section 20: Foreign signatures

This Model Law, consistent with the UNCITRAL instruments that have influenced its development, promotes international trade and interoperability in electronic communications. It encourages the equal treatment of electronic messages and signatures, regardless of whether they originate domestically or from foreign jurisdictions. This principle reflects the Model Law's commitment to legal certainty, cross-border recognition and the removal of unnecessary barriers to electronic commerce.

However, certain cases require a comparative evaluation of reliability, particularly when it comes to electronic signatures or certificates that originate outside the jurisdiction. The principal concern arises when foreign e-signatures, or the certification mechanisms that support them, are presented for legal recognition. Section 20 addresses this issue by establishing that foreign electronic signatures and supporting certificates must be granted the same legal validity as domestic equivalents, provided that their reliability is substantially equivalent to that of the domestic systems.

The Model Law does not prescribe a specific methodology for assessing this reliability or conducting the comparison. Instead, it relies on general criteria for reliability, such as those outlined in subsection 19(3) (for e-signatures) and Section 39 (for certificates and trust services). These sections offer guidance on the technical and procedural indicators that parties or authorities may consider in determining reliability.

23 For a general discussion of digital signatures, see UNCITRAL (2007), *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods*, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/08-55698_ebook.pdf

To further align with its international orientation, subsection 20(2) encourages that the evaluation of foreign electronic signatures and certificates be conducted with reference to relevant international standards. Among the standards that may be considered are those developed or endorsed by UNCITRAL, including the reliability tests set out in the Model Law on Electronic Commerce (MLEC) and the Model Law on Electronic Signatures (MLES). These, in turn, draw from earlier best practices and technical criteria developed by bodies such as the US National Institute of Standards and Technology (NIST).

In addition, more recent international frameworks, such as the Joint Standards Initiative (JSI) co-ordinated under the World Trade Organization, provide an evolving and reputable set of criteria for assessing reliability in cross-border electronic transactions.

The European Union's (EU's) eIDAS Regulation (2014) also offers a structured and influential model for assessing electronic identification and trust services. eIDAS defines multiple levels of assurance, each supported by detailed technical standards. The regulation operates within a comprehensive legal and supervisory framework, ensuring that identification and electronic signatures generated under its rules meet consistent standards of reliability across EU member countries.

National laws in technologically advanced jurisdictions may also serve as models or benchmarks. Countries such as Singapore, Canada and the United Kingdom have developed widely respected legal frameworks for electronic transactions, and their systems are often emulated or cited as standards of reference, both regionally and globally.

Identity, Trust, Reliability

Certification Services

Section 21: Review and certification

A significant portion of this Model Law addresses the concept of reliability and the mechanisms by which it is determined. Many of its provisions rely on the certification of reliability, whether of electronic signatures, systems, services or processes. Section 21 sets out a general framework for certification, designed to apply across all contexts and use cases addressed in the subsequent provisions of the Model Law.

For the sake of clarity, though somewhat arbitrarily, the Model Law adopts a consistent terminology. It refers to first-level certifiers as 'bodies' and to higher-level certifiers, which assess the reliability or operations of those first-level bodies, as 'entities'. Collectively, both are referred to as 'certifiers'. This terminology provides a consistent structure, even though usage in the UNCITRAL model laws is more varied.

The section permits public or private sector bodies to be authorised to certify the existence of specific facts or compliance with particular standards. The Model Law offers flexibility regarding the nature of these certifying bodies. They may include voluntary collectives, industry associations or branches of government. The manner in which they are authorised is not specified within the Model Law, reflecting the diversity of legal systems and regulatory structures. Typically, such bodies may be created or designated by legislation or by regulation issued under another legal authority. In some cases, however, private initiatives may also establish or recognise such bodies. The Model Law accommodates both public and private models and, at a minimum, it affirms the legitimacy of such bodies to operate in this space, provided they are credible to those who rely on electronic trade documentation and data.

Once authorised, bodies created or designated under national legislation will be required to comply with the provisions of the Model Law, as enacted in the relevant jurisdiction. This ensures consistency and legal accountability for the certifiers operating within the framework established by the law.

The Model Law also anticipates the involvement of higher-level certifying entities, as outlined in subsection 21(3). These entities may certify the reliability of first-level bodies or, at a minimum, designate them as compliant with the laws and standards applicable to them. Such designations, when made by an authorised entity, give rise to a presumption of reliability under subsection 21(4). This mechanism streamlines trust in the system and facilitates reliance by third parties, including commercial actors, regulators and courts.

Certifying entities may include trading platforms that host service providers or commercial users, or sector-specific organisations, such as associations representing insurers, freight carriers or supply chain actors in cross-border trade. These entities may also engage third parties, such as technical consultants or auditors, to conduct evaluations and assessments of trust service providers on their behalf, ensuring the necessary expertise is applied.

Transparency is essential in fostering trust in digital trade infrastructure. It is critical that all actors in digital commerce, including trading parties, financial institutions, insurers, legal advisers and technology providers, can access reliable information about certification and reliability designations. To this end, Section 21(5) requires higher-level certifying entities to maintain a publicly accessible record of who and what has been designated as reliable. This record must provide sufficient detail, including references to specific systems, programmes or review processes, so that potential users can confidently identify which certifications or reviews apply to particular services or documents. For example, the documentation provided by the International Protection and Indemnity (P&I) Clubs, which support global shipping and insurance, would typically meet the transparency and credibility standards envisioned by this section.

Identity Management

Section 22: Identification management service provider

One of the most fundamental issues in paperless trade, whether domestic or international, is the question of identity, both of the parties directly involved in transactions and of the supporting institutions and service providers. This issue has two distinct dimensions:

i. identification, which concerns determining who one intends to deal with; and

ii. authentication, which concerns verifying whether the party one is currently communicating with is indeed that intended party.

While the digital age removes traditional means of authentication, such as handwriting analysis, it also introduces new tools. Electronic communications inherently contain metadata, such as timestamps, routing data and source information, which can help to confirm identity. In addition, parties can exchange authentication data directly and may negotiate or agree upon what forms of identification and authentication they will accept and rely on.

Private solutions also play a vital role. Trade associations, industry bodies and non-governmental organisations may develop and promote standards and systems for identifying and authenticating parties, which businesses can adopt voluntarily. Furthermore, specialised organisations have emerged to provide identity management services, offering structured and consistent mechanisms for confirming the identities of transacting parties. The Model Law recognises this evolving landscape in Sections 22 to 26, which govern the operation and reliability of such entities, referred to as identity management service providers (IMSPs).

Global initiatives provide further context. The Global Legal Entity Identifier Foundation (GLEIF), established by the Financial Stability Board (FSB) under the G20, aims to provide each business worldwide with a single, verifiable digital identity. The Model Law accommodates the use of such identifiers in both national and international trade, allowing parties to rely on GLEIF-issued identifiers to enhance trust and transparency in commercial dealings.

The European Union's eIDAS2 initiative, while still under development, offers another example of a structured, cross-border approach to digital identity certification. Although it remains at the conceptual stage, it may eventually serve as a model for other jurisdictions. Implementation of such a system beyond the EU would, however, require significant administrative infrastructure and support, which may not yet exist in all jurisdictions adopting this Model Law.

In the interim, and in the absence of a global identity framework, the provisions set out in this part of the Model Law provide guidance to member countries and private actors. They help define reasonable expectations for identity verification without imposing heavy administrative burdens or requiring sophisticated technological capacity. These provisions may also assist traders in assessing the credibility of identity assertions, either directly or through trusted intermediaries, and help shape future developments in the identity management sector.

There may be concerns that this portion of the Model Law, while based on UNCITRAL's Model Law on Identity Management and Trust Services (MLIT), reflects the European Union's experience too closely. Given the EU's mature institutional and regulatory frameworks, some jurisdictions, particularly within the Commonwealth, may find the emphasis on formality and institutional structure less aligned with local practice. However, the identity management provisions are not mandatory. Commercial parties retain the freedom to adopt any methods they deem appropriate for identifying and authenticating counterparties. What the Model Law offers is a set of tools and best practices to inform and strengthen that process.

By including these identity management provisions, the Model Law provides parties with greater clarity and confidence in assessing identity, while supporting the potential development of specialised identity service businesses. Their inclusion is consistent with the Model Law's broader objective: to operationalise and extend the principles of UNCITRAL's e-commerce framework in a way that is practical, flexible and forward-looking.

Section 22 outlines the functions of an identity management service provider, focusing on its role in facilitating digital trust and secure electronic transactions.

Section 23: Duties of an identity management service provider

Section 23 outlines the core functions and obligations of an identity management service provider. It requires the provider to operate not only in accordance with the Model Law, but also in compliance with its own publicly available rules and procedures. A central duty of the provider is to ensure that the identity management process, including the methods used and the outcomes of identification, is made transparent and accessible. This information must be available to the provider's direct clients, referred to as 'subscribers', as well as to relying parties and other third parties who may base decisions on the reliability of the identification.

In addition, the identity management service provider must clearly disclose any limitations on the scope or purpose for which an identification is valid. This includes specifying the contexts in which the identification may or may not be relied upon, as well as any limitations of liability for errors, inaccuracies or failures in the identification process. Such disclosures are essential for managing expectations and reducing the risk of reliance on information beyond its intended scope.

Finally, the provider is required to establish and maintain a mechanism that allows subscribers to report security breaches. A breach in this context refers to any event that could compromise the reliability or integrity of an issued identification. Prompt notification and response mechanisms are critical to maintaining trust in the identity management framework and ensuring that both subscribers and third parties can respond appropriately to emerging risks.

Section 24: Duties of subscriber to identity management services

Subscribers to an identity management service also bear important responsibilities under the Model Law. Chief among these is the duty to promptly notify their identity management service provider of any security breach that could compromise the reliability of their identity credentials, that is, the digital certificate or other identifier

issued by the provider that attests to their identity. This reciprocal obligation helps maintain the integrity of the identity management system by ensuring that potential vulnerabilities are addressed as quickly as possible.

The Model Law does not specify procedures for resolving disputes that may arise in connection with identity management services. Such disputes, whether between subscribers and providers or involving third parties, must be handled through existing dispute resolution mechanisms, including domestic courts or arbitration. While implementing jurisdictions are free to establish specialised tribunals or regulatory mechanisms to oversee identity management systems and resolve related disputes, the Model Law imposes no requirement to do so. This flexible approach allows each jurisdiction to tailor dispute resolution to its legal infrastructure and resource capacity, while ensuring that identity management practices remain legally accountable.

Section 25: Legal effect of electronic identification

Electronic identification must not be challenged solely on the basis that it was performed electronically. Similarly, while the Model Law allows for an identity management service provider to be designated as reliable by a higher-level certifying entity under Section 21, the absence of such a designation does not, in itself, invalidate the provider's identification services. These provisions ensure that electronic methods of identification are not disadvantaged by default and that reliance on them remains legally secure, provided they meet appropriate reliability standards.

Where a legal requirement exists to identify a person for a particular purpose, that requirement is deemed to be satisfied if the identification method used is appropriately reliable, as assessed under the general reliability standards established in Section 39. To provide additional legal certainty, section 23(3) states that identification will be presumed appropriate if it is shown, in fact, to have fulfilled its intended purpose. In disputed cases, parties may introduce supplementary evidence, including but not limited to the data generated by the electronic identification process, to demonstrate the reliability and adequacy of the method used.

This flexible approach accommodates non-electronic methods of identification and authentication where business circumstances justify their use. The Model Law does not mandate a purely digital approach but rather emphasises practical reliability, thereby supporting diverse commercial environments and technological capacities.

Some stakeholders have proposed the addition of a formal dispute resolution mechanism for cases involving contested or compromised identity verification, such as an appeal process or regulatory oversight body. However, in keeping with the Model Law's decentralised and adaptable structure, the resolution of such disputes is left to domestic law. Jurisdictions implementing the Model Law are free to adopt their own mechanisms based on local legal infrastructure, administrative capacity and policy preferences. Uniformity in dispute resolution is not required under the Model Law and is deliberately left open to national adaptation

Section 26: Determining reliability of identification management services

Section 39 of the Model Law establishes a set of reliability criteria that apply across various processes governed by the statute, including, but not limited to, identification management, electronic signatures and trust services. These criteria serve as a

flexible benchmark to assess whether a particular electronic method, system or provider meets the standard of being ‘as reliable as appropriate in the circumstances’. This approach allows for technological neutrality and scalability, enabling both public and private actors to evaluate reliability based on context, purpose and available safeguards.

Trust Services

Section 27: Trust service provider

Identification and authentication mark only the starting point of an online commercial relationship. As that relationship develops, a more comprehensive and ongoing element becomes essential: trust. Trust underpins the entire lifecycle of digital transactions – from the formation of agreements to their execution and enforcement. It is critical for relying on electronic signatures, electronic seals and electronic time stamps, which confirm the timing of key actions such as message receipt, offer submission and delivery completion. Trust services also play an essential role in verifying the ownership of websites, the integrity of digital archives and other key aspects of digital infrastructure.

Section 27 introduces the concept of a trust service provider, setting out the potential scope of services such providers may offer. While a non-exhaustive list of functions is referenced, the Model Law deliberately leaves the definition open-ended, allowing for evolving forms of trust services to be recognised as technology and practice develop.

Among the most prevalent roles of a trust service provider is the support of electronic and digital signatures. In this context, the provider may be referred to as a 'certification service provider (CSP)', a role that involves issuing and managing digital certificates that verify the identity of signatories and the authenticity of their signatures. The Model Law addresses further aspects of CSP operations in the sections that follow.

The direct clients of trust service providers are known as 'subscribers', who receive and use the trust services to facilitate secure and verifiable digital transactions. These services are foundational to building legal certainty and commercial confidence in electronic trade.

Section 28: Duties of trust service providers

Many of the obligations of a trust service provider closely mirror those imposed on identity management service providers, as set out in Section 23. Trust service providers must establish and adhere to published operating rules and standards, ensuring that these are made readily accessible to their subscribers, as well as to relying parties and other interested third parties. In addition, they are required to clearly disclose any limitations regarding the purpose, scope or value of the trust service provided, along with any limitations on their liability in the event of error, failure or misuse.

Where electronic signatures are involved, trust service providers have a further duty to facilitate transparency and verification. They must enable relying parties to easily determine the method used to identify the subscriber (that is, the signatory), the validity of the signature data, and whether a mechanism exists for revoking or suspending the associated certificate in cases where the integrity of the signature or identity has been compromised. These requirements ensure that trust in the digital environment is not only presumed, but also verifiable and legally supported.

Section 29: Breach of security

The integrity of digital trust is grounded in strong cybersecurity and, for this reason, the Model Law, consistent with UNCITRAL and other international frameworks, imposes important obligations on trust service providers and their subscribers to uphold security and respond effectively to breaches.

Section 29 requires that trust service providers take immediate steps to contain and, where possible, remedy any significant security breach. If a breach cannot be resolved swiftly, the provider is expected to suspend or shut down the affected services for impacted subscribers to prevent further risk. In such cases, the provider must also issue timely notice to both subscribers and relevant public authorities, recognising that security incidents may have rapid and far-reaching consequences across digital networks.

In addition, trust service providers must offer their subscribers channels for reporting suspected or confirmed compromises, particularly those affecting the integrity of trusted data, such as the data used to generate electronic signatures. Ideally, these mechanisms should also allow communication to third parties who may rely on the compromised trust data, thereby helping to limit potential harm.

The Model Law does not define what constitutes a 'significant impact' on services, acknowledging that this will vary depending on the context. The nature of the impact may differ; for some parties, the concern may be financial loss, for others, it may be the exposure of sensitive personal data or confidential business information. Similarly, the Model Law does not prescribe which public authorities should receive notification. In many cases, law enforcement agencies may be appropriate recipients, but in others, specialised authorities such as financial regulators, data protection agencies, securities commissions or customs authorities may be more relevant.

Implementing states are free to add specificity to these provisions, including defining thresholds for notification and designating appropriate authorities to receive breach reports. Many jurisdictions already have data breach notification laws, particularly around privacy and data protection, and may draw from existing formulations such as 'significant risk of harm' or 'risk of significant harm'. The interpretation of these thresholds may vary, but the underlying objective remains consistent: to ensure transparency, accountability and timely mitigation of harm resulting from security breaches.

Section 30: Duties of subscribers

Subscribers to a trust service have a critical obligation to maintain the confidentiality of the data used to generate their electronic signatures. This duty is foundational, as unauthorised access to such data would enable third parties to forge electronic signatures, potentially undermining the integrity of entire transactions. Compromises may occur through various means, including inadequate record-keeping, weak security protocols or malicious cyberattacks. When a subscriber, or the service provider, knows or reasonably suspects that a substantial risk of compromise exists, they are required to notify the trust service provider and any other parties who may be affected, such as transaction counterparties. Additionally, the duty to maintain the accuracy and security of the signature-related data continues throughout the lifecycle of the certificate and the associated signature, ensuring sustained trust in the digital credentials over time.

Sections 31 and 32: Legal effect of trust services

Section 31 reinforces the non-discrimination principle that is an essential element in the Model Law: the legal validity of a trust service, typically reflected in the form of a certificate with specified content, cannot be denied solely because the service is delivered electronically. This provision ensures that trust services are afforded the same legal recognition as their traditional counterparts, maintaining consistency with the broader objective of enabling paperless and technology-neutral commerce. Moreover, a trust service is not invalidated merely because the trust service provider has not been designated as reliable by a higher-level certifying entity under subsection 21(3). This safeguards the legal effect of trust services even when a formal designation of reliability is absent, provided the service otherwise meets applicable legal standards.

Section 32 sets out the general rule for the legal effect of trust services: where the law requires a certain assertion, such as a time stamp, a certification of identity or the confirmation of an electronic signature, that requirement is satisfied if the assertion is made using a method that is reliable. Reliability may be established either by showing that the method is as reliable as appropriate in the circumstances, or by demonstrating that it in fact produced a result consistent with the legal requirement.

Notably, the Model Law does not impose a reliability standard on the electronic signature itself; instead, it focuses on whether the method used to generate or support the signature, such as a trust service, meets the necessary level of reliability. While business parties will naturally assess the perceived reliability of a signature, the technical legal validity does not depend on such subjective considerations. However, when a trust service is used to support or authenticate the signature, that service must meet the standard of being as reliable as appropriate, reinforcing the importance of trust services in maintaining legal and evidentiary integrity.

Importantly, where a trust service has been designated as reliable by a higher-level certifying entity under Section 21, it is presumed to be reliable for the purposes of meeting legal requirements. This presumption facilitates efficiency and confidence in electronic transactions, while still allowing for rebuttal where evidence to the contrary exists.

Section 33: Determining the reliability of trust services

Again, the concept of reliability in this context is assessed with reference to the criteria set out in Section 39 of the Model Law. These criteria provide a flexible, context-sensitive framework for determining whether a method or service, such as those offered by a trust service provider, is 'as reliable as appropriate in the circumstances'. This ensures consistency across the Model Law while allowing adaptability to different technologies, sectors and risk levels.

Electronic Transferable Records

Section 34: Definition of transferable record

This provision marks the beginning of a series of sections intended to implement the UNCITRAL Model Law on Electronic Transferable Records (MLETR), a landmark instrument with the potential to significantly enhance digital trade. MLETR facilitates the legal use of electronic transferable records, electronic equivalents of documents that traditionally convey rights to payment or to property by possession of the physical instrument.

Section 34 introduces the concept of transferable records by listing examples of such instruments, including bills of lading, warehouse receipts, bills of exchange and cheques. The list is illustrative, not exhaustive, and highlights the broad range of instruments used in commerce that rely on the ability to transfer rights through possession in their paper form.

MLETR refers to the paper versions of such instruments as 'documents' and the electronic equivalents as 'records'. However, international terminology is not consistent, and different sectors may use various terms. In recognition of this, the Model Law adopts a flexible approach, allowing any terminology, such as document, record or instrument, to be used, as long as the function is consistent with the principles of transferability. Where the legal context requires clarity, the Model Law follows UNCITRAL's usage of 'records' to describe the electronic version, and this will be made explicit where necessary in the text.

One of the distinctive features of electronic transferable records is that they may be relational in nature; that is, their components may not reside in the same digital location or system. This is similar to the structure of electronic signatures, which are often described as being 'in, on or logically associated with' a document. The 'logical association' may be situational or technical (for example, cryptographic). However, the relationship between components must be clear and verifiable to all parties who may rely on the record. In practice, this could allow different components of a transferable record to be supported or verified by different entities acting on behalf of the intended party.

Despite this complexity, the law treats the electronic transferable record as a single legal entity, akin to a paper document. This simplifies its legal treatment and aligns with commercial expectations of a unitary, transferable instrument.

MLETR is intended to apply to existing, well-established categories of transferable records, rather than to create or validate new types of paper-based instruments with similar characteristics. Its purpose is to enable the digitisation of known and widely used commercial documents, thereby supporting their continued relevance in international trade. Should new types of transferable records emerge, their legal treatment and reliability standards would need to be developed independently, based on their unique features and use cases. The applicability of MLETR's principles to such new instruments would have to be assessed case by case.

Subsection 34(3) provides for certain exclusions from the scope of this part of the Model Law. Specifically, shares, bonds, and other investment instruments are excluded. This reflects their fundamentally different regulatory and legal treatment. The provision also leaves room for additional exclusions by implementing jurisdictions, consistent with the UNCITRAL Guide to Enactment of MLETR.

According to this Guide, jurisdictions may consider excluding:

a. documents and instruments that may appear transferable but should not be treated as such for the purposes of the law;

b. instruments governed by specific international conventions, such as the Geneva Conventions of 1930 and 1931 on Bills of Exchange, Promissory Notes, and Cheques; and

c. purely electronic transferable records that do not correspond to a paper-based counterpart.

These exclusions aim to ensure legal clarity, prevent overlap with other legal instruments, and allow jurisdictions to tailor the law to their domestic legal frameworks and policy objectives.

Section 35: Legal effect of using electronic transferable records

This section affirms the core non-discrimination principle of the Model Law: a transferable record in electronic form must not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic rather than paper form. This ensures consistency with other foundational provisions of the Model Law and promotes technological neutrality in trade and commerce.

In addition, the section introduces a consent requirement, recognising that the use of electronic transferable records cannot be imposed unilaterally. No party is obliged to accept such a record in electronic form unless it has consented, either expressly or implicitly through conduct. This respects the autonomy of parties and acknowledges that engaging with electronic records, particularly those with legal or financial implications, involves a level of trust and technical understanding that not all parties may yet possess.

Importantly, the validity of an electronic transferable record under this framework depends on the use of reliable methods to establish and maintain its legal and functional characteristics. These include demonstrating singularity, integrity, authorship, endorsement and transfer of control. As noted in UNCITRAL's Guide to Enactment of MLETR, the test for reliability is context-specific: what is 'reliable' for one function may not suffice for another. This nuance places a burden on parties, particularly in complex commercial settings, to assess technical and legal sufficiency on multiple fronts.

Given this complexity, some business actors may be hesitant to accept electronic transferable records out of concern for legal risk or technical uncertainty, particularly where mistakes in reliability assessment could carry financial consequences. This justifies the need for a voluntary adoption model, grounded in informed consent.

Nonetheless, the commercial pressure to shift toward electronic formats, driven by gains in efficiency, cost reduction and speed, may render paper-based resistance increasingly impractical. For instance, several global shipping carriers are actively

transitioning toward fully electronic bills of lading, signalling a market-driven evolution that may leave merchants and trading partners with diminishing practical choice in the long term.

Section 36: Using electronic transferable records

This provision authorises the use of electronic versions of transferable documents, records or instruments, terms used inclusively to encompass any data with commercial significance, provided that the electronic record contains all the information required by its paper-based counterpart. The formulation is deliberately broad to ensure coverage of all relevant instruments commonly used in commerce and trade.

Paragraph 36(b) enumerates the key features that must be reliably present in an electronic transferable record for it to have full legal validity. These features mirror those in the UNCITRAL Model Law on Electronic Transferable Records (MLETR), with additional influence from the United Kingdom's Electronic Trade Documents Act 2023 (ETDA).[24] The listed elements collectively aim to ensure that the electronic equivalent is functionally and legally interchangeable with the traditional paper document.

One of the most significant innovations of MLETR, and adopted here, is the replacement of the traditional concept of 'possession' with that of 'control'. In the paper world, possession serves as the basis for enforcing the rights embedded in a transferable document: the person who physically holds the document is entitled to claim the goods, payment or performance it represents. In the digital environment, where physical possession is meaningless, the legal framework substitutes exclusive control as the equivalent functional concept.

To establish the validity of an electronic transferable record, it must be demonstrated that the record is UNCITRAL that it is subject to exclusive control and that the person asserting rights under the record exercises that control. This principle is aligned with the MLETR and is echoed in the ETDA, which also permits indorsement and disposal of electronic records based on demonstrable control. While the UK statute defines control operationally – 'a person exercises control of a document when the person uses, transfers, or otherwise disposes of the document' – the present Model Law and MLETR adopt a functional, fact-based approach without prescribing a fixed legal definition.

The notion of exclusive control is critical. Control must be transferable, but it must also be exclusive at all times; when it is transferred, the transferor must relinquish all control so that only the transferee can assert the rights attached to the record.

This requirement addresses a fundamental issue in common law systems, where 'information' is not recognised as property and cannot be exclusively owned. In theory, one can transmit information to another party and still retain it and even transmit it again. Such replication is problematic in the context of transferable records, which require that rights to performance or property can attach to only one party at a time. Therefore, the form and structure of the electronic transferable record, the 'container' that gives the information legal effect, becomes essential. The information alone, without the defined and controlled electronic record, has no standalone legal force in this context.

24 The UK Electronic Trade Documents Act 2023, www.legislation.gov.uk/ukpga/2023/38/contents

The various elements listed in section 36(2) are designed to establish and preserve the legal integrity of the electronic record. This includes the creation method, which must preserve the integrity of the record, and mechanisms for conversion between electronic and paper formats. However, the law requires that only one valid version of the record can exist at any given time, and it must always be clear which version is active and who exercises control over it.

Because of the unique legal function and risks associated with transferable records, the criteria for validity and reliability are more numerous and stringent than for other types of electronic records addressed in the Model Law. Section 39 sets out specific factors for evaluating the reliability of methods used in the creation, management and transfer of electronic transferable records.

Section 37: Validity of foreign electronic transferable records

This section prohibits the discriminatory treatment of an electronic transferable record solely on the basis that it was issued or used in a foreign jurisdiction. This provision aligns with the broader principle of non-discrimination embedded throughout the Model Law, which seeks to ensure legal interoperability and cross-border recognition of electronic documents and data. It reinforces the objective of facilitating international trade by removing barriers based solely on geographic origin. The only notable exception within the Model Law framework relates to foreign electronic signatures, which are subject to a comparative reliability assessment, as discussed in earlier provisions.

Section 38: Determining reliability of electronic transferable records

The criteria for determining the reliability of electronic transferable records are established in Section 39, consistent with the approach taken for evaluating trust services and other reliability-based assessments throughout the Model Law.

Reliable Services

Section 39: Reliability

UNCITRAL's test for reliability 'as reliable as appropriate in the circumstances' serves as the overarching standard throughout this Model Law. In some instances, this standard includes consideration of whether the parties to a transaction have reached a prior agreement on the applicable processes or practices, reflecting both flexibility and respect for commercial autonomy.

Section 39 consolidates the criteria for determining reliability across the various trust services recognised under the Model Law, including digital data certified by identification and trust service providers. It also provides the key benchmarks for assessing the reliability of the elements required for electronic transferable records, as outlined in section 36(b). These criteria are referenced in multiple sections throughout the Model Law, offering both statutory support and interpretive guidance.

By identifying the importance of these factors, the Model Law facilitates consistency and legal certainty, particularly for jurisdictions or stakeholders less familiar with electronic commerce practices. This structured approach can assist public authorities, courts, arbitrators and business users in evaluating reliability, whether through formal certification or direct, case-specific judgment.

Where a relying party assesses reliability independently, without recourse to a certification service provider or another trusted third party, relevant sections of the Model Law often include contextual criteria. For example, Section 7, which addresses the use of electronic versions of original documents, outlines specific indicators of reliability. Similarly, Section 19, on electronic signatures, details reliability requirements such as exclusive control by the signatory over the signature creation method. In such cases, the relying party bears the burden of satisfying itself that these criteria are met. If a trust service provider is involved, the necessary assurances should be available through the associated certificate or trust service documentation.

Notably, the process of reliability assessment is typically ex post, meaning it occurs after the digital data has been received by the intended relying party (though possibly before it is relied upon). If disputes arise, such evaluations may be subject to judicial or arbitral review. Even in cases where the law does not mandate reliability, practical business considerations will usually lead parties to seek reasonable assurance before relying on electronic data. The factors set out in Section 39 can be instrumental in making such judgments.

Section 39 is organised into three categories of criteria, each inspired by UNCITRAL model texts:

1. Subsection (1) sets out reliability criteria specific to electronic transferable records, although many of these apply more broadly to other forms of digital data under the Model Law.
2. Subsection (2) focuses on the reliability of certificates and the entities that issue them, including trust and identification service providers.
3. Subsection (3) introduces a pragmatic safeguard: even if the method or source is not theoretically sound, the record will be deemed reliable and legally valid if it can be shown to have functioned reliably in practice

The separation of MLETR-consistent criteria in the first subsection is intended to promote the use and acceptance of electronic transferable records and to support cross-jurisdictional consistency in the treatment of these vital instruments in international trade.

Subsection 39(1)

Subsection 39(1) sets out many circumstances that support reliability of electronic transferable records and other digital data. Not all of them will apply to all data whose reliability is to be evaluated. The UNCITRAL Guide to Enactment of MLETR says that each of the elements needing a reliable method to create them may be supported by different reliable methods, and that what is appropriately reliable may be different for each element.

MLETR lists a number of ways that reliability may be demonstrated – and these are included in subsection 39(1) – but this list is not exhaustive. All of the reliability tests are factors that may exist to a greater or lesser extent; they are not 'yes/no' tests that make something reliable or not, legally valid or not.

Some criteria are more flexible or matters of judgment than others. Reliability testing is an open process. The MLETR Guide to Enactment makes it clear that a relying party may use any or none of the methods set out in MLETR. The relying party may use other factors as well or instead.

In short, the list is not mandatory; that is, a relying party will not have to show, to support validity or business-centred reliance, that it has considered each factor or evidence relevant to each factor.

It may be noted in respect of electronic transferable records that the reliable methods for their valid and successful use may be created by the parties presenting the transferable record and evaluated by the relying party and its advisers and allies, without a professional trusted third party as intermediary.

Businesses seeking to rely on electronic transferable records will need to satisfy themselves of the reliability of the seven factors that MLETR lists (and that are listed in section 36(b)) – uniqueness (identified effective record), fact of control of the record, identity of the person with control, ability to effectively transfer control, retention of integrity of the record, tracking of amendments to it and the change of medium from paper to electronic or vice versa.

If the businesses are not going to use trust service providers, then they can best decide for themselves how they prove compliance. The Model Law does not tell them how to do this.

However, MLETR, and this Model Law in following it, do set out in this section indicators of reliability, mainly focused on testing, auditing and certification. It is a matter of being able to evidence the degree to which the system functions in accordance with its specifications, as required by this legislation and sound commercial practice.

Potential relying parties will decide whether this needs to be done by independent testing prior to roll-out, in the absence of trusted third parties. It will probably be easier to find or produce such evidence in some countries or economies than in others.

Business circumstances, including the supports available to evaluate the data relating to the transactions, will vary from place to place and from time to time. The opinions of insurers, financial institutions, technology providers, other participants in

trade supply chains, and legal counsel may all play a part in the decision to rely. The UK statute, the UK Electronic Trade Documents Act 2023 (ETDA), already referred to speaks of reliable systems and not reliable methods to support the essential elements of the records.

The section allows for reference to a 'voluntary scheme or industry standard'. This could extend to widely accepted digital trading platforms or systems by which an industry promotes reliable practices among its members.

Moreover, other guidance is available from experts in digital trade, including trade associations and vendors of digital trade systems. A recent example is the Reliability Appraisal Framework published by the International Chamber of Commerce's Digital Standards Initiative (DSI) and the Digital Governance Council of Canada (DGC).[25] This tool can be used both by creators of electronic transferable records, to increase their acceptability in the market, and by potential relying parties in deciding on their validity and use.

The ICC/DSI tool is also expected in time to lead to a certification process, which in turn could be evaluated under the criteria set out in subsection 39(2) of this Model Law.

As a result, electronic transferable records may be more readily accepted in some countries than others, as commercial and legal supports become available.

Among the criteria in subsection 39(1) that apply to evaluate reliability of other trusted documents (and identified as such in other UNCITRAL model laws) are 39(1)(b), the financial and human resources of the body asserting trustworthiness; s.39(1)(c), the quality of the body's hardware and software systems, and s.39(1)(f), the regularity and extent of an independent audit. All of these can apply to judging electronic signatures and their certificates, and the work in support of other digital data set out earlier in the Model Law.

Subsection 39(2)

Subsection 39(2) mainly expresses criteria for reliability of certificates, which have not been a feature of electronic transferable records. The extent to which a certifying body or reviewing entity complies with the law and its own relevant operational rules is also a factor in its reliability. Whilst this is not mentioned within MLETR, so it is listed in this subsection of the ML in the best interest of completeness. As, someone evaluating the reliability of an electronic transferable record could also take these factors into consideration, if they appeared to be helpful.

By way of example, should the Reliability Assessment Framework recently published by the ICC's Digital Standards Initiative develop to supporting a certification process, then those certificates would stand to be assessed for reliability under subsection 39(2) – depending on the drafting of that subsection.

Subsection 39(3)

Subsection 39(3) of the Model Law recognises that reliability can be demonstrated in fact, not merely in theory or by reference to external indicators such as certification, compliance with standards or system design. Where a relying party can show that

25 See: Information about the Appraisal Framework, https://iccwbo.org/news-publications/news/icc-dsi-launches-digital-trade-reliability-assessment-tool/

the necessary elements of a digital record or system were present and functioned as required, the record will be deemed reliable and will satisfy the applicable legal validity requirements, regardless of any theoretical concerns about potential vulnerabilities.

This approach ensures that practical evidence of performance can prevail over abstract doubts. It supports business confidence in electronic records by focusing on what actually happened in the specific case, rather than hypothetical weaknesses in the technology or process used.

However, it is important to understand that none of the reliability tests set out in Section 39, including demonstrated, factual reliability under subsection (3), constitutes a legal guarantee. Even when one or more criteria are satisfied, the digital record in question may still turn out to be inaccurate, incomplete, corrupted or fraudulent. In such cases, the relying party bears the risk and may suffer financial or legal loss.

Moreover, it is common for certifying bodies and other entities involved in assessing or endorsing reliability to include explicit disclaimers of liability. These disclaimers are designed to limit or exclude their legal responsibility for any reliance placed on their certifications or assessments, regardless of their content or formality.

In short, subsection 39(3) provides a practical, business-oriented means of establishing reliability based on real-world performance. But it does not override the fundamental rule that all reliance on digital records involves risk, and that risk must be managed by due diligence, contractual protections and sound commercial judgment.

Subsection 39(4)

Subsection 39(4) affirms that neither the foreign origin of a trust service provider nor the fact that the data under evaluation was generated or processed abroad shall, in itself, affect the assessment of reliability.

Subsection 39(5)

Subsection 39(5) provides an exception to the general rule in subsection 39(4) for electronic signatures originating from a foreign source or certified by a foreign trust service provider. In such cases, the evaluation of reliability must follow the criteria set out in Section 20, which require a comparative assessment of the foreign process or provider against the standards applicable to domestic counterparts.

Data Protection

Data protection is a critical component of trust in digital trade. In 2023, the Commonwealth adopted Model Legislative Provisions on Data Protection, which are recommended for implementation by member countries seeking to enhance digital trade and the broader use of digital communications.

However, those provisions are limited in scope to the protection of personal data belonging to individuals. They do not extend to commercial information. To address this gap, the present Model Law introduces two supplementary rules specifically for the holders of commercially relevant data.

Section 40: Duties of Data Controllers

Subsection 40(1) imposes a duty on data holders to safeguard commercial data from degradation and loss, and to ensure that access is granted only to individuals or entities who are entitled to it, and only to the extent necessary for the exercise of those entitlements.

Subsection 40(2) aims to guarantee that access rights are not only legally recognised but also practically effective. It requires that any interruption in access be addressed and remedied promptly.

Subsection 40(3) regulates the access of public authorities to commercial data. It responds to concerns that the Commonwealth's personal data provisions may provide excessive discretion to public or law enforcement bodies. Accordingly, this subsection limits such access to situations where no reasonable alternative exists, and only where the data in question are essential for the proper discharge of the authority's functions.

This section does not explicitly address intellectual property rights, such as trade secrets, which are already protected under the common law in most Commonwealth jurisdictions. Nevertheless, the adoption of this Model Law may present an appropriate context for jurisdictions to consider enacting or strengthening legislative protections for trade secrets, if desired.

Section 41: Conflicts of interest

This provision is designed to ensure that entities holding or transmitting commercially valuable data on behalf of others do not derive personal or commercial gain from that data, whether or not such use directly conflicts with the interests of the data's rightful owners or recipients.

It applies in particular to entities such as single window operators or digital trading platform providers, which often manage confidential and commercially sensitive information in the course of facilitating trade. The aim is to uphold the integrity of digital trade systems by preventing unauthorised exploitation of such data and affirming the custodial or fiduciary responsibilities of those entrusted with its handling.

Final Provisions

Section 42: Power to make regulations

Section 42 authorises the body that ordinarily holds regulatory authority under domestic law to make regulations necessary to implement and give effect to the provisions of this Model Law. As with any regulation-making power, such regulations must remain within the scope of authority granted by the enabling legislation. This provision enables jurisdictions to tailor regulations to their specific operational, legal or policy needs, ensuring the effective application of the Model Law in diverse national contexts.

Section 43: Short Title

The law in many jurisdictions require the official title to include all the principal elements of the legislation. Section 43 provides a short title by which the statute can effectively be referred to.

Section 44: Coming into force

Section 44 enables implementing states to determine the commencement date of the statute. Where existing legislative frameworks already permit flexible commencement, such as partial or staged proclamations, allowing different provisions to come into force at different times, no additional language is necessary. However, if such flexibility is not otherwise provided for in the jurisdiction's general law and is considered desirable for the implementation of this Model Law, Section 44 provides the necessary authority to legislate that flexibility.

Liability

This Model Law does not establish rules concerning criminal or civil liability. Questions of civil liability will generally be addressed under existing legal principles, such as negligence or intentional torts, without requiring further elaboration within this statute. Where specific provisions for liability, such as strict liability or a reversal of the burden of proof, are considered appropriate, implementing states may introduce such measures through supplementary legislation.

The Model Law also refrains from prescribing specific standards of care for the use of data. While the activities it contemplates may be novel, the foundational legal principles governing liability remain unchanged and may be applied using established jurisprudence. In this regard, the evolving case law of other common law jurisdictions may offer valuable guidance to courts and policy-makers.

In most cases, the existence of a duty of care should be sufficiently evident and does not require statutory reinforcement. It is generally assumed that in all Commonwealth jurisdictions, a person who fails to meet an applicable standard of care, where a duty of care exists, may be held liable for resulting harm, with compensation measured by the extent of that harm. Although duties of care may, in some instances, arise in the context of activities addressed by this Model Law, it is beyond the intended scope of the statute to anticipate or codify the specific conditions under which such duties will arise.

Dispute Resolution

This Model Law does not establish procedures for resolving disputes arising from the use of electronic communications. It is assumed that implementing states possess existing judicial systems and, in many cases, alternative dispute resolution (ADR) mechanisms, such as arbitration or mediation, that parties may access in the event of a disagreement. The question of whether such mechanisms may be conducted online, and the frameworks required to support them, falls outside the scope of this Model Law. Similarly, the creation of specialised or particularly accessible forums, whether for low-value claims or for disputes involving emerging technologies, is recognised as a potentially valuable initiative but is not addressed within this instrument. Such measures are left to the discretion of each jurisdiction, based on local legal, administrative and technological capacities.

The Commonwealth

D20215