CONSULTATION PAPER ISSUED BY
THE INFOCOMM MEDIA DEVELOPMENT AUTHORITY

ON

REVIEW OF THE ELECTRONIC TRANSACTIONS ACT (ETA) (CAP. 88)

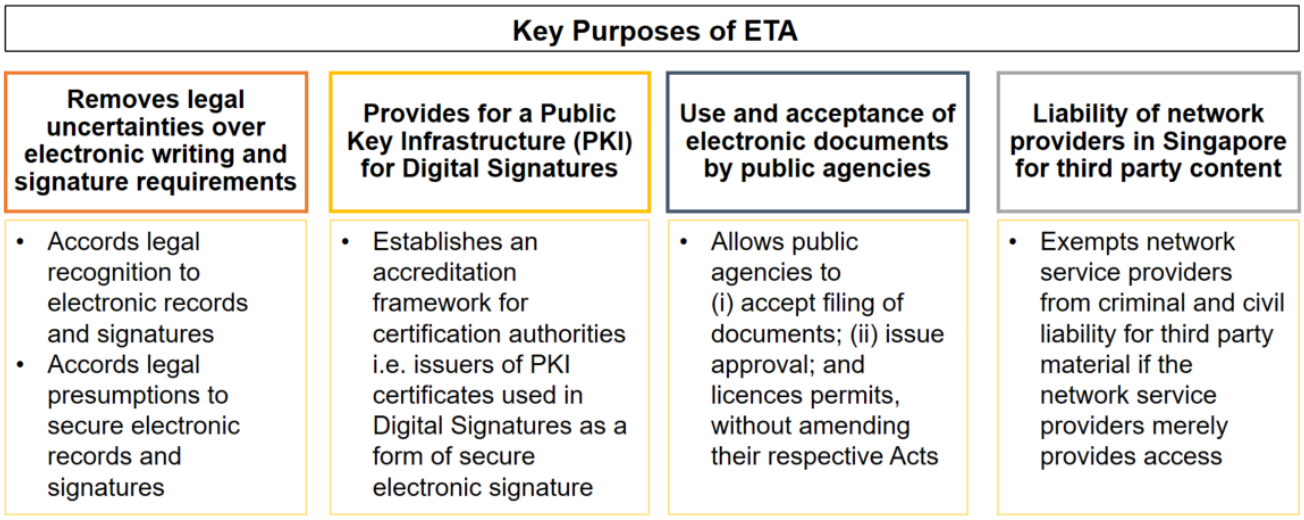
27 June 2019

CONTENTS

1. INTRODUCTION

1.1. Singapore first enacted the Electronic Transactions Act ("**ETA**") (Cap. 88) in 1998[1] and in doing so was the first country in the world to adopt the Model Law on Electronic Commerce from the United Nations Commission on International Trade Law[2] ("**UNCITRAL**"). The aim was to create a trusted environment with supportive legal foundation and business rules that provide predictability and certainty to facilitate electronic transactions in Singapore, thereby enabling more pervasive adoption of digital technologies in our economy. To this end, the ETA provides for the legal recognition and use of electronic signatures and electronic records, thereby giving predictability and certainty to electronic transactions.

1.2. The ETA gives effect to the following purposes:



1.3. The ETA is underpinned by three principles:

a. **Non-Discrimination** - An electronic document should not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form.

[1] In May 2010, the ETA was repealed and re-enacted following policy reviews conducted by then-IDA and AGC to ensure its continued relevance in an increasingly digitised environment. The ETA 2010 implemented the 2005 United Nations (UN) Convention on the Use of Electronic Communications in International Contracts (Singapore being one of the first few countries to do so), and updated the regulatory framework for certification authorities to facilitate growth in secure electronic transactions.

[2] UNCITRAL is the core body of the United Nations system in the field of international trade law, specialising in commercial law reform. It plays an important role in furthering the progressive harmonisation and modernisation of the law of international trade by preparing and promoting the use and adoption of legislative and non-legislative instruments in different areas of commercial law.

b. **Functional Equivalence** - Electronic records or communications are treated as fulfilling a traditional paper-based requirement if specified conditions are met.

c. **Technological Neutrality** - Provisions are drafted to be neutral with respect to the technology used.

1.4. The ETA also establishes a voluntary accreditation framework for Certification Authorities[3] ("**CAs**") which issue Digital Certificates[4]. The CAs verify and vouch for the identity of the subscribers and provide certificate management services to support trusted and secure transactions. CAs seeking accreditation will have to meet stringent criteria in various aspects, including financial soundness, personnel integrity and strict security controls and procedures. This framework establishes an environment of trust and predictability which enables electronic commerce to flourish.

1.5. ETA NEEDS TO REMAIN RELEVANT AND APPLICABLE FOR THE DIGITAL ECONOMY

1.5.1. For Singapore, IMDA's vision is to have a thriving Digital Economy, where every business is digitally-empowered, every worker is digitally-skilled, and every citizen is digitally-connected. Designing supportive and forward-looking policies and regulations will be essential to achieving these objectives.

1.5.2. E-commerce activities and electronic transactions have been expanding exponentially in Singapore and in the region. According to the 2018 study by Temasek Holdings and Google LLC, Singapore's Internet economy market (gross merchandise value) is expected to grow from $7B in 2015 to $22B in 2025 while the Internet economy market size for Southeast Asia could reach $240B by 2025, with a CAGR of 22% between 2015 and 2025[5].

1.5.3. The digital economy and technology landscape are rapidly changing. A recent survey by CPA Australia and PwC in 2018 found that many organisations in Singapore are developing plans to address both the challenges and opportunities arising from the impact of digital disruption. 53% of executives shared that their companies were no longer being disrupted just by competition within their fields, but also from players from other industry sectors[6]. Developments in the digital economy have an impact

[3] Certification Authorities are needed to issue Digital Certificates that certify the electronic identities of users and organisations. The CAs act like trusted electronic notaries, telling people who the valid users are and what their digital signatures should look like.
[4] Digital Certificates are used to create digital signatures.
[5] E-Conomy SEA 2018 (Temasek Holdings, Google LLC, 2018)
[6] State of Digital Report 2018 (PwC, CPA Australia, 2018)

on many parts of the economy, including government rules and regulations, how businesses choose to operate, and user preferences.

1.5.4. On the international front, the UN General Assembly passed the resolution recommending that UN member States consider adopting the UNCITRAL Model Law on Electronic Transferable Records ("**MLETR**"). The MLETR aims to facilitate greater international trade through harmonised and consistent regulatory and legal rules on the use of electronic transferable records. The adoption of the MLETR will enhance economic opportunities and productivity for companies in Singapore potentially benefitting sectors such as shipping and finance.

1.5.5. IMDA has taken a whole-of-government approach in reviewing the ETA. Government Ministries and agencies, such as Ministry of Finance, Ministry of Law, Ministry of National Development, Ministry of Social and Family Development, Council for Estate Agencies, Government Technology Agency, Housing & Development Board, JTC Corporation, Monetary Authority of Singapore, Maritime and Port Authority of Singapore, Singapore Customs, Singapore Land Authority, Smart Nation and Digital Government Office, and Urban Redevelopment Authority were involved in this review.

1.5.6. These Government Ministries and agencies provided views on the policy direction of the ETA, technology and business innovations that the ETA should facilitate, business environment changes in their respective sectors and digitalisation of public services that would need to be considered when driving changes to the ETA.

1.5.7. This Consultation Document sets out the following for discussion:

Section 2: Facilitating Innovation and Digitalisation of Businesses and Government Services

Section 3: Facilitating New Technologies in Electronic Transactions

Section 4: Certification Authority Framework

Section 5: Invitation to Comment

2. FACILITATING INNOVATION AND DIGITALISATION OF BUSINESSES AND GOVERNMENT SERVICES

2.1 The legal certainty and trust provided by the ETA has enabled businesses and citizens to innovate and adopt electronics means of transacting. To better facilitate innovation and digitalisation of businesses and government services, IMDA is reviewing the list of documents and transactions that are currently excluded from the ETA.

2.2 ENABLING MORE TRANSACTIONS TO BE COVERED UNDER THE ETA

2.2.1 Part II of the ETA contains provisions supporting the legal enforceability of electronic records and signatures. This means that electronic records and signatures are recognised as the functional equivalent of paper records and wet ink signatures. In particular, sections 7 and 8 of the ETA provide, respectively, that an electronic record or signature satisfies any rule of law requiring information to be written or be in writing, or requiring a document or record to be signed.

2.2.2 Certain kinds of documents and transactions (listed in the First Schedule to the ETA) are excluded from the scope of operation of Part II of the ETA. These excluded documents and transactions are:

a. The creation or execution of a will;
b. Negotiable instruments, documents of title, bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money;
c. The creation, performance or enforcement of an indenture, a declaration of trust or power of attorney, with the exception of implied, constructive and resulting trusts;
d. Any contract for the sale or other disposition of immovable property, or any interest in such property; and
e. The conveyance of immovable property or the transfer of any interest in immovable property.

2.2.3 The effect of section 4 of the ETA is that for such excluded documents and transactions, one cannot rely on the provisions in the ETA to satisfy the legal

requirements for writing and signature[7]. However, where legal form requirements apply, the exclusion under section 4 may not necessarily prevent such transactions from being carried out electronically. It may be possible for electronic records or signatures to satisfy the requirements for writing or signature without reliance on the provisions of the ETA, and it would be matter for legal interpretation whether an electronic form satisfies a particular legal requirement for writing or signature. To illustrate, in SM Integrated Transware Pte Ltd v. Schenker Singapore (Pte) Ltd [2005] 2 SLR(R) 651, an issue in dispute was whether an agreement for a lease (i.e. a contract for the disposition of an interest in immovable property) that was concluded through the exchange of e-mail correspondence between the parties satisfied the requirements for writing and signature under section 6(d) of the Civil Law Act (Cap. 43) ("**CLA**"). Given that a contract for the disposition of an interest in immovable property (such as the agreement for a lease in question) was listed in the First Schedule to the ETA, Part II of the ETA did not apply and hence could not be relied upon to fulfil the requirements under section 6(d) for such a contract to be "in writing" and "signed". On the facts of the case, however, the court ruled that under common law, the e-mail correspondence between the parties could fulfil the requirements for writing and signature under section 6(d) of the Civil Law Act of "in writing" and "signed", and therefore an enforceable lease agreement was formed.

2.2.4 It should be noted that the exclusion under section 4 of the ETA is not relevant where there are no legal form requirements. In such cases, there is no need to rely on the provisions in Part II of the ETA to validate electronic transactions. In most contractual situations, the law imposes no form requirements, and a contract can generally be concluded by any means intimating an offer and acceptance, electronic or otherwise. As such, parties are not prevented from conducting these matters electronically.

2.2.5 The original rationale for excluding these documents and transactions from the scope of the ETA was that e-commerce was still in its infancy and international developments in this area were still evolving. It was then thought that these classes of documents and transactions were not ready for the transition into the electronic medium. Notwithstanding changes in the common law, it was determined in the previous ETA review that public and industry opinion continue to favour retaining the exclusions. However, with the structural shifts in the information technology landscape, including the

(a) [7] In particular, sections 7 and 8 of the ETA. However, even if the provisions of the ETA are applicable, further legislative provisions may preclude the use of electronic means. For example, the Wills Act (Cap. 352) requires, amongst others, that the testator signs *at the foot of each page*; and that the will is signed by the testator *in the presence of two witnesses*.

proliferation of electronic transactions and expansion of e-commerce in Singapore and Southeast Asia[8], it is timely and opportune to reconsider the removal of these exclusions.

2.2.6 It is noted that New Brunswick, Canada, has taken a position of not excluding any of the above areas[9]. This progressive approach was chosen as the New Brunswick Electronic Transactions Act does not force the usage of electronic documents, and the New Brunswick Department of Justice felt that nothing was really to be gained from 'excluding' them from the Act. Please refer to **Annex A** for the positions taken by other jurisdictions as regards the exclusion of documents and transactions from the scope of legislation relating to electronic transactions.

2.3 PROPOSAL TO REMOVE THE EXCLUSIONS

2.3.1 In view of the rapid pace of technological change, IMDA is mindful that Singapore's legislative framework should continue to be facilitative and not hinder the development and adoption of practical and commercially viable electronic means of communications and transactions as they become more widely available. While important as a form of benchmark, international norms and other jurisdictions' preferences for the use of hardcopies in certain transactions such as the conveyance of immovable property should not, by themselves, restrict our approach to favour a wider application of the ETA. It is in Singapore's interest to ensure that its laws continue to support and facilitate electronic communications and transactions in a future where everything is increasingly digitalised, even if it means moving ahead of international norms and practices.

2.3.2 Thus, IMDA is of the view that, in general, the functional equivalence provisions in the ETA should, in principle, apply to the excluded documents and transactions, unless there are overriding public interest considerations. Where there are concerns about the consequences of such a change, various mitigating measures and safeguards could be implemented to address these concerns.

[8] See Frost and Sullivan "Southeast Asia's E-Commerce market to surpass US$25 billion by 2020 despite market challenges". See also Visa's Consumer Payment Attitudes Survey 2016 which highlights that 87% of Singaporeans prefer to make electronic payments (up 11% from 2015). Further, the survey also noted that more than 60% of all payment/transactions in Singapore are made electronically.

[9] The Electronic Transactions Act by the New Brunswick takes a different approach and does not exclude classes of transactions. Instead, New Brunswick's approach is to exclude the applications to the specific Acts – Family Income Security Act, Family Services Act, Health Services Act, Intercountry Adoption Act, New Brunswick Housing Act, Nursing Homes Act and Vocational Rehabilitation of Disabled Persons Act.

2.3.3 Removing the exclusion list in the First Schedule to the ETA may also address the existing and potential misunderstanding concerning the legal validity of electronic version of documents excluded from the application of the ETA. From discussions with stakeholders, IMDA received feedback that electronic versions of documents excluded from the application of the ETA are commonly thought to be legally invalid. This is notwithstanding that the common law has recognised that it may be possible for electronic records and signatures to satisfy "in writing" and "signed" formalities requirements, even where the electronic version of the document is excluded from the application of the ETA[10].

2.3.4 It is therefore proposed, in view of the ETA's objectives and wider Government's Digital Economy goals, that most matters from the exclusion list under the First Schedule to the ETA be removed, unless there are overriding public interest considerations e.g. if it is required as a safeguard to protect the vulnerable.

2.3.5 To provide the relevant policy and implementing agencies with time to address any policy/implementation challenges or concerns, it is further proposed that a sun-rise period until 2021 be introduced (where required). The target would meet the objective where most transactions with the Government could be conducted digitally by 2023.

***Question 1**: IMDA welcomes general views and comments on IMDA's overall approach to minimise subject matter under the current exclusion list.*

***Question 2**: IMDA welcomes views on the necessity and adequacy of the sunrise period until 2021 to address any policy/implementation challenges with the use of electronic versions of the transactions/documents currently excluded from the application of the ETA.*

2.3.6 The paragraphs below highlight the status of the existing exclusions under section 4 of the ETA and the policy and business considerations for their removal. The sections also discuss possible implementation issues and proposed options forward.

2.4 WILLS

2.4.1 Wills are currently excluded from the application of Part II of the ETA. Wills have been and continue to be universally excluded from similar electronic transactions legislation in other jurisdictions such as New Zealand and

[10] See Para. 2.2.3.

Australia. Wills are also excluded under the Australian Commonwealth Model Law on Electronic Transactions and the Canadian Uniform Electronic Commerce Act. In the United States, there is currently a draft Uniform Electronic Wills Act that deals with the formation, validity and recognition of electronic wills that is being discussed by the Uniform Law Commission. To date, only the American states of Indiana and Nevada[11] have legislatively provided for the creation of electronic wills. This could affect the cross-jurisdictional enforcement of electronic wills.

2.4.2 Even as technology has become more advanced and sophisticated, it remains difficult to replicate the traditional formalities safeguarding the creation and execution of wills electronically. Even if the ETA is amended to apply to wills (i.e., by removing wills from the exclusion list), it does not mean that electronic wills automatically become valid. The Wills Act, as it currently stands, requires a will to be made in writing and to be signed at the end by the testator in the presence of two or more witnesses who shall subscribe the will in the testator's presence. Any dispensation of or modification to the formalities for the execution of wills has to be achieved by way of amendment to the Wills Act.

2.4.3 IMDA recognises that further intervention and innovation is likely required before electronic wills are recognised. In particular, the success of an electronic wills system will likely depend on a number of elements, among which are the:

a. Verification and authentication processes (including ascertaining the latest version of the will, in the event that the earlier will is amended or revoked); and
b. processes for managing and maintaining electronic wills to prevent obsolescence.

Nevertheless, as the validity of a will ultimately depends on the requirements set out in the Wills Act and not the ETA, IMDA takes the view that the ETA should be amended so that the ETA will not in itself be a barrier to the adoption or recognition of electronic wills, should such adoption and recognition take place.

[11] See Indiana House Bill 1303 and Nevada Revised Statutes (NRS) §133.085 (2001); See also Arizona House Bill 2656 enabling the electronic execution of a will (as well as trusts and powers of attorney) which comes into force 1 Jul 2019. In 2017, Florida's legislature passed the Florida Electronic Wills Bill, which would have allowed a will to exist as an electronic record, testators to sign electronically (although still in the presence of two witnesses), and for witnesses to see the testator sign by video and then sign electronically. However, the Bill was vetoed by Florida's governor on 26 June 2017, who cited concerns about fraud and exploitation.

***Question 3**: IMDA welcomes views and comments on IMDA's proposal to remove wills from the exclusion list under the First Schedule to the ETA, on the basis that the safeguards in the Wills Act will be maintained.*

***Question 4**: IMDA welcomes views and comments on the potential challenges/concerns with the use of electronic wills (such as technological obsolescence) and how they may be addressed with existing technology.*

2.5 NEGOTIABLE INSTRUMENTS, DOCUMENTS OF TITLE, BILLS OF LADING AND OTHER TRANSFERABLE DOCUMENTS OR INSTRUMENTS

2.5.1 The ETA does not presently enable the use of electronic equivalents of transferable documents or instruments (referred to as "electronic transferable records" or "ETRs") such as bills of lading, warehouse receipts, dock warrants, and negotiable instruments such as bills of exchange, promissory notes or cheques.

2.5.2 With rapid technological changes, evolving consumer usage patterns and the adoption of the MLETR by UN General Assembly in December 2017, it is appropriate to consider amending the ETA to provide full legal recognition to electronic transferable records. Industry and businesses will then be able to enjoy the advantages offered by an ETR, i.e., faster speeds of transmission and higher security (which will minimise fraud through the use of trusted systems) as compared to the paper equivalent, and reap the opportunities related to the processing of data.

2.5.3 The IMDA and AGC had previously conducted public consultation on the MLETR on 10 March 2017 with the issuance of the paper titled "Joint IMDA-AGC Review of the Electronic Transactions Act (Cap. 88) – Review of Draft UNCITRAL Model Law on Electronic Transferable Records (Public Consultation Paper)". The consultation closed on 10 April 2017 and IMDA and AGC have reviewed the responses received. To recap, the central issue in the use of ETRs is the need to guarantee the singularity or uniqueness of the electronic record constituting the ETR such that only one set of obligations is owed by the person who is obliged to perform. A valid holder of such a transferable document has a right to demand the performance of such obligations. One of the key legal challenges is thus to define the electronic functional equivalent of the requirement for possession of a unique or singular transferable document or instrument. Further details are set out in **Annex B**.

2.5.4 While industry players and members of the public can provide inputs on the text that was adopted by UNCITRAL, separate industry engagement will be conducted to seek views on the adoption of the MLETR into Singapore law once IMDA and AGC have completed the review.

***Question 5**: IMDA welcomes views and comments on IMDA's proposal to remove documents such as bills of lading, warehouse receipts, dock warrants or negotiable instruments such as bills of exchange, promissory notes or cheques from the exclusion list under the First Schedule to the ETA.*

***Question 6**: IMDA welcomes views and comments on IMDA's proposal to adopt the MLETR into Singapore law.*

2.6 POWERS OF ATTORNEY, INDENTURES AND TRUSTS

2.6.1 Powers of attorney ("**POAs**") are currently excluded from the application of Part II of the ETA[12]. POAs have been excluded to varying degrees in the electronic transactions legislation of other jurisdictions. New Zealand (like Singapore) has a complete exclusion[13], whereas some other jurisdictions restrict their exclusions to particular kinds of POAs. For example, Ireland only excludes enduring powers of attorney[14].

2.6.2 In practice, POAs are often used for land transactions. As land transactions are usually significant transactions of high value, there is a strong emphasis on the need for verification and authentication in the creation and enforcement of a POA. This need for verification and authentication of the identities of the parties could be addressed by the use of existing technologies such as digital signatures (through PKI) and distributed ledger technology ("**DLT**"). However, IMDA notes that there could be potential concerns of abuse as family members or close relations may have access to user accounts, passwords and authentication devices of the vulnerable, thereby allowing them to fraudulently execute POAs in place of the vulnerable.

2.6.3 Another type of POA is one that is made for the purpose of the enforcement security interests. However, given that this type of POA is usually executed

[12] At this juncture, IMDA would like to share that not all POAs have to executed by way of deed. At common law, it is not necessary for an instrument granting a POA to be a deed, although authority to execute a deed or to deliver a deed on behalf of another has to be made by way of deed. See Singapore Academy of Law ("**SAL**") Law Reform Committee, Report of the Law Reform Committee on Powers of Attorney (September 2009) at [34].
[13] See New Zealand Electronic Transactions Act 2000.
[14] See Irish Electronic Commerce Act 2000.

in the context of commercial transactions between sophisticated parties, the advantages of enabling this type of POA by removing it from the exclusion list greatly outweigh the disadvantages.

2.6.4 Apart from POAs for the enforcement of security interests and Lasting Power of Attorney, IMDA proposes that all other types of POAs ("True Agency POAs") will remain excluded from the application of Part II of the ETA, given the potential for abuse.

***Question 7**: IMDA welcomes views and comments on how the potential concerns and challenges (such as verification/authentication and technological obsolescence) with the use of electronic POAs can be addressed with existing technologies.*

***Question 8**: IMDA welcomes views and comments on the proposal to remove POAs for the purposes of enforcement of security interests from the exclusion list under the First Schedule to the ETA.*

LASTING POWERS OF ATTORNEY

2.6.5 Similarly, Lasting Powers of Attorney ("**LPAs**") are currently excluded from the application of Part II of the ETA. LPAs are legal instruments which set out the decision-making powers conferred by donors on their appointed donees[15] and which come into effect upon the loss of mental capacity of donors. Under general law, POAs would cease to have legal effect upon the mental incapacity of their donors. However, in many jurisdictions, legislation has been promulgated to make it possible for persons to create LPAs in contemplation of their becoming mentally incapacitated. LPAs in Singapore are governed by the Mental Capacity Act (Cap. 177A)[16].

2.6.6 Currently, LPAs can only be created using hardcopy forms and applications for registration are processed manually. It would not be sustainable to continuously increase manpower to ensure applications are processed timely and within a reasonable timeframe – in the first eight months of 2018, over 16,000 people applied for an LPA. With the increased application numbers and the need to process physical copies of LPAs as quickly as possible, the chances of errors being overlooked due to fatigue could likely increase as well. In this regard, a more effective way of processing applications for LPA registration (and managing subsequent LPA-related

[15] Under the Mental Capacity Act, a donor appoints one or more persons (donee(s)) to make decisions and act on their behalf if and when they lack mental capacity in the future.
[16] See Part IV.

events) and addressing the constraints currently faced with a manual form and its manual processes could be through the use of electronic LPAs.

2.6.7 A further advantage of LPA electronic creation and registration being made and maintained online (without a need for a hardcopy original), is that they can also be easily updated and made available to third parties (through proper access controls) for review and verification. This would help ensure that the online copy will also be the latest and most updated version. In October 2018, it was also published that the Ministry of Social and Family Development ("**MSF**") is planning to develop an online system for LPA creation and registration. The online system will, through data linkages with other agencies, allow for personal data to be auto populated in the electronic LPA form, thus reducing errors.

2.6.8 In addition, the deployment of technology refresh/change management (e.g. conversion of records to new format) and the use of technology solutions such as PKI and DLT could potentially address concerns about technological obsolescence and reliability for LPAs, given the need for the long term storage of documents.

2.6.9 Electronic LPAs will not automatically become valid due to proposed amendments to the ETA. Validity would depend on satisfying the requirements set out in the Mental Capacity Act. Moreover, accepting the creation of an electronic LPA does not render it without safeguards. There already exists an important safeguard in the need for an independent person (e.g., the Certificate Issuer ("**CI**"), defined as a practicing lawyer, accredited doctor or psychiatrist) to confirm amongst other things that the donor understands the purpose and scope of the LPA and is not under any undue pressure or duress. This safeguard will remain in the online system for electronic LPA creation.

***Question 9**: IMDA welcomes views and comments on IMDA's proposal to remove Lasting Powers of Attorney from the exclusion list under the First Schedule to the ETA, on the basis that safeguards in the Mental Capacity Act will be maintained.*

INDENTURES AND TRUSTS

2.6.10 An indenture is a type of deed, which is made between two or more parties. The formality requirements for deeds would therefore also apply to indentures. In Singapore, these are governed by the common law, which

requires deeds to be signed, sealed and delivered to be effective[17]. In practice, deeds are also almost always attested, although this is not a legal requirement.

2.6.11 If indentures were removed from the exclusion list, this would facilitate the recognition of electronic indentures which is currently governed only by the common law. The current ETA amendments do not seek to amend or supplant these specific common law requirements for indentures or deeds (i.e., sealing and delivery[18]). Given that indentures usually feature in the context of commercial transaction between sophisticated parties, there could be greater benefits from removing indentures from the exclusion list.

2.6.12 Part II of the ETA also does not apply to declarations of trust, except for implied, constructive and resulting trusts. For a trust to be recognised and enforceable in law, there are no formality requirements; rather, the common law requires that there be certainty of intention, certainty of subject matter and certainty of object. However, there are 3 specific categories of express trusts which currently have additional formality requirements. These are:

a. Testamentary trusts, which must adhere to the same formality requirements as wills, under the Wills Act[19];
b. Trusts in respect of immovable property (i.e., land) or interests in immovable property, which must be in writing and signed by the person making the declaration of trust if the person is declaring himself as trustee. In addition, if the trust declares that a third party is to serve as trustee, the legal title to the immovable property must be transferred to the trustee in the appropriate manner i.e. by deed in the English language for unregistered land, and by way of registered transfer under the Land Titles Act for registered land; and
c. Trusts effecting a disposition of equitable interest, which must be in writing and signed by the person making the disposition[20].

[17] Whilst the mere act of signing next to the words "signed, sealed and delivered", without more, may not meet the formality requirements for a deed. IMDA notes that the act of sealing may be satisfied where the document which is expressed to be a deed contains a circle with the letters "L.S." imprinted (see First National Securities v Jones [1978] Ch 109, cited in United Overseas Bank Ltd v Lea Tool and others [1998] 1 SLR(R) 373). This may be wide enough to recognise certain acts performed on an electronic medium as amounting to sealing, but this is yet to be tested in Singapore's Courts.
[18] At common law, a deed is delivered when a party expresses his intention to be bound by the deed. It does not require physical delivery of the deed.
[19] "Wills" is defined in the Wills Act as including "a testament and an appointment by will or by writing in the nature of a will in exercise of a power and also a disposition by will and testament and any other testamentary disposition".
[20] Section 7(2) of the Civil Law Act.

2.6.13 For testamentary trusts, similar to IMDA's position on wills, IMDA is of the preliminary view that testamentary trusts can be removed from the exclusion list as the safeguards in the Wills Act continue to apply.

2.6.14 For declarations of trust relating to immovable property, and dispositions of equitable interest via a trust, it is observed that these two types of transactions are commonly used in a familial context. Family members or close relations may have access to user accounts, passwords and authentication devices of the vulnerable, thereby allowing them to fraudulently execute such transactions in place of the vulnerable. Given concerns of potential abuse, it is recommended that declarations of trust relating to immovable property, and dispositions of equitable interest should not be removed from the exclusion list.

***Question 10**: IMDA welcomes views and comments on IMDA's proposal to remove indentures from the exclusion list under the First Schedule to the ETA.*

***Question 11**: IMDA welcomes views and comments on IMDA's proposal to remove testamentary trusts from the exclusion list under the First Schedule to the ETA on the basis that safeguards in the Wills Act will be maintained.*

***Question 12**: IMDA welcomes views and comments on IMDA's proposal to not remove declarations of trust relating to immovable property, and dispositions of equitable interest.*

2.7 CONTRACTS FOR THE SALE OR OTHER DISPOSITION OF IMMOVABLE PROPERTY

2.7.1 Section 6 of the CLA prevents contracts for the sale or other disposition of immovable property, or any interest in such property, from being enforced unless they are evidenced in writing and signed. The rationale for this requirement is the prevention of fraud[21].

2.7.2 Any contract for the sale or disposition of immovable property (i.e., land or real estate) is currently excluded from the application of Part II of the ETA. The electronic equivalents of such contracts therefore do not enjoy the certainty provided by the ETA.

2.7.3 The current exclusion of contracts for the sale and disposition of immovable property from the application of Part II of the ETA is attributable to the high value and significance of such transactions (especially to individuals),

[21] The predecessor to these requirements in the CLA is called the statute of fraud.

balanced against the risk of fraud arising from the challenge of verifying the identities and intentions of vendors and purchasers for electronic transactions. IMDA is mindful of the need to protect vulnerable parties, who may inadvertently enter into electronic transactions for their property e.g. through simple click-wrap contracts.

2.7.4 In light of the changing nature of how land transactions are carried out today, with more transactions taking place over electronic communications, the law should be updated to reflect how these transactions are conducted in reality. In some cases, the entire transaction can take place online, with only the final documents produced on paper and signed in wet ink. In practice, although electronic contracts for such instruments have been recognised[22], hardcopy versions of documents continue to be executed for the sale of property, and a buyer would typically deliver a hardcopy option to purchase together with a cashier's order or cheque for the option fee.

2.7.5 IMDA proposes that a solution to mitigate the risk of fraud and to protect the vulnerable is to require the use of secure electronic signatures. A secure electronic signature is unique to the person using it and capable of identifying such person. It serves as evidence of authentication of a document by binding individuals to that document. The additional legal requirements before an electronic signature can qualify as a secure electronic signature would provide additional assurance and protection.

2.7.6 The Singapore Government recognises the impact of digitalisation and a workgroup chaired by the Council for Estate Agencies ("**CEA**") was formed to move Singapore towards seamless, efficient and secure residential property transactions. The workgroup - named Digitalised Property Transactions Workgroup ("**DPTWG**") - involves key government agencies as well as consumer and industry associations with touchpoints in the property transaction process[23]. With digitalisation, we can minimise the use of

[22] The courts have clarified that the law does not require handwritten signatures for the purposes of satisfying the signature requirement of section 6 of the CLA: see *SM Integrated Transware Pte Ltd v. Schenker Singapore (Pte) Ltd* [2005] 2 SLR 651 and *Joseph Mathew v Singh Chiranjeev* [2010] 1 SLR 338 (Court of Appeal). In other words, there is no real distinction between a printed document with a handwritten signature, and a softcopy document that has been sent via e-mail to the recipient with the inscription of the sender's name next to his e-mail address at the top of the e-mail. IMDA notes that the court in *SM Integrated Transware Pte Ltd v. Schenker Singapore (Pte) Ltd* [2005] 2 SLR 651 at [92] opined that: "This conclusion which I think is dictated by both justice and common sense since so much business is now negotiated by electronic means rather than by letters written on paper and, in the future, the proportion of business conducted electronically will only increase.".

[23] Government agencies include CEA, HDB, URA, SLA, CPFB, IRAS, MAS, MinLaw and GovTech. The workgroup also includes industry representatives across the real estate value chain – the Association of Banks in Singapore, Consumers Association of Singapore, Institute of Estate Agents Singapore, PropTech Association Singapore, Real Estate Developers' Association of Singapore, Singapore Estate

hardcopy documents and physical payments such as cheques and cashier's orders, all of which are time-consuming to process. For citizens and consumers, this means less time spent on paperwork and queueing up at the bank. For businesses - lawyers, property agents, and bankers - this means fewer administrative burdens to process, thus allowing them to focus on productive and higher value-added tasks.

2.7.7 A benefit of removing the exclusion for land transactions is that landowners such as corporations or statutory boards, and buyers or tenants of their property, would enjoy the ease and convenience of being able to carry out certain land transactions electronically. An obvious example would be the high volume of repetitive standard term transactions carried out by property developers or statutory boards. In 2017, there were about 250,000 residential property sale and lease transactions. Based on the findings under DPTWG's consultancy study, around 70% of residential property transactions documents are still transacted via hardcopy and 77% of payments are still via cheque or cashier's order. In addition, the possibility of effecting the renewal of commercial leases digitally may be useful to institutional owners and their tenants. In this case, the danger of the parties being duped into an unintended transaction is minimal since both parties are already familiar with the property in question and the value of the lease.

2.7.8 In IMDA's view, applying Part II of the ETA to contracts for the sale or disposition of immovable property (or any interest in such property) and trusts over interests in immovable property may not materially impact the existing legal position since the common law already recognises, in certain cases, electronic writing and signatures as satisfying the formality requirements of "in writing" and "signed".[24]

2.7.9 IMDA also proposes a requirement that only secure electronic signatures or digital signatures be accepted for property transactions conducted electronically to ensure greater certainty, mitigate concerns of fraud and safeguard the vulnerable.

***Question 13**: IMDA welcomes views and comments on how the potential challenges (such as verification/authentication and technological obsolescence) with the use of electronic contracts for the sale or disposition of immovable property can be addressed with existing technologies.*

Agents Association, Singapore FinTech Association, SGTech, Singapore Institute of Surveyors and Valuers, and the Law Society of Singapore.

[24] See para 2.2.3.

Question 14: *IMDA welcomes views and comments on IMDA's proposal to remove contracts for the sale or disposition of immovable property from the exclusion list under the First Schedule to the ETA.*

Question 15*: IMDA welcomes views and comments on the proposed requirement that only secure electronic signatures or digital signatures will be accepted for property transactions conducted electronically to ensure greater certainty, mitigate concerns of fraud and safeguard the vulnerable.*

Question 16*: IMDA welcomes views and comments on whether Singapore should amend its legislation to facilitate the use of electronic contracts for the sale or disposition of immovable property.*

2.8 CONVEYANCE OF IMMOVABLE PROPERTY AND/OR TRANSFERS OF INTEREST IN AN IMMOVABLE PROPERTY

2.8.1 Currently, Part II of the ETA does not apply to the conveyance of immovable property and transfers of interest in immovable property.

2.8.2 Singapore had in 2003 implemented an Electronic Lodgement System ("**STARS ELS**") which enabled documents to be lodged online with the Registrar of Titles. This complements the existing Singapore Titles Automated Registration System ("**STARS**") which was implemented in 1995.

2.8.3 The STARS ELS allowed for the following:

a. Electronic filing of caveats and other documents which did not involve passing of interests in land and where production of the Certificate of Title is not required;
b. Electronic priority lodgement system for documents such as mortgages and transfers which require the signature of the land owner;
c. Electronic preparation of documents;
d. Automated billing system (for registration fees); and
e. Automated imaging and work assignment system.

2.8.4 This played an important role in safeguarding the integrity of the land register given that the registration of documents will be based on information entered at source without the need to re-enter the data, i.e., removed one layer of possible human error and ensuring greater accuracy. Other benefits include the automated notification of successful registration of documents and facilities to request for financial reports on outstanding bills.

2.8.5 The above notwithstanding, not all property-related documents are covered under the STARS ELS. For example, the STARS ELS does not extend to e-marketing of properties, online execution of options to purchase, sale and purchase agreements and other relevant deeds. It also does not cater for electronic exchange of funds (which would obviate the need for cashier's orders for legal completion).

2.8.6 Since the implementation of the STARS ELS, the Singapore Government has been working towards a fully electronic land registration system in order to bring both private and public land transactions under a single electronic land title registration system. Earlier attitudes and international practices towards electronic transactions that prevented the legal recognition of e-conveyances of immovable property have become more permissive.

2.8.7 Given the above, it is noted in the implementation of e-conveyancing in these jurisdictions, that some of the earlier concerns regarding a fully electronic land registration system (such as the technical difficulty of combining paper and electronic documents in a single transaction or chain of transactions or the need to provide proper assurance of an agent's authorisation where the agent signed a document electronically on behalf of the principal) might no longer be as relevant today given the advances in authentication and fraud-protection technologies.

2.8.8 It is therefore proposed that the class of documents and transactions relating to the conveyance of immovable property or the transfer of any interest in immovable property be removed from the exclusion list under the First Schedule to the ETA such that electronic conveyancing of immovable property would not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record. At the same time, it is recognised that amendments to other relevant statutes may be required, e.g., the CLPA and Land Titles Act (Cap. 157), to ensure that the necessary provisions and safeguards are put in place to support electronic submissions and the conveyancing process.

Question 17: *IMDA welcomes views and comments on IMDA's proposal to remove the conveyance of immovable property or the transfer of any interest in immovable property from the exclusion list under the First Schedule to the ETA.*

2.8.9 In summary, with the proposed changes, IMDA would remove all the exclusions under the First Schedule of the ETA for most business related transactions, while retaining personal or familial transactions which could require greater safeguards. This would mean the removal of all items in the

exclusion list[25] with the exception of trusts relating to immovable property or dispositions of equitable interest and "True Agency" POAs. IMDA will also propose to insert a requirement for the use of secure electronic signatures for contracts for the sale or disposition of immovable property.

3. FACILITATING NEW TECHNOLOGIES IN ELECTRONIC TRANSACTIONS

3.1. As new technologies emerge and existing technologies mature, there is potential for businesses and consumers to interact and transact with one another, and with government agencies, in more seamless and trusted ways. Given rapid technological advancements and recognising that uncertainty has the potential to hinder technology adoption, it is important to emphasise that the ETA is technology neutral and focuses on functional equivalence. The following paragraphs seeks to illustrate how the ETA and these principles apply to specific technologies increasingly used in connection with electronic transactions such as distributed ledger technology, smart contracts and biometrics.

3.2. DISTRIBUTED LEDGER TECHNOLOGY ("**DLT**")

3.2.1. DLT has been generally described as a digital system in which transactions and their details are recorded in multiple places at the same time without a central database or administrator. In a DLT system, all participants within the network store an identical copy of the ledger (instead of keeping data centralised as in a traditional ledger) and coordinate using the software protocol that precisely dictates how the participants store information and engage in transactions. Any change to the ledger is recorded, validated and replicated across the decentralised network of nodes. Given the widely replicated nature of the ledger, any data stored in it is highly resilient and can survive even if a copy of the ledger is corrupted or if a node on the network fails.

3.2.2. Blockchain is a particular type of DLT designed to solve trust in digital asset transactions. At a generalised level, blockchains store and transmit data in encrypted packages called "blocks" that are connected to each other in a digital "chain". Each new block is validated and added to the "chain" when the network reaches a consensus through a mechanism (i.e., a software protocol) which governs how data can be added to the ledger in an orderly manner. This process removes the need to rely on any centralised operator or middleman[26].

[25] Wills, Negotiable Instruments, Indentures, Trusts and POAs, Contracts and Conveyance for Immovable Property

[26] This consensus mechanism used for the network may be Proof-of-Work, Proof-of-Stake or a variety of other consensus mechanisms.

3.2.3. Businesses have generally deployed DLT such as blockchain technology for three objectives: (i) the processing and coordination of data, (ii) to ensure trusted and immutable records, and (iii) the digitisation of assets. DLT is also being explored to facilitate digital identity products (such as national ID, birth, marriage and death records) or build tamper-proof, decentralised records of the flow of commodities and materials across a supply chain by using trusted stakeholders to validate flows and movements. It is also recognised that there are different ways to deploy DLT in order to bring different values to the stakeholders (e.g. Hyperledger Fabric, R3 Corda and Ethereum).

3.2.4. The World Bank Report[27] shared that DLT is still evolving and may pose new risks and challenges, many of which are yet to be resolved. The most commonly cited technological, legal and regulatory challenges related to DLT concern scalability, interoperability, operational security and cybersecurity, identity verification, data privacy, transaction disputes and recourse frameworks, and challenges in developing a legal and regulatory framework for DLT implementation, which can bring fundamental changes to the roles and responsibilities of the stakeholders in various sectors.

3.2.5. The ETA is drafted in a technology neutral manner and focuses on functional equivalence. IMDA takes the view that the ETA does not prevent the adoption of DLT by the industry and stakeholders. Section 6 of the ETA states that: “For the avoidance of doubt, it is declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.”.

3.2.6. Where data on the DLT such as blockchain exists as an electronic record, such data can be recognised under the ETA. In summary, IMDA is of the preliminary view that DLT is not inconsistent with ETA concepts such as “electronic record”, “in writing”, “electronic signature”, “secure electronic record” and “secure electronic signature”. IMDA has set out its views on the application of ETA concepts, namely “electronic signature”, “secure electronic record” and “secure electronic signature” in the context of blockchain below while application of concepts like “electronic record” and “in writing” are set out in **Annex C**.

3.2.7. **“Electronic Signature”**

3.2.7.1. Although the term “electronic signature” is not expressly defined in the ETA, the terms “signed” or “signature” and its grammatical variations are defined in section 2(1) of the ETA to mean “a method (electronic or otherwise) used to identify a person and to indicate the intention of that person in respect of the information contained in a record”.

3.2.7.2. An electronic signature essentially is an acknowledgement provided in an electronic format that a business can use to demonstrate the intention of a party (e.g., acceptance) and that can electronically be used to authenticate

[27] Distributed Ledger Technology (“DLT”) and Blockchain (World Bank Group, 2017)

the party involved[28]. In determining whether something amounts to a signature, IMDA understands that the court will generally look at whether the method of signature used fulfils the authenticating function of a signature, rather than whether the form of signature used is one which is commonly recognised[29].

3.2.7.3. In a blockchain scenario, data will be cryptographically hashed before it is written into and stored in the blockchain as an electronic record. Where the implementation of blockchain provides that the hashing is unique or traceable to a person or account, IMDA is of the view that it may be possible for the cryptographic hash to be considered as an electronic signature, or at least form a possible component of an electronic signature. While there may be other possibilities, it will depend on the specific technical implementation.

3.2.8. **"Secure Electronic Record"**

3.2.8.1. The term *"secure electronic record"* is defined in section 2(1) of the ETA to mean *"an electronic record that is treated as a secure electronic record by virtue of section 17(1) or any other provision of this Act".*

3.2.8.2. Section 17(1) of the ETA in turn states that:

"[if] a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic record to verify that the electronic record has not been altered since a specific point in time, such record shall be treated as a secure electronic record from such specific point in time to the time of verification."

3.2.8.3. In order to make an electronic record "secure", parties must either apply a specific security procedure or an agreed form of security procedure that is commercially reasonable.

3.2.8.4. Given the above, where an electronic record on a blockchain is signed in a secure manner, e.g. using digital signatures as defined in the Third Schedule to the ETA (see further paragraphs 3.2.9.1. – 3.2.9.2. below), IMDA takes the view that such an electronic record may qualify as a secure electronic record. Alternatively, a record on the blockchain may be treated as a "secure electronic record" if a commercially reasonable security procedure, which has been agreed to by the parties, has been properly applied to the record to verify that such record has not been altered since a specific point in time.

[28] Some examples of electronic signatures include: (i) a person typing their name into a contract or email concerning the terms of the contract; (ii) a person electronically pasting their signature (e.g. in the form of an image) into an electronic version (e.g. soft copy) of the contract (e.g. next to the relevant party's signature block); (iii) a person accessing a contract through a web-based signature platform and clicking to have their name inserted into the contract in the appropriate place; and (iv) a person using a finger, light pen or touchscreen to write their name in the appropriate place in a contract, etc.

[29] In the case of SM Integrated Transware Pte Ltd v. Schenker Singapore (Pte) Ltd [2005] 2 SLR 651, the Singapore High Court held that the typed names of the signatories in the emails sent out were sufficient to be regarded as signatures since the authenticating intention of the signatories had been clearly demonstrated.

3.2.9. **"Secure Electronic Signature"**

3.2.9.1. The term *"secure electronic signature"* is defined in section 2(1) of the ETA to mean *"an electronic signature that is treated as a secure electronic signature by virtue of section 18 or any provision of this Act"*. An electronic signature can be made "secure" through the application of a specified security procedure or a commercially reasonable security procedure agreed to by the parties involved, in accordance with section 18 of the ETA.

3.2.9.2. To make an electronic signature "secure", parties must either apply a specific security procedure, e.g. a digital signature as defined in the Third Schedule to the ETA, or an agreed form of security procedure. The procedure must be able to verify that an electronic signature was, at the time that it was made: (a) unique to the person using it; (b) capable of identifying such a person; (c) created in a manner or using a means under the sole control of the person using it; and (d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated.

3.2.10. **"Digital Signature"**

3.2.10.1. The term "*Digital Signature*" broadly refers to PKI based electronic signatures. It is specifically defined in paragraph 1 of the Third Schedule to the ETA as "*an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine – (a) whether the transformation was created using the private key that corresponds to the signer's public key and; (b) whether the initial electronic record has been altered since the transformation was made.*".

3.2.10.2. As a type of electronic signature, a digital signature is similarly indicative of a person's identity and intent, and serves as evidence of authentication of a document by binding individuals to that document. A digital signature however goes further by adding a layer of security via the use of an asymmetric cryptosystem and hash function.

3.2.10.3. In the context of blockchain, whether the "signature" applied will be considered a secure electronic signature will likely depend on the robustness of the cryptographic procedure applied as well as other factors such as the nature of the transaction, the sophistication of the parties, etc[30]. Where the cryptographic procedure is PKI-based, IMDA is of the view that there is a high likelihood that such procedure can constitute a secure electronic signature, considering that PKI solutions certified under the ETA are considered "digital signatures". There will, however, need to be agreement

[30] See further section 17(2) of the ETA.

(e.g. via the terms and conditions of the platform) between the transacting parties as regard such security procedure used[31].

3.2.10.4. IMDA notes that permissionless blockchains (please refer to **Annex D** for different types of distributed ledgers) are generally characterised by their pseudonymity, meaning to say that it is possible for a person to store information or engage in transactions without revealing one's true identity. For such blockchains, there is no requirement to have authentication of users to confirm their identity. In such instances, the concept of secure electronic signatures may be inapplicable as any digital signature created by such users would not be capable of identifying the person who created such signatures[32].

3.3. SMART CONTRACTS

3.3.1. While there is no universally accepted definition for smart contracts, a typical definition of a smart contract is as follows:

"an automatable and enforceable agreement; automatable by computer, although some parts may require human input and control, and enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code"[33].

3.3.2. There are generally two types of smart contracts:

a. **Automated contracting:** This is where the term 'smart contract' is used to refer to legal contracts, or elements of legal contracts, automatically entered into by software; and
b. **Automated execution/implementation of obligations:** This is where the term 'smart contract' is used to refer to code that is designed to execute certain tasks if pre-defined conditions are met. Such tasks are often embedded within, and performed on, a distributed ledger.

3.3.3. Smart contracts can be described as lying on a spectrum with smart contracts entirely written in code on one end, and smart contracts written in natural language with encoded payment mechanism on the other. Along this spectrum, there are smart contracts that are written in code with duplicated natural language versions, as well as smart contracts that are both human and machine readable with encoded performance of non-human (these are Ricardian contracts[34] with automated execution).

3.3.4. In relation to automated contract formation, IMDA notes that in addition to contracts concluded via electronic communications, the ETA allows for the

[31] See further section 3(b)(iv) of the Third Schedule to the ETA.
[32] Section 18(1)(b) of the ETA.
[33] Smart Contract Templates: foundations, design landscape and research directions (Clack, Bakshi and Braine, 2017)
[34] According to the creator, Ian Griggs, a Ricardian contract is "a digital contract that defines the terms and conditions of an interaction, between two or more peers, that is cryptographically signed and verified. Importantly, it is both human and machine readable."

use of automated message systems in the formation of a contract. An *"automated message system"* is defined in section 2(1) of the ETA as:

"a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the program or electronic or other means".

3.3.5. In particular, section 15 of the ETA provides that such contracts formed via automated message systems shall not be denied validity or enforceability. IMDA further notes that this position concerning automated message systems has been affirmed by the Singapore courts[35]. For example, in the copyright industry, a smart contract could automatically be entered into between parties based on pre-defined price and content parameters. This would then allow for royalty payments to be automatically and transparently delivered based on stakeholder information contained in the smart contract. The contract formed is unlikely to be denied validity or enforceability by sole virtue of its automatic formation. In summary, IMDA is of the preliminary view that the ETA does not prevent the use and formation of smart contracts by organisations.

3.4. BIOMETRICS

3.4.1. Biometrics are biological measurements, commonly physical characteristics, that can be used to identify individuals, e.g. fingerprint-mapping, facial recognition, retina scans. Given that physical characteristics are relatively fixed and individualised, and do not easily change over time, biometric authentication is increasingly being used to replace or at least augment password systems to access sensitive documents, etc.

3.4.2. Biometric technology used to identify or authenticate a person has progressed beyond fingerprint recognition to other biometric modalities such as facial recognition, voice recognition, ocular-based biometrics (iris recognition and retinal scans), vein matching, etc. Biometrics identification is typically a combination of different types of recognition.

3.4.3. It is noted that biometrics technology is deployed for e-ID projects of jurisdictions such as Israel[36] and Estonia[37]. However, the primary technology for e-transactions such as in the case of Estonia's e-ID remains that of PKI[38].

3.4.4. IMDA is of the view that use of biometrics technology, by itself, does not typically allow for non-repudiation and also does not allow for the detection of error or alteration in the communication, content of storage of an electronic

[35] *Chwee Kin Keong and others v. Digilandmall.com Pte Ltd* [2004] SGHC 71.
[36] See Biometric Identification Methods and Biometric Identification Data in Identification Documents and Database (2009).
[37] See Identity Documents Act (2009).
[38] See Digital Signatures Act (2000) and Estonia's Mobile ID (https://www.ria.ee/en/mobile-id-service-launched.html).

record since a specific point in time. Hence, biometrics alone is unlikely to be understood as a secure electronic procedure as defined under the ETA.

3.4.5. IMDA however notes that the ETA, being technology neutral, permits biometrics to be deployed as a supporting technology for authentication purposes (e.g. especially when paired with another factor for authentication of a subscriber of a digital certificate in a PKI).

3.4.6. In summary, IMDA is of the preliminary view that no further amendments to the ETA are necessary to facilitate the usage of biometric technology in electronic transactions.

Question 19*: IMDA welcomes views and comments on IMDA's views that the ETA does not prohibit the use of DLT, smart contracts and biometrics and that no further amendments to the ETA are necessary to facilitate the usage of biometric technology in electronic transactions.*

Question 20: *IMDA welcomes views on other possible technologies that enterprises or sectors may wish to deploy, but are unclear whether the ETA facilitates or prohibits these.*

4. CERTIFICATION AUTHORITY FRAMEWORK

4.1. The ETA provides for the enactment of the Electronic Transactions (Certification Authority) Regulations 2010 ("**CA Regulations**"). The CA Regulations provide a legal framework to facilitate the establishment of trusted certification authority services in Singapore.

4.2. The review of the ETA also includes the review of the CA Regulations to ensure the technical relevance of the CA Regulations in relation to international developments in this area. With the emergence of a more mature PKI market and the burgeoning sophistication of cybercrimes, the CA Regulations, in particular the existing CA compliance audit framework (security guidelines) which sets out the necessary requirements for the accreditation CAs, may require further review to ensure its relevance.

4.3. The following issues are discussed in this Part:

a. Currency of the voluntary accreditation framework for Certification Authorities; and
b. Compliance Audit Checklist to adopt a set of baseline requirements which are aligned to international standards.

4.4 ACCREDITATION FRAMEWORK

4.4.1 The ETA was amended in 2010 to replace the licensing of CAs of Digital Signatures with an accreditation framework. The amendment was premised on the assessment that a voluntary accreditation framework would be more conducive to the growth of the industry. It also provided CAs with the flexibility to determine whether their business interests are best served by complying with IMDA's relevant CA framework.

CAs seeking accreditation must comply with IMDA's Compliance Audit Checklist which covers the CAs' operational policies, procedures and security. The other criteria that CAs will be evaluated against include their financial standing and track record. Upon accreditation, accredited CAs enjoy limits to liability, for example where there was loss caused by reliance on a forged digital signature, so long as the accredited CA has complied with the requirements of the ETA and the CA Regulations. Accredited CAs also enjoy the benefits of evidentiary presumption for digital signatures generated from the certificates they issue. Without such a presumption, a party that intends to rely on a digital signature must produce enough evidence to convince the court that the signature was created under conditions that will render it trustworthy. With the presumption, the party relying on the signature

merely has to show that the signature has been correctly verified, and the onus is on the other party disputing the signature to prove otherwise.

4.4.2 Adoption of a voluntary accreditation framework was also in keeping with the practices adopted by other countries such as Australia[39], the US[40], UK[41], the Netherlands[42], and Japan[43]. Further, based on a scan of the approaches adopted by other countries, it was observed that adopting a licensing approach did not result in any notable difference in the quality of outcomes when compared to an accreditation approach[44].

4.4.3 Given the above, IMDA proposes to retain the current voluntary accreditation framework. This give CAs the flexibility to determine if there is a business case for applying for accreditation by IMDA.

Question 21: *IMDA welcomes views and comments on whether the existing voluntary nature of the CA accreditation framework for Digital Signatures should be maintained.*

4.5 COMPLIANCE AUDIT FRAMEWORK

4.5.1 As mentioned in the section above, Accredited CAs (or CAs applying for accreditation) must comply with IMDA's Compliance Audit Checklist which covers the CA's operational policies, procedures and security (the "**Checklist**"). At present, the Checklist criteria are categorised across 6 broad areas of focus:

a. Certificate Authority Overall Governance (Criteria 1-26)
b. Certificate Management Controls (Criteria 26-51)
c. Key Management Controls (Criteria 52-72)
d. System and Operational Controls (Criteria 73-84)
e. Application Integration Controls (Criterion 85)
f. Compliance with ETA and ETR 2010 (Criteria 86-87)

4.5.2 IMDA conducted a technical review of the Checklist to ensure the relevance of IMDA's compliance audit requirements in view of the evolving cybersecurity landscape. This review also took into consideration that large

[39] See Gatekeeper Public Key Infrastructure Framework.
[40] See Public Key Infrastructure Assessment Guidelines.
[41] See Electronic Communications Act (2000)
[42] See TTP.NL scheme for Certification Authorities.
[43] See Electronic Signatures Act (2000).
[44] Based on Capstone CTS Asia Pacific's study *Report for Comparison Study of Audit Requirements for Certification Authorities* prepared for IMDA.

international IT firms (such as those that run root CA programmes) have also been updating their CA frameworks and aligning their requirements to international standards. As part of the review, the requirements under the Checklist were compared against the latest versions of globally recognised CA standards such as WebTrust and those set by the European Telecommunications Standards Institute ("**ETSI**").

4.5.3 An analysis of the WebTrust 2.1[45] and ETSI[46] CA standards, along with other related standards such as ISO 15408 and the baseline requirements of the CA Browser forum, revealed that the enhancements made to the latest versions of these standards were primarily meant to improve the interoperability of the standards by users globally and within their domestic environments when compared to earlier versions (such as the WebTrust 1.0 and the earlier versions of ETSI).

4.5.4 Given the above, IMDA is of the view that to ensure the currency and effectiveness of IMDA's compliance audit requirements, there are two possible options considered:

a. Review and update IMDA's existing Checklist using the WebTrust 2.1 or ETSI standards or both as reference (IMDA will need to review and update the Checklist every time the WebTrust or ETSI standards, or both standards, are updated); or

b. Adopt WebTrust or ETSI's standards or both directly for compliance (update is done on WebTrust's or ETSI's end or both ends). Additional requirements (if necessary) can then be added on top of the standards.

4.5.5 Given that WebTrust and ETSI are established international standards, IMDA proposes to adopt option (b). By virtue of directly adopting WebTrust or ETSI standards or both as proposed under option (b), IMDA's Compliance Audit requirements would remain, at all times, the latest version of the mentioned standard(s). This could reduce the duplicative work of updating a separate set of audit requirements every time WebTrust or ETSI updates their respective standards. Local regulatory/technical requirements, if any, can then be added on top of the adopted standard.

4.5.6 As part of the proposed adoption of option (b), IMDA also considered if there was merit to specify the use of either or both WebTrust and ETSI standards. It was observed that the cybersecurity landscape continues to evolve at an

[45] WebTrust v 2.1 has reformatted its original framework to make it more user friendly and has added some additional material to help both the auditor and the CA to align their processes.
[46] ETSI's changes focused on expanding areas where the standard was less explicit.

increasing pace. Leveraging either or both of the mentioned international standards will, in general, mitigate the risk brought about by the changing landscape. Further, as internationally recognised standards, the broad areas covered by WebTrust and ETSI are already similar. Therefore, adopting the latest versions of either standard will sufficiently provide IMDA with a default coverage position which gives IMDA the flexibility to calibrate and refine its framework (especially in view of the fast evolving landscape).

4.5.7 IMDA is of the view that the review of the CA accreditation framework and the adoption of international CA audit framework would facilitate the adoption of digital signature and authentication services, including the rolling out of the National Digital Identity project. The CA accreditation framework sets out baseline requirements and accredited CAs may incorporate additional requirements to meet its needs or contractual obligations.

Question 22: *IMDA welcomes views and comments on the adoption of the latest version of either (or both) International CA audit frameworks (WebTrust and ETSI) directly for applicants applying/renewing for CA accreditation to comply with.*

Question 23: *IMDA welcomes views and comments on whether the above areas adequately cover what the ETA Review should include.*

5. INVITATION TO COMMENT

5.1 IMDA would like to seek the views and comments from members of the public and the industry on the above issues.

5.2 Parties that submit comments on the issues identified in this Consultation Document should organise their submissions as follows:

a. Cover page (including their personal/company particulars and contact information);
b. Table of contents;
c. Summary of major points (structured to follow the individual Parts of the Consultation Document);
d. Statement of interest;
e. Comments (in response to the Questions set out in the Consultation Document and any other comments); and
f. Conclusion.

Supporting material may be placed in an Annex.

5.3 Where feasible, parties should identify the specific sections of the Consultation Document on which they are commenting and provide reasons for their proposals.

5.4 All submissions must reach IMDA by 12 noon on 27 August 2019. Softcopy of submissions in both Microsoft Word and Adobe PDF format should be provided. Parties submitting comments should include their personal/company particulars as well as the correspondence address, contact number and email addresses on the cover page of their submission. All comments should be addressed to:

Aileen Chia (Ms)
Deputy Chief Executive (Policy, Regulation & Competition Development),
Director-General (Telecoms & Post)
Infocomm Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Please submit your softcopy via email to: consultation@imda.gov.sg

5.5 IMDA reserves the right to make public any written submissions and to disclose the identity of the source. Commenting parties may request confidential treatment of any part of the submission that the commenting party believes to be proprietary, confidential or commercially sensitive, with supporting justification for IMDA's consideration. In such cases, the submission must be provided in a non-confidential form suitable for publication, with any confidential information redacted as necessary and placed instead in a separate annex.

5.6 If IMDA grants confidential treatment, it will consider, but will not publicly disclose the information. If IMDA rejects the request for confidential treatment, it will return the information to the party that submitted it and will not consider the information as part of its review. As far as possible, parties should limit any request for confidential information submitted. IMDA will not accept any submission that requests confidential treatment for the entire, or a substantial part of, the submission.

Annex A

Comparison of the Exclusion Lists in ETA-Equivalent Legislation of Key Benchmark Countries

	Negotiable Instruments	Wills	Indentures, Trusts and PoAs	Contracts for Immovable Property	Conveyance for Immovable Property	Other exclusions[1]
Singapore (Current)	Excluded					N.A.
Singapore (Proposed)	Not Excluded		Not Excluded[2]	Not Excluded[3]	Not Excluded	N.A.
United Kingdom	Not Excluded					N.A.
Norway	Not Excluded					N.A.
Canada[4]	Excluded[5]		Excluded[6]	Not Excluded		N.A.
New Zealand[7]	Excluded		Excluded[8]	Not Excluded		N.A.
New York	Excluded[9]	Excluded		Not Excluded		N.A.
Australia	Excluded			Not Excluded[10]	Excluded	Yes[11]
Hong Kong	Excluded					Yes[12]

N.A. – Not Applicable

Footnotes for Annex A

[1] This is a comparison of Singapore's ETA with the ETA-equivalent legislation of other countries. In Singapore and other countries, notwithstanding the ETA, there may be other laws which impose requirements which preclude the use of electronic signatures or records. This comparison does not take into account such exclusions found in other laws.
[2] Trust relating to immovable property or dispositions of equitable interest and "True Agency" POAs remain excluded.
[3] To require secure electronic signatures.
[4] The Uniform Electronic Commerce Act is being used for comparison. It however does not have the force of law. The actual laws are the enactment in each Province which may or may not have enacted the UECA in its entirety, may omit exclusions that are in the UECA or may include new exclusions. For example, most provinces have adopted the UECA. Some provinces have legislation that are almost identical to the UECA. However, while the UECA excludes powers of attorney, to the extent that they are in respect of the financial affairs or personal care of an individual, section 7(1) of the Alberta Electronic Transactions Act excludes only enduring powers of attorney under the Powers of Attorney Act. Also, while both the Alberta Electronic Transactions Act and the British Columbia Electronic Transactions Act exclude records or documents that create or transfer interests in land, this exclusion was repealed in the Newfoundland and Labrador Electronic Commerce Act in 2009.
[5] Part of the Uniform Electronic Commerce Act applies to negotiable instruments (see section 2(4) and Part 3).
[6] Excluded are trusts created by wills or by codicils to wills, powers of attorney in respect of the financial affairs or personal care of an individual.
[7] The updated position in New Zealand is in the Contract and Commercial Law Act 2017 which repealed the Electronic Transactions Act 2002.
[8] Powers of attorney and enduring powers of attorney are excluded.
[9] For negotiable instruments and other instruments of title where possession of the instrument is deemed to confer title, not excluded if allows for the creation of 1 unique, identifiable and unalterable version.
[10] The Commonwealth electronic transactions legislation does not preclude electronic conveyancing. The Electronic Conveyancing National Law has been introduced for adoption in each state. This national law has been adopted in all the states e.g. in NSW, this is done through the Conveyancing Act 1919 and the Electronic Conveyancing (Adoption of National Law) Act 2012. While all the states have adopted the legislation, it would appear that electronic conveyancing is currently live in 5 states – NSW, Vic, QLD, WA and SA. In SA, electronic conveyancing is currently being carried out. There are only certain transactions that still need to be completed on paper e.g. application to register a death of a joint registered proprietor.
[11] Corporations Act 1989 and Corporations Law (Commonwealth) and a list of other legislation.
[12] Statutory declarations, judgments, warrants issued by a court or magistrate.

Annex B

Background of the Model Law on Electronic Transferable Records

1. Transferable documents or instruments include documents such as the bill of lading, warehouse receipt, dock warrant or negotiable instruments such as the bill of exchange, promissory note or cheque. By virtue of section 4(1) read with item 2 of the First Schedule to the ETA, Part II of the ETA does not apply to "[n]egotiable instruments, documents of title, bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money".

2. As a shorthand, this category of documents or instruments is referred to as "transferable documents or instruments", which refers to two categories of documents — (i) transferable instrument for payment of money and (ii) transferable document of title. A transferable document or instrument evidences an obligation owed by the person issuing the document, or a third party, to another named in the document or to the bearer. A valid holder of such a transferable document or instrument has a right to demand the performance of this obligation. This holder may transfer this right to another person by transferring the transferable document or instrument[1].

3. An ETR is the electronic equivalent of a transferable document or instrument. The electronic transmission of an electronic record typically involves the replication of the electronic record. As an electronic copy of an electronic record is identical to the "original" (resulting in the "original" document being no longer unique), if the electronic record is given legal recognition as an ETR, replication of the electronic record could give rise to multiple claims founded on identical electronic records. This illustrates the central issue in the use of ETRs — the need to guarantee the singularity or uniqueness of the electronic record constituting the ETR such that only one set of obligations is owed by the person who is obliged to perform. This would ensure that only one party would be entitled to require performance of the obligations embodied in the ETR. The key legal challenge is therefore to define the electronic functional equivalents of the requirement for possession of a unique or singular transferable document or instrument.

[1] A "negotiable" instrument is a transferable instrument which can confer a more valid title to the transferee, assuming the transferor's title was somehow defective and the transferee received the negotiable instrument in good faith (i.e., without knowledge or suspicion of the defect) and for value (i.e., payment in money or money's worth).

Annex C

IMDA's Preliminary Views on the Application of ETA Concepts on "Electronic Record" and "In Writing" in the Context of Distributed Ledger Technology

1. **"Electronic Record"**

1.1. The term "electronic record" is defined in section 2(1) of the ETA to mean "a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another", for example, emails and digital images etc. This definition is a functional description, and does not *prima facie* exclude the use of any technology where the function requirement can be demonstrated.

1.2. As the ETA does not mandate the specific type of electronic storage system, IMDA takes the view that that information stored electronically, whether using traditional databases such SQL[48] or using DLT such as blockchain, may satisfy the requirements and hence qualify as an electronic record as defined under the ETA.

2. **"In Writing"**

2.1. In respect of the term "in writing", section 7 of the ETA provides that:

"where a rule of law requires information to be written, in writing, to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference".

2.2. Consistent with principle of technological neutrality espoused in the ETA, the Singapore courts have also confirmed that under the common law, the legal requirement for something to be "in writing" may also include electronic writing, e.g. email correspondence[49].

2.3. IMDA is of the view that it is possible for records of transactions or contracts which are stored on a distributed ledger to satisfy the "in writing" requirement, save for exceptional circumstances where the information contained in the record is somehow not usable for subsequent reference.

[48] SQL refers to Structured Query Language, a domain specific standard language used in programming for the purposes of managing data stored in relational databases.
[49] SM Integrated Transware Pte Ltd v. Schenker Singapore (Pte) Ltd [2005] 2 SLR(R) 651 (SGHC) at [76]-[77].

Annex D

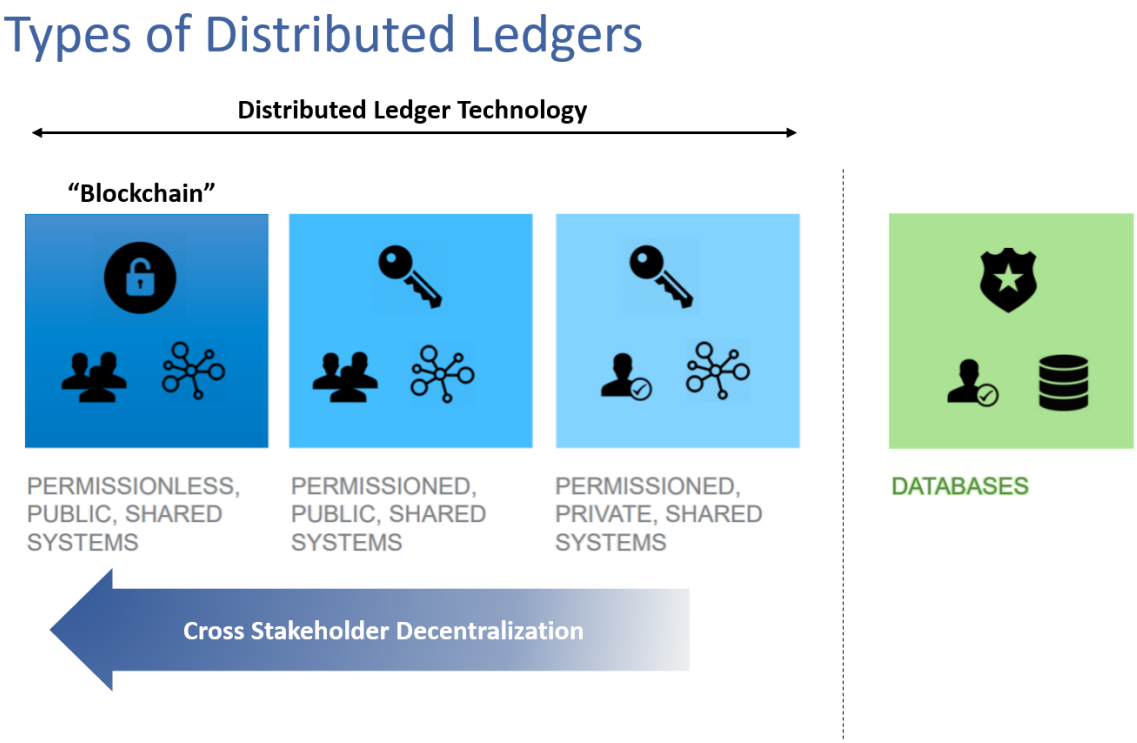
Different Types of Distributed Ledgers

1. Broadly, there are three main types of Distributed Ledgers:

   a. **Type 1: Permissionless, public systems:** These type of systems allow anyone to join the network, to write to the network, and to read the transactions from those networks. These systems do not have a single owner; everyone on the network has an identical copy of the "ledger". The most common examples are the Bitcoin blockchain and Ethereum blockchain.

   b. **Type 2: Permissioned, private systems:** Only certain individuals who are 'whitelisted' have access to read or write to such systems. There may be one or many owners to manage the system. An example would be a financial institution's use of a permissioned, private blockchain to reduce time of international payments.

   c. **Type 3: Permissioned, public (hybrid) systems:** This consists of a public blockchain that all participants are a part of, and a private (permissioned) network that restricts participation to those invited by a centralised body. Whitelisted access is required to write to such systems but all the transactions are publicly viewable. The hybrid model is suitable for governments, financial institutions and large, multi-national corporations due to the flexibility of control over what data and/or transactions are kept private and what is shared on the public ledger. A private sector example is the use of blockchain in food safety where the tracking device will write on the chain but can be viewed by vendors and the public.



Source: Blockchain Beyond the Hype – A Practical Framework for Business Leaders: World Economic Forum (2018)