**APPENDIX A**

**COVER PAGE**

**RESPONSE TO THE CONSULTATION PAPER ISSUED BY THE INFOCOMM MEDIA DEVELOPMENT AUTHORITY ("IMDA") DATED 27 JUNE 2019 RELATING TO REVIEW OF THE ELECTRONIC TRANSACTIONS ACT ("ETA") (CAP 88)**

| | |
|---|---|
| Submitted By: | **Law Society of Singapore, 28 Maxwell Road, #01-03, Maxwell Chambers Suites, Singapore 069120** |
| Name of Submitting Person's Representative: | **Ms Genie Gan, Head of Department, Director of Representation and Law Reform** |
| Submitting Person's Contact Information: | **geniegan@lawsoc.org.sg, 65300249** |
| Date of Submission: | **27 August 2019** |

**APPENDIX A**

## TABLE OF CONTENTS

## APPENDIX A

### SUMMARY OF MAJOR POINTS

1. The **Corporate Practice Committee's views** on "Facilitating Innovation and Digitalisation of Businesses and Government Services"

   a. As long as there are sufficient safeguards to protect the interests of members of the public who are dealing as consumers, there is no cogent public policy reason to delay the date of bringing the amended ETA in force until 2021.
   b. Distributed ledger technology ("**DLT**") could provide an effective solution to the problem described above as it promises to offer a way for an immutable set of records to be kept without relying on one "single source of truth". Therefore, we welcome taking way wills and testamentary dispositions from the exclusion list to allow DLT to address this problem.
   c. We agree that documents of title and negotiable instruments should be removed from the exclusion list in the First Schedule as typically it would only be businesses that handle such legal documents and one would assume that corporations and businessmen have the sophistication to deal with an electronic form of such documents. In fact, we would believe that such a move would be warmly welcomed by forward-looking enterprises in the shipping and logistics sectors, and commodities trading and financing sector who wish to automate the task of processing such documents.
   d. We do not agree that only POAs for the purposes of enforcement of security interests should be removed from the exclusion list. We would advocate that all POAs be removed.
   e. We agree that Lasting Powers of Attorney which must be registered with the Ministry of Social and Family Development ("**MSF**") to take effect should be removed from the exclusion list. Exercising its administrative power and discretion, MSF could decide on the appropriate safeguards to implement before MSF would accept electronically signed Lasting Powers of Attorney, and it is unnecessary to legislate for this matter through the ETA.
   f. We agree that testamentary trusts should be removed from the exclusion list for the same reasons as canvassed in question 4 below to support our position that wills and testamentary dispositions should be removed as well.
   g. We do not agree that declarations of trust relating to immovable property and dispositions of equitable interests should be retained in the First Schedule. We do not agree that the nature of these types of legal documents present unique risks to the elderly and vulnerable in the society as opposed to wills and testamentary dispositions for instance.
   h. Real estate transactions of lesser value such as leases of immovable property of a period less than seven years are generally not registered by tenants with the Singapore Land Authority. For such lease transactions (which would form the bulk of property transactions every year), we do not see any utility to require "secure electronic signatures" or "digital signatures" to be appended before they have legal effect. In fact, it would create unfairness if a person who wish to renege on his/her obligations in a lease to rely on the fact that an electronic signature is not a "secure electronic signature" or "digital signature" as probably most laypersons would not

appreciate the difference between an electronic signature as opposed to a "secure electronic signature" or "digital signature".

i. Finally, we wish to point out that under the current ETA, the only difference between using a "secure electronic signature" and an "electronic signature" is that the use of the former creates evidential presumptions regarding the authenticity and provenance of the electronic record. An evidential presumption can be rebutted by producing evidence to the contrary, such as the conduct of the parties after the date of execution of the electronic contract. The proposal of IMDA to require "secure electronic signatures" to be used for transactions involving immovable property greatly accentuates the legal impact of having appended a "secure electronic signature" versus an "electronic signature", and it would be unfortunate that a measure meant to mitigate fraud and create greater certainty will end up causing more uncertainty of its own.

2. The **Cybersecurity & Data Protection Committee's views** on "Facilitating New Technologies in Electronic Transactions"

a. We agree with the IMDA's view that the ETA does not prohibit the use of smart contracts, and that no further amendments to the ETA in this regard should be necessary.

b. Indeed, to avoid confusion in terminology, and for the ETA to remain technology-neutral, we are of the view that the expression "smart contract" should <u>not</u> be codified into the ETA, as the reference to a "smart contract" is not a legal term (and requires disambiguation).

c. Accordingly, our view is that no legislative refinements are necessary to the ETA in order to recognise the concept of "smart contracts" in the sense of "automated contracting".

d. Since a reference to "smart contracts" may mean either Automated Contracting or Automated Execution, and Automated Contracting is already sufficiently addressed under the existing framework of the ETA (and consistent with common law orthodoxy), we find no necessity to disturb the status quo by legislatively introducing the ambiguous concept of "smart contracts" and all the uncertainties with it. Certainty in contract is extremely important in everyday exchanges.

e. Nevertheless, we accept, parenthetically, the observations in the decision in *B2C2* that "*the law in relation to the way in which ascertainment of knowledge in cases where computers have replaced human actions is to be determined will, no doubt, develop as legal disputes arise as a result of such actions. This will particularly be the case where the computer in question is creating artificial intelligence and could therefore be said to have a mind of its own*".

f. We note that the IMDA has concluded that biometrics technology is "unlikely to be understood as a <u>secure electronic procedure</u>" under the ETA as biometrics technology "by itself, does not typically allow for <u>non-repudiation</u>": see paragraphs 3.4.4 and 3.4.5 of the Consultation Paper. From a legal perspective, given that biometrics technology is technically complex, we find no reason to disturb the technical conclusion reached by the IMDA, especially in relation to the finding that biometrics technology does not typically allow for non-repudiation.

3. The **Cybersecurity & Data Protection Committee's views** on "Certification Authority Framework"

   a. We are of the view that it ought not to be an issue to maintain the existing voluntary nature of the CA accreditation framework for Digital Signatures. But it may be worth looking into the actual process and to review the framework to take into account new technologies in the field. To date, there has been no alternative to the Public Key Infrastructure methodology in terms of identification and authentication although other technologies are being used for identification such as biometrics, facial recognition etc. The voluntary nature of the CA accreditation should be maintained.
   b. We agree with the proposed approach by IMDA to adopt the prevailing version of **either** WebTrust or ETSI's standards as the relevant standard for complying with CA accreditation requirements. This is because a single adopted standard is easier for implementation and compliance for market consistency although it may affect interoperability with countries that choose the other alternative. While a single standard can be preferred and adopted, the other standard should not be prohibited so as to allow companies to choose what the best way forward for them is.
   c. We also agree that there should be a residual discretion to calibrate or refine the CA framework should this be necessary. Specifically, on this discretion, we respectfully submit that amendments to the ETA regulations set out further details on this discretion expressly including on when this discretion may be invoked, any criteria to be met for this discretion to be exercised and by whom this discretion can be exercised.

## APPENDIX A

### STATEMENT OF INTEREST

The Law Society of Singapore was established under the Legal Profession Act in 1967. It carries out various statutory functions, including:

- maintaining and improving the standards of conduct and learning of the legal profession in Singapore;
- facilitating the acquisition of legal knowledge by members of the legal profession;
- representing, protecting and assisting members of the legal profession in Singapore; promoting in any manner the Society thinks fit the interests of the legal profession in Singapore; and
- protecting and assisting the public in all matters ancillary or incidental to the law.

As the members of the Law Society comprise mainly practising lawyers with the rest being in-house counsels. Our members may give advice to clients on the impact of the Electronic Transactions Act in the course of their practice of law. The comments in this document have been provided by both the **Corporate Practice Committee (Questions 1 to 17)** and the **Cybersecurity & Data Protection Committee (Questions 19 to 23)**.

The **Corporate Practice Committee** addresses and provides guidance on matters relating to corporate practice, provides feedback in public and other consultations on legislative and practice changes in corporate practice and liaises with the Courts, and other bodies on corporate practice matters.

The **Cybersecurity & Data Protection Committee** provides guidance on all matters relating to cybersecurity including but not limited to information security management, data privacy and protection, data governance, cybercrime, and digital forensic investigation and legal practice.

## COMMENTS AND FEEDBACK

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

No comments/feedback received on this question.

**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.**

We unreservedly agree that the current exclusions in the First Schedule to the ETA could be significantly, and perhaps even totally, repealed. As mentioned repeatedly in the Consultation Paper, e-commerce was in a nascent stage when the ETA was first enacted and the Singapore society in tandem with the rest of the developed world has since widely embraced the "digital age".

There is an economic imperative for the Singapore legal system to be regarded by MNCs and international investors to be "digitally ready" or even to be seen as a friendly jurisdiction for disruptive enterprises. To meet this objective, we believe a "sun-rise period" of 2021 will be perceived as being too conservative and will send a mixed signal to the market. As long as there are sufficient safeguards to protect the interests of members of the public who are dealing as consumers, there is no cogent public policy reason to delay the date of bringing the amended ETA in force until 2021. There will always be a section of the Singapore society who are not be ready to cope with technological disruptions for a variety of reasons and even a delayed start in 2021 or 2022 would not make them more ready.

**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.**

No comments/feedback received on this question.

**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.**

Wills are unique in the sense that unlike other legal documents dealt with in the First Schedule which need to be registered by a centralised government agency (such as Lasting Powers of Attorney made under the Mental Capacity Act (Cap 177A) or transactional documents that alienate an interest in immoveable property), testamentary dispositions become valid and effective once the formalities prescribed in the Wills Act (Cap 352) are performed. Therefore, it can be disputed whether a testator made one or more versions of his/her will as there is no single depository that indicate when a will has been executed or give directions to where a copy of the will can be found.

Distributed ledger technology ("**DLT**") could provide an effective solution to the problem described above as it promises to offer a way for an immutable set of records to be kept without relying on one

"single source of truth". Therefore, we welcome taking way wills and testamentary dispositions from the exclusion list to allow DLT to address this problem.

We believe the fears that it would present greater risks of fraud and exploitation if electronic versions of wills are allowed are misplaced. Although the elderly and vulnerable might be misled to execute electronic wills or allow their electronic signatures to be appended to wills, it could be said that the same group may also be misled in executing "paper wills". The courts would surely take judicial notice that it would be highly and extremely unusual for an elderly or vulnerable person to choose to execute an electronic will if in the daily life of the testator, he/she has shown little inclination to embrace technology. Hence, in our view, this amendment to the exclusion list will not present greater risks of exploitation to the vulnerable persons in society.

**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.**

No comments/feedback received on this question.

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

We agree that documents of title and negotiable instruments should be removed from the exclusion list in the First Schedule as typically it would only be businesses that handle such legal documents and one would assume that corporations and businessmen have the sophistication to deal with an electronic form of such documents. In fact, we would believe that such a move would be warmly welcomed by forward-looking enterprises in the shipping and logistics sectors, and commodities trading and financing sector who wish to automate the task of processing such documents.

For the SMEs that may lack the sophistication to deal with the risks of handling electronic versions of documents of title and negotiable instruments, they could elect to continue to use paper form of such legal documents until it becomes an industry standard to prefer the use of electronic version of such legal documents.

Our only caveat to the above observations is that the ordinary person in the street may handle cheques (which is a negotiable instrument) in his/her daily life and allowing an electronic version of cheques does mean putting them in the "hands" of the ordinary person. Notwithstanding this:

(a) one would assume that no bank in Singapore would force its retail customer to use an electronic version of a cheque if the customer prefers not to do so, and in any event the retail customer already has a surfeit of choice in making electronic payments such as through the FAST system or PayNow system and adding one more choice is hardly ground-breaking to their banking experience; and

(b) since the Monetary Authority of Singapore has decided to allow three digital banks to be established who would be allowed to have retail customers, one would imagine that the customers would want to have the equivalent of a chequing bank account and therefore, electronic versions of a cheque should become the norm.

**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.**

No comments/feedback received on this question.

**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.**

We do not agree that only POAs for the purposes of enforcement of security interests should be removed from the exclusion list. We would advocate that all POAs be removed.

First of all, it should be appreciated that POAs are widely used in commercial contracts between corporations and not only as a standalone document for the purposes of enforcement of security interests. It is common for investment agreements, joint venture agreements and consortium agreements for the contracting parties to either enter into an ancillary POA or embed a POA clause in the main legal document to allow a party to perform an act on behalf of the other party(ies) which the latter has or have contractually undertaken to perform in certain circumstances.

It would present a strange result if POAs are selectively excluded in the First Schedule. It would call into question whether a commercial agreement, say, a joint venture agreement governed by Singapore law with an embedded POA clause and executed by the parties as an electronic agreement would fall within Part II of the ETA because of the non-excluded POA.

We do recognise that for the ordinary person in the street, the POA that he/she is likely to encounter would be a standalone POA to allow a donee to effect property transactions on the donor's behalf. If it is believed that there are policy reasons to include such POAs in the First Schedule, then our suggested alternative to the proposal in the Consultation Paper would be to exclude POAs not executed by donors dealing as consumers.

The Unfair Contract Terms Act (Cap 396) and Consumer Protection (Fair Trading) Act (Cap 52A) are two excellent examples where the law recognises that persons dealing as consumers should receive greater legislative protection. Both legislation defines persons who are not acting in the course of carrying out a business to be "consumers". The Unfair Contract Terms Act has been in force since 1993 and in the Singapore court cases that had applied or interpreted provisions of this Act, the application of the statutory definition of "dealing as consumers" as used in that Act did not appear to cause hardship. Thus, we believe that it would not cause any inherent difficulty to provide that only POAs as executed by donors dealing as consumers should be included in the First Schedule.

**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.**

We agree that Lasting Powers of Attorney which must be registered with the Ministry of Social and Family Development ("**MSF**") to take effect should be removed from the exclusion list. Exercising its administrative power and discretion, MSF could decide on the appropriate safeguards to implement before MSF would accept electronically signed Lasting Powers of Attorney, and it is unnecessary to legislate for this matter through the ETA.

**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.**

No comments/feedback received on this question.

**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.**

No comments/feedback received on this question.

**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.**

We agree that testamentary trusts should be removed from the exclusion list for the same reasons as canvassed in question 4 above to support our position that wills and testamentary dispositions should be removed as well.

As we understand, the term "indenture" which is not statutorily defined under Singapore law, means a legal document that sets out rights and obligations of lenders and borrowers, or mortgagees and mortgagors. A legal agreement does not have to be labelled as an "indenture" in order to be legally defined as one, and there is no policy reason why legal agreements evidencing a debt should be excluded from the ambit of Part II of the ETA as opposed to legal agreements that sets out other obligations such as to sell and purchase securities.

We do not agree that declarations of trust relating to immovable property and dispositions of equitable interests should be retained in the First Schedule. We do not agree that the nature of these types of legal documents present unique risks to the elderly and vulnerable in the society as opposed to wills and testamentary dispositions for instance. In paragraph 2.6.14 of the Consultation Paper, it is written:

> *"… 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".*

Our response to the hypothetical example above is that such fraudulently executed electronic agreements should be regarded as a forgery and nullity as the user accounts, passwords and devices were effectively stolen from the vulnerable and misused by the rogue caregivers. Perhaps the more apposite scenario is where the vulnerable acting under misrepresentation by their family members applied or agreed to apply their electronic signature to a legal document. In that case, the legal issue should be whether such a person shall be deemed to have agreed to execute the legal document.

The legal issue should be answered by determining how the doctrine of *non est factum* should apply to agreements signed by electronic means. In Singapore, the seminal case on *non est factum* is the Court of Appeal decision of *Mahidon Nichiar bte Mohd Ali and others* v *Dawood Sultan Kamaldin [2015] 5 SLR 62*. It is sufficient for us to quote two passages from the Court of Appeal's judgement:

> *"[119] Non est factum is a specific category of mistake that operates as an exception to the general rule that a person is bound by his signature on a contractual document even if he did*

> *not fully understand the terms of the document. If successfully invoked, the transaction entered into by the document so signed is void …*
>
> *[123] The doctrine of non est factum, as the Judge was right to point out, is a narrow one (see the GD at [185]–[186]). It will only be successfully raised in exceptional circumstances, and, so, much will depend on the facts of each case … If, for example, an elderly and poorly educated client enters into a complex transaction by signing a set of documents without receiving adequate legal advice on those documents, it is unlikely that he would be precluded from raising a plea of non est factum even if he had read the documents, simply because he would be unlikely to have understood them in the circumstances …"*

There is no reason to think the doctrine of *non est factum* would not apply to electronically executed documents, especially to complex legal arrangements like a declaration of trust involving immovable property or a disposition of equitable interests. That we submit is the true safeguard provided under Singapore law and it is not necessary to single out declarations of trust involving immovable property and dispositions of equitable interests for special consideration.

We would also like to take the opportunity to comment on the observation made by IMDA in footnote 17 to paragraph 2.6.10 of the Consultation Paper. Specifically, in relation to whether a deed may be executed in an electronic form, it was written that:

> *"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."*

One observation is that the Singapore law in relation to the delivery and execution of deeds should be reviewed and updated. It has never been modernised in the same way as the UK (which did away the need for foreign companies and individuals to use a seal, whereas Singapore only relaxed the requirements for local companies). It is at odds with the aim of making electronic transactions easier to cling on to outmoded concepts that increasingly are alien to business people and just cause confusion, even among lawyers who are supposed to know. Relying on the common law generally in the area of execution of deeds is increasingly out of touch with the need to make law accessible. The IMDA consultation paper at paragraph 2.6.10 stated that:

> *"In practice, deeds are also almost always attested, although this is not a legal requirement".*

This statement may have overlook some of the practical issues that need to be addressed in relation to the execution of deeds by electronic means. The issues around the English High Court decision in R *(on the Application of Mercury Tax Group Limited and another) v HMRC [2008] EWHC 2721 (Admin)* is also not mentioned.

We agree that it is a vexing question and unsettled law whether a deed can be truly said to be executed by an individual if it is in an electronic form. In the case of Singapore incorporated companies, the recently introduced section 41B of the Companies Act has answered the question affirmatively by providing that a company may execute a deed without affixing its common seal when certain signatories execute the legal document or certain attestation is performed. We believe that it is salutary for Part II of the ETA to be amended to insert a new section that deems a seal to be affixed on an electronic record by an individual if he/she has placed an electronic reproduction of a seal on

that electronic record. This would greatly assist corporations to use Singapore law to govern their electronic contracts as it would remove an area of doubt.

Recognition of "electronic seals" using trust services for both individuals and corporate might go some way to alleviating some of the complications that arise with the virtual execution of deeds, given the law on deeds as it stands, which requires either one or more of a seal, a witness or multiple signatures, none of which intuitively relevant to a virtual world where authenticity can be established by digital methods, involving third party trust services where needed.

**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.**

No comments/feedback received on this question.

**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.**

No comments/feedback received on this question.

**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.**

No comments/feedback received on this question.

**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.**

No comments/feedback received on this question.

**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.**

Real estate transactions form a very large part of Singapore's economy and Singapore cannot be truly said to have a thriving digital economy unless real estate conveyancing and transactions can be undertaken in a paperless form. Thus, we support removing contracts for the sale or disposition of immovable property from the exclusion list.

Most real estate transactions of large value, such as transfers of title and registration of mortgages, would have to be registered with the Singapore Land Authority in order to take effect. Exercising its administrative power and discretion, the Singapore Land Authority could decide on the appropriate safeguards to implement before they would accept electronically signed instruments for registration and it is unnecessary in our opinion to legislate in the ETA that only "secure electronic signatures" or

"digital signatures" must be appended on such documents. This will give more flexibility to the Singapore Land Authority to decide on the appropriate measures from time to time based on the feedback received from end-users.

Real estate transactions of lesser value such as leases of immovable property of a period less than seven years are generally not registered by tenants with the Singapore Land Authority. For such lease transactions (which would form the bulk of property transactions every year), we do not see any utility to require "secure electronic signatures" or "digital signatures" to be appended before they have legal effect. In fact, it would create unfairness if a person who wish to renege on his/her obligations in a lease to rely on the fact that an electronic signature is not a "secure electronic signature" or "digital signature" as probably most laypersons would not appreciate the difference between an electronic signature as opposed to a "secure electronic signature" or "digital signature".

We would also observe that the current definition of a "secure electronic signature" in the ETA requires a "commercially reasonable security procedure" to be applied before a signature could be deemed as such. Section 17(2) of the ETA sets out rather general guidance on the meaning of "commercially reasonable security procedure". We set out the text of section 17(2) below for ease of reference:

> "*whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including —*
>
> *(a) the nature of the transaction;*
>
> *(b) the sophistication of the parties;*
>
> *(c) the volume of similar transactions engaged in by either or all parties;*
>
> *(d) the availability of alternatives offered to but rejected by any party;*
>
> *(e) the cost of alternative procedures; and*
>
> *(f) the procedures in general use for similar types of transactions.".*

The non-exhaustive and general guidance creates doubt whenever a new or fledgling technology like DLT is deployed, whether it would meet the test of a "commercially reasonable security procedure".

If the proposal for a "secure electronic signature" to be appended to electronic records for real estate transactions is accepted, we think it would hinder the adoption of technology and spawn disputes regarding the fulfilment of the formality of execution of the legal document. It is simply difficult for lawyers to advise clients whether a "secure electronic signature" has been appended to an electronic record. The only solution to this problem would be for IMDA to regularly publish in the Government Gazette what are the technological products that are statutorily regarded as a "secure electronic signature", e.g. a DocuSign™ signature.

We also noted in the Consultation Paper that IMDA has tentatively and preliminarily espoused views whether certain technology meets the test of a "secure electronic signature". For instance:

(a) para 3.2.8.4 - "*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*." (*our emphasis added*)

(b) para 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.*"

(c) para 3.2.10.4 – "*IMDA notes that permissionless blockchains … 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*." (*our emphasis added*).

It seems to us that it could be a daunting task to anybody who is not a subject matter expert in cryptography to determine what a secure electronic signature is in the context of a blockchain. If the legal validity of a legal document depends on determining whether a secure electronic signature is appended, we submit that a much clearer and simpler test must be available to determine what a secure electronic signature is.

Finally, we wish to point out that under the current ETA, the only difference between using a "secure electronic signature" and an "electronic signature" is that the use of the former creates evidential presumptions regarding the authenticity and provenance of the electronic record. An evidential presumption can be rebutted by producing evidence to the contrary, such as the conduct of the parties after the date of execution of the electronic contract. The proposal of IMDA to require "secure electronic signatures" to be used for transactions involving immovable property greatly accentuates the legal impact of having appended a "secure electronic signature" versus an "electronic signature", and it would be unfortunate that a measure meant to mitigate fraud and create greater certainty will end up causing more uncertainty of its own.

**Question 18: Not found within Consultation Paper.**

[N/A]

**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.**

**A. <u>Smart Contracts</u>**

We agree with the IMDA's view that the ETA does not prohibit the use of smart contracts, and that no further amendments to the ETA in this regard should be necessary.

Indeed, to avoid confusion in terminology, and for the ETA to remain technology-neutral, we are of the view that the expression "smart contract" should **<u>not</u>** be codified into the ETA, as the reference to a "smart contract" is not a legal term (and requires disambiguation).

As the IMDA has recognised (at paragraph 3.3.3 of the Consultation Paper), conceptually, "smart contracts" may broadly refer to either: (a) "*legal contracts, or elements of legal contracts, automatically entered into by software*" ("**<u>Automated Contracting</u>**"); or (b) "*code that is designed to*

*execute certain tasks if pre-defined conditions are met*" ("**Automated Execution**"), though a spectrum of "smart contracts" exists.

For the reasons which follow, we find that the existing legal framework of the ETA is already consistent with the current orthodox approach of: (a) not denying the validity or enforceability of a contract solely because it arises from Automated Contracting; and (b) rejecting Automated Execution as constituting a legal contract *per se*.[1] Accordingly, we are of the view that it would be unnecessary to codify the terminology of a "smart contract" in the ETA or make legislative amendments in relation thereto,[2] as this is confusing a term of art with a legal definition of a contract as discussed below.

***Automated Contracting***

From the outset, we agree with the IMDA that "smart contracts", in the sense of Automated Contracting, are not prohibited by the ETA. As the IMDA has observed, the existing ETA framework (especially section 15 of the ETA, in relation to "*automated message systems for contract formation*") already recognises that a contract shall not be denied validity or enforceability solely because it arises from Automated Contracting such as electronic auctions.

In *Chwee Kin Cheong v Digilandmall.com Pte Ltd* [2004] SGHC 71, as referenced by the IMDA at footnote 35 of the Consultation Paper, the Court applied an "objective standard" taking into account, *inter alia* "the elements of an offer and acceptance … in every transaction", and "intention to enter into a legal relationship" to determine whether contracts "have in fact been entered into and concluded between the parties" in relation to "programmed computers sending out automated responses", which may, in principle, "bind the sender": see, e.g. *ibid* at [134].

Even if an argument may be made that Automated Contracting could somehow be technically broader than the concept of "automated message systems" under the ETA, section 11 of the ETA clarifies that the offer and acceptance (in the context of contract formation) may be expressed by means of electronic communications generally, and where electronic communication is used in the formation of a contract, "*that contract shall not be denied validity or enforceability solely on the ground that an electronic communication was used for that purpose*".

The foregoing position also appears to be consistent with the position taken by the English courts: see, e.g. *Software Solutions Partners Ltd, R (on the application of) v HM Customs & Excise* [2007] EWHC 971, where the English Court accepted that one party could programme a set of codes to generate binding offers on its behalf, based on pre-agreed parameters being met without any human intervention.

Accordingly, our view is that no legislative refinements are necessary to the ETA in order to recognise the concept of "smart contracts" in the sense of "automated contracting".

---

[1] Indeed, other members of the Society have also observed that current ETA definitions, concepts and provisions are broad enough to cater for contracts formed electronically through DLT (save for those excluded under Civil Law etc. and discussed under other parts of the public consultation). That said, the clarification that blockchains qualify as "digital signatures" under section 18, save for "permission-less blockchains", is also welcomed.

[2] In any event, the Society observes that the categories in Annex D to the Consultation Paper, broadly cover all types of DLTs. The main issue arising will be that the hybrid based systems are spread over a wide range. There may be therefore a need to further group them into sub-categories or industry / sector base, as some issues may arise only in a particular sector. Depending on how widespread the application, key sectors that will be of concern will be the implementation of DLTs in the financial, healthcare or other sectors.

***Automated Execution***

However, we propose that the IMDA avoid legitimising or giving recognition to Automated Execution as a recognised form of electronic "contracting" per se under the ETA, because so-called "smart contracts" – in the sense of Automated Execution – are not yet, and should not be conflated with, true contracts in the *legal* sense **unless** the usual legal requirements for legal contracts are somehow met in the circumstances, *viz*: offer and acceptance, valid consideration, intention to create legal relations, certainty of terms, absence of vitiating factors, etc.

In particular, in the absence of requisite ingredients to found a legal contract at law, any computer code for Automated Execution would merely constitute a program for the automation of the *performance* of an *aspect* of a legal agreement, and would not constitute the entirety of the legal agreement itself. Indeed, a computer code for Automated Execution would be unlikely to comprise the *complete* legal agreement if interpretive concepts such as "reasonable endeavours" and "good faith" (which may be difficult to address within code) are intended between contracting parties to be part of a broader agreement.

More significantly, Automated Execution cannot, in principle, be construed as self-enforcing in the *legal* sense. "Smart contracts" are sometimes said to be "self-enforcing" in the sense that they automatically execute a function on the occurrence of a pre-defined event (e.g. automatically execute a transfer of data, or automatically block access to cars or flats in the event of non-payment of a loan). However, *technically* guaranteed performance is not the same as enforceability in the *legal* sense, which relies on "jurisdiction-specific systems of adjudication" and judicial remedies (such as award of damages, rescission of contract, or specific performance). In other words, Automated Execution may, at the highest, be described as "self-enforcing" *practical* performance, but *legal* enforceability of an agreement relates, instead, to the court's jurisdiction to void an automatically-executed outcome by exercise of judicial power on grounds of, e.g. the code does not contain legally binding commitments between parties or vitiating factors, or that the code does not properly reflect the parties' agreement. Parties may make many changes along the way to reflect their intentions and these cannot be coded in unless every single change is coded. This will then contribute to raising the cost of the contracting. Smart contracts envisage a near ideal situation that each term has been agreed upon without any change, including change of dates and the like. It is almost an utopian-like situation.

For example, as one commentator has noted, if Automated Execution, for some reason, executes incorrectly due to a purported coding error (or some other glitch), "it seems more appropriate to speak of a *malfunction* than of breach". In this regard, we agree that the correct inquiry should be whether the Automated Execution has executed "*as intended or as promised, i.e. that the code correctly reflects the parties' agreement [and] that implementation matches intention*".[3] Such an orthodox approach to analysing mistakes arising from automated systems would also be consistent with the approach under the existing ETA which seems to emphasise the significance of the *intention of the contracting parties* (being natural persons). For example, section 16 of the ETA provides that, where a person inputs erroneously into an electronic communication exchanged with the automated message system of another party, and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error

[3] MIK, Eliza. Smart contracts: Terminology, technical limitations and real world complexity. (2017) *Law, Innovation and Technology.* 9, (2), 269-300. Research Collection School of Law. Available at: https://ink.library.smu.edu.sg/sol_research/2341.

was made. The current stance in the ETA strikes the correct balance between allowing automated contracting and human intervention where needed.

We are also fortified by the recent decision of *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 3 ("***B2C2***"), which held that "*when the law is faced with a contention that a contract made by and between two computer systems acting as programmed but otherwise without human intervention is void or voidable for mistake, it is necessary to have regard to the mindset of the programmer when the relevant programs, or the relevant part of those programs, were written. The knowledge of the programmer in question is to be inferred by the Court from the evidence adduced and from all the surrounding circumstances*" (see *ibid*, at [106] and [211]). In addition to recognising the existence of a broader agreement between natural persons in the context of Automated Execution, the decision of *B2C2* also demonstrates that courts continue to recognise the difference between the practical performance (which may be achieved by automation by a "smart contract") purportedly guaranteed by Automated Execution, and the legal enforceability of an agreement (which is interpretive in nature, and in this regard, the court's jurisdiction may not be ousted).

***Conclusion on "Smart Contracts"***

Since a reference to "smart contracts" may mean either Automated Contracting or Automated Execution, and Automated Contracting is already sufficiently addressed under the existing framework of the ETA (and consistent with common law orthodoxy), we find no necessity to disturb the status quo by legislatively introducing the ambiguous concept of "smart contracts" and all the uncertainties with it. Certainty in contract is extremely important in everyday exchanges.

Nevertheless, we accept, parenthetically, the observations in the decision in *B2C2* that "*the law in relation to the way in which ascertainment of knowledge in cases where computers have replaced human actions is to be determined will, no doubt, develop as legal disputes arise as a result of such actions. This will particularly be the case where the computer in question is creating artificial intelligence and could therefore be said to have a mind of its own*".

**B. Further Observations – Evolution to Distributed Ledger Technology ("DLT")**

A further observation relates as to the future ahead for DLT/blockchain. It cannot be denied that the integrity of data and encryption is one risk of DLTs; in cases where there is a cyberattack or system failure, the integrity of the data will be an issue. When the DLT is relied upon to identify a person under section 18(1)(b) of the ETA, there may be risks that the data integrity may be compromised. If DLT is deemed a secure electronic record, then a presumption of data integrity applies, but is the burden to prove that the data integrity has been compromised one that can be reasonably discharged? The third parties relying on a permissioned DLT may not know or have access to sufficient information to be able to prove or raise such issues. Furthermore, unless one is technically competent, it is not easy to raise questions that are relevant to the issue at hand. DLT is a complex technical subject matter even for technologists.

Here, the House of Lords Select Committee on Economic Affairs Inquiry on Distributed Ledger Technologies 2016 (19 July 2016) pointed out that in the long term, there may be an issue as to the encryption used to protect data stored on the ledger. This is because quantum computing technology advances could render current encryption standards deficient, as the amount of computing power is increasingly available at a lower cost to a wide community, including those who are using it for illegal means. The quantum of computing power and its access are no longer confined to universities and

governments, but is widely available to the members of the public. Are there regulations being contemplated over hybrid DLTs as to how the data is going to be stored (e.g. directly on the ledger itself or an off-ledger location)?

There have also been concerns raised over a 51% attack situation (to which permission-less DLTs may be more susceptible). Whilst this does not raise an issue in relation to "secure electronic signatures", this may be an issue in relation to "secure electronic records". We note that section 19(1) of the ETA provides for a presumption of the integrity of a secure electronic record, unless evidence to the contrary is adduced. For the party challenging the presumption, how would one prove that the signature was not secure "at the time it was made" because of intervening events such as hacking or a 51% attack situation or some other event? What is the remedy therein? The forensic enquiry for this exercise is still not yet to be subject to broadly accepted standards.

**C. Biometrics**

We note that the IMDA has concluded that biometrics technology is "unlikely to be understood as a secure electronic procedure" under the ETA as biometrics technology "by itself, does not typically allow for non-repudiation": see paragraphs 3.4.4 and 3.4.5 of the Consultation Paper.

From a legal perspective, given that biometrics technology is technically complex, we find no reason to disturb the technical conclusion reached by the IMDA, especially in relation to the finding that biometrics technology does not typically allow for non-repudiation. Nevertheless, we provide some preliminary comments as follows:

***Non-repudiation***

First, since the ETA does not contain the expression "*secure electronic procedure*", for the purposes of analysis herein we have assumed that the IMDA is inquiring whether biometrics ought to be included as a type of "specified security procedure" which, if applied to an electronic signature, results in such signature being verified as a "secure electronic signature" within the meaning of section 18 of the ETA for being: (a) unique to the person using it; (b) capable of identifying such person; (c) created in a manner or using a means under the sole control of the person using it; and (d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated.

Hence, the IMDA may wish to engage in technical consultation with security experts in the biometrics space to determine if there might be any technical basis to justify including biometrics as a "specified security procedure" under the ETA, e.g. by analysing the extent of non-repudiation that biometrics technology would able to offer, including whether (and to what extent) biometrics technology allows for accurate determination of whether an electronic "imprint" corresponds to the "imprinter".

***Integrity and authenticity of the record***

Second, apart from non-repudiation, we are of the view that electronic contracting also presents additional risks in relation to the *integrity and authenticity* of the electronic record. Therefore, the IMDA may wish to explore whether the use of biometrics (similar to the use of digital certificates) can assist to address the integrity of a record (i.e., whether it has been changed from the time of creation).

By way of comparison, under the current framework of the ETA, the use of a digital certificate associated with a particular credential may establish that the holder of that credential had digitally signed the relevant document, but this (at the highest) merely addresses the risk associated with non-repudiation (i.e., the party identified in the agreement denying that he was indeed the person who signed it) if that person's identity was verified against the certificate in question.

In this regard, we note that the only accepted "specified security procedure" under the ETA is currently a "digital signature", which in turn is defined in the Third Schedule of 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.

Therefore, a possible line of inquiry which the IMDA may wish consider exploring could be whether biometrics technology is to be accepted as having a degree of security (capable of establishing *integrity* of the record) that is analogous in strength and/or accuracy to the matching of private and public keys in an asymmetric cryptosystem.

**D. Conclusion**

Otherwise, we find no reason (barring future technological developments) to disturb the status quo that the ETA should, at the highest, facilitate biometrics to be deployed as a "supporting technology" for identification and/or authentication purposes.

In any event, even if biometrics technology will not be prescribed as a "specified security procedure" under the ETA, the ETA already provides a flexible mechanism (that is technology-agnostic) to determine whether a security procedure is "*commercially reasonable*" under section 17 of the ETA, by having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including: the nature of the transaction; the sophistication of the parties; the volume of similar transactions engaged in by either or all parties; the availability of alternatives offered to but rejected by any party; the cost of alternative procedures; and the procedures in general use for similar types of transactions. This view is premised on the assumption that biometrics technology will constitute a "security procedure" under the ETA in the first place.

**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.**

We have no comment on the potential technologies.

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

Generally, we are of the view that it ought not to be an issue to maintain the existing voluntary nature of the CA accreditation framework for Digital Signatures. But it may be worth looking into the actual process and to review the framework to take into account new technologies in the field. To date, there has been no alternative to the Public Key Infrastructure methodology in terms of identification and

authentication although other technologies are being used for identification such as biometrics, facial recognition etc. The voluntary nature of the CA accreditation should be maintained.

We note that paragraph 4.4.2 of the Consultation Paper refers to *"Capstone CTS Asia Pacific's study Report for Comparison Study of Audit Requirements for Certification Authorities prepared for IMDA".* We note this relates to the attached report which was issued in November 2007. If this is correct, then there should be efforts undertaken to ensure that the context and the frameworks are updated as 2007 as this was 12 years ago.

Notably, what has impaired our ability to truly assess the effectiveness of the voluntary framework has been availability of information in terms of the use cases / needs which are most popularly served by the accreditation framework – i.e. which organisations have benefited the most and in what way, whether the accreditation has assisted in addressing evidential challenges. Hence, if anything, we would submit that greater transparency as to the operation of the framework be provided so that a better understanding of the potential for application and its effectiveness can be further studied and promulgated.

**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.**

We agree with the proposed approach by IMDA to adopt the prevailing version of **either** WebTrust or ETSI's standards as the relevant standard for complying with CA accreditation requirements. This is because a single adopted standard is easier for implementation and compliance for market consistency although it may affect interoperability with countries that choose the other alternative. While a single standard can be preferred and adopted, the other standard should not be prohibited so as to allow companies to choose what the best way forward for them is.

We also agree that there should be a residual discretion to calibrate or refine the CA framework should this be necessary. Specifically, on this discretion, we respectfully submit that amendments to the ETA regulations set out further details on this discretion expressly including on when this discretion may be invoked, any criteria to be met for this discretion to be exercised and by whom this discretion can be exercised.

Clarity that any discretion is not an unfettered one is important as otherwise, there is a risk that calibration or refinement to the CA framework will unintentionally create non-compliance with WebTrust or ETSA standards.

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

No comments/feedback received on this question.

## APPENDIX A

### CONCLUSION

We are supportive of having a much reduced exclusion list in the First Schedule of the ETA or even completely removing the exclusion list. We have reservation on creating a requirement to use "secure electronic signatures" rather than an "electronic signature" to make certain high value contracts valid; we respectfully submit that the current statutory definition of a "secure electronic signature" is too amorphous for practical use.

We find no reason (barring future technological developments) to disturb the status quo that the ETA should, at the highest, facilitate biometrics to be deployed as a "supporting technology" for identification and/or authentication purposes.

In any event, even if biometrics technology will not be prescribed as a "specified security procedure" under the ETA, the ETA already provides a flexible mechanism (that is technology-agnostic) to determine whether a security procedure is "*commercially reasonable*" under section 17 of the ETA, by having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including: the nature of the transaction; the sophistication of the parties; the volume of similar transactions engaged in by either or all parties; the availability of alternatives offered to but rejected by any party; the cost of alternative procedures; and the procedures in general use for similar types of transactions. This view is premised on the assumption that biometrics technology will constitute a "security procedure" under the ETA in the first place.