Netrust Ptd Ltd
70 Bendemeer Road
#05-03, Luzerne
Singapore 339940

NETRUST
YOU CAN BE SURE

26th August 2019

Ms Aileen Chia
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

Dear Ms Chia,

**NETRUST'S RESPONSE TO CONSULTATION ON REVIEW OF THE ELECTRONIC TRANSCTIONS ACT (ETA)**

We are pleased to enclose Netrust's response on the stated review. We would not be responding to individual questions, but would provide comments for each Section.

Should you require any clarifications on this submission, please do not hesitate to contact me at email: jongai.foo@netrust.net or Tel: 62121368.

Yours Sincerely,

Digitally signed
by Jong Ai FOO
Date: 2019.08.26
21:40:12 +08'00'

FOO JONG AI
Chief Executive Officer

## NETRUST'S RESPONSE TO REVIEW OF THE ELECTRONIC TRANSACTIONS ACT (ETA)

### SECTION 2: FACILITATING INNOVATION AND DIGITALISATION OF BUSINESSES AND GOVERNMENT SERVICES

NETRUST'S COMMENTS:

Netrust supports the removal of the exclusion list as much as possible, and we agree that the concerns about 'vulnerable' persons must be addressed. Sufficient checks and balances must be in place for the protection of 'vulnerable' persons. For most of the situations, processes can be built in to require the signatures of a practicing lawyer and/ or an accredited medical professional, where relevant.

To protect against technological obsolescence, all digitalisation initiatives require conscious efforts in 'digital preservation'. This basic requirement is not just for the protection of the signatures but also to ensure the recoverability of the actual documents that may be stored/ archived in various formats.

For transactions that require long term preservation, it's important to dictate that secure electronic signatures or digital signatures are used. The PKI based digital signature technology is a proven technology that has widespread adoption all over the world. That's why it's important not to rush into new and unproven technologies.

### SECTION 3: FACILITATING NEW TECHNOLOGIES IN ELECTRONIC TRANSACTIONS

NETRUST'S COMMENTS:

Netrust shares the view that the ETA should remain technology neutral and focuses on functional equivalence. It is our understanding that any technologies introduced must satisfy the requirements for reliability and non-repudiation. The main legislation should remain technology neutral, while leaving the details on the CA Regulation to the ETR.

As stated in the ETA, to accept an electronic signature as "secure", parties 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. PKI meets the requirements stated above, and is one of the most secure authentication architectures that have the key attributes for supporting non-repudiation. Its standards are well defined and internationally recognised, and therefore can easily support cross-border applications. For the 20 over years of PKI adoption in Singapore, instead of technology obsolescence, PKI is increasingly adopted internationally in many other areas, including e-passport, travel credentials, etc.

For the other technologies mentioned in the consultation paper, the basic question to address is whether from the signed document, it is capable of identifying the person performing the signature and whether data integrity can be assured.

## SECTION 4: CERTIFICATION AUTHORITY FRAMEWORK

### NETRUST'S COMMENTS:

Netrust agrees that the existing voluntary nature of the accreditation framework for Certification Authority should be maintained.

On the audit framework, we are neutral to either maintaining the existing Checklist approach (Option a) or adopting the WebTrust and/ or ETSI standards (Option b) for compliance. It must be clear, however, that adopting Option b does not imply mandating getting actual WebTrust or ETSI certification. It should be sufficient to simply adopt the standard(s) as a part of the Singapore's CA audit framework.

If the decision is to adopt Option b, IMDA must dictate additional country specific requirements for compliance with the ETA and ETR, with stringent control over the requirements to ensure proper identity verification before certificate issuance. The internationally recognized WebTrust and ETSI standards for CA have their roots in ensuring compliance for browser trust, which is important for SSL certificates. The focus of the ETA and audit framework, however, is to ensure integrity of individual identity credentials issued for support of digital signatures.

If a choice is to be made between either WebTrust or ETSI, Netrust's preference is for WebTrust, as the WebTrust framework has included illustrative controls with each evaluation criterion to provide guidance to CAs and auditors on the types of controls that should be evaluated to achieve each criterion.