Response from UOB Centralised Credit Operations Division ("CCOD") on

JOINT IDA-AGC REVIEW OF ELECTRONIC TRANSACTIONS ACT
STAGE III: REMAINING ISSUES

In respect of the above-mentioned paper, our responses are made below. Please note that the responses below are not made on behalf of the whole bank, but in respect of UOB CCOD only.

Response to Q1: - it's a good move. Approach proposed therein is very similar to MAS's top down risk management framework of setting broad based supervisory parameters that institutions are expected to comply with. Choice is still left to the user of CAs. This will spur creativity from the respective CAs to establish the most effective solutions so long as it is within the security risk parameters set out by IDA.

Response to Q2: It's a good move - provided the standards for accreditation is high. What standards does the accreditation authority set. E.g., ISO 9000 standards are internationally recognized and they have a formalized structure on policy standards, level of operational compliance and audits before a candidate is ISO certified.

Response to Q5: Compliance with security guidelines should be one of the areas that the audit must comply with but scope should not be limited to this. Using Banking as an analogy, there are no statutory guidelines controlling type of loans that the bank books. But because loans account for more than 65% of its total assets, auditors do look at, other than compliance with statutory requirements e.g., unsecured lending, director/shareholder interested loans, issues relating to concentrations and loan quality as it affects credit and reputational "risk". Similarly whether the CA has a similar robust operations framework must be an area that must be within the scope of audit review.

Response to Q12: Given different levels of e-documentation savvyness of organizations in Singapore, and technological constraints e.g., converting existing hard copy security documents to "good" e-formats, a phased in or parallel approach would be preferred.

Response to Q15: It is normal banking procedure to accept customer's signature as identification as well as approval to terms of credit and/or mandate to bank to carry out specified transactions. Hence this provision may create some confusion on banking transactions.

Response to Q16: For operations security risk control, electronic signatures must satisfy prescribed reliability criteria to minimize if not prevent future allegations similar to handwritten signatures e.g., fraud. Similar IT security "safety" risk

issues must be addressed. The same reason why there is still low usage of internet banking…. is my pin safe?