M1'S RESPONSE TO IDA'S CONSULTATION PAPER ON THE ENACTMENT OF A LEGISLATIVE FRAMEWORK TO REGULATE AUTHENICATION OPERATORS IN SINGAPORE

19 September 2008

M1'S RESPONSE TO IDA'S CONSULTATION PAPER ON THE ENACTMENT OF A LEGISLATIVE FRAMEWORK TO REGULATE AUTHENTICATION OPERATORS IN SINGAPORE

1. M1 has been providing cellular mobile services to the Singapore market since 1 April 1997 and in 2000, we launched our international telephone services. In February 2005, M1 took the lead in introducing 3G technology and launching our 3G services. This was followed by the launch of our Mobile Broadband service in December 2006. In August 2008, M1 became a fully-fledged broadband player with the introduction of M1 Fixed Broadband service, transforming M1 from a single-play mobile operator to a dynamic multi-play operator with interests in the mobile and fixed sectors.

2. M1 welcomes the opportunity to submit our comments to IDA for its consideration on the enactment of a legislative framework to regulate Authentication Operators ("AOs") in Singapore. We view that the introduction of a regulatory regime for AOs in Singapore is timely and would ensure uniformity and provide adequate security in this nascent market for both a level playing field and industry stability.

3. We focus our comments primarily on the following issues:

a. Policy Objectives of Legislation to Regulate Authentication Operators

Question 1

Do you agree that there is a need to regulate AOs serving key economic sectors given the critical functionality that they provide in supporting online services from these sectors?

We support IDA's view that it is necessary to regulate AOs serving key economic sectors given the critical functionality that they provide in supporting online services from these sectors.

Question 2

Are the policy objectives of the proposed legislative approach to regulate AOs serving key economic sectors comprehensive and appropriate? Are there other policy objectives that IDA should consider for the proposed legislation?

The proposed regulatory regime should not focus only on existing AOs, but encompass all other regulatory aspects, including having policy objectives of legislation that beget regulatory mechanisms such as appropriate pre-requisites and criteria that operators must satisfy to qualify as an AO.

Question 3

Are there instruments other than legislation to better ensure that AOs comply with requirements including security, confidentiality, reliability, availability, service level standards, and financial stability so that their services are not unnecessarily disrupted?

With the Call-for-Collaboration for the National Authentication of Framework planned for 2008, the proposed legislation can be further reviewed to determine if it is adequate. However, M1 would like to emphasise the need for balance, as defining legislative requirements that are too stringent or introduction of extraneous regulatory instruments may impede efforts to promote growth in a nascent market.

b. Regulating Authentication Operators via Accreditation

Question 4

Do you agree that an accreditation scheme is an appropriate instrument that balances the need for regulatory oversight and the reduction of regulatory burden to regulate AOs and to promote growth in a nascent AO market?

A light-touch approach could encourage a proliferation of AOs in the market especially for AOs intending to provide services only to non-critical sectors. IDA should be mindful of potential issues such as:

- Having too many AOs in a small market like Singapore;
- Introduction of too many different authentication credential technologies resulting in complex interconnection procedures; and
- Short-lived AOs that eventually decide to discontinue their services.

Question 5

Are the considerations for an accreditation framework comprehensive and appropriate? Are there other considerations that IDA should include in the proposed accreditation scheme for AOs?

With reference to Para 4.2(b) of IDA's consultation paper, the accreditation framework will allow sector regulators to make individual assessments of the criticality of different online services. However, it would be likely that the implementation of the eventual accreditation framework would commence at different times by respective sector regulators. As such, M1 would recommend that IDA continually monitor to instil and maintain interest within each industry and more importantly, match the pace of technology.

c. Proposed Legislations for the Regulation of Authentication Operators

Question 6

Do you agree that in order to establish an accreditation scheme to regulate AOs, IDA should be given the legal powers to accredit AOs and to issue Codes of Practice and Standards of Performance? Do you agree with IDA's approach to develop Codes of Practice and Standards of Performance in consultation with regulators of key economic sectors so that they are not out of line with other sectoral requirements, but AOs may still need to comply with additional sector-specific rules and regulations if they wish to service SPs from sectors with these additional requirements?

IDA should have regulatory oversight and at the same time, align itself with the regulators of the various economic sectors to ensure consistency in the applicable Codes of Practice and Standards of Performance and not hinder the AOs from providing its services to more than one sector, if permitted.

Question 7

Do you agree with the policy intent to provide legal certainty to AOs by expressly stating the conditions for liability exclusion?

Yes.

Question 8

Is the proposed liability exclusion provision for AOs (Para 5.4) comprehensive and appropriate? Are there other cases to consider where it is clear that liability should be excluded for AOs?

AOs should not be liable in instances where they may have to change the authentication method as current technology becomes obsolete.

Question 9

Are the proposed penalties sufficient and appropriate for their corresponding contraventions?

Strong authentication services are vital, especially for key economic sectors, to protect customer data, transactions and other sensitive information. Hence, the proposed penalties should commensurate with the severity of the contravention. To align the penalties to similar existing penalty systems, we propose a maximum fine of $1 million[1] and imprisonment terms not exceeding 3 years [2, 3].

[1] Code of Practice for Competition in the Provision of Telecommunication Services 2005

Question 11

Should IDA also have the power to request for information from AOs, from time to time, if it considers it necessary in the public interest?

IDA should have the power to request for information from AOs for the purpose of discharging its functions.

Question 12

Do you agree that for consistency, relevant sections of ETA should be amended to allow IDA to be the single entity to regulate both CA and AO regimes?

We would recommend that the entity be comprised of IDA and at least one other representative from the sector regulators to regulate both CA and AO regimes.

d. Proposed Industry Best Practices for Compliance by Accredited Authentication Operators.

Question 18

Is the coverage of competition and interconnection requirements comprehensive and appropriate? Are the proposed competition and interconnection requirements comprehensive, appropriate and sufficient to promote fair market conduct? If not, please describe additional requirements that IDA should consider.

There will be a need to further define and refine the requirements pertaining to competition and interconnection, especially with the proposed light-touch approach for accreditation framework. Specifically, seamless migration between AOs, particularly in the case where authentication credentials may differ, will need to be addressed.

Question 19

Is there a need to prescribe a competition code, which could include price regulation, so as to prevent anti-competitive behaviours? If so, should the competition code be prescribed from the onset, so as to achieve legal certainty in the accreditation scheme?

In line with the proposed light touch regulatory approach, IDA should preferably allow market forces to act as the self-regulating mechanism.

---

[2] Telecommunications Act (Chapter 323)
[3] Banking Act (Chapter 19)

Question 20

Is interconnection an appropriate accreditation requirement to establish a competitive market and achieve a consistent strong authentication experience for end-users? Are there alternatives that can achieve the same objectives without the need for interconnection?

Interconnection is an appropriate accreditation requirement. However, interconnection should not be mandated but rather based on mutual agreement among AOs. To ensure business viability, interconnection costs should also be kept to the minimum.

Question 22

Are the proposed disclosure and liability requirements comprehensive appropriate and sufficient to protect the interests of end-users, SPs and AOs? If not, please describe additional requirements that IDA should consider.

M1 views that the proposed disclosure and liability requirements are adequate to protect the interests of end-users.

Question 24

Are the proposed credentials lifecycle management requirements comprehensive, appropriate and sufficient to provide assurance of credential strength? If not, please describe additional requirements that IDA should consider.

We agree that the proposed credentials lifecycle management requirements adequately provide assurance of credential strength.

Question 25

Do you agree that AOs shall be responsible and accountable for credential lifecycle management?

M1 supports IDA's view that it should be the responsibility of the AO to manage and streamline the credential lifecycle management.

Question 29

Are there alternatives to better ensure that authentication services are not unreasonably interrupted should an AO decide to discontinue operations? Should IDA have step-in right to take over the operation of an AO in order to ensure that availability of AO services?

Given the relatively small market size, a possible alternative is for IDA to limit the total number of AOs based on the size of each economic sector and to establish guidelines and conditions for AOs who wish to offer their services across different economic sectors. This will ensure sustainability of AO services within each industry.