ENACTMENT OF A LEGISLATIVE FRAMEWORK TO REGULATE AUTHENTICATION OPERATORS IN SINGAPORE (CONSULTATION PAPER)

POLICY OBJECTIVES OF LEGISLATION TO REGULATE AUTHENTICATION OPERATORS

Q1. 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?

<RESPONSE> AOs play a critical role in the management of accesses to specific resources/services/privileges. There is a need for full accountability to the different stakeholders; be it end-users or downstream service providers. To do this, it is necessary to have regulations that are firm, transparent and enforceable and should take into account the relevant regulatory/legal requirements.

Q2. 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?

<RESPONSE> This question implies that AO will only serve key economic sectors. The principles expounded should extend to all recipients of the service. While there is a liability exclusion clause for the AO, it is silent on the SPs and end-users. By virtue of the service provided, all stakeholders that rely on the AO should have a right of recourse. Having liability exclusion may not give confidence to these parties.

Paragraph 5.5 proposes aggrieved parties to appeal to the minister. To have segregation of duties and avoid conflict of interest, it is more appropriate for an independent party/group to accredit AOs rather than IDA. In this case, there is no need to appeal to the minister.

Q3. 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?

<RESPONSE> Legislation is one means. However, what is important is the contractual/moral obligations of the AO to its customers. Expectations need to be transparent and spelled out clearly. There should also be avenues for mediation for grey areas.

Q4. 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?

<RESPONSE> No. Accreditation means that the AOs are certified to deliver a service of a specific quality. For authentication, there cannot be any compromise to the service nor quality of service provided.

Further, a one-time accreditation is not enough. Periodic review and assessment are needed to ensure the AO has maintained the minimum required standards.

Q5. 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?

<RESPONSE> As the authority specifying the policies, standards and framework for this proposal, would it not be more transparent if another independent body be made responsible for accrediting the AOs?

From the service recipient standpoint, the accreditation body also has a responsibility for the quality of the accreditation process. There is nothing mention about the liability of the accreditation body.

There is also a need to monitor and, if needed, refine the processes adopted by the accreditation body. The critical success factor/baseline requirements for the accreditation body should also be defined.

Exclusion of Liability for Accredited AOs

Q6. 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?

<RESPONSE> See answer to Q5 above. What exactly does IDA mean by development of the code of practice and standards of performance in consultation with regulators?

If the AOs are certified based on codes and standards that are specified by all the relevant authorities (e.g. IDA, MAS), why can't it be all encompassing so that there is less reference to other requirements? Too much cross reference may result in things falling through the gap.

Currently, banks have to perform due diligence of outsourced service providers. With accreditation, is this still necessary? If this is yes, then what is the purpose of accreditation?

Q7. Do you agree with the policy intent to provide legal certainty to AOs by expressly stating the conditions for liability exclusion?

<RESPONSE> The conditions and amounts need to be transparent, reasonable and based on absolute risks. Also, would the accreditation body have similar responsibilities? (See response to Q5 above.)

Q8. 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?

<RESPONSE> What exactly is meant by "reasonable means of detection" and "reasonable control". These terms are too generic and does not provide assurance to the users of the services provided. As most end-users may not be savvy about such "contractual rights", they will end up losing confidence in the system. Further, there is the concern of whether the service providers (eg banks) will end up being the party that the end user seek recourse from.

Regulatory Enforcement Powers

Q9. Are the proposed penalties sufficient and appropriate for their corresponding contraventions?

<RESPONSE> The sum should be the minimum and not maximum.

Monetary punishment may not resolve the issue.

There is also no mentioned of compensation to end-users or SPs.

General Powers

Q10. Are the proposed general powers to be accorded to IDA (Para.5.7) comprehensive and appropriate for the implementation of the AO regulatory regime?

<RESPONSE> As the policy maker, it is more appropriate for an independent party to be responsible for the execution such as accreditation.

Q11. 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?

<RESPONSE> IDA need to abide by other statutes and laws governing the case(s). How can IDA assure the public that there will not be any "abuse" of privileges?

Proposed Amendments to ETA

Q12. 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?

<RESPONSE> It is more appropriate for another party to execute the policies established/proposed by IDA.

The amendment should be based on roles and responsibilities, and not on consistency.

Security Requirements

Q13. Are the proposed security requirements comprehensive, appropriate and sufficient to address the security risks posed by hackers and other forms of malicious attacks on or through the authentication infrastructure provided by the AO? If not, please describe additional security requirements that IDA should consider.

<RESPONSE> The principles proposed sounds logical but some of these need further refinement/clarity for easier implementation and avoiding confusion. For example:

a. what is deemed appropriate (see Annex A paragraph 1)?
b. what is meant by periodically?
c. what is considered sensitive data?

Some requirements may not be comprehensive or are contradictory:

a. timeout and automatic logout for non-active sessions for all administrative accesses only? Should it not be for all accesses? (see 2.3.3.3)
b. 2.3.2.12 contradicts 2.3.2.22.

Suggest that the details be reviewed again to ensure comprehensiveness, clarity, operability/implementability and auditability.

Q14. Is it appropriate to require AOs to be ISO/IEC 27001 certified? Do you agree that AOs shall use international and established standards as described in Annex A, including standards for authentication mechanisms, authentication protocols, encryption, and digital signing? If not, how else can security assurance be achieved?

<RESPONSE> Does being ISO certified mean that security assurance is achieved? Case histories have shown that this may not be the case.

Q15. Can the proposed security requirements be further streamlined to facilitate AO's compliance without compromising the security of the authentication infrastructure?

<RESPONSE> No comments.

Business Requirements – Confidentiality

Q16. Are the proposed confidentiality requirements comprehensive, appropriate and sufficient for the protection of sensitive information? If not, please describe additional requirements that IDA should consider.

<RESPONSE> It is necessary to determine what is sensitive. It is also necessary to consider encrypting backup media stored onsite.

It should be noted that the notion of sufficiency depends on the industry. In banking, these security requirements may not able to cover the data confidentiality.

Also, there is no mention about segregation of customer types, system administrators cannot access the database, etc.

Note: System administrators are not regarded as authorized personnel to customer data.

Q17. Can the proposed confidentiality requirements be further streamlined to facilitate AO's compliance without compromising the protection of sensitive information?

<RESPONSE> No comment.

Business Requirements – Competition and Interconnection

Q18. 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.

<RESPONSE> The principle and objective is reasonable. However, a chain is only as strong as its weakest link. The criteria for interconnection should be established; especially if AOs have different security levels and serves different sectors.

Q19. Is there a need to prescribe a competition code, which could include price regulation, so as to prevent anti-competitive behaviors? If so, should the competition code be prescribed from the onset, so as to achieve legal certainty in the accreditation scheme?

<RESPONSE> If the market is truly competitive, would pricing matters not be automatically taken care of by market forces? There is the danger that price fixing may stifle innovation.

Q20. 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?

<RESPONSE> The answer depends on the objective of the accreditation. If it is certifying that the AO has met minimum requirements for controls, then interconnection is not appropriate.

Q21. Can the proposed competition and interconnection requirements be further

streamlined to facilitate AO's compliance without compromising the inhibition of unfair market conduct and the availability of a consistent strong authentication experience for end-users?

<RESPONSE> No comments.

Business Requirements – Disclosure & Liability

Q22. 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.

<REPONSE> Okay. However, would the accreditation body be liable too?

Q23. Can the disclosure and liability standards be further streamlined without compromising the protection of interests of the respective stakeholders?

<RESPONSE> No comments.

Operational Requirements – Credential Lifecycle Management

Q24. Are the proposed credential lifecycle management requirements comprehensive, appropriate and sufficient to provide assurance of credential strength? If not, please describe additional requirements that IDA should consider.

<RESPONSE> If not managed well, this can create reputation risk for the SPs and may also result in losses for end-users and SPs. SLAs for credential management should be established.

Q25. Do you agree that AOs shall be responsible and accountable for credential lifecycle management?

<RESPONSE> AOs will operate. However, an independent body should specify the standards required.

Q26. Can the requirements on credential lifecycle management be further streamlined to facilitate AO's compliance without compromising the strength of the credential?

<RESPONSE> See Q24 above.

Operational Requirements – Continuity of Authentication Services

Q27. Are the proposed requirements to achieve continuity of authentication services comprehensive, appropriate and sufficient to minimise the impact of system failures and disasters on the provision of authentication services? If not, please describe additional requirements that IDA should consider.

<RESPONSE> The principles expounded appears reasonable. However, as this is an authentication service, SLAs must be established and adhered to strictly.

Para 4.7.2.1 allows activation of DR plans after two hours of downtime. This is not appropriate for an authentication service.

Q28. Can the requirements for ensuring the continuity of authentication service be further streamlined to facilitate AO's compliance?

<RESPONSE> Having a 99.5% availability translates into two days of downtime per year. This cannot be acceptable.

Further, under paragraph 4.7.2.2, there is a requirement for BIA to be performed. However, there is no checks to ensure appropriate measures are implemented.

Q29. 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 the availability of AO services?

<RESPONSE> To preserve its objectivity and independence, IDA should appoint a caretaker to run the AO.

Other Operational Requirements

Q30. Are the proposed best practices comprehensive, appropriate and sufficient to ensure the proper functioning of AOs and enforceability of service quality? If not, please describe additional requirements that IDA should consider.

<RESPONSE> No comment.

Q31. With reference to 6.8(b), in addition to informing IDA on changes to management staff, do you agree that an AO must seek IDA's approval before a significant change in its shareholding takes place?

<RESPONSE> IDA should be informed of significant changes. However, is it necessary to seek approval? For example, if someone wants to resign, must IDA approve?

Q32. Are there any requirements in these sections that can be further streamlined without compromising the proper functioning of AOs and enforceability of service quality?

<RESPONSE> No comments.

Any Other Comments

Q33. Do you have any other inputs, comments or suggestions on any aspects of the proposed policy positions and industry best practices that have not been covered in your responses to the questions above?

<RESPONSE> An independent party should be responsible for accreditation of AOs and not IDA. Further, the accreditation body should be accountable if there is negligence/oversight in accrediting AOs.

The accreditation body should be independent and objective from a management and technical perspective and at the same time ensure strict adherence to the standards stipulated by the authorities. It should also be responsive to the security needs of the industry as well as standards stipulated by the authority. It must be sufficiently flexible to enable new priorities and demands to be addressed.