Questions and Responses

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?

A1. **Yes**

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?

A2. **For fair competition between AOs, there should be policy to ensure that existing service provider of UserId and Password authentication service cannot leverage on existing consumer base for the NAF initiative.**

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?

A3. **No.**

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?

A4. **With voluntary accreditation, potential AOs can enter and exit at will. Then the remaining AOs will have problems taking over the service and offer the same low pricing to SP. We will prefer a licensing or mandatory accreditation model as there is huge upfront investment for the accredited AO to maintain a high service level. Potential AO will make serious consideration before offering the service.**

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?

A5. **As above.**

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?

A6. **IDA can be given legal powers but Codes of Practice must be drafted with consultation with existing AOs. Otherwise, AOs which have already operated in a specific sector may be forced to exit and abandon their SPs.**

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

A7. **Yes**

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?

A8. **There should be provision against acts of God.**

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

A9. **The penalties should be restricted to fines.**

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?

A10. **With such powers given to IDA, AOs will need to factor in increased running business costs for compliance. Such measures may also stifle creative business growth.**

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?

A11. **There should be clear scenarios that IDA can request information from the AO.**

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?

A12. **No preference.**

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.

A13. **It is sufficient.**

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?

A14. **The AO can comply with the security requirements in section 2 without compliance to ISO/IEC 27001. IDA can perform the audit on the AO on a periodic basis. Then there is no need to reference to two separate overlapping sets of requirements (which will have impact on costs and pricing)**

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

A15. **It is appropriate.**

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.

A16. **It is sufficient.**

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

A17. **It is appropriate.**

Q18. Is the coverage of competition and interconnection requirements omprehensive 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.

A18. **If IDA require AO to make available reference interconnection offers to be approved by the Authority, it should take in considerations of sunken and operational costs of the AO in attempt to grow the 2FA adoption.**

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?

A19. **If IDA choose to include price regulation, then the price range should be make known upfront for the potential AO to facilitate more accurate assessment of commercial viability.**

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?

A20. **It is sufficient.**

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?

A21. **It is appropriate.**

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.

A22. **It is sufficient.**

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

A23. **It is appropriate.**

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.

A24. **It is sufficient.**

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

A25. **Yes**

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

A26. **It is appropriate.**

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.

A27. **It is sufficient.**

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

A28. **It is appropriate.**

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?

A29. **It is appropriate.**

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.

A30. **It is sufficient.**

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?

A31. **It would be more relevant for AO which has some foreign ownership or interest, or the intention to include any foreign interest into its shareholders, to seek IDA's approval for any change on its shareholdings, in the interest of national security. This may not be necessary for AOs who are wholly owned by local shareholders.**

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?

A32. **It is appropriate.**

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?

A33. **No.**