ENACTMENT OF A LEGISLATIVE FRAMEWORK TO REGULATE AUTHENTICATION OPERATORS IN SINGAPORE

(Consultation Paper)

29 August 2008

ENACTMENT OF A LEGISLATIVE FRAMEWORK TO REGULATE AUTHENTICATION OPERATORS IN SINGAPORE

CONTENTS

IDA CONSULTATION PAPER

ENACTMENT OF A LEGISLATIVE FRAMEWORK TO REGULATE AUTHENTICATION OPERATORS IN SINGAPORE

EXECUTIVE SUMMARY

The need to regulate authentication operators ("AOs"), who are entities that provide third-party strong authentication services, stems from the fact that AOs perform functions that are integral to online service providers ("SPs"). When an SP outsources its strong authentication function to an AO, it relies on the AO to help validate the identities of its customers. However, disruption to AO services will adversely impact the identity validation process, rendering online services potentially inaccessible to the end-users. This is an outcome that SPs from key economic sectors (e.g. banking and finance, government and healthcare) can ill-afford. It is thus proposed that a regulatory regime for AOs is needed to ensure that they meet essential requirements including security, confidentiality, reliability, availability, service level standards and financial stability.

2 This Consultation Paper seeks feedback on the proposed legislative framework to implement a regulatory regime for the AOs. Specifically, feedback on the following issues is sought from members of the public:

(a) Policy objectives of legislation to regulate authentication operators;

(b) Regulating authentication operators via accreditation;

(c) Proposed legislation for the regulation of authentication operators; and

(d) Proposed industry best practices for compliance by authentication operators.

Policy objectives of legislation to regulate authentication operators

3 Besides being an instrument to implement a regulatory regime to safeguard the availability of strong authentication services for key economic sectors, legislation is also aimed at protecting the interests of the various stakeholders through the introduction of clear guidelines to provide certainty and predictability in how issues are to be managed. Moreover, legislation is poised at fostering a competitive market for strong authentication services, through the promotion of fair competition and interconnection requirements.

Regulating authentication operators via accreditation

4 Accreditation is proposed as the mechanism to regulate AOs as this light-touch approach provides a balance between the need for regulatory oversight and the reduction of regulatory burden in order to promote growth in this nascent market. An accreditation regime also allows sector regulators to assess the criticality of different online services within their sectors, so that any requirements to use accredited AOs

will be appropriately targeted. A light touch approach can also promote greater participation of potential AOs, thereby facilitating a competitive market for third-party strong authentication services.

Proposed legislation for the regulation of authentication operators

5 Corresponding provisions are proposed to implement an accreditation scheme. These include powers for IDA to accredit AOs, issue codes of practices and standards of performance and other associated administrative powers. The provisions also include liability exclusions for AOs, appeal to Minister against IDA's decisions, etc. Some amendments to the Electronic Transactions Act ("ETA") are also proposed, so that the regulatory scheme for Certificate Authorities ("CAs") can be consistent with the proposed scheme for AOs.

Proposed industry best practices for compliance by authentication operators

6 To ensure that AOs perform their functions in a proper manner, industry best practices are also proposed for AO's compliance. These include various security, business and operational requirements as detailed in Annex A.

IDA CONSULTATION PAPER

ENACTMENT OF A LEGISLATIVE FRAMEWORK TO REGULATE AUTHENTICATION OPERATORS IN SINGAPORE

PART 1
INTRODUCTION

1.1 Authentication is the process of establishing or confirming a person's identity for security purposes. For end-users to access an online service, the provider for the online service normally requires the end-users to key in their UserIDs and Passwords before access to the service is granted. This is commonly known as the single-factor authentication. End-users provide something they know (in this case, UserIDs and Passwords) as a proof of their identities, or a factor of authentication.

1.2 However, UserIDs and Passwords alone are no longer sufficient to protect consumers against identity theft today. For added rigour and assurance in proving the identities of their customers, many online service providers have implemented their own strong authentication systems. The process of strong authentication normally requires end-users to provide, in addition to something they know (e.g. UserIDs and Passwords), something they have (e.g. one-time passwords generated by a hardware token or sent to their mobile phones) as a second factor of authentication. The use of two or more factors of authentication is known as strong authentication.

1.3 Along with an increasing demand for strong authentication, there now exists a potential business opportunity for vendors to provide third-party strong authentication services to online service providers wishing to outsource such operations. The provider of this third-party strong authentication service is known as the Authentication Operator ("AO"). However, if the AOs who perform strong authentication functions for online Service Providers ("SPs") from key economic sectors (e.g. government, banking and finance, healthcare) become unavailable, end-users may lose access to these key online services. To ensure that the AOs meet essential requirements including security, confidentiality, reliability, availability, service level standards and financial stability, a regulatory regime for the AOs may be required. This Consultation Paper thus highlights the main features of the proposed legislative framework for this regulatory regime.

1.4 Part 2 of this paper describes an overview of the authentication landscape in Singapore, which points towards the case for third party strong authentication services. Part 3 discusses the need to regulate these third parties, as well as the policy objectives of legislation. In Part 4, accreditation is argued as an appropriate regulatory instrument. Parts 5 and 6 then respectively describe the proposed legislative provisions and industry best practices to implement this accreditation scheme. The details of the proposed industry best practices are listed in Annex A.

1.5 We invite comments and feedback on the proposed legislative framework. A compiled list of questions can be found in Annex B.

- Please send your feedback to the Infocomm Security & Trust Division of IDA via email to **IDA_AO_Consult@ida.gov.sg**, with **"Re: Public Consultation on AO Framework"** in the subject header. In addition, you may also submit a hard copy by post to "**Infocomm Security & Trust Division, Infocomm Development Authority of Singapore, 8 Temasek Boulevard, #14-00 Suntec Tower Three, Singapore 038988**", indicating **"Re: Public Consultation on AO Framework"** on the envelope.

  Please include your personal / company particulars as well as your correspondence address, contact number and email address in your response.

  IDA reserves the right to discount or make public all or parts of any responses to this consultation (including your name and your personal / company particulars). Your response may also be quoted or referred to in subsequent publications or made available to third parties. Any part of the response which is considered confidential must be clearly marked and placed as an annex to the comments raised.

- The closing date for this consultation is **2359 Hrs, 21 September 2008**.

PART 2
OVERVIEW OF THE AUTHENTICATION LANDSCAPE IN SINGAPORE

2.1 The pervasive use of infocomm technologies has seen the availability of mainstream consumer services such as government services, banking services and retail shopping on the Internet. To ensure that a transaction is performed by an authorised person, a service provider will require the person who requests to effect a transaction to prove his identity. Currently, most online service providers accept UserID and Password as the only proof of identity. However, online identity is subject to cyber attacks such as identity theft. Common methods of identity theft include Trojan programmes which log keystrokes to steal passwords and credit card numbers, as well as the use of password cracker programmes which can be readily obtained from the Internet. Identity theft may result in unauthorised release of sensitive information, financial losses, loss in consumer confidence and business reputation, and in worse cases, harm to enterprise systems, personal safety, as well as civil and criminal violations.

2.2 As the current implementation of UserID and Password is insufficient to protect consumers' online identities, many online service providers have independently turned to strong authentication for added rigour and assurance in proving the identities of their customers. The banking and finance industry has taken the lead in implementing strong authentication in compliance with the two-factor authentication directive for online banking issued by the Monetary Authority of Singapore (MAS).

2.3 However, the current implementation of strong authentication sees independent deployments that result in market fragmentation, leading to duplication of costs and efforts. With more service providers turning to strong authentication, the cost and effort duplication will be proportionately exacerbated. The inconvenience of having to learn to use and manage different authentication devices such as tokens and smart cards, can also lead to consumer reluctance in accessing online services. In view of the duplication of costs and efforts, as well as the increased inconvenience for the customer, there is potential business case for online service providers to outsource the implementation and operation of strong authentication function to independent third parties (i.e. AOs).

2.4 Even though strong authentication operations can be outsourced to AOs, it will remain integral to the online services that leverage on it. This is because the identity verification process will not be complete if the second-factor credential cannot be validated in the event of a service disruption at the AO. This may result in end-users losing access to their online services. To mitigate this risk and ensure the proper functioning of AOs, a regulatory regime for AOs is required.

2.5 Due to the market size of Singapore, the number of AOs is expected to be small. This presents an additional need for regulation, in order to mitigate the risks of anti-competitive behaviour and to promote competition. This

Consultation Paper thus highlights the main features of the proposed legislative framework for the regulation of AOs.

PART 3
POLICY OBJECTIVES OF LEGISLATION TO REGULATE AUTHENTICATION OPERATORS

3.1 The footprint of strong authentication services provided by AOs is expected to be significant, especially in key economic sectors such as Banking and Finance, Government and Healthcare, where the financial and reputation impacts of security breaches can be ill-afforded. We envisage that Service Providers that could leverage on AO services potentially include financial institutions in compliance with Monetary Authority of Singapore's Two-Factor Authentication directives, Government initiatives such as Standard Operating Environment (about 60,000 users) and SingPass (about 3 million users). We also envision that institutions in the healthcare sector that provide online services which access sensitive and/or confidential patient information could also leverage on AO services. The impact of a disruption in AO services that results in end-users losing access to such online services can be severe.

3.2 Public confidence in using online services and strong authentication will also be undermined if AOs do not adequately protect the confidentiality of sensitive personal and corporate information used in the provisioning of strong authentication service. Moreover, in the green field market of third-party strong authentication services, there is a need for clarity in the roles and responsibilities and associated liabilities of various stakeholders, namely, AOs, SPs and end-users.

3.3 To ensure that AOs meet essential requirements including security, confidentiality, reliability, availability, service level standards and financial stability, and to introduce legal certainty and predictability in this emerging industry, it is envisaged that a regulatory regime for AOs is necessary. Furthermore, IDA intends to conduct a Call-for-Collaboration for the National Authentication Framework (NAF) in 2008, to catalyse the industry deployment of AOs that can cater to demand for strong authentication, including those from the financial and government sectors. This gives rise to additional impetus to regulate AOs.

3.4 Having considered options such as guidelines and self-regulation, IDA has assessed that a regulatory regime, backed by legislation, is needed to achieve the following policy objectives:

(a) **To safeguard the availability of strong authentication services for key economic sectors** – For AOs providing strong authentication services to Service Providers ("SPs") in key economic sectors (e.g. banking and finance, government and healthcare), a disruption of AO service will have significant impact on the proper functioning of these online services. The financial and reputation impacts that can result from security breaches or other systemic failures in AOs are risks that need to be properly managed. As such, regulatory mechanisms are needed to ensure that such AOs can be required to comply with minimum requirements including the security, confidentiality, reliability, availability, service level standards, and financial stability.

(b) **To protect the interests of end-users, SPs and AOs** – Legislation will be required to protect parties that rely on AO services, such as SPs and end users. This includes areas such as protection of confidentiality of sensitive information, ensuring appropriate disclosure of risks and potential liabilities to both SPs and end-users, and requiring AOs to prepare a liability framework with dispute resolution procedures to introduce legal certainty. Liability exclusions offer legal protection for AOs. The presence of transparent guidelines on how liabilities and disputes are handled will boost consumer confidence and encourage participation by AOs and SPs, leading to industry vibrancy and the growth of high-value online services.

(c) **To ensure a competitive market for strong authentication services for key economic sectors** – It is anticipated that the number of AOs providing services to SPs in key economic sectors will be small. In order to mitigate the risk of anti-competitive behaviour, AOs will need to be regulated to promote fair market competition. Competition in turn will stimulate innovation to benefit SPs and end-users. In addition, a requirement for AOs to interconnect with one another (i.e. other AOs) will allow easier migration by SPs and end-users. By 'interconnection', IDA refers to an arrangement through which any AO will be able to service an authentication request for a credential that is issued by another AO (e.g. by forwarding the authentication request to the issuer). Hence SPs need only to subscribe to a single AO, who will either validate a credential if it is the issuer of that credential, or forward it to the AO that issued the credential for validation. SPs will not need to subscribe to multiple AOs in order to accept different credentials issued by different AOs. For the end-user, this would also mean that s/he will be able to use a single credential to access all services leveraging on these AOs, regardless of which AO issues that credential.

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?
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?
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?

PART 4
REGULATING AUTHENTICATION OPERATORS VIA ACCREDITATION

4.1 The approach in regulating AOs has to find a balance between the need for regulatory oversight and the reduction of regulatory burden in order to promote growth in the nascent market for third-party authentication services. Thus, the legislative framework IDA proposes is an accreditation framework, developed in consultation with regulators of key economic sectors, in which AOs wishing to serve SPs from these sectors can voluntarily subject themselves to comply with stipulated accreditation requirements and seek endorsement (i.e. accreditation) under the legislation as a mark of their competence and standards of operation. This is akin to the current voluntary licensing scheme for Certificate Authorities (CAs).

4.2 The considerations for an accreditation framework are as follows:

(a) An accreditation framework is light-touch compared to a mandatory licensing scheme, in which AOs will not be able to legally operate without a license. A light-touch approach will not unnecessarily curtail AOs that may wish to provide their services to only non-critical sectors or to small pockets of demand. As the consequences of failure of such AOs may be less significant, they may not need to be held to the same high standards of operations expected of AOs serving key economic sectors. Moreover, currently, there is no legislation that outlaws any organisation wishing to provide AO services today.

(b) An accreditation framework will allow sector regulators (e.g. MAS, MOH, MOF) to make individual assessments of the criticality of different online services within their sector, so that any requirement to use accredited AOs will be appropriately targeted. This will also enable AOs wishing to provide a level of assurance to their customers to voluntary apply for accreditation.

(c) Given the nascent nature of the market for third-party strong authentication services, a light-touch approach through accreditation will also promote greater participation by potential AOs, thus facilitating a competitive market for strong authentication services.

4.3 However, should the market evolves to a state where third-party authentication service becomes an essential resource in the same class of water, electricity and basic telephony, and a dominant AO is offering this essential service, IDA reserves the right to impose additional regulations, including price regulations, to protect the interests of SPs and end users.

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?

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?

PART 5
PROPOSED LEGISLATIONS FOR THE REGULATION OF AUTHENTICATION OPERATORS

Powers of Accreditation

5.1 To establish an accreditation scheme for AOs, there will be a need to provide for legal powers to enable IDA to accredit AOs that have met stipulated requirements and having necessary processes for handling discontinuation of operations. These provisions would also include the power to impose conditions of accreditation that accredited AOs must comply with and the power to modify such accreditation criteria.

Powers to issue Codes of Practices and Standards of Performance for AO's Compliance

5.2 IDA will also need legal powers to enable it to publish codes of practices and standards of performance that contain technical and operational details for compliance by accredited AOs. Acknowledging that technological development may outpace timeframes needed to enact changes in the regulatory regime, having the power to formulate and enforce such codes of practices and standards of performance will allow the regime to better match the pace of technology. The codes of practice and standards of performance will be developed in consultation with regulators of key economic sectors to ensure that they are not out of line with other sectoral requirements. However, 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.

5.3 The codes of practice and standards of performance will cover major areas including but not limited to:

(a) Security requirements;
(b) Confidentiality;
(c) Competition and interconnection;
(d) Disclosure and liability;
(e) Operational requirements;
(f) Business continuity management and service level standards;
(g) Discontinuation of operations of AOs.

Exclusion of Liability for Accredited AOs

5.4 Liability exclusions offer legal protection to accredited AOs as a result of their accreditation. IDA proposes that accredited AOs not be liable for cases where:

(a) forged credentials are used that are beyond AO's reasonable means of detection;
(b) end-users failing to adequately safeguard their credentials; and
(c) any delays or prevention of access of online services due to the AOs not receiving the authentication request,

provided that it is beyond the AO's reasonable control, and that the AO has complied with all legislative and accreditation requirements. Through the reduction of business uncertainties, liability exclusions may decrease costs of operations and encourage participation from AOs, thereby fostering a competitive market for strong authentication services.

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

Appeal to Minister

5.5 IDA proposes to include provisions to offer avenues for accredited AOs and other parties who feel aggrieved by IDA's decisions or directions (e.g. AOs who are refused accreditation) to appeal to the Minister.

Regulatory Enforcement Powers

5.6 In the event where an AO contravenes IDA's conditions of accreditation, codes of practice, standards of performance, etc., powers are sought for IDA to impose penalties or take other appropriate action to ensure compliance such as by suspending or cancelling the AO's accreditation. The following table describes the proposed regulatory enforcement powers, with corresponding penalties referenced from relevant frameworks such as the one for Certificate Authorities under the ETA.

Contraventions	Penalties
Contraventions of conditions of accreditation, codes of practice, or standards of performance	Fines up to $50,000.
Non-compliance with directions	Fines up to $50,000 and imprisonment up to 12 months.
Obstruction of IDA's access to computer systems in connection to offences	Fines up to $50,000 and imprisonment up to 12 months.

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

General Powers

5.7 To support the accreditation scheme for AOs, IDA proposes that the following legal provisions be provided as implementing powers of the regulatory regime.

General power required	Description
IDA may give directions for compliance	To empower IDA to direct an AO to take steps to ensure compliance with legislation.
Power to require information	To empower IDA to require information from AOs, from time to time, if necessary in the public interest.
Power to investigate	To empower IDA to investigate the activities of an AO in relation to its compliance with legislation.
Access to computers and data	To empower IDA to access and use any computer system which it has reasonable cause to suspect has been used in connection with an offence committed.
Obstruction of IDA	To render any person who obstructs, impedes, assaults or interferes with IDA guilty of a criminal offence.
Production of documents, data, etc	To empower IDA to require the production of records and documents from AOs or any person, and make inquiries as a precursor to investigations.
Composition of offences	To empower IDA to compound offences and issue regulations to prescribe which offences are compoundable.

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?
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?

Proposed Amendments to ETA

5.8 Currently, Certificate Authorities (CAs) are regulated by Director-General (Telecoms) of IDA, who is appointed as the Controller of Certificate Authorities (CCA) under the ETA. For consistency with the proposed regulation regime for AOs, IDA proposes that the ETA be amended to confer the powers to regulate CA directly on IDA. The proposed amendments of relevant sections of the ETA are as follows:

Section No.	Content	Amendments required
41	Appointment of	To provide for IDA (instead of the Controller) to

	Controller and other offices	accredit and regulate CAs.
42	Regulation of CAs	To empower IDA (instead of the Minister) to issue Regulations to regulate CAs.
43	Recognition of foreign CAs	To empower IDA (instead of the Minister) to issue Regulations to recognise foreign CAs.
46	Regulation of repositories	To empower IDA (instead of the Minister) to issue Regulations to regulate repositories.
50	Authorised officer	To delete this provision as it is no longer required.
51	Controller may give directions for compliance	To amend this section to empower IDA (instead of the Controller) to give directions.
52	Power to investigate	To amend this section to empower IDA (instead of the Controller) to conduct investigations.
53	Access to computers and data	To amend this section to empower IDA (instead of the Controller) to have access to computers and data.
54	Obstruction of Controller or authorised officer	To amend this section to refer to the obstruction of an officer of IDA (instead of the Controller).
55	Production of documents, data, etc	To amend this section to empower IDA (instead of the Controller) to have access to documents, data, etc.
59	Composition of offences	To amend this section to empower IDA (instead of the Controller) to compound offences and also to empower IDA (instead of the Minister) to issue regulations to prescribe which offences are compoundable.

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?

PART 6
PROPOSED INDUSTRY BEST PRACTICES FOR COMPLIANCE BY ACCREDITED AUTHENTICATION OPERATORS

6.1 As mentioned in Part 5, codes of practices and standards of performance will help allow the regulatory regime to keep up with technological development and advancement. The scope of these industry best practices cover the following (please see Annex A for details on IDA's initial positions regarding these best practices):

Security Requirements

6.2 To ensure that mechanisms are put in place to mitigate the risk of hackers and other forms of malicious attacks on or through the authentication infrastructure provided by the AOs, AOs will be required to adhere to security standards that will be published by IDA. With reference to Section 2 of Annex A, these include:

(a) Risk management standards, to ensure risks to the security of the authentication infrastructure can be adequately identified, assessed and mitigated.

(b) Information security management standards, to ensure that policies and processes are present to manage information security within the AO. This includes human resource controls to manage employees, physical security controls to prevent physical interference, and asset management controls for the protection of organisational resources. Standards on how information is handled, stored and backed up are defined to ensure that data is managed securely. Specifications may also include requirements for AOs to be ISO/IEC 27001 certified.

(c) Systems and operations security standards, to provide for the security of the authentication system with respect to its operations. This includes access controls to manage access to information, controls to ensure that security is integral during acquisition, development and maintenance of information systems, as well as cryptographic controls to protect the confidentiality, authenticity and integrity of information. It also details requirements for logs and system reviews, as well as requirements to ensure that customers are aware of good security practices, and staff are security-trained.

(d) Security incident management and response standards, to ensure that incidents are reported and managed in a timely manner.

(e) Technical security standards for the different authentication mechanisms that can be offered to end-users, such as One Time Passwords, biometrics, certificates, and smart cards.

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.

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?

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

Business Requirements – Confidentiality

6.3 Confidentiality requirements help to protect sensitive information against unauthorised access, modification and disclosure. With reference to Section 3.1 of Annex A, these include standards pertaining to the collection, use, exchange, storage and destruction of end-user data and commercially-sensitive information from the SPs.

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.

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

Business Requirements – Competition and Interconnection

6.4 Competition and interconnection requirements are proposed in Section 3.2 of Annex A, so as to inhibit unfair market conduct by the AOs. To facilitate this, a competition code similar to that in the telecommunications industry may be prescribed if necessary, which IDA will assess as the market develops Requirements for the AO to interconnect are also included. The interconnection requirements will allow SPs and end-users to migrate to another AO easily. The interconnection requirements will also minimise the need for end-users to carry multiple strong authentication credentials and allow end-users to have a consistent strong authentication experience by using any credential issued by an AO to access different online services. IDA will also reserve the right to require AOs to make available reference interconnection offers that are capable to be accepted by other AOs without negotiation.

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.

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?

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?

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?

Business Requirements – Disclosure and Liability

6.5 To protect the interests of end-users, SPs and AOs, disclosure and liability requirements will oblige AOs to avail clear and precise information such as the respective rights, risks, potential liabilities, and obligations of end-users, SPs and AOs, as well as terms and conditions regarding the provision of authentication services. (Please see Section 3.3 of Annex A.)

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.

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

Operational Requirements – Credential Lifecycle Management

6.6 AOs shall be responsible and accountable for the issuance, suspension and revocation of credentials, as proposed in Sections 4.4 to 4.6 of Annex A. This requirement provides assurance of the strength of credential an AO issues.

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.

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

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

Operational Requirements – Continuity of Authentication Services

6.7 With key economic sectors leveraging on the authentication platform provided by the AOs, business continuity requirements will help to mitigate the risks of system failures and other disasters, thus minimising their impact on the provision of authentication services. Authentication services should not be unnecessarily disrupted by AOs who wish to discontinue their services. Thus, such AOs will be required to provide sufficient notice before ceasing operations and may also be required to transfer its customers to other AOs. (Please see Sections 4.7 and 4.14 of Annex A.)

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.

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

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?

Other Operational Requirements

6.8 Other operational requirements for compliance by AOs include:

(a) Standards on the quality of service to be offered to AO's customers. This includes service level standards to ensure high resiliency and availability, capacity planning requirements to ensure that requests for authentication services can be met, as well as customer support requirements to improve the experience of AO's customers. (Please see Sections 4.2, 4.8 and 4.11 of Annex A.)

(b) AO's obligations to IDA, such as requirements for AOs to inform IDA upon changes in management staff, and the submission of regular statistics and reports for monitoring purposes. (Please see Sections 4.12 and 4.13 of Annex A.)

(c) Compliance requirements to technical standards that IDA specifies, so as to facilitate the entry of potential AOs, as well as the switching of AOs by SPs. These standards may include communication protocols

between AOs and AOs, as well as between AOs and SPs. (Please see Section 4.10 of Annex A.)

(d) Further specifications including requirements for key personnel to be trusted, requirements for the AO to notify relevant parties should the trustworthiness or reliability of the service be affected, and requirements for the AO to maintain proper system documentations. (Please see Section 4.1, 4.3 and 4.9 of Annex A.)

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.

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?

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?

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?

Annex A

PROPOSED INDUSTRY BEST PRACTICES

1 Introduction

1.1 Purpose

1.1.1 The purpose of this document is to define the requirements for the accreditation of an Authentication Operator (AO).

1.1.2 These requirements cover three broad aims:

- To protect the integrity, confidentiality and availability of the authentication services provided by AOs, data, systems and operations;
- To accord appropriate protections end-users, service providers (SPs), and authentication operators; and
- To ensure smooth and reliable operations of AOs.

1.2 Definitions

The following abbreviations and expressions shall have the meanings hereby assigned to them except where the context otherwise requires.

"Key Personnel" refers to AO's personnel who are assigned to perform the works construed for the IT Security Service.

"Penetration Test" refers to the security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.

"Authentication Operator" refers to the entity who offers third-party strong authentication services.

"Authentication Service" refers to the strong authentication service provided by the Authentication Operator to the service providers and/or end users.

"System" means the hardware and software associated with the operations of the Authentication Service.

"Trusted Person" means any person who has
(a) direct responsibilities for the day-to-day operations, security and performance of those business activities in respect of an authentication operator; or
(b) duties directly involving the issuance, renewal, suspension, revocation of credentials (including the identification of any person requesting a credential from an authentication operator), administration of an authentication operator's computing facilities.

"Authority" means the Infocomm Development Authority of Singapore.

1.3 Scope

1.3.1 The scope of the document covers three areas:

- Minimum security requirements that an AO shall need to achieve to be accredited;
- Minimum business requirements in order to protect end users, SPs and AOs; and
- Minimum operational requirements in order to ensure smooth and reliable operations.

2 Security Requirements

2.1 Risk Management

2.1.1 The AO shall document the risk management policy, approved by the Chief Executive Officer (CEO) and the Board of the AO, used in the operations of the Authentication Service.

2.1.2 The AO shall document and implement a risk management framework in line with the approved risk management policy. The risk management framework shall include detailed description of their risk management process and how it will be applied to the running of the AO's operations.

2.1.3 The CEO of the AO shall oversee and be responsible and accountable for managing and controlling the risk of running the AO's operations. The monitoring and measurement of effectiveness of controls shall flow upwards towards the Chief Executive Officer (CEO).

2.1.4 The information security risk management framework shall include but is not limited to the following:

- Risk Identification
- Risk Assessment
- Risk Response
- Risk Control Activities
- Risk Monitoring and Review

2.1.5 The AO shall implement control strategies consistent with its information security policy upon identification of threats and vulnerabilities.

2.1.6 The AO shall ensure risk management activities shall be conducted periodically to identify internal and external threats that may undermine the system integrity, interfere with the Authentication Services of the AO or result in the destruction of information.

2.1.7 The AO shall ensure that the risk management activities shall be conducted for the provision of Authentication Service to every Service Provider (SP) to

determine the additional security controls that shall be implemented for each SP.

2.1.8 The AO shall have documented agreements including all relevant security requirements in the provisioning of Authentication Service to the Service Providers.

2.1.9 The AO shall ensure that all security risks associated with the delivery of the Authentication Service shall be addressed before commencement of Authentication Service to the end user.

2.1.10 The AO shall have documented agreements including all relevant security requirements in the provisioning of Authentication Service to the end users.

2.1.11 The AO shall ensure that the risk management policies, analysis and controls shall be reviewed and updated periodically as part of a comprehensive risk management approach.

2.1.12 The AO shall ensure that the risk management policies, analysis and controls shall be reviewed and updated accordingly when a risk parameter changes

2.2 Information Security Management

2.2.1 Information Security Management and ISO/IEC 27001/27002

2.2.1.1 The AO shall be certified compliant with ISO/IEC 27001 by a certification body accredited by a National Accreditation Body. All AOs shall provided documentary evidence that it is ISO/IEC compliant.

2.2.1.2 Design, configuration, operation and maintenance of the systems used for the Authentication Service and networks are critical to the security of IT-enabled businesses. The scope includes availability, confidentiality, integrity and access control of critical AO's systems and operations.

2.2.1.3 The requirements listed here are intended to be specific to the Authentication Services and to supplement the general IT security controls addressed in the ISO/IEC 27001 and ISO/IEC 27002:2005. Where not specified directly in this requirement document, the AO shall take reference from ISO/IEC 27001 and ISO/IEC 27002:2005.

2.2.2 Security Management and Policy

2.2.2.1 The CEO of the AO shall oversee and be responsible and accountable for information security of the AO’s operations.

2.2.2.2 The AO shall document and implement an information security management and governance framework approved by the Chief Executive and the Board and shall be implemented by the AO. The framework shall include at least the following:

a. Security policies, standards and procedures for the running of the AO's operations;
b. Security architecture and design; and
c. Security management and operation processes.
d. Review processes

2.2.2.3 The AO shall document and implement security policies, standards and procedures specific to the operations of the Authentication Service operations which are maintained and communicated to all personnel and widely published throughout the organisation to ensure that the personnel are aware and reminded of the policy.

2.2.2.4 The AO shall ensure that the security policies, standards and procedures for the systems and operations shall fully comply with the Authority's system security policies, standards and instructions as well as standards and policies issued by the Authority subsequently.

2.2.2.5 The AO shall ensure the security policies and security controls should be reviewed periodically or when significant changes occur to ensure its continuing suitability and effectiveness. These reviews should take place through both self audits and third party audits or reviews.

2.2.2.6 The AO shall document and implement a change management process approved by the Authority to manage changes to security policies, procedures and controls approved.

2.2.2.7 The AO shall document and implement a plan that would coordinate information security activities across the AO's organisation in the operation of the Authentication Service.

2.2.2.8 The AO shall have clearly defined roles for all information security responsibilities in accordance to the information security policies. The information security roles shall take into account the need for segregation of duties required of each role and the level of authorisation accorded to the roles.

2.2.3 Asset Management

2.2.3.1 The AO shall document and implement a system to correctly track assets related to the running of the Authentication Service. This is to ensure that the information security of the system is not compromised through loss of equipment or assets.

2.2.3.2 The AO shall ensure that all assets related to the operations of the Authentication Service are assigned to a designated person or department for the purpose of accountability.

2.2.3.3 The AO shall develop and implement an acceptable use of assets policy approved by the CEO and the Board of the AO's organisation.

2.2.3.4 The AO's organisation shall have internal guidelines on the classification of information assets in accordance to the sensitivity of the information assets.

2.2.3.5 The AO shall document and implement an appropriate set of procedures for the labelling of information assets in line with the classification scheme defined in the developed classification guidelines.

2.2.4 Human Resource Control

2.2.4.1 The AO shall define and document all security roles and responsibilities of all personnel involved in the operations of the AOs operations. This shall include personnel of any third party organisation that the AO engages for the operations of the Authentication Service.

2.2.4.2 The AO shall ensure that all their personnel are informed of their security responsibilities and accountability/liability within the terms and conditions of employment and that their personnel agree and acknowledge before putting the person in his/her assigned areas of work.

2.2.4.3 The AO shall ensure job responsibilities and access rights shall be designed and reviewed yearly to ensure proper segregation of duties and alignment of access rights to business functions. In addition, periodic cross checks on personnel performing trusted roles or security sensitive functions for incompatible duties or interests (internal or external) shall be conducted.

2.2.4.4 The AO shall ensure that background checks and verifications are conducted for all employees and all its personnel's security clearance commensurate with the highest security classification of information that he/she has been be given access to. In addition, the AO's personnel shall only be granted access to information that is relevant to the performance of his/her responsibility.

2.2.4.5 The AOs shall subject their personnel to security re-screening at regular periods to ensure that they continue to be trustworthy. The screening shall ensure that the personnel does not have any criminal records or dubious links that may jeopardise or compromise the trustworthiness of the Authentication Service operations.

2.2.4.6 The AO shall ensure that third parties providing outsourced functionalities for the running of the Authentication Service operations will be subjected to security requirements at least as stringent as those for the AO. The responsibilities with respect to the information security requirements expected of the third party shall be explicitly included in the contract or service level agreement with the third party.

2.2.4.7 The Authority reserves the right to include the third parties in the security audit of the AOs.

2.2.4.8 The AO shall ensure that their personnel shall be provided with the information security policy upon employment. It shall be the responsibility of each personnel to read and understand it.

2.2.4.9 The AO shall ensure that all their personnel shall be educated on basic IT principles and safeguards. Personnel responsible for security areas (e.g. systems and operations security administrator) shall be trained on advanced IT security principles and safeguards. The security personnel shall be trained in the security features and vulnerabilities of the systems and operations.

2.2.4.10 The AO shall ensure that all their personnel apply security in line with the established security policies and procedures of the AO's organisation.

2.2.4.11 The AO shall ensure that all their personnel shall fully comply with any written instructions on security matters that may be issued by the Authority from time to time with reference to the operations of the Authentication Service.

2.2.4.12 The AO shall document and implement a formal disciplinary process and ensure that all its personnel and subcontractors are informed that failure to comply with would lead the AO to take disciplinary action against the AO's personnel and subcontractors.

2.2.4.13 The AO's personnel shall be required to sign a confidentiality agreement as part of their initial terms and conditions of employment prior to being given access to the Authentication Services and processes facilities.

2.2.4.14 The AO shall ensure confidentiality or non-disclosure agreements shall be reviewed when there are changes to the terms of employment or contract, particularly when employees are due to leave the organisation or contracts are due to end.

2.2.4.15 The AO shall ensure that all personnel are equipped with the relevant skills and experience to operate and run the Authentication Service based on their roles. Personnel who have not been adequately trained shall not be allowed to independently operate the System without the presence or supervision of trained personnel.

2.2.4.16 The AO shall ensure that their personnel shall be familiar with the requirements of the system and shall adhere to the security policy, standards and procedures as approved by the Authority.

2.2.4.17 The AO shall document and implement policies to ensure that when personnel or contractors are transferred by appointment, assignment, redeployment, termination or resignation, a formalised return of asset procedure is in place to account for all issued assets.

2.2.4.18 The AO shall document and implement policies to ensure that when personnel or contractors are transferred by appointment, assignment, redeployment, termination or resignation, all access privileges to IT systems, information and assets are reviewed, modified or revoked accordingly in a timely manner.

2.2.5 Physical and Environmental Security

2.2.5.1 The AO shall document and implement controls to ensure that all threats, vulnerabilities and exposures relating to physical and environmental security found during risk assessments are properly addressed with effective security control measures.

2.2.5.2 The AO shall document and implement security control measures to ensure the premises housing the systems used in the operations of the Authentication Service shall be physically secured according to the level of security prescribed in their security policies in the running of the AO's operation.

2.2.5.3 The AO shall document and implement policies and controls addressing the controlled access of various areas within the physical building. These controls shall include but shall not be limited to the controlled movement of equipment and property in and out of the site.

2.2.5.4 The AO shall ensure that responsibilities for the physical security of the AO's systems shall be defined and assigned to named individuals.

2.2.5.5 The AO shall document and implement controls against all identified environmental threats specific to the operations of the Authentication Service at the physical premise of the system. The environmental threats shall include both natural and man-made disasters.

2.2.5.6 The AO shall document and implement controls to prevent the disruption of the Authentication Service due to the disruption of service to supporting facilities.

2.2.5.7 The AO shall document and implement controls to ensure the physical infrastructure supporting the operations of the Authentication Service are protected from interception, unauthorised access or damage.

2.2.5.8 The AO shall document and implement controls to ensure devices used for the operations of the Authentication Service which can and are authorised to be taken off-site are adequately protected relative to their sensitivity of information stored on the devices.

2.2.5.9 The AO shall document and implement a process for the periodic preventive maintenance and technology or equipment refresh to ensure the continued availability and integrity of the Authentication Service.

2.2.5.10 The AO shall document and implement procedures to ensure the secure and proper disposal of equipment that may hold remnants of sensitive data. This shall include the re-use of equipment for other purpose other than the provision of the Authentication Service.

2.2.6 Operations Management

2.2.6.1 The AO shall document and implement all process and procedures related to the operation of the Authentication Service and communicate these process and procedures to all relevant personnel to fulfil their roles and responsibilities.

2.2.6.2 The AO shall document and implement a change management process and procedure to ensure changes to the operation processes are approved by the appropriate level of management.

2.2.6.3 The AO shall maintain a testing facility separate from the operation system used for live deployment. All changes to the system and corresponding controls should be tested on in the test environment and validated before deployment into the operational system.

2.2.6.4 The AO shall ensure dual control and segregation of duties shall be implemented for it's critical services and processes. Security related roles shall be given to personnel who are adequately trained to perform the job without any conflict of interest.

2.2.6.5 The AO shall document and implement clear service delivery levels and security controls in the engagement of third party organisation for the purpose of operations of the Authentication Service.

2.2.7 Backup

2.2.7.1 The AO shall document and implement a backup policy, processes and procedures that will ensure the AO's operations would be able to meet the required service levels as indicated in Section 4.8 Service Level Standards. The backup policy shall include processes for the periodic testing of data that have been archived.

2.2.7.2 The AO shall document and implement security controls to ensure the continued confidentiality, integrity and availability of the backed up data.

2.2.7.3 The AO shall ensure offline data storage media will be stored in a safe in a physical secure location with intrusion detection. The minimum period of data retention will follow the requirements of the relevant legislation. For privacy enhancing purposes, data may be destroyed after this minimum period has expired.

2.2.7.4 The AO shall ensure the destruction of data storage media will follow formal procedure and performed using mechanisms approved for this purpose.

2.2.8 Storage Media Handling

2.2.8.1 The AO shall document and implement procedures for the management of all forms of removal storage media. The procedures shall address the entire lifecycle of the removal storage media from its introduction to the AO's system, to the disposal of the storage media and shall be properly documented.

2.2.8.2 The AO shall document and implement security controls to ensure the continued confidentiality of data stored on removal storage media and to deny unauthorised access. This shall include any scenarios where the physical storage media storing the information may need to be physically out of the physical boundaries of the AO's organisation. Security controls would include the encryption of backup tapes when they are transported off-location.

2.2.9 Information and Data Handling

2.2.9.1 The AO shall ensure the secure usage and handling of all information related to the operations of the Authentication Service. Where there is a need to access Government provided information, the AO's personnel shall sign a confidentiality agreement to protect all Government information against unauthorised disclosures by the personnel in the course of their work.

2.2.9.2 The AO shall document and implement procedures and security controls to protect the privacy and confidentiality of the data under the AO's custody and access privilege to these data shall be implemented. Confidential information must not be disclosed to a third party unless the information is required to be disclosed under the law of the Republic of Singapore or a court order.

2.2.9.3 The AO shall document and implement security controls to ensure that system documentation of the Authentication Service is well protected against unauthorised access.

2.2.9.4 The AO shall be responsible for the safeguarding of security-sensitive information under its care and security controls are to be documented and implemented to ensure the safeguarding of these information. All the AO's personnel are responsible for safeguarding security-sensitive information entrusted to or accessed by them.

2.2.9.5 The AO shall ensure transactional data relating to the end user activities generated in the course of its operation shall be protected to ensure the end users' privacy and shall not be linked to any individual end-users.

2.2.9.6 The AO shall ensure that information resources shall be monitored to minimise risk of corruption and unauthorised disclosure, access, modification or deletion.

2.2.9.7 The AO shall document and implement controls to ensure the secure storage of data to ensure the confidential, integrity and availability of the data.

2.2.9.8 The AO shall ensure different classification of data, where applicable, on the AO's system should be segregated into different trust zones according to its security classification and sensitivity with regards privacy.

2.2.9.9 The AO shall ensure that zones requiring higher levels of protection will be safeguarded by a variety of methods including encryption, hardware security modules and strict access control. Sensitive data should be stored in encrypted form.

2.2.9.10 The AO shall ensure only authorised persons will have access to data registered and maintained by AO based on their access level prescribed in their roles and responsibilities.

2.2.9.11 The AO shall ensure that file integrity monitoring tools should be deployed to alert personnel to unauthorised modification of critical system or content files.

2.2.9.12 The AO shall document and implement control measures to protect security-sensitive information against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use, or modification. The control measures shall include administrative, technical, physical and personnel control measures. The AO shall protect the data regardless of the format in which they are held.

2.2.9.13 The AO shall document and implement control measures that are needed to protect the confidentiality and integrity of end user's credentials, which include end users' passwords, 2nd factor credentials, and other security-sensitive information.

2.2.10 Information Exchange policies

2.2.10.1 The AO shall document and implement formal information exchange procedures and policies with the Authority and third parties to ensure the accountability of information that would be exchanged. These shall include non disclosure agreements (NDA) where appropriate.

2.2.10.2 The AO shall perform a privacy impact assessment on AO's Authentication Services provided to Service Providers (SP). Specific recommendations resulting from this assessment should be implemented and may be addressed by the information security committee formed within the AO's organisation.

2.2.10.3 The AO shall ensure that all equipment used in the operations of the Authentication system (includes both the primary and alternate sites) shall only be physically in Singapore.

2.2.10.4 The AO shall not transfer security-sensitive information; data derived through the operations of the Authentication Service or privileged access, outside of Singapore, or allow parties outside Singapore to have access to it, without the prior approval of the Authority.

2.2.10.5 The AO shall not disclose security-sensitive information, received or generated, to anyone. This includes the source of the information.

2.2.10.6 The AO shall document and implement security controls that would ensure the continued security of the information being exchanged.

2.2.10.7 The AO shall ensure that no person shall remove any security-sensitive information upon resignation from his/her appointment or retain such information when he/she no longer requires them.

2.3 Systems and Operations Security Framework

2.3.1 Systems Security review

2.3.1.1 The AO shall review and monitor the security practices and processes on a regular basis, including commissioning or obtaining periodic expert reports on security adequacy and compliance in respect of the operations of the System. A process of monitoring service delivery, performance reliability and processing capacity of the System shall also be established for the purpose of gauging ongoing compliance with agreed service level and the viability of its operations.

2.3.1.2 The AO shall document and maintain up-to-date documentation on all information assets, which include hardware, software, personnel, system/user accounts, application IDs as well as all the operations and security processes, procedures and system configurations.

2.3.1.3 The AO shall engage a third party, at their own cost, to conduct a Penetration testing (PT) at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:

- Network-layer penetration tests
- Application-layer penetration tests.

2.3.1.4 The AO shall ensure that network and systems security audits shall be performed periodically using automated tools to help identify new security vulnerabilities. In addition, network penetration test may be performed periodically to help identify gaps that may have been introduced.

2.3.1.5 The AO shall document and provide detailed description of the review and monitoring process and tools.

2.3.2 Access Control Management

2.3.2.1 The AO shall develop and implement a access control policy in line with the security policy approved by the CEO and the Board of the organisation. The access control policy shall include but not limited to physical, personnel and application access control.

2.3.2.2 The AO shall ensure that the facilities required for the deployment of the solution shall be exclusively used for the System and cannot be shared with

other systems, unless written approval and authorisation has been given by the Authority.

2.3.2.3 The AO shall document and implement a proper approval process and tracking mechanism for all access to the system and information to ensure proper usage and accountability.

2.3.2.4 The AO shall document and implement physical security control measures and procedures to prevent any unauthorised access to the System.

AO's Organisation's User Access Management

2.3.2.5 The AO shall ensure that individual user accounts are given and documented for administrative access to the system and networks to provide clear user accountability.

2.3.2.6 The AO shall document and implement processes and procedures for managing and administering accounts and issued credentials. These procedures must comply with this set of security requirements as spelled out in this document and include registration, credential issuance, authentication and credential expiry and revocation.

2.3.2.7 The AO shall ensure that only authorised personnel are able to access applications required for their responsibility and that there are no accidental escalation of privileges of the personnel.

2.3.2.8 The AO shall document and implement procedures or mechanisms implemented so that access rights of all registered users, their levels of access and their continued requirement for access will be checked on a regular basis (re-authentication).

End User Access Management

2.3.2.9 The AO shall conduct routine verification of end users accounts and credentials to determine whether accounts and credentials issued are still valid or are required to be expired/revoked.

Network access control

2.3.2.10 The AO shall document and implement a change management process approved by the Authority for the purpose of adding new network connections to the Authentication System.

2.3.2.11 All unnecessary network protocols and traffic shall be filtered at the network perimeter gateways.

2.3.2.12 The AO shall ensure that there are no network connections that bypass the controls enforced at the central gateway. This shall include remote administrative connections into the network.

2.3.2.13 The AO shall document and implement the following security design practices into the System:

- Isolate the internal network segments from the Internet and other geographically separate sites through appropriate access control such as firewall, proxy servers or application security gateways. Where possible, all incoming and outgoing traffic shall be subject to filtering and scrutiny.

- Provide separate environments for the system development, testing, staging and production. Connect only the production internet-facing applications to the internet.

2.3.2.14 The AO shall ensure that mutual strong authentication occurs between the AO and another Authentication Operator before data transfer takes place.

2.3.2.15 The AO shall ensure that all communication among AOs and SPs occur via secured means. This could include usage of leased lines and may include other additional means such as secure web services, VPN or other transmission security solutions.

2.3.2.16 The AO shall ensure that all transmissions between AO and end users be secured from eavesdropping and replay.

2.3.2.17 The AO shall ensure that mutual strong authentication take place between the AO and any Service Provider before data transfer takes place.

2.3.2.18 The AO shall ensure that server authentication occurs between AOs and end users before data transfers take place.

2.3.2.19 The AO shall ensure that all end users' and authentication data transfers between Service Provider and AO shall be encrypted and digitally signed and all transmission should be encrypted end to end.

2.3.2.20 The AO shall ensure that that the internal networks be continuously monitored for unauthorised traffic by intrusion detection and prevention systems and that the detection of unauthorised activity should result in immediate remedial action.

2.3.2.21 The AO shall document and provide detailed description of the network, which shall at least include the architecture and design, the protocols, the System and their interfaces, the security features, the technologies and solutions, the administration and usage processes and procedures.

2.3.2.22 The AO shall not allow remote access to the System unless the access is properly justified and approved by the Authority.

<u>Application and Information access control</u>

2.3.2.23 The AO shall document and provide detailed description of the security measures to prevent the privileged system users from having direct access to

the stored data, which shall at least include the security features, the technologies and solutions, the administration and usage processes and procedures.

2.3.2.24 The AO shall conduct checks on all its application's functional capabilities and implementation related to the operations of the Authentication Service to ensure that adequate security measures are taken throughout the entire lifecycle of the application.

2.3.2.25 The AO shall document and provide detailed description of the security checks for all applications related to the Authentication service, conducted throughout the application development lifecycle.

2.3.2.26 The AO shall ensure that mutually dependent applications used in the development or operations of the Authentication Service are not given privileges beyond the required level that the application is required to operate.

2.3.3 Information Systems acquisitions, development and maintenance

2.3.3.1 The AO shall document and implement security mechanisms such as the secure sockets layer (SSL) server-authentication which allows the Service Providers to authenticate the AO's system. The AO must ensure that encrypted and authenticated sessions remain intact throughout the duration of the communications.

2.3.3.2 The AO shall document and provide detailed description of security mechanisms and controls to be used in the mitigation of risks identified through the risk analysis within the risk management methodology.

2.3.3.3 The AO's shall ensure their system shall have a timeout and automatic logout feature for non-active sessions for all administrative access to the system.

2.3.3.4 The AO shall provide hardware security modules or similar tamper-resistant devices for carrying out encryption and decryption functions. Other methods may also be considered acceptable if they can offer protection of encryption keys and confidential data in an end-to-end authentication operation at a similar level. The cryptographic security module shall be certified to FIPS 140-2 level 3.

2.3.3.5 The AO shall document and provide detailed description of the hardware encryption and decryption functions, or equivalent.

2.3.3.6 The AO shall document and implement built-in redundancies to prevent single point of failure which can bring down the entire System.

2.3.3.7 The AO shall document and implement a multi-tier application architecture which differentiates session control, presentation logic, server side input validation, business logic and database access.

2.3.3.8 The AO shall document and implement appropriate security controls within the billing module and audit trails to facilitate financial reconciliation.

2.3.3.9 The AO shall ensure that the security of the System and processes have been certified or reviewed by an independent third party security certifier or reviewer before system commissioning or before a new service or enhancement to a service is implemented.

2.3.3.10 The AO shall ensure that cryptographic modules are functioning correctly as intended through certification of the products through International Standards such as Federal Information Processing Standards (FIPS). For all other security solutions, it is preferred that they are subjected to certification against international standards such as Common Criteria (CC) at an appropriate Evaluation Assurance Level.

2.3.3.11 The AO shall ensure the security configuration of critical IT resources, such as operating systems, firewalls, network and security devices, are hardened according to international best practices and reviewed before the System becomes operational.

2.3.3.12 The AO shall document and provide detailed descriptions of the system hardening and secure configuration checklists for operating systems, network devices, security devices, patch management and applications.

2.3.3.13 The AO shall document, implement and maintain detailed security configurations of the System, from applications down to the operating system level.

2.3.3.14 The AO shall document, implement and maintain the security plan that is specific to the system, which includes the monitoring of security vulnerabilities that affect the Authentication Services, the actions that need to be taken to address the security vulnerabilities, the timeline and the function responsible for reviewing or testing, authorizing and implementing the security patch.

2.3.3.15 The AO shall document and provide detailed description of the security plan.

2.3.3.16 The AO shall perform periodic scanning for unauthorised codes and applications, viruses and system vulnerabilities, on the System. If any of the security weaknesses mentioned above has been found, the AO shall also be required to perform follow-up actions to rid the system of these weaknesses in a timely manner.

2.3.3.17 The AO shall perform vulnerability scanning of the Internet-facing systems at least once every three (3) months or whenever the AO's System undergoes software updates/upgrades. The AO shall address all vulnerabilities found in a timely manner and shall document the measures taken.

2.3.3.18 The AO shall document and provide detailed description of the process, products and tools, used for vulnerability scanning.

2.3.3.19 The AO shall document and provide detailed description of the security measures and procedures to prevent malicious codes and back doors from being introduced and harming the System and networks.

2.3.3.20 The AO shall ensure that any changes to the original design, implementation and setup of the System will continue to ensure that the AO is compliant to all requirements specified by Authority for AOs.

2.3.3.21 The AO shall document and provide detailed description of the change and security review conducted on the change before implementation into the production system. The AO shall include the detailed description of this process as part of the change control process.

2.3.3.22 The AO shall document and implement a change control process to ensure that all intended changes to the production systems are properly reviewed, tested and authorised before implementation. Detailed description of the change and configuration control in the change control process shall be provided by the AO.

2.3.3.23 The AO shall document and provide detailed description of the change control process, which shall at least include the people involved in reviewing, authorising and implementing the change, the system products or solutions used if any.

2.3.3.24 The AO shall document and provide an appropriate change and configuration control environment to manage the development and maintenance of applications.

2.3.3.25 The AO shall document and provide a detailed description of the helpdesk management process for operational issues, which details issue identification, classification, prioritisation, monitoring and resolution.

2.3.3.26 The AO shall document and implement procedures to ensure that all data and information stored in the System are securely erased such that the stored data and information cannot be recovered when the situation requires the erasure of data. The AO shall provide detailed description of the procedures, tools and solutions, used to ensure secure erasure of security-sensitive data.

2.3.3.27 The AO shall document and implement a plan for a comprehensive security evaluation and testing program that shall be developed for compliance monitoring with accreditation requirements. These security evaluation and testing processes are prescribed by the security requirements of the accreditation framework and should be performed in addition to the normal routine of information security testing and evaluation.

2.3.3.28 The AO shall ensure that the application (and system) build shall have an in built exception/error handling mechanism to provide fail safe processing

under various error and exception conditions. Leakage of sensitive information should not occur due to system/exceptions/errors.

2.3.3.29 The AO shall ensure through the provision of evidence of due diligence any application services that are developed shall not be vulnerable to attacks due to insecure software codes. Due diligence can take the form of source code review, stress loading, compliance and exception testing.

2.3.3.30 The AO shall document and provide a detailed description of the security controls implemented for all applications related to the operations of the Authentication Service to be approved by the Authority. These controls shall include but not limited to the following:

- Input Validations
- Workflow Controls
- Message Integrity
- Output Validations

2.3.3.31 The AO shall ensure that the design and implementation of all applications related to the operations of the Authentication Service shall undergo security testing to ensure that it is not be affected by at least but not limited to the following vulnerabilities:

- Parameters not validated e.g. SQL injection and parameter manipulation;
- Broken access controls;
- Broken accounts and session management;
- Cross-site scripting;
- Buffer overflows;
- Command injection; and
- Error handling.

2.3.4 Cryptographic controls

2.3.4.1 The AO shall document and provide detailed description of how the cryptographic keys are protected.

2.3.4.2 The AO shall document and provide detailed description of the key management standard defining key hierarchy, custodian, generation, loading, storage, distribution, renewal and backup.

2.3.4.3 The AO shall ensure that no single individual have access to the protected information and data, e.g. not a single person will know the entire encrypting key or have access to all the constituents making up these keys. The AO shall ensure that all cryptographic keys, which include master keys, key encrypting keys or data encrypting keys, shall be created, stored, distributed or changed without compromising the security of the cryptographic keys.

2.3.4.4 The AO shall use only select encryption algorithms which are well established international standards and which have been subjected to

rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies and/or the Authority.

2.3.5 Audit Log and Compliance

2.3.5.1 The AO shall document and implement policies, process and procedures to ensure all necessary logs to be kept, archived, and reviewed regularly. The policies shall include usage policies and accessibilities of the logs.

2.3.5.2 The AO shall ensure that all data exchanges should be logged so that the parties involved can be uniquely identified and a strong audit trail of all access attempts (read, write and delete at all levels) should be maintained and proactively monitored.

2.3.5.3 The AO shall ensure that the individual actions of all employees working on the system are accounted for and auditable.

2.3.5.4 The AO shall ensure that logging mechanisms shall be enabled on the user accounts held by the AO's personnel. The AO shall ensure that the logs include account, name, activities (both normal and exceptional activities), time, data and source of occurrence.

2.3.5.5 The AO shall ensure that logs shall record all activities carried out by privileged accounts – like administrator, auditor, and database administrator accounts.

2.3.5.6 The AO shall document and implement security controls measures to ensure that the logs are not accessed, modified and deleted by unauthorised personnel.

2.3.5.7 The AO shall document and provide detailed description of the security measures used to protect the logs from unauthorised modification and deletion.

2.3.5.8 The AO shall ensure that the logs are kept for at least seven (7) years.

2.3.6 Time Synchronisation

2.3.6.1 The AO shall document and implement a control to ensure time synchronisation between all the systems used in the operation of the Authentication Service within the AO's organisation. Where possible, the AO shall take time reference from an authoritative source.

2.3.7 Security Training and Awareness Requirements

<u>End Users</u>

2.3.7.1 The AO shall document and implement a security awareness programme for end users about the usage of the credentials issued by the AO. The user awareness programme should also educate users on phishing attacks, how to

verify Service Provider and AO's websites, what security measures to take on their personal computers at home, and how to protect their second-factor authentication credentials/devices.

2.3.7.2 The AO shall advise the public users to adopt good security practices such as installing anti-virus, anti-spyware and personal firewall and updating the anti-virus and personal firewall software to newer versions on a regular basis.

2.3.7.3 The AOs shall document and provide detailed description of the good security practices for the public users.

Staff and Employees

2.3.7.4 The AO shall ensure an information security awareness program shall be implemented and conducted on at least an annual basis to ensure that all personnel are informed of the potential security risks and exposures in the AO's operations and systems. In particular, personnel, especially those in the frontline service, shall be informed of typical social engineering attacks and the safeguards against them.

2.3.7.5 The AO shall document and demonstrate that they have a comprehensive security programme to train its personnel involved in the operation of the Authentication Service in security and in their assigned role.

2.4 Security Incident Management and Response

2.4.1 The AO shall document and implement procedures to actively keep track of security vulnerabilities and attacks that are reported by reputable sources and develop countermeasures or correct them promptly. The procedures should include an incident response capability to provide active defence and corrective actions against security exploits and attacks.

2.4.2 The AO shall document and implement a security incident handling and response plan for the operations of the AOs operations and establish formal incident escalation procedures for information security incidents that apply and impact the Authentication Service.

2.4.3 The AO shall ensure that the incident management procedures and plans shall be approved by the AO's CEO and the Board. The Authority, and affected Service Provider(s) shall be notified immediately in case of any significant information on security incident.

2.4.4 The AO shall ensure an incident response action plan shall be established and periodically tested to ensure the readiness of the AO to respond to incidents. The plan shall include but not limited to the following areas:

- Compromise control;
- Notification to user community; (if applicable)
- Revocation of affected authentication devices; (if applicable)

- Personnel incident handling responsibilities;
- Service disruption procedures and investigation;
- Monitoring and audit trail analysis; and
- Media and public relations.

2.4.5 The AO shall closely monitor and review activities undertaken by the AO's personnel on the system and these should be documented. The Authority reserves the right to review the logs as and when required, and the AO shall provide the required logs to the Authority in a timely manner.

2.4.6 The AO shall document and implement real-time monitoring to detect and report any abnormal activities such as unauthorised changes to system and network files and directories for further investigation.

2.4.7 The AO shall document and provide to the Authority detailed description of the process and tools used for real-time monitoring and detection.

2.4.8 The AO shall ensure that all their personnel be briefed on the incident reporting procedures.

2.4.9 The AO shall ensure that all security incidents such as virus infection, security compromises, unauthorised access and security vulnerability, shall be reported directly to the security manager of the AO's organisation. The security manager shall take the necessary actions to ensure that all security incidents are properly handled and managed.

2.4.10 The AO shall document and implement preventive measures to thwart the recurrence of security incidents. For all such incidents, the AO shall submit a preliminary incident report to the Authority within 24 hours, and a post-incident review report within three (3) working days. A summary of all incidents shall be submitted to the Authority on a monthly basis. The AO's organisation and its security manager shall also work closely and give full support to the Authority in resolving the security incidents when the need arises.

2.4.11 The AO shall ensure that alert mechanisms to notify on viruses, worms, vulnerability and exploits are established and documented. The AO shall draw out and implement a security alert procedure.

2.4.12 The AO's personnel shall be familiar with the alert procedure and mechanisms established.

2.4.13 The AO shall document and provide detailed description of the alert and notification processes/tools for viruses, worms, security vulnerabilities, and system and network intrusions.

2.4.14 The AO shall ensure incident response procedures shall be established for documenting an event as a basis for subsequent action including forensics where necessary.

2.5 Authentication Mechanism Requirements

2.5.1 General Requirements

2.5.1.1 The AO shall ensure that any proposed form of authentication mechanism are approved by the authority and adhere to an international recognised standard and the proposed deployment design should be deemed secure based on international standards.

2.5.1.2 The AO shall document and implement end-to-end encryption of the end users' data and other sensitive information wherever possible. This means that the encryption is kept intact from the point of entry to the final system destination where decryption or authentication takes place.

2.5.1.3 The AO shall document and provide detailed description of the security measures or mechanisms, which include the solutions and associated processes, for achieving end-to-end encryption of end users' credentials and other sensitive information.

2.5.1.4 The AO shall ensure that any secrets (e.g. passwords, etc.) distributed to public users should be done in such a way that the confidentiality and integrity of the secrets are intact.

2.5.1.5 The AO shall document and provide detailed description of enrolment and distribution of the user tokens, one time passwords (OTP) or private keys.

2.5.1.6 The AO shall ensure that any password generation process shall be secured such that any information related to the passwords is not exposed to the person generating the passwords nor exposed in the computer used for generating the passwords.

2.5.1.7 The AO shall document and provide detailed description of the authentication mechanism life cycle process. Where applicable, process shall adhere to the requirements for the various stages as spelled out in Section 2.5.2

2.5.1.8 The AO shall document and implement enforcement rules on:

- Account lockout (both temporary and permanent) after a predefined number of invalid logon attempts;
- Authentication session timeout and, if applicable, account logout after a predefined inactivity time per user session. The timeout will require the end-user to restart his authentication session; and
- Credential suspension after a predefined number of invalid authentication attempts.

2.5.1.9 The AO shall ensure that tamper proof Hardware Security Modules (HSM) are deployed within their system design for areas where sensitive information is aggregated.

2.5.1.10 The AO shall ensure that the authentication mechanism chosen shall be resistant to replay attacks. Where susceptibility to replay attacks is inherent to the authentication mechanism, the AO shall have in place controls to ensure the window of opportunity for attack is minimised.

2.5.1.11 The AO shall ensure that the authentication mechanism chosen shall be resistant to race conditions. Where susceptibility to race condition attacks is inherent to the authentication mechanism, the AO shall have in place controls to ensure the window of opportunity for attack is minimised.

2.5.1.12 The AO shall ensure that credentials that are stored in the AO's system shall always be stored in encrypted form.

2.5.1.13 The AO shall ensure that the credential administration process shall be secure such that any information related to the credential is not exposed to the personnel managing, administering, safekeeping, transporting or involved in any other ways with the credentials. The AO shall provide detailed description of the credentials administration process.

2.5.1.14 The AO shall ensure that authentication mechanism solutions chosen shall adhere to ISO/IEC standards for the domain. The AO shall provide documentary prove of areas of deviation satisfactory to the Authority for any deviation from this clause.

2.5.1.15 The AO shall ensure that authentication mechanism solutions chosen shall have internationally and/or industry recognised certifications.

2.5.1.16 The AO shall document and provide to the Authority the exact implementation plan of the Authentication solution.

2.5.1.17 The AO shall conduct a detailed risk management study of the authentication mechanism used and provide the Authority with full details of the study through appropriate documentations. This study shall include a detailed threat assessment of the proposed authentication mechanism and the security controls proposed to mitigate the possible threat/vulnerability pairing. The AO shall obtain the Authority's written approval for each authentication mechanism/solution it intends to deploy.

2.5.1.18 The AO shall document and implement a control to ensure that concurrent/ parallel Authentication session cannot take place between a end user and Service Provider.

2.5.1.19 The AO shall ensure the risk management study include all technology and processes required for the deployment of the AO Authentication Service. The risk management study shall include but not limited to the following:

a. Risk Analysis of the authentication mechanism / solutions
b. Risk mitigation strategy
c. Risk mitigation controls
d. Residual risk management

2.5.2 Authentication Credential Life Cycle

Enrolment of End-User

2.5.2.1 The AO shall document and implement controls to ensure the confidentiality and the integrity of the data for the enrollment process.

2.5.2.2 The AO shall document and implement a secure means to enrol users for their personalised 2nd factor authentication.

2.5.2.3 The AO shall documents and implement a process to minimise enrolment time if the end-user is required to be present in person for registration or enrolment.

2.5.2.4 The AO shall document and implement processes and controls to securely conduct the initial validation of the specific public-user before the initialization of any Authentication Service for the specific public-user.

Distribution of Credentials

2.5.2.5 The AO shall document and implement controls and procedures for the secure distribution of tokens for generation of credentials, secure storage mechanism for credentials where appropriate.

2.5.2.6 The AO shall document and implement controls and procedures or the secure publishing of the created credentials into the production system.

Key generation

2.5.2.7 The AO shall document and implement processes and controls to ensure that all key generation processes are secure and truly random. Details of the key generation process shall be provided to the Authority.

2.5.2.8 The AO shall ensure that the seed used for the generation of credentials are truly random and compliant to FIPS-140-2.

Storage of Credentials

2.5.2.9 The AO shall ensure that the credential shall be stored in an international open format available for exchange, where applicable. The AO shall seek approval from the Authorities if deviation from this requirement is required.

This shall include but is not limited to the following reference standards

- ICAO Standards for e-passports
- Singapore Standards SS 529 : 2006

2.5.2.10 The AO shall document and provide for a means to translate the credential format to an open exchange format in the event approval is given by the

Authorities for storage of credentials in formats other than international open format.

2.5.2.11 The AO shall document and implement security controls to ensure the secure storage of the collected credential data.

Database used

2.5.2.12 The AO shall ensure that the Authentication server chosen shall use established authentication protocols.

Transmission of Credentials

2.5.2.13 The AO shall document and implement controls to ensure the secure transmission of data between any end points of the authentication system. The level of controls required will be based on the risk associated with the transmission medium and ends points.

2.5.2.14 The AO shall document and implement controls to ensure the integrity and confidentiality of the credentials during transmission to ensure that no credential information is changed or compromised

Revocation of credentials

2.5.2.15 The AO shall document and implement policies, procedures and processes to secure the revocation of credentials.

Key Compromise processes

2.5.2.16 The AO shall document and implement policies, procedures and processes to address the events of key compromise.

Lost procedures

2.5.2.17 The AO shall document and implement policies, procedures and processes to securely address the events of end-user losing their credentials

Reset procedures

2.5.2.18 The AO shall document and implement policies, procedures and processes to securely address the events of end-user need to reset their credentials.

Key Management

2.5.2.19 The AO shall document and implement policies, procedures and processes for key management.

2.5.2.20 The AO shall ensure that no single individual should know entirely what the keys are or have access to all the constituents making up these keys.

2.5.2.21 The AO shall ensure that security controls are in place to address all the threats in key creation, storage, distributed and key change.

Key Change

2.5.2.22 The AO shall document and implement processes and procedures to securely address the events of key change required of the system.

Renewal

2.5.2.23 The AO shall document and implement processes and procedures to securely address the events of end-user need to renew their credentials.

Suspension and reactivation

2.5.2.24 The AO shall document and implement processes and procedures to securely address the suspension and reactivation of end-user credentials.

Software Interface

2.5.2.25 The AO shall ensure that the authentication solution selected shall have software APIs that can be used to build interface for inter-operability for different platforms. Deviation from this requirement shall be subjected to the approval of the Authority.

2.5.2.26 The AO shall ensure proper documentation for the API must be available to the Authority on request.

Backup

2.5.2.27 The AO shall document and implement security controls that will ensure the timely backup of credential information and transactional logs of Authentication Service provided.

Destruction

2.5.2.28 The AO shall document and implement controls to securely destroy returned end-user authentication devices.

Cryptography

2.5.2.29 The AO shall ensure that the cryptographic algorithms used in the various areas of deployment for the Authentication Service shall be a recognised international standard which is deemed up-to-date and of a level that is fit for deployment for the particular areas.

2.5.2.30 The following cryptographic algorithms, where appropriate, shall be implemented for end user authentication devices.

- 3DES

- AES 128 and 256
- RSA 1024 and 2048
- ECC (ECDSA B191, P192,)
- SHA-1 and SHA-256

2.5.2.31 The AO shall ensure that key strength for the cryptographic algorithms used for any server side devices should be twice the key strength used for any end-user devices.

2.5.3 One Time Password (OTP)

2.5.3.1 The AO shall ensure that the chosen authentication system that utilises a One Time Password (OTP) mechanism shall be implemented using well established international standards which have been subjected to rigorous scrutiny by an international community or approved by authoritative professional bodies and/or the Authority. The AO shall engage an independent entity with expertise in OTP deployment to evaluate and certify the security of the OTP solution. The evaluation report shall be submitted to the Authority. The AO shall rectify any points deemed insecure by the Authority, at the AO's own cost.

2.5.3.2 The AO shall ensure that hardware tokens used for the generation of OTPs shall be tamper resistant and of a key length and algorithm that is acceptable to the Authority for the period of deployment.

2.5.3.3 The AO shall ensure that the OTP window shall not exceed 100 seconds on either side of the server time and should be further minimised where possible.

2.5.4 Biometrics

2.5.4.1 The AO shall ensure that the chosen authentication system that utilises a Biometrics mechanism shall be implemented using well established international standards which have been subjected to rigorous scrutiny by an international community or approved by authoritative professional bodies and/or the Authority. The AO shall engage an independent entity with expertise in Biometrics deployment to evaluate and certify the security of the Biometrics solution. The evaluation report shall be submitted to the Authority. The AO shall rectify any points deemed insecure by the Authority, at the AO's own cost.

2.5.4.2 The AO shall document and demonstrate that the biometric feature selected as the identifier for the end subscribers is accurate, has relatively unalterable, distinguishing, physical or behavioral characteristic that can be captured, recognized, and authenticated over an indefinite period of time.

2.5.4.3 The AO shall only collect specific biometric data required for the biometric template for the specific authentication mechanism.

2.5.4.4 The AO shall document and demonstrate that the method of capturing the biometric identifying feature shall be unobtrusive to the user. The method selected must be socially acceptable and must not endanger the health, safety, or welfare of any user.

2.5.4.5 The AO shall plan and document a procedure for the work-around for the non-enrollment of the biometrics template due to temporary or permanent situation of the end user. This procedure shall be tested periodically to ensure the continued relevance of the plan.

2.5.4.6 The AO shall document and implement controls to ensure the notifications of non-acceptable biometric sample during the course of the enrollment.

2.5.4.7 The AO shall demonstrate that the biometric system used is capable of performing automated self diagnostics and calibration.

2.5.4.8 The AO shall document and implement controls to ensure the accurate translation of the captured biometric data into a stored template.

2.5.4.9 The AO shall document and implement policies and procedures to ensure the privacy of the subscriber in the collection of the biometric data.

2.5.4.10 Then AO shall demonstrate the effectiveness of the controls implemented to ensure the privacy of the collected biometric data.

2.5.4.11 The AO shall demonstrate that the biometrics solution(s) chosen shall be resistant to physiological and mimicry spoofing attacks.

2.5.5 Certificates

2.5.5.1 The AO shall ensure adherence to the most current Security Guidelines for Certificate Authorities (now version 2.0) in their implementation of a Certificate based infrastructure for Authentication in the provision of the 2nd Factor Authentication

2.5.6 Smart Card Specifications

2.5.6.1 The AO shall ensure that the chosen smart cards when used in any part of the authentication mechanism shall be of a standard fit for its particular usage and shall be implemented using well established international standards which have been subjected to rigorous scrutiny by an international community or approved by authoritative professional bodies and/or the Authority. The AO shall engage an independent entity with expertise in smart card deployment to evaluate and certify the security of the smart card solution. The evaluation report shall be submitted to the Authority. The AO shall rectify any points deemed insecure by the Authority, at the AO's own cost

3 Business Requirements

3.1 Confidentiality

3.1.1 Except for the purposes of Part XII of the Electronic Transactions Act, or for any prosecution under any written law or pursuant to an order of court, every AO and its authorised agent must keep all end-user-specific information confidential.

3.1.2 Any disclosure of end-user-specific information by the AO or its agent must be authorised by the end-user.

3.1.3 An AO shall store end-user specific information only in a data store housed within Singapore.

3.1.4 End-user specific information shall be handled in a secure manner in transit, and properly destroyed upon expiry.

3.1.5 End-user specific information not collected upon registration, which may become available in the day-to-day operations such as end-users' usage patterns, shall not be collected by an AO without the explicit written consent of end-user.

3.1.6 Data passed from an AO to any service provider or another AO shall be kept to the minimum that is required for the purpose of authentication.

3.1.7 End-user data shall not be used for purposes other than the provisioning of authentication services.

3.1.8 AOs shall not disclose any commercially-sensitive information on their service providers that may be obtained during the provisioning of authentication services. This includes business-customer relationships.

3.1.9 An AO shall not store or disclose any details obtained regarding the online service transactions to be secured by the authentication service.

3.1.10 AOs may negotiate and enter into individual confidentiality agreements with other AOs, service providers, or end-users, provided that the terms of the individual confidentiality agreements are not inconsistent with these requirements.

3.1.11 The AO shall implement control measures that prohibit the storage of data transmitted by the SP that is not required by the AO to perform the Authentication Service.

3.2 Competition and Inter-Connection

3.2.1 An AO shall engage in fair market conduct and shall not:

a. engage in any anti-competitive practices; or
b. abuse any dominant position in the market.

3.2.2 Without prejudice to the generality of 3.2.1, the following practices shall constitute unfair market conduct

a. Pricing abuses by dominant AOs, including predatory pricing, price squeezes, and cross-subsidisation;
b. Discrimination by dominant AOs towards non-affiliated AOs or service providers;
c. Provision of false or misleading information to competitors;
d. Price fixing or bid rigging;
e. Market and customer allocation; or
f. Group boycotts of specific service providers.

3.2.3 The Authority may, from time to time, publish on its Internet website a competition code for compliance by every AO.

3.2.4 All AOs shall interconnect with other AOs, either directly or indirectly. An end-user managed by an AO shall be able to authenticate at service providers served by other AOs.

3.2.5 The Technical Standard published by the Authority, shall be implemented to inter-connect with existing AOs.

3.2.6 AOs shall negotiate individual commercial agreements with other AOs for interconnection.

3.2.7 The Authority may require AOs to make available reference interconnection offers, approved by the Authority, that are capable to be accepted by other AOs without negotiation.

3.2.8 Any AO that has been harmed, or is likely to be harmed as a result of anti-competitive practices by any other AO may submit a written request asking the Authority to investigate and take enforcement action against the contravening AO.

3.3 Disclosure and Liability

3.3.1 The AO shall ensure that end-users shall be informed clearly and precisely on the respective rights, risks, potential liabilities, obligations and responsibilities of the end-users, service providers and the AO on all matters relating to the use of the Authentication Service, and in particular, any problems that may arise from processing errors and security breaches. The end-users shall be informed before they subscribe to the Authentication Service.

3.3.2 The terms and conditions applying to the Authentication services, including end-user agreements, privacy and security policy, shall be publicly published at the AO's web site. The AO shall clearly define customer dispute handling, reporting and resolution procedures, including the expected timing for the AO's response, and make this information available on the AO's website.

3.3.3 The AO shall explicitly define the liability of the end user, the service provider and the AO in the use of using the Authentication Service provided by the AO.

3.3.4 The AO shall ensure that an appropriate liability framework is implemented. The latest version of the AO's baseline liability framework shall be filed with the Authority. The liability framework shall minimally cover.

a. Sources of liability the AO is exposed to;
b. Obligations of the AO;
c. Scope of liability (e.g. monetary loss, loss of goodwill, other indirect loss);
d. Limitation of liability in monetary terms (e.g. maximum liability per incident);
e. Exception to limitation of liability;
f. Indemnity against third-party claims;
g. Dispute resolution;
h. Liquidated damages.

3.3.5 The following information shall be published on each AO's Internet website accessible to members of the public:

a. The terms and conditions applying to the provision of authentication services;
b. End-user agreements and privacy policy; and
c. Latest version of the AO's liability framework.

3.3.6 Every AO must log all changes to their liability framework together with the effective date of each change.

3.3.7 An AO shall keep in a trustworthy manner a copy of each version of the liability framework, together with the date it came into effect and the date it ceased to have effect.

4 Operational Requirements

4.1 Personnel

4.1.1 An AO shall take reasonable measures to ensure that every trusted person —

a. is a fit and proper person to carry out the duties assigned to him;
b. is not an undischarged bankrupt in Singapore or elsewhere or has made a composition or an arrangement with his creditors; and
c. has not been convicted, whether in Singapore or elsewhere, of —
   i. an offence the conviction for which involved a finding that he acted fraudulently or dishonestly; or
   ii. an offence under the proposed AO legislation or these requirements.

4.1.2 Every trusted person must —

a. have a good knowledge of the proposed AO legislation and these requirements; and

b. possess the relevant technical qualifications, expertise and experience to effectively carry out his duties.

4.1.3 An AO shall ensure that the lead personnel responsible and accountable for the overall security and day-to-day operations —
a. is a trusted person; and
b. is a Singapore citizen with at least five years of working experience in managing IT security in a large organisation.

4.2 Customer Support

4.2.1 The AO shall provide a single point of contact to call for problem reporting. The technical support personnel shall escalate the problems to the relevant parties for actions if required and track the status of any problems reported until they are resolved or closed. The AO shall meet any service levels stated in Section 4.8 Service Level Standards for support and problem management.

4.2.2 The AO shall provide a technical support management plan to service providers subscribing to its services. The technical support management plan shall outline the following:
a. Contact information of technical support personnel;
b. Service level targets (in terms of response times, severity levels classification, problem resolution times); and
c. Process for problem reporting, problem analysis, impact analysis, escalation, resolution and closure.

4.2.3 The AO shall provide customer servicing officers for potential customers to make enquiries on its authentication service and for sales engagements. There shall be two modes to contact the customer servicing officers, that is, via email and phone.

4.2.4 The AO shall put in place a service request procedure to allow service providers to put up service requests to be done by the AO.

4.3 Notification of Risk in Trustworthiness of Credentials

4.3.1 In the event of an occurrence that materially and adversely affects an AO's trustworthy system or the reliability of any credentials that the AO has issued, the AO shall —
a. use reasonable efforts to notify any person who is known to be or foreseeably will be affected by that occurrence; or
b. act in accordance with procedures governing such an occurrence specified in its risk management framework.

4.4 Issuance/Re-issuance of Credentials

4.4.1 The AO shall be responsible for the issuance of credentials to end-users.

4.4.2 The AO shall confirm by itself or through an authorised agent that the end-user is the person to be associated to the credential to be issued.

4.4.3 The date and time of all transactions in relation to the issuance of a credential must be logged and kept in a trustworthy manner.

4.4.4 The AO shall allow for batch issuance of the 2nd-factor authentication credentials/devices.

4.4.5 The AO shall support issuance of credentials to Singapore residents (i.e. NRIC holders and FIN holders), foreigners with valid travel documents, as well as entities (e.g. companies).

4.5 Suspensions of Credentials

4.5.1 Unless the AO and the end-user agree otherwise, the AO that issued a credential shall suspend the credential as soon as possible after receiving a request by a person whom the AO validates to be the end-user associated with the credential.

4.5.2 An AO may suspend a credential that it has issued if the AO has reasonable grounds to believe that the credential is unreliable, regardless of whether the end-user consents to the suspension; but AO shall complete its investigation into the reliability of the credential and decide within a reasonable time whether to reinstate the credential or to revoke the credential in accordance with section 4.6.

4.5.3 An AO shall suspend a credential after receiving a valid request for suspension (in accordance with section 4.5.1); but if the AO considers that revocation is justified in the light of all the evidence available to it, the credential must be revoked in accordance with section 4.6.

4.5.4 An AO must terminate a suspension initiated by a request if the AO discovers and confirms that the request for suspension was made without authorisation by the end-user.

4.5.5 The date and time of all transactions in relation to the suspension of credentials must be logged and kept in a trustworthy manner.

4.5.6 Upon effecting a suspension, the AO shall immediately notify the end-user associated with the credential.

4.5.7 An AO must maintain facilities to receive and act upon requests for suspension at all times of the day and on all days of every year.

4.6 Revocation of Credentials

4.6.1 An AO shall revoke a credential that it issued —

a. after receiving a request for revocation by the end-user associated with the credential; and confirming through appropriate verification measures

that the person requesting the revocation is the end-user, or is an agent of the end-user with authority to request the revocation;

b. after receiving a certified copy of the end-user's death certificate, or upon confirming by other evidence that the end-user is dead.

4.6.2 An AO must maintain facilities to receive and act upon requests for revocation at all times of the day and on all days of every year.

4.6.3 The date and time of all transactions in relation to the revocation of credentials must be logged and kept in a trustworthy manner.

4.6.4 An AO shall revoke a credential, regardless of whether the end-user associated with the credential consents, if the AO confirms that —

a. a material fact represented by the end-user during registration is false;
b. a requirement for issuance of the credential was not satisfied;
c. the AO's trustworthy system was compromised in a manner materially affecting the credential's reliability; or
d. an individual end-user is dead.

4.6.5 Upon effecting a revocation, other than under subsections 4.6.1(b) or 4.6.4(d), the AO shall immediately notify the end-user associated with the credential.

4.7 Business Continuity Management

4.7.1 Business Continuity Planning

4.7.1.1 The AO shall provide to the Authority, and have in place, a Business Continuity Plan (BCP) to meet the required Service Level Standards. The plan should show the involvement of senior management's responsibility within the BCM. The AO shall periodically review and enhance the business continuity plan.

4.7.1.2 The scope of the business continuity plan shall address disruptions, including short-term disruptions (spanning less than 24hrs), loss of service due to a natural disaster, system failures caused by system faults, hardware malfunction or operating errors, as well as catastrophic events that results in the destruction of the primary site.

4.7.1.3 The AO shall ensure that the business continuity plan includes controls and measures that will maintain the security level required of the AO's operations.

4.7.1.4 The business continuity plan shall address all phases of a disaster: activation, recovery and reconstitution.

4.7.1.5 The business continuity plan shall cover at least the following areas:

a. Line of succession, roles and responsibilities
b. Activation procedures that addresses the following:
    - Call tree for activation

- Primary and alternate contact methods;
- Procedures to be followed if an individual cannot be contacted;
- Information to convey; and;
- Instructions, if any.

c. Damage assessment guidelines which include:
   - Cause of disruption;
   - Potential for additional disruption;
   - Areas or systems affected;
   - Status of physical infrastructure;
   - Inventory and functional status of equipment
   - Type of damage
   - Items to be replaced; and
   - Estimated time to restore services.

d. Plan activation criterion;
e. Recovery strategies and priorities
f. Recovery procedures that address the following:
   - Obtaining authorization to access damage facilities
   - Notifying internal and external associated service providers;
   - Obtaining and installing necessary hardware and software;
   - Obtaining and loading backup media;
   - Restoring critical operating systems and application software;
   - Restoring system data;
   - Testing system functionality including security controls;
   - Connecting systems to network and external systems; and
   - Operating alternate infrastructure successfully.

g. Reconstitution procedures;
h. Contact information;
i. Standard operating procedures and checklist for processes;
j. List of hardware, software, firmware and other resources that are required to support operations. Details like model or version number, specifications and quantity shall be documented;
k. Description of and direction to alternate site;
l. Assumptions;
m. Dependency on other systems, service providers, and vendors, and their business continuity plans;
n. Public relations plan to maintain customer confidence;
o. Training and communications plan to ensure all personnel are well equipped to activate and execute the business continuity plan; and
p. Business continuity plan maintenance.

4.7.1.6 The AO shall incorporate business continuity management activities into their operations management plan.

4.7.1.7 The business continuity plan shall be reviewed for adequacy, completeness, and effectiveness at least annually or whenever significant changes occur to any element of the plan. In particular, the AO shall ensure that contact information and hardware and software configurations remain updated at all times.

4.7.1.8 The personnel in the recovery team shall be provided with adequate training to deal with the crisis.

4.7.1.9 The AO shall conduct regular testing of the business continuity and disaster recovery plans. These exercises are normally conducted on Saturday, Sunday or a Public Holiday. The testing shall include validating the readiness of the backup site.

4.7.1.10 The AO shall carry out the post-test review activities such as being involved in post-test review meetings and highlight areas of improvements in the business continuity plan as well as application operations to support business continuity.

4.7.1.11 The AO shall review and update the business continuity plan prior and after the test. The AO shall submit the updated plans and test reports to the Authority. Evidence of the review shall be documented for management's review.

4.7.2 Business Continuity and Recovery

4.7.2.1 Activation shall be initiated at such times when the primary site is rendered unavailable for a foreseeable extended period of two (2) hours. This includes, but is not limited to:

- A deliberate attack on the Primary site; and
- A natural disaster that disables the Primary Site.

4.7.2.2 The AO shall conduct a Business Impact Analysis (BIA) to determine the appropriate Recovery Time Objectives (RTO) and Recovery Point Objective (RPO). The BIA shall be submitted to the Authority, and the RTO and RPO shall be approved by the Authority prior to implementation. The Authentication Service shall be restored within the time specified by the RTO, and minimally to the point specified by the RPO.

4.7.2.3 The AO shall also ensure that the Authentication Service via the Internet is available despite disaster such as power failure at AO's site. The security and data integrity of the service shall not be compromised.

4.7.2.4 A recovery site geographically separate from the primary site must be established to enable restoration of critical systems and resumption of business operations in a timely manner should a disruption occur at the primary site.

4.7.2.5 For all service disruptions, the AO shall inform all affected service providers, and submit a preliminary incident report to the Authority within 24 hours. A post-incident review report shall be submitted to the Authority within three (3) working days. The post-incident review report shall minimally detail the cause of the incident, actions taken to address the disruptions, and steps taken where possible to ensure that such disruptions will not happen in future.

4.7.2.6 If a "hot" disaster recovery location is part of the Business Continuity Plan, it shall have security measures and controls equivalent to the actual site in place.

4.7.2.7 The AO shall provide a monthly system availability of at least 99.5% for the systems at the alternate site having the ability to support 50% of the Primary Site load at a service response time of one (1) second. Response time is defined as from the time the authentication request is received by the System to the time the authentication response leave the System. System availability shall be computed on the following basis:

- The computation of system availability shall commence on the day of resumption of service at the alternate site; and
- A system shall be deemed unavailable during the times when it's services are impacted by problems occurring in the alternate site or other parts (e.g. network) of the alternate infrastructure.

4.7.2.8 In the event that the Primary Site is restored, operations shall be swung back to the Primary Site. The AO shall plan an appropriate time for the swing-back, in consultation with its Service Providers and other AOs. The Service Providers reserves the right to bring forward or delay the swing back in consideration of the factors listed below or other factors where appropriate.

- Stability of the situation;
- Readiness of Primary Site;
- Appropriateness of timing; and
- Chances of the Primary Site being rendered unavailable again.

4.7.2.9 In the event that the alternative site becomes the Primary Site for the provision of the Authentication Service, the AO shall ensure that the Alternate Infrastructure is upgraded to meet the service levels defined in the Service Level Standards within two (2) calendar months, from the day the decision is made. The Alternate Infrastructure shall be of equal performance or better (in terms of user response time) than the Primary Infrastructure.

4.8 Service Level Standards

4.8.1 The Authentication Service shall be available to the subscribing service providers and end-users on a 24x7 basis including Saturdays, Sundays and Public Holidays.

4.8.2 All Authentication services must be completed in the systems within one (1) second for 99.9% of the time and within three (3) seconds for 100% of the time per month. The response time is defined as from the time the authentication request is received by the System to the time the authentication response leave the System.

4.8.3 The Authentication Service shall achieve at least 99.9% availability in any calendar month. The availability is defined as the availability of the Authentication Service to other AOs, service providers, and end-users, i.e. if other AOs, service providers and end-users are unable to access or use the

Authentication Service, the service would be deemed unavailable (excluding isolated connection problems occurring at the other AOs, SPs, and end-users).

4.8.4 All issuance/re-activation/re-issuance of credentials shall be completed within a reasonable time of receiving the request from the end-user. This shall include end-user identity verification, dispatch and receipt of the credential. Re-issuance of credentials will be required for expiry of credentials, or replacement requests due to loss or compromise of credentials.

4.8.5 For queries, feedback, and complaints received by the AO, the AO shall service all such issues within a reasonable time.

4.8.6 The AO's key personnel shall be contactable at all times by the Authority via pager or mobile phone and shall respond promptly.

4.9 Documentation

4.9.1 The AO shall ensure that proper documentation of the System, the changes made and the reasons or rationale for changes are recorded for traceability. This includes, but is not limited to, the following:

a. Asset records
b. Overall System Architecture Specifications;
c. Functional Design Specifications;
d. System Design Specifications;
e. User Guides / Training Guides;
f. Operational, backup & recovery policies and procedures;
g. Quality records e.g. progress reports, minutes of meeting, audit reports, system performance statistics, service requests, sales orders, and bills;
h. Processes and Procedures; and
i. Contracts and Contact Information.

4.9.2 The AO shall ensure that all proper documentation stated in **Section 4.9.1** are kept for at least seven (7) years.

4.10 Technical Standards

4.10.1 An AO shall comply, within a stipulated period, with any applicable mandatory technical standards that the Authority may, from time to time, publish on its Internet website.

4.11 Capacity Planning

4.11.1 The AO shall perform a business analysis to determine the threshold for resource utilisation that will serve as an appropriate trigger for a capacity upgrade, such that all additional requests for authentication services can be supported within a reasonable time. The AO shall also perform annual capacity planning to ensure adequate system resources being put in place promptly to meet the projected growth of business volume.

4.11.2 For all Service Providers' requests for authentication services, the AO shall service the requests within a reasonable time from their dates of requests. Having "serviced the requests" means that the end-users of the Service Providers can use strong authentication services via the AO.

4.11.3 Once the AO has decided to support Service Providers' requests for authentication services, the AO shall ensure adequate system resources for the new requests and the existing services already using the authentication services. The AO shall verify the adequacy of system resources by means of load simulation or other methods deemed appropriate. The AO shall have strategies or put in place measures to ensure that the system infrastructure is able to handle transaction volume without additional cost to the Service Provider.

4.12 Change in Management

4.12.1 An AO shall inform the Authority of any changes in the appointment of any person as its director or chief executive, or of any person to perform functions equivalent to that of a chief executive, within 3 working days from the date of appointment of that person.

4.13 Reporting

4.13.1 The AO must submit half-yearly reports to the Authority. The half-yearly reports must include information on:

a. the number of end-users subscribed to the AO;
b. the number of active end-users, which are defined by end-users that use the authentication service at least 3 times a year;
c. the number of new end-users per month;
d. the monthly breakdown on the number of end-users having each authentication mechanism offered by the AO (e.g. hardware OTP, SMS OTP, etc.). It is noted that a single end-user can be holding multiple authentication mechanisms from the AO;
e. the number of credentials issued, reissued, suspended, revoked, expired and renewed per month;
f. system performance including system up and down time (both scheduled and unscheduled) and any extraordinary incidents;
g. supporting documents that they meet the service level stated in **Section 4.8 Service Level Standards;**
h. security incidents encountered (both physical security and infocomm security);
i. successful and unsuccessful authentication transaction volumes per month;
j. changes in the organisational structure of the AO; and
k. changes in the particulars of any trusted person since the last submission to the Authority, including the name, identification number, residential address, designation, function and date of employment of the trusted person.

4.14 Discontinuation of Operations of AO

4.14.1 If an AO intends to discontinue its operations, the AO must arrange for its end-users and its service providers to re-subscribe to another AO. The AO shall provide all necessary assistance to facilitate another AO to successfully service its customers.

4.14.2 The AO shall make arrangements for its records to be archived in a trustworthy manner. The records shall be transferred to another AO, and the transfer must be done in a trustworthy manner

4.14.3 An AO shall

a. Give the Authority a minimum of 6 months' written notice of its intention to discontinue its operations;
b. Give its customers a minimum of 4 months' written notice of its intention to discontinue its operations; and
c. Advertise in such daily newspaper and in such manner as the Authority may determine, at least 3 months' notice of its intention to discontinue its operations.

Annex B

COMPILED LIST OF QUESTIONS

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?

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?

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?

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?

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?

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?

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

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?

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

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?

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?

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?

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.

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?

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

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.

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

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.

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?

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?

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?

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.

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

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.

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

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

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.

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

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?

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.

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?

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?

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?