NCS Pte Ltd
(Reg. No. 198101793G)
5 Ang Mo Kio Street 62
NCS Hub, Singapore 569141
Telephone: (65) 65568000 Fax: (65) 64834263

Public Consultation on Authentication Operators Framework

Date: 21 September 2008

NCS Pte Ltd
(Reg. No. 198101793G)
5 Ang Mo Kio Street 62
NCS Hub, Singapore 569141
Telephone: (65) 65568000 Fax: (65) 64834263

COMPILED LIST OF QUESTIONS

S/N	Question	NCS Comment/Feedback
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?	We agree that some form of regulation will help to ensure standards are upheld, provided the extent of regulation is balanced judiciously against any resulting increase for the AO(s) in terms of business cost and operational needs.
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?	We hope that IDA may consider the commercial viability and sustainability of AO(s) as one of the key policy objectives in addition to the rest already stated. It is vital for AO(s) to be able to garner sufficient transaction volume and growth to ensure that there will be long-term stability and availability of strong authentication services in Singapore. Re para 2.5 of the consultation paper, we hope that IDA will be able to share its market study findings in terms of potential market size by economic sectors, forecasted growth as well as price versus take-up rates corelation estimates if any. Will IDA be able to share information from the study about how much higer the take-up rate will be in a regulated AO regime versus an unregulated one ? Of interest is also the question of whether AO(s) will be restricted, under the proposed legislation/accreditation, to serve only one or a limited number of Service Providers. Also, whether AO(s) will be restricted to serving only Service Providers which are based in Singapore. There is much needed economy of scale for AO(s) to provide sustainable and affordable strong authentication services.

NCS Pte Ltd
(Reg. No. 198101793G)
5 Ang Mo Kio Street 62
NCS Hub, Singapore 569141
Telephone: (65) 65568000 Fax: (65) 64834263

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?	Commercial contracting between the parties. Self regulation based on the AO(s)'s vested interest to provide a well-accepted AO service so as to be a viable going concern.
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?	A voluntary accreditation scheme would be preferred to a mandatory licencing scheme, given the current uncertainty in the nascent AO market or the extent of demand for commercially available strong authentication services.
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?	As the accreditation framework (assumed to be a common framework), will cater to multiple key economic sectors, the sum of all the requirements should still be a baseline to meet a general usage level. Too high a requirement, or incorporating specific requirements from any particular sector, will skew the framework and increase the cost for the AO to provide the strong authentication services. We would like to further suggest to consider capping the number of AO(s) accreditated. Too many AO(s) will overly stretch the business case for each AO. IDA, in conjunction with other government regulatory authorities, may want to provide estimates of potential user-bases in the various identified spaces where AO services are mandated. This will also help facilitate right match of setup to scale the AO market to a matured status in an expedited manner.

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?	Should legal powers be deemed the appropriate means to accredit AOs, the Codes of Practice and Standards of Performance need to take into account the associated cost burden to the AO, as every mandatory requirement has a corresponding cost to be managed. One approach would be to define a skeletal and non-restrictive Codes of Practice and Performance Standards to ensure adherence to the fundamental principles, which the AOs can further refine and publish to suit both their operating business model and the target markets which they serve.
Q7.	Do you agree with the policy intent to provide legal certainty to AOs by expressly stating the conditions for liability exclusion?	If legislation is deemed necessary to regulate the AO, then it would be necessary for the AO to be accorded relevant liability exclusions, to ensure a balance of legal protection for the SPs, AOs, and Users, as well as to encourage AOs to be accredited. For strong authentication to serve its purpose, there are necessary responsibilities to be undertaken by all 3 parties involved in the transaction. This liability exclusion will help to limit the risks (and some costs) the accredited AO faces beyond its control.

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?	In addition to the proposed liability exclusions, considerations should be given to exclude the following: (1) Failure of service that is beyond the AOs reasonable control (e.g. Power failure, extensive WAN failure, 'Act-of-God' such as flooding,etc). (2) Consequential damages due to operating failure of the AOs, since such damages are difficult to quantify in advance, and the costs to mitigate such risks are prohibitive. (3) A reasonable cap on cumulative liabilities.
Q9.	Are the proposed penalties sufficient and appropriate for their corresponding contraventions?	One of the major cost component incurred by the AO would be a function of the penalties imposed (ie. to cover the risks in the event of a contravention), hence the higher the penalities, the higher would be the upfront costs needed to mitigate it. We would recommend that the imprisonment penalty be applied specifically for fraud and criminal offences only. We would recommend that the penalty of fines up to $50,000 are generally stiff relative to the revenue potential and liabilities of AO(s). This is especially so in the initial years of the service. We would also recommend more granularity in defining the contraventions and their corresponding penalties.
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?	Only if it is in accordance to prevailing laws which are relevant to such investigatigation and information acquisition. Clear measures on how the information so acquired will be protected for commercial and other interests must be made.
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.	The Security requirement specified is in priciple very comprehensive.
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?	ISO/IEC 27001 certification, due to its comprehensive 3-stage audit process, may create a barrier to entry for AOs as this certification process can be both involved and costly. More importantly, this certification requirement adds another layer to the accreditation process, and may discourage AOs from participation in the new and uncertain market. This requirement could be considered for future inclusion, once the AO market has matured.

Q15.	Can the proposed security requirements be further streamlined to facilitate AO's compliance without compromising the security of the authentication infrastructure?	We would recommend that in order not to limit the AOs to provide a cost-effective, yet appropriate security solution, adherance to standards should focus on international or open standards, without necessarily imposing a specific standard where possible. For example: Annex A 2.5.2.9 requires the storage of credential to include the ICAO standard as reference, implying the mandatory use of the ICAO standard, rather than as one possible standard to be adopted.
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.	The confidentiality requirement is in principle comprehensive and appropriate for the protection of sensitive information.
Q17.	Can the proposed confidentiality requirements be further streamlined to facilitate AO's compliance without compromising the protection of sensitive information?	Some clarity may be required for the following clauses: Annex A clause 3.1.5 pertaining to the collection of information, including day-to-day usage patterns. Whilst it is without a doubt necessary to ensure confidentiality of such information, the collection of such information may be inherent in the need to collect and maintain proper audit logs for the purpose of dispute resolution, and other such requirements. For Annex A clause 3.1.9, in the event a particular service transaction from a SP contractually requires the AO to provide value-added service, eg. added validation, or higher level of authentication, etc, the collection (but not disclosure) of such service transaction information may be necessary.

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.	Inter-connection can be complex, especially when multiple and diverse parties are involved, and will substantially increase the overall operating costs of AOs without necessarily ensuring the viability or sucess of the AO market. We envisage that a strong middleman role by IDA to provide a basic but well-defined framework for interconnection among AOs would be a crucial success factor.
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?	We would not recommend prescibing a competition code at this nascent stage, until some such time when the AO market has reached some maturity. We envisage the competition code would add complexity to both the initial AO business model as well as the business cost at the time when the market for commercial AO services is still uncertain.

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?	This has dependence on the proposed detailed framework for interconnection between AOs. On one hand, the inter-connection requirement will forge greater convenience to users, and so encourage more users to be favourable to using strong authentication services, thereby improving the overall security for Singapore e-commerce. On the other hand, inter-connection requirements add complexity at the back-end and a distinct overhead cost to the AOs, which either the SPs are not necessarily willing to defray, or that the transaction revenues may not cover for. Some certainty to the market size may help AOs to decide if the cost of interconnectivity and other operating costs will be viable to being an accredited AO. Another consideration is to simplify both the business and technical inter-connection requirement, without necessarily requiring "interoperation" or "federation" to be done at the backend.
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?	The technical standard to be defined by IDA therefore needs to be well defined (to minimise uncertainty) and yet sufficiently basic and flexible in order to grow with the increased sophistication and expectation of the market over time. Interconnection through "interoperation" or "federation" should not be a mandatory requirement in the initial standard, when the AO market and the AO players are in a flux.

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.	The credential lifecycle management is in principle appropriate for an accredited AO.
Q25.	Do you agree that AOs shall be responsible and accountable for credential lifecycle management?	AOs, by nature of being the credential provider, should have proper faciliities for credential management and hence have accountability for managing those credentials within the scope of the services provided. However, it is also necessary for the credential owner to have a corresponding accountability for their own credentials, including the need to inform the AO in case of any suspected loss or disclosure of those credentials.
Q26.	Can the requirements on credential lifecycle management be further streamlined to facilitate AO's compliance without compromising the strength of the credential?	We have no additional suggestion at this point. Depending upon the authentication technology used, some of the credential management considerations may need to be revisited.
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.	In principle, the proposed requirement to achieve continuity of authentication services are appropriate.

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?	As service providers will have contractual agreements with the AO pertaining to their specific SLAs and service continuity, an alternative is for the continuity arrangements to be managed via commercial agreements. IDA, playing a regulatory role, should make clear and published the required SLA, penalties and obligations of AOs. To have step-in rights to take over AO's operation may lead to conflicts of interest.

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.	With reference to Annex A clause 4.8.2, the response time of 1 second for 99.9% of the time may not always be commercially achievable depending upon the authentication mechanism supported, the level of interoperation, and other factors including the overheads of encryption or other security measures. As an example, an authentication request involving federated authentication, will require several back-and-forth data communication dialogue between parties as part of the federation protocol. It is unlikely in such an instance that this SLA can be met.
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?	If IDA's approval is required, the criteria for accreditation based on shareholding must be clear and made known so that the appropriate business considerations may be made prior to seeking accreditation.
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?	

NCS Pte Ltd
5 Ang Mo Kio Street 62
NCS Hub
Singapore 569141

NCS Pte Ltd
(Reg. No. 198101793G)
5 Ang Mo Kio Street 62
NCS Hub, Singapore 569141
Telephone: (65) 65568000 Fax: (65) 64834263

Contact #1
Jimmy Chua
Email: jimmyc@ncs.com.sg
Tel: 65566288
Handphone: 96219857

Contact #2
Ng Tong Seng
Email: tsng@ncs.com.sg
Tel: 65566147
Handphone: 96746088