



---

# **CONSULTATION PAPER ON THE ENACTMENT OF A LEGISLATIVE FRAMEWORK TO REGULATE AUTHENTICATION OPERATORS IN SINGAPORE**

**Submission by the StarHub Ltd to the Info-  
communications Development Authority of Singapore**

**21 September 2008**

Contact Details :	StarHub Ltd 51 Cuppage Road #07-00 StarHub Centre Singapore 229469 Phone +65 6825 5000 Fax +65 6721 5004  Tim Goodchild Email <a href="mailto:timothy@starhub.com">timothy@starhub.com</a>
-------------------	--

# **ENACTMENT OF A LEGISLATIVE FRAMEWORK TO REGULATE AUTHENTICATION OPERATORS IN SINGAPORE**

## **Introduction**

StarHub welcomes the release of the consultation paper on the regulation of Authentication Operators (“AO”) in Singapore. With the increasing acceptance of online services, and the consequential increase in online transactions, we believe that it is timely for IDA to review the regulatory framework for AOs.

Under the current environment, each online service provider manages its own strong authentication function. Going forward, some customers may wish to sign-up with a single AO and be able to access multiple services. We believe that the regulatory framework should not prevent this outcome, but should also avoid imposing unnecessary regulation on operators.

## **General Comments**

### **Balanced Regulation**

StarHub supports IDA’s objective to encourage market competition amongst AOs. However, as IDA itself has pointed out, the AO market is nascent, and therefore there is a need to strike a balance between regulating AOs and the burden (financial, operational and administrative) that such regulation would impose on AOs.

StarHub therefore believes that IDA should focus on ensuring that AOs provide minimum quality of services to end-users, in terms of security, confidentiality and service availability. We also believe that AOs outside of the “key economic sectors” (e.g. banking and finance, government and healthcare) should not be subject to additional regulation.

Further, we also submit that IDA must be willing to regularly review its regulatory framework to ensure that regulation remains appropriate to current market conditions.

### **Competition**

While we note that Sections 3.2.1 and 3.2.2 of the Proposed Industry Best Practices alludes to the concept of “dominant AOs”, there are stated no criteria by which “dominance” will be assessed or determined. StarHub would therefore propose that the criteria for dominance should be determined by market share. We would note that the Competition Commission of Singapore has stipulated a threshold of 60% market share for the presumption of Significant Market Power (SMP).

We believe that IDA can consider the same threshold as its criteria for determination of dominance.

### **Specific Responses to Consultation Questions**

StarHub has provided our comments to specific questions in the consultation document in this section.

**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 sector?**

StarHub accepts that AOs in certain, defined, “key economic sectors” (e.g. banking and finance, government and healthcare) should be subject to regulation. However, we would note three points:

- First, we do not believe that AOs outside of the “key economic sectors” should necessarily be subject to regulation. We can see little evidence of market failure or public policy reasons to justify such regulation.
- Second, it is important to understand that imposing additional heavy regulation on AOs will discourage their establishment, and will limit the growth of the sector. This would, in turn, reduce the competitiveness and efficiency of AOs in Singapore. We strongly believe that a “light-handed” regulatory regime is needed for this sector.
- Third, IDA should not under-estimate the importance of contractual measures to ensure that Service Providers receive the services they need. The consultation paper suggests that, if left unregulated, AOs will provide an unreliable service, and Service Providers will be powerless to prevent this. In practice, matters such as security, confidentiality, reliability, availability, and service level standards can all be addressed via the contract between the AO and the Service Provider, and the AO can be provided with the necessary incentives to provide a reliable service. In fact, given that contracts can be customized for the particular transaction between the AO and the Service Provider, contractual solutions may be a more effective solution than a “one-size-fits-all” regulatory measure.

---

**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?**

StarHub supports the policy objectives as stated in the consultation document for defined “key economic sectors”. However, we believe that “key economic sectors” should be limited to the narrowly-defined Banking, Government and Healthcare sectors. We do not believe that these policy objectives should be applied to AOs outside of the “key economic sectors”.

---

**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?**

We would highlight the importance of the contractual arrangements between Services Providers and AOs in ensuring adequate performance by AOs. Matters such as security, confidentiality, reliability, availability, and service level standards can all be addressed via the contract between the AO and the Service Provider. Contracts can also be customized to meet the particular needs of the parties, in a more flexible manner than regulation or legislation can.

We would also note the importance that AOs will attach to their business reputations. If AOs are seen to be unreliable in their services, operating in a manner that disrupts services to Service Providers, they will be endangering their future viability. AOs will already have very strong incentives to ensure they deliver a reliable service to the Service Providers.

---

**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?**

StarHub believes that “light-handed” regulatory solutions, such as accreditation, are appropriate for regulating AOs in “key economic sectors”. In other sectors, we do not believe that regulation is warranted, at this point in time.

---

**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?**

StarHub believes that an accreditation scheme is an appropriate instrument at this juncture.

---

**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?**

StarHub agrees that IDA should be accorded sufficient powers to regulate the AO industry. However, we would submit that, in developing Codes of Practice and Standards of Performance, it is important for IDA to also seek the opinions of AOs. This will help ensure that the Codes of Practice and Standards of Performance developed are able to meet the requirements of the various sectors, as well as reflect the operational challenges faced by AOs.

---

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

StarHub would not recommend specifying the liability provisions that will apply between AOs and their Service Providers. Liability is an important commercial consideration between contracting parties. If the conditions of liability exclusion are mandated by IDA, this may restrict the ability of the parties to negotiate on this issue.

---

**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?**

As noted above, StarHub would not recommend specifying the liability provisions that will apply between AOs and their Service Providers.

---

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

StarHub would note that a regime based on heavy penalties may discourage entry into the Authentication industry. We would therefore suggest that penalties should be limited in the nascent stage of the industry.

---

**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?**

We believe that the proposed general powers to be accorded to IDA are comprehensive and appropriate.

---

**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?**

StarHub believes that IDA should have the power to request for information from AOs from time to time. We further support the proposal that this should only be done when IDA considers such an exercise necessary in the public interest, so as not to place an undue administrative burden on AOs.

---

**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?**

StarHub agrees that for consistency, the relevant sections of the ETA should be amended to allow IDA to be the single entity to regulate both CA and AO regimes. Given the close linkage between both regimes, we believe that it is practical to give IDA regulate oversight over both regimes. We would submit that this will provide for more efficient regulation.

---

**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.**

StarHub would suggest that the security requirements on AOs should vary, depending on the sensitivity of the information and the importance the Service Provider. We would respectfully suggest that the proposed security requirements would not be appropriate for all AOs, and that a more variegated system of requirements might be more appropriate.

---

**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 protocols, encryption, and digital signing? If not, how else can security assurance be achieved?**

We would respectfully suggest that it should not be necessary for all AOs to be ISO/IEC 27001 certified. Such certification should only be set on those AOs carrying our particularly sensitive roles.

---

---

**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.**

Again, StarHub would be concerned by a “one-size-fits-all” approach to confidentiality. Confidentiality requirements may well vary from sector-to-sector, in line with the information collected by the AOs. We believe that there are certain confidentiality principles (such as those set out in Section 3.2.6 of the Telecoms Code) which should apply to all regulated AOs. However, we believe that more detailed obligations on AOs may be inappropriate.

---

**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 competition? 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 behaviours? 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?**

StarHub believes that it is important to establish a competition code from the outset. StarHub agrees that this will provide legal certainty in the accreditation scheme.

Further, StarHub believes that in an environment where competition is developing, there is a strong likelihood for disputes to arise. In such circumstances, we believe that a clear framework for dispute resolution and enforcement must be in place to ensure that disputes and/or breaches can be swiftly dealt with.

---

**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.**

StarHub would support the proposed disclosure and liability requirements.

---

**Q27. Are the proposed requirements to achieve continuity if authentication services comprehensive, appropriate and sufficient to minimize 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?**

StarHub would suggest that business continuity is a commercial matter between the AO and its Service Providers. As such, we would suggest that it not be subject to regulation.

---

**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 that availability of AO services?**

Providing IDA with step-in rights is likely to be seen very negatively by potential AOs, and may well discourage entry into the Authentication market. StarHub would suggest that step-in rights should not be granted.

---

**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 take place?**

StarHub would not support an obligation for AOs to obtain IDA's approval for changes to their shareholding. Such an obligation will slow the AO and reduce its commercial flexibility. Given the nascent nature of the authentication industry, we are unable to see a policy justification for setting this obligation.

---

**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 may have been covered in your responses to the questions above?**

StarHub believes that AOs are likely to vary considerably in size and importance to the economy. The authentication industry is still evolving, and its growth could be impaired by heavy regulation. StarHub therefore believes that, at this point in time, only AOs in "key economic sectors" should be subject to regulation, and that the sector regulator should take a light-handed approach to regulation of AOs.

## **Summary**

StarHub supports a review of the regulatory framework for AOs. However, we believe that there is a need to strike a balance between regulation and consumer protection, whilst ensuring that AOs are not faced with a heavy administrative burden. This balance is particularly important, given the developing nature of the authentication industry.

We believe that it is important to give AOs some level of certainty as to their operating environment. However, in order to facilitate the growth of the industry, we would encourage IDA to engage the industry players, and to implement a light-handed regime for AOs.