Response to NAF Consulting Paper

Author: Tan Chuan Jin Email: chuanjin.tan@atosorigin.com
Yeo Chien Jen Email: chienjen.yeo@atosorigin.com
Version: 1.3
Document date: 21 September 2008

Contents

1 Responses to IDA Consulting Paper

1.1 Policy Objectives of Legislation to Regulate Authentication Operators

We agree to a certain extent on the need to regulate AOs. However, the form of regulation could be based on the proposed accreditation framework described in Part 5. This form of self-regulation would be more flexible and effective. These objectives should take into consideration key principles similar to the Model Code in the Trust SG programme, established by the National Trust Council for businesses that engage in sound e-commerce practices, including data protection. Please refer to the following links for more information on online authentication services:

1. Article 29 Data Protection Working Party, Working Doc on on-line authentication services (Adopted 23 Jan 2003): http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf
2. NZ eGovernment Online Authentication Programme: http://www.e.govt.nz/archive/services/authentication/Online%20authentication

This policy also provides an opportunity to create a wider trust framework that will allow different Service Providers and Identity Providers/AOs to have a structured trust relationship with one another. Establishing shared trust between different organizations has always been a significant challenge in the development of federated identity solutions and the creation of a trust framework formalises an approach that could be appropriate to a variety of different shared services and information sources across Singapore.

In UK, the government uses an independent regulatory body, tScheme, for accreditation of trust for both Identity Providers (similar to AOs) and Service Providers. Any third party providing registration and authentication services to support e-Government transactions must be approved under a scheme recognized by the UK government such as tScheme. http://www.tscheme.org/

Please refer to following link for more information on Registration & Authentication Framework v 3.0
http://archive.cabinetoffice.gov.uk/e-envoy/frameworks-authentication/$file/authentication.htm

1.2 Regulating Authentication Operators via Accreditation

The proposed accreditation scheme similar to the current voluntary licensing scheme for Certificate Authorities under the Electronic Transacions Act would be appropriate to start with.

This approach is appropriate and has a number of benefits including the provision of a single referenceable standard that can be adopted and audited on a widespread basis t-Scheme is the UK electronic trust service self-regulatory body and a variety of auditors, such as KPMG, compete in the market to deliver the accreditation.

In UK, the tScheme framework is used to provide the accreditation of both the Service Provider and the System (including processes). Specific service profiles will be used to achieve the service assurance, while the application of a BaseProfile and ISO27001 Statement of Applicability (SoA) will act as the basis for assurance in the service delivery.

1.3 Proposed Legislations for the Regulation of Authentication Operators

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

In principle, we agree 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. However, would prefer to be able to participate in the consultation process in the development of such Codes of Practice & Standards of Performance.

1.3.2 Exclusion of Liability for Accredited AOs

In principle, we agree but would prefer to be able to participate in the consultation process in the development of liability exclusion

The following are situations which IDA should consider to exclude AOs for liability;

1. Service Providers incorrectly stating their level of authentication requirement to AO.
2. Service Providers misinterpreting the SAML assertion and providing incorrect access to the e-service.
3. Registration authority not conforming to process when registering/enrolling users.
4. Smart cards being modified with the addition of photos or other applications such as PKI certificates, which impacts upon their operation for the AOs.
5. Forged credentials are used that are beyond AO's reasonable means of detection;
6. End-users failing to adequately safeguard their credentials
7. Any delays or prevention of access of online services due to the AO's not receiving the authentication request, provided that it is beyond the AO's reasonable control.
8. Attacks that two-factor authentication is unable to address or be protected from, such as Man-in-the-Middle or session hijacking attacks on end users.

1.3.3 Regulatory Enforcement Powers

The proposed penalties appear to be inconsistent with the consideration of the accreditation framework for consequences of failure which may be less significant and thus would not be held to the same high standards of operations as expected of AO's serving key economic sectors. The right of appeal to an impartial adjudication body where an AO feels it is wrongly penalised or who feel aggrieved by IDA's decisions or directions should be included.

1.3.4 General Powers

General powers should be exercised with minimal disruption to the normal business operations of the AO and with reasonable prior written notice where possible to ensure the AO is given a reasonable opportunity to comply. The right to appeal to an impartial adjudication body should also be applicable to the IDA's exercise of power.

We agree in principle that IDA has the power to request for information from AOs as long as there is a mechanism built into the IDA’s SOPs to ensure that:

1. the request does not cause the AO to incur any unnecessary and unreasonable costs;
2. there is minimal disruption to the normal business operations of the AO and
3. with reasonable prior written notice where possible to ensure the AO is given a reasonable opportunity to comply.

The right to appeal to an impartial adjudication body should also be applicable to the IDA's exercise of power.

1.3.5 Proposed Amendments to ETA

IDA should be the single entity to regulate both CA and AO regimes as long as the spirit of the accreditation framework is maintained to allow appropriate controls for non-critical sectors or small pockets of demand cf. key economic sectors.

1.4 Best Practices for Compliance by Accredited Authentication Operators

1.4.1 Security Requirements

ISO 27001 forms the baseline for international security standards, and being a certified operator signifies the commitment towards information security by the Authentication Operator. An Authentication Operator should be ISO 27001 certified in order to handle the project, providing the best security practices.

1.4.2 Business Requirements

1.4.2.1 Confidentiality

Authentication Operators should ensure sensitive information is not disclosed through extracting error logs and submitting to solution/product vendor for troubleshooting. Error logs should be sanitized and kept to the minimum when there is a requirement for data or information to be removed from the secured production facility.

1.4.2.2 Competition and Interconnection

Proposed solutions should use open standards such as SAML 2.0 assertions to confirm the authentication of user with service provider, including any attributes about the user. Processes can also be put in place to ensure that the migration of users (without the need to reissue cards) can be completed from one Identity Provider/AO to another.

When identity provider and authentication operator are separate entities, it presents a challenge to maintain the trust between the identity provider and the authentication provider. Basic requirements such as secure WAN links must be deployed and further customization is required to modify the solution to build in some form of validation to determine the authenticity when the transactions request for second factor authentication services.

Alternatively, the identity provider and authentication operator may require consolidating their authentication infrastructure into a single physical location or data centre.

We agree the need to prescribe a competition code to prevent anti-competitive behaviours, and this should be prescribed from the onset

1.4.2.3 Disclosure and Liability

The details of the liability requirements should be discussed in more detail as these may require corporate approvals if there is any deviation from the AO's corporate policy on limits of liability, indemnities, dispute resolution process and liquidated damages. There is a need to consider where liability sits in the case of the registration authority process (i.e. the Identity Provider) becoming non-compliant. In the UK this would incur a downgrade of the Trust Maturity level. The extent of the Trust Maturity downgrade will depend on the nature and impact of the fault. Thereafter, assertions from that Identity Provider organisation would continue to be accepted by the Trust Broker, yet stamped with the downgraded Trust Maturity level. Authorisation decisions remain with the Service Provider based on a combination of knowledge of Trust Maturity level and of the organization.

We propose further consultation on establishing the guidelines and model forms of disclosure on IDA's website for use by the AO's on their website to ensure consistency and to enable streamlining.

1.4.3 Operational Requirements

1.4.3.1 Credential Lifecycle Management

Authentication operator should include issuance, suspension and revocation of credentials in order to provide efficient services. This allows flexibility for the operator to develop their own process to integrate with the proposed solution.

1.4.3.2 Continuity of Authentication Services

Atos Origin primary production data centre is located at Suntec City Tower 3. The Data Centre is a tier III facility and houses more than 100 racks of critical business systems for our clients and manned 24x7x365 by our operational staff. It offers comprehensive facility infrastructure, redundancies and necessary security to meet hosting requirements.

The Disaster Recovery data center is located at SingTel Complex at Telepark. This facility is a purpose built complex for high technology industries. 24-hour technical support is available on site in the event of incidents and alerts. Regular maintenance contracts are in place to service and provide breakdown repair for UPS, Air-conditioning and Fire Protection equipment. The building is a high security with strict access restrictions. Only authorized personnel by Atos Origin are granted access to the facility. Our services will meet the requirements of a reliable service provider for IDA.

Atos Origin UK's implementation for the UK Government Gateway UK solution is based on the use of open standards including OATH tokens and APACs CAP Smart Cards. This means that the credential may be treated more like a commodity and different suppliers selected on price. However it is noted that some functionality such as PIN management on a SMART card is not provided by the APACs CAP standard so some customization is required.

1.4.3.3 Other Operational Requirements

IDA can be informed when there are changes to the staffs supporting or maintaining the AO operations, and can provide inputs and raise any concerns on the suitability of these personnel before deployment.

1.5 Other Comments

Has thought been given as to the Service Provider accreditation and self-certification?
In UK each Service Provider (Government organisations only) will go through its own Government department's system accreditation process.

This scheme service registration is envisaged to be a simple functional self certification (e.g. in the form of a questionnaire). Service Providers are requested to complete self-certification and demonstrate they have an appropriate access control model in place to allow them to properly interpret and use the SAML assertions. Atos Origin UK provides a service to test against prior to joining the scheme.

Service Providers will need to complete a functional accreditation against this test service prior to connection to the live service.