INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE
8 Temasek Boulevard #14-00 Suntec Tower Three Singapore 038988
Tel (65) 6211 0888 Fax (65) 6211 2222 www.ida.gov.sg

FACT SHEET
(June 2010)

NATIONAL AUTHENTICATION FRAMEWORK

The National Authentication Framework (NAF) seeks to realise the vision of the iN2015 masterplan for a secure and trusted enabling infocomm infrastructure that can facilitate the delivery of online services offered by the public and private sectors.

With the increased availability of online services offered by key sectors such as banking & finance, Government and healthcare, NAF can safeguard against unauthorised access to sensitive information, such as bank account numbers or electronic health records. The NAF will be a timely nationwide strong authentication infrastructure that can provide consumers greater assurance when performing online transactions.

The NAF aims to facilitate a nationwide common platform for strong authentication that will:

a. Enable consumers to enjoy the convenience of using a single authentication device to access multiple online services that require strong authentication;

b. Enable businesses to enjoy cost savings when they leverage on NAF instead of implementing their own strong authentication systems;

c. Boost online trust and confidence, thus helping to entrench Singapore’s status as a trusted infocomm hub; and

d. Enhance protection against online identity theft for online services for both consumers and online business owners.

The NAF RFP

IDA has launched the Request for Proposal (RFP) to appoint an Outsourced Operator to design and build the NAF infrastructure. Upon completion of infrastructure set up, the Outsourced Operator will operate and maintain the NAF infrastructure and perform the day-to-day operations of the NAF services. The RFP Documents are available on GeBIZ (www.gebiz.gov.sg). The closing date for submission of proposals to this RFP is expected to be on 8 July 2010.

About Authentication

Authentication is a process of validating a person’s identity for security purposes. There are three recognised factors of authenticating individuals: “Something you know”, such as a password or PIN, “Something you have”, such as hardware security token, and “Something you are”, such as a finger print, a retina scan or other biometric. A system is said to use strong authentication when it requires at least two of the three factors before access to the system is granted. This contrasts with traditional single-factor authentication which requires only one authentication factor (normally the knowledge of a password) in order to gain access to a system.

Two-Factor Authentication (2FA): Currently available as a more rigorous process of validating identities. A popular second-factor authentication method that many banks are offering to their online consumers today is One-Time Password or OTP. When a user accesses an online service, in addition to User-ID and Password, the user would be required to enter an additional “second factor password”, which is generated on demand. The dynamically-generated “second factor password” could be delivered through a token (hardware or software) or via SMS. Other types of authentication methods include certificates and biometrics.

Service providers are today deploying their own two-factor authentication infrastructure. As a result, an authentication device or method tends to be proprietary and can only be used to access specific online services.

FOR MORE INFORMATION, PLEASE CONTACT:

Ms Felicia Yeo, Manager, +65 6211 1536, felicia_yeo@ida.gov.sg

Mr Sheo S. Rai, Assistant Director, +65 6211 1073, sheo_s_rai@ida.gov.sg