INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE
8 Temasek Boulevard #14-00 Suntec Tower 3 Singapore 038988
Tel : 65-62110888 Fax : 65-62112222 www.ida.gov.sg

**June 2008**

# FACT SHEET

# National Authentication Framework

## Aim

To realise the vision of IDA's iN2015 masterplan, a secure and trusted enabling infocomm infrastructure is needed to facilitate the delivery of online services offered by the public and private sectors. The National Authentication Framework (NAF), spearheaded by the Infocomm Development Authority of Singapore, with support from the Monetary Authority of Singapore and the Ministry of Finance, will be a nationwide platform where consumers can enjoy:

a. consistent experience in using strong authentication to access key online services (e.g. In Government, Finance, Healthcare).

b. A more rigorous process of verifying online identities.

## 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.

## How NAF Works

**A Nationwide Deployment 2FA:** When the National Authentication Framework (NAF) is implemented, online service providers such as government agencies and financial institutions will be able to outsource their second-factor authentication infrastructure to trusted third parties (also known as the Authentication Operators or AOs). AOs are free to offer multiple authentication devices and methods, depending on market needs. Consumers can hold more than one authentication device (e.g. a security token or an SMS OTP). However, regardless of the device a consumer chooses to use, that chosen device can be used to access multiple online e-services that require strong authentication. Consumers can thus benefit from the enhanced security of strong authentication without the inconvenience of having to carry multiple devices.

**Call for Collaboration:** To catalyse the deployment of NAF, IDA intends to invite the industry to participate in the upcoming Call-for-Collaboration (CFC). The CFC is expected to be launched in the second half of 2008 and will seek industry partners to operate as Authentication Operators.

## Numbers to Note

Initial demand drivers of NAF are likely to come from the Government sector. Government initiatives such as SingPass[1] and Standard ICT Operating Environment[2] will leverage on NAF, where stronger (i.e. second-factor and beyond) authentication is required.

Currently, about 40 Government agencies authenticate users with SingPass for access to some 370 e-services requiring user-authentication (User-ID and Password). Since its launch, the total volume of SingPass authentication transactions have increased from 4.5 million in 2003 to 18.9 million in 2006, representing a more than three-fold increase in usage over four years. The SingPass system today has three million registered users. Government e-services that have stronger authentication needs due to a change in their business requirements would be able to leverage on NAF for the second factor authentication. With the implementation of SOEasy, more than 60,000 public officers will enjoy a robust, connected, innovative and agile infocomm environment. SOEasy will also improve overall operational efficiency in the public sector. SOEasy services requiring strong authentication could leverage on NAF for its strong authentication needs.

[1] For more information on SingPass, please refer to SingPass Fact Sheet at http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20071105103244/SingPass5Nov07AnnexA.pdf

[2] For more information on SOEasy, please refer visit http://www.ida.gov.sg/News%20and%20Events/20080228151049.aspx?getPagetype=20

Another potential demand driver could be financial institutions. There are about three million internet banking customers in Singapore in 2007. A media report on a local bank noted that after it implemented 2FA, the total number of online banking transactions, and the average dollar value transacted per customer increased by 20 per cent and 50 per cent respectively[3]. Financial institutions (e.g. banks, securities, insurance) seeking to increase the adoption of their online channels could leverage on the NAF, instead of building their own.

The NAF is also expected to grow in tandem with the introduction of more Next Generation Services enabled through the deployment of the Next Generation National Broadband Network from 2010 onwards.

**FOR MORE INFORMATION**
**IDA Communication Contact:**

-Ms HO Hwei Ling, Assistant Director, +65 6211 1996, ho_hwei_ling@ida.gov.sg

-Mr HO Ka Wei, Manager, +65 6211 0273, ho_ka_wei@ida.gov.sg

[3] Source: “Online banking draws more Singaporeans,” The Business Times, 18 June 2007.