**FACT SHEET**
**(January 2011)**

## Assurity Trusted Solutions

A wholly-owned subsidiary of the Infocomm Development Authority of Singapore (IDA), Assurity Trusted Solutions (Assurity) serves as the National Authentication Framework (NAF) operator for 2nd Factor Authentication (2FA), set up to offer NAF 2FA services to Service Providers (SPs) and consumers at a national level.

Assurity is expected to roll out its service to SPs starting from the second half of 2011. ST Electronics (Info-Security) has been appointed to design, build, operate and maintain the NAF infrastructure for Assurity.

### Establishing the National Authentication Framework

Assurity seeks to realise the vision of IDA's 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.

The management of Assurity reports to their Board of Directors which include senior management staff from IDA, public and private sectors. They will be responsible for charting corporate strategy, performing a supervision function and ensuring that Assurity's operations comply with Board approved policies and are consistent with sound and prudent practices.

As Singapore steadily transforms itself into a vibrant and connected global city, online services offered by key sectors such as banking and finance, Government and healthcare have become increasingly accessible.

Assurity aims to:

a. Give consumers the convenience of a single authentication device to access multiple online services;

b. Enable businesses to enjoy time and cost savings when using NAF instead of implementing their own authentication systems;

c. Safeguard against online identity theft on a national level and inspire greater online confidence and trust, thereby enhancing Singapore's status as a secure infocomm hub.

**Two-Factor Authentication (2FA)**

Authentication refers to the process of validating a person's identity for security purposes. Currently there are three recognised ways of doing so:

- Something you know, such as a password or Personal Identification Number (PIN)
- Something you have, such as a hardware security token or card
- Something you are, such as biometric data, like a fingerprint or a retina scan

Assurity adopts the more rigorous process of two-factor authentication, also known as strong authentication. This contrasts with traditional single-factor authentication that requires only one authentication factor, usually the knowledge of a password, to gain access to a system.

An example of a popular second-factor authentication method that many banks offer online consumers today is the One-Time Password or OTP. When accessing an online service, consumers are required to enter an additional password generated on demand, which is delivered through a token or SMS.

For more information, please contact:

Angeline Zheng
Executive Assistant
DID: +65 6211 0166

Fiona Khong
Executive Assistant
DID: +65 6211 1683

Email: *info@assurity.sg*