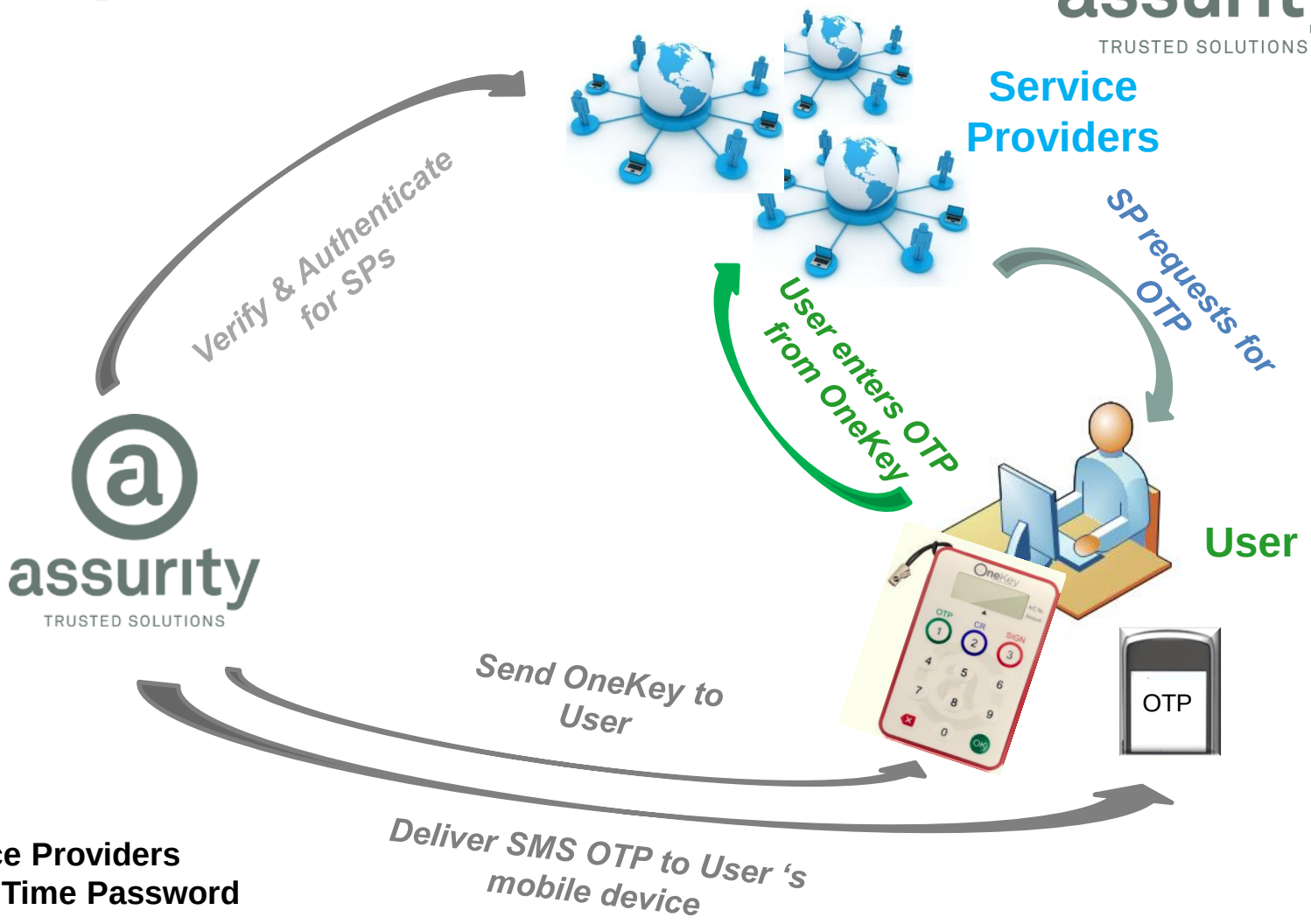
Secure Online Transactions

One Person One Token

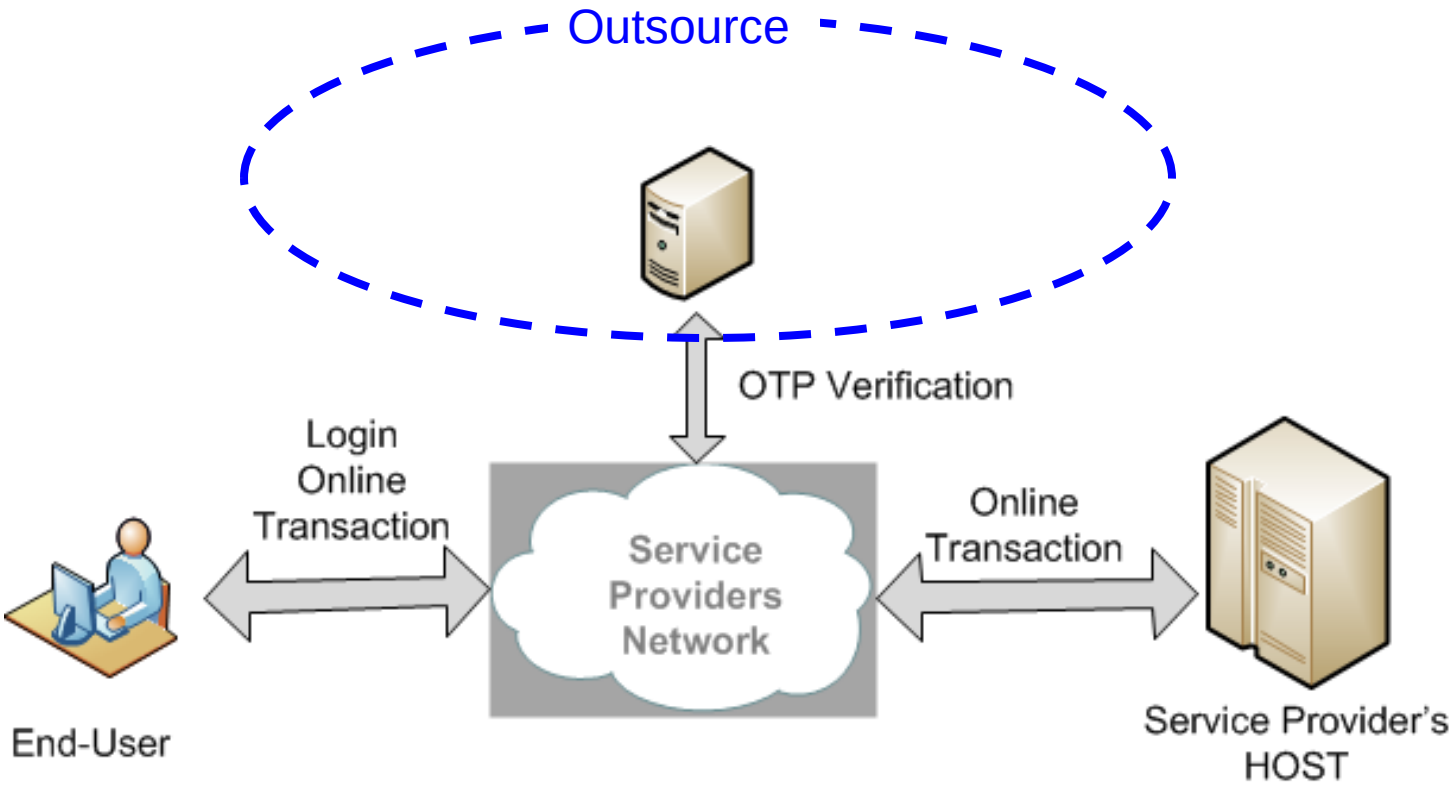
assurity
TRUSTED SOLUTIONS

Assurity's Service Model

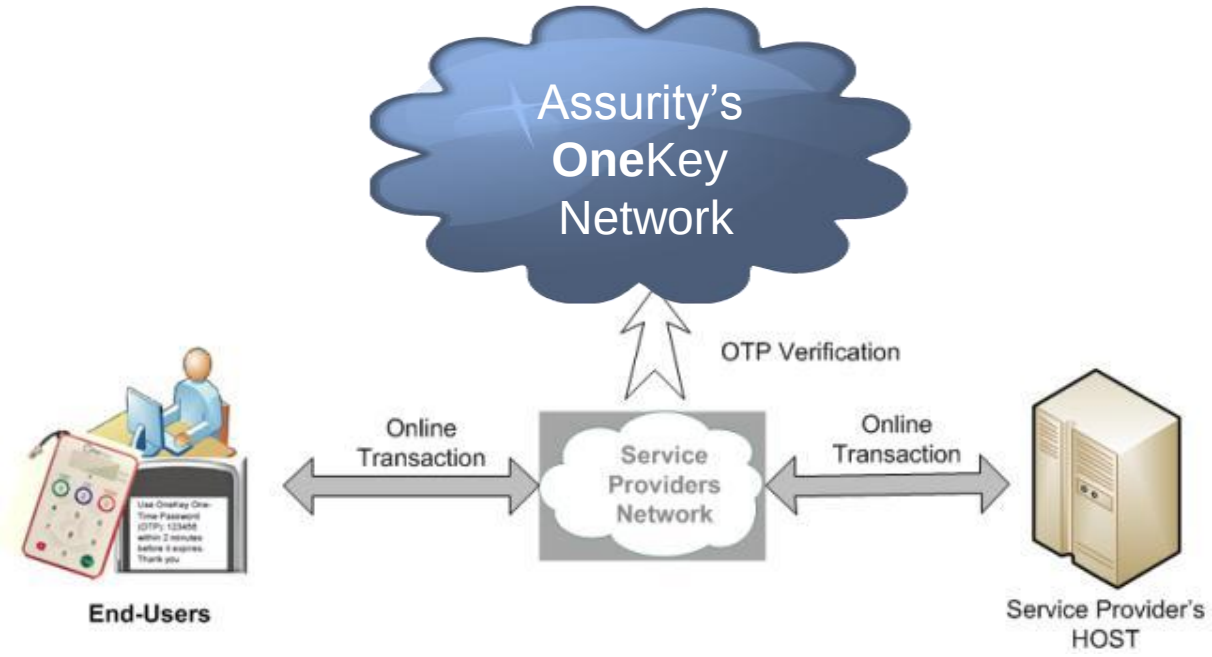


SP – Service Providers
OTP – One Time Password

Service Provider's OTP Setup

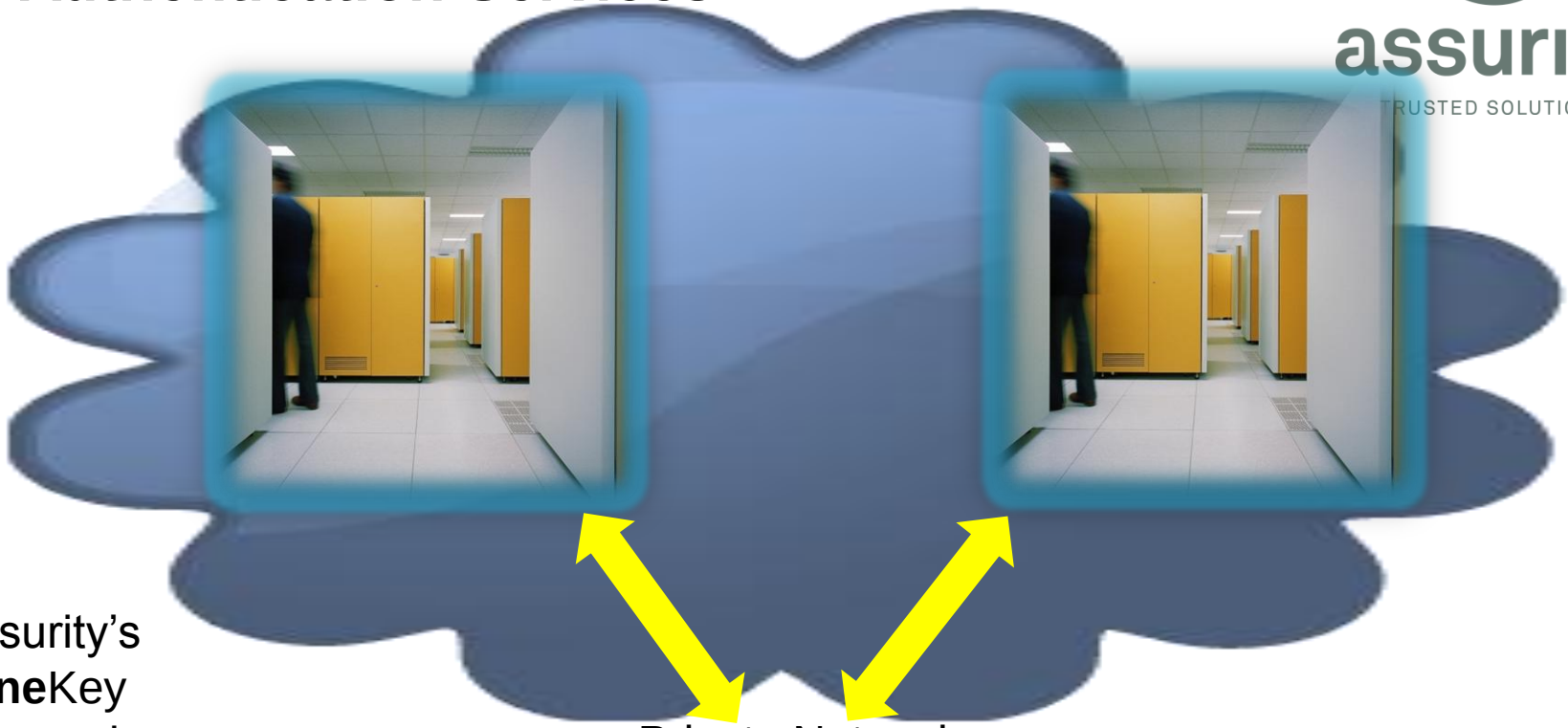


Service Providers Subscribe to Assurity's Authentication Services



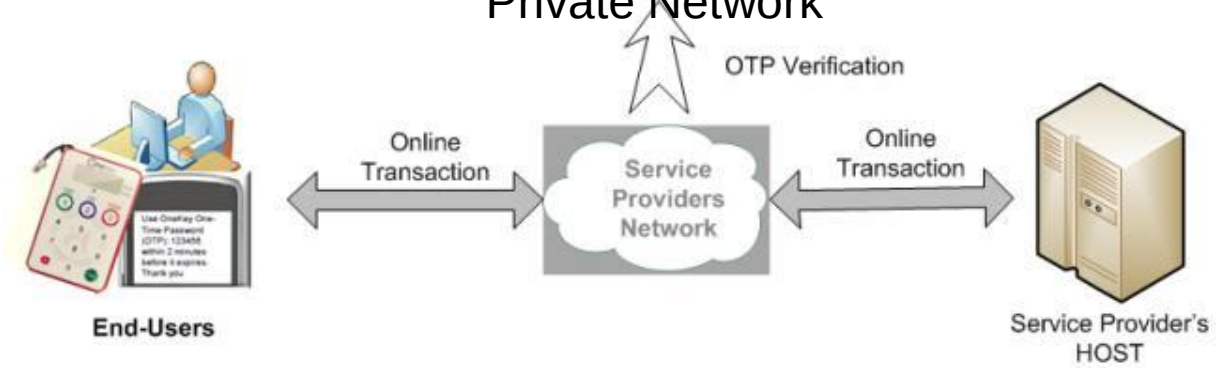
Service Providers Subscribe to OneKey Authentication Services

assurity
TRUSTED SOLUTIONS



Assurity's **One**Key Network

Private Network



Incorporating OneKey in SP's Portal

Registering and linking OneKey

Users need to do a one-time **registration** for their **One**Key and then **link** their **One**Key to their account. Both actions should be done at the SP's portal.

On log-in to SP's portal, user will see the following two links:

Register for your OneKey

User gets redirected to Assurity's online registration page

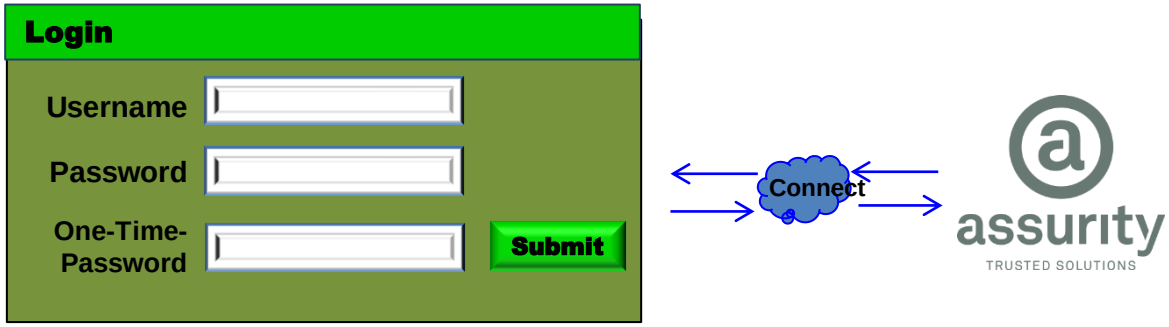
Link my OneKey

Clicking this links user's account to **One**Key

Incorporating One**Key in SP's Portal**

OneKey enables Service Providers to provide strong authentications

Before **One**Key is incorporated

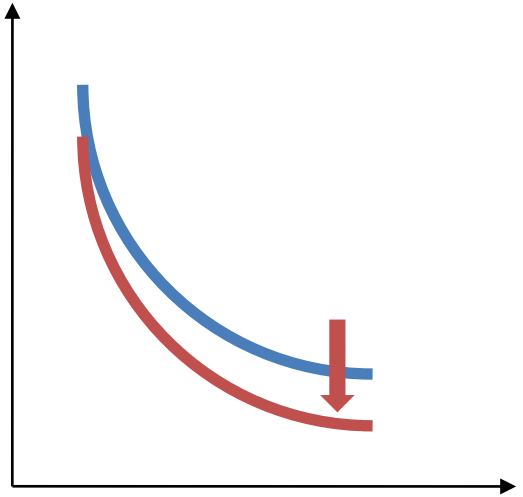


After **One**Key is incorporated

Service Provider Log-in Page

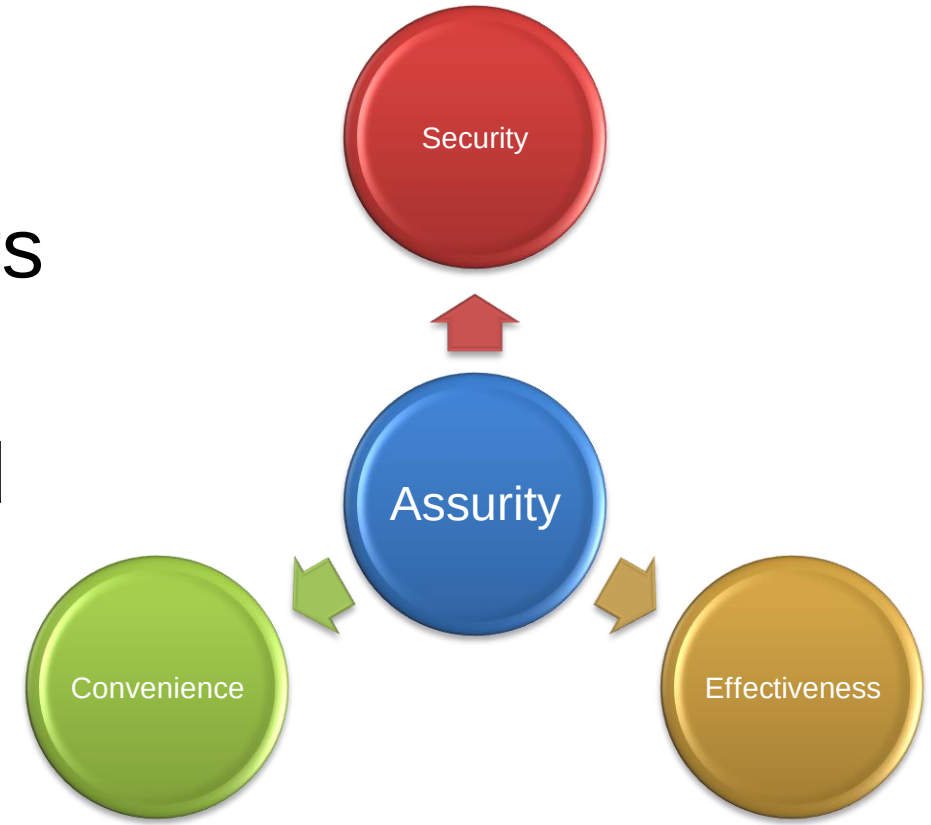
Motivations Behind NAF

- **Aggregate** the needs for securing authentication to **minimise** cost
- **Consolidate** infrastructure to **maximise** utility
- **Innovate** our infrastructure to bring **additional value** to enhance the competitive edge of businesses



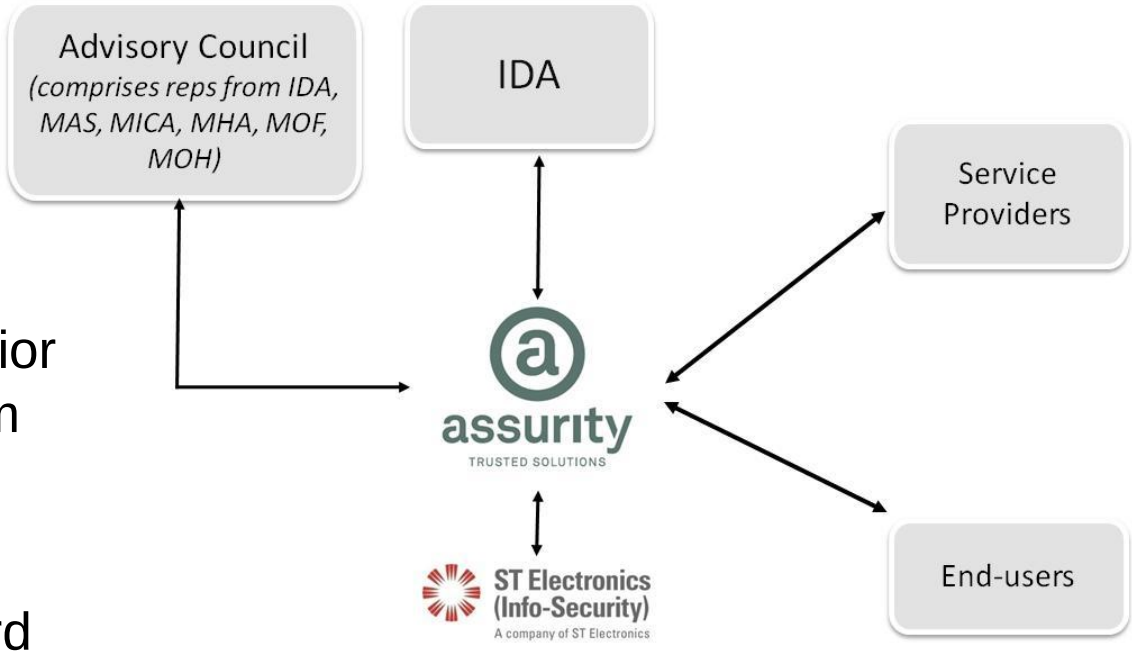
Operating Ethos

- **Security** of online transactions
- **Convenience** to users
- **Effectiveness** in function, purpose and cost



NAF Governance Model

- Trusted infrastructure
  - A subsidiary wholly owned by IDA
  - Assurity's Board of Directors includes senior management staff from IDA, MICA and MOHH
  - Overseen by IDA Board
  - Advisory Council comprising senior management representatives from IDA, MAS, MOF, MICA, MHA and MOHH to act as a focal point to harmonise strong authentication development across respective sectors



Challenges

- Changing security threats, such as breaches of:
  - Trusted devices e.g. RSA, root CAs
  - Users' security e.g. APT, Zeus
  - Hardened infrastructure
- Adoption of 2FA by service providers
  - Beyond banks
- Adoption of 2FA by end users
  - Individual responsibility for cyber security

Some Reference Materials

assurity
TRUSTED SOLUTIONS

- US National Strategy for trusted Identities in Cyberspace http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
- Australia's "National e-Authentication" Framework http://www.finance.gov.au/e-government/security-and-authentication/docs/NeAF-framework.pdf
- Bahrain's NAF http://www.ega.gov.bh/wps/wcm/connect/30ce1b80487c4a05b62bbf0304bf950d/NAF.pdf?MOD=AJPERES&CACHEID=30ce1b80487c4a05b62bbf0304bf950d
- NPS NAF Thesis http://www.dtic.mil/dtic/tr/fulltext/u2/a514358.pdf
- Estonia's Mobile-ID http://e-estonia.com/components/mobile-id

chinloon@assurity.sg