Singapore update - 2014

(17-18 Apr 2014 – Asia IC Card Forum @ Seoul, Korea)

Mr. LIN YIH

email: dartpl@singnet.com.sg

Chairman, Cards and Personal Identification Technical Committee

Singapore IT Standards Committee

* Convenor, ISO/IEC JTC1 SC17 WG11 “Biometrics”

* Director, Digital Applied Research and Technology Pte Ltd

an industry partnership supported by SPRING Singapore and IDA

Items from 2013 Sep 24 in Singapore

- Submit printed copy of SS518 : 2006 “CEPAS” to Korea and Japan representatives, for future discussion of standards work in AICF
- Singapore hosted ISO/IEC JTC1 SC17 work group and plenary meetings (2013 Sep 23 - Oct 4)
- NFC CEPAS PlugFest and CEPAS v3.0 meetings should start in Q3 2014
- Update of Singapore’s NAF (National Authentication Framework) project (more info later)

ISO/IEC JTC1 SC17 WG and Plenary

- Singapore hosted ISO/IEC JTC1 SC17 WG and Plenary, 2013 Sep 23 to Oct 4 (total about 160 people over 2 weeks)

CEPAS (SS518:2006 Contactless e-Purse Application standard)

Singapore Standard SS 518 : 2006

SINGAPORE STANDARD

SS 518 : 2006

(ICS 35.240.15)

SPECIFICATION FOR

Contactless e-purse application

Published by
SPRING Singapore
2 Bukit Merah Central
Singapore 159835
SPRING Singapore Website: www.spring.gov.sg
Standards Website: www.standards.org.sg

SPRING singapore

Contents

		Page
Foreword		7
CLAUSES		
Section One – General		
0	Introduction	9
1	Scope and objectives	10
2	Normative references	10
3	Definitions	11
Section Two – Overview of contactless e-purse application		
4	Purse file structure	12
5	Atomicity	14
6	Key management issues	14
7	Overview of purse security and authentication	15
Section Three – Detailed description of CEPAS 1.0		
8	CEPAS 1.0 purse commands	15
8.1	CEPAS 1.0 overview	15
8.2	Debit command (CEPAS 1.0)	15
8.3	Credit command (CEPAS 1.0)	19
8.4	Read purse command (CEPAS 1.0)	23
8.5	Computation of signed certificate (CEPAS 1.0)	24
Section Four – Detailed Description of CEPAS 2.0		
9	CEPAS 2.0 purse commands	25
9.1	CEPAS 2.0 overview	25
9.2	Debit command (CEPAS 2.0)	28
9.3	Credit command (CEPAS 2.0)	31
9.4	Read purse command (CEPAS 2.0)	34
9.5	Computation of signed certificate (CEPAS 2.0)	36

Revision on CEPAS 2.0

- Updates are more for clarity
- No major changes to the specification
- Main gist of it as below :
  - Move CEPAS Atomic Update, Read Binary, Reset Bit and Get Challenge to main section as part of the CEPAS requirements
  - Added logical data offset in Credit command
  - Added VEP (Vehicle Entry Permit) file structure requirements in Annex

Drafting of CEPAS 3.0

- To enhance security (i.e. AES, ECDSA, etc. to be explored)
- To provide more flexibility in command to providing further inputs
- To provide more flexibility and detailed information in transaction recovery
- To provide needs for NFC mobile devices
- To provide personalization, loyalty schemes, etc. specification
- To provide SAM specification
- To provide Standard Interoperability Test Specification

CEPAS NFC DEVICES, CARDS and READERS PLUGFEST

- Identify RF issues
- Identify interoperability issues
- Identify performance and reliability issues

Interest in ECC

- Elliptic Curve Cryptography is “light weight” and suitable for smart cards
- Use of ECC for authentication in CEPAS has been presented before for future consideration (please see separate slides, attached)
- ECC also applicable to e-ID
- If there is interest, AICF can do more work in ECC standards or compatibility testing

Information on NAF

- Assurity Trusted Solutions Pte Ltd ("Assurity") is a wholly-owned subsidiary of the Infocomm Development Authority of Singapore ("IDA")
- It was incorporated to operate the National Authentication Framework (NAF)
- The following slides are contributed by Assurity

assurity

TRUSTED SOLUTIONS

NAF

National Authentication Framework

National Authentication Framework:

Integrating Consumer Online Security into Businesses

iDA SINGAPORE NAF

National Authentication Framework

- ## What

A **nationwide platform** for the pervasive adoption of **strong authentication** by online services that handle sensitive information and/or facilitate transactions, as well as provide **trusted and cost-effective** authentication.

- ## Why

To fulfill the requirements for strong authentication from key stakeholders and regulators, including government, healthcare, financial and banking sectors.

- ## When

The National 2FA system has been launched since

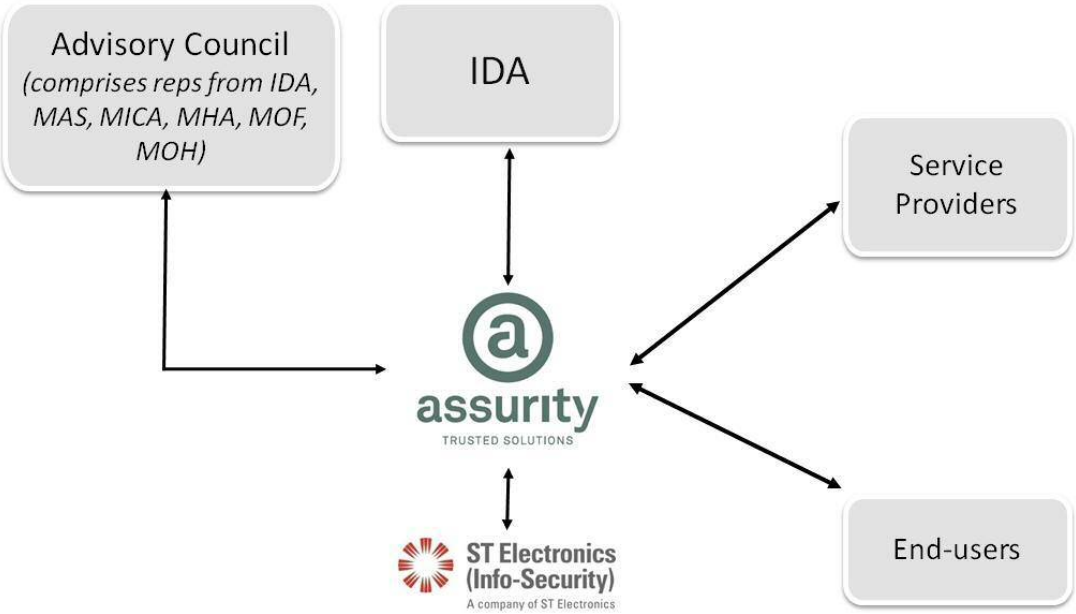
12 December 2011

Value Proposition

- **Cost savings** when businesses leverage on NAF
- **Enhanced protection against online identity theft** for online services
- **Convenience** to end-users: a single authentication device across multiple online services
- **Boost online trust and confidence** to underscore Singapore's status as a trusted infocomm hub

Assurity's Governance Model

- Assurity
  - A subsidiary wholly owned by IDA to be the 2FA operator for NAF
  - Entrusted by governing authorities
  - Overseen by IDA Board



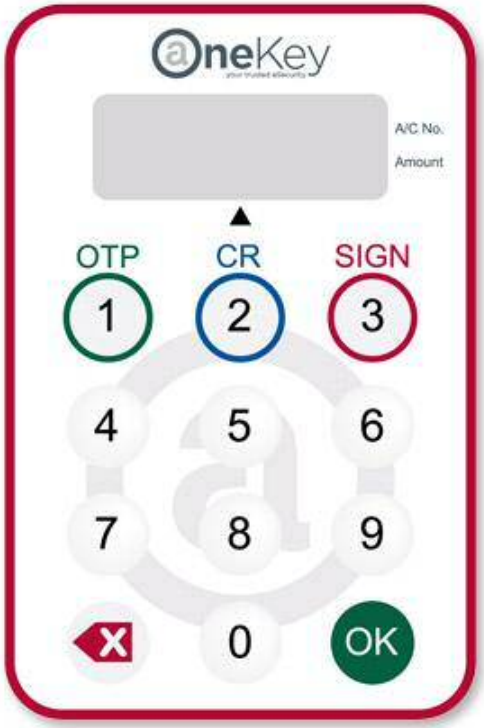
Advisory Council comprising senior management representatives from **IDA, MAS, MOF, MICA, MHA** and **MOHH** to act as a focal point to harmonise strong authentication development across respective sectors.

OneKey: A Convenient, Secure Authentication Mechanism

- Assurity provides 2FA services via the OneKey device – a robust and integrated mechanism that is **secure, convenient and cost-effective**

- OneKey offers 3 options of 2FA - **OTP, Challenge Response and Transaction Signing.**

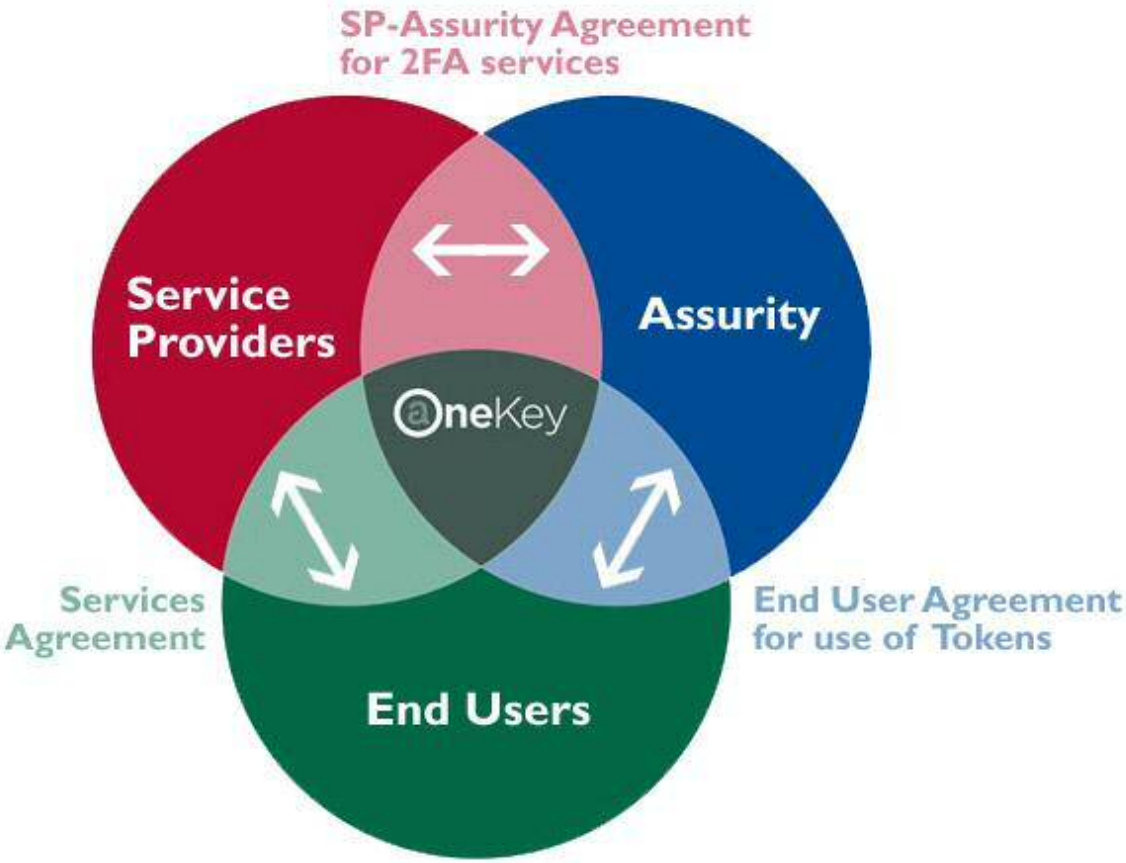
- It functions under **World Class SLAs**, delivering secure authentication.



One Person, One Device

OneKey can be used across multiple platforms, providing convenience to consumers.

Relationship Model

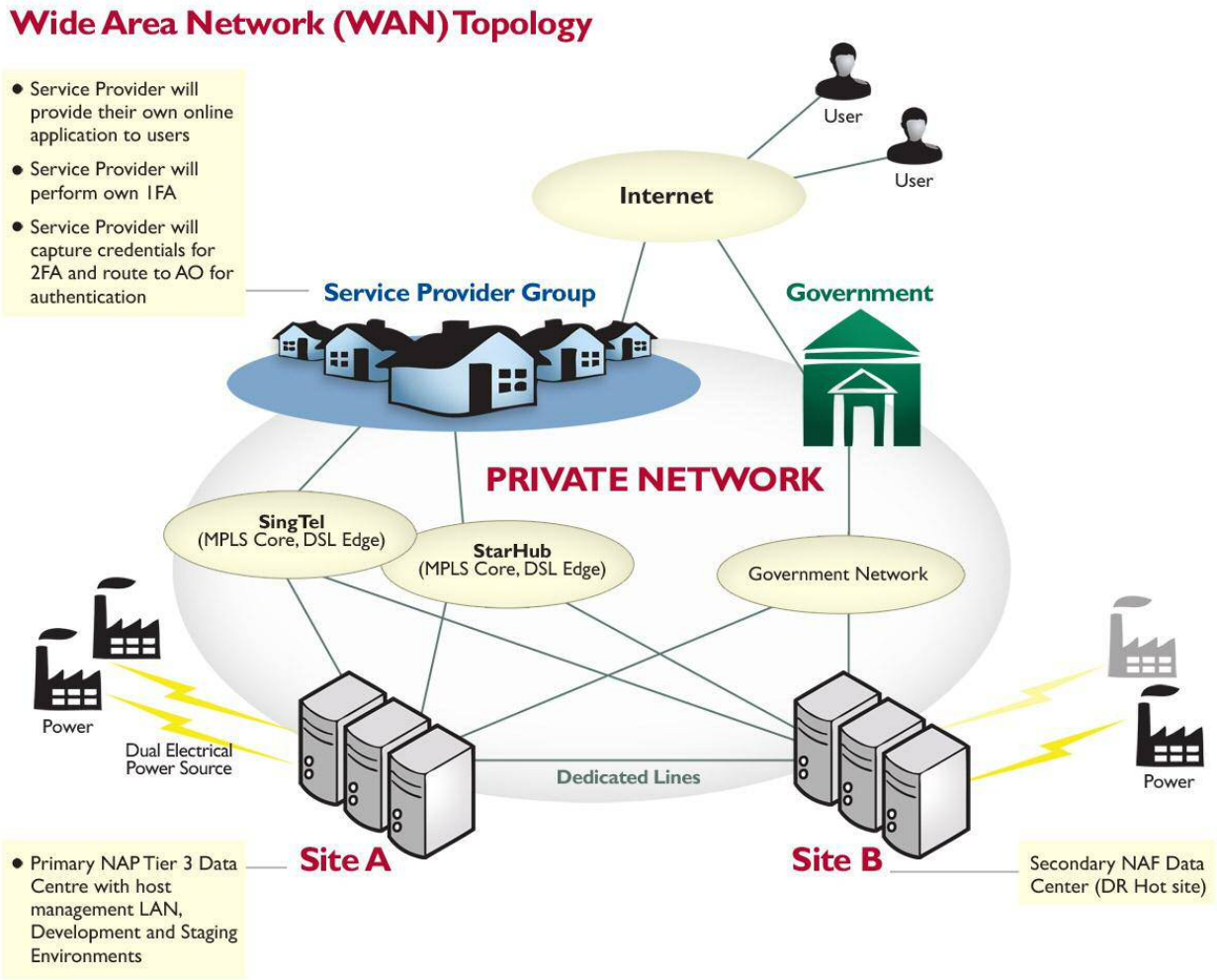


2 Key Incentives

- From system live-date (Dec 11), **2FA transaction fees waived for 2 years**

- **Free 1st Token** for Singapore Citizens & Permanent Residents

NAF Technical Architecture



Fully redundant Architecture

2 Data centres with:

- Dual tele-communications providers and Internet service providers
- Dual power supply
- Synchronised data between both Active sites

Educating the End-User: A Nationwide Effort

- To assist in **end-user training**, Assurity actively carries out Public Education activities to aid:
  - Public awareness of Cyber Security
  - Understanding of 2FA
  - Usage of **One**Key.

***One**Key Admail on Cyber Security distributed to 250,000 households*

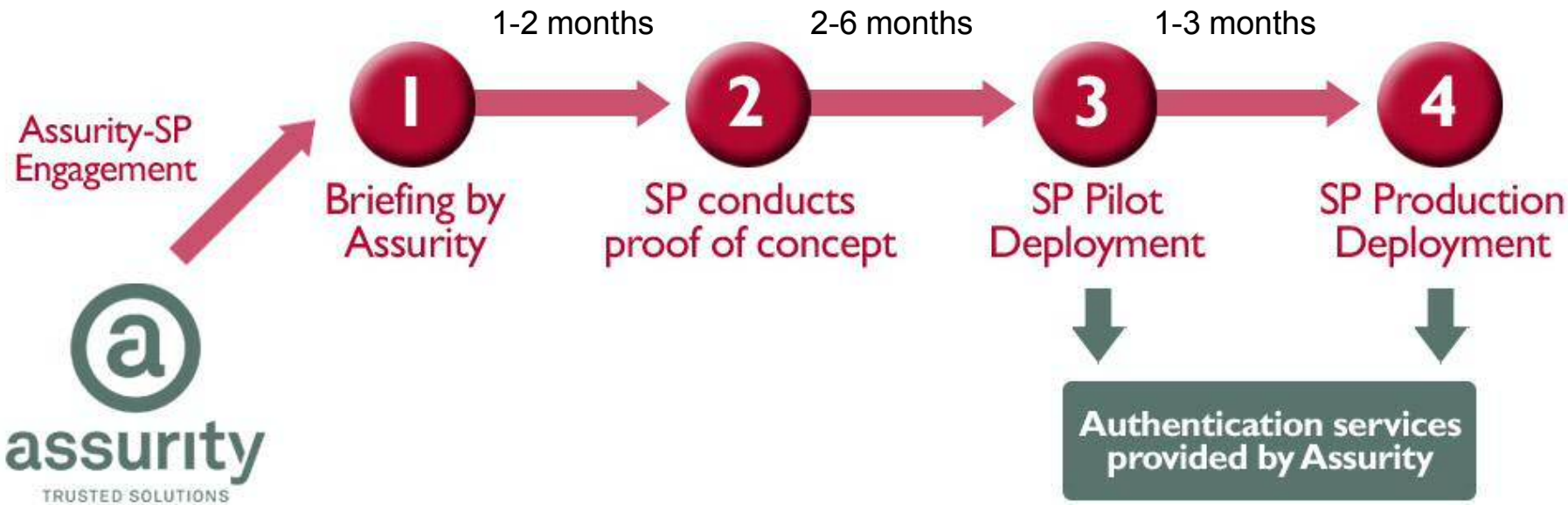
Educating the End-User: A Nationwide Effort

- Channels
  - Public education website: www.onekey.sg
  - Social Media
  - Admail to 250,000 households
  - Roadshows:
    - **One**Key Cyber Security Roadshow at Chevron House
    - **One**Key exhibition at National Libraries islandwide as part of IDA's Cyber Awareness Week

*One*Key exhibition at NLBs islandwide, as part of IDA's Cyber Awareness Week

*One*Key Cyber Security Roadshow at Chevron House

Integration Process for SPs



Question & Answer Session

Chai Chin Loon, Chief Operating Officer
chinloon@assurity.sg, chai_chin_loon@ida.gov.sg

Jason Kong, Business Development Director
jason@assurity.sg

Patrick Ong, Business Development Director
patrick@assurity.sg

THANK YOU!

End of Country Update
Thank you
Q&A