Singapore update - CEPAS, SSID, NFC-CFC

(5-6 Dec 2011 – Asia IC Card Forum @ Korea)

Mr. LIN YIH
email: dartpl@singnet.com.sg
Chairman, Cards and Personal Identification Technical Committee
Singapore IT Standards Committee

an industry partnership supported by SPRING Singapore and IDA
CEPAS (SS518:2006 Contactless e-Purse Application standard)
## Contents

<table>
<thead>
<tr>
<th>Clause</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>7</td>
</tr>
<tr>
<td><strong>CLAUSES</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Section One – General</strong></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Introduction</td>
</tr>
<tr>
<td>1</td>
<td>Scope and objectives</td>
</tr>
<tr>
<td>2</td>
<td>Normative references</td>
</tr>
<tr>
<td>3</td>
<td>Definitions</td>
</tr>
<tr>
<td><strong>Section Two – Overview of contactless e-purse application</strong></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Purse file structure</td>
</tr>
<tr>
<td>5</td>
<td>Atomicity</td>
</tr>
<tr>
<td>6</td>
<td>Key management issues</td>
</tr>
<tr>
<td>7</td>
<td>Overview of purse security and authentication</td>
</tr>
<tr>
<td><strong>Section Three – Detailed description of CEPAS 1.0</strong></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>CEPAS 1.0 purse commands</td>
</tr>
<tr>
<td>8.1</td>
<td>CEPAS 1.0 overview</td>
</tr>
<tr>
<td>8.2</td>
<td>Debit command (CEPAS 1.0)</td>
</tr>
<tr>
<td>8.3</td>
<td>Credit command (CEPAS 1.0)</td>
</tr>
<tr>
<td>8.4</td>
<td>Read purse command (CEPAS 1.0)</td>
</tr>
<tr>
<td>8.5</td>
<td>Computation of signed certificate (CEPAS 1.0)</td>
</tr>
<tr>
<td><strong>Section Four – Detailed Description of CEPAS 2.0</strong></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>CEPAS 2.0 purse commands</td>
</tr>
<tr>
<td>9.1</td>
<td>CEPAS 2.0 overview</td>
</tr>
<tr>
<td>9.2</td>
<td>Debit command (CEPAS 2.0)</td>
</tr>
<tr>
<td>9.3</td>
<td>Credit command (CEPAS 2.0)</td>
</tr>
<tr>
<td>9.4</td>
<td>Read purse command (CEPAS 2.0)</td>
</tr>
<tr>
<td>9.5</td>
<td>Computation of signed certificate (CEPAS 2.0)</td>
</tr>
</tbody>
</table>
Deadline over; 4.6m ez-link cards replaced

BY YEO GHIM LAY

The deadline for commuters to replace their old ez-link cards for free ended yesterday, with 138,400 cards swapped since the deadline was extended a week ago.

As of noon yesterday, 4.64 million old cards have been exchanged for the new ones, said the Land Transport Authority (LTA).

Commuters were initially supposed to replace their cards by last Wednesday, but the LTA extended the deadline because many commuters had not done so. The free exchange programme began in January.

Last week, the LTA said 200,000 old ez-link cards that were being actively used on public transport had yet to be replaced.

Shorter queues were seen at TransitLink ticket offices yesterday compared to the long queues that formed last week.

Checks by The Straits Times found fewer than 10 people queuing at Ang Mo Kio and Toa Payoh MRT stations yesterday morning.

Madam Tay Phek Noi, 57, was among those in line at Toa Payoh MRT station.

She had found an old ez-link card at home on Tuesday. Her family has more than 10 ez-link cards and most of them were replaced in July.

"Today is the last day, so I quickly came here to exchange it," she said.

Queues were longer at Novena and Orchard MRT stations, with more than 20 people in line at the ticket offices around noon. However, not all of them were waiting to exchange their cards. Some commuters were topping up their cards or buying tourist passes.

From today, commuters who replace their cards will have to pay $15 for a new one. The old card is no longer accepted on buses and trains.

The new card can eventually be used to pay Electronic Road Pricing and parking charges as well. It is also accepted at the National Library and 7-Eleven outlets, among other places.

Despite the souped-up features, not all commuters welcome it.

Those who top up their cards automatically via Giro now have to pay a 25-cent fee for each top-up. Giro top-ups on the old card were free and covered by TransitLink, which managed the Giro scheme for the old card.

Asked by The Straits Times yesterday if it would consider lifting the fee, card issuer Ez-Link would only reiterate that the fee was to cover the processing and operating costs of the top-up service, which is a "value-added service".

It added that nine in 10 commuters use free top-up channels such as ticketing machines.
At least 8-9 million cards in 2011

CEPAS stored value cards for low value purchases

Leveraging on the >7m base of CEPAS stored value cards

Adult Cards

Concession Cards

In everyone’s wallets for public transport

A cost-effective e-payment instrument for merchants

To convert cash transactions to e-payments

CEPAS stored value card is the best instrument to effect a change of consumer habit towards the use of e-payment for low value purchases.
CEPAS cards continue to spread...

- **Singapore Tourist Pass**
  (1, 2, or 3 day, unlimited travel)
CEPAS cards continue to spread...

- Go Singapore Pass

Choose Your Pass

**Sentosa + USS Day Pass**
- Sentosa 4 Combo 1 Day Non Peak USS
- **ADULT**
  - Retail Price: **$119.00**
  - Total value: **$153.90**
- **CHILD**
  - Retail Price: **$99.00**
  - Total value: **$121.60**

**Participating Attractions:**
- Universal Studios Singapore
- Underwater World Singapore
- Skyline Luge
- Zoological Gardens
- Butterfly Park
- Go Green

**Use for 48 Hours**
- Includes ez-Link card worth $12
- Includes admission to Sentosa

**Contact Us**

**Do Your Math**

**Participating Attractions**

**FAQs**
CEPAS cards continue to spread...

• More and more car parks can accept CashCard (contact interface) and CEPAS cards

• 345 car parks as of 30 Nov 2011

CEPAS cards continue to spread...

• 2nd generation IU (2GIU, dual mode IU) can accept CEPAS and CashCard. IU (in-vehicle unit) is used for Electronic Road Pricing (ERP)

• Optional auto-top if subscribe to EZ-Reload (by credit card or GIRO)
Senior citizens can activate the Green Man Plus function by using their new CEPAS-compliant senior citizen concession cards on the card readers mounted above the standard push button on the traffic light poles.
New CEPAS readers

New card reader on trial in buses

Larger screen, fonts make reading it easier

NEW transit-card readers are being tested out on 40 public buses. The devices have larger screens and fonts to make it easier for commuters, especially senior citizens, to read them, said the Land Transport Authority. They work in the usual way, with commuters tapping their fare cards.

The current readers are reaching the end of their 10-year lifespan, said the authority. It was therefore the right time to improve the design. The trial, involving buses from both SBS Transit and SMRT, will be completed at the end of this month. The authority will fine-tune the readers before expanding the trial to another 150 buses, then hopefully installing them in the whole fleet by the middle of 2013.

Since 2009, all transit cards have been Contactless e-Purse Application Standard-compliant. This means commuters can use them to pay for other everyday items, from electronic road-pricing chargers to shopping in convenience stores. So far, however, relatively few stores have started accepting them.

MARIA ALMENAR
CEPAS going thru periodic review

- CEPAS SS518 was published in 2006. Every 5 years, Singapore Standards go through periodic review (just like ISO)
- The Review Task Force is chaired by Land Transport Authority (LTA)
- Minor improvements will be published as a Amendment
- Major improvements *may be* approved and published as new parts – for example, changing cryptography from 3DES to AES or ECC, standardize card personalization, standardize purse file structure
- (more details of ECC is available as a separate presentation)
- Review is *WORK IN PROGRESS!*
SSID (SS529:2006 Smart Card ID)
What is SSID?

- A standard for smart card ID, 90-95% same as ICAO e-passport
- Meant for multiple issuers – reader can read cards from different issuers
- Trust based on digitally signed data – signed by issuer private key
- Reader should be able to handle multiple public keys
- Name, “Document Number” mandatory, but biometrics, photo are optional
- If there is biometrics, sharing is optional
Table 4 - Items within DG11

<table>
<thead>
<tr>
<th>Item name</th>
<th>Short description</th>
<th>Type</th>
<th>Size (bytes)</th>
<th>Req</th>
<th>TAG</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>UN</td>
<td>Unique identification number</td>
<td>C</td>
<td>9</td>
<td>M</td>
<td>SF 10'</td>
<td>For example: NRIC, FIN, staff ID</td>
</tr>
<tr>
<td>Name</td>
<td>Full name</td>
<td>C</td>
<td>66</td>
<td>M</td>
<td>SF 06'</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>Gender</td>
<td>C</td>
<td>1</td>
<td>M</td>
<td>SF 33'</td>
<td>&quot;M&quot; or &quot;F&quot;</td>
</tr>
<tr>
<td>Race</td>
<td>Race or ethnic group</td>
<td>C</td>
<td>16</td>
<td>M</td>
<td>DF 15'</td>
<td></td>
</tr>
<tr>
<td>Date_of_birth</td>
<td>Date of birth</td>
<td>C</td>
<td>9</td>
<td>M</td>
<td>SF 29'</td>
<td>YYYYMMDD format</td>
</tr>
<tr>
<td>Country_of_birth</td>
<td>Country of birth</td>
<td>C</td>
<td>20</td>
<td>M</td>
<td>SF 11'</td>
<td></td>
</tr>
<tr>
<td>Citizenship</td>
<td>Citizenship</td>
<td>C</td>
<td>2</td>
<td>M</td>
<td>SF 20'</td>
<td>ISO 3166 (alpha-2)</td>
</tr>
<tr>
<td>Address_registered</td>
<td>Address as in nrc</td>
<td>C</td>
<td>68</td>
<td>M</td>
<td>SF 42'</td>
<td></td>
</tr>
<tr>
<td>Date_issued</td>
<td>Date of issue</td>
<td>C</td>
<td>8</td>
<td>M</td>
<td>SF 23'</td>
<td>YYYYMMDD format</td>
</tr>
<tr>
<td>Date_expiry</td>
<td>Date of expiry</td>
<td>C</td>
<td>8</td>
<td>M</td>
<td>SF 19'</td>
<td>YYYYMMDD format</td>
</tr>
<tr>
<td>Date_last_update</td>
<td>Date of last update</td>
<td>C</td>
<td>8</td>
<td>M</td>
<td>DF 25'</td>
<td>YYYYMMDD format</td>
</tr>
<tr>
<td>Blood_group</td>
<td>Blood grouping</td>
<td>C</td>
<td>3</td>
<td>O</td>
<td>DF 20'</td>
<td></td>
</tr>
<tr>
<td>Other_name</td>
<td>Alias or additional name</td>
<td>C</td>
<td>66</td>
<td>O</td>
<td>SF 06'</td>
<td></td>
</tr>
<tr>
<td>Profession</td>
<td>Profession or occupation</td>
<td>C</td>
<td>20</td>
<td>O</td>
<td>SF 13'</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Title or salutation</td>
<td>C</td>
<td>6</td>
<td>O</td>
<td>SF 14'</td>
<td></td>
</tr>
<tr>
<td>Mailing_address</td>
<td>Correspondence or contact address</td>
<td>C</td>
<td>60</td>
<td>O</td>
<td>DF 21'</td>
<td></td>
</tr>
<tr>
<td>Telephone_nc</td>
<td>Telephone number</td>
<td>C</td>
<td>13</td>
<td>O</td>
<td>SF 12'</td>
<td></td>
</tr>
<tr>
<td>Email_address</td>
<td>Email address</td>
<td>C</td>
<td>50</td>
<td>O</td>
<td>DF 22'</td>
<td></td>
</tr>
<tr>
<td>Religion</td>
<td>Religion</td>
<td>C</td>
<td>15</td>
<td>O</td>
<td>DF 23'</td>
<td></td>
</tr>
<tr>
<td>Nick</td>
<td>Name of next of kin</td>
<td>C</td>
<td>66</td>
<td>O</td>
<td>DF 26'</td>
<td></td>
</tr>
<tr>
<td>Nick_address</td>
<td>Address of next of kin</td>
<td>C</td>
<td>69</td>
<td>O</td>
<td>DF 27'</td>
<td></td>
</tr>
<tr>
<td>Drug_allergy</td>
<td>Drug allergy</td>
<td>C</td>
<td>2</td>
<td>O</td>
<td>DF 24'</td>
<td></td>
</tr>
<tr>
<td>Issuer_level</td>
<td>Issuer level</td>
<td>C</td>
<td>1</td>
<td>O</td>
<td>DF 28'</td>
<td></td>
</tr>
<tr>
<td>Ns_eligibility</td>
<td>Eligibility for ns</td>
<td>C</td>
<td>2</td>
<td>O</td>
<td>DF 29'</td>
<td></td>
</tr>
<tr>
<td>Service_status</td>
<td>Civilian status or uniformed status or both</td>
<td>C</td>
<td>1</td>
<td>O</td>
<td>DF 2A'</td>
<td></td>
</tr>
<tr>
<td>Civilian_salutation</td>
<td>Civilian salutation</td>
<td>C</td>
<td>6</td>
<td>O</td>
<td>DF 26'</td>
<td></td>
</tr>
<tr>
<td>Civilian_organisation</td>
<td>Civilian organisation</td>
<td>C</td>
<td>16</td>
<td>O</td>
<td>DF 25'</td>
<td></td>
</tr>
<tr>
<td>Civilian_sub_organisation</td>
<td>Civilian sub-organisation</td>
<td>C</td>
<td>20</td>
<td>O</td>
<td>DF 2F</td>
<td></td>
</tr>
</tbody>
</table>
SSID deployment

- Singapore Changi Airport Terminals, 80K+++ cards
- Singapore Seaport Terminals (PSA), 80K+++ cards
- IDA @ MICA, 400++ cards
- Changi Naval Base, 20K++ cards (completed)
- Jurong Island, 70K in 2011, up to 220K cards by 2018
- MHA, 3K++ cards, incorporates SOD-Lite

* combination of different card vendors, reader vendors, door controllers, system integrators

an industry partnership supported by SPRING Singapore and IDA
SSID going thru periodic review

• SSID SS526 was published in 2006. Every 5 years, Singapore Standards go through periodic review (just like ISO)
• SOD-Lite will be published as an Amendment to SS526
• A new part for public / private key *may be* approved and standardized as SSID-PKX
• (more details of SSID-PKX is available as a separate presentation)
• Review is *WORK IN PROGRESS!*
Proposal to enhance SSID - SODLite option
Why SODLite?

The “security data object” (SOD) as specified in SS529:2006 is a “signed data” typically produced by PC based software such as Microsoft CAPI (Crypto API) or OpenSSL. It is a ASN.1 DER encoded data that is rich in structure and information, but cumbersome for many door access controllers. As an example, a SOD that is produced by SHA-1+RSA-1024 is typically 1.5 kilobytes but inside, the two most useful data are (a) about 81 bytes for 3 SHA-1 hashes of 3 data groups, and (b) about 128 bytes for a RSA-1024 bit integer output. The bulk of the overhead is attributed to information regarding the signer, public key identifier, and signing time (if applicable).
Why SODLite?

In a relatively closed application such as door access, the extra information is not required and the extra overhead imposes longer data reading time (i.e. reading out SOD), and requires the controller firmware to parse a complex ASN.1 DER encoded string before it can extract out the useful SHA hashes and RSA values. **This imposes a serious barrier to entry (steep learning curve) for door access reader manufacturers.** Even if there are secure access modules (SAMs) capable of computing SHA, RSA and ECC, the software work to parse ASN.1 structure is still required on the door controller. The purpose of this amendment is to define a SOD structure that comprises only “raw, essential” bytes while complying with the typical tag-length-value (TLV) rules widely used in smart cards.
Example of SOD creation

SOD core value (hash of DGs) 81 bytes

SHA-1 20 bytes RSA-1024 128 bytes

81 bytes + 128 bytes

complete SOD to be stored on card

an industry partnership supported by SPRING Singapore and IDA
What is SSID-PKX?

SSID – Private Key eXtension
Purpose

• SS 529 : 2006 SSID provides a standard for personal data on a smart card (or device)
• But it does not cover private key, public key certificate, and other cryptographic operations that are required for applications such as digital signature, secure email, and other strong authentication needs
Where SSID-PKX applies

Smart Card

- Personal Data
  - NRIC, name, face, fingerprint
- Private key & Public key certificate

Reader Terminal

- ID apps
  - door access, attendance, student concession
- Digital signature, secure email

ISO + SSID cmd & data
ISO + SSID-PKX cmd & data

an industry partnership supported by SPRING Singapore and IDA
Tentative Scope

• Define where private and public keys are stored (key containers)
• Define where public key certificates are stored (certificate store)
• Define APDUs for reading of public key / certificates
• Define APDUs for cryptographic operations that involve public & private keys
What it is not

• For the first phase, main attention is to define APDU, data structure, and security protection for applications such as digital signature and secure email

• Other application needs can come later
NFC CFC (Call for Collaboration)
NFC CFC background

- Singapore NFC e-purse trials started back in 2007
- However users are “locked into” consortium that cannot cross transact
- 2011 CFC is a new effort
NFC CFC 2011 Model

Figure 1. Role of TTP in the NFC ecosystem.

- Payment Service Provider - DBS, Citibank, EZ-Link
- TTP - Gemalto
- Mobile Operator - M1, SingTel, StarHub
NFC CFC 2011 Model – role of members

- DBS, EZ-Link and Citibank will enable a wide range of their credit / debit scheme cards and stored value payment products,
- To be issued over-the-air through Gemalto, and stored on the secure chips in their customers' NFC-enabled mobile phones.
- The services will be launched progressively across all three mobile operators (M1, SingTel and StarHub)
- A TTP infrastructure eliminates the need for any service provider to establish separate technical connections with individual mobile operators.

an industry partnership supported by SPRING Singapore and IDA
NFC CFC 2011 Features

• Merchants can likewise enjoy the NFC benefits as long as their payment terminals can accept contactless payment cards from MasterCard or Visa, or support Singapore's CEPAS payment standard.

• Beyond payment, merchants can also work with Point-of-Sale terminal providers to develop new and exciting customer **reward and loyalty** redemption services, based on NFC technology on these terminals.

• Integrating proximity ("tapping") transactions with social networks, reducing physical merchandise with **NFC-tagged** displays etc. are novel ideas to improve customer service and convenience.
NFC CFC 2011 Features

- From the middle of 2012, consumers can "tap" and pay for their purchases at more than 20,000 retail points and taxis using their Near Field Communication1 (NFC) enabled mobile phones.
- Businesses can also provide interactive and targeted contents to consumers through NFC-enabled digital signages located at more than 600 locations in major shopping malls and office buildings throughout Singapore.
- IDA and the consortium members will be working with LTA to assess NFC mobile payment readiness for transit in early 2013
End of Country Update
Thank you
Q&A