Singapore update - 2015

(26-27 May 2015 – Asia IC Card Forum @ Jeju, 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

Some new updates

- The last AICF meeting took place on 5 Dec 2014, in Singapore
- I gave some updates at that meeting, and my slides can be downloaded from AICF website
- NEW – CEPAS 2014 edition published !
- Some ideas for SSID-PKX (to leverage on built-in drivers provided by Microsoft Windows)
- Discussion in ISO/IEC JTC1 SC37 to have biometric data formats in ASN.1

CEPAS (SS518:2014 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

Singapore Standard SS 518 : 2014

SINGAPORE STANDARDS COUNCIL

SS 518 : 2014
(ICS 35.240.15)

SINGAPORE STANDARD

Specification for contactless e-purse application

Published by
SPRING singapore
Enabling Enterprise

Contents

		Page
Foreword		7
Section One General		
0	Introduction	9
1	Scope and objectives	10
2	Normative references	10
3	Definitions	10
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)	16
8.3	Credit command (CEPAS 1.0)	20
8.4	Read purse command (CEPAS 1.0)	24
8.5	Computation of signed certificate (CEPAS 1.0)	25
Section Four Detailed description of CEPAS 2.0		
9	CEPAS 2.0 purse commands	26
9.1	CEPAS 2.0 overview	26
9.2	Debit command (CEPAS 2.0)	28
9.3	Credit command (CEPAS 2.0)	32
9.4	Read purse command (CEPAS 2.0)	36
9.5	Atomic Update command (CEPAS 2.0)	38
9.6	Reset Bit command (CEPAS 2.0)	38
9.7	Computation of signed certificate (CEPAS 2.0)	38
9.8	Read Binary	40
9.9	Get Challenge	40

COPYRIGHT

Changes not substantial

This standard is a revision of SS 518 : 2006. The changes in the revised edition include the following:

- Clearly defined the transaction amount setting in the Debit and Credit commands;
- Described the validity of random number/challenge generated for secure authentication;
- Included Credit command's logical data offset definition within the purse EF;
- Made the 4 commands, Atomic update, Reset bit, Read Binary and Get challenge essential requirements;
- Added an overview of CEPAS file structure in a new annex.

Added Royalty Free clause

- If SS518 is used by an entity, local or overseas, to develop products or services, the company can do so **without** paying royalty to SPRING. However, users have to ensure that the standard is not reproduced or that third party intellectual property rights are not infringed.

- Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. SPRING Singapore shall not be held responsible for identifying any or all of such patent rights.

Buy from SPRING e-Shop

Home | FAQs | Sitemap | Contact Us

Managed Exclusively by
TOPPAN
TOPPAN LEEFUNG PTE. LTD.

Singapore Standards eShop

About Singapore Standards eShop | About Singapore Standardisation Programme | General Terms & Conditions | Resources

www.singaporestandardseshop.sg

Advanced Search

Login (0)

Browse by Product Categories

- Singapore Standards
- Standards of your Industry
- International Standards
- ISO Standards
- IEC Standards
- British Standards

My Account | **New Member?**

Email

Password

Login

Forgotten password?

Email Address

Send Password

Signup eAlerts
Fill in your email below

Subscribe

What's New

1. SS 604 : 2014
   ($22.45)
   Guidelines on nutrition and food service for older adults
2. SS 518 : 2014
   ($49.75)
   Specification for contactless e-purse application (CEPAS)

SG$49.75

Best Selling Singapore Standards (Feb 2015)

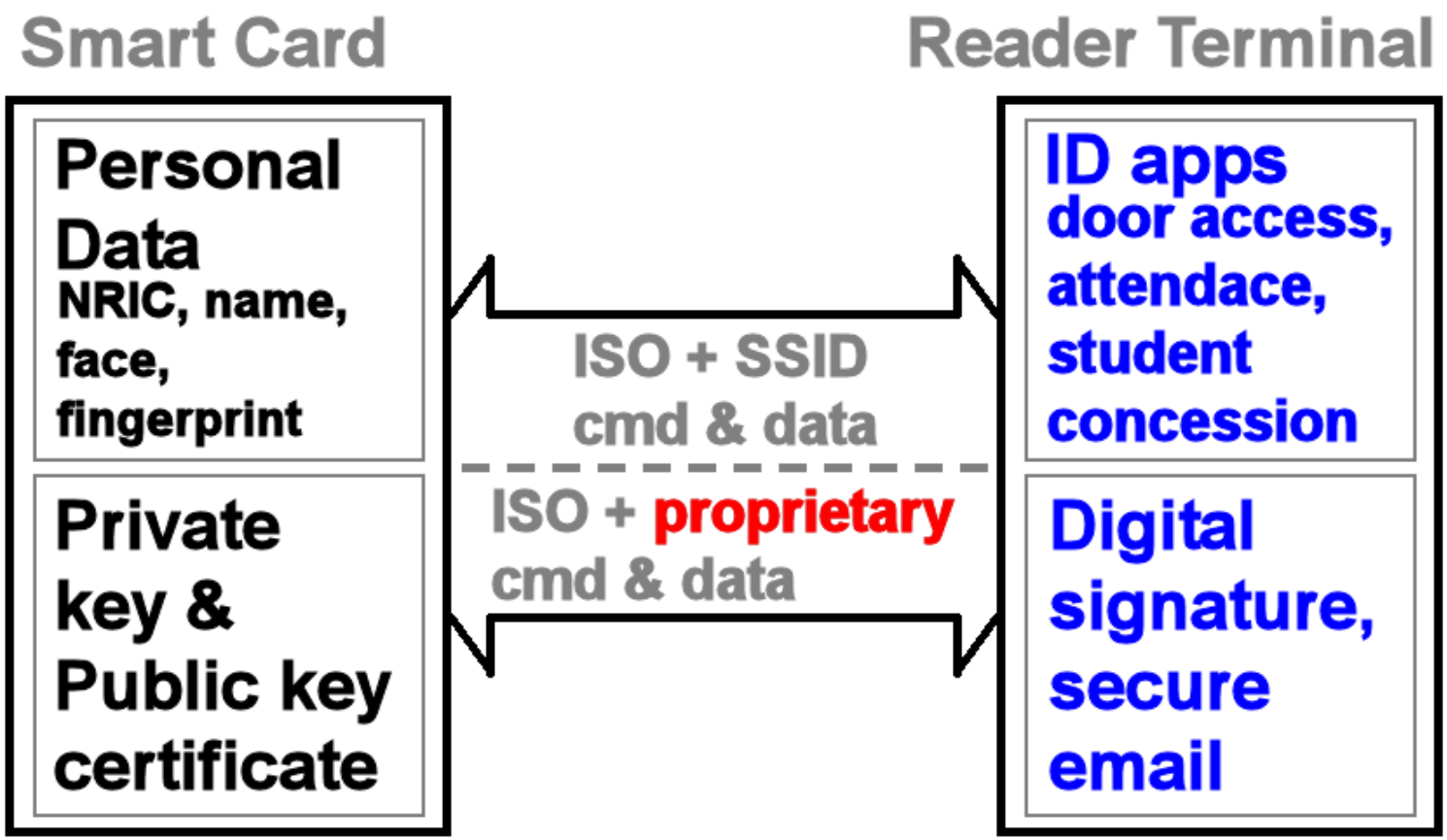
1. SS 600 : 2014
   Code of practice for bunkering
2. SS 599 : 2014
   Guide for wayfinding signage in public areas
3. SS 5 - F6 : 2014
   Methods of test for paints, varnishes and related materials - Part F6 : Determination of wet-scrub resistance

SSID-PKX
What is it?

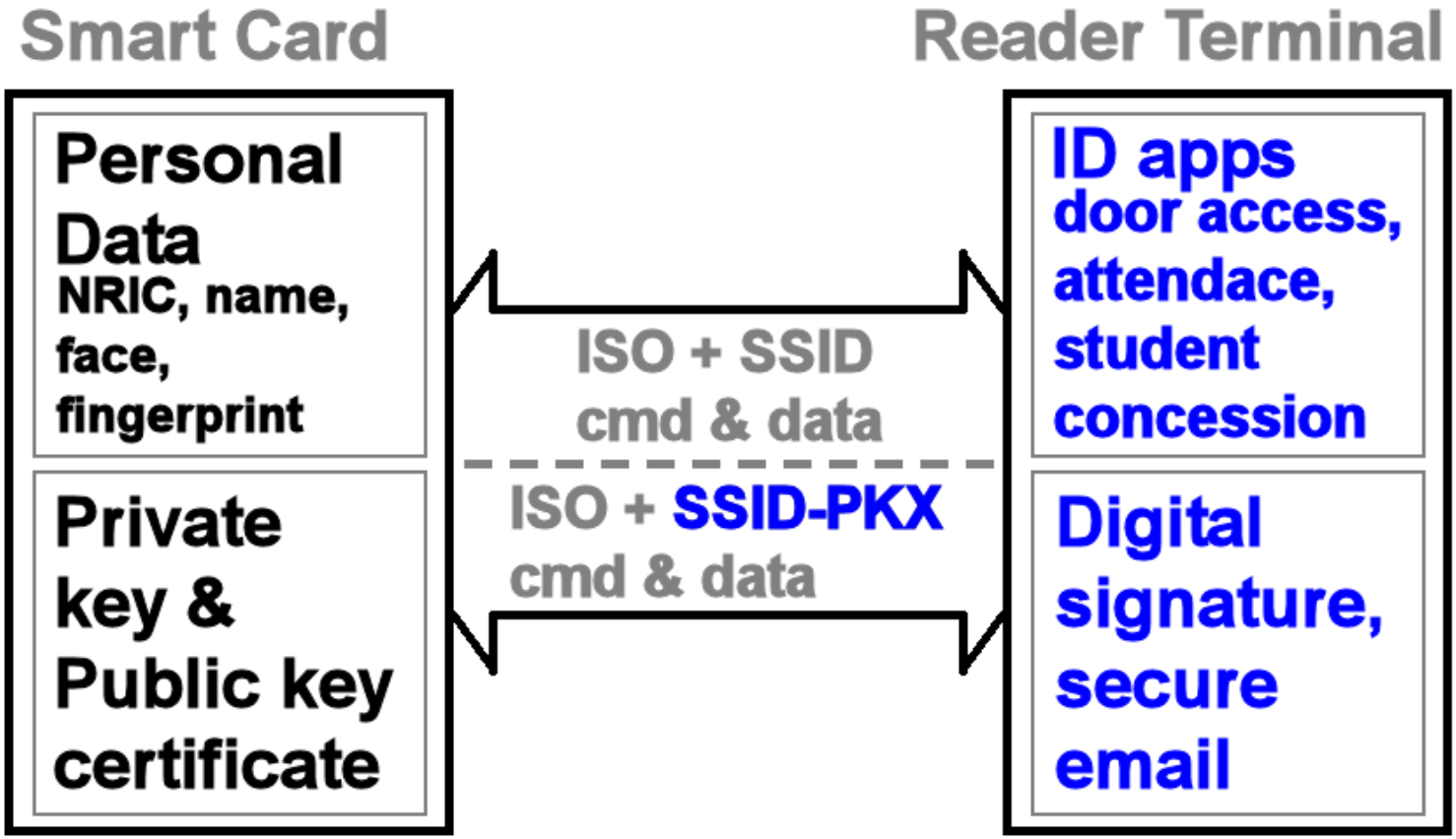
Purpose

- 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

Problem to solve



Where SSID-PKX applies



Architecture – software interface

Microsoft Smart Card MiniDriver Specification (Vista, Win7)

Smart card vendors can write card minidrivers to present a consistent interface to their smart card type to the Microsoft Smart Card Base Cryptographic Service Provider (CSP) or Crypto Next Generation (CNG) Key Storage Provider (KSP) and to the Smart Card Management Interface. These card minidrivers plug in to Windows operating system code. The functionality in a card minidriver is narrowly scoped and carefully defined so that the card-dependent code is simple to implement and easy to verify functionally.

This specification provides implementation guidelines for Base CSP and KSP card minidrivers.

New observation

- Microsoft publishes a GIDS specifications for smart cards, and provides a built-in minidriver for GIDS cards
- This means no need to download and install minidrivers from different smart card companies
- GIDS provides capability to perform PKI operations !

Minidriver for GIDS

Discovery Process

Beginning with Windows 7, smart card minidrivers that are logo-certified through the Windows Logo Program (WLP) are automatically downloaded and installed by the Windows Plug and Play components. Windows 7 also introduces a class minidriver for PIV-compatible cards and cards that support the GIDS card edge.

When a smart card is inserted into the reader, Windows performs the following discovery processes:

- Smart Card Plug and Play Process:

  This process requests and download a logo-certified minidriver from Windows Update through Plug and Play.

- Winscard Discovery Process:

  This process associates a compatible smart card with a PIV- or GIDS-compatible class minidriver.

- Windows Smart Card Class Minidriver Discovery Process:

  This process associates an installed minidriver with a smart card.

The following table lists the AID values that the different discovery processes use.

GIDS v2.0 from Microsoft

Generic Identity Device Specification

GIDS v2.0

Version 2.0

October 19, 2012

Abstract

This document specifies the profile (card edge and the data model) that can be supported by a physical identity device such as a smart card that fully complies with ISO/IEC 7816.

References and resources discussed here are listed at the end of this paper.

The current version of this paper is maintained on the Web at:
Generic Identity Device Specification

For feedback or questions, send an e-mail to:
gids@microsoft.com

Microsoft

So what's next for SSID-PKX ?

- Call for industry meeting to survey adoption and readiness of GIDS v2
- Evaluate the quality of GIDS and see if it matches the needs of SSID-PKX

ISO/IEC JTC1 SC37 Plenary

- I attended the recent SC37 “Biometrics” meeting in Toledo, Spain (19-20 Jan 2015)
- There was a discussion on using ASN.1 for “Generation 3” of biometrics data format (ISO 19794 series)
- Gen1 (2005) uses binary encoding, Gen2 (2011) introduces XML, now Gen3 discussion
- If you are interested in this new standards development, please contact your national standard body

End of Country Update
Thank you
Q&A