Singapore Standards Council

SS 518:2014+A1:2019
(ICS 35.240.15)

SINGAPORE STANDARD

Specification for contactless e-purse application

Amendment No. 1

Published by
Enterprise Singapore

SS 518:2014+A1:2019
(ICS 35.240.15)

SINGAPORE STANDARD

Specification for contactless e-purse application

ISBN 978-981-4557-64-1

This Singapore Standard was approved by Information Technology Standards Committee on behalf of the Singapore Standards Council on 4 December 2014.

First published, 2006
First revision, 2014

The Information Technology Standards Committee, appointed by the Standards Council, consists of the following members:

		Name	Capacity
Chairman	:	Mr Yap Chee Yuen	*Standards Council*
Deputy Chairman	:	Mr Chak Kong Soon	*Singapore Computer Society*
Secretary	:	Ms Ho Buaey Qui	*Infocomm Development Authority of Singapore*
Members	:	Assoc Prof Chan Mun Choon	*National University of Singapore*
		Mr Cheong Tak Leong	*SPRING Singapore*
		Mr Robert Chew	*Individual Capacity*
		Assoc Prof Benjamin Gan Kok Siew	*Singapore Management University*
		Ms Ho Buaey Qui	*Infocomm Development Authority of Singapore*
		Dr Derek Kiong	*Individual Capacity*
		Mr Karl Kwan Kar Kin	*Singapore Polytechnic*
		Mr Lee Kee Siang	*Information Technology Management Association*
		Mr Kelvin Ng	*Nanyang Polytechnic*
		Mr Patrick Pang	*National Research Foundation*
		Mr Harish Pillay	*Internet Society*
		Mr Victor Tan Hein Kiat	*Defence Science and Technology Agency*
		Dr Tham Jo Yew	*Institute for Infocomm Research*
		Mr Thomas Ting	*Association of Small and Medium Enterprises*
		Mr Yow Tau Keon	*Singapore Infocomm Technology Federation*

The Cards and Personal Identification Technical Committee, appointed by the Information Technology Standards Committee and responsible for the preparation of this standard, consists of representatives from the following organisations:

		Name	Capacity
Chairman	:	Mr Lin Yih	*Digital Applied Research and Technology Pte Ltd*
Secretary	:	Mr Kelvin Lim	*Land Transport Authority*
Members	:	Mr Chai Chin Loon	*Assurity Trusted Solutions Pte Ltd*
		Mr Lawrence Chen Tai Pang	*Institute for Infocomm Research*
		Mr Sunny Ho	*3M*
		Mr Loh Kar Whee	*Defence Science and Technology Agency*
		Mr Binu Pillai	*Network for Electronic Transfers (Singapore) Pte Ltd*
		Mr Raja Rajeshkumar	*Auctorizium Pte Ltd*

Members	:	Mr Silvester Prakasam	*Land Transport Authority*
		Mr Noah Tay Chin Seng	*Integrated Health Information Systems Pte Ltd*
		Mr Yu Chien Siang	*Ministry of Home Affairs*

The Working Group appointed by the Technical Committee to assist in the preparation of this standard comprises the following experts who contribute in their *individual capacity*:

		Name
Convenor	:	Ms Lee Phaik Lan
Members	:	Mr Bernard Cheong Kong Wee
		Mr Johnny Chung
		Mr Ryan Koo
		Mr Edward Leong
		Mr Leow Siew Kiat
		Mr Lin Yih
		Mr Ng Poh Chang
		Mr David Quek
		Mr Seow Aun Chuan
		Mr Wang Qiang
		Mr Simon Wu

The organisations in which the experts of the Working Group are involved are:

Digital Applied Research and Technology Pte Ltd
EZ-Link Pte Ltd
Infineon Technologies Asia Pacific Pte Ltd
Gemalto Technologies Asia Pte Ltd
Giesecke & Devrient Asia Pte Ltd
Land Transport Authority
Network for Electronic Transfers (Singapore) Pte Ltd
NXP Semiconductors Singapore Pte Ltd
Watchdata Technologies Pte Ltd

(blank page)

Contents

Page

Annexes

Figures

Foreword

This Singapore Standard was prepared by the Work Group appointed by the Cards and Personal Identification Technical Committee (CPITC) under the purview of the Information Technology Standards Committee. The CPITC participates actively in ISO/IEC JTC1 SC17 (Cards and Personal Identification) and mirrors its standardisation activities.

SS 518 was first developed based on work done on the EZ-Cash trial run project. The two main participants of the trial run were NETS and EZ-Link Pte Ltd.

The trial run was supported by the Infocomm Development Authority of Singapore (IDA). The EZ-Cash project started in July 2002 and the first draft of the specification was ready in October 2002. After a number of revisions, a draft EZ-Cash specification was presented to industry for their participation at the end of 2002. Following that, successful laboratory test and demonstration were conducted in September 2003, where compliant products were supplied by card vendors. The EZ-Cash specification was submitted to the CPITC in February 2004 for development into a national standard. It was published as a Singapore Standard in January 2006.

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.

In preparing this standard, references were made to the following publications:

ISO/IEC 7816-4 : 2005	Identification cards – Integrated circuit cards – Organization, security and commands for interchange
ISO/IEC 9797-1 : 1999	Information technology – Security techniques – Message Authentication Codes (MACs) – Mechanisms using a block cipher
SS 372 :	Specification for identification cards – Integrated circuit(s) cards with contacts
	Part 3 : 2000 Electronic signals and transmission protocols (Identical adoption of ISO/IEC 7816-3 : 1997)
	Part 4 : 1999 Interindustry commands for interchange
SS 467 : 2002	Specification for smart card reader APIs
SS 468 : 1999	Specification for stored value card application
SS 484 : 2000	Specification for debit and credit card applications on smart card

Acknowledgement is made for the use of information from the above publications.

This specification describes the technical requirements for a smart card that can be used in a multi-issuer deployment scenario. Issuers are responsible for the personalisation of their own cards. Interoperability is achieved by multiple sets of keys residing in the terminal readers and in the card. For interoperability, smart card readers will contain debit keys of all the participating Issuers, but not their credit keys. Credit operation is thus limited to selected terminals (readers) that contain the required credit keys.

Key management is meant to be flexible and the final implementation choice is left with the card Issuer. The debit command requires 1 key reference while the credit command requires 2 key references. In the simplest case, all 3 references (1 for debit, and 2 for credit) could all refer to the same key.

The design allows *partial refund*, in contrast with a normal *credit*. The partial refund is limited to the most recent amount debited. There is no restriction for a credit operation.

Transaction logging can be performed as an integrated operation of debit and credit, instead of separate updates.

While the ISO/IEC 7816 series of standards provide a sophisticated and rich set of commands for smart cards, this specification makes use of only the relevant portions. In particular, since the standardisation of e-purse commands are not covered in the international standards, this specification is suitable for our local needs.

This standard is expected to be used by electronic purse payment issuers and acquirers and smartcard vendors.

If SS 518 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. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations*

Specification for contactless e-purse application

Section One – General

0 Introduction

This standard contains details for a command set that can be used for contactless e-purse application. The focus is on *credit and debit* and not the rest of the file management aspects. Where possible, the ISO/IEC 7816 series of standards are adopted and referenced. However since the ISO/IEC 7816 series does not attempt to define credit and debit commands, this specification serves to cover these areas. For backward compatibility reasons, the commands are deliberately designed to be similar to the existing SS 468 : 1999 (2012) "Specification for Stored Value Card Application". Changes were made to improve on transaction speed and integrity, as typically demanded by contactless transit fare applications.

This standard describes 2 versions of the contactless e-purse application – CEPAS 2.0 and CEPAS 3.0. *As amended, Jan 19*

Annex A lists some additional supporting commands which can be used by issuers based on their project needs. Annex B provides some test vectors for commands that use cryptographic operation. An overview of the CEPAS file structure is given in Annex C.

Where necessary the definitions and notation used in this standard follows ISO/IEC 7816-4 : 2005 "Identification cards – Integrated circuit cards – Organisation, security and commands for interchange". The command/response pairs highlighted in this standard also follows the convention in ISO/IEC 7816-4 : 2005. CEPAS 2.0 commands (Read purse, Debit, Credit and Atomic Update except Reset Bit command) shall follow ISO/IEC 7816-4 : 2005 case 4 APDU structure with Lc and Le fields present.

The following standards are useful background materials:

SS 468 : 1999 (2012)	Specification for stored value card application
SS 372 :	Specification for identification cards – Integrated circuit(s) cards with contacts
	Part 4 : 1999 Interindustry commands for interchange
ISO/IEC 7816-3 : 1997	Identification cards – Integrated circuit cards – Electronic signals and transmission
ISO/IEC 7816-4 : 2005	Identification cards – Integrated circuit cards – Organization, security and commands for interchange
ISO/IEC 7816-9 : 2004	Identification cards – Integrated circuit cards – Commands for card management
ISO/IEC 9797-1 : 1999	Information technology – Security techniques – Message Authentication Codes (MACs) – Mechanisms using a block cipher

1 Scope and objectives

1.1 Scope

This specification provides a command set for performing electronic purse (e-purse) operations on a stored value smart card. It covers commands for debit, credit and transaction logging. However, this specification does not cover additional file creation, file protection profile, security control and other details that will be required for full operational deployment. These details will be discussed and resolved by the respective smart card issuers.

1.2 Objectives

This specification aims to:

- make the commands more *atomic*. Instead of issuing a number of commands to achieve a debit operation, it can now be done with one command. The balance in the purse is also returned after the debit or credit operation.

- provide a simpler and more *atomic* command flow that will lead to faster and more robust transactions. This will make the command set more usable for contactless (as well as contact) smart cards.

- provide a common ground between the traditional file and directory structure of the contact smart card domain, and the flat fixed sized sector structure of the contactless smart card domain. This command set is meant to be used by the major contactless stored value card issuers in Singapore.

2 Normative references

The following reference documents are indispensable for the application of this standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-4	Identification cards – Integrated circuit cards – Organisation, security and commands for interchange
ISO/IEC 9797-1	Information technology – Security techniques – Message Authentication Codes (MACs) – Mechanisms using a block cipher
ISO/IEC 14443-3	Identification cards – Contactless integrate circuit cards – Proximity cards – Part 3 : Initialization and anticollision

As amended, Jan 19