Singapore Standards Council

SS 529 : 2006
(ICS 35.240.15)

SINGAPORE STANDARD

Specification for smart card ID

Published by

Enterprise Singapore

SS 529 : 2006
(ICS 35.240.15)

SINGAPORE STANDARD

Specification for smart card ID

ISBN 981-4154-47-4

This Singapore Standard was approved by Information Technology (IT) Standards Committee on behalf of the Standards Council of Singapore on 2 December 2006.

First published 2006.

The IT Standards Committee appointed by the Standards Council consists of the following members:

		Name	Capacity
Chairman	:	Mr Robert Chew	*Member, Standards Council*
Secretaries	:	Ms Ho Buaey Qui	*Infocomm Development Authority of Singapore*
		Ms Kong Pei Wee	*Infocomm Development Authority of Singapore*
Members	:	Assoc Prof Clement Chia	*Nanyang Technological University*
		Ms Susan Chong	*SPRING Singapore*
		Dr Derek Kiong	*Institute of Systems Science*
		Mr Raymond Lee	*Infocomm Development Authority of Singapore*
		Mr Lim Sah Soon	*Singapore Chinese Chamber of Commerce & Industry*
		Mr Harish Pillay	*Singapore Computer Society*
		Assoc Prof Pung Hung Keng	*National University of Singapore*
		Dr Susanto Rahardja	*Institute for Infocomm Research*
		Mr Kenny Tan	*Information Technology Management Association*
		Mr Wilson Tan	*Individual Capacity*

The Technical Committee on Cards and Personal Identification appointed by the IT 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	:	Ms Kristy Chan	*Citigroup Inc*
Members	:	Mr Chan Kai Sum	*ST Electronics (Info-Comm Systems)*
		Mr Chang Yew Kong	*ST Electronics (Info-Software Systems)*
		Mr Cheong Chung Chin	*Oberthur Card Systems Asia Pacific Pte Ltd*
		Mr Cheong Mun Wai	*Ernst & Young*
		Mr Steven Chew	*Stevic Singapore Pte Ltd*
		Mr Victor Chia	*X-Bio Pte Ltd*
		Mr Andrew Chow	*DigiSafe Pte Ltd*
		Mr Colin Chow	*Secur-Card Solutions*
		Mr Chu Yew Fai	*Infineon Technologies Asia Pacific Pte Ltd*
		Mr Chua Boon Kien	*Bearing Point Pte Ltd*
		Ms Chua Siew Ling	*QB Pte Ltd*
		Mr Chua Thian Yee	*CASSIS International Pte Ltd*
		Dr Chua Ting Kin	*Euroasia Technology Pte Ltd*
		Dr Michael W David	*Cubic Corporation*
		Ms Charlene Foo	*Mark Grow Technology Pte Ltd*

Member	:	Mr Foo Jong Ai	*Netrust Pte Ltd*
		Mr Anthony Hay	*NEC Solutions Asia Pacific Pte Ltd*
		Mr Sunny Ho	*NEC Solutions Asia Pacific Pte Ltd*
		Mr Keith Kee	*Asian Resources Centre*
		Mr James Koh	*Economic Development Board*
		Mr Daniel Kusmanto	*ST Microelectronics Asia Pacific Pte Ltd*
		Mr Lai L T	*Oakwell Engineering Limited*
		Mr Lee Ching Kie	*Autostar Technology Pte Ltd*
		Mr Lee Choon Kwee	*Defence Science & Technology Agency*
		Mr Nicholas Lee	*EZ-Link Pte Ltd*
		Mr Nick Lee Sheng Weng	*Wavex Technologies Pte Ltd*
		Mr Liew Kah Thiam	*ADC Technologies International (Bosch Group)*
		Mr Lim Boon Seng	*Sony Electronics (S) Pte Ltd*
		Ms Eileen Lim	*HID Corporation (Singapore)*
		Mr Daniel Lim Fang Liang	*Smartrac Technology Ltd*
		Mr Lim Hwee Kwang	*MINDEF CIO Office*
		Mr Lim Khee Ming	*Network for Electronic Transfers (S) Pte Ltd*
		Mr Alex Mak	*Philips Electronics*
		Mr Yoshihide Nakata	*OKI Semiconductor (S) Pte Ltd*
		Mr Ng Hoo Ming	*PCS Security*
		Mr Ng Kah King	*CISCO Computer Security*
		Mr Lawrence Ng	*Sagem Orga (Singapore) Pte Ltd*
		Mr Ng Poh Chang	*Gemalto*
		Dr Ngair Teow Hin	*SecureAge Technology Pte Ltd*
		Mr Ngin Hoon Tong	*Infocomm Development Authority of Singapore*
		Mr Charles Oh	*Defence Science & Technology Agency*
		Ms Rita Ong Yat Been	*National Computer Systems Pte Ltd*
		Mr Jack Pan	*VISA International*
		Mr Priyesh Panchmatia	*i-Sprint Innovations Pte Ltd*
		Mr Silvester Prakasam	*Land Transport Authority*
		Mr Quek Han Lim	*Network for Electronic Transfers (S) Pte Ltd*
		Mr Samuel Quek	*RadianTrust Pte Ltd*
		Mr Winstedt Rasiah	*Land Transport Authority*
		Mr Holger Roessner	*ACG (Asia Pacific) Pte Ltd*
		Mr Tam Chek Fran	*Immigration Checkpoints Authority*
		Mr Tam Chi Keung	*National Library Board*
		Mr Tan Keng Boon	*Advanced Card Systems Ltd*
		Mr Tan Koh Hock	*ST Electronics (Large Scale Systems Group)*
		Mr Tan Kok Tian	*ASK*
		Dr Tan Poh Chuan	*Hewlett-Packard Singapore (Sales) Pte Ltd*
		Mr Tan Swee Cheng	*Renesas Technology Singapore Pte. Ltd.*

Member	:	Mr Tan Teik Guan	*Data Security Systems Solutions Pte Ltd*
		Mr Tan Tzann Chang	*Institute of System Science*
		Mr Axel Teh	*INSIDE Contactless Asia Pacific*
		Mr Teh Kor Lak	*Azuren Services*
		Mr Teo Poh Soon	*SafeNet Singapore*
		Mr Raymond Teo	*Gemalto*
		Mr Davion Than	*Stoval Technologies Pte Ltd*
		Mr Philip Thong	*Giesecke & Devrient Asia Pte Ltd*
		Mr John Tze	*Asis Technologies Pte Ltd*
		Mr Raman Venky	*Unisys Singapore*
		Mr Simon Wu	*Samsung Asia Pte Ltd*
		Mr Yap Tek Seng	*Digital Imaging Asia Pacific Pte Ltd*
		Dr Yau Wei Yun	*Institute for Infocomm Research*
		Mr Anthony Yeap	*SCM Microsystems (Asia) Pte Ltd*
		Mr John Yong	*Symantec*
		Mr Yu Chien Siang	*Ministry of Home Affairs*
		Mr Michael Yu	*WatchData Technologies Pte Ltd*

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	:	Mr Lin Yih
Members	:	Mr Anthony Hay
		Mr Samnoeuk Khim
		Mr Koh Kim Huat
		Mr Lim Hwee Kwang
		Mr Lim Shih Hsien
		Mr Farouk Musthafa
		Mr Samuel Quek
		Mr Wilson Tan
		Mr Raymond Teo

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

CISCO Computer Security
Digital Applied Research and Technology Pte Ltd
Gemalto
Giesecke & Devrient Asia Pte Ltd
Infocomm Development Authority of Singapore
MINDEF CIO Office
Ministry of Home Affairs
NEC Solutions Asia Pacific Pte Ltd
Oberthur Card Systems Asia Pacific Pte Ltd
RadianTrust Pte Ltd

Contents

Page

Foreword 7

CLAUSES

Section One – General

0 Introduction 8

1 Scope 8

2 Normative references 9

3 Definitions/Abbreviated terms 10

Section Two – Data structures

4 Overview of data structures 10

4.1 Data group definition 10

4.2 EF.COM 11

4.3 EF.DG1 12

4.4 EF.DG2 13

4.5 EF.DG3 13

4.6 EF.DG11 13

4.7 EF.DG13 15

4.8 EF.DG15 18

4.9 EF.ACL 20

4.10 EF.SOD 21

4.11 EF.PFD 21

Section Three – Security and smart card commands

5 Security 21

5.1 Additional authentication 22

5.2 Data group access control 22

5.3 Data confidentiality 23

5.4 Distribution and protection of EAC key 23

6 Smart card commands 24

6.1 Application selection 24

6.2 EF selection 24

6.3 Reading binary data 25

6.4 Reading large binary data file 25

6.5 PIN verification 26

6.6 Internation authenticate 27

6.7 Get challenge 27

Page

6.8 External authenticate 27
6.9 Secure messaging 28
6.10 Data group update mechanism 28

Section Four – Additional requirements
7 Unique card serial number 28
7.1 Get Card Serial Number command 28
8 AID (application ID) 28
9 Guidelines for smart card reader 29
10 Guidelines for migration 29
11 Guidelines for elliptic curve cryptography 29

ANNEXES

A Elliptic curve specification 31
B Sample SOD with ECDSA 35

TABLES

1 Overview of data groups 11
2 Items within EF.COM 11
3 Items within EF.DG1 12
4 Items within EF.DG11 14
5 Items within EncryptedEACKeyInfo 16
6 Items within subject distinguish name 16
7 Structure of EF.DG13 16
8 Example of EncryptedEACKeyInfos 17
9 Example of RSA public key 18
10 Example of ECC public key 19
11 EF.ACL definition 20
12 Authentication methods 22
13 List of authentication operation and key 23
14 ASN.1 length encoding 25
15 Mapping of 16-byte sectors 29

Foreword

This Singapore Standard is prepared by the Cards and Personal Identification Technical Committee under the purview of the IT Standards Committee.

The technical committee develops national standards in the area of smart card, smart card reader application programming interface (API), cryptography and biometrics as applied to smart card and personal identification.

This standard specifies the structure, security and access conditions for data structures that are stored on a smart card or smart chip-enabled devices.

In preparing this standard, reference was made to the following publications:

ISO/IEC 7816-4 : 2005	Organisation, security and commands for interchange
ICAO Doc 9303 Part 1 Vol 2	Specifications for electronically enabled passports with biometric identification capability
ISO/IEC 14443-4	Transmission protocol
ISO/IEC 19794-2	Finger minutiae
ISO/IEC 19794-5	Face image data
ISO/IEC 15444-1	JPEG 2000 image coding system
Federal Information Processing Standard (FIPS) 46-3	Data Encryption Standard (DES)
Federal Information Processing Standard (FIPS) 197	Advanced Encryption Standard (AES)
Federal Information Processing Standard (FIPS) 186-2	Digital Signature Standard (DSS)
Standards for Efficient Cryptography	SEC1: Elliptic Curve Cryptography
American National Standard X9.62	The Elliptic Curve Digital Signature Algorithm (ECDSA)
PKCS #1	RSA Cryptography Standard
SS 372 : Part 4 : 1999	Specification for identification cards – Integrated circuit(s) cards with contacts, Part 4 : interindustry commands for interchange

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

This standard is expected to be used by issuers of smart cards that contain data for personal identification. It can also be used by developers of smart card readers and application software that need to read and verify these smart cards.

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 Smart Card ID

Section One – General

0 Introduction

Nowadays it is quite common for a person to carry more than one card that identifies the owner of the card. It may be a card that is issued by a government agency, such as a national identity card, a student card, or a library card. It may be a card issued by a private agency such as a staff card, a club membership card or a loyalty programme card. They all carry similar information: name, sex (gender), age or date of birth, some kind of unique identification number, and perhaps address. However there is a lack of standard to define the structure and placement of these data. For example, the name can be of different length, font, and position for different ID cards. Similarly the dimension and resolution of the photograph can be different. Technically, it is costly to do automated reading and verification of cards from different issuers. One has to use different hardware equipment and software to cope with the diversity. Hence there is a need to have a standard to define a basic minimum set to achieve some interoperability while allowing optional items for specific needs.

This standard specifies the data structure, security and access conditions for a smart card that contains personal identification data. This standard can also be used by smart chip-enabled devices such as handheld computing devices (personal digital assistants – PDAs), watches and mobile phones. The smart card or smart chip-enabled devices can communicate by contact or contactless means, and they only need to comply with the data structures, security and application protocol data units (APDUs) specified in this standard.

The trust model and data structure defined in this standard is based on the e-passport specifications developed by ICAO (International Civil Aviation Organisation). This is a deliberate design decision so that with minimum change, smart card readers that can read international electronic passports can also be used to read smart cards and devices that comply with this standard. Like e-passports, this standard requires that all data be digitally signed so that the data can be trusted. The choice of “which card can be trusted” is a decision to be resolved between the card issuer and the party who wants to verify the card.

1 Scope

This standard defines the data structure, security architecture and command set for a smart card with identification data. Some of the requirements are mandatory and some are optional. When optional parts are implemented, they shall comply with this standard.

By offering mandatory and optional parts, this standard allows "application profiles" to be created for different security requirements, cost requirements and ease of usage. The minimum memory requirement for the base mandatory data set is less than 1 kilobyte. The smart card need not have any cryptographic capability – but the data set can be cloned. In this case, the verifier shall ensure that the data does belong to the card holder. A card with cryptographic capability will eliminate this vulnerability.

Annex A contains a description of four elliptic curves. For the purpose of interoperability, usage of a curve not described in Annex A is not recommended.

This standard does not cover physical aspects such as printing and positioning of the name and photo on the surface of the card. Its main focus is the data and security aspects that are required for electronic reading and processing. Furthermore, the specification covers only data for identification, and not any other data. Hence a smart card may contain multiple applications such as electronic payment (e-purse) and loyalty points, but only the identification data portion is covered by this standard.

This standard also does not attempt to address the legal and certification aspects of the trust framework.

2 Normative references

The following referenced 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 ISO/IEC 7816-4: 2005	Organisation, security and commands for interchange
ICAO Doc 9303 Part 1 Vol 2	Specifications for Electronically Enabled Passports with Biometric Identification Capability
ISO/IEC 7816-6: 2005	Interindustry data elements for interchange
ISO/IEC 14443-1	Physical characteristics
ISO/IEC 14443-2	Radio frequency power and signal interface
ISO/IEC 14443-3	Initialization and anticollision
ISO/IEC 14443-4	Transmission protocol
ISO/IEC 7816-3	Electronic signals and transmission
ISO/IEC 7816-8	Commands for security operations
ISO/IEC 7816-9	Card and file management
ISO/IEC 19794-2	Finger minutiae
ISO/IEC 19794-5	Face image data
ISO/IEC 15444-1	JPEG 2000 image coding system
Federal Information Processing Standard (FIPS) 46-3	Data Encryption Standard (DES)
Federal Information Processing Standard (FIPS) 197	Advanced Encryption Standard (AES)
Federal Information Processing Standard (FIPS) 186-2	Digital Signature Standard (DSS)
Standards for Efficient Cryptography	SEC1: Elliptic Curve Cryptography
American national standard X9.62	The Elliptic Curve Digital Signature Algorithm (ECDSA)
PKCS #1	RSA Cryptography Standard
SS 372 : Part 4 : 1999	Specification for identification cards – Integrated circuit(s) cards with contacts. Part 4 : interindustry commands for interchange
SmartVIP lite multi-factor authentication, published by Ministry of Home Affairs (MHA)	
Intelligent nation biometric access controls, published by Ministry of Home Affairs	
SVIP – Technical Specification v1.4, jointly published by Infocomm Development Authority (IDA) and Ministry of Home Affairs	