SS 529:2006(2023)
(ICS 35.240.15)

SINGAPORE STANDARD

Smart Card ID

Confirmed and classified as a mature standard 2023

Singapore Standards Council

SS 529:2006(2023)
(ICS 35.240.15)

SINGAPORE STANDARD

Smart Card ID

Published by Enterprise Singapore

ISBN 981-4154-47-4

Contents

Page

ANNEXES

TABLES

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 the 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.

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. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as "mature standards". Mature standards will not be subject to further review, unless there are requests to review such standards.*

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 and the Singapore Standards Council 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. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*

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.