
Review of specification for Smart Card ID of Singapore

Cheon, Sungrock(johncheon@korea.com)

Overview

- Purpose

- ❑ To grab chance to proliferate this specification as Asian e-ID card
- ❑ To fulfill missing item
- ❑ To Cultivate diverse applications

- What we did

- ❑ KEPIA's internal WG1(IC card standardization group) reviewed and had 5 times F2F meetings
- ❑ Implemented this specification on Open platform
- ❑ Implemented standard Viewer S/W

- Refer to the previous presentation done by Mr. Yih

Characteristics of SS-ID

- Necessity
 - Individuals carry plural ID cards for their identification
 - Each ID cards contain identical, similar information like name, address, and ID number.
 - Needs standardization
- Specifies the data structure, security and access conditions for a smart card that contains personal identification data.
- The trust model and data structure is based on the e-passport specifications developed by ICAO.
- Does not say about physical issues

Normative references

ISO/IEC 7816-4: 2005	Organization, 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
SmartVIP Lite Multi-Factor Authentication	Published by Singapore Ministry of Home Affairs (MHA)
Intelligent Nation Biometric Access Controls	Published by Singapore Ministry of Home Affairs
SVIP – Technical Specification v1.4	Joint publication by Singapore Infocomm Development Authority (IDA) and Ministry of Home Affairs

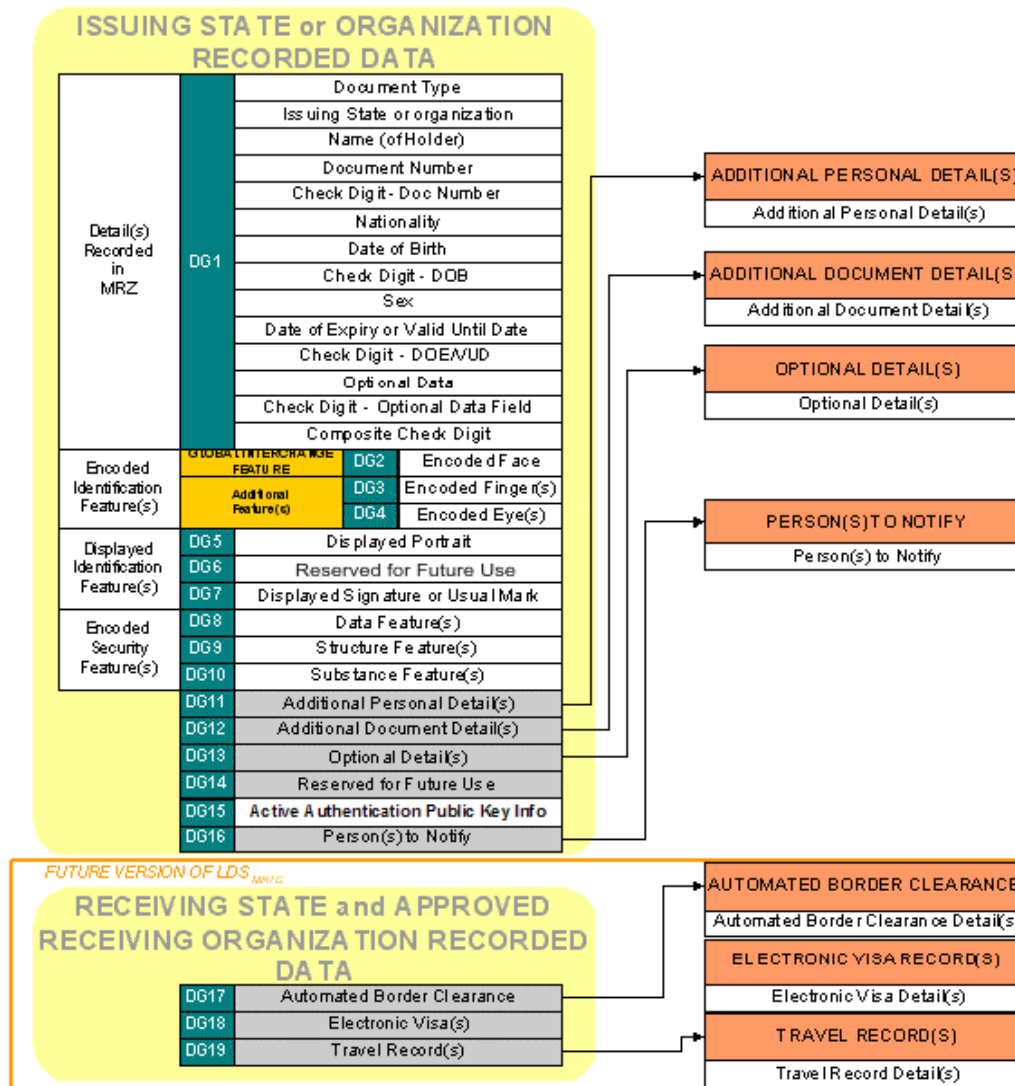
Data structure

- Personal ID data is organized into eleven DGs(Data Groups) and stored in EFs(Elementary Files).
- Similarity and compatibility to e-passport spec.
- Four main DGs
 - DG1 : main personal data
 - DG11 : additional personal data
 - DG2 : Facial image
 - DG3 : Fingerprint
- Four mandatory data and others are optional.

Data groups

Data Group Name	Identifier	EFID	SFID	Tag	Size	Req	Remarks
Common Data	EF.COM	'011E'	'1E'	'60'	≈32	M	As per e-passport, a tag list of DGs
MRZ data	EF.DG1	'0101'	'01'	'61'	93	M	As per e-passport with slight variance in interpretation
Encoded Face	EF.DG2	'0102'	'02'	'75'	≈4096 or 8192	O	Color JPEG2000, compressed from 240 x 320 or 320 x 427 respectively
Encoded Finger	EF.DG3	'0103'	'03'	'63'	Up to ≈1024	O	Finger minutiae template, may be proprietary
Additional Personal Details	EF.DG11	'010B'	'0B'	'6B'	≈256 or more	M	TLV structure
Optional Details	EF.DG13	'010D'	'0D'	'6D'	≈2048 or more	O	Storage of encryption keys for fingerprint DG3 access control
Authentication Key	EF.DG15	'010F'	'0F'	'6F'	≈256 or more	O	Either RSA or ECC public key, or a symmetric secret key to be used by INTERNAL AUTHENTICATE
Access Control List	EF.ACL	'011A'	'1A'	'7A'	≈128	O	Door access control list in ASN.1 structure
Security Data Object	EF.SOD	'011D'	'1D'	'77'	≈512 or more	M	SHA-256 hashed and signed using RSA or ECDSA
Personal Folder	EF.PFD	'011B'	'1B'	'7F'	≈2048	O	Reserved for future use

Data groups of e-Passport



EF.COM

Tag	Length	Value
'5F01'	04	LDS version, in ASCII characters, defined to be "8001" in this standard. This version number is different from e-passport (usually the value "0107")
'5F36'	06	Unicode version, in ASCII characters, defined to be "040000" in this standards
'5C'	X	Tag list. List of data groups present

Logical Data Structure (LDS): The collection of groupings of Data Elements stored in the optional capacity expansion technology.

Tag of
EF.COM

Length of
Value field

'60'15'

'5F01' '04' '38303031'

'5F36' '06' '303430303030'

'5C' '03' '616B77'

EF.DG1

S/N	Name of Data Element	Size	Req	Remarks
1	Document Type	2	M	"ID"
2	Issuing State or Organization	3	M	“SGP”
3	Name of Holder	39	M	As per ICAO 9303
4	Document Number	9	M	e.g. NRIC, FIN
5	Check digit – document number	1	M	As per ICAO 9303
6	Nationality	3	M	As per ICAO codes
7	Date of birth	6	M	As per ICAO 9303
8	Check digit – date of birth	1	M	As per ICAO 9303
9	Sex (gender)	1	M	“M” or “F”
10	Date of expiry or valid until date	6	M	YYMMDD format
11	Check digit – date of expiry	1	M	As per ICAO 9303
12	Check digit - composite	1	M	As per ICAO 9303

EF.DG11

Item Name	Short Description	Type	Tag	Size	Req	Remarks
UIN	Unique Identification Number	C	'5F 10'	9	M	For example: NRIC, FIN, Staff ID
Name	Full Name	C	'5F 0E'	66	M	
Gender	Gender	C	'5F 35'	1	M	“M” or “F”
Race	Race or ethnic group	C	'76 01'	16	M	
Date_of_birth	Date of Birth	C	'5F 2B'	18	M	YYYYMMDD format
Country_of_birth	Country of Birth	C	'5F 11'	20	M	
Citizenship	Citizenship	C	'5F 2C'	2	M	As per IANA (Internet Assigned Numbers Authority)
Address_registered	Address as in NRIC	C	'5F 42'	69	M	
Date_issue	Date of issue	C	'5F 26'	8	M	YYYYMMDD format
Date_expiry	Date of expiry	C	'59'	8	M	YYYYMMDD format
Date_last_update	Date of last update		'76 07'	8	M	YYYYMMDD format

EF.SOD

```
LDSSecurityObject ::= SEQUENCE {  
    version                LDSecurityObjectVersion,  
    hashAlgorithm          DigestAlgorithmIdentifier,  
    dataGroupHashValues   SEQUENCE SIZE (2..ub-DataGroups) OF  
                          DataGroupHash  
}  
DataGroupHash ::= SEQUENCE {  
    dataGroupNumber       DataGroupNumber,  
    dataGroupHashValue   OCTET STRING  
}
```

Security

- Security Control Option
 - Hash, Sign (except EF.PFD)
 - Read prohibited (Use EF.SOD)

- Process
 - Verify Hash, Sign (EF)
 - Check Hash, Sign (ex) External Auth
 - Additional Authentication
 - PIN, Internal Auth (AES, T-DES, RSA)

Data group access

- Free read
 - EF.COM, EF.DG1, EF.DG2, EF.DG11, ACL, EF.SOD

- EF.DG3 (finger print)
 - Protect option
 - Content is not encrypted but read access require a authentication process (or)
 - Content encrypted and data group is free read
 - External Auth
 - Not protected by access control
 - Mandatory : AES-256
 - Alternative : T-DES

Data group access

- EF.DG15 (Internal Auth)
 - Symmetric Key (AES-256, T-DES)
 - Asymmetric Key (RSA, ECC Public Key)

Distribution & Protection of EAC Key

- EAC Key (used to control access to EF.DG3)
 - Random number
 - Different for each card
- Distribution & Protection
 - Encrypted using an asymmetric key
 - Stored in EF.DG13 (each authorized verifier)
- Generate Asymmetric Key to be used to encrypt EAC Key
 - Issuer -> verifier (or)
 - Issuer <- verifier

Command

- Select File
- Read Binary (normal, large)
- PIN verification (verify, change)
- Internal Authentication
- External Authentication
- Get Challenge

Other issue

- Secure Messaging &
 - Recommend ISO7816-4

- Data group update
 - proprietary

Additional requirements

- Unique card serial number
 - Contact : ATR - Historical bytes
 - Contactless
 - Type A : ATS (Answer to Select)
 - Type B : 7816-4 Command

- AID
 - D0 00 00 XX XX 00 01
(XX XX - Singapore national Stands)

Additional requirements

- Smart Card Reader
 - Offline Authentication
 - Use SAM (ECDSA, AES256, 3DES) - Internal Auth
 - If there is a need to maintain “black list” or “white list” then unique identifier shall be
Card Serial Number + UIN (in EF.DG11)

Implementation

- Used card
 - OCS ID-One
 - GP2.1.1
 - Multi Security Domain
 - Delegated Management
 - DAP verification
 - Java Card 2.2
 - Dual Interface(ISO7816, ISO14443 Type A)
 - T=0, T=1, T=CL
 - 72K EEPROM
 - AES256, DES, RSA(2048bits), SHA-1
 - BioAPI

Implementation

- Applet development environment
 - Eclipse2.1
 - Emulator : JCOP30 plug-in
- Standard Reader S/W
 - Refer to Golden Reader Tool




E-ID Reader

Reader Connect
 Mifare RF Reader Connect Disconnect

Operation
Read Elapsed time 0.474 Seconds

Personal Data

	Name	JOHN T	Surname	SMITH
	Date of Birth (yy.mm.dd)	740622	Nationality	HMD
	Sex	M	Valid until (yy.mm.dd)	101231
	Document Number	123456789	Document Type	P
	Issuer	ATA	Optional Data	0121
	Chip Data	UID: B0771E94 ATR/ATS: 10 78 B3 C0 02 00 31 C0 64 77 E9 10 00 00 90 00 00 00		

Exit

Evaluation

- Return Codes should be defined in detail.
- Personalization flow should be defined.
- Consider concrete countermeasure to new threatening method
 - RF Dump
 - CSN is important

Application

- We should think of multi application.
- Pure ID card
- Traveler's card
- Point card
- Network gaming