Card Layout for Driving License Card

Version 1.5 dated 08-04-2004

Table of Contents

Introduction

In this document, layout of the DL card is described. All the cards described in this document are multi-function SCOSTA compliant smart cards. Only the machine-readable zone data format is described in this document. The visual printed details on the two sides of the cards are not described and such details are out of scope of this document.

Related Documents

- Specifications for the Smart-Card Operating System for Transport Applications (SCOSTA) v1.2b dated March 15, 2002
- Addendum to Smart Card Operating System Specification v 1.2b Dated July 31, 2002
- Errata to Smart Card Operating System Specification v 1.2b Dated July 10, 2002
- Addendum to SCOSTA 1.2b dated 23rd January 2003.
- Errata to SCOSTA 1.2b dated 23rd January 2003.
- Key Management System for the Driving License (DL) Application v1.0 dated Feb 15, 2002
- Application Specifications for the DL related operations v 1.1 dated August 10, 2002

Various Cards

- Driving License Card (DL)
- Issuing Authority –I (IA1)
- Issuing Authority –II (IA2)
- Endorsing Authority (EA *e.g.* Police)
- Reviewing Authority (RA *e.g.* Judiciary)
- State Key Managing Authority (SKMA *aka* State Government Agency)

Structure of the Blank Cards

The blank cards will be SCOSTA compliant and will have a MF without any security conditions attached for creating DF and EF within the DF. The FCP of the MF will have at least the following contents.

FDB = 38H, File identifier 3F00H, LCSI = 05H (activated).

Data structures relevant to this document

The following data structures are used.

Integers

Application data items that are integers will be stored in files using the packed BCD representation. That is, one byte will store two digits of the integer. Thus the number of bytes required to store a 2*n* digit integer will be *n*. The digits will be stored in a fashion that the most significant digit is written first.
For example, a 6 digit integer 123456 will be stored in the file as 12H, 34H, and 56H.

Strings

The strings will be stored in the ASCII format. The size of the strings will be fixed as per the details given for each data element. There will not be any termination pattern (such as null termination etc.). All unused bytes of the string will be stored as blanks by the applications.

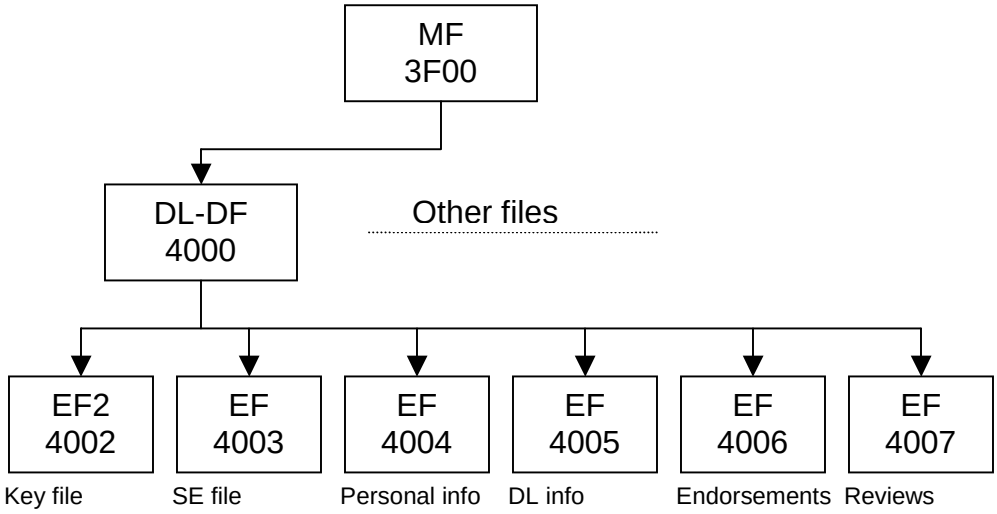
Date

The dates will be stored as a 8 digit integer in packed BCD format in the ddmmyyyy format.

For example, February 21, 2002 will be stored as integer 21022002 (i.e. individual bytes are 21H, 02H, 20H, 02H).

DL card Layout

The DL card will have a file structure shown below.



The key file EF2 will contain CR, CE, CT and CV keys in that order. The keys are numbered as 1, 2, 3 and 4 respectively.

Directory DL-DF

The directory DL-DF will have the following FCP.

Tag	Len	Value	Remarks
82	01	38	FDB only
83	02	40 00	File identifier
84	10	DL	DF Name (To be Padded with Spaces)
8A	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state)
8C	08	7F 23 23 23 23 FF FF 23	Security Attributes. AM Byte: 7F Delete self (SE#3) Terminate DF (SE#3) Activate (SE#3) Deactivate (SE#3) Create DF (child): Never Create EF (child): Never Delete child (SE#3)
AB	06	84 02 22 2A 97 00	Security Attributes: Expanded form. MSE, PSO commands never allowed
8D	02	40 03	File id of the SE file

Key File EF2

The key file will have the following FCP.

Tag	Len	Value	Remarks
82	05	0C	FDB (Linear variable record internal EF)
		01	DCB (Write once, 1 byte Data unit)
		00 16	MRL (22 bytes)
		04	No. of records (4 keys)
83	02	40 02	File identifier
88	01	10	Short EF id 02 coded in 5 MSBs
8A	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state)
8C	06	6B	Security Attributes. AM Byte: 6B
		23	Delete self: (SE#3)
		23	Terminate EF: SE#3
		23	Deactivate EF: SE#3
		FF	Update record: Never
		FF	Read record: Never

The EF2 will have the following records.
Record 1: Key CR (Key #1, valid for external auth, usage counters, algorithm reference 00 (valid for all), 16 byte key.

81 01 FF 00 <16 byte CR>

Record 2: Key CE

82 01 FF 00 <16 byte CE>

Record 3: Key CT

83 01 FF 00 <16 byte CT>

Record 4: Key CV

84 03 FF FF FF 00 <16 byte CV>

SE File

The SE file will have the following FCP.

Tag	Len	Value	Remarks
82	05	0C	FDB (Linear variable record internal EF)
		01	DCB (Write once, 1 byte Data unit)
		00 14	MRL (20 bytes)
		04	No. of records (4 SEs)
83	02	40 03	File identifier
88	01	18	SFI 03 coded in 5 MSBs
8A	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state)
8C	06	6B	Security Attributes. AM Byte: 6B
		23	Delete self: SE#3
		23	Terminate EF: SE#3
		23	Deactivate EF: SE#3
		FF	Update record: Never
		FF	Read record: Never

The SE file will have the following records.

Record 1: SE #1 External Auth with Key CR
80 01 01 // SE #1
A4 06 83 01 81 95 01 80 // AT Template, key reference 81, use for
// external auth
Record 2: SE #2 External Auth with Key CE
80 01 02 A4 06 83 01 82 95 01 80
Record 3: SE #3 External Auth with Key CT
80 01 03 A4 06 83 01 83 95 01 80
Record 4: SE#4 External Auth with Key CR, CE or CT or CV
80 01 04 A4 0C 83 01 81 83 01 82 83 01 83 83 01 84 95 01 C0

Personal Info file

The FCP of the personal info file will be as follows.

Tag	Len	Value	Remarks
80	02	00 A0	File size (160 bytes with enough growth space)
82	02	01 41	FDB (Transparent working EF) DCB (Write OR, 1 byte Data unit)
83	02	40 04	File identifier
8A	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state)
8C	06	6E 23 23 23 FF FF	Security Attributes. AM Byte: 6E Delete self: SE#3 Terminate EF: SE#3 Deactivate EF: SE#3 Write EF: Never Update Binary: Never

The contents of the file will include the following as simple TLV data. (The entries in the Max size column are in shown in decimal numbers. All other entries are in hexadecimal number representation)

Field	Tag	Max size	Data format	Example
Version	C0	4 bytes	String	C0 03 “1.00”
Name	C1	40 bytes	String	C1 10 “B V Ramana Kumar”
Father’s Name	C2	40 bytes	String	C2 10 “K V Mohan Murthy”
Date of Birth	C3	4 bytes	Date	C3 04 23 02 19 56
DL Number	C4	16 bytes	String	C4 10 “AP03N1997002433A”
Issuing Authority	C5	16 bytes	String	C5 10 “AP003AR012345RTX”
Date of Issue	CA	4 bytes	Date	CA 04 23 02 20 03
DLSequence Number	CB	9 bytes	String	CB 09 “P12345045”

DL Info file

The FCP of the DL info file will be as follows.

Tag	Len	Value	Remarks
80	02	01 90	File size (400 bytes with enough growth space)
82	02	01 41	FDB (Transparent working EF) DCB (Write OR, 1 byte Data unit)
83	02	40 05	File identifier
8A	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state)
8C	06	6E 23 23 23 FF 23	Security Attributes. AM Byte: 6E Delete self: SE#3 Terminate EF: SE#3 Deactivate EF: SE#3 Write EF: Never Update Binary: SE #3

The contents of the file will include the following as simple TLV data. (The entries in the Max size column are in shown in decimal numbers. All other entries are in hexadecimal number representation)

Field	Tag	Max size	Data format	Example
Version	C0	4 bytes	String	C0 03 “1.00”
Valid till (Transport)	C6	4 bytes	Date	C6 04 23 03 20 11
Valid till (non-transport)	C7	4 bytes	Date	C7 04 10 02 2007
Vehicle info	C8	50 bytes	String	C8 32 <vehicle class and testing authority info>
Badge info	C9	28 bytes	String	C9 1C <badge details>

There can be several TLV for the vehicle info and badge info. All of these will carry the same tag. As per the data-elements, up to four vehicle classes and at most one badge information can be there. The file size is suitably kept at 400 bytes.

Vehicle info TLV will contain *50* bytes string composed of Vehicle class (6 bytes string), Name of testing authority (20 bytes) and designation of testing authority (20 bytes) and respective date of issue (4 bytes) in that order.

Badge info TLV will contain 28 bytes string composed of Badge Number (10 bytes string), last date of validity (4 bytes date), authorization number (10 bytes string) and authorization date (4 bytes date) in that order.

Endorsement file

The FCP of the endorsement file will be as follows.

Tag	Len	Value	Remarks
82	05	03	FDB (Linear fixed record simple TLV working EF)
		01	DCB Write Once (one byte data unit)
		00 5C	MRL (size of each record including Tag and length)
		0A	Number of records
83	02	40 06	File identifier
8A	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state)
8C	05	6A	Security Attributes. AM Byte: 6A
		23	Delete self: SE#3
		23	Terminate EF: SE#3
		23	Deactivate EF: SE#3
		22	Update record: SE#2

The contents of the file will include the records with simple TLV structure. The tags will be a number from 01 to 0A, unique for each record. The same tag will be used in the review file data to cross reference the data. The length of the record will be fixed (92 bytes).

Records 1 to 10 are initialized with corresponding tag 0x01 to 0x0A, length 0x5A and value all zeroes at the time of personalization.

Each record will contain the following.

Field	Size	Data format
Endorsement number	10 bytes	String
Endorsement date	4 bytes	Date
Endorsement Authority id	16 bytes	String
Section/Rule/Proceeding number	60 bytes	10 strings (6 bytes each)

Review file

The FCP of the review file will be as follows.

Tag	Len	Value	Remarks
82	05	03	FDB (Linear fixed record simple TLV working EF)
		41	DCB Write OR (one byte data unit)
		00 25	MRL (size of each record including Tag and length)
		0A	Number of records
83	02	40 07	File identifier
8A	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state)

8C	06	6E	Security Attributes. AM Byte: 6E
		23	Delete self: SE#3
		23	Terminate EF: SE#3
		23	Deactivate EF: SE#3
		21	Write record: SE#1
		21	Update record: SE#1

The contents of the file will include the records with simple TLV structure. The tags will be a number from 01 to 0A, unique for each record. The same tag will be used in the endorsement file data to cross reference the data. The length of the record will be fixed (37 bytes).

Records 1 to 10 are initialized with corresponding tag 0x01 to 0x0A, length 0x22 and value all zeroes at the time of personalization.

Each record will contain the following.

Field	**Size**	**Data format**
Fine	6 bytes	String
Review date	4 bytes	Date
Review Authority id	16 bytes	String
Disqualification period from	4 bytes	Date
Disqualification period To	4 bytes	Date
Backend Update Flag (BUF)	1 Byte	Integer (00 or 01)

BUF will have a value of 00 initially while storing the review details. Once the record is added to the back end database, BUF is updated to 01 using WRITE RECORD command.