A few forumers asked me questions regarding reading of MyKad surface information. The answer is there is no encryption; it is just about knowing what (APDU) command to send.

There will be 5 APDU commands that I'll introduce. I name them as:

* Select Application
* Get Response
* Set Length
* Select Info
* Read Info

Instead of viewing a particular command to read "Name", another command to read "IC no.", it is better to interpret a sequence of 3 commands (Set Length, Select Info, Read Info) as "reading a section (or the whole) file". The fact is "Name", "IC no." etc are stored in fixed-length fields (padded on the right), and concatenated together (without separator) to form files. For example,

"Name" stored in file jpn-1-1, offset 0x00E9, length 0x28

"IC no." stored in file jpn-1-1, offset 0x0111, length 0x0D

When you want to read "Name", you read jpn-1-1, offset 0x00E9, length 0x28.

When you want to read "IC no.", you read jpn-1-1, offset 0x0111, length 0x0D.

When you want to read both "Name" and "IC no.", you read jpn-1-1, offset 0x00E9, length 0x35.

Conversely, you can read only part of the field; if you want only first 6 digits of "IC no.", read jpn-1-1, offset 0x111, length 6.

Now, the first 2 commands, "Select Application" and "Get Response", are used to select either one of JPN, JPJ, IMM appplication. (Actually you can have 2 active at the same time by using logical channels, but that's a little bit advanced at this stage.) You must select an application after reset, and you'll do it only once except you want to change application.

Reader: 00 A4 04 00 0A A0 00 00 00 74 4A 50 4E 00 10 (Send 10 bytes data, expect receive 0 bytes)

Card : 61 05

Reader: 00 C0 00 00 05 (Send 0 bytes data, expect receive 5 bytes)

Card : 6F 03 82 01 38 90 00

"00 A4 04 00 0A" is the "CLA INS P1 P2 P3" for "Select Application". The data part of the APDU consists of 10 bytes: "A0 00 00 00 74 4A 50 4E 00 10". The "A0 00 00 00 74" and "00 10" parts are constant. "4A 50 4E" represents "JPN". Change to "JPJ" or "IMM" for those applications. "00 C0 00 00 05" is the "CLA INS P1 P2 P3" for "Get Response". The 5 data bytes received is not significant, but you can verify whether it is successful.

That's the end of description of "Select Application" and "Get Response". Now move on to the 3 commands to read a section of file.

Example: read jpn-1-1, offset 0x00E9, length 0x28.

Reader: C8 32 00 00 05 08 00 00 28 00

Card : 91 08

Reader: CC 00 00 00 08 01 00 01 00 E9 00 28 00

Card : 94 28

Reader: CC 06 00 00 28

Card : 4D 59 20 4E 41 4D 45 20 20 20 20... 90 00

Green is length

Red is offset

Blue is jpn1-1 based on

**static final** String ***JPN***[] = { **"00 00 01 00"**, *//just an empty so can get JPN[1] for JPN\_1\_1, look prettier*

**"01 00 01 00"**,

**"02 00 01 00"**,

**"03 00 01 00"**,

**"04 00 01 00"**,

**"05 00 01 00"**,

**"06 00 01 00"**};

The 3 commands "Set Length", "Select Info", and "Read Info" are shown above. The colored parts are those which varies. It seems from above that the maximum length will be 0xFF, so you'll have to break long file section (particularly when reading JPEG) into multiple reads (repeat the 3 commands with different length and offset). But actually, for advanced users, you can specify a length >= 0x0100, (provided you don't read past the end of file which results in no bytes returned,) in the "Set Length" and "Select Info". You only need multiple "Read Info", with the single byte length set to big a number (eg. 0xFF or 0xFC), except the last read. "Read Info" is just like retrieving out from a FIFO buffer, you can read however you want, but don't over-read it.

To read jpn-1-4, replace 01 00 01 00 to 04 00 01 00.

Those double byte "Offset" and "Length" are in little endian.

Tables:

jpn-1-1

Offset Length Length SDK Function Name Description

(Hex) (Dec)

0000 03 3 01 04 24

0003 96 150 JPN\_OrgName original name

0099 50 30+30+20 JPN\_GMPCName GMPC name

00E9 28 20+20 JPN\_KPTName KPT name

0111 0D 13 JPN\_IDNum ID number

011E 01 1 JPN\_Gender gender

011F 08 8 JPN\_OldIDNum old ID number

0127 04 4 JPN\_BirthDate date of birth

012B 19 25 JPN\_BirthPlace place of birth

0144 04 4 JPN\_DateIssued date issued

0148 12 18 JPN\_Citizenship citizenship

015A 19 25 JPN\_Race race

0173 0B 11 JPN\_Religion religion

017E 01 1 JPN\_EastMalaysian East Malaysian

017F 02 2 JPN\_RJ RJ?

0181 02 2 JPN\_KT KT?

0183 0B 11 JPN\_OtherID other ID

018E 01 1 JPN\_Category category

018F 01 1 JPN\_CardVer card version

0190 04 4 JPN\_GreenCardExpiry green card expiry date

0194 14 20 JPN\_GreenCardNationality green card nationality

01A8 23 35 All 00

jpn-1-2

0000 03 3 01 40 03

0003 FA0 4000 JPN\_Photo JPEG photo

0FA3 08 8 All 00

jpn-1-3

0000 03 3 01 12 03

0003 14 20 "R1L1",0,0...

0017 256 598 JPN\_Thumb1 thumprint 1 (right thumb)

026D 256 598 JPN\_Thumb2 thumprint 2 (left thumb)

04C3 08 8 All 00

jpn-1-4

0000 03 3 01 01 52

0003 1E 30 JPN\_Address1 address line 1

0021 1E 30 JPN\_Address2 address line 2

003F 1E 30 JPN\_Address3 address line 3

005D 03 3 JPN\_Postcode postcode

0060 19 25 JPN\_City city

0079 1E 30 JPN\_State state

0097 14 20 FF 00 00...

jpn-1-5

0000 03 3 01 12 00

0003 09 9 JPN\_SocsoNum socso number

000C 1F 31 All 00

jpn-1-6

0000 03 3 01 17 00

0003 0A 10 JPN\_Locality locality

000D 1E 30 All 00

jpj-1-1

Offset Length Length SDK Function Name Description

(Hex) (Dec)

0000 03 3 01 04 16

0003 01 1 JPJ\_OwnerCategory owner category

0004 0C 12 JPJ\_LicenseType licence type

0010 1E 30 JPJ\_VehicleClass vehicle class

002E 06 6 JPJ\_PSVUsage PSV usage

0034 96 150 JPJ\_PSVDesc PSV description

00CA 06 6 JPJ\_GDLUsage GDL usage

00D0 96 150 JPJ\_GDLDesc GDL description

0166 20 32 JPJ\_ValidityPeriod validity period

0186 14 20 JPJ\_HandicappedReg handicapped registration

019A 01 1 JPJ\_KejaraPoints kejara points

019B 01 1 JPJ\_SuspensionNum suspension number

019C 04 4 JPJ\_LastKejaraUpdate last kejara update

01A0 0B 11 All 00

imm-1-1

0000 03 3 01 22 00

0003 0C 12 IMM\_PMAPassportNum PMA passport number

000F 03 3 IMM\_PMADocType PMA document type

0012 04 4 IMM\_PMAExpiryDate PMA expiry date

0016 15 21 All 00

imm-1-2

0000 03 3 01 22 00

0003 0C 12 IMM\_PMTSporePassportNum PMT S'pore passport no

000F 03 3 IMM\_PMTSporeDocType PMT S'pore doc type

0012 04 4 IMM\_PMTSporeExpiryDate PMT S'pore expiry date

0016 15 21 All 00

imm-1-3

0000 03 3 01 22 00

0003 0C 12 IMM\_PMTBruneiPassportNum PMT Brunei passport no

000F 03 3 IMM\_PMTBruneiDocType PMT Brunei doc type

0012 04 4 IMM\_PMTBruneiExpiryDate PMT Brunei expiry date

0016 15 21 All 00

imm-1-4

0000 03 3 01 22 00

0003 0C 12 IMM\_PMTResvPassportNum PMT Resv passport no

000F 03 3 IMM\_PMTResvDocType PMT Resv doc type

0012 04 4 IMM\_PMTResvExpiryDate PMT Resv expiry date

0016 15 21 All 00

SDK Function Name Data type Data when unused (hex)

JPN\_OrgName string

JPN\_GMPCName stringM

JPN\_KPTName stringM

JPN\_IDNum string

JPN\_Gender 'L' or 'P'

JPN\_OldIDNum string

JPN\_BirthDate date

JPN\_BirthPlace string

JPN\_DateIssued date

JPN\_Citizenship string

JPN\_Race string

JPN\_Religion string

JPN\_EastMalaysian ' ' or ? 20

JPN\_RJ ? 20 20

JPN\_KT ? 20 20

JPN\_OtherID string spaces

JPN\_Category ? 20

JPN\_CardVer 02?

JPN\_GreenCardExpiry date 00 00 00 00

JPN\_GreenCardNationality string spaces

JPN\_Photo JPEG

JPN\_Thumb1 thumbprint

JPN\_Thumb2 thumbprint

JPN\_Address1 string

JPN\_Address2 string spaces

JPN\_Address3 string spaces

JPN\_Postcode postcode

JPN\_City string

JPN\_State string

JPN\_SocsoNum string spaces

JPN\_Locality string spaces

JPJ\_OwnerCategory '1' or others

JPJ\_LicenseType 3 char codes spaces

JPJ\_VehicleClass 3 char codes spaces

JPJ\_PSVUsage string spaces

JPJ\_PSVDesc string spaces

JPJ\_GDLUsage string spaces

JPJ\_GDLDesc string spaces

JPJ\_ValidityPeriod dates zeros

JPJ\_HandicappedReg string spaces

JPJ\_KejaraPoints ? 00

JPJ\_SuspensionNum ? 00

JPJ\_LastKejaraUpdate date 00 00 00 00

IMM\_PMAPassportNum string spaces

IMM\_PMADocType 3 char code spaces

IMM\_PMAExpiryDate date 00 00 00 00

IMM\_PMTSporePassportNum string spaces

IMM\_PMTSporeDocType 3 char code spaces

IMM\_PMTSporeExpiryDate date 00 00 00 00

IMM\_PMTBruneiPassportNum string spaces

IMM\_PMTBruneiDocType 3 char code spaces

IMM\_PMTBruneiExpiryDate date 00 00 00 00

IMM\_PMTResvPassportNum string spaces

IMM\_PMTResvDocType 3 char code spaces

IMM\_PMTResvExpiryDate date 00 00 00 00

Types:

string

ANSI/ASCII code character string, not null terminated, space (0x20) padded

stringM

ANSI/ASCII code character string, not null terminated

multi-line, each line is space (0x20) padded

Example name: Lee Kee Lim @ Lee Key Lim

is coded as

"Lee Kee Lim @ "

"Lee Key Lim "

which is

4C 65 65 20 4B 65 65 20 4C 69 6D 20 20 20 20 20

20 20 20 20 4C 65 65 20 4B 65 79 20 4C 69 6D 20

20 20 20 20 20 20 20 20

date

Four byte, packed BCD, yy yy mm dd

20 01 05 30 (hex) = 30 May 2001

postcode

3 byte, packed BCD

12 34 50 (hex) = 12345

3 char codes (JPJ\_LicenseType)

Four fields of 3-character codes concatenated.

Unused positions are filled with " " (3 spaces).

"PDL" Learner's Licence

"PRB" Probationary (P) Licence

"CDL" Competence Driving Licence

3 char codes (JPJ\_VehicleClass)

Four fields of 3-character codes concatenated.

Unused positions are filled with " " (3 spaces).

"1D " Class D, cars

dates (JPJ\_ValidityPeriod)

Four pairs {Begin, Expire} of date.

Unused positions are filled with zeros.

3 char code (IMM\_\*DocType)

Unknown