**SPESIFIKASI TEKNIS APPLET E-KARIP**

**V1.1**

1. **Spesifikasi Perangkat Keras dan Lunak**

Sistem operasi yang digunakan untuk *Smart Card* e-Karip adalah *Java Card* 2.2.2, yang merupakan *open platform operation system* dan menggunakan protokol ISO-7816 untuk berkomunikasi dengan *card reader*. Dalam penggunaannya, applet e-Karip melakukan komunikasi atau transaksi data baik dengan hardware maupun software pendukung aplikasi e-Karip.

1. **Kebutuhan Minimum Perangkat Keras (*Smart Card*)**

|  |  |
| --- | --- |
| EEPROM | 36 *Kilo Byte* |
| ROM | *8 Kilo Byte* |
| RAM | *4 Kilo Byte* |
| CPU | 16 *bits* |
| 3-DES | Ya ( Kunci Minimal 168 bit) |
| *Mutual Authentication* | Ya |
| Protokol Transmisi | T=1 |
| Unit Perlindungan Memori | Ya |
| Durabilitas *Read/Write* | Minimal 100.000 kali |
| Daya Tahan Penyimpanan Memori | Minimal 25 Tahun |
| Fitur Tambahan | * *Encrypted Memory* * *Internal Clock* * *Anti Cloning* |
| Temperatur Operasional | -25 ˚ C sampai 85˚ C |

1. **Kebutuhan Minimum Perangkat Lunak (*Smart Card Operation System*)**
   1. ISO7816
   2. JavaCard version 2.2.2
   3. GlobalPlatform version 2.1.1
2. **Struktur Data dan File**

Kartu e-Karip berisi applet dengan **Applet ID (AID): A000000255020000.** Implementasi struktur data kartu ini disesuaikan dengan ICAO 9303 (*Tersedianya Master File, Dedicated File,* dan *Elementary File,* beserta mekanisme akses masing-masing file). Semua struktur file pada kartu berupa TLV (*Tag Length Value*). Terdapat 5 buah file record (*binary*) yang tersimpan di dalam applet, yaitu:

1. **ID File1 = 0001,** digunakan untuk menyimpan biodata (ukuran file di kartu 512 bytes).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Tag**  **(byte)** | **Nama Field** | **Panjang Maksimum**  **(byte)** | **Keterangan** |
| 1 | 11 | NoTas / NoPen | 15 | Wajib |
| 2 | 12 | Nama Pensiun | 60 | Wajib |
| 3 | 16 | NoRek | 15 | Wajib |
| 4 | 17 | Jari\_Invalid | 1 | Opsional (0-1) |
| 5 | 21 | Optional\_Bank 1 | 2 | Opsional |
| 6 | 22 | Optional\_Bank 2 | 60 | Opsional |

1. **ID File2 = 0002,** digunakan untuk menyimpan foto (ukuran file di kartu 10 kbytes).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Tag**  **(byte)** | **Nama Field** | **Panjang Maksimum**  **(byte)** | **Keterangan** |
| 1 | 41 | Format Foto | 32 | Opsional – (Contoh: jpg/jpeg,bmp,png) |
| 2 | 42 | Foto | 10200 | Wajib |

1. **ID File3 = 0003,** digunakan untuk menyimpan sidik jari pertama (ukuran file di kartu 512 bytes). Berdasarkan library MOC yang dipakai, sudah di automatisasi besar template fingerprint adalah max  246 bytes.

Keterangan Indeks Sidik Jari:

1 = Jari Kelingking Kiri

2 = Jari Manis Kiri

3 = Jari Tengah Kiri

4 = Jari Telunjuk Kiri

5 = Jari Jempol Kiri

6 = Jari Jempol Kanan

7 = Jari Telunjuk Kanan

8 = Jari Tengah Kanan

9 = Jari Manis Kanan

10 = Jari Kelingking kanan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Tag**  **(byte)** | **Nama Field** | **Panjang Maksimum**  **(byte)** | **Keterangan** |
| 1 | 51 | IndexFinger1 | 1 | Wajib (0 – 10) |
| 2 | 52 | TemplateFingerPrint1 | 246 | Wajib (Jika Jari Valid atau nilai IndexFinger1 ada nilainya) |

1. **ID File4 = 0004,** digunakan untuk menyimpan sidik jari kedua (ukuran file di kartu 512 bytes). Berdasarkan library MOC yang dipakai, sudah di automatisasi besar template fingerprint adalah max  246 bytes.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Tag**  **(byte)** | **Nama Field** | **Panjang Maksimum**  **(byte)** | **Keterangan** |
| 1 | 53 | IndexFinger2 | 1 | Wajib (0 – 10) |
| 2 | 54 | TemplateFingerPrint2 | 246 | Wajib (Jika Jari Valid atau nilai IndexFinger1 ada nilainya) |

Struktur data file di dalam applet e-Karip, dapat dibuat menjadi bagan berikut:

**Master File**

**Dedicated File**

**EF 0003**

**Finger Print1**

**Index1**

**EF 0002**

**Photo**

**EF 0001**

**NoTas/NoPen**

**Nama Pensiun**

**Tanggal Lahir**

**Jenis Pensiun**

**TMT\_Pensiun**

**No Rek**

**Jari Invalid**

**NoTas Rangkap 1,2,3**

**Optional\_Bank 1,2**

**EF 0004**

**Finger Print2**

**Index2**

**Gambar 1. Struktur Data e-Karip**

1. **Format Komunikasi (Perintah APDU)**
2. **SELECT APPLET**

Perintah untuk memilih applet yang digunakan pada kartu e-Karip**.**

**Perintah 🡪 00A40400 <P3> <ID APPLET>**

P3 adalah panjang ID File.

**Contoh 🡪 00A40400 08 A000000255020000**

1. **SELECT FILE**

Perintah untuk memilih file tertentu.

**Perintah 🡪00A40000 <P3> <ID FILE>**

P3 adalah panjang ID File.

**Contoh 🡪00A40000 02 0001**

**00A40000 02 0002**

**00A40000 02 0003**

1. **UPDATE BINARY**

Perintah untuk mengubah isi *file* dengan data yang diinginkan pada *offset* tertentu.

**Perintah 🡪 04D6 <P1> <P2><P3><DATA>**

P1, P2 adalah offset dan P3 adalah panjang data yang akan di update.

**Contoh 🡪04D60000 02 0001**

1. **READ BINARY**

Perintah untuk membaca data pada *elementary file* yang ada pada *offset* tertentu.

**Perintah 🡪04B0 <P1> <P2><P3><LENGTH OF DATA>**

P1, P2 adalah offset dan P3 adalah panjang data yang akan di baca.

**Contoh 🡪 04B00000 02**

1. **Algoritma Keamanan Kartu**

*Secure Access Module* (SAM) bertanggung jawab terhadap enkripsi atau pengamanan data pada aplikasi *Smart Card* e-Karip. Setiap komunikasi yang berlangsung antara Kartu dengan *Reader* yang terintegrasi SAM memerlukan proses *mutual authentication,* dijelaskan dalam diagram alir berikut:

**PDU Command**

**Sam Process Needed**

**Compose PDU Command**

**Proses Result12 Command**

**Result1 + SW1SW2**

**Result Confirmation** **+ SW1SW2**

**Proses Result1 Command**

**Result2 + SW1SW2**

**Process PDU Commands**

**Log and Result**

**Log and Result**

Yes

No

Wrap

Wrap and Execute Command

Wrap

|  |  |
| --- | --- |
| **E-Karip** | **SAM Card** |

**Gambar 2 Aliran Proses *Mutual Authentication***

Berdasarkan aliran proses *Mutual Authentication*, berikut merupakan *command* yang terjadi selama proses autentikasi berlangsung:

1. Pemilihan applet e-Karip.

**e-Karip 🡨 00A40400 08 A000000255020000**

**e-Karip** 🡪 **9000 (*Expected Result*)**

1. Pemilihan applet SAM-Card.

**SAM 🡨 00A40400 08 A000000255010000**

**SAM**  🡪 **9000 (*Expected Result*)**

1. Terminal mengirimkan *command Get Card* ID untuk mendapatkan nomor serial kartu sebanyak 8 *bytes* dan kartu memberikan respon nomor serial kartu dan disimpan dalam variabel. Terminal mengirimkan *command Get Challenge* ke kartu dan kartu mengirimkan respons nomor random dan disimpan dalam variabel.

**e-Karip 🡨 80B8000008 (Get Card ID)**

**e-Karip 🡪 CSN + 9000**

**e-Karip** 🡨 **0084000008 (Get Challenge)**

**e-Karip 🡪 RAN +9000**

1. Terminal mengirimkan *command* + *card* ID (8 *bytes*) + *Random Number* (8 *bytes*) ke SAM. SAM melakukan enkripsi dan meng-generate *heade*r + *cryptogram data* (32 *bytes*) + Mac (8 *bytes*) yang disimpan dalam variable.

**SAM 🡨 002A0000 10 <CSN> <RAN>**

**SAM**  🡪 **Result1 +9000**

1. Result1 diteruskan ke kartu dan kartu merespon dengan *key cryptogram* data (32 *bytes*) + MAC (8 *bytes*)

**e-Karip** 🡨 **Result1**

**e-Karip 🡪 Result2 + 9000**

1. Result2 diteruskan ke SAM dan SAM melakukan otentikasi kunci dan memberikan respon ke terminal apakah koneksi telah berhasil atau gagal.

**SAM 🡨 002A0001 <Length Result2> <Result2>**

**SAM**  🡪 **9000**

Setelah proses autentikasi selesai, *command* untuk memanipulasi data dapat dilakukan, yaitu *Update Binary* dan *Read Binary*.

* + 1. *Update Binary*

Ex : Command yang akan dienkrip adalah A4D60000 03 1164FF

**e-Karip 🡨 00A40400 08 A000000255020000 (Pilih Applet)**

**e-Karip** 🡪 **9000 (Hasil yang diharapkan)**

**SAM 🡨 00A40400 08 A000000255010000 (Pilih Applet)**

**SAM**  🡪 **9000 (Hasil yang diharapkan)**

**[mutual authentication]**

**SAM** 🡨 **002A 0100 08 A4D60000 03 1164FF (Enkrip)**

**SAM 🡪 Result1 + 9000**

**e-Karip** 🡨 **Result1 (Jalankan sebagai PDU Command)**

**e-Karip 🡪 Result2 + 9000**

**SAM 🡨 002A0001 <Length Result2> <Result2>**

**SAM**  🡪 **9000 (Proses berhasil)**

* + 1. *Read Binary*

Ex : Command yang akan dienkripsi 04B00000 02

**e-Karip 🡨 00A40400 08 A000000255020000 (Pilih Applet)**

**e-Karip** 🡪 **9000 (Hasil yang diharapkan)**

**SAM 🡨 00A40400 08 A000000255010000 (Pilih Applet)**

**SAM**  🡪 **9000 (Hasil yang diharapkan)**

**[mutual authentication]**

**SAM** 🡨 **002A 0100 08 04B00000 02 (Enkrip)**

**SAM 🡪 Result1 + 9000**

**e-Karip** 🡨 **Result1 (Jalankan sebagai PDU Command)**

**e-Karip 🡪 Result2 + 9000**

**SAM 🡨 002A 0200 <Length Result2> <Result2>**

**SAM**  🡪 **Result3 + 9000 (Result3 adalah data Read Binary)**

**------ Akhir dari Dokumen -----**