**SPESIFIKASI READER VERIFIKASI APPLET E-KARIP**

**V1.1**

Spesifikasi verifikasi applet e-Karip menjabarkan tentang komunikasi antara kartu, aplikasi, dan *device* yang ada diperlukan dalam komunikasi data e-Karip dimulai dari fingerprint template, transaksi untuk verifikasi sidik jari, hingga penyimpanan data.

1. **Kebutuhan *Template* Sidik Jari**

Aplikasi e-Karip menggunakan aplikasi *finger print identification and matching* dengan spesisfikasi sebagai berikut:

1. Spesifikasi Teknis

* Code Size : < 8192 bytes
* RAM Size : < 600 bytes
* FAR (False Acceptance Rate) : 1 : 1.000.000
* FRR (False Rejection Rate) : 1 : 100
* Template Size : < 256 bytes
* Matching Speed : < 0.6 S ( Tergantung Kartu)

1. Standard yang didukung

* ISO/IEC 7816
* SUN Microsystems Java Card 2.1.2
* Java Card Forum API Version 2.2
* FIPS 140-1 Level-2

1. **Diagram Alir Aplikasi Verifikasi**

Scan Fingerprint

Card

Choose Finger Index

Match ?

Verify Fingerprint

yes

no

Repeat ?

yes

Pdu command

Pdu command

Display Score

Display Score

Get Data from Card

Display Data

Read PDU Command

Get Finger Index

Display Finger Index

Read PDU Command

**Gambar 2. Verifikasi Sidik Jari**

Berdasarkan aliran proses di atas, proses verifikasi sidik jari nasabah dapat dijabarkan sebagai berikut:

1. Aplikasi membaca index sidik jari mana yang telah terdaftar di dalam kartu.
2. Aplikasi menampilkan index sidik jari yang terdaftar di kartu.
3. User memilih sidik jari mana yang akan dipilih untuk proses verifikasi, index sidik jari pertama dan index sidik jarikedua.
4. Sidik jari di-*scan* dengan *device Fingerprint Scanner* yang telah terhubung dengan aplikasi e-Karip.
5. Pastikan kartu dikoneksikan untuk mendapatkan sidik jari yang tersimpan dalam file di kartu.
6. Proses verifikasi berlangsung dengan interaksi PDU Commmand antara kartu dan terminal.
7. Nilai kecocokan ditampilkan dari hasil verifikasi apabila cocok maka akan ditampilkan nilai kecocokan tersebut.
8. Apabila nilai kecocokan tidak sesuai, maka proses verifikasi diulang kembali dari proses awal pengambilan *sample* sidik jari. Nilai kecocokan direkomendasikan minimal 4000.
9. Setelah verifikasi berhasil, aplikasi dapat mengakses data dari kartu.
10. Data yang diinginkan diambil dari kartu dan kemudian ditampilkan ke user.
11. **Spesifikasi Komunikasi (Perintah APDU)**
12. **SELECT APPLET**

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

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

P3 adalah panjang dari ID File

**Contoh 🡪 00A40400 08 A000000255020000**

1. **SELECT FILE**

Perintah untuk memilih file tertentu.

**Perintah 🡪00A40000 <P3> <ID FILE>**

P3 adalah panjang dari 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. **Interaksi Antara SAM dan e-Karip**

|  |  |
| --- | --- |
| **Applet** | **SAM** |
|  |  |

PDU COMMAND

Sam process needed?

Process PDU Command

Process PDU Command

Process Result Command

Result

ess

ess

wrap

Result

ess

ess

No

Yes

unwrap

Process Result Command

Result Confirmation

ess

ess

Display Log and Result

Display Log and Result

wrap

**Gambar 3. Interaksi *E-Karip & SAM***

Berdasarkan aliran di atas, berikut merupakan *command* yang terjadi selama proses interaksi e-Karip dan SAM:

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**

1. **Log APDU *Command***

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)**

**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)**

**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 -----**