**SPESIFIKASI PERSONALISASI APPLET E-KARIP**

**V1.1**

Personalisasi kartu dilakukan untuk mengisi data-data pada kartu e-Karip seperti biodata dan foto masing-masing nasabah pemegang kartu e-Karip.

1. **Diagram Alir Personalisasi Kartu**

Connect the cards

XML Data

Display Biodata and Photo

Personalize Applet Card

Berdasarkan diagram alir di atas, personalisasi kartu dilakukan dengan tahapan sebagai berikut:

1. Data dan foto yang tersimpan dalam XML Data ditampilkan.
2. Kartu e-Karip dihubungkan dengan reader.
3. Personalisasi dapat dilakukan setelah kartu terhubung.
4. **Algoritma Autentikasi antara Kartu dan SAM.**

|  |  |
| --- | --- |
| **Applet** | **SAM/HSM** |
|  |  |

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. **Contoh Log APDU Personalisasi Kartu**

e-Karip <- 00A4040008A000000255020000

e-Karip -> 9000

e-Karip <- 00A4040008A000000255010000

e-Karip -> 6B00

SAM <- 00A4040008A000000255010000

SAM -> 6700

SAM <- 00A4040008A000000255010000

SAM -> 9000

\*\*Perso Started\*\*

Mutual Started

e-Karip <- 00A4040008A000000255020000

e-Karip -> 9000

SAM <- 00A4040008A000000255010000

SAM -> 9000

e-Karip <- 80B8000008

e-Karip -> 1079000247830C279000

e-Karip <- 0084000008

e-Karip -> 00000000000000009000

SAM <- 002A00001000000000000000001079000247830C27

SAM -> 0082000028230F7729C7557B9BBC9894F6D68A72D99B90C83F515319431A34D2AD946D4D20B21AD70A6693E8429000

e-Karip <- 0082000028230F7729C7557B9BBC9894F6D68A72D99B90C83F515319431A34D2AD946D4D20B21AD70A6693E842

e-Karip -> E348317FF71746E2894C2E67560FBC43918A9309EC1137B1885A2FC93B773F38E315CAF7CF03DE0C9000

SAM <- 002A000128E348317FF71746E2894C2E67560FBC43918A9309EC1137B1885A2FC93B773F38E315CAF7CF03DE0C

SAM -> 9000

Mutual Finished

Verify PIN Started

SAM <- 002A01000D0020000008FFFFFFFF31323334

SAM -> 0C2000002087110174248404D5B8E68143A11E0B0DF261A39701088E08670CBADDFC5010E59000

e-Karip <- 0C2000002087110174248404D5B8E68143A11E0B0DF261A39701088E08670CBADDFC5010E5

e-Karip -> 990290008E08945188FF1DC150C79000

SAM <- 002A02000E990290008E08945188FF1DC150C7

SAM -> 90009000

Verify PIN Finished

Insert Biodata

e-Karip <- 00A40000 02 0001 // select file

e-Karip -> 9000 //resp select file

SAM <- 002A0100 7D 04D60000 78 0076110B3132333431323334323334121263687269737469616E20736574796177616E130830393038323031321404717265771508333130383230313216073233333232333417013018083233343233343233190932333432333432333420073234323334323321023234220B3233343233343233343233 // compose update binary command

SAM -> 0CD600009187818101253101976F3CA5C10D6D2130AB4334F65F43B9B9682F8432806AFBB1800E1E42C939EF7366CC673372F19C7ECDB16167B0CD984CA6424BA1F9EA0C5B3BD190368EDE0FC1D8237BF833510A6D41FF94F149D4D65CA91C0B65CA56089190C877853CAEF91A41416E32076CA8060CBD88B5AE96346386D20BCDC9C3826541A53DD19701788E08C5BDFE4FD0352B3D9000 // response1

e-Karip <- 0CD600009187818101253101976F3CA5C10D6D2130AB4334F65F43B9B9682F8432806AFBB1800E1E42C939EF7366CC673372F19C7ECDB16167B0CD984CA6424BA1F9EA0C5B3BD190368EDE0FC1D8237BF833510A6D41FF94F149D4D65CA91C0B65CA56089190C877853CAEF91A41416E32076CA8060CBD88B5AE96346386D20BCDC9C3826541A53DD19701788E08C5BDFE4FD0352B3D // execute response1 without sw1sw2 9000

e-Karip -> 990290008E089D5F7F279388277A9000 // response2

SAM <- 002A0200 0E 990290008E089D5F7F279388277A // execute response2 without sw1sw2 9000

SAM -> 90009000 // successed respons

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