

## Specification SAM BRI

BRI SAM mempunyai kemampuan sebagai perso SAM dan SAM transaksi. Untuk memfungsikan SAM sebagai perso SAM atau SAM transaksi digunakan perintah set phase. Dengan perintah ini maka SAM diset sebagai SAM transaksi dan SAM ini hanya bisa melakukan transaksi saja, tidak bisa melakukan personalisasi kartu Desfire. Berikut perintah-perintah SAM untuk Perso dan Transaksi.

### I. Perintah-perintah SAM untuk Transaksi

#### 1. Authentication SAM

Authentication ini berguna untuk mengauthentication DESFIRE CARD melalui key yang berada didalam kartu.

CLA	80
INS	B0
P1	00
P2	00
LC	20

Data :

Untuk data-data yang dikirimkan menggunakan format seperti dibawah ini:

Diversify Data	16 byte	Data-data kartu
Application Reference	8 byte	Appication ID + Key Number
Random Desfire	8 byte	Nilai Random Yang Dihasilkan oleh DESFIRE CARD

##### a. Diversify Data

Card Number	8 byte	Nomor Kartu EMoney
UID	7 byte	UID Desfire Card
Padding	FF	

##### b. Application Reference

Application ID	3 byte	Application ID DESFIRE Card
Key Number	1 byte	Key Number Yang akan di authenticate
Padding	4 byte	80 00 00 00

**Result :**

**Hasil dari operasi Authentication SAM menghasilkan data keluaran 32 byte,yang terdiri dari :**

<b>Session Key</b>	<b>16 byte</b>	<b>16 byte session key hasil authentication</b>
<b>Random SAM</b>	<b>16 byte</b>	<b>Nilai Random untuk diversify DESFIRE Card</b>

## **2. Authentication HOST**

**Authentication ini berguna untuk Authentication via HOST.**

<b>CLA</b>	<b>80</b>
<b>INS</b>	<b>B2</b>
<b>P1</b>	<b>00</b>
<b>P2</b>	<b>00</b>
<b>LC</b>	<b>37</b>

**Data :**

**Untuk data-data yang dikirimkan menggunakan format seperti dibawah ini:**

<b>Data From HOST</b>	<b>24 byte</b>	<b>Data-data kartu</b>
<b>Parameter Diversify</b>	<b>15 byte</b>	<b>Parameter untuk Diversifikasi Data</b>
<b>Application Reference</b>	<b>8 byte</b>	<b>Appication ID + Key Number</b>
<b>Random Desfire</b>	<b>8 byte</b>	<b>Nilai Random Yang Dihasilkan oleh DESFIRE CARD</b>

### **a. Data From HOST**

<b>Data</b>	<b>24 byte</b>	<b>Data yang dikirimkan dari HOST.</b>
-------------	----------------	--

### **b. Parameter Diversify**

<b>Card Number</b>	<b>8 byte</b>	<b>Nomor Kartu Emoney</b>
<b>UID</b>	<b>7 byte</b>	<b>UID Desfire Card</b>

### **c. Application Reference**

<b>Application ID</b>	<b>3 byte</b>	<b>Application ID DESFIRE Card</b>
<b>Key Number</b>	<b>1 byte</b>	<b>Always 0x01</b>
<b>Padding</b>	<b>4 byte</b>	<b>80 00 00 00</b>

**Result :**

**Hasil dari operasi Authentication SAM menghasilkan data keluaran 32 byte,yang terdiri dari :**

<b>Session Key</b>	<b>16 byte</b>	<b>16 byte session key hasil authentication</b>
<b>Random SAM</b>	<b>16 byte</b>	<b>Nilai Random untuk diversify DESFIRE Card</b>

### **3. Create Hashing**

**Perintah ini digunakan untuk menghasilkan Hashing pada saat Debit transaction**

<b>CLA</b>	<b>80</b>
<b>INS</b>	<b>B4</b>
<b>P1</b>	<b>00</b>
<b>P2</b>	<b>00</b>
<b>LC</b>	<b>58</b>

**Data :**

**Untuk data-data yang dikirimkan menggunakann format seperti dibawah ini:**

<b>Diversify Data</b>	<b>16 byte</b>	<b>Data-data kartu</b>
<b>Application Reference</b>	<b>8 byte</b>	<b>Appication ID + Key Number</b>
<b>Random Desfire</b>	<b>8 byte</b>	<b>Nilai Random Yang Dihasilkan oleh DESFIRE CARD</b>
<b>Hashing data</b>	<b>56 byte</b>	<b>Parameter untuk Menghasilkan Hashing</b>

#### **c. Diversify Data**

<b>Card Number</b>	<b>8 byte</b>	<b>Nomor Kartu Emoney</b>
<b>UID</b>	<b>7 byte</b>	<b>UID Desfire Card</b>
<b>Padding</b>	<b>FF</b>	

#### **d. Application Reference**

<b>Application ID</b>	<b>3 byte</b>	<b>Application ID DESFIRE Card</b>
<b>Key Number</b>	<b>1 byte</b>	<b>Key Number Yang akan di authenticate</b>
<b>Padding</b>	<b>4 byte</b>	<b>80 00 00 00</b>

**Result :**

**Hasil dari operasi Create Hash menghasilkan 4 byte ,yang terdiri dari :**

<b>MAC Key</b>	<b>4 byte</b>	<b>Hashing Untuk Di Tulis di EDC Database</b>
----------------	---------------	---

**4. Generate Random**

**Generate bilangan Random untuk Di kirimkan ke Host Saat Top Up.**

<b>CLA</b>	<b>80</b>
<b>INS</b>	<b>B3</b>
<b>P1</b>	<b>00</b>
<b>P2</b>	<b>00</b>
<b>LC</b>	<b>13</b>

**Data :**

**Untuk data-data yang dikirimkan menggunakan format seperti dibawah ini:**

<b>Card Number</b>	<b>8 byte</b>	<b>Nomor Kartu Emoney</b>
<b>UID</b>	<b>7 byte</b>	<b>UID Desfire Card</b>
<b>Terminal ID</b>	<b>4 byte</b>	<b>Terminal ID Transaksi</b>

**Result :**

**Hasil dari operasi Generate Random menghasilkan data keluaran 24 byte,yang terdiri dari :**

<b>Random</b>	<b>24 byte</b>	<b>Nilai Random untuk Host saat melakukan Top Up</b>
---------------	----------------	--