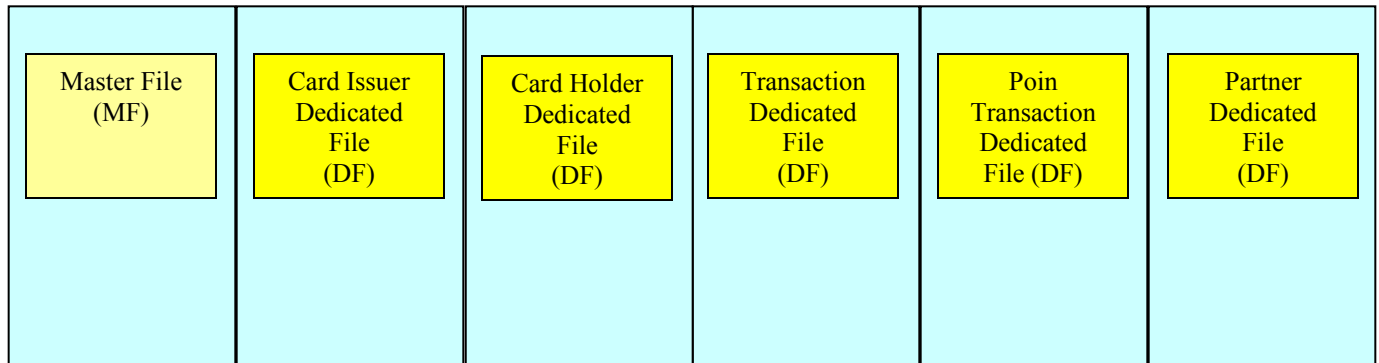


# Spesifikasi E-Money BRI Berbasis Mifare Desfire

*Prepared By NOP*

## I. Mapping Memory DesFire BRI

Untuk mengakomodasi E-Money secara umum, ada 5 kelompok informasi yang diperlukan, yaitu kelompok informasi berisi data-data Issuer (penerbit kartu), data pemegang kartu, data value (saldo), data data poin dan kelompok informasi berisi data-data rekanan.



## II. Security Features

### II.1 Data Transmisi

Data transmisi antara IC-card dan reader pada DesFire dapat dilakukan melalui 3 level keamanan :

- Plain Text : data dikirimkan dalam bentuk clear teks
- MACed : data dikirimkan bersamaan dengan data hasil perhitungan otentikasi (checksum data) yang ditambahkan di akhir data yang ditransmisikan (DES/3 DES MAC computation).
- Encrypted : data yang dikirimkan di enkripsi dengan session key sehingga setiap transaksi akan berbeda-beda.

Setting data transmisi dilakukan di level file dan di setting pada saat create file.

Penggunaan MAC dan enkripsi akan berdampak pada waktu transaksi, oleh karena itu penggunaa MAC disarankan hanya pada file yang dilakukan penulisan didalamnya.

## II.2. File Akses

Akses file data dilakukan pada level aplikasi menggunakan mekanisme otentikasi melibatkan secret key. Untuk setiap aplikasi, dapat menggunakan sampai 14 key untuk mengontrol data pada kartu.

## II.3. Akses Kondisi

Ada 4 akses kondisi yang dapat diterapkan pada setiap file untuk setiap aplikasi :

- Read Access ( Get Values, Debit for Values Files )
- Write Access ( Get Values, Debit , Limited Credit for Values Files )
- Read & write access ( Get Values , Limited Credit , Debit , Credit for Values Files )
- Change Access Rights

Catatan. Untuk yang didalam kurung menunjuk pada value files.

Akses kondisi direpresentasikan dalam 4 bit.

### III. Mapping File untuk spesifikasi BRI

Bagian ini menggambarkan struktur file dan isi dari direktori yang telah di mapping pada bagian pertama.

Application ID	Directory / File Name	Type	Content	Besar File	Dijelaskan Pada
0x000000	MF ( Master File )	DF			III.1
	PICC Master Key	Key	Keys (M)		
0x000001 ( Hexadecimal )	CardIssuerDF	DF			III.2
	CI Keys	Key	Keys ( 2 Keys )		
	CI Header (FileID 0)	Standard		32 Bytes	
	CI Status (File ID 1)	Standard		32 Bytes	
0x000002 ( Hexadecimal )	CardHolderDF	DF			III.3
	CH Keys	Key	Keys ( 2 Keys )		
	CH Data (File ID 0)	Standard		128 bytes	
0x000003 ( Hexadecimal )	TransactionDF	DF			III.4
	Transaction Keys	Key	Keys ( 2 Keys )		
	Value_Purse (File ID 0)	Value		64 bytes	
	Log_Data (File ID 1)	Record (Cyclic ) 12 Records		768 bytes (32 x 12 x 2)	
	Rec_Flag (File ID 2)	Standard		32 bytes	
	LastTransDate&AkumDebit (File ID 3)	Standard		32 bytes	
0x000004 (Hexadecimal)	PoinTransactionDF				III.5
	Poin Keys	Key	Keys ( 2 Keys )		
	Value Poin (File ID 0)	Standard		32 bytes	
	Log_Poin (File ID 1)	Record (Cyclic ) 5 Records		320 bytes (32 x 5 x 2)	
	Rec Flag (File ID 2)	Standard		32 bytes	
0x000005 ( Hexadecimal )	PartnerDF	DF			III.6
	Partner Keys	Key	Keys (14 Keys )		
	Parkir File (FileID 0)	Standard		128 bytes	
	Angkasa Pura File (FileID 1)	Standard		128 bytes	
	Partner Data3 (FileID 2)	Standard		128 bytes	
	Partner Data4 (FileID 3)	Standard		128 bytes	
	Partner Data5 (FileID 4)	Standard		128 bytes	
	Partner Data6 (FileID 5)	Standard		128 bytes	
	Partner Data7 (FileID 6)	Standard		128 bytes	
	Partner Data8 (FileID 7)	Standard		128 bytes	
	Partner Data9 (FileID 8)	Standard		128 bytes	
	Partner Data10 (FileID9)	Standard		128 bytes	
	Partner Data11 (FileID10)	Standard		128 bytes	
	Partner Data12 (FileID 11)	Standard		128 bytes	
	Partner Data13 (FileID 12)	Standard		128 bytes	

Application ID	Directory / File Name	Type	Content	Besar File	Dijelaskan Pada
0x000006 ( Hexadecimal )	PartnerDF	DF			
	Partner Keys	Key	Keys (14 Keys )		
	Partner Data14 (FileID 0)	Standard		128 bytes	
	Partner Data15 (FileID 1)	Standard		128 bytes	
	Partner Data16 (FileID 2)	Standard		128 bytes	
	Partner Data17 (FileID 3)	Standard		128 bytes	
	Partner Data18 (FileID 4)	Standard		128 bytes	
	Partner Data29 (FileID 5)	Standard		128 bytes	
	Partner Data20 (FileID 6)	Standard		128 bytes	
	Partner Data21 (FileID 7)	Standard		128 bytes	
	Partner Data22 (FileID 8)	Standard		128 bytes	
	Partner Data23 (FileID 9)	Standard		128 bytes	
	Partner Data24 (FileID 10)	Standard		128 bytes	
	Partner Data25 (FileID 11)	Standard		128 bytes	
	Partner Data26 (FileID 12)	Standard		128 bytes	
0x000007 ( Hexadecimal )	PartnerDF	DF			
	Partner Keys	Key	Keys (14 Keys )		
	KRL Files (FileID 0)	Standard		128 bytes	
	KRL Files (FileID 1)	Standard		128 bytes	
	KRL Files (FileID 2)	Standard		128 bytes	
	KRL Files (FileID 3)	Standard		128 bytes	
	Partner Data31 (FileID 4)	Standard		128 bytes	
	Partner Data32 (FileID 5)	Standard		128 bytes	
	Partner Data33 (FileID 6)	Standard		128 bytes	
	Partner Data34 (FileID 7)	Standard		128 bytes	

### III.1. Master File

Aplikasi default dalam kartu dan berada dalam level PICC.

Karakteristik untuk aplikasi ini :

- AID : 0x000000
- KeySetting : 0x0B ( Configuration changeable , no free create/delete file, free directory list, master key changeable )
- Banyak Key : 1 ( Master Key M #0)

### III.2. CardIssuer Directory

Aplikasi ini berisi data-data dari BRI sebagai penerbit kartu.

Karakteristik untuk aplikasi ini :

- AID : 0x000001
- KeySetting : 0x12 ( Configuration not changeable, no free create/delete file, free dirsctory list, master key not changeable, other key changeable using key #1 )
- Banyak 3DES key : 2 (Read (R, #0), Card Issuer Key (Read/Write) (I,#1) )

#### III.2.1 CI\_Header File

File ini berisi data fix tentang card issuer, panjang data file ini 23 bytes, dengan File ID 0.

Access Rights and Security Level :

- Read : always ; read is free and no key required
- Write : never
- Read&Write : key #1
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text ( communication setting 0x00 )

#### CI\_Header Structure Description

Data Element	Data Type	Size	Description
BRI	BCD	3 Bytes	Value = BRI
Card Number	Hexadecimal	8 Bytes	Nomor Kartu
Issue Date	Hexadecimal	3 Bytes	Tanggal Kartu Di Cetak
Expiry Date	Hexadecimal	3 Bytes	Tanggal Expire Kartu
Cabang Issue	Hexadecimal	2 Bytes	Cabang Issue (optional)
Tipe Kartu Bisnis	BCD	2 Bytes	Tipe Kartu Bisnis (optional)
Model Kartu	BCD	2 Bytes	Model Kartu (optional)

#### III.2.2 CI\_Status File

File ini berisi status dari kartu berupa status kartu aktif atau tidak dan activation date. Panjang data file ini 32 bytes, dengan File ID 1.

Access Rights and Security Level :

- Read : always ; read is free and no key required
- Write : Key #0
- Read&Write : read and write dilakukan pada saat aktivasi kartu dengan mengupdate data activation date dan status kartu.(key #1)
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text ( communication setting 0x00 )

#### CI\_Status Structure Description

Data Element	Data Type	Size	Description
Activation Date	Hexadecimal	3 Bytes	Tanggal saat kartu di aktivasi
Status	BCD	2 Bytes	Status kartu active atau close
Interoperability	Hexadecimal	27 Bytes	Interoperability Merchant

### III.3. CardHolder Directory

Directory ini berisi data pemegang kartu

Karakteristik untuk aplikasi ini :

- AID : 0x000002
- KeySetting : 0x12 ( Configuration not changeable, no free create/delete file, free dirsctory list, master key not changeable, other key changeable using key #1 )
- Banyak 3DES key : 2 (Read (R, #0), Card Issuer Key (Read/Write) (I,#1) )

#### III.3.1 CH\_Data

File ini berisi data-data pemilik kartu, panjang data file ini 96 bytes, dengan File ID 0.

Access Rights and Security Level :

- Read : Key #0
- Write : Never
- Read&Write : read and write dilakukan pada saat mengupdate data pemegang kartu (key #1).
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text ( communication setting 0x00 )

#### CH\_Data Structure Description

Data Element	Data Type	Size	Description
ID Num	Hexadecimal	8 Bytes	No ID (KTP or Other) (optional)
Name	BCD	20 Bytes	Nama Pemilik Kartu (optional )
Address	BCD	30 Bytes	Alamat Pemilik Kartu (optional )
DOB	Hexadecimal	3 Bytes	Tanggal Lahir (optional )
POB	BCD	16 Bytes	Tempat Lahir (optional )
Phone	Hexadecimal	6 Bytes	Telephone Pemilik Kartu (optional )
Gender	BCD	1 Bytes	Gender Pemilik Kartu (optional )
NamaGadisIbu	BCD	16 Bytes	Nama Gadis Ibu ( optional )

### III.4 Transaction Directory

Directory ini berisi file untuk nilai saldo dari kartu, log transaction , dan data yang berhubungan dengan purse operation.

Karakteristik untuk aplikasi ini :

- AID : 0x000003
- KeySetting : 0x12 ( Configuration not changeable, no free create/delete file, free dirsctory list, master key not changeable, other key changeable using key #1 )
- Banyak 3DES key : 2 (Read (R, #0), Card Issuer Key (Read/Write) (I,#1)

#### III.4.1 Value Purse File

File ini berisi nilai saldo. Panjang dari file ini 64 Bytes, dengan File ID 0

Access Rights and Security Level :

- Read : Key #0 ( Debit dan Get Value )
- Write : Never
- Read&Write : Dilakukan Issuer Key pada Saat Top Up ( GetValue, Debit,Limited Credit dan Credit) key #1
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text

#### III.4.2 Log Data File

File ini berisi pencatatan jenis transaksi yang dilakukan, aktifitas transaksi, tempat, besar transaksi dan sisa saldo. File ini berupa record file dengan cara penulisan cyclic.Panjang yang diperlukan 768 bytes dengan asumsi log yang dicatat sebanyak 12 record.Dengan File ID 1.

Access Rights and Security Level :

- Read : Key #0
- Write : Key #0
- Read&Write : Key #1
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text ( communication setting 0x00 )

#### Log\_Data

Data Element	Data Type	Size	Description
Merchant ID	Hexadecimal	8 Bytes	Id Merchant
Terminal ID	Hexadecimal	4 bytes	Terminal ID
Transaction DateTime	Hexadecimal	6 Bytes	Tanggal Transaksi
Transaction Type	Hexadecimal	1 Bytes	Jenis Transaksi
Value Transaction	Hexadecimal	3 Bytes	Besar Transaksi
Saldo Awal	Hexadecimal	3 Bytes	Saldo Sebelum Transaksi
Saldo Akhir	Hexadecimal	3 Bytes	Sisa Saldo

#### III.4.3 Flag Rec

File ini berisi flag letak record transaksi terakhir yang ditulis.Panjang data yang diperlukan 1 byte. Data ini menunjukkan letak posisi terakhir record log yang ditulis.Dengan File ID 2

Access Rights and Security Level :

- Read : Key #0
- Write : Key #0
- Read&Write : Key #1
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text ( communication setting 0x00 )

Data Element	Data Type	Size	Description
Flag Rec Data	Hexadecimal	1 Bytes	Letak Log terakhir

#### III.4.4 LastTransDate&AkumDebit File

File ini berisi data tanggal transaksi terakhir dan Akumulasi Debit. Panjang data dari file ini 6 Bytes, dengan File ID 3

Access Rights and Security Level :

- Read : Key #0
- Write : Key #0
- Read&Write : key #1
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text

#### CI\_Status Structure Description

Data Element	Data Type	Size	Description
Last Transaction Date	Hexadecimal	3 Bytes	Tanggal terakhir transaksi
Akumulasi Debit	Hexadecimal	4 Bytes	Akumulasi debit selama 1 bulan

#### III.5 Poin Directory

Directory ini berisi file untuk nilai poin dari kartu, log poin .

Karakteristik untuk aplikasi ini :

- AID : 0x000003
- KeySetting : 0x12 ( Configuration not changeable, no free create/delete file, free dirsctory list, master key not changeable, other key changeable using key #1 )
- Banyak 3DES key : 2 (Read (R, #0), Card Issuer Key (Read/Write) (I,#1))

#### III.4.1 Value Poin File

File ini berisi nilai poin. Panjang dari file ini 32 Bytes, dengan File ID 0

Access Rights and Security Level :

- Read : Key #0
- Write : Key #0
- Read&Write : Key #1
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text ( communication setting 0x00 )

#### III.4.2 Log Poin File

File ini berisi pencatatan jenis transaksi poin yang dilakukan, aktifitas transaksi poin, tempat, besar transaksi poin dan sisa poin. File ini berupa record file dengan cara penulisan cyclic. Panjang yang diperlukan 768 bytes dengan asumsi log yang dicatat sebanyak 5 record. Dengan File ID 1.

Access Rights and Security Level :

- Read : Key #0
- Write : Key #0
- Read&Write : Key #1
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text ( communication setting 0x00 )



## Log\_Poin

Data Element	Data Type	Size	Description
Partner_ID	Hexadecimal	15 Bytes	Id Partner
Trans_poin_DateTime	Hexadecimal	6 Bytes	Tanggal Transaksi poin
Trans_poin_Type	Hexadecimal	1 Bytes	Jenis Transaksi poin
Value Poin	Hexadecimal	3 Bytes	Besar Transaksi poin
Poin Awal	Hexadecimal	3 Bytes	Poin Sebelum Transaksi
Poin_Akhir	Hexadecimal	3 Bytes	Sisa Poin

### III.6 Partner Directory

Directory ini berisi space file untuk Di isi oleh partner yang bekerja sama dengan BRI. Directory untuk partner ini terdiri dari 4 directory yaitu 0x000005 , 0x000006, 0x000007

Karakteristik untuk aplikasi ini :

- AID : 0x000005, 0x000006
- KeySetting : 0x12 ( Configuration not changeable, no free create/delete file, free directory list, master key not changeable, other key changeable using key #1 )
- Banyak 3DES key : 14. Directory ini masing-masing terdiri dari 13 file, masing masing file memiliki key masing-masing dengan 1 tambahan key untuk Issuer.

Untuk tiap file diberi key untuk Read dan Write, dengan satu key yang dapat Read/Write ke semua file yaitu key untuk card issuer (key #1).

#### III.6.1 Partner Data File

File ini berisi data-data yang diperlukan oleh partner. Data element yang mengisi file ini belum ditentukan, hanya disediakan space sebesar 128 byte. Tiap partner boleh menggunakan lebih dari 1 partner file, sesuai dengan kesepakatan.

Access Rights and Security Level :

- Read : Key #0,2,3,4,5,6,7,8,9,10,11,12,13
- Write : Key #0,2,3,4,5,6,7,8,9,10,11,12,13
- Read&Write : Key #1
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text ( communication setting 0x00 )

Khusus untuk Directory KRL 0x000007, menggunakan Key Setting 0xE2 yang berarti untuk mengubah key digunakan key yang sama.

Khusus untuk Partner Data Directory 0x000007, hanya ada 8 File, dengan access file dan security level sebagai berikut :

- Read : Key #0,2,3,4,5,6,7,8
- Write : Key #0,2,3,4,5,6,7,8
- Read&Write : Key #1
- Change Config : hanya Card Issuer Key (key #1) yang dapat mengubah configuration
- Security Level : plain text ( communication setting 0x00 )

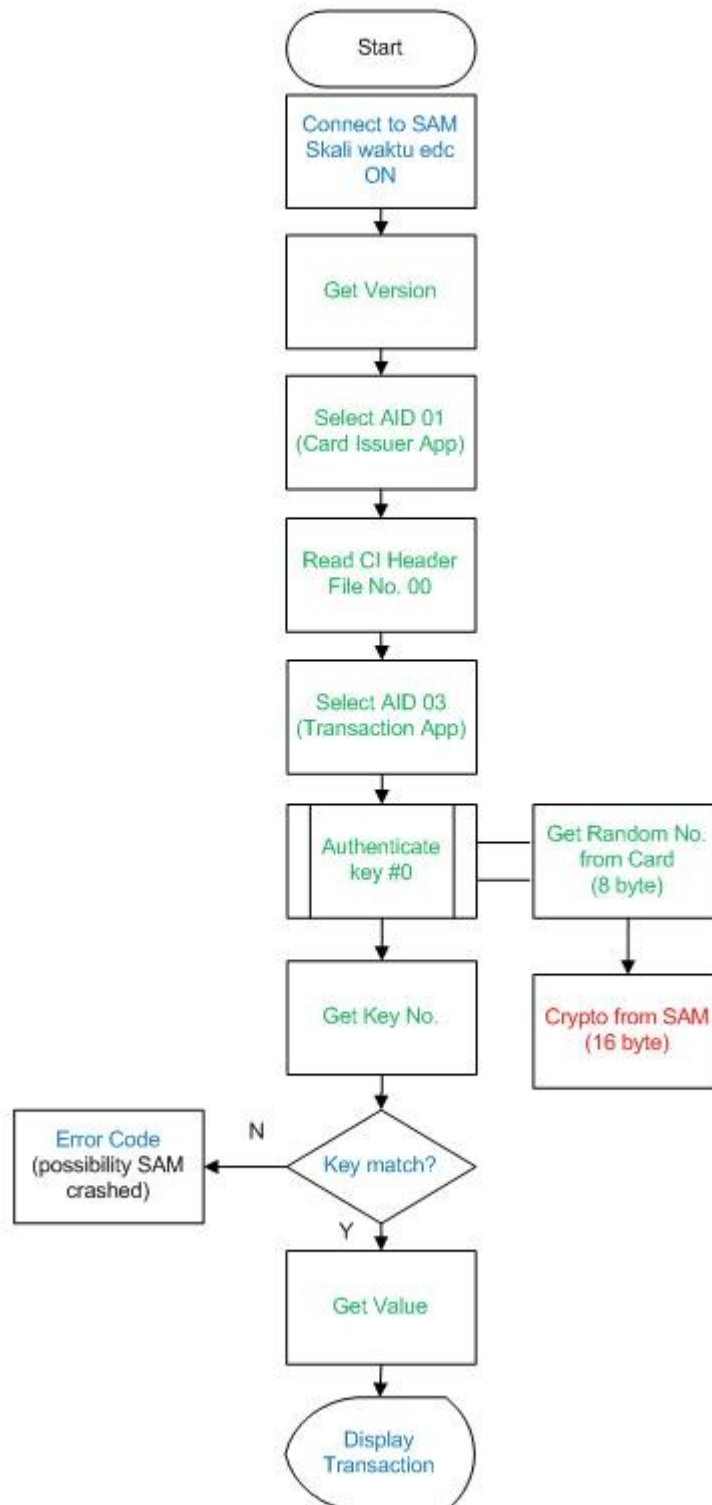
## IV. Flow Transaksi

Bagian ini menjelaskan transaksi-transaksi yang dilakukan dan alur dari transaksi.

### IV.1. Informasi Saldo

Transaksi ini untuk mengetahui jumlah saldo yang ada di dalam kartu.

Check Balance



## IV.2 Transaksi Offline

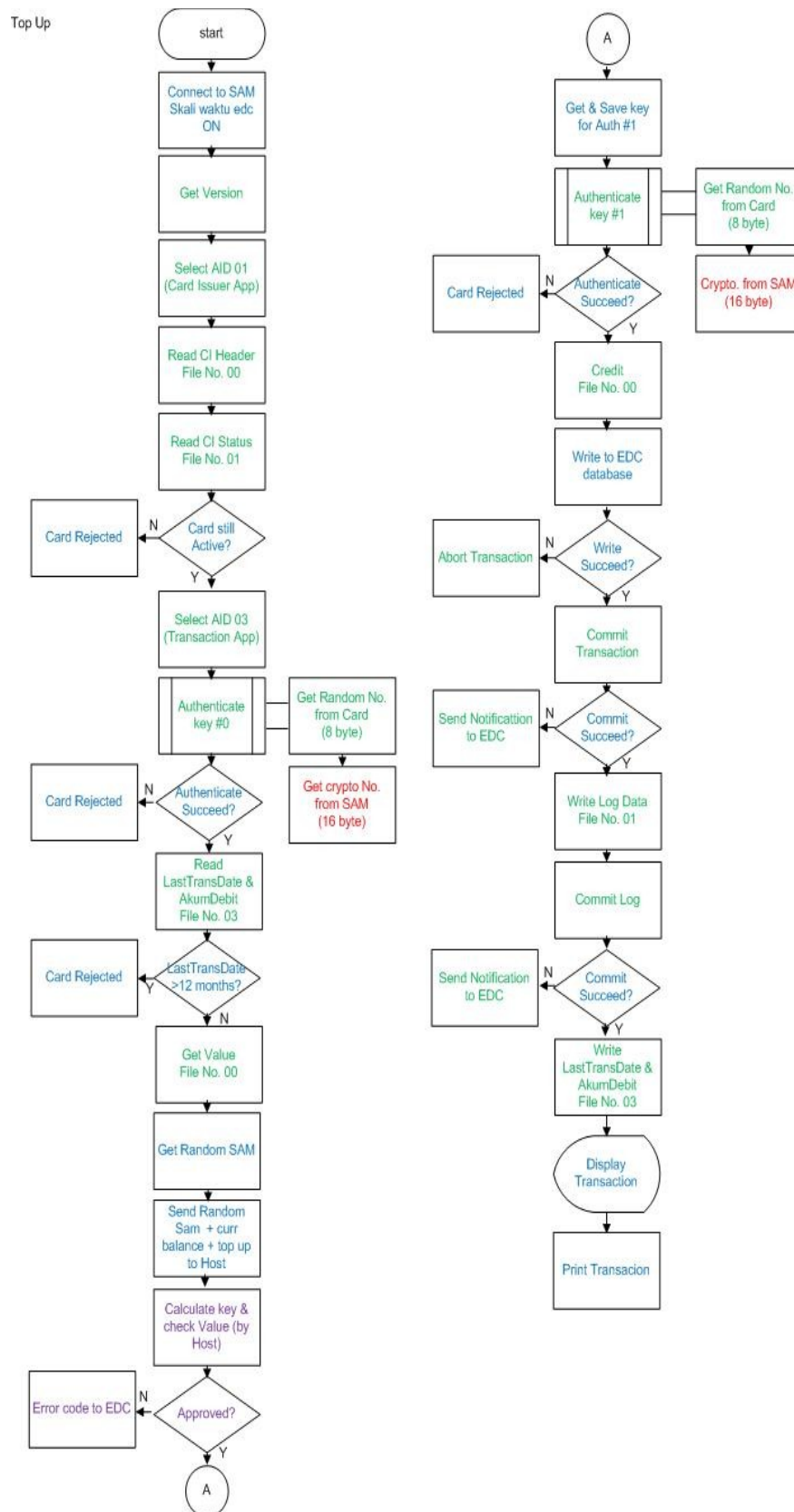
Transaksi ini digunakan untuk melakukan pembayaran secara Offline.

Offline Payment



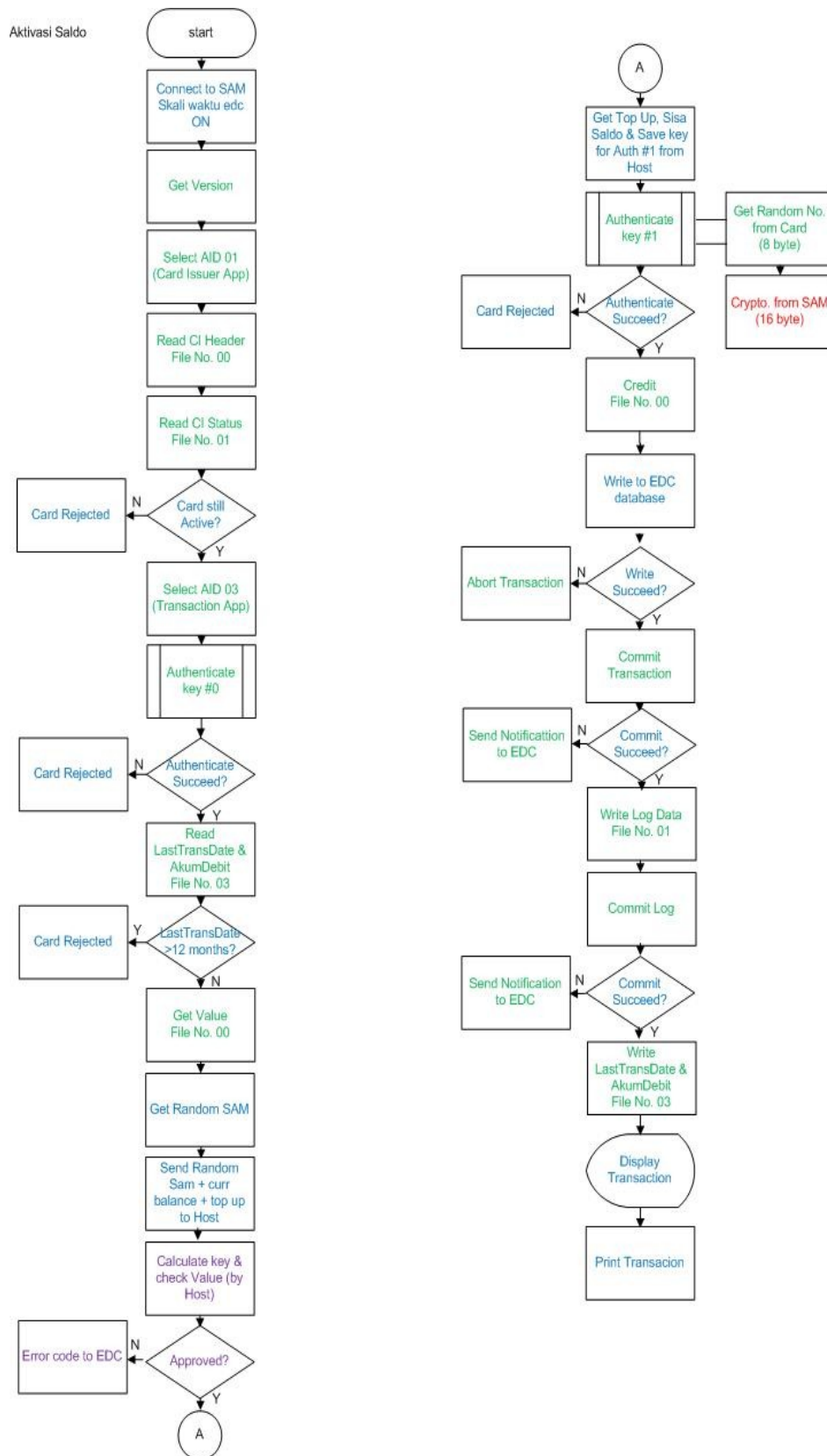
### IV.3 Top Up Saldo

Top Up Transaksi adalah transaksi untuk menambah saldo pada kartu prabayar. Untuk melakukan Top Up digunakan Key dari Host.



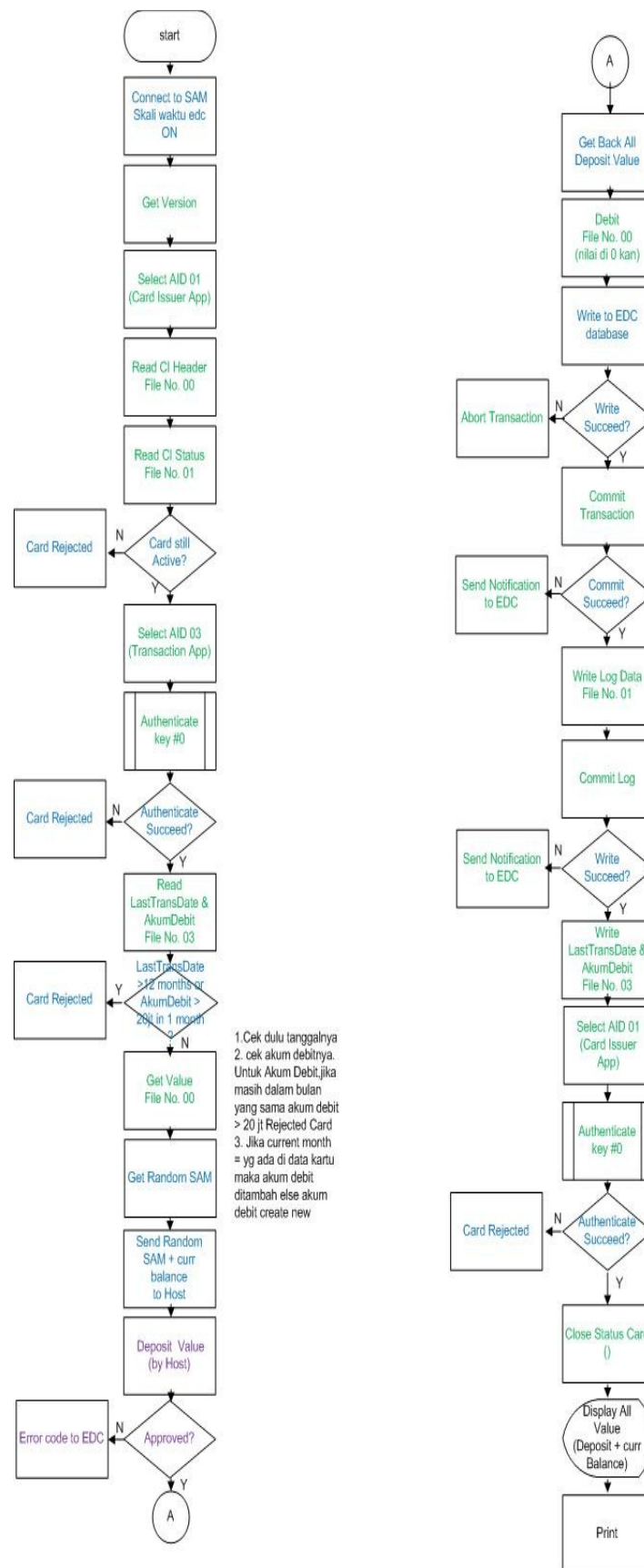
#### IV.4 Aktivasi Saldo

Aktivasi saldo adalah transaksi dimana kita telah melakukan topup saldo melalui media lain seperti ATM, dan internet banking. Pada jenis transaksi ini saldo telah di topup pada host tetapi topup belum dilakukan pada kartu.



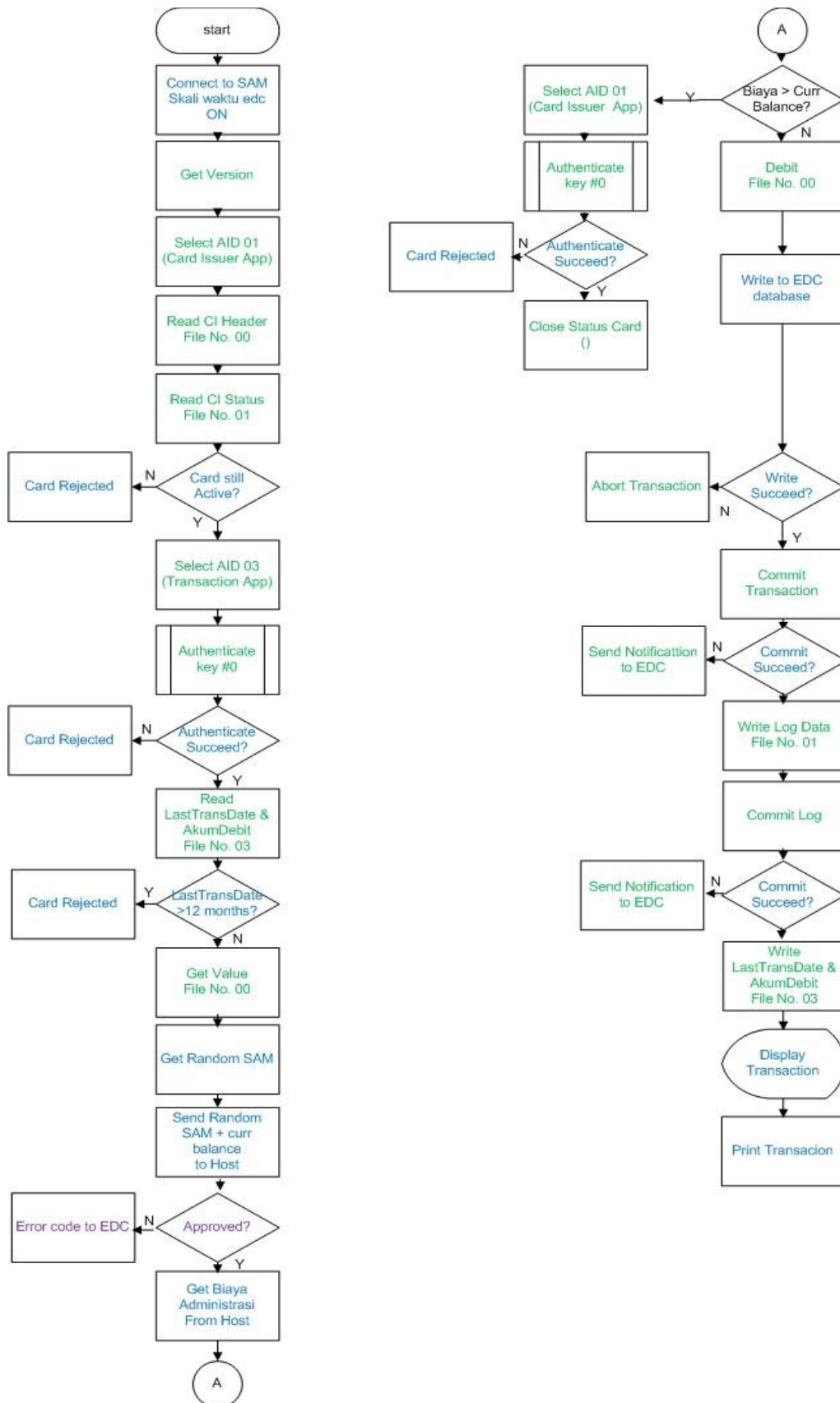
#### IV.4 Reedem

Reedem adalah transaksi untuk menutup kartu emoney kemudian mengambil saldo kartu dalam kartu yang tersisa



#### IV.5 Synchronize saldo

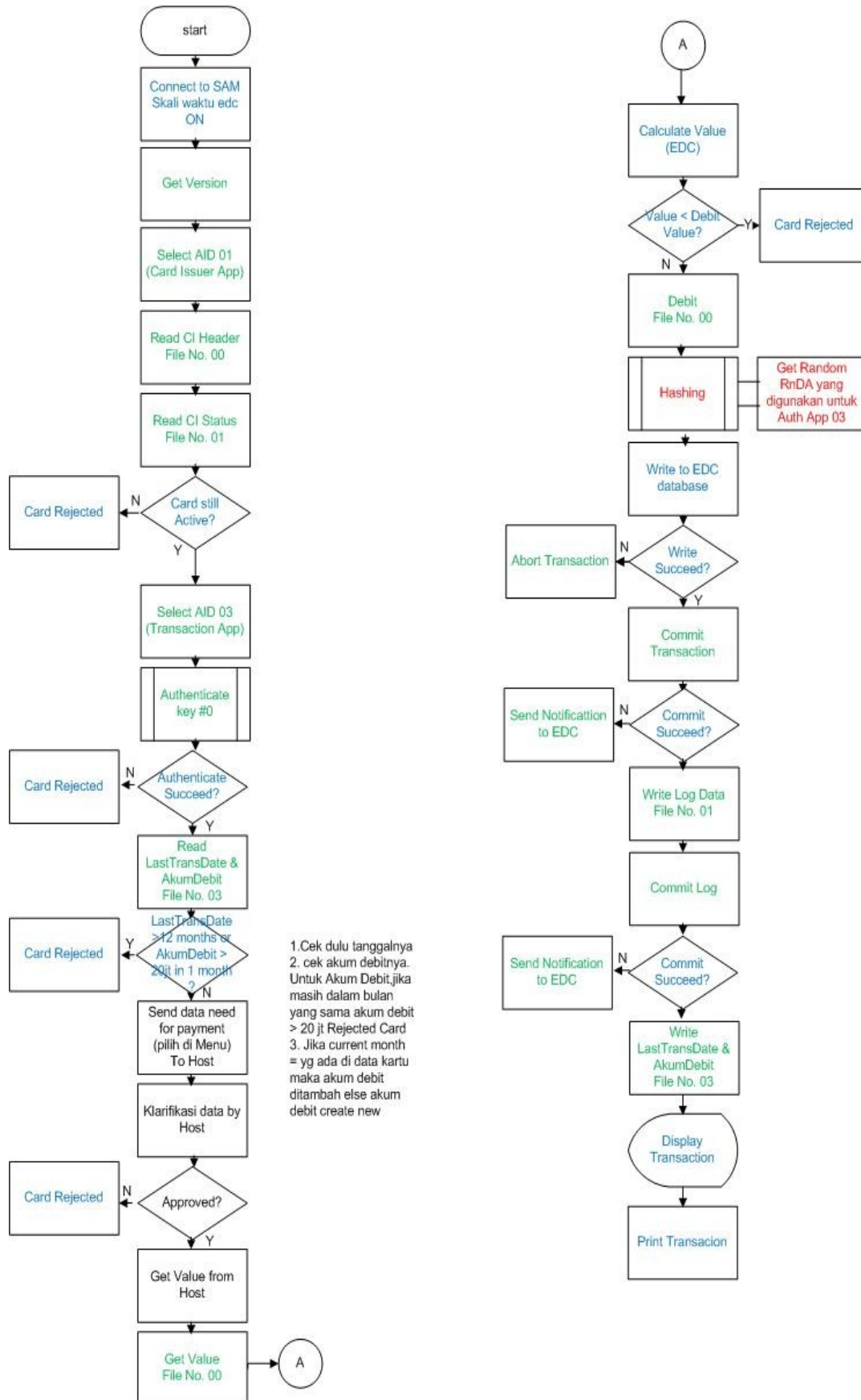
Transaksi ini adalah untuk menyamakan saldo di host dengan di kartu jika transaksi tidak dilakukan lebih dari 12 bulan kemudian user melakukan transaksi setelah 12 bulan.





## IV.6 Online Payment

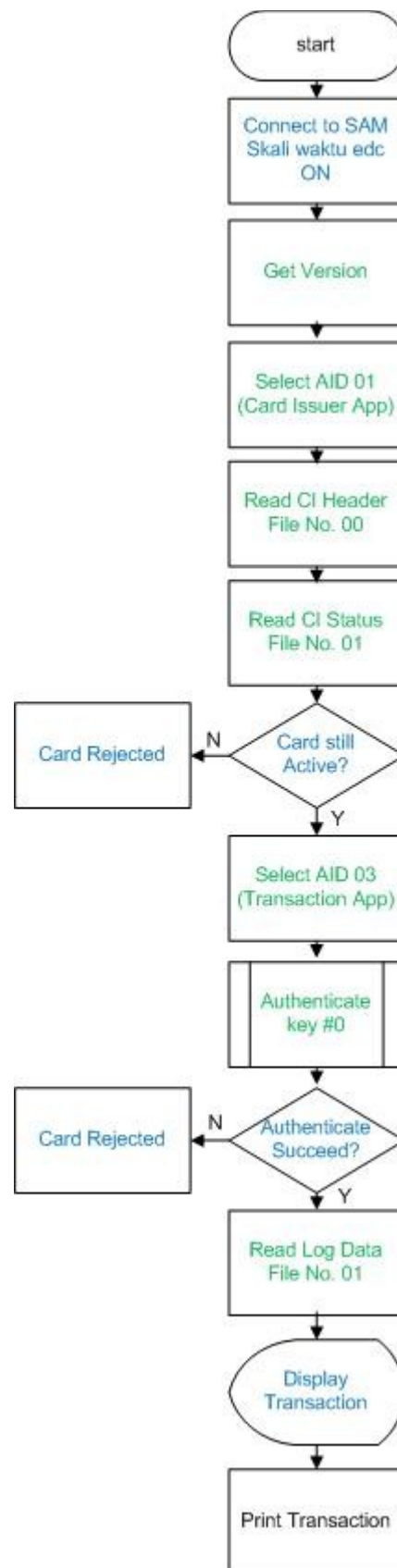
Transaksi ini adalah digunakan untuk pembayaran secara online, seperti pembayaran PLN, Telepon, dll





#### IV.7 Print Transaction

Transaksi ini adalah untuk melihat transaksi yang telah kita lakukan sampai 12 transaksi terakhir



#### IV.8 Info Card

Transaksi ini untuk menampilkan info kartu

