PERANCANGAN SISTEM *MICROPAYMENT* MENGGUNAKAN TEKNOLOGI *NEAR FIELD COMMUNICATION*

Arina Listyarini Dwiastuti
(13512006)

LATAR BELAKANG

Perkembangan transaksi semakin canggih dan mudah

Transaksi dengan jumlah kecil namun sering dilakukan disebut *micropayment*

Micropayment sudah dijumpai di Indonesia

- Contoh: E-Toll Mandiri, Flazz BCA, Kartu Commet
- Memanfaatkan teknologi NFC

NFC: teknologi koneksi jarak pendek tanpa kabel

NFC + *micropayment* = **aman**

RUMUSAN, TUJUAN, BATASAN

Rumusan masalah

Bagaimana rancangan sistem *micropayment* yang aman menggunakan teknologi NFC

Tujuan

Rancangan sistem *micropayment* yang aman menggunakan teknologi NFC

Batasan masalah

- Perancangan sistem *micropayment* menggunakan teknologi NFC
- Menerapkan metode pengamanan yang sesuai pada transaksi *micropayment* yang dirancang

ANALISIS SISMIC

ANALISIS KEBUTUHAN SISMIC

SISMIC dapat melakukan transaksi *top-up* saldo kartu.

- SISMIC dapat menambah saldo kartu.
- SISMIC dapat memberikan biaya pembayaran *top-up* saldo kartu ke penerbit kartu.
- SISMIC dapat menyimpan riwayat transaksi *top-up* saldo kartu ke dalam kartu.
- SISMIC dapat menyimpan riwayat transaksi *top-up* saldo kartu ke dalam basisdata.

SISMIC dapat melakukan transaksi pembelian menggunakan kartu.

- SISMIC dapat mengurangi saldo kartu.
- SISMIC dapat memberikan biaya transaksi pembelian pemilik kartu ke *merchant*.
- SISMIC dapat menyimpan riwayat transaksi pembelian ke dalam kartu.
- SISMIC dapat menyimpan riwayat transaksi pembelian saldo kartu ke dalam basisdata.

SISMIC dapat menunjukkan saldo kartu pada pemilik kartu.

SISMIC dapat menunjukkan riwayat transaksi kartu pada pemilik kartu.

Kartu SISMIC memiliki masa berlaku (tanggal kadaluarsa).

HARDWARE SISMIC

Kartu SISMIC (tag *NFC*)

Smartphone (NFC & Android)

Mesin EDC, yang dimiliki oleh *merchant*.

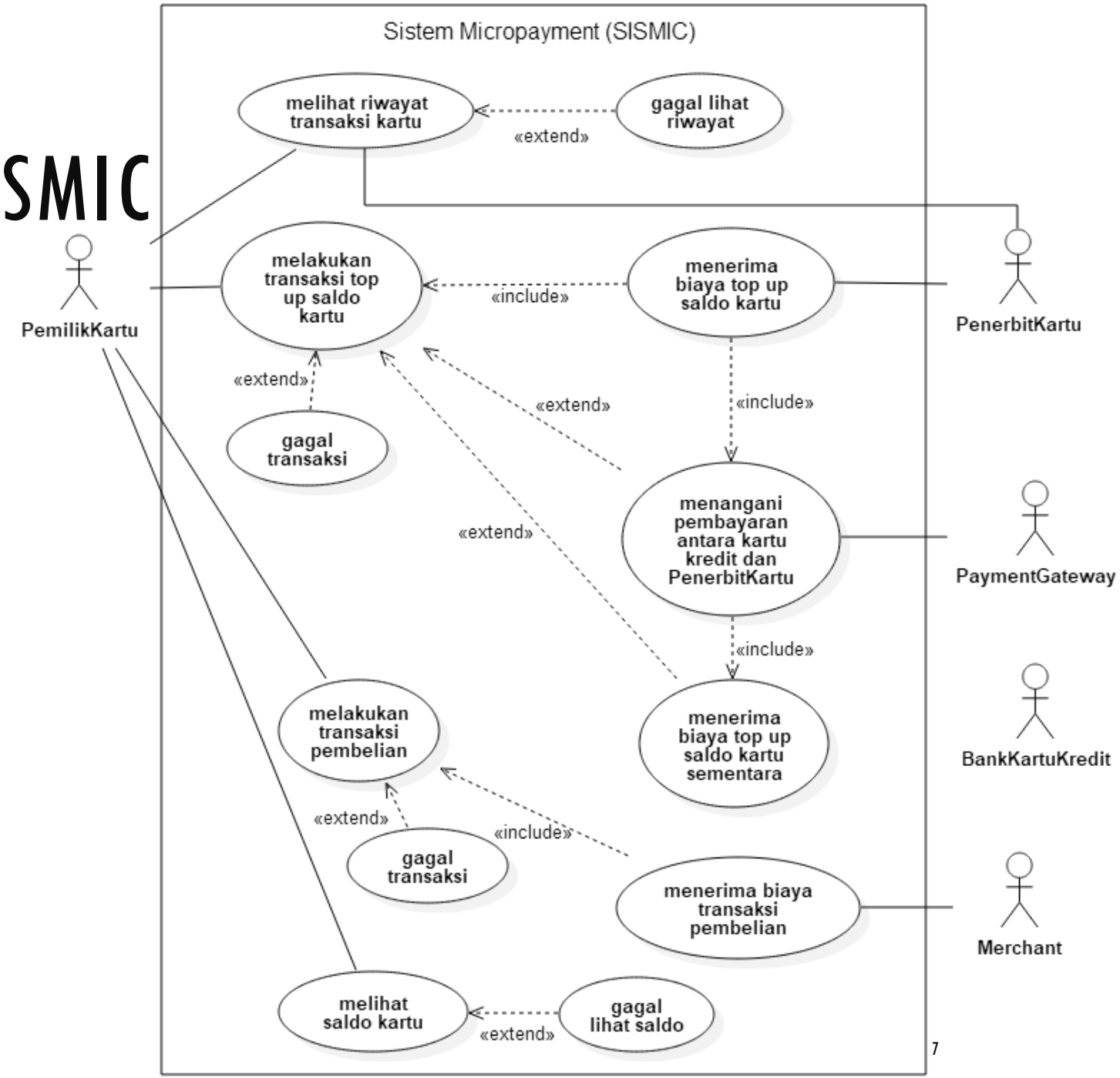
- disimulasi dengan NFC *reader* & laptop

Mesin ATM, yang dimiliki oleh penerbit kartu.

- disimulasi dengan NFC *reader* & laptop

GAMBARAN UMUM SISMIC

Diagram *usecase*



ANALISIS KEBUTUHAN KEAMANAN SISMIC

Confidentiality

- Data yang ada pada SISMIC bersifat rahasia & tidak dapat diakses oleh orang yang tidak berhak.

Integrity

- Data SISMIC tidak boleh berubah tanpa izin dari pihak yang berhak.

Availability

- Ketika berbagai pihak menggunakan SISMIC, layanan dan data SISMIC harus dapat digunakan.

Authentication

- Transaksi SISMIC hanya dapat dilakukan pada *hardware* dan *software* yang resmi

Authorization

- Semua pihak melakukan transaksi secara legal sesuai tugas dan perannya masing-masing pada SISMIC.

Accountability

- Segala aktivitas yang terjadi di SISMIC ada catatannya.

Non-repudiation

- Tidak ada pihak yang dapat menyanggah suatu transaksi yang telah terjadi.

PERANCANGAN SISMIC

OPERASI APLIKASI SISMIC

Transaksi *top-up* kartu SISMIC

- Via *smartphone,* ATM, dan *merchant*

Transaksi pembelian

- Via *smartphone* dan *merchant*

Lihat Saldo

- Via *smartphone,* ATM, dan *merchant*

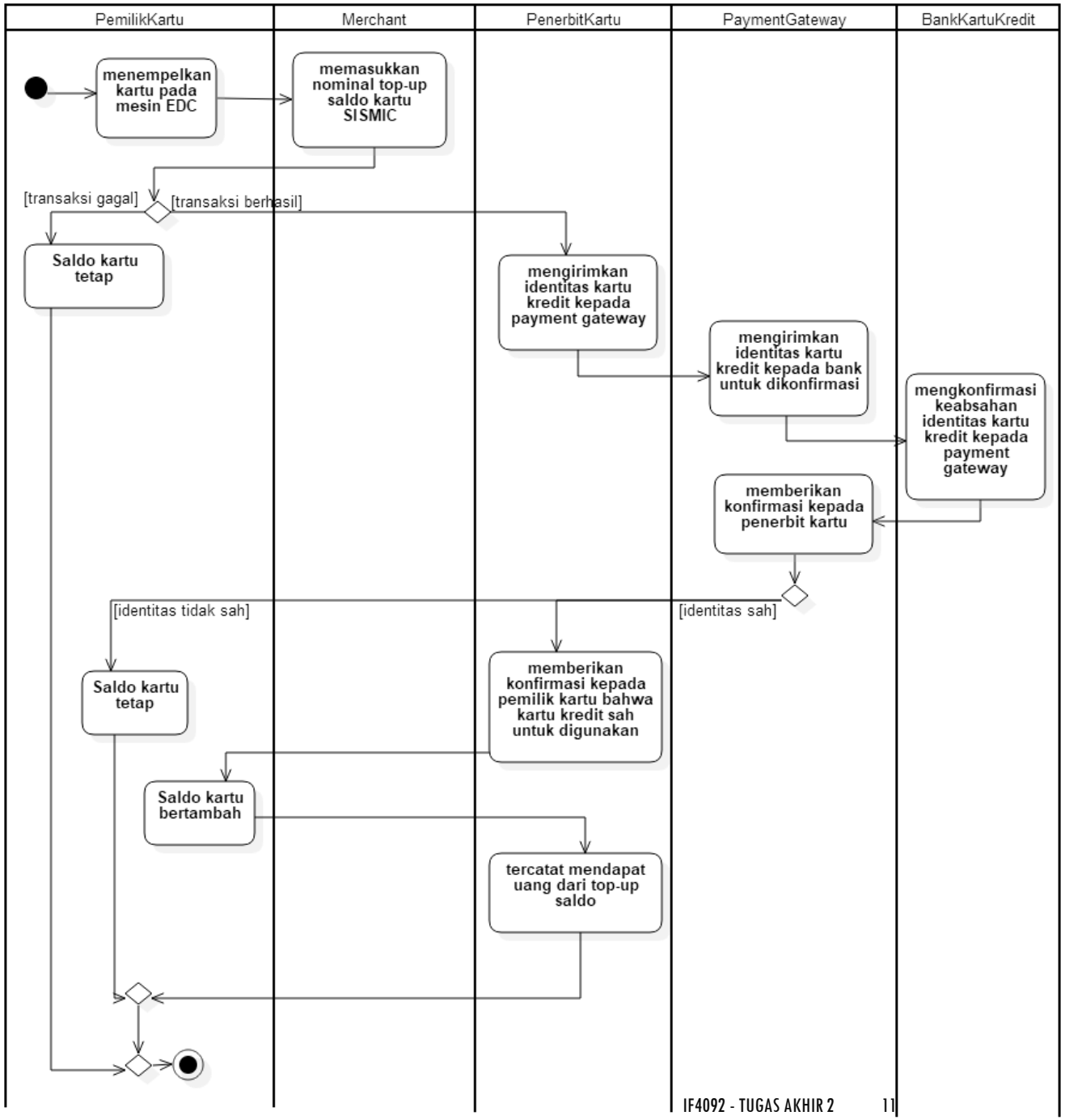
Lihat Riwayat Transaksi

Lihat Masa Berlaku Kartu SISMIC

- Via *smartphone,* ATM, dan *merchant*

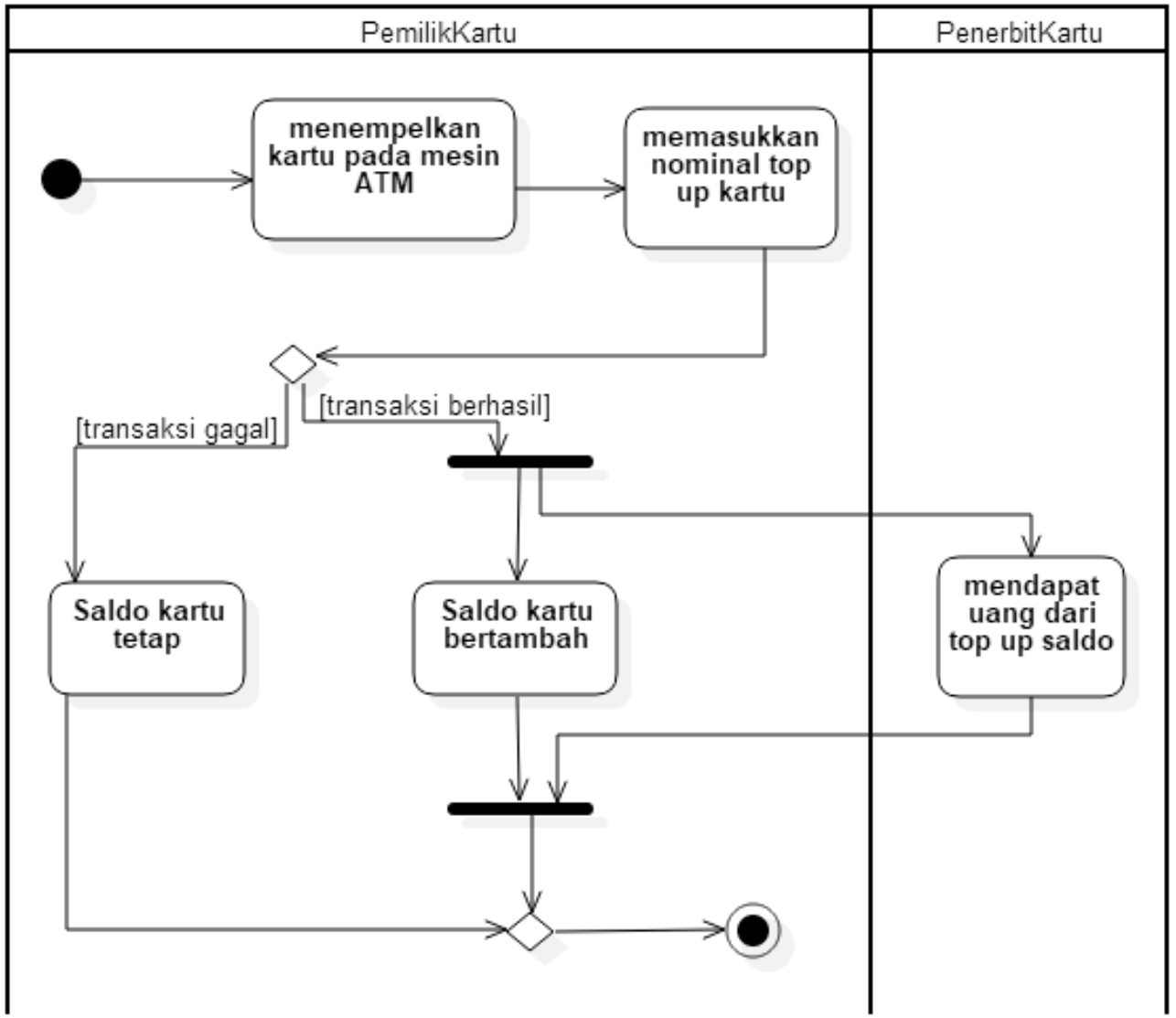
TRANSAKSI *TOP-UP*

Via Smartphone



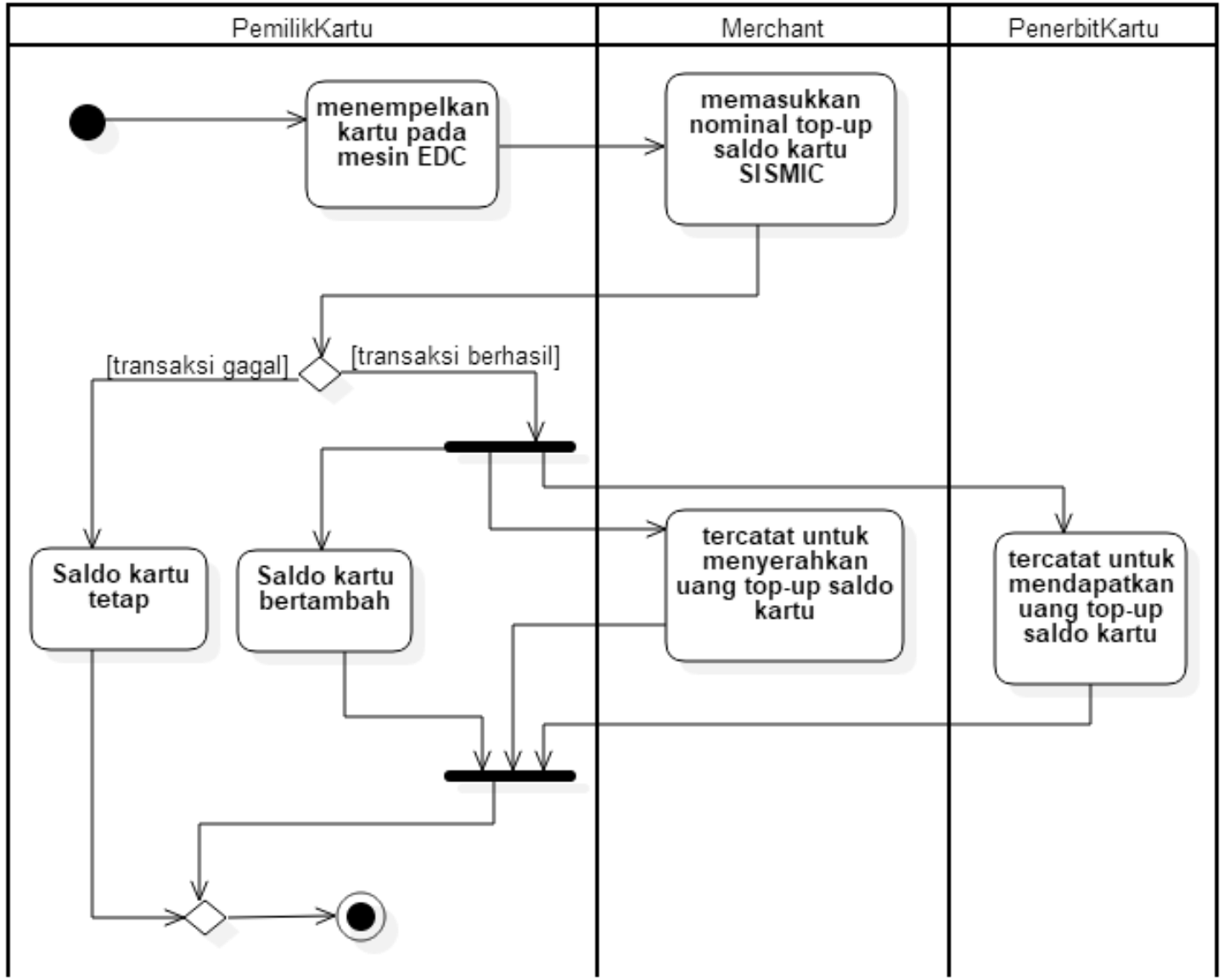
TRANSAKSI *TOP-UP*

Via ATM



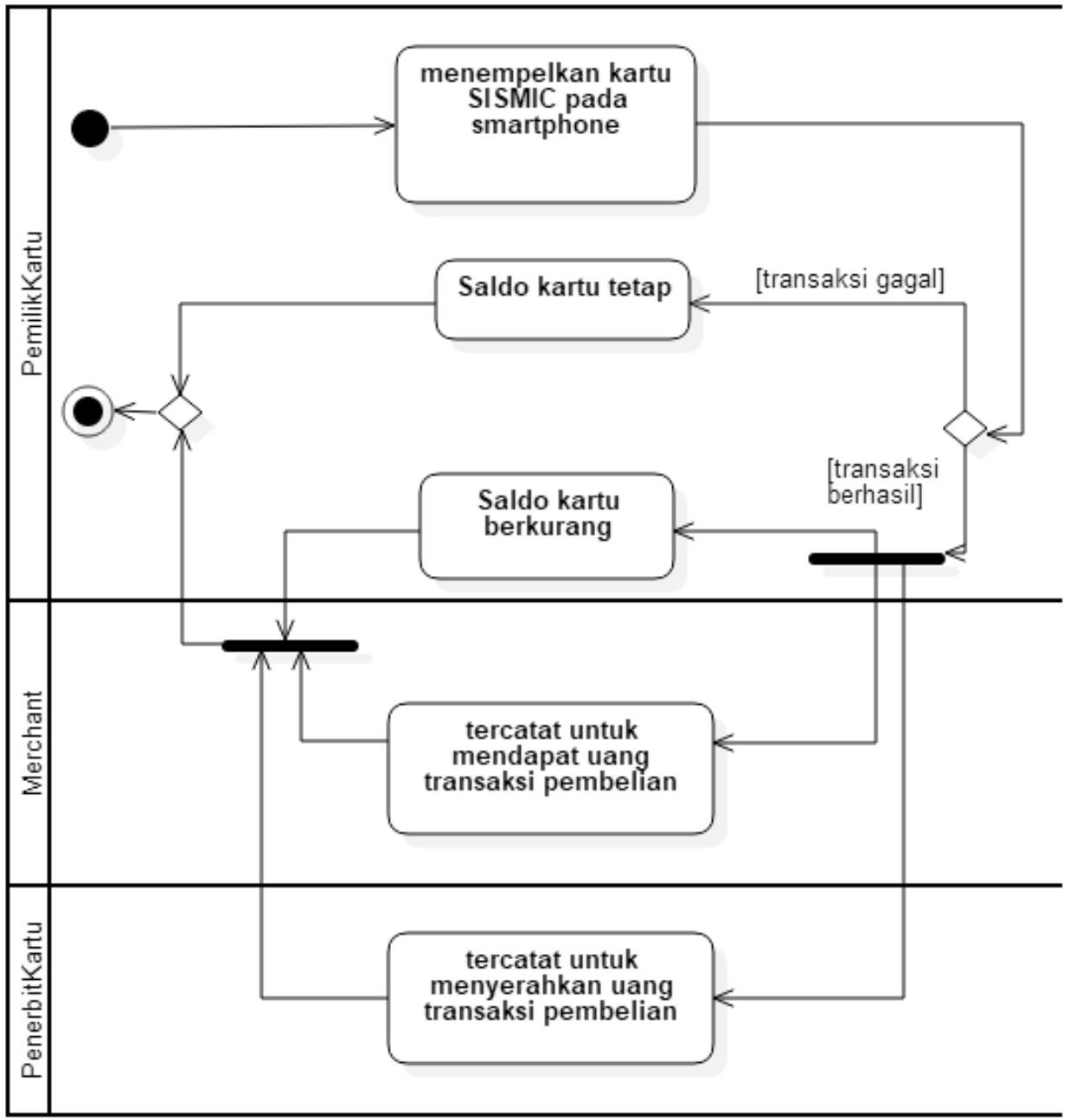
TRANSAKSI *TOP-UP*

Via *merchant*



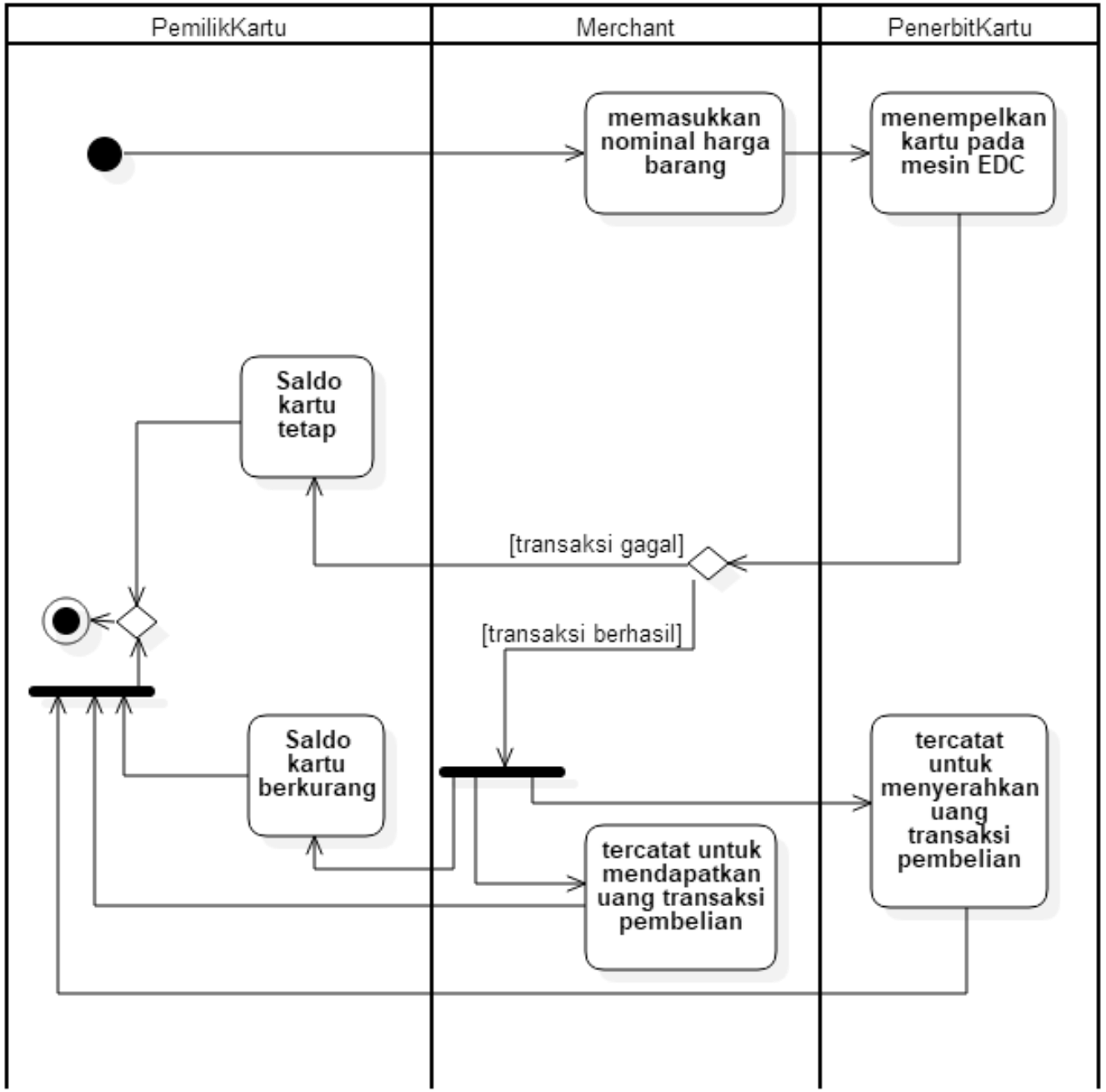
TRANSAKSI PEMBELIAN

Via *smartphone* (tanpa parameter)



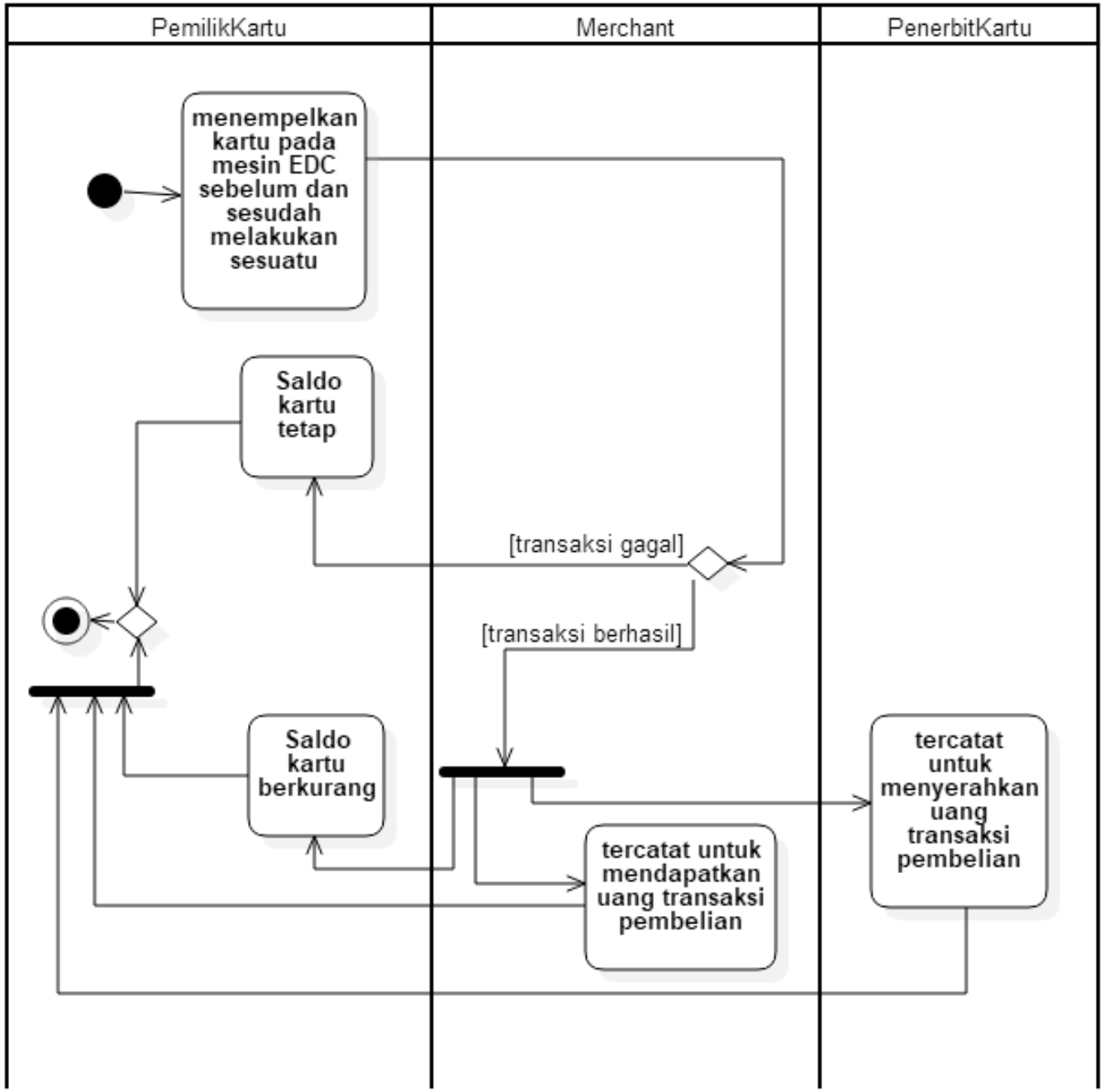
TRANSAKSI PEMBELIAN

Via *merchant* (tanpa parameter)



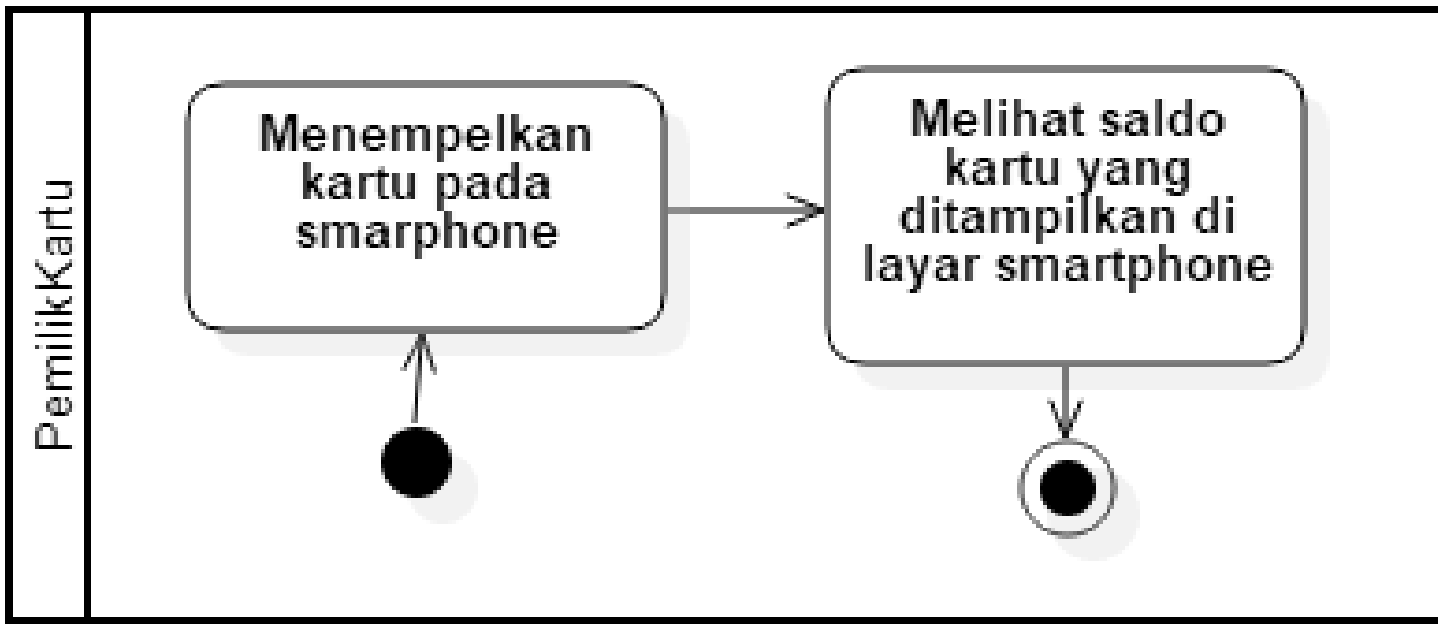
TRANSAKSI PEMBELIAN

Via *merchant* (dengan parameter)



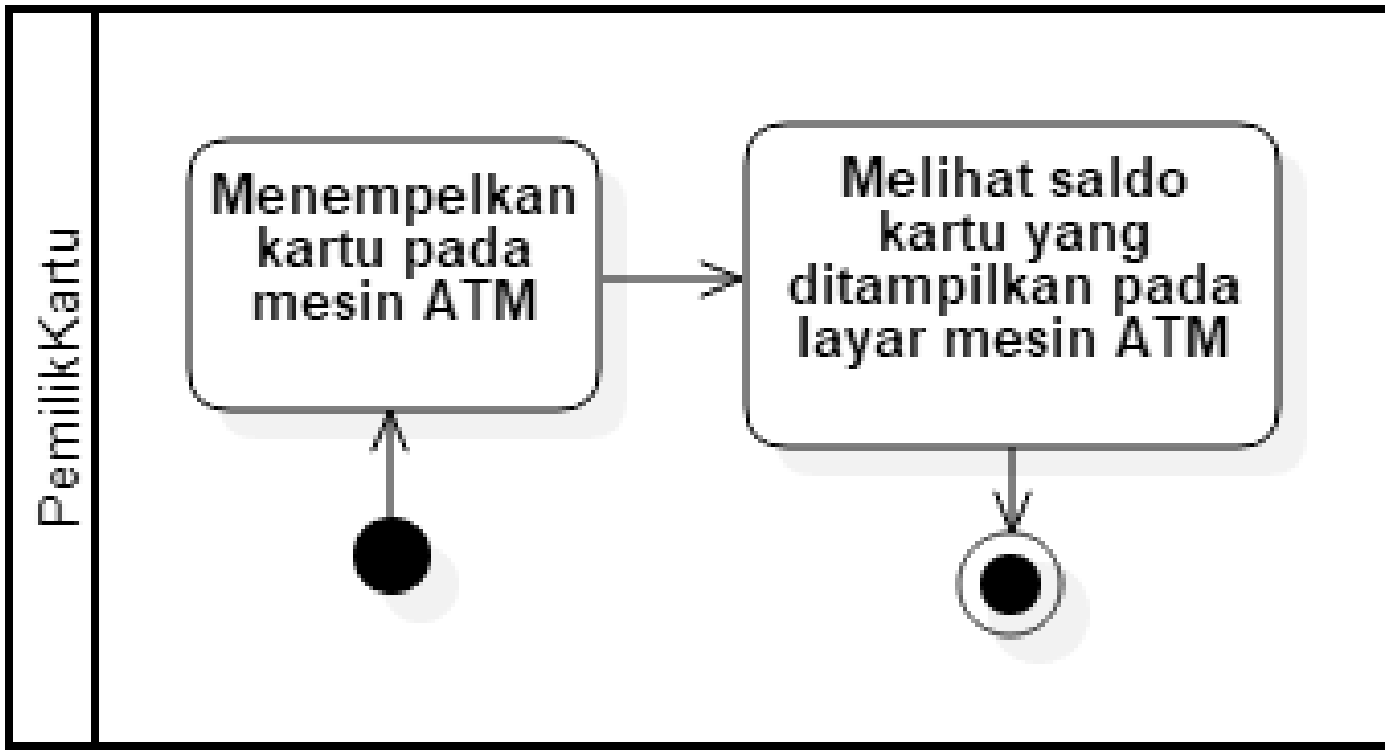
LIHAT SALDO

Via *smartphone*



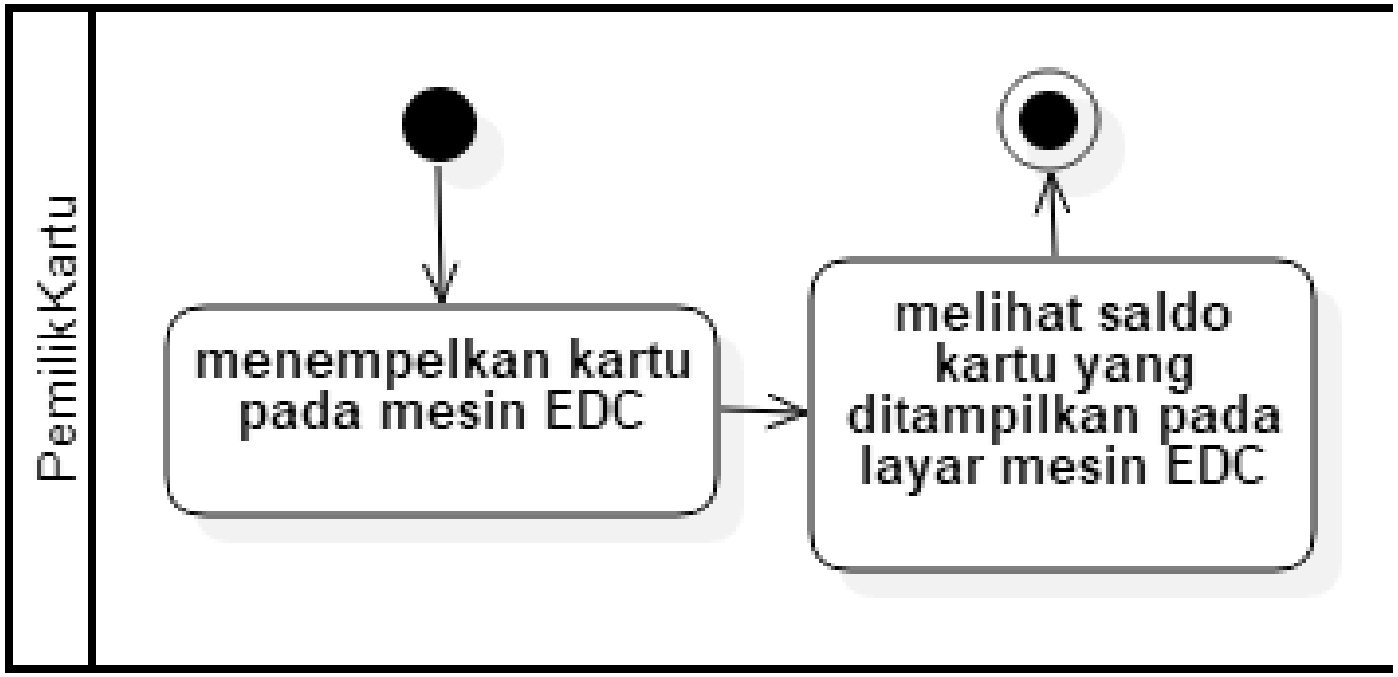
LIHAT SALDO

Via ATM



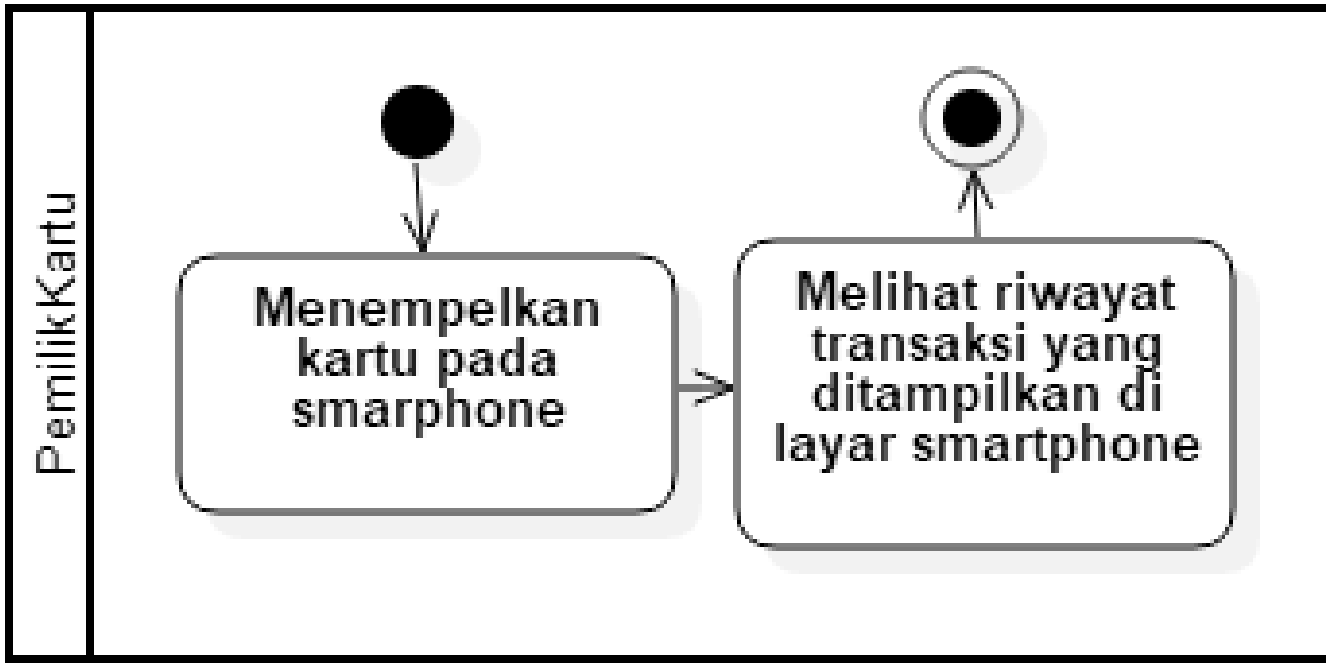
LIHAT SALDO

Via *merchant*



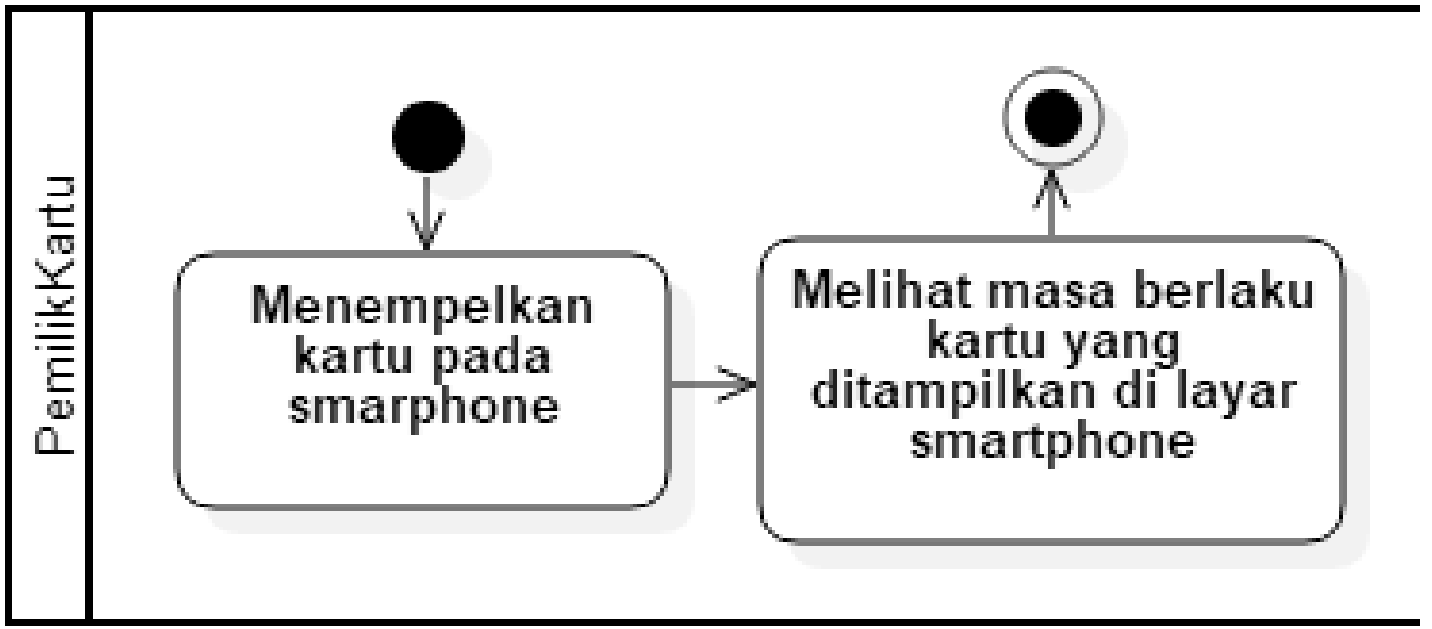
LIHAT RIWAYAT TRANSAKSI

Via *smartphone*



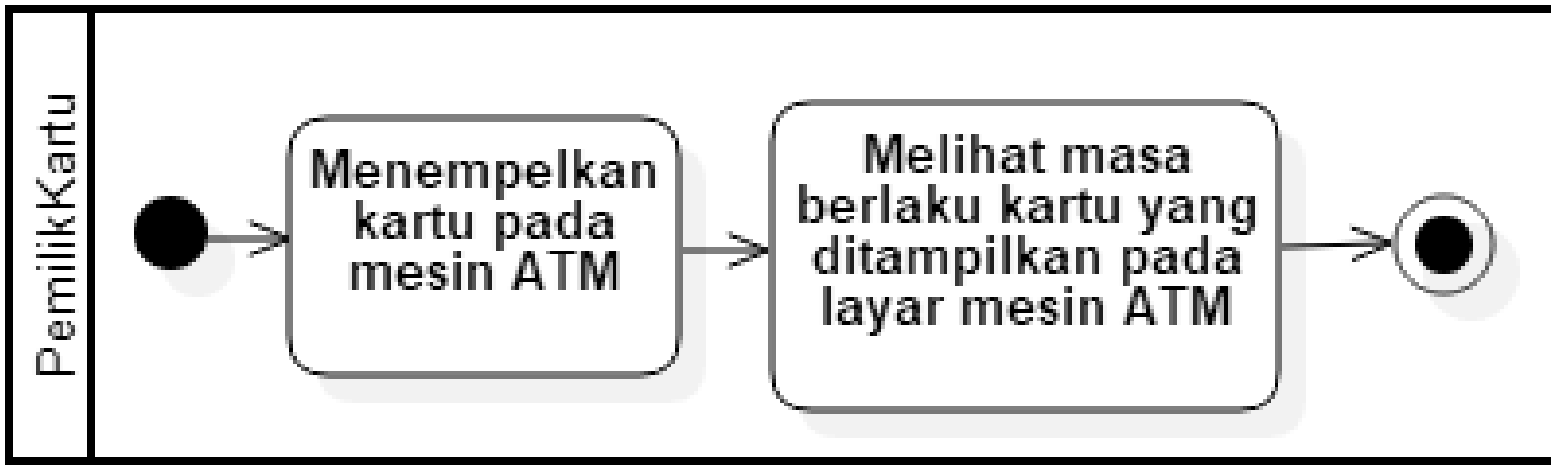
LIHAT MASA BERLAKU

Via *smartphone*



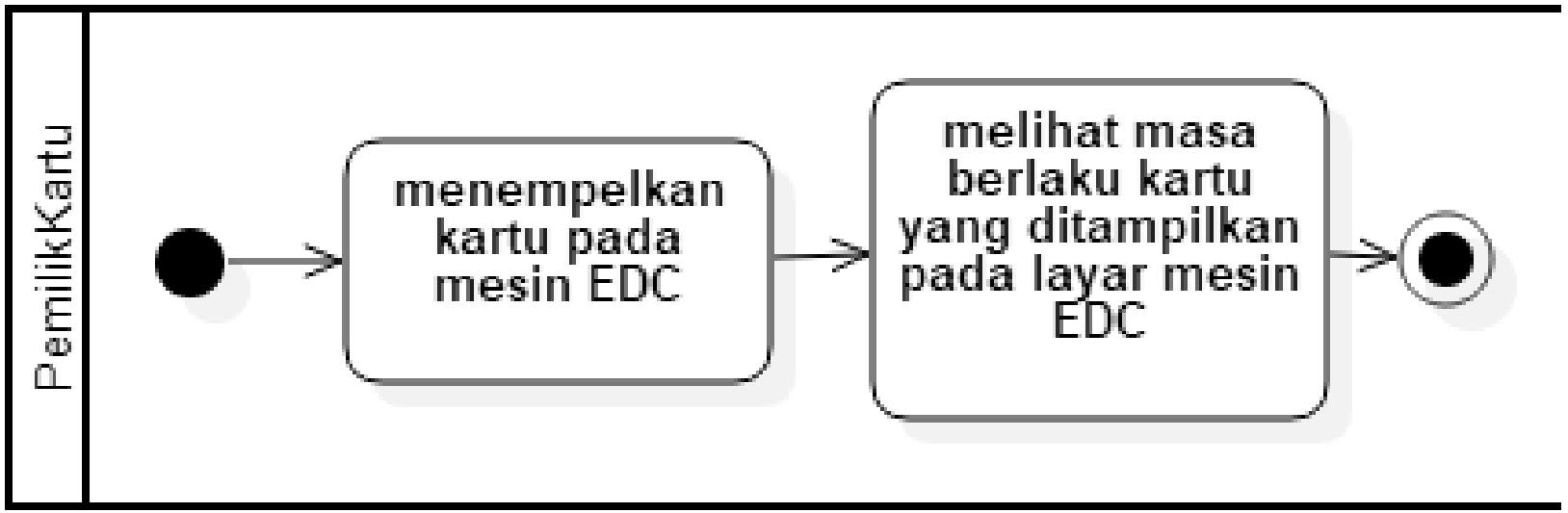
LIHAT MASA BERLAKU KARTU SISMIC

Via ATM



LIHAT MASA BERLAKU KARTU SISMIC

Via *merchant*



STRUKTUR PENYIMPANAN KARTU SISMIC

Memori 1KB, 16 sektor

- 1 sektor: 4 blok
- 1 blok: 16 *bytes*

Konfigurasi penyimpanan:

- Sektor ke-0 Blok ke-1: tanggal masa berlaku kartu
- Sektor ke-0 Blok ke-2: saldo kartu
- Sektor ke-1 - 5 Blok ke-0: waktu transaksi pembelian atau top-up
- Sektor ke-1 - 5 Blok ke-1: nominal transaksi pembelian atau top-up
- Sektor ke-1 - 5 Blok ke-2: jenis transaksi (pembelian/top-up)
- Sektor ke-6 - 14 Blok ke-0: untuk transaksi dengan parameter
- Sektor ke-6 - 14 Blok ke-1: iv dari sektor ke-6 - 14 blok ke-0
- Sektor ke-15 Blok ke-1: iv dari sektor ke-0 slok ke-1
- Sektor ke-15 Blok ke-2: iv dari sektor ke-0 slok ke-2

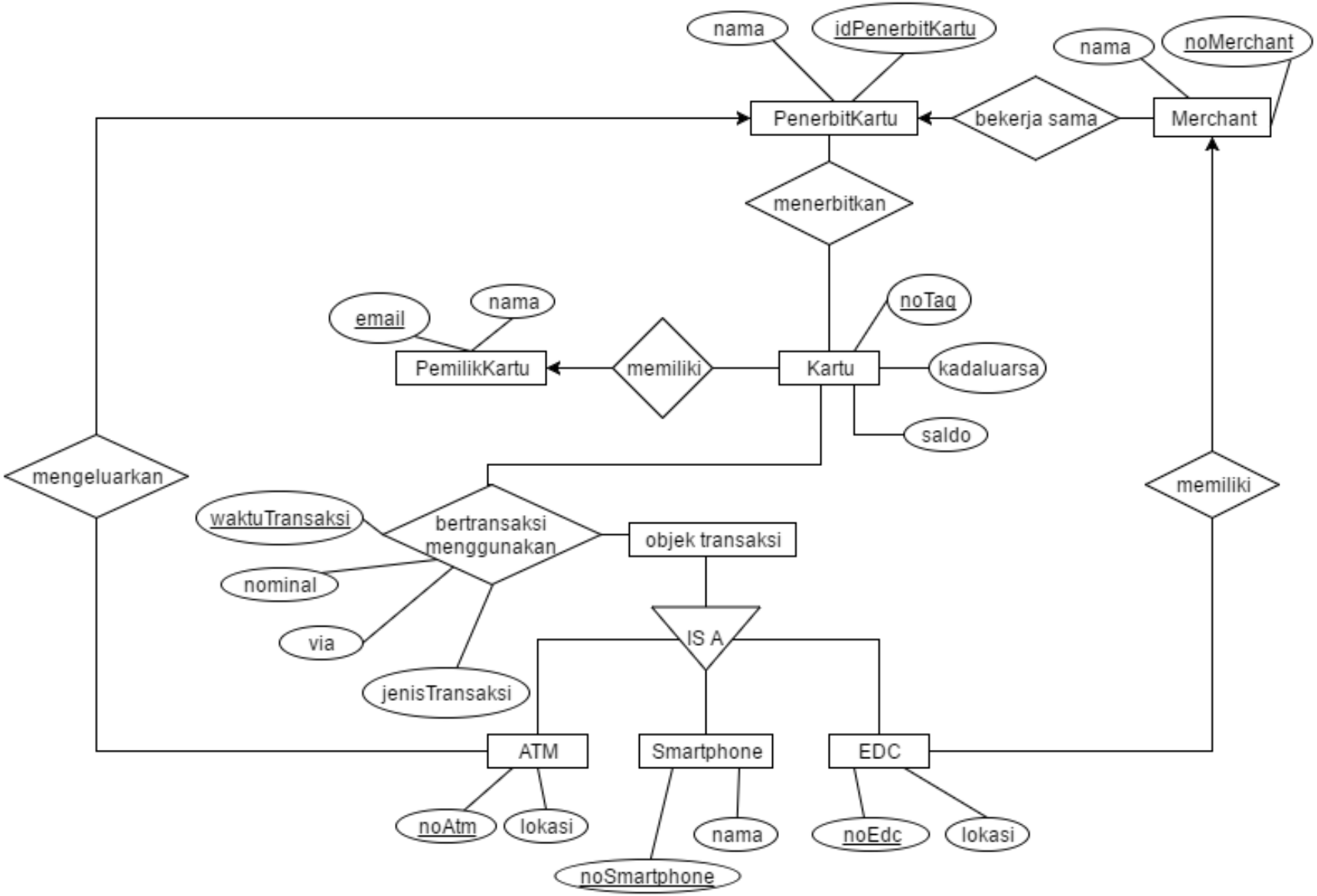
Menggunakan algoritma *round-robin*

HAK AKSES KARTU SISMIC

Sektor	Blok	Data	Hak Akses			
			Pemilik Kartu	Penerbit Kartu	Merchant	Payment Gateway
0	0	Nomor kartu	Baca	Baca	-	-
	1	Tanggal masa berlaku kartu	Baca	Baca	Baca	-
	2	Saldo Kartu	Baca	Baca, tulis	Baca, tulis	-
1-5	0	Riwayat waktu transaksi pembelian atau top-up dalam bentuk epoch	Baca	Baca, tulis	-	-
	1	Riwayat nominal transaksi pembelian atau top-up	Baca	Baca, tulis	-	-
	2	Riwayat jenis transaksi apakah transaki merupakan transaksi pembelian atau top-up	Baca	Baca, tulis	-	-
6-14	0	Parameter jarak atau waktu pertama kartu disentuh pada reader	-	-	Baca, tulis	-
	1	Iv hasil dari enkripsi blok ke-0 di sektor 6 sampai 14	-	-	-	-
	2	-	-	-	-	-
15	1	Iv hasil dari enkripsi blok ke-1 di sektor 0	-	-	-	-
	2	Iv hasil dari enkripsi blok ke-2 di sektor 0	-	-	-	-

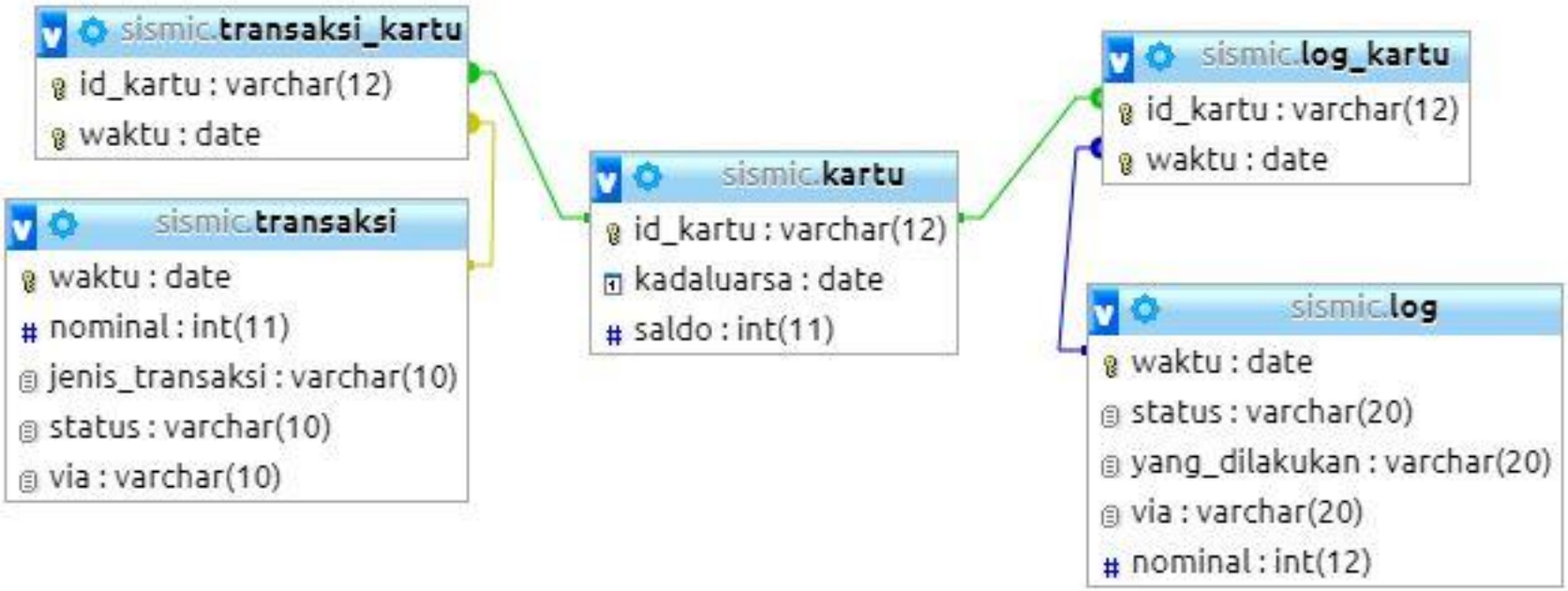
BASISDATA

Entity-Relationship Diagram



BASISDATA RELASIONAL

Basisdata SISMIC



BASISDATA RELASIONAL

Basisdata *Merchant*

BASISDATA RELASIONAL

Basisdata *Payment Gateway*

DIAGRAM KELAS

Diagram Kelas ATM

Diagram Kelas *Merchant*

Diagram Kelas *Web Service* SISMIC

Diagram Kelas *Web Service Payment Gateway*

Diagram Kelas *Web Service Merchant*

DIAGRAM KELAS

Diagram Kelas ATM

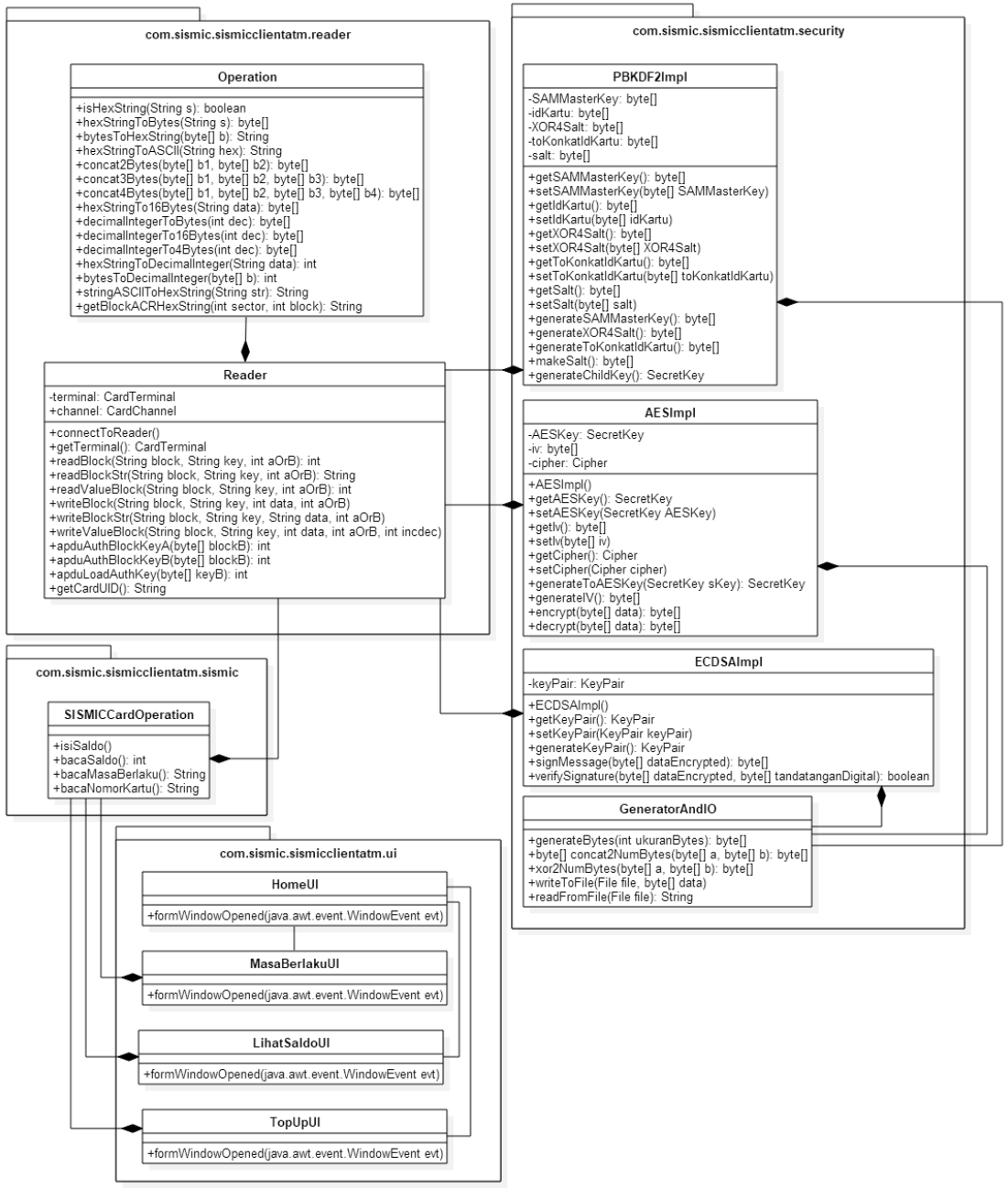


DIAGRAM KELAS

Diagram Kelas *Merchant*

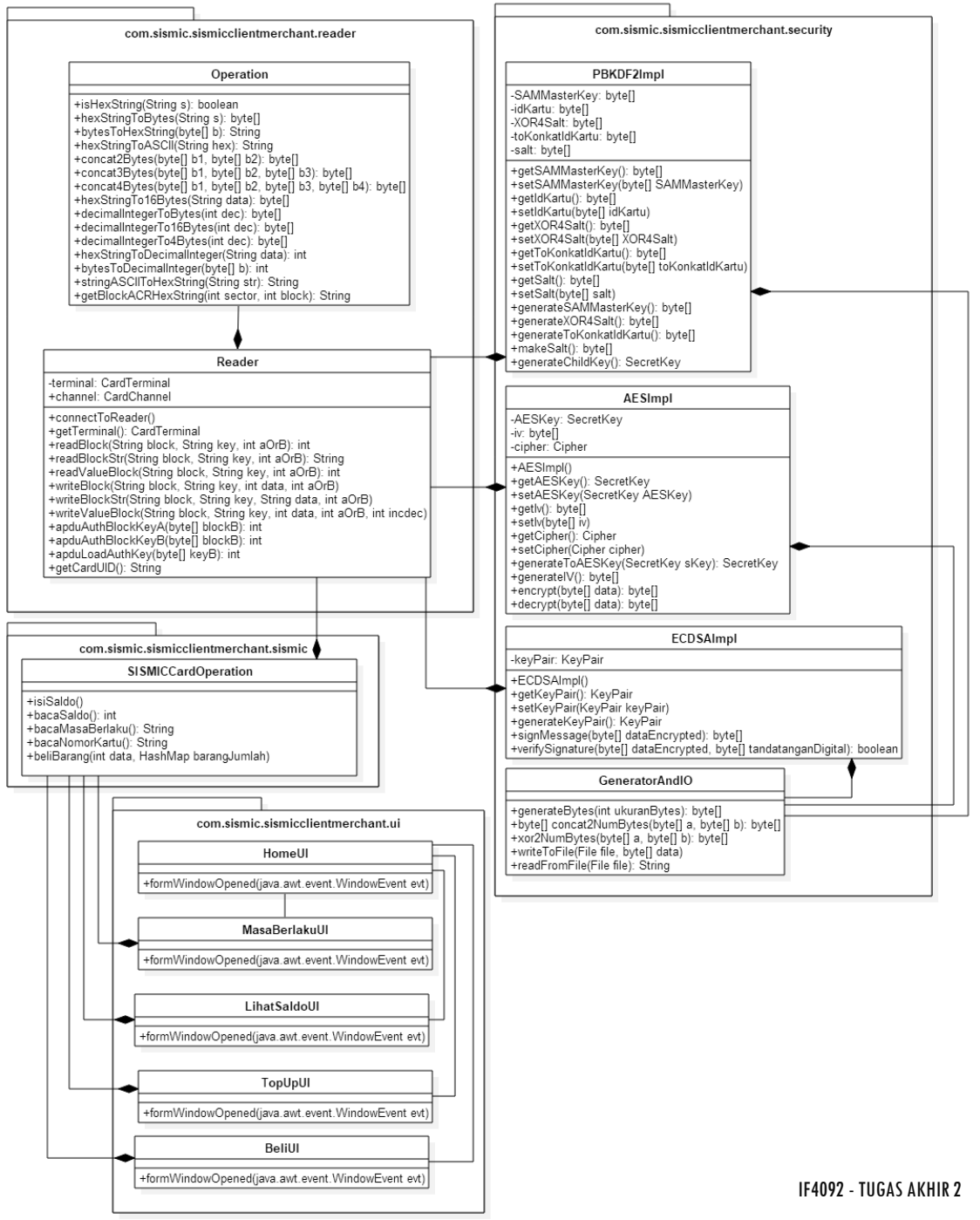


DIAGRAM KELAS

Diagram Kelas *Web Service* SISMIC

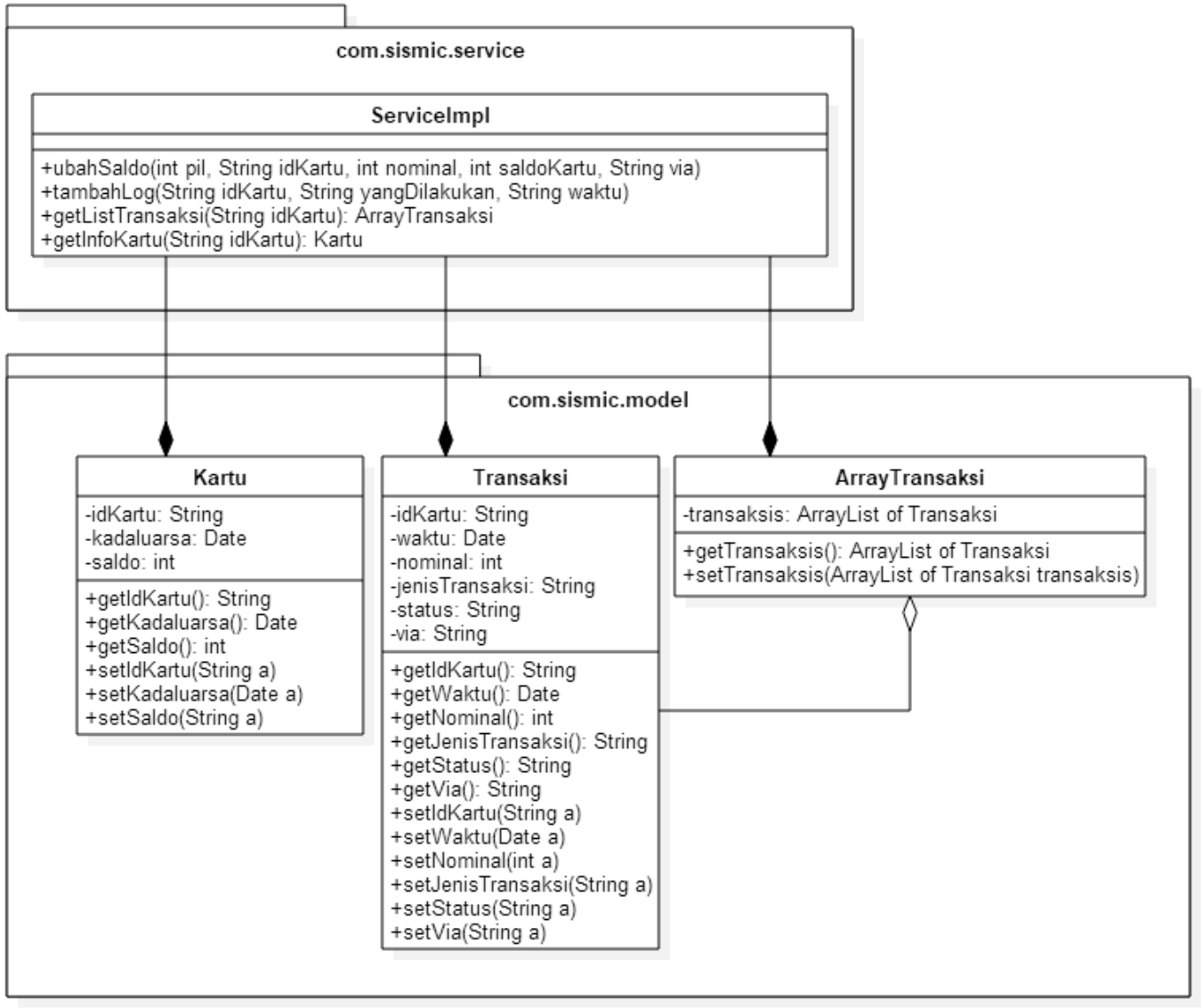


DIAGRAM KELAS

Diagram Kelas

Web Service Payment Gateway

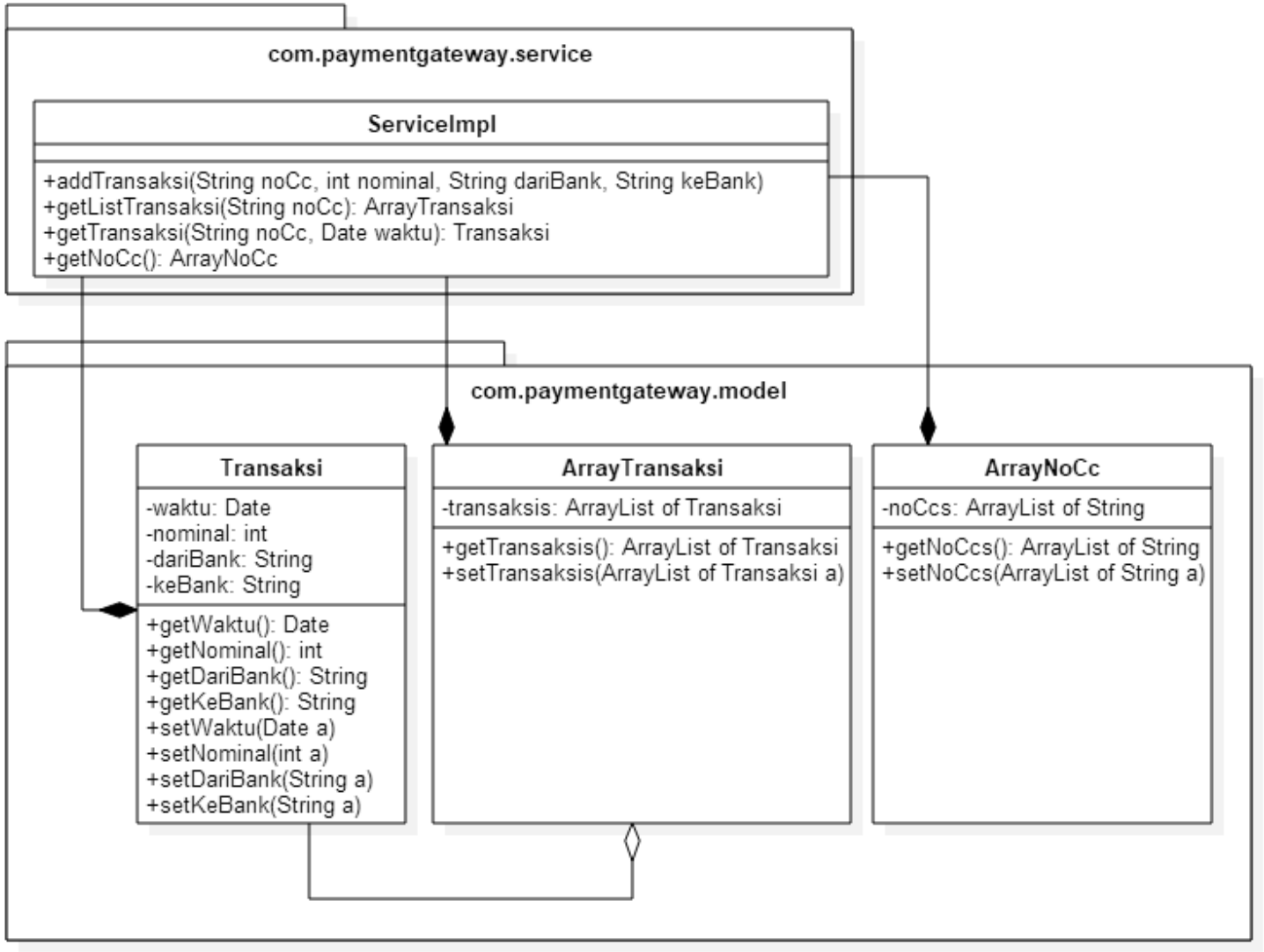
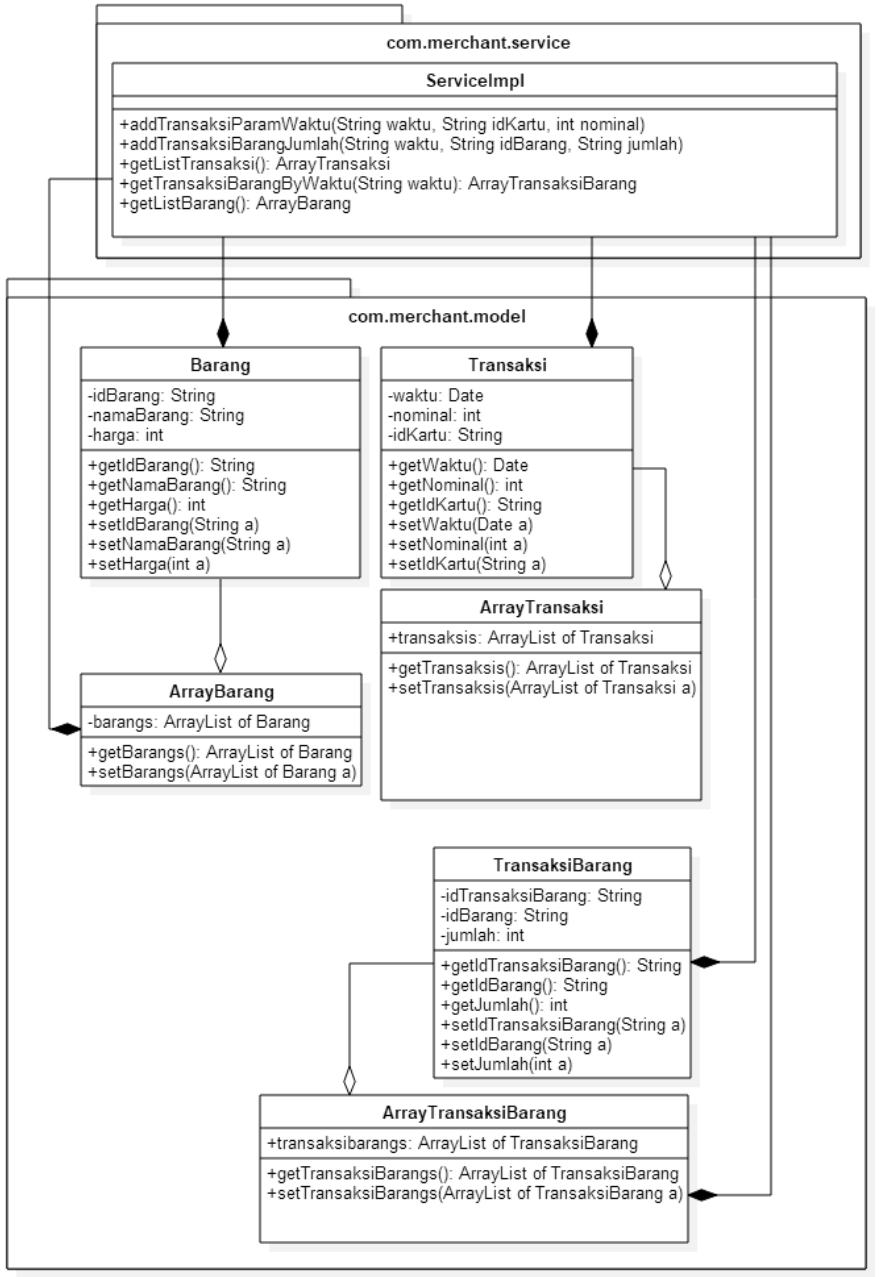


DIAGRAM KELAS

Diagram Kelas *Web Service Merchant*



ASPEK KEAMANAN SISMIC

Confidentiality

- Mengubah *key* A dan *key* B dari semua sektor di kartu SISMIC dengan manajemen kuncinya diatur di SAM
- Melindungi basisdata SISMIC dengan enkripsi dan *password*

Integrity

- Menerapkan enkripsi dan dekripsi pada SISMIC
- Pencatatan (*logging*) segala aktivitas yang terjadi di mesin EDC dan mesin ATM

Availability

- Membuat sistem cadangan redundan sehingga jika sistem utama ada gangguan, ada sistem cadangan yang dapat menggantikannya

Authentication

- SISMIC menyimpan identitas mesin EDC yang dikeluarkan resmi oleh penerbit kartu
- Menerapkan *digital signature*

Authorization

- *Key* A atau *key* B yang digunakan untuk melakukan transaksi dengan kartu SISMIC berbeda-beda tiap pihak

Accountability dan *Non-repudiation*

- Pencatatan (*logging*) segala aktivitas yang terjadi di SISMIC

MANAJEMEN & DISTRIBUSI KUNCI

Manajemen dan distribusi kunci akan diatur pada *Secure Access Module* (SAM).

SAM menyimpan dan mengolah kunci pada SISMIC (*key* A → baca kartu, *key* B → tulis kartu, kunci AES → kriptografi).

SAM sudah memiliki sistem kriptografi sendiri → kunci aman.

SAM punya kunci master → diturunkan menjadi kunci-kunci lain (PBKDF2).

Kunci AES (16 bytes) → salt: idKartu (8 bytes) + bil.random (12 bytes) XOR bil.random (20 bytes)

Key A & *Key* B (6 bytes) → salt: idKartu (8 bytes) + posisi sektor (1 bytes) + bil.random (11 bytes) XOR bil.random (20 bytes)

Key untuk *merchant* → salt: idKartu (8 bytes) + posisi sektor (1 bytes) + bil.random (11 bytes) XOR bil.random (20 bytes) XOR idMerchant (20 bytes)

SAM disimpan pada aplikasi

KRIPTOGRAFI PADA SISMIC

Enkripsi dan dekripsi: algoritma AES

Digital signature

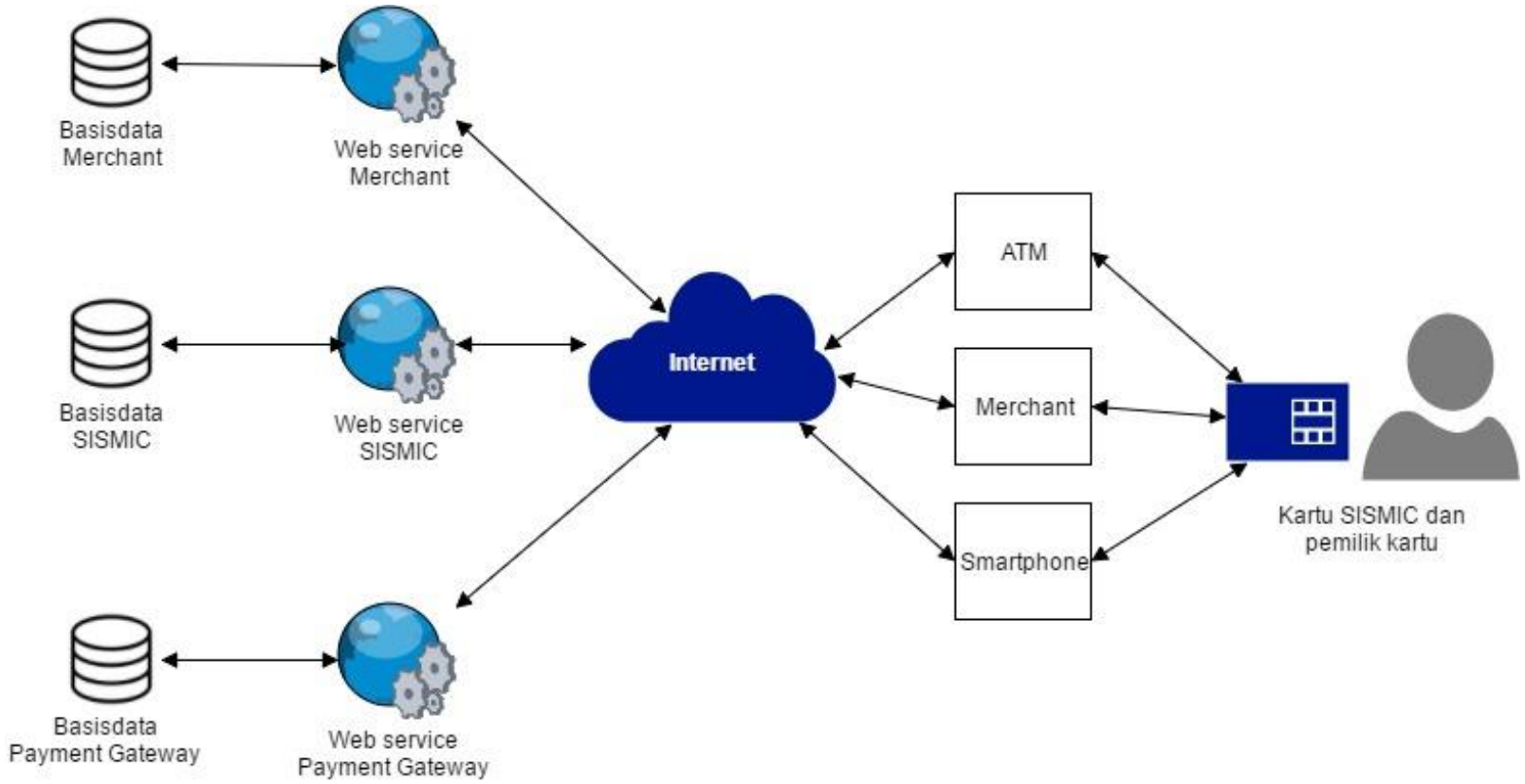
- algoritma ECDSA.
- apakah pesan berasal dari pihak yang benar atau tidak

Proses:

- Kunci AES → mengenkripsi pesan yang akan dikirim ke mesin pembaca kartu
- Pesan yang dienkripsi → diberi *digital signature* dengan **kunci privat.** dikirim ke mesin pembaca kartu
- Mesin pembaca kartu → periksa *digital signature* dengan **kunci publik**
- OK → pesan didekripsi dengan **kunci AES** dan instruksi dijalankan

IMPLEMENTASI

ARSITEKTUR SISMIC



KAKAS & *LIBRARY*

IDE NetBeans (bahasa Java)

Basisdata menggunakan NoSQL dan disimpan *online* di Firebase. *Library* Firebase versi 2.5.2.

CFX JAXWS untuk Heroku yang dibuat oleh Chamerling

API Java Smart Card I/O

Library Bouncy Castle (PBKDF2, AES, dan ECDSA)

LINGKUNGAN IMPLEMENTASI

Sistem operasi: Windows 10 64-bit

Bahasa pemrograman: Java

Basisdata: NoSQL dengan disimpan di Firebase

Web Service: CXF JAXWS di Heroku

HASIL IMPLEMENTASI

Aplikasi ATM

Aplikasi *merchant*

Aplikasi *Smartphone* SISMIC & merchant tidak diimplementasi

PENGUJIAN

TUJUAN & BATASAN

Tujuan: Membuktikan bahwa fungsionalitas aplikasi ATM dan *merchant* dapat berjalan dengan baik dan benar

Batasan: Aspek keamanan tidak diimplementasi semua → celah keamanan tidak diuji

PERANGKAT & LINGKUNGAN

Perangkat: NFC *reader* & kartu Mifare Classic ukuran 1 KB

Lingkungan:

- Sistem operasi: Windows 10 64-bit
- Bahasa pemrograman: Java
- Basisdata: NoSQL dengan disimpan di Firebase
- *Web Service*: CXF JAXWS di Heroku

STRATEGI PENGUJIAN

Top-down testing → *bug* lebih cepat dan mudah ditemukan di awal

Blackbox → menguji fungsionalitas program tanpa melihat kode program

KASUS, SKENARIO, DAN HASIL UJI

Kasus Uji Aplikasi ATM

- 1. Pengujian *top-up* saldo
- 2. Pengujian lihat saldo
- 3. Pengujian lihat masa berlaku

Kasus Uji Aplikasi Merchant

- 1. Pengujian transaksi pembelian tanpa parameter
- 2. Pengujian transaksi pembelian dengan parameter
- 3. Pengujian *top-up* saldo
- 4. Pengujian lihat saldo
- 5. Pengujian lihat masa berlaku

KESIMPULAN HASIL UJI

Pengujian fungsionalitas aplikasi ATM & *merchant* = diterima

Skenario yang dilakukan pengujian berbeda dengan perancangan

KESIMPULAN & SARAN

KESIMPULAN

Perancangan sistem *micropayment* NFC selesai dirancang

Aplikasi ATM & *merchant* berhasil dibuat tetapi berbeda dari perancangan.

Aplikasi *smartphone* SISMIC & aplikasi *smartphone merchant* tidak berhasil diimplementasi

Aspek keamanan tidak diuji

SARAN

Implementasi perancangan diterapkan pada studi kasus yang lebih rinci & nyata

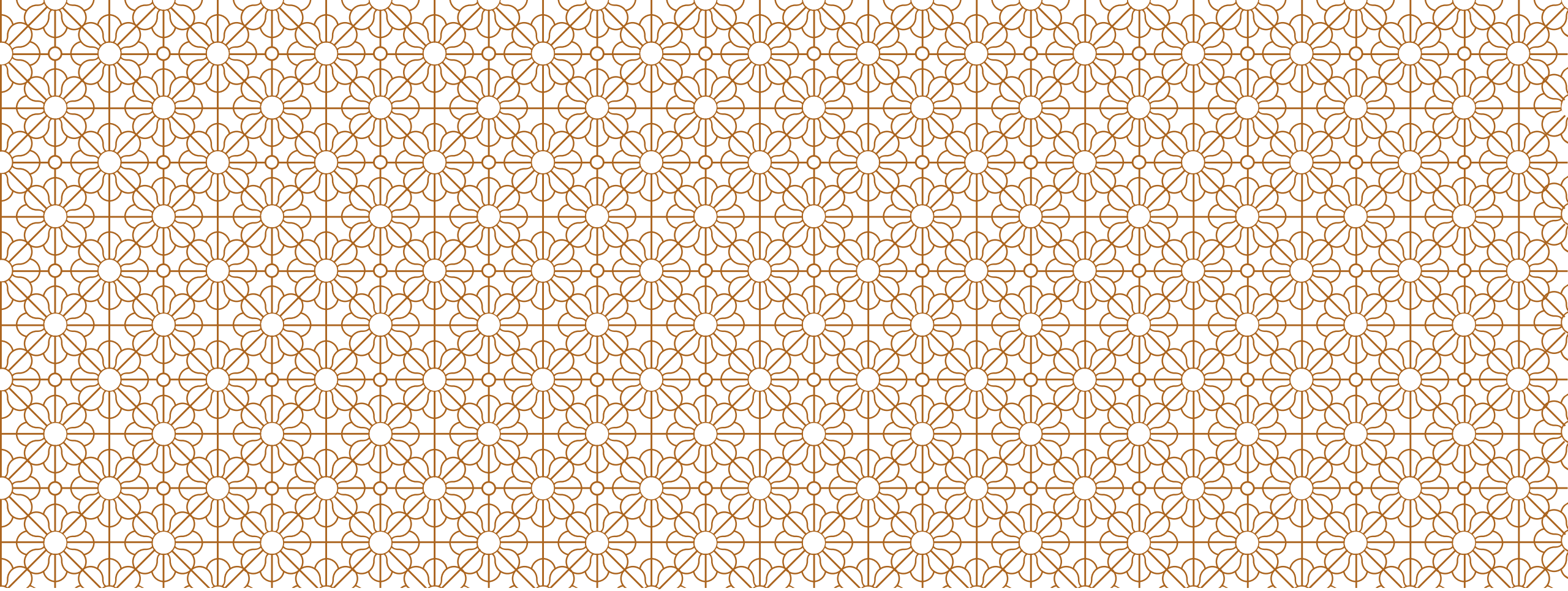
Aplikasi *smartphone* SISMIC & aplikasi *smartphone* SISMIC diimplementasi sesuai rancangan

Implementasi transaksi pembelian aplikasi *merchant* dikembangkan sesuai perancangan

Ditambah perancangan yang mengatasi transaksi yang gagal dilakukan.

Pengembangan pada implementasi kriptografi untuk NFC *reader* → aspek keamanan dapat diuji.

Memikirkan aspek *user-experience* → aplikasi lebih mudah, nyaman, dan menarik untuk digunakan → daya tarik dan nilai jual yang lebih baik.



TERIMA KASIH