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

Draft Laporan Tugas Akhir II

Oleh

Arina Listyarini Dwiastuti

NIM: 13512006

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TEKNIK ELEKTRO & INFORMATIKA

INSTITUT TEKNOLOGI BANDUNG

Agustus 2017

DAFTAR ISI

BAB III

ANALISIS KEBUTUHAN DAN PERANCANGAN SISTEM *MICROPAYMENT* DENGAN TEKNOLOGI NFC

III.1 Analisis Kebutuhan dan Keamanan SISMIC

Subbab ini meliputi pembahasan tentang analisis kebutuhan SISMIC dan analisis kebutuhan keamanan SISMIC.

III.1.1 Analisis Kebutuhan SISMIC

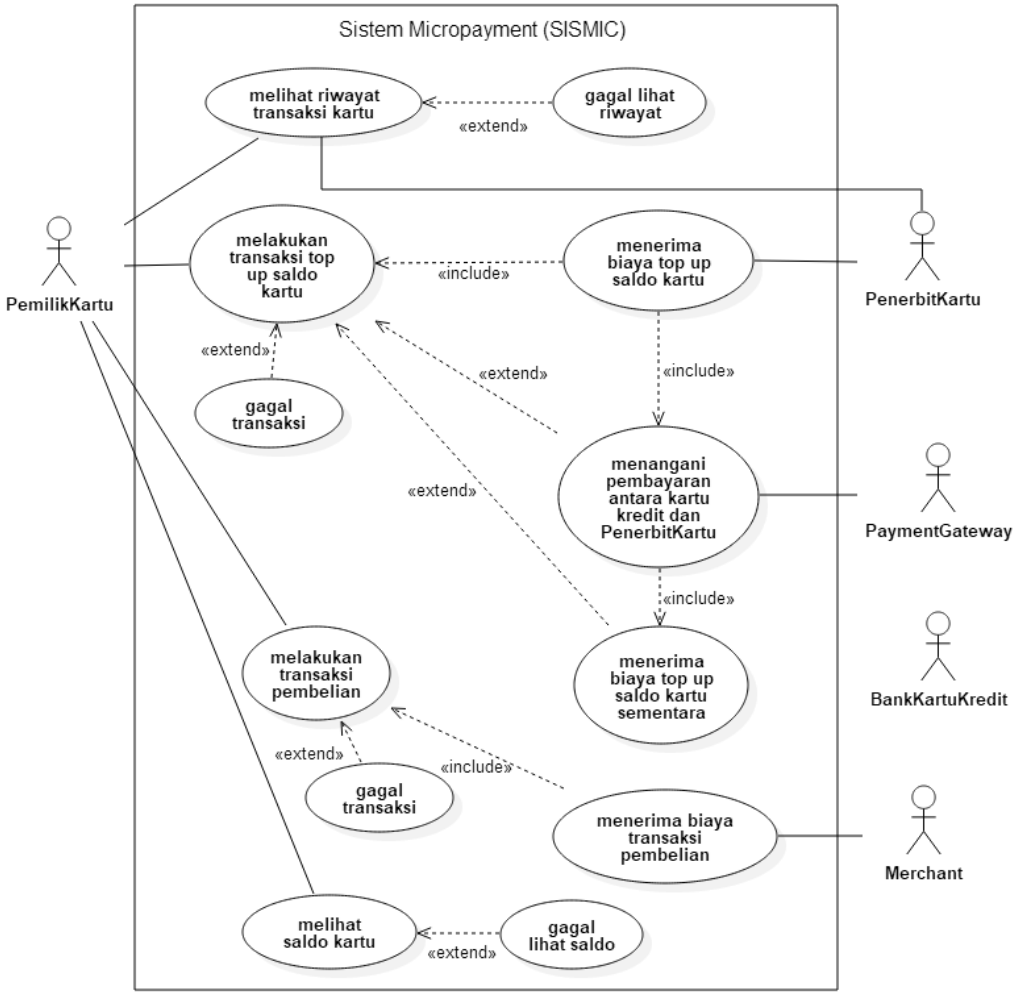
Tugas akhir ini membuat perancangan untuk sebuah sistem transaksi *micropayment* yang disebut SISMIC. SISMIC harus memenuhi kebutuhan-kebutuhan sebagai berikut:

1. SISMIC dapat melakukan transaksi *top-up* saldo kartu.
   1.1. SISMIC dapat menambah saldo kartu.
   1.2. SISMIC dapat memberikan biaya pembayaran *top-up* saldo kartu ke penerbit kartu.
   1.3. SISMIC dapat menyimpan riwayat transaksi *top-up* saldo kartu ke dalam kartu.
   1.4. SISMIC dapat menyimpan riwayat transaksi *top-up* saldo kartu ke dalam basisdata.
2. SISMIC dapat melakukan transaksi pembelian menggunakan kartu.
   2.1. SISMIC dapat mengurangi saldo kartu.
   2.2. SISMIC dapat memberikan biaya transaksi pembelian pemilik kartu ke *merchant*.
   2.3. SISMIC dapat menyimpan riwayat transaksi pembelian ke dalam kartu.
   2.4. SISMIC dapat menyimpan riwayat transaksi pembelian saldo kartu ke dalam basisdata.
3. SISMIC dapat menunjukkan saldo kartu pada pemilik kartu.

4. SISMIC dapat menunjukkan riwayat transaksi kartu pada pemilik kartu.
5. Kartu SISMIC memiliki masa berlaku (tanggal kadaluarsa).

Benda-benda yang ada pada SISMIC adalah sebagai berikut:

1. Kartu SISMIC yang merupakan sebuah *tag* NFC.
2. *Smartphone* yang mendukung fitur NFC dan berplatform Android.
3. Mesin EDC, yang dimiliki oleh *merchant*.
4. Mesin ATM, yang dimiliki oleh penerbit kartu.



Gambar III-1 Diagram *Use Case* SISMIC

Gambaran umum apa saja yang dapat dilakukan SISMIC dapat dilihat pada Gambar III-1 di atas yang berupa diagram *use case*. Pada Gambar III-1, ada

beberapa aktor pada SISMIC. Aktor-aktor yang ada pada SISMIC dapat dilihat sebagai berikut:

1. Penerbit kartu. Penerbit kartu bisa berasal dari bank, *provider* kartu telepon selular, dan lain-lain. Pada umumnya di Indonesia, penerbit kartu berasal dari bank. Pada tugas akhir ini, penerbit kartu adalah sebuah bank.
2. Pemilik kartu, yaitu orang yang membeli kartu dari penerbit kartu dan dapat menggunakan kartu tersebut untuk melakukan berbagai transaksi dengan memanfaatkan teknologi NFC.
3. *Merchant*, yaitu tempat di mana pemilik kartu dapat melakukan transaksi pembelian. *Merchant* dapat berupa supermarket, restoran, dan lain-lain. *Merchant* ini telah bekerja sama dengan penerbit kartu.
4. *Payment gateway*, yaitu perantara transaksi yang terjadi antara penerbit kartu dan bank kartu kredit yang dimiliki pemilik kartu. *Payment gateway* adalah adalah layanan transaksi perdagangan menggunakan teknologi informasi (Gulati & Srivastava, 2007). *Payment gateway* melayani proses pembayaran menggunakan kartu kredit atau pembayaran langsung. Layanan *payment gateway* dapat disediakan oleh bank kepada pelanggannya atau penyedia layanan keuangan lainnya sebagai layanan terpisah oleh penyedia layanan keuangan elektronik.
5. Bank Kartu Kredit, yaitu bank di mana pemilik kartu membuat kartu kredit. Bank kartu kredit berperan ketika pemilik kartu melakukan transaksi *top-up* saldo kartu melalui *smartphone*. Bank kartu kredit dapat menerima biaya *top-up* saldo kartu yang nantinya akan diserahkan ke penerbit kartu melalui *payment gateway*.

Seperti yang dapat dilihat pada Gambar III-1, pemilik kartu dapat melakukan transaksi *top-up* saldo kartu, transaksi pembelian, melihat saldo kartu SISMIC, dan melihat riwayat transaksi kartu SISMIC. Penerbit kartu dapat menerima uang *top-up* saldo kartu SISMIC dari pemilik kartu. *Merchant* dapat menerima biaya uang transaksi pembelian oleh pemilik kartu SISMIC. *Payment gateway*

menangani pembayaran antara kartu kredit dan penerbit kartu jika pemilik kartu melakukan *top-up* kartu SISMIC menggunakan kartu kredit melalui *smartphone*.

III.1.2 Analisis Kebutuhan Keamanan SISMIC

Aspek keamanan yang harus dicapai oleh SISMIC adalah berikut:

- *Confidentiality*
  - Data yang ada pada SISMIC bersifat rahasia dan tidak dapat diakses oleh orang yang tidak berhak.
- *Integrity*
  - Data SISMIC tidak boleh berubah tanpa izin dari pihak yang berhak.
- *Availability*
  - Ketika orang, baik penerbit kartu, pemilik kartu, ataupun *merchant*, menggunakan SISMIC, layanan dan data pada SISMIC harus dapat digunakan.
- *Authentication*
  - Transaksi SISMIC hanya dapat dilakukan pada *hardware* dan *software* yang resmi dikeluarkan oleh penerbit kartu.
- *Authorization*
  - Penerbit kartu, pemilik kartu, dan *merchant* 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 dari penerbit kartu, pemilik kartu, maupun *merchant* yang dapat menyanggah suatu transaksi yang telah terjadi.

Pada subbab berikutnya, akan dijelaskan operasi apa saja yang dapat dilakukan SISMIC.

III.2 Perancangan SISMIC

Subbab ini meliputi pembahasan tentang apa saja operasi yang ada pada aplikasi SISMIC, bagaimana penyimpanan dan struktur data pada SISMIC, dan bagaimana rancangan keamanan SISMIC.

III.2.1 Operasi Aplikasi SISMIC

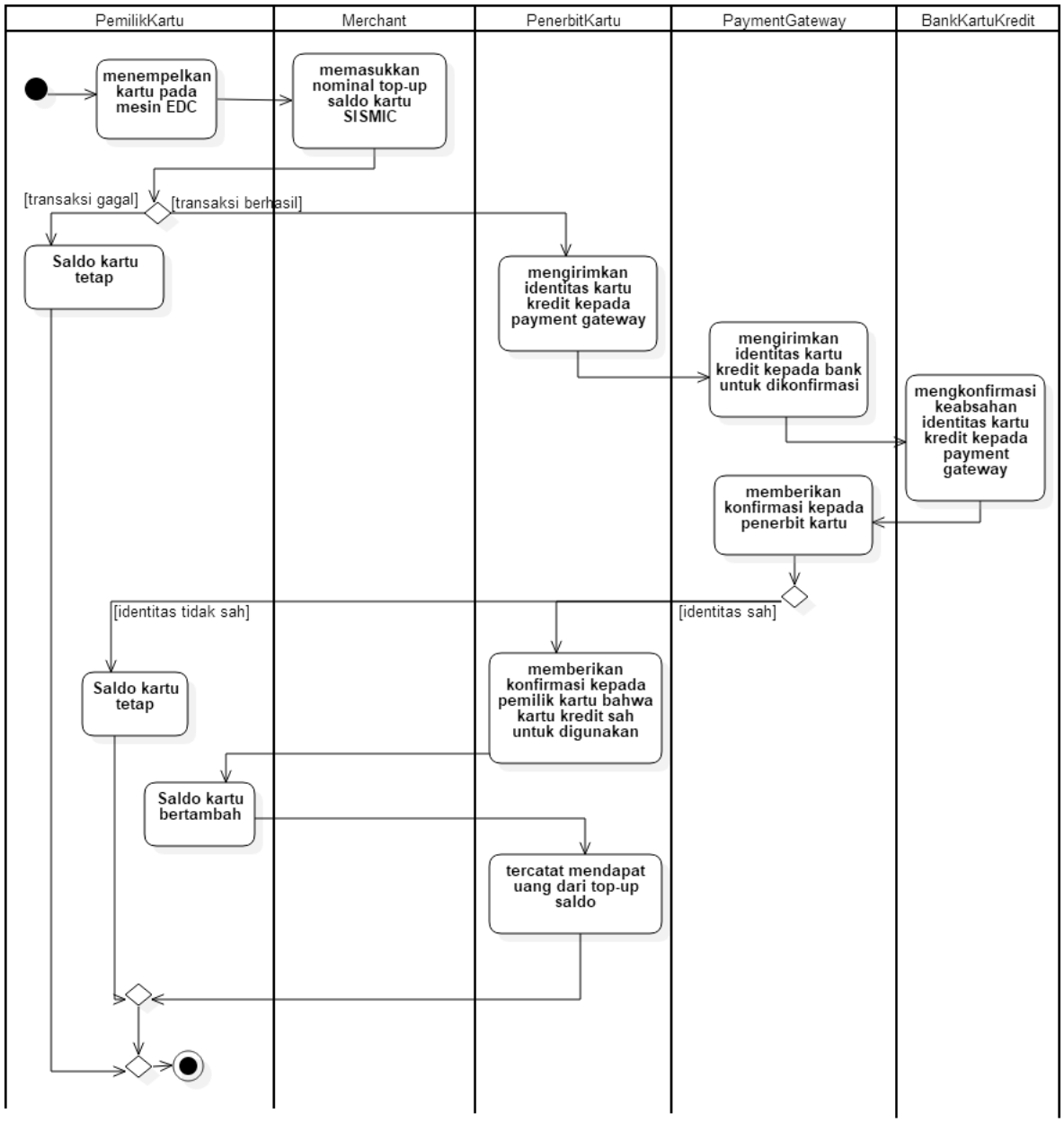
Operasi Aplikasi SISMIC meliputi pembahasan tentang bagaimana terjadinya transaksi *top-up* kartu SISMIC, terjadinya transaksi pembelian, proses melihat saldo, proses melihat riwayat transaksi, dan proses melihat masa berlaku kartu.

III.2.1.1 Transaksi *Top-Up* Kartu SISMIC

Transaksi *Top-Up* Kartu SISMIC meliputi pembahasan tentang transaksi *top-up* kartu SISMIC melalui *smartphone*, ATM, dan *merchant*.

III.2.1.1.1 Melalui *Smartphone*

Transaksi *top-up* kartu SISMIC dapat dilakukan secara *online* melalui *smartphone* yaitu melalui aplikasi SISMIC. Diagram aktivitas untuk transaksi *top-up* kartu SISMIC melalui *smartphone* dapat dilihat pada gambar III.2 berikut ini.



Gambar III-2 Diagram Aktivitas Transaksi *Top-Up* Saldo Melalui *Smartphone*

Pada Gambar III-2, dapat dilihat bagaimana alur kerja transaksi *top-up* saldo pada SISMIC melalui *smartphone*. Pertama, pemilik kartu memasukkan nominal *top-up* saldo kartu SISMIC pada *smartphone* melalui aplikasi SISMIC. Setelah itu, pemilik kartu memasukkan nomor kartu kredit dengan nomor CVV dan pemilik kartu menempelkan kartu pada *smartphone*. Jika transaksi berhasil, saldo kartu SISMIC akan bertambah. Jika transaksi gagal, saldo kartu SISMIC akan tetap

seperti sebelumnya. Hal yang menyebabkan transaksi *top-up* gagal adalah nominal *top-up* yang membuat kartu SISMIC memiliki jumlah saldo melebihi batas maksimal saldo dan masa berlaku kartu SISMIC sudah habis.

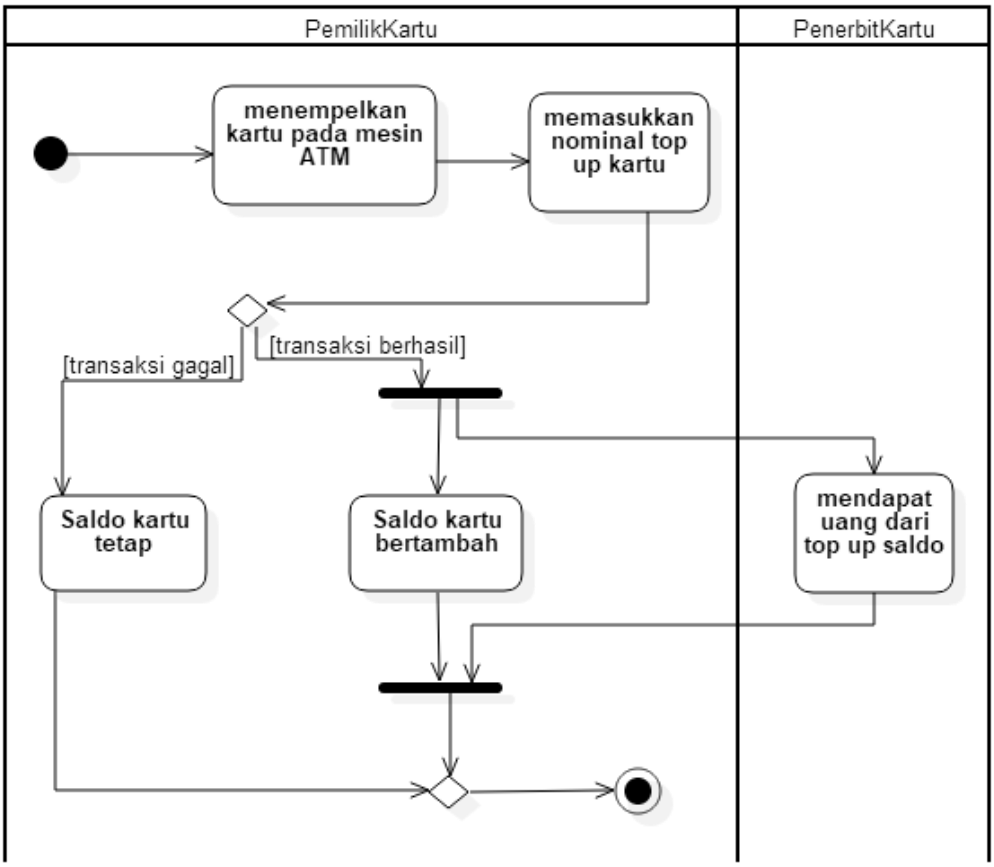
Setiap transaksi *top-up* melalui *smartphone* yang terjadi akan dicatat ke riwayat transaksi *top-up,* baik yang berhasil ataupun yang gagal, pada basisdata SISMIC, kartu SISMIC, dan basisdata *payment gateway*.

Pemilik kartu harus memiliki kartu kredit untuk melakukan transaksi pada *smartphone*. Pembayaran dilakukan dengan pemilik kartu memasukkan nomor kartu kredit dan nomor CVV. Penerbit kartu akan bekerja sama dengan *payment gateway* untuk melakukan transaksi dengan kartu kredit. Berikut ini adalah proses bagaimana penerbit kartu dapat menerima pembayaran transaksi *top-up* dari pemilik kartu yang melakukan transaksi *top-up* melalui *smartphone* dengan kartu kredit:

1. Aplikasi SISMIC mengirimkan identitas kartu kredit kepada *payment gateway*.
2. *Payment gateway* mengirimkan identitas kartu kredit kepada bank kartu kredit untuk dikonfirmasi apakah identitas kartu kredit benar atau salah dan apakah masih dapat digunakan atau tidak.
3. Bank kartu kredit memberikan konfirmasi keabsahan identitas kartu kredit kepada *payment gateway*.
4. *Payment gateway* memberikan konfirmasi kepada penerbit kartu.
5. Jika kartu kredit sah untuk digunakan pembayaran, penerbit kartu melalui aplikasi SISMIC memberikan konfirmasi kepada pemilik kartu bahwa kartu kredit sah untuk digunakan.
6. Saldo kartu pemilik kartu bertambah.
7. *Payment gateway* menangani pembayaran transaksi *top-up* antara penerbit kartu dan bank kartu kredit dengan mencatat uang *top-up* saldo kartu yang harus diserahkan dari bank kartu kredit ke penerbit kartu di basisdata *payment gateway*. Penerbit kartu dalam periode tertentu akan menerima uang *top-up* saldo kartu.

III.2.1.1.2 Melalui ATM

Selain melalui *smartphone*, transaksi *top-up* kartu SISMIC dapat dilakukan secara *offline* melalui mesin ATM yang dikeluarkan oleh penerbit kartu. Mesin ATM yang dapat digunakan untuk transaksi *top-up* kartu SISIMC harus memiliki slot untuk membaca kartu SISMIC. Mesin ATM pada tugas akhir ini akan disimulasikan dengan NFC *reader* dan *desktop*.



Gambar III-3 Diagram Aktivitas Transaksi *Top-Up* Melalui Mesin ATM

Pada Gambar III-3 di atas, dapat dilihat bagaimana alur kerja transaksi *top-up* saldo pada SISMIC melalui mesin ATM. Sedangkan untuk diagram komunikasi transaksi *top-up* saldo pada SISMIC melalui mesin ATM dapat dilihat di lampiran B. Pemilik kartu mendatangi langsung mesin ATM. Pertama, pemilik kartu menempelkan kartu SISMIC pada mesin ATM. Setelah itu, pemilik kartu memasukkan nominal *top-up* saldo kartu SISMIC. Jika transaksi berhasil, saldo

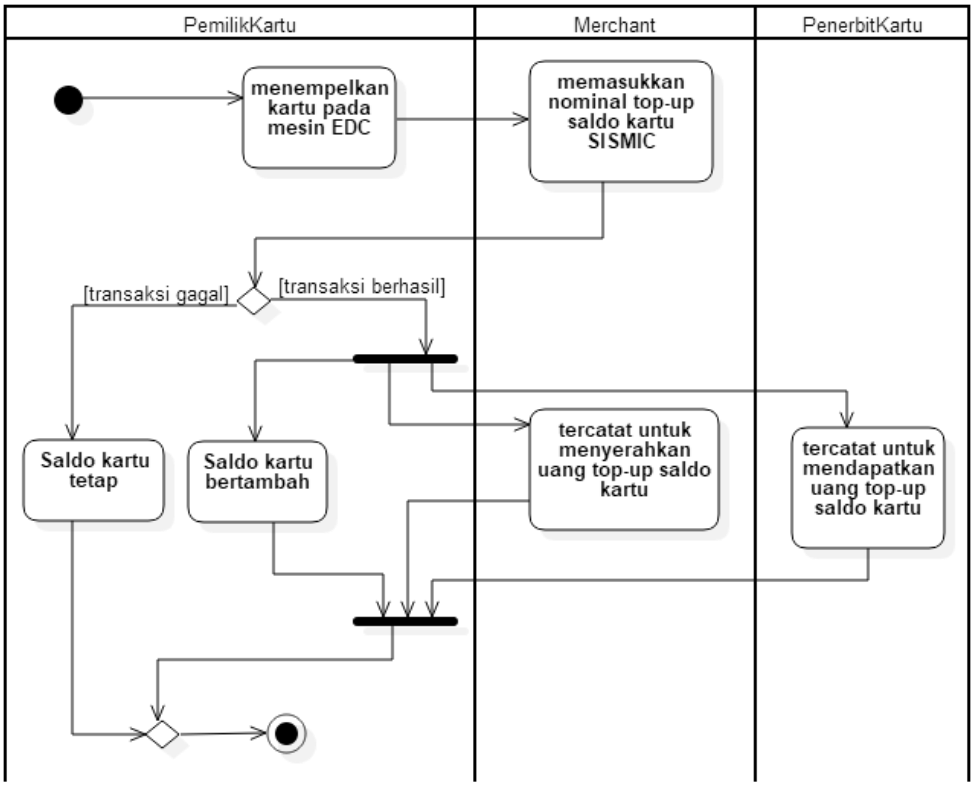
kartu SISMIC akan bertambah dan penerbit kartu akan menerima uang dari biaya *top-up* saldo pemilik kartu. Jika transaksi gagal, saldo kartu SISMIC akan tetap seperti sebelumnya. Hal yang menyebabkan transaksi *top-up* gagal adalah nominal *top-up* yang membuat kartu SISMIC memiliki jumlah saldo melebihi batas maksimal saldo dan masa berlaku kartu SISMIC sudah habis.

Setiap transaksi *top-up* melalui ATM yang terjadi akan dicatat ke riwayat transaksi *top-up*, baik yang berhasil ataupun yang gagal, pada basisdata SISMIC, kartu SISMIC, dan log di dalam mesin pembaca kartu SISMIC pada mesin ATM.

Pemilik kartu harus memiliki kartu debit diterbitkan oleh penerbit kartu dan melakukan pengisian pada mesin ATM yang dikeluarkan oleh penerbit kartu untuk melakukan transaksi *top-up* pada mesin ATM. Kartu debit dan mesin ATM yang dikeluarkan oleh bank lain selain penerbit kartu tidak dapat digunakan. Setelah transaksi *top-up* melalui mesin ATM dilakukan, saldo kartu debit milik pemilik kartu akan berkurang sesuai biaya transaksi pembelian dan uang dari pengurangan saldo tersebut akan diterima oleh penerbit kartu.

III.2.1.1.3 Melalui *Merchant*

Selain melalui *smartphone* dan ATM, transaksi *top-up* kartu SISMIC dapat dilakukan secara *offline* dengan mendatangi *merchant* yang bekerja sama dengan penerbit kartu. Masing-masing *merchant* memiliki mesin EDC yang digunakan untuk membaca kartu SISMIC. Mesin EDC pada tugas akhir ini akan disimulasikan dengan NFC *reader* dan *desktop*.



Gambar III-4 Diagram Aktivitas Transaksi *Top-Up* Melalui *Merchant*

Pada Gambar III-4 di atas, dapat dilihat bagaimana alur kerja transaksi *top-up* saldo pada SISMIC melalui *merchant*. Sedangkan untuk diagram komunikasi transaksi *top-up* saldo pada SISMIC melalui *merchant* dapat dilihat di lampiran B. Pemilik kartu mendatangi langsung *merchant* yang bekerja sama dengan penerbit kartu. Pertama, pemilik kartu menempelkan kartu SISMIC pada mesin EDC. Lalu, pemilik kartu memberitahu *merchant* nominal *top-up* saldo kartu SISMIC. Setelah itu, *merchant* akan memasukkan nominal *top-up* saldo pada mesin EDC. Jika transaksi berhasil, saldo kartu SISMIC akan bertambah. Selain itu, pada basisdata *merchant* dan penerbit kartu akan tercatat uang *top-up* saldo yang harus diserahkan *merchant* ke penerbit kartu. Jika transaksi gagal, saldo kartu SISMIC akan tetap seperti sebelumnya. Hal yang menyebabkan transaksi *top-up* gagal adalah nominal *top-up* yang membuat kartu SISMIC memiliki jumlah saldo melebihi batas maksimal saldo dan masa berlaku kartu SISMIC sudah habis.

Setiap transaksi *top-up* melalui *merchant* yang terjadi akan dicatat ke riwayat transaksi *top-up,* baik yang berhasil ataupun yang gagal, pada basisdata SISMIC, kartu SISMIC, dan log di dalam mesin pembaca kartu SISMIC pada mesin EDC.

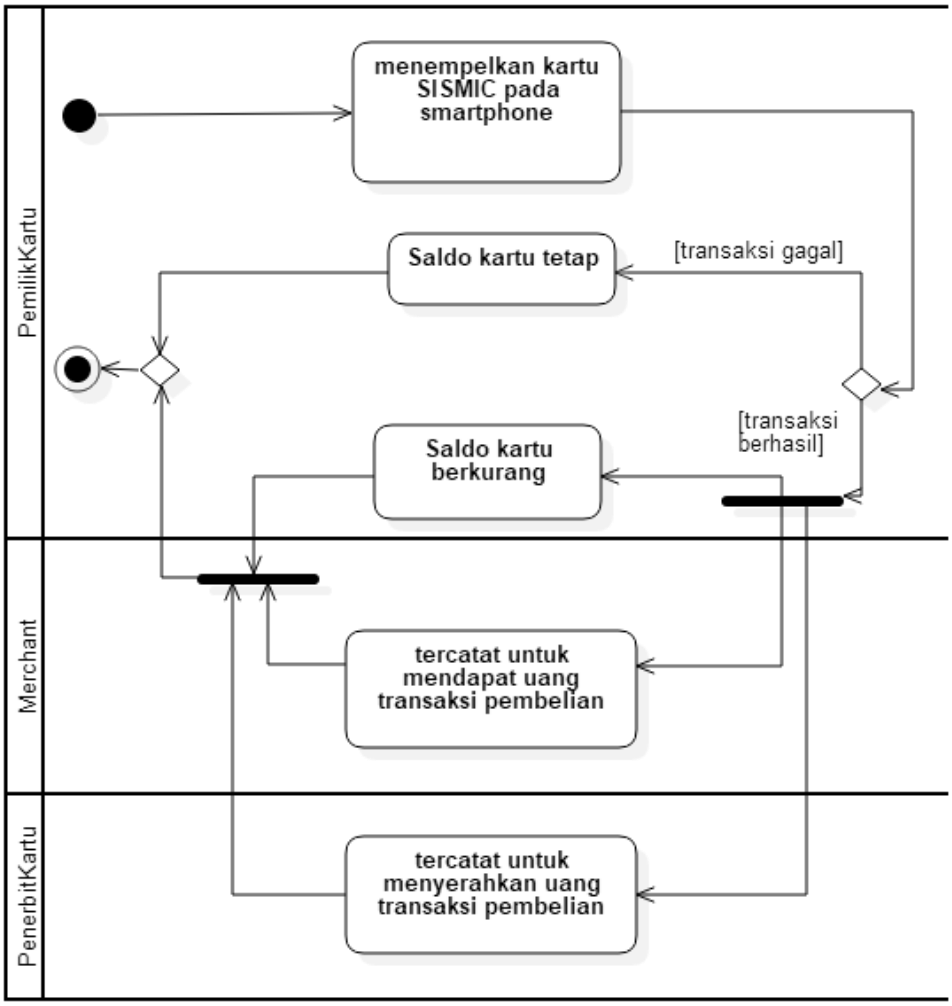
Pemilik kartu harus mendatangi *merchant* yang telah bekerja sama dengan penerbit kartu untuk melakukan transaksi *top-up* pada *mechant*. Semua *merchant* yang bekerja sama dengan penerbit kartu memiliki mesin EDC. Mesin EDC dapat digunakan untuk melakukan transaksi *top-up* atau transaksi pembelian.

III.2.1.2 Transaksi Pembelian

Sub subbab ini meliputi pembahasan tentang transaksi pembelian melalui *smartphone* tanpa parameter dan *merchant* baik tanpa parameter ataupun dengan parameter.

III.2.1.2.1 Melalui *Smartphone* Tanpa Parameter

Transaksi pembelian dalam SISMIC dapat dilakukan melalui *smartphone* secara *online* melalui *smartphone* dengan aplikasi *e-commerce* yang telah bekerja sama dengan penerbit kartu. Diagram aktivitas untuk transaksi pembelian melalui *smartphone* dapat dilihat pada Gambar III-5 berikut ini.



Gambar III-5 Diagram Aktivitas Transaksi Pembelian Melalui *Smartphone*

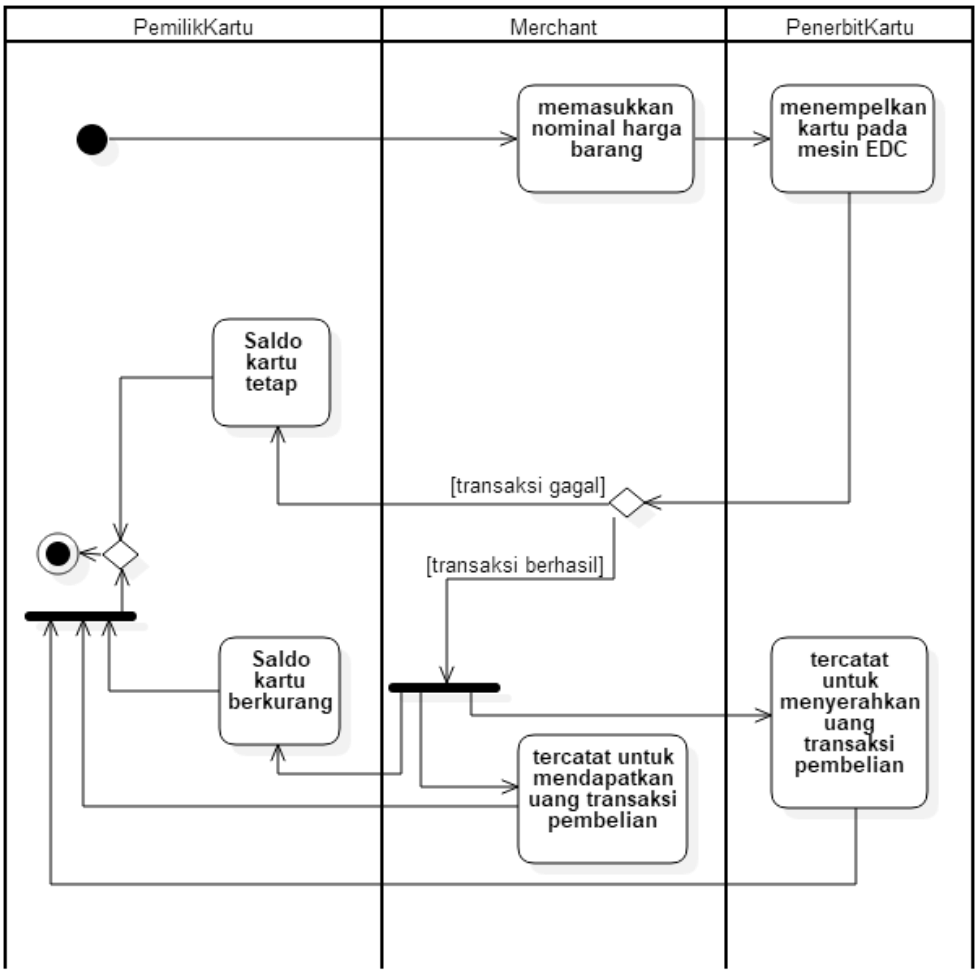
Pada Gambar III-5 di atas, dapat dilihat bagaimana alur kerja transaksi pembelian melalui *smartphone*. Sebelum masuk ke SISMIC, pemilik kartu melakukan pembelian melalui aplikasi *e-commerce* pada *smartphone* yang telah bekerja sama dengan penerbit kartu. Lalu, pemilik kartu memilih menu pembayaran melalui SISMIC. Dari tahap ini, aplikasi akan ditangani oleh SISMIC untuk melakukan pembayaran. Pemilik kartu menempelkan kartu SISMIC pada *smartphone*. Jika transaksi berhasil, saldo kartu SISMIC akan berkurang. Selain itu, *merchant* (pihak *e-commerce*) di mana pemilik kartu membeli barang akan tercatat untuk menerima uang dari biaya transaksi pembelian melalui penerbit kartu. Penerbit kartu juga tercatat untuk menyerahkan uang biaya transaksi pembelian ke *merchant*. Pencatatan tersebut disimpan di basisdata SISMIC dan *merchant*.

Merchant akan mendapat uang transaksi pembelian dalam periode tertentu sesuai dengan catatan yang tersimpan di basisdata. Jika transaksi gagal, saldo kartu SISMIC akan tetap seperti sebelumnya. Setelah itu, aplikasi akan kembali ke aplikasi *e-commerce*. Hal yang menyebabkan transaksi pembelian gagal adalah saldo kartu yang tidak mencukupi nominal transaksi pembelian dan masa berlaku kartu SISMIC sudah habis.

Setiap transaksi pembelian melalui *smartphone* yang terjadi akan dicatat ke riwayat transaksi pembelian, baik yang berhasil ataupun yang gagal, pada basisdata SISMIC, kartu SISMIC, dan basisdata *merchant*.

III.2.1.2.2 Melalui *Merchant* Tanpa Parameter

Selain melalui *smartphone*, transaksi pembelian dapat dilakukan dengan mengunjungi *merchant* yang telah bekerja sama dengan penerbit kartu secara *offline*. Transaksi pembelian di *merchant* menggunakan kartu SISMIC yang dibaca oleh mesin EDC. Diagram aktivitas untuk transaksi pembelian melalui *merchant* tanpa parameter dapat dilihat pada gambar Gambar III-6 berikut ini. Transaksi pembelian melalui mesin EDC ada dua jenis, ada pembelian tanpa parameter, ada pembelian dengan parameter. Yang dimaksud dengan pembelian tanpa parameter adalah pembelian barang yang cukup hanya dengan satu kali menempelkan kartu SISMIC.



Gambar III-6 Diagram Aktivitas Transaksi Pembelian Melalui *Merchant*

Pada Gambar III-6 di atas, dapat dilihat bagaimana alur kerja transaksi pembelian di *merchant* melalui mesin EDC tanpa parameter. Sedangkan untuk diagram komunikasi transaksi pembelian di *merchant* dapat dilihat di lampiran B. Sebelum melakukan transaksi pembelian, pemilik kartu memilih barang yang akan dibeli di *merchant*. Setelah itu, pemilik kartu menghampiri penjaga *merchant* untuk melakukan transaksi pembelian melalui mesin EDC. *Merchant* akan memasukkan nominal barang yang dibeli pemilik kartu pada mesin EDC. Lalu, pemilik kartu menempelkan kartu SISMIC pada mesin EDC. Jika transaksi berhasil, saldo kartu SISMIC akan berkurang. Selain itu, *merchant* di mana pemilik kartu membeli barang akan tercatat untuk menerima uang dari biaya transaksi pembelian melalui penerbit kartu. Penerbit kartu juga tercatat untuk menyerahkan uang biaya

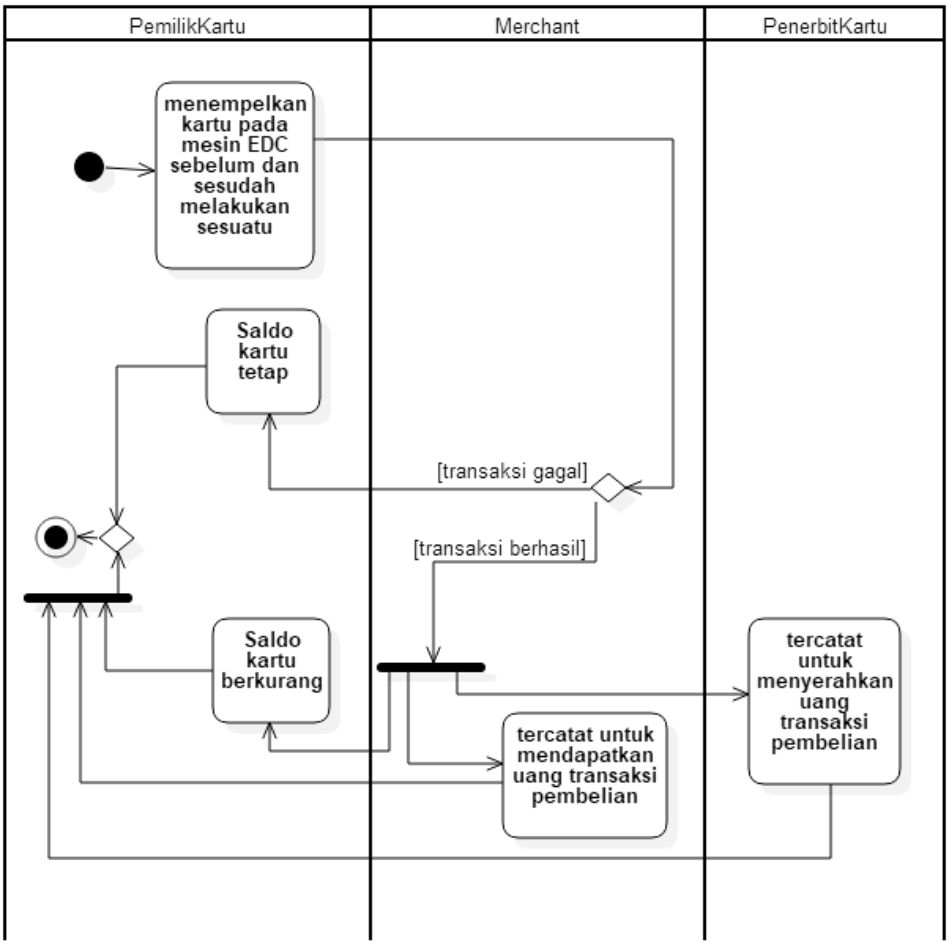
transaksi pembelian ke *merchant*. Pencatatan tersebut disimpan di log mesin pembaca kartu SISMIC di *merchant*, yaitu mesin EDC. *Merchant* akan mendapat uang transaksi pembelian dalam periode tertentu sesuai dengan catatan yang tersimpan di log mesin EDC. Jika transaksi gagal, saldo kartu SISMIC akan tetap seperti sebelumnya. Hal yang menyebabkan transaksi pembelian gagal adalah saldo kartu yang tidak mencukupi nominal transaksi pembelian dan masa berlaku kartu SISMIC sudah habis.

Setiap transaksi pembelian melalui *merchant* yang terjadi akan dicatat ke riwayat transaksi pembelian, baik yang berhasil ataupun yang gagal, pada basisdata SISMIC, kartu SISMIC, dan log di dalam mesin pembaca kartu SISMIC pada mesin EDC. Mengenai log pada mesin EDC akan dijelaskan di sub subbab ”Log *Offline* di Mesin Pembaca Kartu SISMIC”.

Merchant akan menerima uang hasil transaksi pembelian dari penerbit kartu dalam periode tertentu seperti yang sudah disebutkan sebelumnya. Penerbit kartu akan memberikan uang tersebut ke *merchant* dengan mengirimkan uang tersebut melalui kartu debit yang dimiliki *merchant*. *Merchant* yang bekerja sama dengan penerbit kartu akan memiliki kartu debit yang diterbitkan oleh penerbit kartu untuk menerima uang dari berbagai macam transaksi pembelian dengan SISMIC.

III.2.1.2.3 Melalui *Merchant* dengan Parameter

Pada dasarnya, transaksi pembelian melalui *merchant* dengan parameter sama saja dengan transaksi pembelian melalui *merchant* tanpa parameter. Hanya saja, transaksi pembelian melalui *merchant* dengan parameter pembayarannya berdasarkan jarak ataupun waktu. Diagram aktivitas transaksi pembelian dengan parameter melalui *merchant* dapat dilihat pada Gambar III-7 berikut ini.



Gambar III-7 Diagram Aktivitas Transaksi Pembelian dengan Parameter Melalui *Merchant*

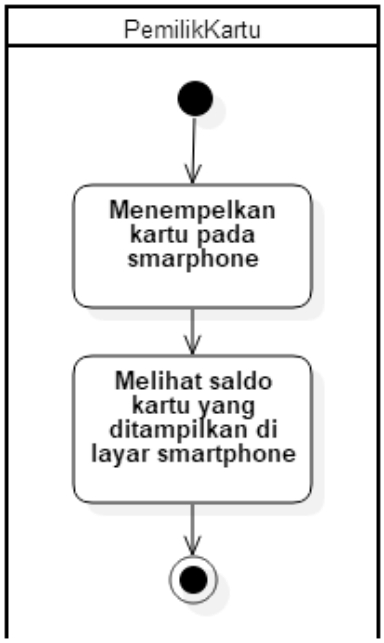
Pada gambar Gambar III-7 di atas, dapat dilihat bagaimana alur kerja transaksi pembelian di *merchant* melalui mesin EDC tanpa parameter. Pemilik kartu akan mendatangi *merchant* di mana pembayarannya dihitung berdasarkan waktu atau jarak seperti tempat bermain anak yang tarifnya dihitung per-jam, tempat bermain *ice skating* yang tarifnya dihitung per-jam, tempat olahraga yang tarifnya dihitung per-jam, transportasi seperti bus ataupun kereta. Pertama, pemilik kartu menempelkan kartu SISMIC pada mesin EDC. Setelah itu, pemilik kartu melakukan sesuatu sesuai *merchant* yang ia datangi, misal jika pemilik kartu ke tempat *ice skating*, pemilik kartu akan bermain *ice skating*. Setelah selesai, pemilik kartu akan menempelkan kartu SISMIC pada mesin EDC lagi. Apa yang

terjadi selanjutnya sama dengan transaksi pembelian dengan parameter melalui *merchant*.

III.2.1.3 Lihat Saldo

Sub subbab ini meliputi pembahasan tentang bagaimana proses melihat saldo melalui *smartphone* dan melalui ATM.

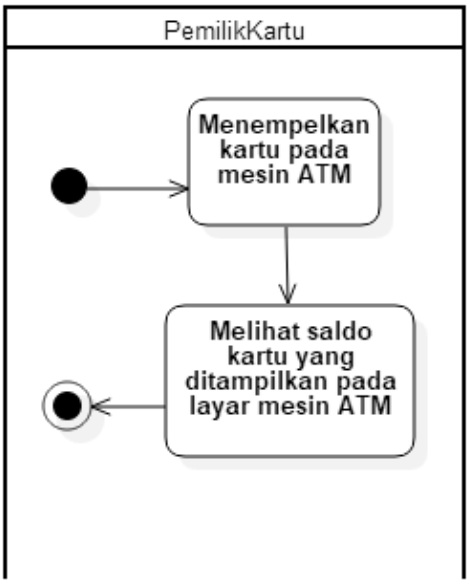
III.2.1.3.1 Melalui *Smartphone*



Gambar III-8 Diagram Aktivitas Lihat Saldo SISMIC Melalui *Smartphone*

Pada Gambar III-8 di atas, dapat dilihat bagaimana alur kerja pemilik kartu melihat saldo kartu SISMIC melalui aplikasi SISMIC pada *smartphone*. Pertama, pemilik kartu menempelkan kartu pada *smartphone*. Setelah itu, saldo kartu SISMIC akan ditampilkan di layar *smartphone*. Diagram komunikasi untuk proses melihat saldo kartu SISMIC dapat dilihat pada lampiran B.

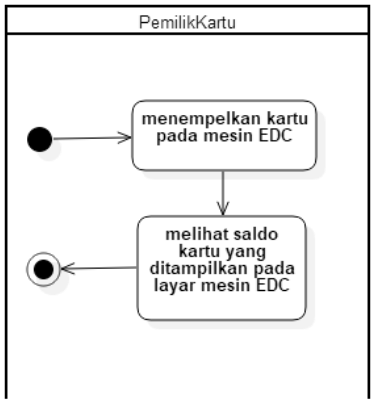
III.2.1.3.2 Melalui ATM



Gambar III-9 Diagram Aktivitas Lihat Saldo SISMIC Melalui ATM

Selain melalui *smartphone*, saldo kartu dapat dilihat secara *offline* melalui ATM. Sedangkan untuk diagram komunikasi lihat saldo SISMIC melalui mesin ATM dapat dilihat di lampiran B. Pada Gambar III-9 di atas, dapat dilihat bagaimana alur kerja pemilik kartu melihat saldo kartu SISMIC melalui mesin ATM. Pertama, pemilik kartu menempelkan kartu pada mesin ATM. Setelah itu, pemilik kartu memilih menu untuk melihat saldo kartu SISMIC pada mesin ATM. Terakhir, saldo kartu SISMIC akan ditampilkan di layar mesin ATM.

III.2.1.3.3 Melalui *Merchant*



Gambar III-10 Diagram Aktivitas Lihat Saldo SISMIC Melalui *Merchant*

Selain melalui *smartphone* dan ATM, saldo kartu dapat dilihat secara *offline* melalui *merchant* menggunakan mesin EDC. Sedangkan untuk diagram komunikasi lihat saldo SISMIC melalui *merchant* dapat dilihat di lampiran B. Pada Gambar III-10 di atas, dapat dilihat bagaimana alur kerja pemilik kartu melihat saldo kartu SISMIC melalui *merchant*. Pertama, pemilik kartu meminta *merchant* untuk melihat saldo kartu SISMIC milik pemilik kartu. Lalu, pemilik kartu akan menempelkan kartu pada mesin EDC. Setelah itu, *merchant* akan memilih menu ”Lihat Saldo dan Masa Berlaku“ pada mesin EDC. Terakhir, saldo dan masa berlaku kartu SISMIC akan ditampilkan pada layar mesin EDC.

III.2.1.4 Lihat Riwayat Transaksi

Gambar III-11 Diagram Aktivitas Lihat Riwayat Transaksi

Pada Gambar III-11 di atas, dapat dilihat bagaimana alur kerja pemilik kartu melihat riwayat transaksi SISMIC. Melihat riwayat transaksi SISMIC dilakukan melalui aplikasi SISMIC pada *smartphone*. Pertama, pemilik kartu menempelkan kartu pada *smartphone*. Setelah itu, riwayat transaksi SISMIC akan ditampilkan di layar *smartphone*, baik transaksi yang berhasil ataupun yang gagal.

III.2.1.5 Lihat Masa Berlaku Kartu SISMIC

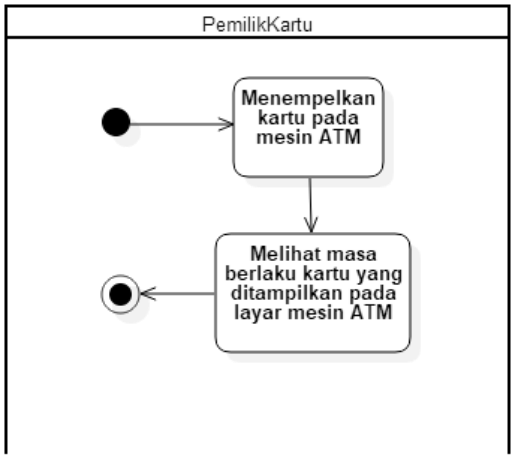
Sub subbab ini meliputi pembahasan tentang bagaimana proses melihat masa berlaku kartu SISMIC melalui *smartphone* dan ATM.

III.2.1.5.1 Melalui *Smartphone*

Gambar III-12 Diagram Aktivitas Lihat Masa Berlaku Kartu SISMIC Melalui *Smartphone*

Pada Gambar III-12 di atas, dapat dilihat bagaimana alur kerja pemilik kartu melihat masa berlaku kartu SISMIC melalui aplikasi SISMIC pada *smartphone*. Pertama, pemilik kartu menempelkan kartu pada *smartphone*. Setelah itu, masa berlaku kartu SISMIC akan ditampilkan di layar *smartphone*.

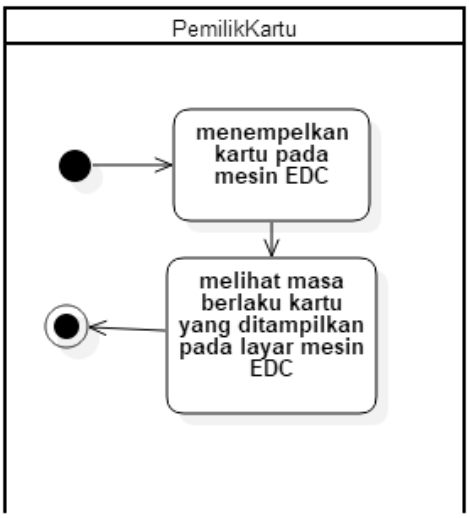
III.2.1.5.2 Melalui ATM



Gambar III-13 Diagram Aktivitas Lihat Masa Berlaku SISMIC Melalui ATM

Selain melalui *smartphone*, masa berlaku kartu dapat dilihat secara *offline* melalui ATM. Pada Gambar III-13 di atas, dapat dilihat bagaimana alur kerja pemilik kartu melihat masa berlaku kartu SISMIC melalui mesin ATM. Sedangkan untuk diagram komunikasi lihat masa berlaku SISMIC melalui mesin ATM dapat dilihat di lampiran B. Pertama, pemilik kartu menempelkan kartu pada mesin ATM. Setelah itu, pemilik kartu memilih menu untuk melihat masa berlaku kartu SISMIC pada mesin ATM. Terakhir, masa berlaku kartu SISMIC akan ditampilkan di layar mesin ATM.

III.2.1.5.3 Melalui *Merchant*



Gambar III-14 Diagram Aktivitas Lihat Masa Berlaku Kartu SISMIC Melalui *Merchant*

Selain melalui *smartphone* dan ATM, masa berlaku kartu dapat dilihat secara *offline* melalui *merchant* menggunakan mesin EDC. Pada Gambar III-14 di atas, dapat dilihat bagaimana alur kerja pemilik kartu melihat masa berlaku kartu SISMIC melalui *merchant*. Sedangkan untuk diagram komunikasi lihat masa berlaku SISMIC melalui *merchant* dapat dilihat di lampiran B. Pertama, pemilik kartu meminta *merchant* untuk melihat masa berlaku kartu SISMIC milik pemilik kartu. Lalu, pemilik kartu akan menempelkan kartu pada mesin EDC. Setelah itu, *merchant* akan memilih menu ”Lihat Saldo dan Masa Berlaku“ pada mesin EDC. Terakhir, saldo dan masa berlaku kartu SISMIC akan ditampilkan pada layar mesin EDC.

III.2.2 Penyimpanan dan Struktur Data SISMIC

Subbab ini meliputi pembahasan tentang bagaimana struktur penyimpanan dan hak akses kartu SISMIC, basisdata, dan diagram kelas pada SISMIC.

III.2.2.1 Struktur Penyimpanan dan Hak Akses Kartu SISMIC

Kartu SISMIC memiliki teknologi NFC dan memori berukuran 1 KB dengan 16 sektor, di mana 1 sektornya terdiri dari 4 blok dengan ukuran 16 *bytes* per blok.

Saat pertama kali kartu diterbitkan, beberapa sektor kartu SISMIC akan dikonfigurasi seperti pada Tabel III-1 berikut ini.

Tabel III-1 Konfigurasi Sektor dan Blok Kartu SISMIC

Sektor	Blok	Jenis Blok	Data
0	0	-	Nomor kartu dari manufaktur
	1	*Reader/writer block*	Tanggal masa berlaku kartu
	2	*Value block*	Saldo Kartu
1-5	0	*Reader/writer block*	Riwayat waktu transaksi pembelian atau *top-up* dalam bentuk epoch
	1	*Value block*	Riwayat nominal transaksi pembelian atau *top-up*
	2	*Reader/writer block*	Riwayat jenis transaksi apakah transaki merupakan transaksi pembelian atau *top-up*
6-14	0	*Reader/writer block*	Parameter jarak atau waktu pertama kartu disentuh pada *reader*
	1	*Reader/writer block*	Iv hasil dari enkripsi blok ke-0 di sektor 6 sampai 14
	2	-	-
15	0	-	-
	1	*Reader/writer block*	Iv hasil dari enkripsi blok ke-1 di sektor 0

Sektor	Blok	Jenis Blok	Data
	2	*Reader/writer block*	Iv hasil dari enkripsi blok ke-2 di sektor 0

Penjelasan lebih lengkap mengenai Tabel III-1 pada uraian berikut ini:

1. Sektor ke-0 blok ke-1 yang berupa *reader/writer block* menyimpan tanggal masa berlaku kartu. Blok ini pada awalnya ditentukan dan ditulis oleh penerbit kartu. Lalu, blok ini dapat dibaca oleh pemilik kartu dan tidak dapat ditulis ulang oleh siapapun kecuali ada wewenang dari penerbit kartu. Data yang tersimpan di blok ini dienkripsi menggunakan algoritma AES.
2. Sektor ke-0 blok ke-2 yang berupa *value block* menyimpan saldo kartu. Blok ini dapat ditulis ketika kartu digunakan untuk transaksi pembelian atau *top-up* oleh pemilik kartu pada *smartphone*, mesin EDC, atau mesin ATM yang telah dipastikan keamanannya. Selain itu, blok ini dapat dibaca oleh pemilik kartu. Nominal saldo pada blok ini dibatasi, tergantung dari kebijakan penerbit kartu. Data yang tersimpan di blok ini dienkripsi menggunakan algoritma AES.
3. Sektor ke-1 sampai sektor ke-5 akan menyimpan 5 transaksi pembelian atau *top-up* terakhir dengan konfigurasi blok berikut ini:
    a. Blok ke-0 yang berupa *reader/writer block* menyimpan waktu transaksi pembelian atau *top-up* dalam bentuk epoch
    b. Blok ke-1 yang berupa *value block* menyimpan nominal transaksi pembelian atau *top-up*. Transaksi pembelian tidak dapat dilakukan jika saldo *kartu* lebih kecil dari nominal transaksi pembelian.
    c. Blok ke-2 yang berupa *reader/writer block* menyimpan jenis transaksi apakah transaksi pembelian atau *top-up*
4. Sektor ke-6 sampai sektor ke-14 blok ke-0 digunakan untuk menangani kasus di mana transaksi pembelian membutuhkan parameter seperti waktu dan jarak. Masing-masing *merchant* menempati satu sektor. Jumlah

maksimal *merchant* yang bekerja sama dengan penerbit kartu adalah 10 *merchant.* Lebih dari itu, penerbit kartu harus mengganti kartu Mifare Classic 1KB dengan kapasitas yang lebih besar. Contoh parameter jarak adalah pembayaran yang dihitung berdasarkan jarak seperti ketika kartu SISMIC digunakan sebagai tiket transportasi untuk pembayaran tol, tiket bus, ataupun tiket kereta. Contoh parameter waktu adalah pembayaran yang dihitung berdasarkan waktu seperti ketika kartu SISMIC digunakan untuk pembayaran tempat bermain anak ataupun *ice skating* yang dihitung per-jam. Perhitungan nominal pembayaran akan ditangani oleh aplikasi *merchant*. Data yang tersimpan di blok ini dienkripsi menggunakan algoritma AES. Sektor ke-6 sampai sektor ke-14 blok ke-1 menyimpan iv yang digunakan untuk mendekripsi blok ke-0 menggunakan algoritma AES.

5. Sektor ke-15 blok ke-1 menyimpan iv yang digunakan untuk mendekripsi sektor ke-0 blok ke-1 menggunakan algoritma AES.
6. Sektor ke-15 blok ke-2 menyimpan iv yang digunakan untuk mendekripsi sektor ke-0 blok ke-2 menggunakan algoritma AES.

Pada tabel Tabel III-2 berikut, dapat dilihat bagaimana hak akses dari masing-masing blok pada kartu SISMIC. Pengaturan hak akses pada kartu SISMIC akan disimpan pada *Secure Access Module* (SAM). Pihak *merchant* akan diberikan *key* kartu SISMIC sesuai dengan hak aksesnya.

Tabel III-2 Hak Akses Kartu SISMIC

Sektor	Blok	Data	Hak Akses			
			Pemilik Kartu	Penerbit Kartu	Merchant	Payment Gateway
0	0	Nomor kartu dari manufaktur	Baca	Baca	-	-

Sektor	Blok	Data	Hak Akses			
			Pemilik Kartu	Penerbit Kartu	Merchant	Payment Gateway
	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	-

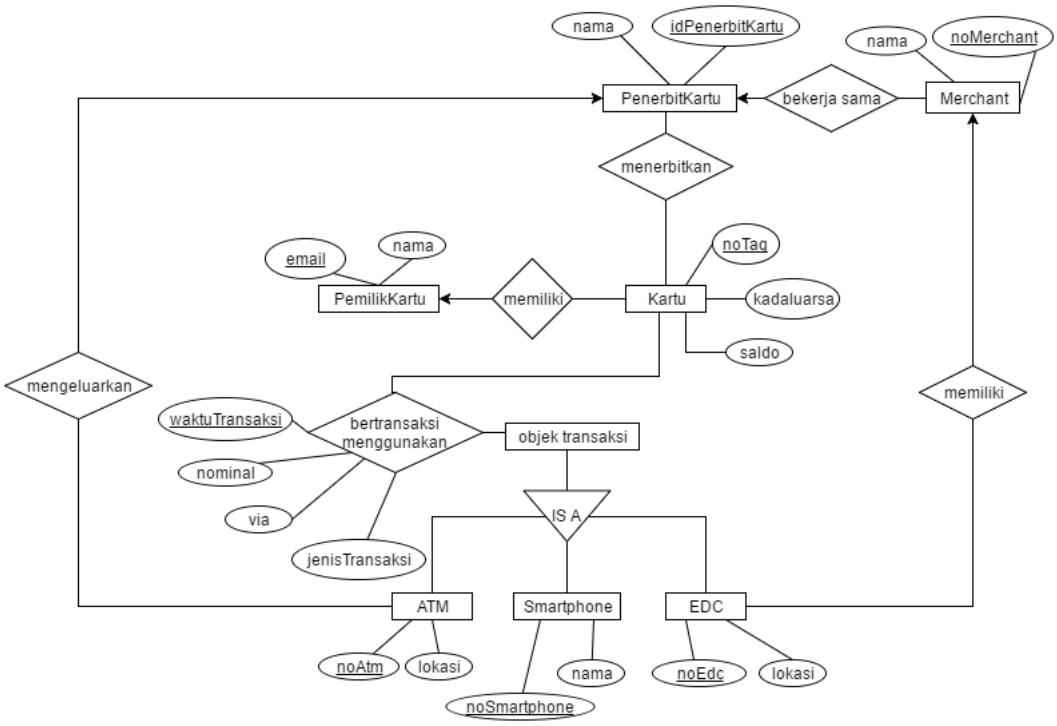
Sektor	Blok	Data	Hak Akses			
			Pemilik Kartu	Penerbit Kartu	Merchant	Payment Gateway
	1	Iv hasil dari enkripsi blok ke-0 di sektor 6 sampai 14	-	-	-	-
	2	-	-	-	-	-
15	1	Iv hasil dari enkripsi blok ke-1 di sektor 0	-	-	-	-
	2	Iv hasil dari enkripsi blok ke-2 di sektor 0	-	-	-	-

Blok-blok ini dapat dilihat oleh pemilik kartu dan ditulis menggunakan algoritma *round-robin* ketika kartu digunakan untuk transaksi pembelian atau *top-up*. Algoritma *round-robin* yang dimaksud adalah di mana transaksi pembelian atau *top-up* yang paling lama disimpan akan ditimpa dengan yang paling baru sampai memenuhi kapasitas penyimpanan riwayat transaksi, yaitu lima buah. *Payment gateway* tidak memiliki hak akses apapun ke kartu SISMIC.

III.2.2.2 Basisdata

Sub subbab ini meliputi pembahasan tentang basisdata pada server SISMIC, *merchant*, dan *payment gateway*.

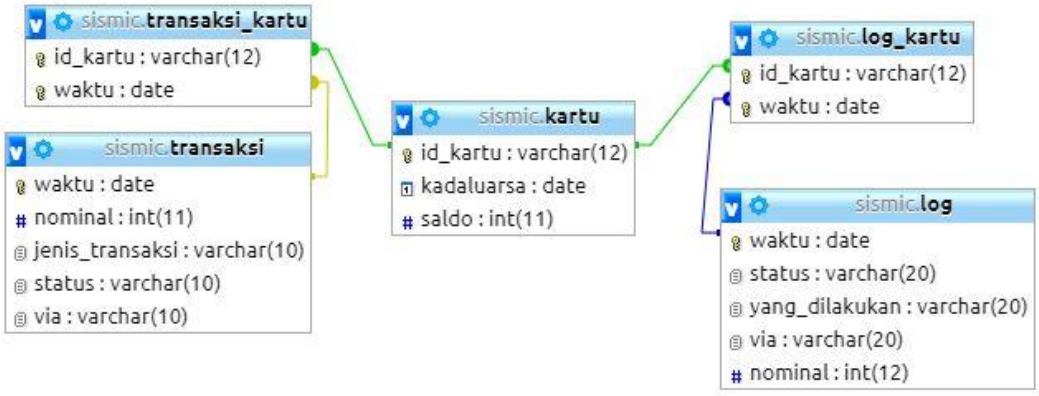
III.2.2.2.1 Model Data SISMIC



Gambar III-15 Diagram *Entity-Relationship* SISMIC

SISMIC memiliki tempat penyimpanan untuk menyimpan data. Penyimpanan data SISMIC disimpan pada basisdata dan kartu SISMIC yang berupa *tag* NFC. Basisdata SISMIC dan kartu SISMIC akan saling bersinkronisasi ketika kartu NFC ditempelkan pada *smartphone* dan mesin EDC. Diagram *Entity-Relationship* (Diagram ER) untuk basisdata SISMIC dapat dilihat pada Gambar III-15 di atas. Ada tujuh entitas yang terlibat di basisdata SISMIC, yaitu Kartu, PenerbitKartu, Merchant, serta objek transaksi yang terdiri dari ATM, Smartphone, dan EDC. Karena kartu tidak ada kepemilikan, entitas pemilik kartu tidak akan dilibatkan pada level basisdata berikutnya. Basisdata yang akan digunakan di SISMIC ada tiga, yaitu basisdata SISMIC, basisdata *merchant*, dan basisdata *payment gateway*.

III.2.2.2.2 Basisdata SISMIC

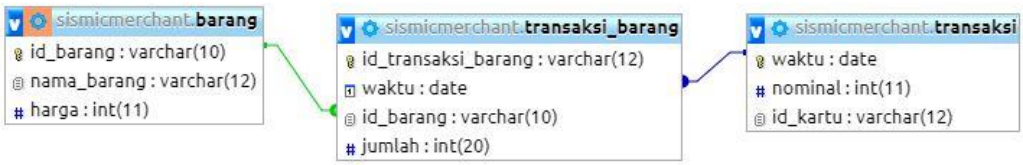


Gambar III-16 Basisdata SISMIC

Skema basisdata relasional untuk basisdata SISMIC dapat dilihat pada Gambar III-16 di atas. Basisdata SISMIC digunakan untuk menyimpan segala riwayat transaksi yang terjadi pada SISMIC. Riwayat transaksi yang disimpan seperti waktu transaksi, nominal transaksi, jenis transaksi apakah transaksi yang dilakukan transaksi pembelian atau *top-up*, status transaksi apakah transaksi yang dilakukan gagal atau berhasil, dan melalui apa transaksi dilakukan, apakah ATM, *merchant*, atau *smartphone*. Selain itu, basisdata SISMIC juga menyimpan informasi kartu yang digunakan untuk transaksi seperti ID kartu, masa berlaku kartu, dan saldo kartu. Basisdata SISMIC dapat dilihat secara lengkap oleh penerbit kartu.

Selain itu, basisdata SISMIC juga mencatat log apa saja yang dilakukan oleh pemilik kartu (lihat saldo, lihat masa berlaku, melakukan transaksi pembelian, dan melakukan transaksi *top-up*), kapan hal tersebut dilakukan, melalui apa transaksi dilakukan, nominal transaksi, dan apakah transaksi berhasil atau gagal.

III.2.2.2.3 Basisdata *Merchant*



Gambar III-17 Basisdata *Merchant*

Skema basisdata relasional untuk basisdata SISMIC dapat dilihat pada Gambar III-17 di atas. Basisdata *merchant* yang dibuat pada tugas akhir ini hanyalah yang berpengaruh pada SISMIC saja, bukan basisdata *merchant* keseluruhan. Basisdata *merchant* digunakan untuk menyimpan segala riwayat transaksi pemilik kartu yang terjadi pada *merchant*. Riwayat transaksi yang disimpan adalah ID kartu yang melakukan transaksi, waktu transaksi, nominal transaksi, dan barang apa saja yang dibeli oleh pemilik kartu. Selain riwayat transaksi, basisdata *merchant* juga menyimpan harga barang beserta ID barang yang dijual di *merchat*. Basisdata *merchant* dapat dilihat secara lengkap oleh *merchant*.

III.2.2.2.4 Basisdata *Payment Gateway*

Gambar III-18 Basisdata *Payment Gateway*

Skema basisdata relasional untuk basisdata *payment gateway* dapat dilihat pada Gambar III-18 di atas. Basisdata *payment gateway* yang dibuat pada tugas akhir ini hanyalah yang berpengaruh pada SISMIC saja, bukan basisdata *payment gateway* keseluruhan. Basisdata *payment gateway* digunakan untuk menyimpan segala riwayat transaksi pembayaran yang harus ditangani *payment gateway*. Riwayat transaksi yang disimpan adalah waktu transaksi, nomor kartu kredit yang melakukan transaksi, nominal transaksi, dari bank apa kartu kredit milik pemilik kartu yang digunakan untuk *top-up*, dan ke bank mana transaksi *top-up* dilakukan

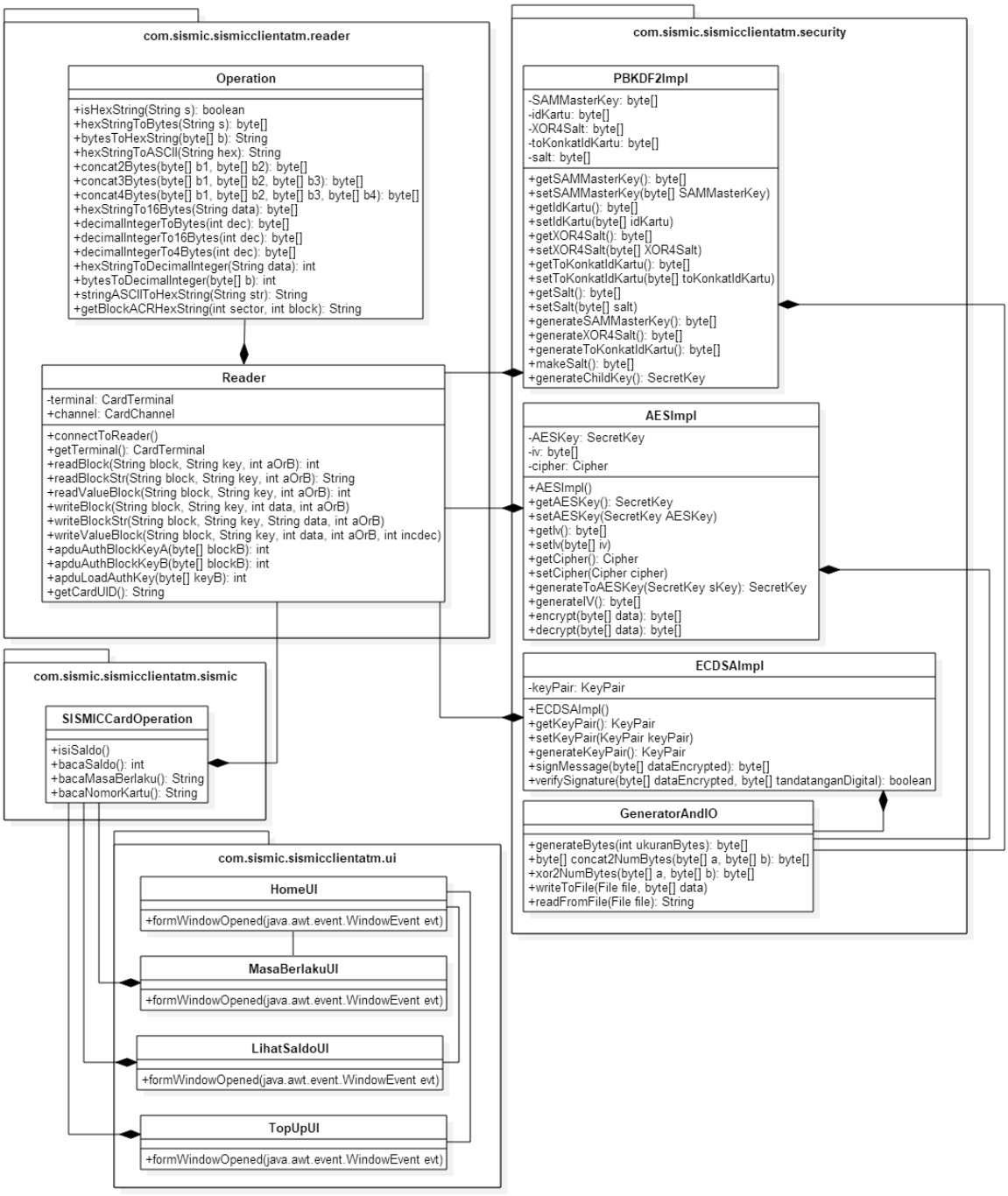
atau bisa disebut juga bank penerbit kartu. Basisdata *merchant* dapat dilihat secara lengkap oleh *payment gateway*.

III.2.2.3 Diagram Kelas

Sub subbab ini meliputi pembahasan tentang diagram kelas yang digunakan untuk aplikasi ATM, aplikasi EDC, aplikasi *Smartphone*, *web service* SISMIC, *web service payment gateway*, dan *web service merchant*.

III.2.2.3.1 Diagram Kelas untuk ATM

Diagram kelas pada Gambar III-19 di bawah adalah diagram kelas yang digunakan untuk aplikasi ATM. Aplikasi ATM ini akan terhubung ke *web service* SISMIC. Diagram kelas ATM memiliki empat *package*, yaitu *package* com.sismic.sismicclientatm.reader, com.sismic.sismicclientatm.security, com.sismic.sismicclientatm.sismic, dan com.sismic.sismicclientatm.ui.



Gambar III-19 Diagram Kelas ATM

Package com.sismic.sismicclientatm.reader berisi dua kelas, yaitu kelas Reader dan Operation. *Package* ini berhubungan dengan mesin pembaca kartu SISMIC. Kelas Reader memiliki *methods* untuk membuat koneksi dengan mesin pembaca kartu, membaca kartu, dan menulis kartu SISMIC. Kelas Operation memiliki

methods yang diperlukan untuk operasi-operasi di kelas Reader seperti mengubah bilangan hexa menjadi bytes, menggabungkan dua sampai empat bilangan bytes, dan operasi-operasi lain yang berhubungan dengan bilangan hexa.

Package com.sismic.sismicclientatm.security berisi empat kelas, yaitu kelas PBKDF2Impl, AESImpl, ECDSAImpl, GeneratorAndIO. Kelas PBKDF2Impl memiliki *methods* untuk membuat kunci SAM, membuat salt, dan membuat kunci turunan yang akan digunakan untuk mengenkripsi kartu SISMIC. Kelas AESImpl memiliki *methods* untuk membuat kunci AES dari kunci turunan, membuat IV, mengenkripsi data, dan menkripsi data. Kelas ECDSAImpl memiliki *methods* untuk membuat kunci publik dan kunci privat, memberi *digital signature* pada data, dan memverifikasi *digital signature*. Kelas GeneratorAndIO memiliki *methods* yang dibutuhkan kelas PBKDF2Impl, AESImpl, dan ECDSAImpl untuk membuat bilangan random, menggabungkan dua bilangan, melakukan operasi XOR, menulis ke *file* txt,dan membaca *file* txt.

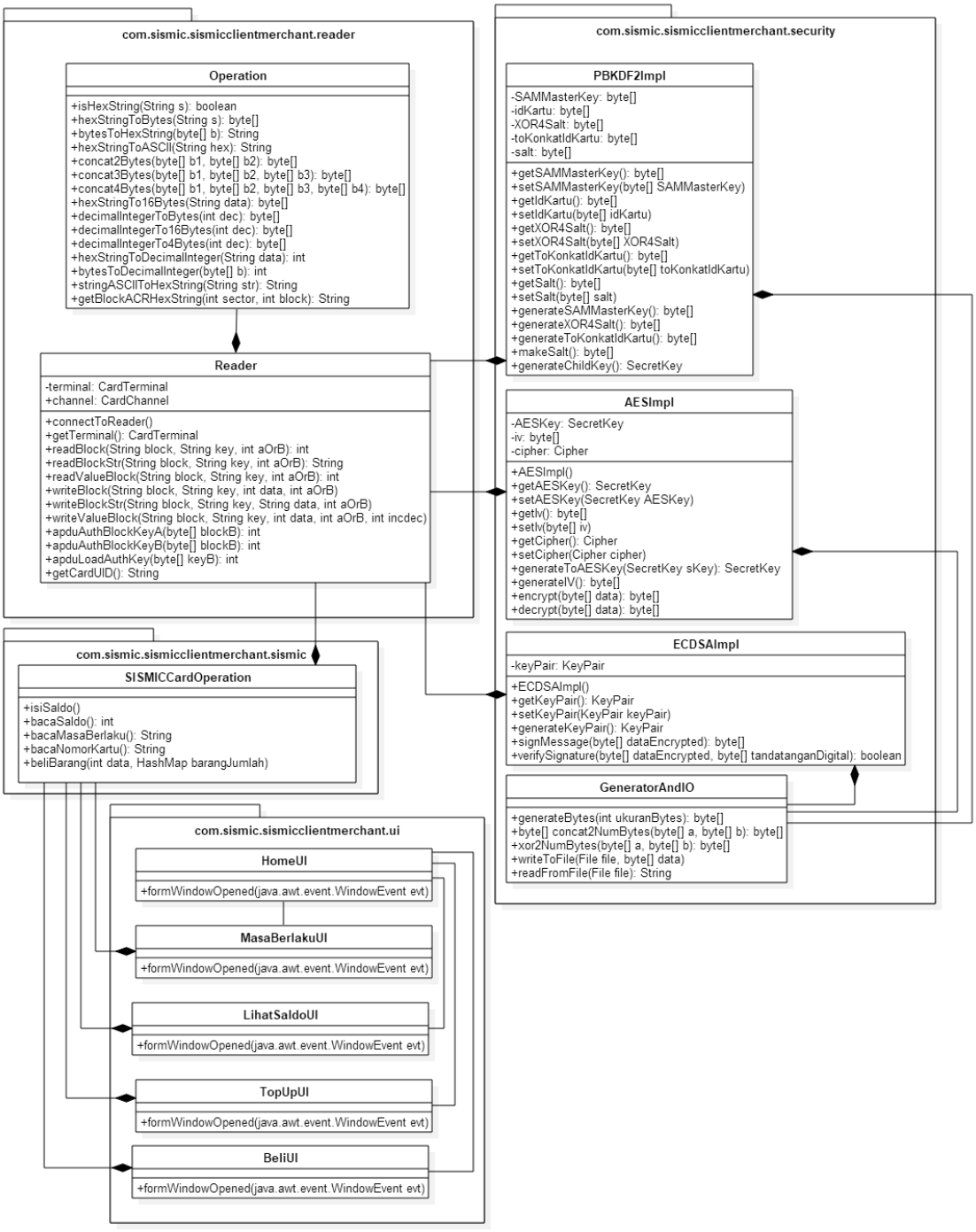
Package com.sismic.sismicclientatm.sismic berisi satu kelas saja, yaitu kelas SISMICCardOperation. Kelas ini memiliki *methods* untuk mengisi saldo kartu, melihat saldo kartu, melihat masa berlaku kartu, dan membaca nomor kartu SISMIC.

Package com.sismic.sismicclientatm.ui berisi empat kelas, yaitu kelas HomeUI, MasaBerlakuUI, LihatSaldoUI, dan TopUpUI. Kelas-kelas ini digunakan untuk menampilkan tampilan aplikasi ATM. Kelas HomeUI menampilkan tampilan menu utama dari aplikasi ATM, kelas MasaBerlaku menampilkan tampilan untuk melihat masa berlaku kartu SISMIC, kelas LihatSaldoUI menampilkan tampilan untuk melihat saldo kartu SISMIC, dan kelas TopUpUI menampilkan tampilan untuk melakukan transaksi *top-up* saldo kartu SISMIC.

III.2.2.3.2 Diagram Kelas *Merchant*

Diagram kelas pada Gambar III-20 di bawah adalah diagram kelas yang digunakan untuk aplikasi *merchant*. Aplikasi *merchant* ini akan terhubung ke *web service* SISMIC dan *web service merchant*. Diagram kelas *Merchant* memiliki

empat *package*, yaitu *package* com.sismic.sismicclientmerchant.reader, com.sismic.sismicclientmerchant.security, com.sismic.sismicclientmerchant.sismic, dan com.sismic.sismicclientmerchant.ui.



Gambar III-20 Diagram Kelas *Merchant*

Package com.sismic.sismicclientmerchant.reader berisi dua kelas, yaitu kelas Reader dan Operation. *Package* ini berhubungan dengan mesin pembaca kartu SISMIC. Kelas Reader memiliki *methods* untuk membuat koneksi dengan mesin pembaca kartu, membaca kartu, dan menulis kartu SISMIC. Kelas Operation memiliki *methods* yang diperlukan untuk operasi-operasi di kelas Reader seperti mengubah bilangan hexa menjadi bytes, menggabungkan dua sampai empat bilangan bytes, dan operasi-operasi lain yang berhubungan dengan bilangan hexa.

Package com.sismic.sismicclientmerchant.security berisi empat kelas, yaitu kelas PBKDF2Impl, AESImpl, ECDSAImpl, GeneratorAndIO. Kelas PBKDF2Impl memiliki *methods* untuk membuat kunci SAM, membuat salt, dan membuat kunci turunan yang akan digunakan untuk mengenkripsi kartu SISMIC. Kelas AESImpl memiliki *methods* untuk membuat kunci AES dari kunci turunan, membuat IV, mengenkripsi data, dan menkripsi data. Kelas ECDSAImpl memiliki *methods* untuk membuat kunci publik dan kunci privat, memberi *digital signature* pada data, dan memverifikasi *digital signature*. Kelas GeneratorAndIO memiliki *methods* yang dibutuhkan kelas PBKDF2Impl, AESImpl, dan ECDSAImpl untuk membuat bilangan random, menggabungkan dua bilangan, melakukan operasi XOR, menulis ke *file* txt,dan membaca *file* txt.

Package com.sismic.sismicclientmerchant.sismic berisi satu kelas saja, yaitu kelas SISMICCardOperation. Kelas ini memiliki *methods* untuk mengisi saldo kartu, melihat saldo kartu, melihat masa berlaku kartu, melakukan transaksi pembelian, dan membaca nomor kartu SISMIC.

Package com.sismic.sismicclientmerchant.ui berisi empat kelas, yaitu kelas HomeUI, MasaBerlakuUI, LihatSaldoUI, BeliUI, dan TopUpUI. Kelas-kelas ini digunakan untuk menampilkan tampilan aplikasi ATM. Kelas HomeUI menampilkan tampilan menu utama dari aplikasi ATM, kelas MasaBerlaku menampilkan tampilan untuk melihat masa berlaku kartu SISMIC, kelas LihatSaldoUI menampilkan tampilan untuk melihat saldo kartu SISMIC, kelas BeliUI menampilkan tampilan untuk melakukan transaksi pembelian, dan kelas

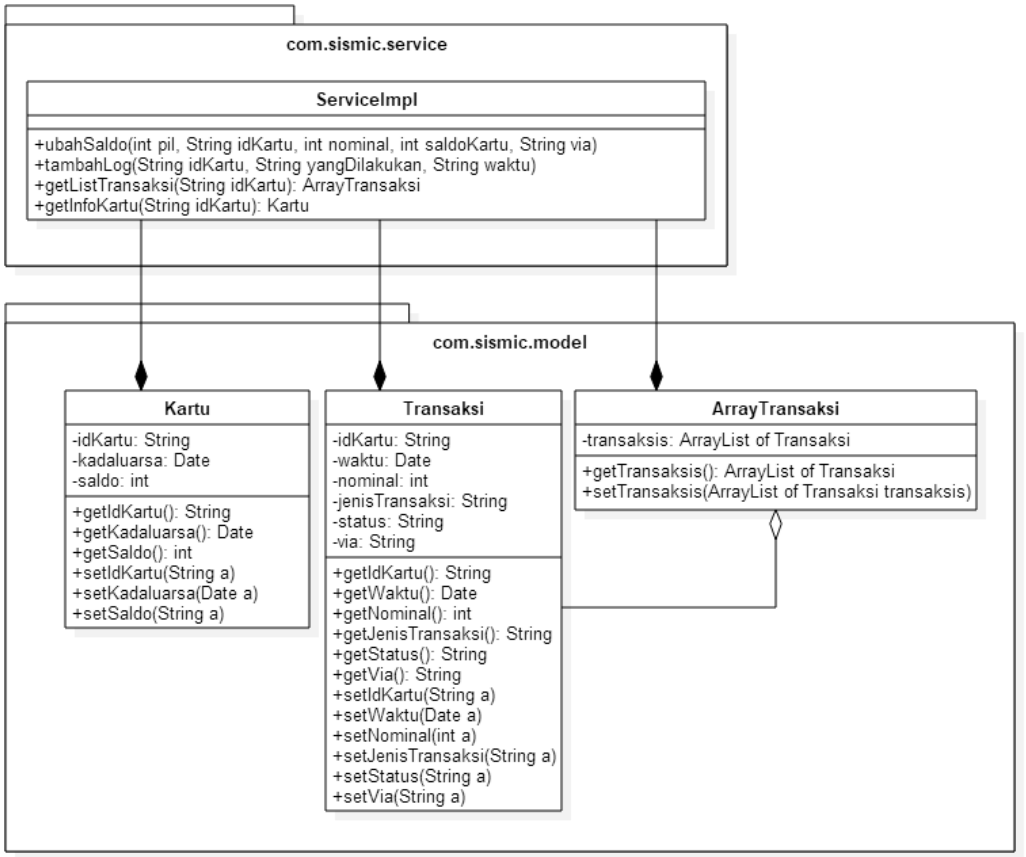
TopUpUI menampilkan tampilan untuk melakukan transaksi *top-up* saldo kartu SISMIC.

III.2.2.3.3 Diagram Kelas *Smartphone*

Aplikasi *smartphone* pada tugas akhir ini tidak diimplementasi.

III.2.2.3.4 Diagram Kelas *Web Service* SISMIC

Diagram kelas SISMIC digunakan untuk *web service* SISMIC yang terhubung ke basisdata SISMIC. Basisdata SISMIC adalah basisdata paling penting agar sistem *micropayment* bisa berjalan dan akan terhubung ke *web service SISMIC*. *Web service* SISMIC akan digunakan oleh seluruh aplikasi yang ada pada SISMIC yaitu aplikasi ATM, aplikasi *merchant*, dan aplikasi *smartphone*. *Web service* SISMIC menangani operasi-operasi yang berhubungan dengan basisdata SISMIC.



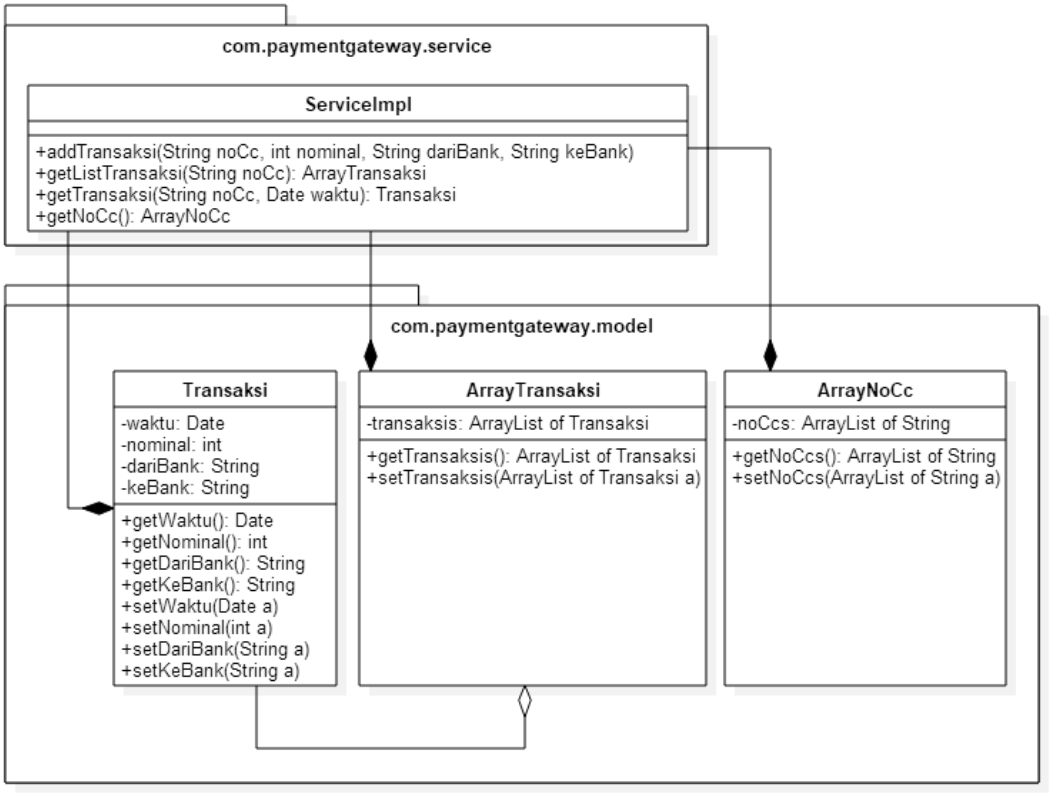
Gambar III-21 Diagram Kelas SISMIC

Bisa dilihat pada Gambar III-21 di atas, diagram kelas SISMIC memiliki dua *package*, yaitu *package* com.sismic.service dan com.sismic.model. com.sismic.service adalah *package* yang berisi *methods* yang ada di *web service.* com.sismic.service hanya memiliki satu kelas, yaitu kelas ServiceImpl yang mengimplementasi *web service*. *Methods* ini akan menulis, mengubah, atau membaca basisdata SISMIC.

Package com.sismic.model adalah *package* yang berisi kelas Kartu dan Transaksi, yaitu kelas yang memodelkan entitas di basisdata SISMIC. Selain kelas Kartu dan Transaksi, *package* com.sismic.model memiliki kelas ArrayTransaksi, yaitu kelas untuk merepresentasikan array dari kelas Transaksi.

III.2.2.3.5 Diagram Kelas *Web Service Payment Gateway*

Diagram kelas *payment gateway* digunakan untuk *web service payment gateway* yang terhubung ke basisdata *payment gateway*. *Web service payment gateway* akan digunakan oleh aplikasi *smartphone*. *Web service payment gateway* menangani operasi-operasi yang berhubungan dengan basisdata *payment gateway*.



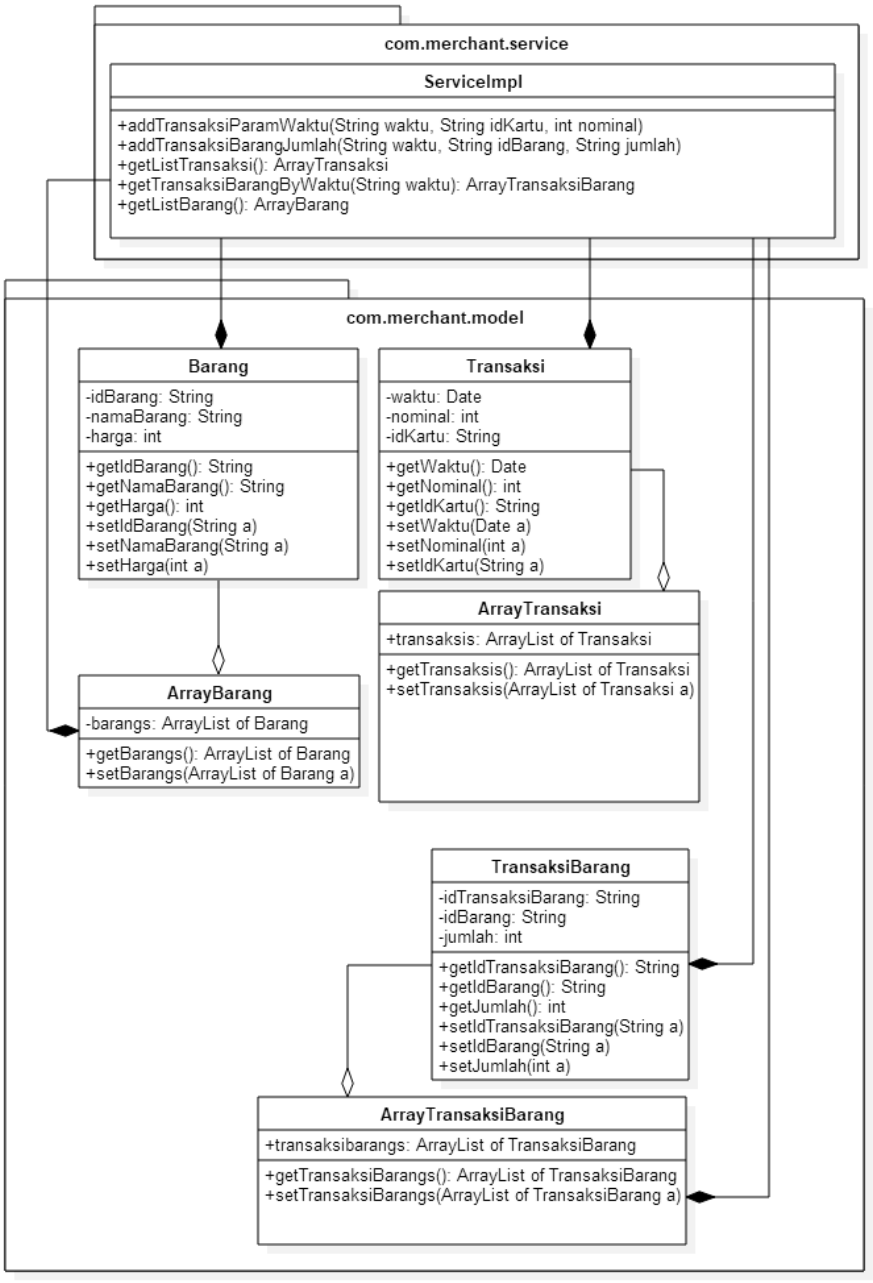
Gambar III-22 Diagram Kelas *Payment Gateway*

Bisa dilihat pada Gambar III-22 di atas, diagram kelas *Payment Gateway* memiliki dua *package*, yaitu *package* com.paymentgateway.service dan com.paymentgateway.model. com.paymentgateway.service adalah *package* yang berisi *methods* yang ada di *web service.* *Package* com.paymentgateway.service hanya memiliki satu kelas, yaitu kelas ServiceImpl yang mengimplementasi *web service*. *Methods* ini akan menulis, mengubah, atau membaca basisdata *payment gateway*.

Package com.paymentgateway.model adalah *package* yang berisi kelas Transaksi, yaitu kelas yang memodelkan entitas di basisdata *payment gateway*. Selain kelas Transaksi, *package* ini juga memiliki kelas ArrayTransaksi yang merepresentasikan array dari kelas Transaksi, dan kelas ArrayNoCc yang merepresentasikan array dari nomor kartu kredit yang berupa String.

III.2.2.3.6 Diagram Kelas *Web Service Merchant*

Diagram kelas *merchant* digunakan untuk *web service merchant* yang terhubung ke basisdata *merchant*. *Web service merchant* akan digunakan oleh aplikasi *smartphone* dan *merchant*. *Web service merchant* menangani operasi-operasi yang berhubungan dengan basisdata *merchant*.



Gambar III-23 Diagram Kelas *Merchant*

Bisa dilihat pada Gambar III-23 di atas, diagram kelas *Merchant* memiliki dua *package*, yaitu *package* com.merchant.service dan com.merchant.model. com.merchant.service adalah *package* yang berisi *methods* yang ada di *web service.* com.merchant.service hanya memiliki satu kelas, yaitu kelas ServiceImpl yang mengimplementasi *web service*. *Methods* ini akan menulis, mengubah, atau membaca basisdata *merchant*.

Package com.merchant.model adalah *package* yang berisi kelas Barang, Transaksi, dan TransaksiBarang, yaitu kelas yang memodelkan entitas di basisdata *merchant*. Selain itu, *package* ini juga memiliki kelas ArrayBarang yang merepresentasikan array dari kelas Barang, ArrayTransaksi yang merepresentasikan array dari kelas Transaksi, dan kelas ArrayTransaksiBarang yang merepresentasikan array dari kelas TransaksiBarang.

III.2.3 Rancangan Keamanan SISMIC

Subbab ini meliputi pembahasan tentang aspek keamanan SISMIC, enkripsi dan dekripsi pada SISMIC, dan manajemen dan distribusi kunci pada SISMIC.

III.2.3.1 Aspek Keamanan SISMIC

Seperti yang disebutkan pada subbab sebelumnya, ada beberapa aspek keamanan yang harus dicapai oleh SISMIC agar SISMIC dapat disebut sebagai sistem *micropayment* yang aman. Berikut ini adalah cara bagaimana agar aspek keamanan SISMIC dapat terpenuhi:

- *Confidentiality*
    - Mengubah *key* A dan *key* B dari semua sektor di kartu SISMIC dengan manajemen kuncinya diatur di SAM sehingga data yang ada pada sistem tidak mudah diakses oleh orang yang tidak berhak. *Key* A dan *key* B digunakan untuk membaca dan menulis kartu. Jika *key* A dan *key* B tersebut diganti, pihak yang ingin mengakses data sulit mengetahui *key* A dan *key* B tersebut sehingga pihak tersebut kesulitan mengakses data yang ada di SISMIC.

- Melindungi basisdata SISMIC dengan enkripsi dan *password* sehingga data yang ada pada sistem tidak mudah dibaca oleh pihak yang tidak berhak. Pada tugas akhir ini, pengamanan di basisdata tidak diimplementasi.

- *Integrity*
  - Menerapkan enkripsi dan dekripsi pada SISMIC
  - Pencatatan (*logging*) segala aktivitas yang terjadi di SISMIC pada mesin EDC sehingga *merchant* dapat meminta hasil pembayaran transaksi yang terjadi ke penerbit kartu sesuai dengan transaksi yang pernah terjadi.
- *Availability*
  - Membuat sistem cadangan redundan sehingga jika sistem utama ada gangguan, ada sistem cadangan yang dapat menggantikannya. Pada tugas akhir ini, sistem cadangan redundan tidak diimplementasi.
- *Authentication*
  - Menerapkan *digital signature* agar transaksi hanya dapat terjadi jika menggunakan *hardware* ataupun *software* yang resmi dikeluarkan oleh penerbit kartu.
- *Authorization*
  - *Key* A atau *key* B yang digunakan untuk melakukan transaksi dengan kartu SISMIC berbeda-beda tiap pihak (*merchant*, penerbit kartu, dan pemilik kartu) sehingga pihak-pihak tersebut melakukan transaksi sesuai perannya.
- *Accountability* dan *Non-repudiation*
  - Pencatatan (*logging*) segala aktivitas yang terjadi di SISMIC agar sehingga tidak ada pihak yang dapat menyanggah transaksi yang telah dilakukannya ataupun mengaku telah melakukan transaksi yang telah dilakukannya.

III.2.3.2 Manajemen dan Distribusi Kunci

Pada SISMIC, manajemen dan distribusi kunci akan diatur pada *Secure Access Module* (SAM). SAM akan menyimpan dan mengolah kunci-kunci yang ada pada SISMIC seperti *key* A untuk membaca kartu, *key* B untuk menulis kartu, kunci AES untuk enkripsi dan dekripsi kartu. SAM sudah memiliki sistem kriptografi sendiri sehingga kunci-kunci yang tersimpan di dalam SAM akan aman. SAM memiliki kunci master yang dapat diturunkan menjadi kunci-kunci lain yang dapat digunakan untuk baca atau tulis kartu, yaitu *key* A, dan untuk enkripsi, yaitu kunci AES.

Kunci AES diturunkan dari kunci master menggunakan algoritma PBKDF2. Kunci AES pada tugas akhir ini berukuran 16 bytes dan diturunkan dengan algoritma PBKDF2 dengan pengulangan 1000 kali. Salt yang digunakan untuk penurunan kunci menggunakan algoritma PBKDF2 adalah ID kartu SISMIC berukuran 8 bytes disatukan dengan bilangan random berukuran 12 bytes. Setelah itu, hasil konkatenasi tersebut akan di-XOR dengan bilangan random berukuran 20 bytes.

Key A dan *key* B juga diturunkan dari kunci master menggunakan algoritma PBKDF2, sama seperti kunci AES. *Key* A dan *key* B tiap sektor pada kartu SISMIC akan berbeda-beda, *key* A dan *key* B satu kartu SISMIC dengan kartu SISMIC yang lain juga akan berbeda. *Key* A atau *key* B berukuran 6 bytes, namun kunci turunan yang dihasilkan akan berukuran 16 bytes. Kunci turunan ini akan dipotong menjadi 6 bytes sebagai *key* A. *Key* A atau *key* B diturunkan dari kunci master menggunakan algoritma PBKDF2 dengan pengulangan 1000 kali. Salt yang digunakan adalah konkatenasi antara ID kartu SISMIC berukuran 8 bytes, posisi sektor kartu yang akan dibuat kuncinya yang berukuran 1 bytes, dan bilangan random berukuran 11 bytes yang di-XOR dengan bilangan random berukuran 20 bytes. Pada tugas akhir ini, SAM akan disimulasikan dengan disimpan pada aplikasi dalam bentuk *file* .txt karena keterbatasan alat.

Key A dan *key* B akan berbeda-beda untuk tiap *merchant*. Contohnya, *key* A dan *key* B untuk *merchant* A akan berbeda dengan *key* A dan *key* B untuk *merchant* B.

Hal ini dilakukan agar tiap *merchant* tidak dapat menyanggah transaksi yang pernah dilakukannya ataupun menuduh pihak lain yang melakukan transaksi. *Key* A dan *key* B untuk tiap *merchant* didapat dari menurunkan kunci master menggunakan algoritma PBKDF2. Hasil dari turunan ini berukuran 20 *bytes*. Hasil turunan ini akan dipotong menjadi 6 *bytes* untuk menjadi *key* A dan *key* B. *Key* A atau *key* B untuk masing-masing *merchant* diturunkan dari kunci master menggunakan algoritma PBKDF2 dengan pengulangan 1000 kali. Salt yang digunakan adalah konkatenasi antara ID kartu SISMIC berukuran 8 bytes, posisi sektor kartu yang akan dibuat kuncinya yang berukuran 1 bytes, dan bilangan random berukuran 11 bytes yang di-XOR dengan bilangan random berukuran 20 bytes, lalu di-XOR kembali dengan ID *merchant* yang berukuran 20 *bytes*.

III.2.3.3 Enkripsi dan Dekripsi pada SISMIC

Enkripsi dan dekripsi pesan yang akan digunakan pada SISMIC menggunakan algoritma AES. Pesan yang dienkripsi akan diberi *digital signature* dengan menggunakan algoritma ECDSA. Tujuan pemberian *digital signature* ini adalah agar sistem mengetahui apakah pesan berasal dari pihak yang benar atau tidak, jika berasal dari pihak yang tidak seharusnya, pengiriman pesan akan digagalkan sehingga tidak akan terjadi transaksi apapun.

Pesan yang akan dikirim ke mesin pembaca kartu SISMIC akan dienkripsi dahulu menggunakan algoritma AES. Enkripsi ini akan membutuhkan kunci AES. Kunci AES didapatkan dari kunci turunan yang disimpan di dalam SAM, seperti yang telah dijelaskan di sub subbab sebelumnya. Kunci AES ini akan digunakan untuk mengenkripsi dan juga mengdekripsi pesan.

Setelah dienkripsi, pesan tersebut akan diberi *digital signature* menggunakan kunci privat yang dibuat dari aplikasi SISMIC. Aplikasi SISMIC ini akan membuat kunci privat dan kunci publik. Lalu, pesan akan dikirim ke mesin pembaca kartu. Mesin pembaca kartu akan memverifikasi pesan dengan memeriksa *digital signature* yang berada di pesan yang terenkripsi. Verifikasi akan menggunakan kunci publik. Jika *digital signature* terbukti berasal dari pihak

yang benar, pesan akan didekripsi menggunakan kunci AES dan instruksi seperti baca saldo, transaksi pembelian, ataupun transaksi *top-up* saldo dapat dilakukan. Aspek keamanan yang dilindungi dengan enkripsi dan dekripsi ini adalah *integrity*.

III.2.3.4 Log *Offline* di Mesin Pembaca Kartu SISMIC

Pada mesin EDC yang berada di *merchant* ataupun mesin ATM, mesin pembaca kartu SISMIC menyimpan log transaksi kartu SISMIC milik pemilik kartu, baik transaksi *top-up* atau pembelian. Log ini bersifat *offline* tersimpan di dalam mesin pembaca kartu SISMIC. Log ini dilindungi dengan enkripsi menggunakan algoritma AES, dan kuncinya akan tersimpan di SAM, sehingga pihak *merchant* ataupun bank tidak bisa sembarangan mengutak-atik log ini. Isi log ini adalah ID kartu dari pemilik kartu yang melakukan transaksi, waktu transaksi, status, transaksi yang dilakukan, via, dan nominal. Tidak hanya transaksi *top-up* ataupun pembelian yang disimpan di log, operasi baca saldo dan lihat masa berlaku juga akan disimpan. Log ini berfungsi agar *merchant* dapat meminta pembayaran hasil transaksi pembelian pemilik kartu ke penerbit kartu dan begitu juga sebaliknya, agar penerbit kartu dapat meminta pembayaran hasil transaksi *top-up* kartu ke *merchant*. Log *offline* ini akan disimpan dengan diekripsi terlebih dahulu menggunakan algoritma AES yang kuncinya disimpan di SAM.

DAFTAR PUSTAKA

Chen, C.-H., Lin, I.-C., & Yang, C.-C. (2014). NFC Attacks Analysis and Survey.

Coskun, V., Ok, K., & Ozdenizci, B. (2013). *Professional NFC Application Development For Android™.* United Kingdom: John Wiley & Sons Ltd.

Gulati, V. P., & Srivastava, S. (2007). The Empowered Internet Payment Gateway. *Towards Next Generation E-government*, 98-107.

Igoe, T., Coleman, D., & Jepson, B. (2014). *Beginning NFC.* Sebastopol: O'Reilly.

Jara, A. J., Zamora, M. A., & S, A. F. (2009). Secure use of NFC in medical environments. 8.

Knudsen, J. (1998, May). Java Cryptography. O'Reilly.

Munir, R. (2004). Diktat Kuliah Kriptografi. Bandung, Indonesia.

NFC Forum. (2015). *NFC Forum - NFC Forum Specification Architecture*. Retrieved 12 3, 2015, from NFC Forum: http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/

NFC Forum. (2015). *NFC Forum - NFC in Action.* Retrieved 12 3, 2015, from NFC Forum: http://nfc-forum.org/what-is-nfc/nfc-in-action/

NFC Forum. (2016, Desember 27). *What is NFC?* Retrieved from NFC Forum: http://nfc-forum.org/what-is-nfc/

Rankl, W., & Effing, W. (2010). Smart Card Handbook Fourth Edition. United Kingdom: John Wiley & Sons, Ltd.

Society, T. I. (2000). *RFC 2898 - PKCS #5: Password-Based Cryptography Specification Version 2.0.* Retrieved from IETF Tools: https://tools.ietf.org/html/rfc2898#section-5.2

Stallings, W. (2005). *Cryptography and Network Security: Principles and Practice, Fourth Edition.* New Jersey: Prentice Hall.

WhatIs.com. (2016, December 28). *What is micropayment? - Definition from WhatIs.com*. Retrieved from WhatIs.com: http://whatis.techtarget.com/definition/micropayment