

SISTEM PENCATATAN KEHADIRAN BERBASIS JAVA CARD

Lidya Octarina

Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Bina Nusantara University
Jln. K.H. Syahdan No 9, Palmerah, Jakarta Barat 11480
lidya.octarina@binus.ac.id

ABSTRACT

The purposes of this research are to prevent jockey in exams, reduce the occurrence of error in attendance record at practicum or exams, and reduce error in filling students' attendance status to the attendance system. Three main parts of software development method are used; analysis, design, and literature method. Current system survey, analysis of the survey findings, identify the information, and identifying system requirements are implemented in analysis method. The design method that is used in this research is Unified Modeling Language (UML). The using of attendance recording system that uses Java Card-based application makes students identity card has a new function as the tool to make attendance. Conclusion of the research has shown that it can prevent identity fraud, minimize the time wasted in attendance system, reduce the printing paper, and reduce tagging errors eligibility status exam of students.

Keywords: Kehadiran, Java Card, joki, Smart Card, RFID

ABSTRAK

Tujuan dari penelitian ini adalah menghindari joki pada saat ujian, mengurangi terjadinya kesalahan dalam pencatatan kehadiran pada saat praktikum maupun ujian, dan mengurangi kesalahan dalam pengisian status kehadiran mahasiswa. Metode pengembangan piranti lunak yang digunakan meliputi tiga bagian pokok yaitu metode analisa, perancangan, dan studi pustaka. Metode analisa meliputi survei atas sistem yang sedang berjalan, analisa terhadap temuan survei, identifikasi kebutuhan informasi, dan identifikasi persyaratan sistem. Metode perancangan menggunakan pendekatan Unified Modelling Language (UML). Hasil yang dicapai adalah penggunaan sistem pencatatan kehadiran yang menggunakan aplikasi berbasis Java Card. Selain sebagai kartu identitas mahasiswa, fungsi BiNus Card menjadi bertambah yaitu sebagai alat absensi. Simpulan dari penelitian ini adalah menghindari pemalsuan identitas, meminimalisasikan waktu yang terbuang pada saat melakukan absensi, mengurangi pencetakan kertas, dan mengurangi kesalahan penandaan status kelayakan ujian mahasiswa.

Kata kunci: Kehadiran, Java Card, joki, Smart Card, RFID

PENDAHULUAN

Seiring dengan perkembangan teknologi yang berkembang pesat, hampir semua sektor kehidupan menggunakan teknologi informasi untuk mendukung pekerjaan operasional mereka menjadi lebih baik lagi. Dunia pendidikan juga seakan-akan tidak mau ketinggalan untuk mengikuti perubahan dan perkembangan teknologi informasi. Hal ini dilakukan untuk meningkatkan kualitas sistem pendidikan sehingga memberikan kepuasan tersendiri kepada konsumen, yaitu mahasiswa. Dengan meningkatnya kualitas sistem dari suatu instansi pendidikan, maka diharapkan terjadi peningkatan minat calon mahasiswa untuk memilih instansi pendidikan tersebut.

Salah satu instansi pendidikan yang selalu mengikuti perkembangan teknologi informasi adalah BINUS University. Dikarenakan mahasiswa BINUS University berjumlah besar, maka universitas ini memiliki sistem pengelolaan kehadiran yang kompleks. Sebagai contohnya, sistem kehadiran ujian pada Software Laboratory Center (SLC) yang merupakan salah satu unit terkait dari BINUS University yang bertugas melaksanakan kegiatan praktikum. Proses sistem kehadiran dari tahap persiapan sampai dengan tahap implementasi di ruangan praktikum membutuhkan waktu yang cukup banyak dan kemungkinan terjadi kesalahan juga sangat besar dikarenakan pencatatan kehadiran yang masih menggunakan sistem kehadiran yang memakai kertas.

Selain itu, jumlah mahasiswa yang ikut serta dalam ujian tidaklah sedikit. Diperlukan pengawasan dari asisten yang bertugas untuk mengecek satu-persatu foto yang terlampir pada kartu identitas mahasiswa (KMK/BINUS Card). Sistem kehadiran ujian dengan menggunakan Kartu Mata Kuliah (KMK) menimbulkan sebuah masalah baru, yaitu terjadinya joki dalam ujian dikarenakan adanya pemalsuan identitas diri.

Untuk menangani masalah-masalah tersebut di atas, maka dirancanglah sistem pengelolaan kehadiran yang baru yaitu sistem kehadiran dengan penggunaan teknologi Smart Card. Dengan penggunaan teknologi Smart Card, maka memungkinkan sistem kehadiran dengan menggunakan kertas dikurangi. Smart Card juga memungkinkan data yang diperlukan disimpan dan diproses lebih aman dengan adanya kriptografi, sehingga meminimalisasi terjadinya joki. Dengan sistem yang terkomputerisasi, tingkat kesalahan dari manusia dapat diminimalisasi.

METODE

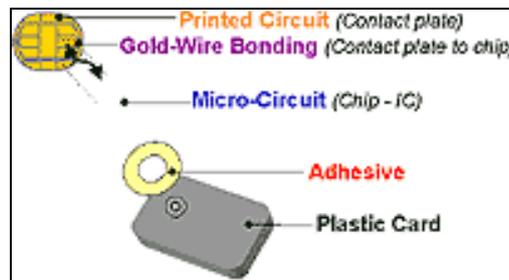
Metode penelitian yang digunakan meliputi studi pustaka dan studi lapangan. Pada metode studi pustaka dilakukan pengumpulan bahan-bahan pustaka baik yang dilakukan di perpustakaan maupun pencarian melalui internet. Metode ini berguna dalam membantu memperdalam pembahasan materi, pembuatan program aplikasi, dan penyusunan laporan penelitian. Pada metode studi lapangan dilakukan analisis sistem yang melalui empat tahapan yaitu survei atas sistem yang sedang berjalan sekarang, melakukan wawancara dengan pihak yang bersangkutan, mempelajari dokumen dan sistem yang sedang berjalan, analisis terhadap hasil wawancara dan dokumen perusahaan. Metode ini berguna untuk mengetahui kebutuhan pengguna, model tampilan yang disukai, dan kemudahan pengoperasian.

Pengenalan *Smart Card*

Smart card adalah sebuah kartu plastik yang digabung dengan *Integrated Circuit* (IC) yang

menyerupai ukuran kartu kredit dan bersifat *tamper resistant*, yaitu usaha ilegal pengambilan data dari dalam kartu tidak dimungkinkan (Ortiz, 2003). *Smart card* didesain untuk menyimpan data yang bersifat pribadi dengan tingkat keamanan yang tinggi dan kartu mudah untuk dibawa kemana saja (*portable*). Penyimpanan dan pemrosesan informasi dalam *smart card* dilakukan melalui sirkuit elektronik yang digabungkan dalam silikon pada bahan plastik (umumnya PVC atau ABS) dari kartu, seperti pada

Gambar 1.



Gambar 1 Komponen Smart Card

Integrated Circuit (chip) berukuran sangat kecil dan *printed circuit* berbentuk plat emas yang tipis. *Printed circuit* ini memberikan kontak elektrik dengan lingkungan luar dan juga melindungi chip dari kerusakan mekanik dan gangguan elektrik (Bezakova, Pashko & Surendan, 2000). Kartu dapat ditanamkan hologram untuk menghindari pemalsuan.

Untuk pemrosesan dan penyimpanan data yang aman digunakan *public-key* atau *shared-key algorithm*. Beberapa *smart card* memiliki *cryptographic coprocessors* yang terpisah yang mendukung algoritma seperti RSA (*Rivest-Shamir-Adleman's algorithm*), AES (*Advanced Encryption Standard*) dan *Triple DES (Triple Data Encryption Standard)*.

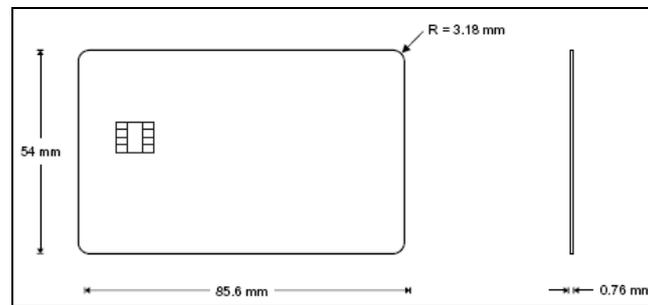
Cara komunikasi yang dipakai *smart card* adalah *half duplex*, yaitu jenis komunikasi dua arah, namun tidak dilakukan secara bersamaan. Fungsi mengirim dan menerima harus dilakukan secara bergantian. Data yang dikirimkan dan diterima dari *smart card* disimpan dalam *buffer* yang terdapat dalam RAM *smart card*.

Standar Internasional Smart Card

Smart card merupakan sebuah komponen dalam sebuah sistem yang kompleks. *Interface* yang berhubungan dengan kartu dalam sebuah sistem harus memiliki kesesuaian dan spesifikasi. *Smart card* memungkinkan pemecahan masalah dalam sebuah sistem dengan mengabaikan sistem lainnya. Ini berarti, akan diperlukan *smart card* yang berbeda-beda untuk setiap sistem. Oleh karena itu, diperlukan standarisasi untuk memungkinkan sebuah kartu multifungsional dapat dikembangkan (Rankl & Effing, 2003).

Standar ISO/IEC digunakan untuk menentukan standarisasi dari *smart card*. Kepanjangan dari ISO adalah *International Organization for Standardization*, sedangkan kepanjangan IEC adalah *International Electrotechnical Commission*. ISO/IEC 7816 dan ISO/IEC 7810 adalah standar yang menentukan hal-hal seperti bentuk fisik kartu, posisi dan ukuran dari konektor elektrikal kartu, karakteristik dari sirkuit elektronik, protokol komunikasi, termasuk format perintah yang dikirim ke kartu dan tanggapan dari kartu, ketahanan kartu, dan fungsionalitas kartu. Ukuran kartu *smart card* dengan format ID-1 berdasarkan ISO/IEC 7810 adalah 85,60mm x 53,98mm dan memiliki ketebalan

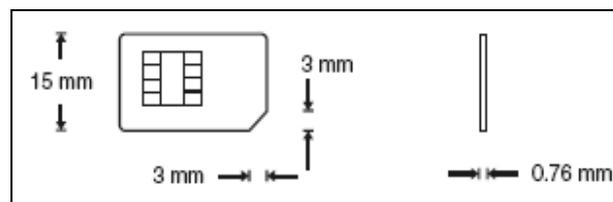
kartu $0,76\text{mm} \pm 0,08\text{mm}$ serta jari-jari sudutnya $3,18\text{mm}$, seperti pada Gambar 2.



Gambar 2 Ukuran standar Smart Card format ID-1

Ukuran lainnya adalah format ID-000 (berdasarkan sistem telepon *mobile* berbasis GSM) yaitu $25\text{mm} \times 15\text{mm}$ dengan ketebalan $0,76\text{mm} \pm 0,08\text{mm}$. Bagian kanan bawah kartu dipotong dengan sudut sebesar 45° . Jari-jari sudut kartu adalah $1\text{mm} \pm 0,10\text{mm}$ dan panjang sisi sudut yang dipotong sebesar $3\text{mm} \pm 0,03\text{mm}$, seperti pada

Gambar 3.



Gambar 3 Ukuran standar Smart Card format ID-000

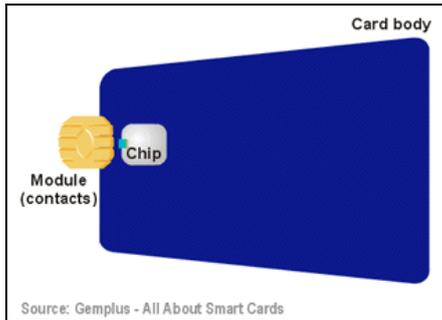
Tipe Smart Card

Secara umum ada dua tipe dari *smart card* yaitu *Memory card* dan *Microprocessor card*. *Memory card* hanya menyimpan dan memproteksi data secara lokal, namun tidak mengandung sebuah prosesor untuk melakukan perhitungan komputer pada data. Sedangkan *microprocessor card* memiliki memory dan *microprocessor* yang dapat melakukan kalkulasi pada data dan menyimpan data dalam kartu secara aman.

Biasanya, *memory card* dapat menyimpan data sebesar 1K sampai 4K dan keuntungan dari *memory card* terletak pada teknologinya yang sederhana. Sedangkan *microprocessor card*, menawarkan keamanan yang ditingkatkan dan kemampuan multifungsional. Data yang disimpan dalam *microprocessor card* tidak dapat diakses secara langsung melalui aplikasi di luar kartu. *Microprocessor* mengontrol data dan memory mengatur pengaksesan data menurut kondisi yang diberikan seperti *password*, enkripsi dan lainnya. Keuntungan *microprocessor card* adalah dapat diintegrasikan ke lebih dari satu aplikasi. Secara fisik, *smart card* dibedakan menjadi dua jenis yaitu *contact smart card* dan *contactless smart card*.

Contact Smart Card

Contact Smart Card bekerja dengan cara berkomunikasi secara fisik antara *card reader* dan *smart card's pin contact* yang berbentuk segiempat berukuran ± 1 cm. *Contact smart card* tidak membutuhkan baterai dan akan aktif ketika terhubung dengan *card reader*. Saat terhubung dengan *reader*, maka *chip* menunggu perintah request dari *client/host* dari aplikasi untuk membaca informasi dari *chip* atau menulis informasi ke *chip*, seperti pada **Error! Reference source not found.** dan **Error! Reference source not found.**



Gambar 4 Contact Smart Card

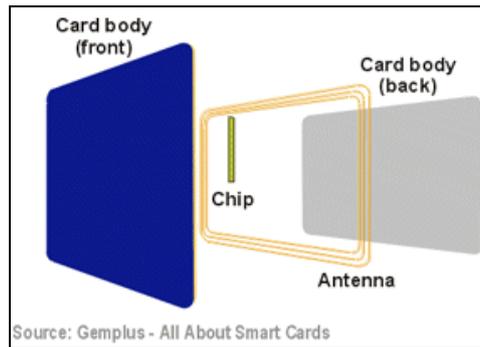


Gambar 5 Smart Card's pin contact

Berikut adalah fungsi dari masing-masing *contact* menurut ISO/IEC 7816, yaitu (1) VCC (*Supply Voltage*), sebagai penyedia tegangan listrik, biasanya sebesar 3 atau 5 volt dengan toleransi maksimum $\pm 10\%$; (2) RST (*Reset Input*), berfungsi mengirimkan sinyal untuk me-reset *microprocessor*; (3) CLK (*Clock Input*), berfungsi sebagai *timing* atau *clocking signal* yang mengatur frekuensi waktu atau kecepatan mikroprosesor; (4) GND (*Ground*), merupakan reference voltage yang berlawanan dengan Vcc dimana energi potensialnya diukur. Nilainya dianggap 0 volt; (5) VPP (*Programming Voltage*), berfungsi menyediakan tegangan listrik yang berbeda dari VCC. C6 biasa digunakan untuk aplikasi lain seperti konektivitas USB; (6) I/O (*Input/Output*), berfungsi memonitor semua komunikasi yang keluar maupun yang masuk pada kartu; (7) C4 dan C8, *Contact C4* dan *C8* merupakan *contact* tambahan yang digunakan bila diperlukan untuk operasi pada kartu atau penggunaan *interface* di masa akan datang, seperti USB. Kedua *contact* ini dapat dihilangkan untuk mengurangi biaya produksi. Oleh karena itu, *Smart card* ada yang memiliki 6 atau 8 *pin contact*.

Contactless Smart Card

Contactless Smart Card berkomunikasi dengan terminal melalui sinyal frekuensi radio. Komunikasi *contactless smart card* berdasarkan dengan teknologi yang sama dengan *Radio Frequency Identification (RFID)*. *Contactless smart card* tidak memiliki baterai, sehingga kartu ini memiliki induktor yang menangkap sinyal frekuensi radio sebagai sumber daya elektronik kartu. *Contactless card* memerlukan jarak tertentu untuk melakukan pertukaran data dengan *card reader*, seperti pada Gambar 6.



Gambar 6 *Contactless Smart Card*

Standar komunikasi *contactless smart card* adalah ISO/IEC 14443. Standarisasi ISO/IEC *Contactless Smart Card* seperti pada Tabel 1 dan Tabel 2.

Tabel 1 Standarisasi ISO/IEC *Contactless Smart Card*

Standar	Tipe <i>contactless smart card</i>	Jarak komunikasi
ISO/IEC 10 536	<i>Close-coupling card</i>	± 1 cm
ISO/IEC 14 443	<i>Proximity coupling card (PICC)</i>	± 10 cm
ISO/IEC 15 693	<i>Vicinity coupling card (VICC)</i>	± 1 m

Tabel 2 Perbandingan Teknologi Smart Card dengan RFID [2]

	RFID	<i>Smart Card</i>
Jarak Komunikasi	± 30 cm (pendek)	± 1 cm (pendek)
	± 3 m (menengah)	± 10 cm (menengah)
	± 10 m (jauh)	± 1 m (jauh)
		tinggi, karena adanya enkripsi
Authentikasi (pembuktian keaslian)	Rendah, oleh karena itu mudah dipalsukan.	sehingga memiliki tingkat keamanan yang tinggi.
Penyimpanan data	sedikit, ± 2 KB	besar, ada yang mencapai 72 KB

Sistem Memori Smart Card

Menurut Chen (2000), *Smart Card* terdiri dari tiga buah jenis memori, yaitu: (1) ROM (*Read-Only Memory*), digunakan untuk menyimpan program yang bersifat tetap dari kartu, dan tidak dibutuhkan tenaga untuk menyimpan data. ROM tidak dapat ditulis kembali setelah kartu dibuat, dan berisikan sistem operasi. ROM dari *smart card* berisikan data dan aplikasi user yang bersifat permanen; (2) EEPROM (*Electrical Erasable Programmable Read Only Memory*), hampir serupa dengan ROM yang dapat menyediakan data ketika tenaga dari memori dimatikan. Perbedaannya adalah isi dari memori ini dapat dimodifikasi selama penggunaan kartu yang normal. EEPROM dapat menerima setidaknya 100.000 kali penulisan, dan dapat menyimpan data selama 10 tahun. Membaca dari EEPROM sama cepatnya dengan membaca dari RAM, namun menulis pada EEPROM 1000 kali

lebih lama dibandingkan menulis dari RAM; (3) RAM (*Random Access Memory*), digunakan sebagai tempat kerja sementara untuk menyimpan dan memodifikasi data. RAM merupakan memori yang bersifat *nonpersistent* yaitu informasi yang disimpan pada RAM akan dihilangkan ketika tenaga dari kartu hilang.

Protokol Application Protocol Data Units (APDU)

Seperti yang telah dispesifikasikan dalam ISO 7816-4, protokol APDU adalah sebuah protokol pada tingkatan aplikasi antara *smart card* dengan *host-application*. Memiliki dua buah struktur, yaitu (1) Pesan APDU yang dikirim pada kartu *smart card* oleh *host application* melalui *Card Acceptance Device* (CAD), yang dikenal sebagai *Command APDU* (C-APDU), seperti pada

Gambar 7; (2) Pengiriman respon balik kepada *host-application* dari kartu, yang dikenal sebagai *Response APDU* (R-APDU), seperti pada Gambar 8.

Mandatory header				Optional Body		
CLA	INS	P1	P2	Lc	Data Field	Le

Gambar 7 *Command APDU*

Optional Body	Mandatory trailer	
Data Field	SW1	SW2

Gambar 8 *Response APDU*

Protokol Transmission Protocol Data Units (TPDU)

APDU dikirimkan melalui *transport protocol* yang didefinisikan pada ISO 7816-3. Struktur penukaran data antara *host* dan kartu menggunakan *transport protocol* yang disebut dengan *Transmission Protocol Data Units* (TPDU). Dua buah *transport protocol* utama yang digunakan adalah protokol T=0 dan protokol T=1. Protokol T=0 bersifat *byte oriented* dimana unit terkecil yang diproses dan dikirimkan oleh protokol berbentuk sebuah byte. Sedangkan protokol T=1 merupakan protokol yang bersifat *block oriented*, dimana yang dikirimkan adalah serangkaian *byte*.

Teknologi Java Card

Java Card adalah teknologi yang memungkinkan aplikasi berbasis *Java* (*Applet*) dapat berjalan secara aman pada *Smart Card* dan alat-alat sejenisnya [3]. *Java Card* merupakan program terkecil yang ditargetkan oleh *Java* untuk digabung ke dalam *embedded device*. *Java Card* dipergunakan secara luas pada kartu SIM (digunakan pada kartu GSM *handphone*) dan kartu ATM.

Teknologi *Java Card* dikembangkan untuk menyimpan informasi yang bersifat *personal* di dalam *Smart Card*. Keamanan terlihat dalam beberapa aspek, yaitu (1) Enkapsulasi data, Data disimpan ke dalam aplikasi *Java Card* dan dieksekusi di dalam lingkungan yang terisolasi (*Java Card VM*), terpisah dari sistem operasi dan *hardware*; (2) *Applet* firewall, aplikasi-aplikasi yang berbeda dipisahkan antara satu dan yang lain oleh *applet firewall* yang membatasi dan mengecek akses elemen data antara satu *applet* ke *applet* lainnya; (3) kriptografi, mendukung algoritma enkripsi seperti DES, 3DES, AES, RSA. Dan mendukung kriptografi lainnya seperti *signing*, *key generation* and *key*

exchange; (4) *applet*, adalah sebuah aplikasi konfigurasi yang hanya memproses perintah yang masuk dan memberikan balasan dengan mengirimkan data atau status respon ke *interface device*.

Elemen dari aplikasi *Java Card* terdiri dari *back-end application and systems*, *host (off-card) application*, *interface device (card reader)*, *applet* dalam kartu, data yang diperlukan dan *software* yang mendukung. Semua elemen ini bersama-sama menyusun sebuah aplikasi *end-to-end* yang aman. Berikut ini adalah arsitektur dari aplikasi *Java Card*:

Back-End Application and Systems

Adalah aplikasi dan sistem yang tidak berinteraksi secara langsung dengan pengguna, tapi secara tidak langsung mendukung *host application*. *Back-end application* mendukung *applet Java* di dalam kartu, sebagai contoh memberikan konektivitas dengan sistem keamanan, memberikan pelayanan seperti informasi pembayaran elektronik yang disimpan dalam *database*.

Reader-Side Host (off-card) Application

Adalah aplikasi yang berada pada *desktop* atau terminal seperti PC, telepon genggam, mesin ATM. *Host application* mengatur komunikasi antara pengguna, *applet Java Card*, dan *back end application*.

Reader-Side Card Acceptance Device (CAD)

Adalah alat yang menjadi jembatan antara *host application* dan *Java Card device*. CAD dapat berupa sebuah *card reader* yang dipasang pada sebuah komputer melalui *serial port* atau diintegrasikan kepada sebuah terminal seperti mesin pembayaran elektronik pada restoran atau tempat perbelanjaan. Alat ini meneruskan perintah APDU (*Application Protocol Data Unit*) dari *host application* ke kartu, dan meneruskan umpan balik dari kartu ke *host application*.

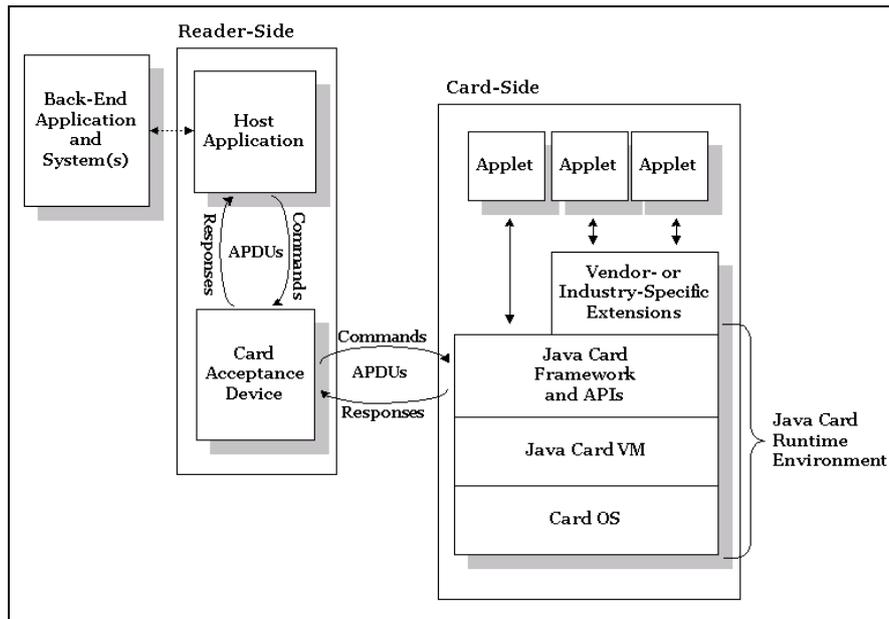
Card-Side Applets dan lingkungannya

Java Card platform adalah lingkungan yang mendukung *multiple application*. Dalam hal ini, dalam satu kartu bisa memiliki satu atau lebih *Java Card applet* yang berjalan bersamaan dengan perangkat lunak yang mendukungnya yaitu sistem operasi pada kartu dan *Java Card Runtime Environment (JCRE)*. JCRE terdiri dari *Java Card VM (Virtual Machine)*, *Java Card Framework and APIs*, dan beberapa pengembangan *APIs*, seperti pada

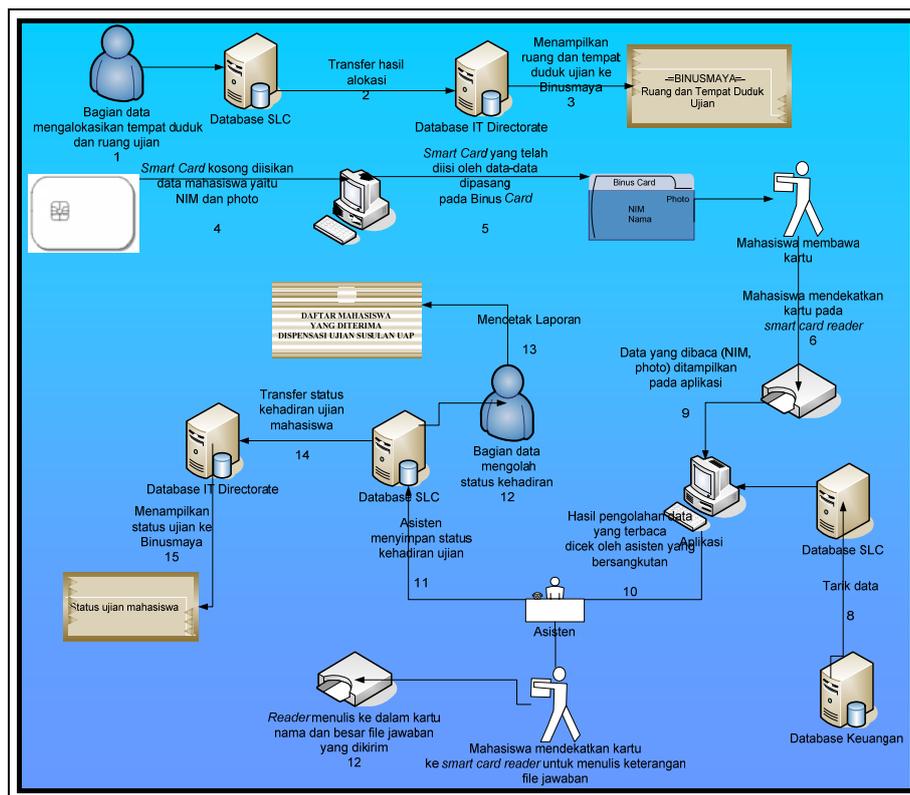
Gambar 9.

Model Konseptual

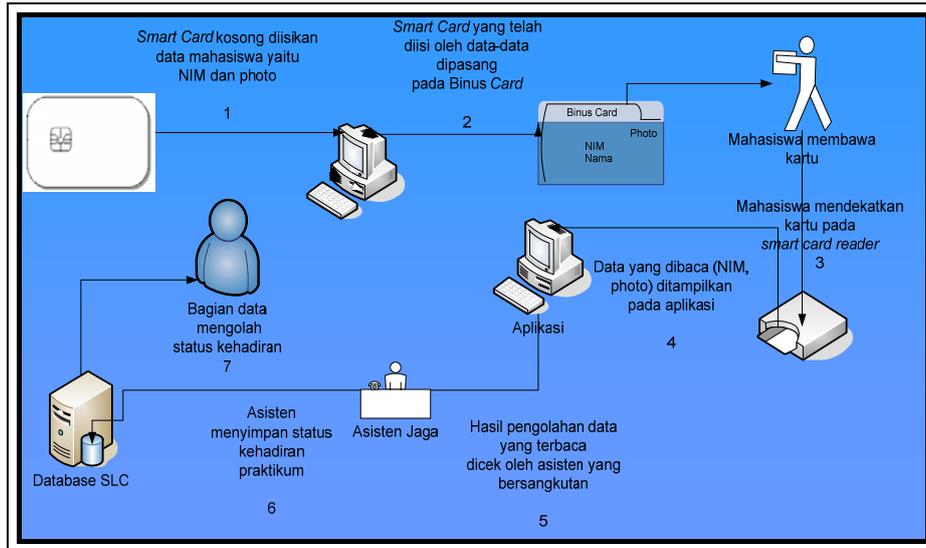
Model Konseptual dari system kehadiran terdiri dari model konseptual yang dipakai saat praktikum dan pada saat ujian seperti pada Gambar 10 dan Gambar 11. aplikasi POS yang terhubung dengan EDC seperti pada Gambar 4, Gambar 5 dan Gambar 6. Cara kerja dari aplikasi POS yang terhubung dengan EDC digambarkan pada Gambar 4. *Class diagram* yang dibangun digambarkan pada Gambar 5. Gambar 6 menggambarkan kebutuhan komponen perangkat lunak yang dibutuhkan.



Gambar 9 Arsitektur Aplikasi Java Card



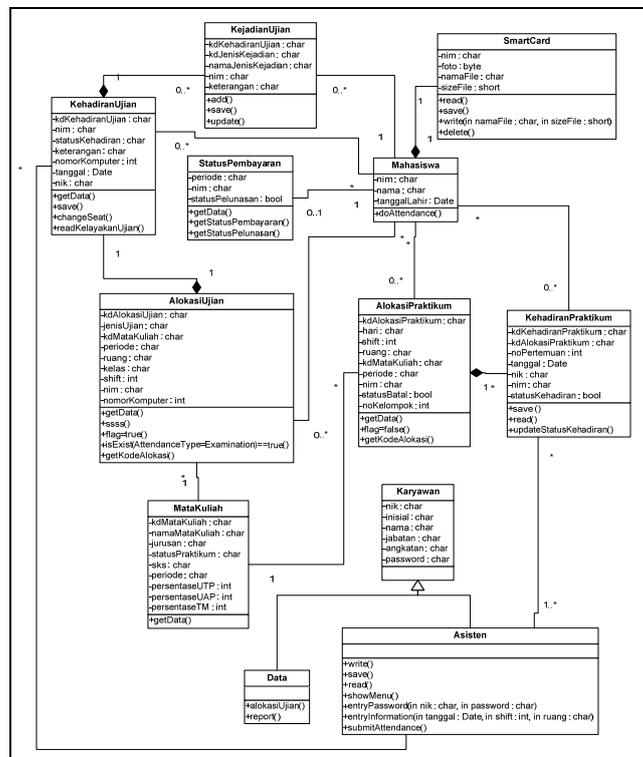
Gambar 10 Model Konseptual Proses Pengisian Kehadiran Ujian dengan Smart Card



Gambar 11 Model Konseptual Proses Pengisian Kehadiran Praktikum dengan *Smart Card*

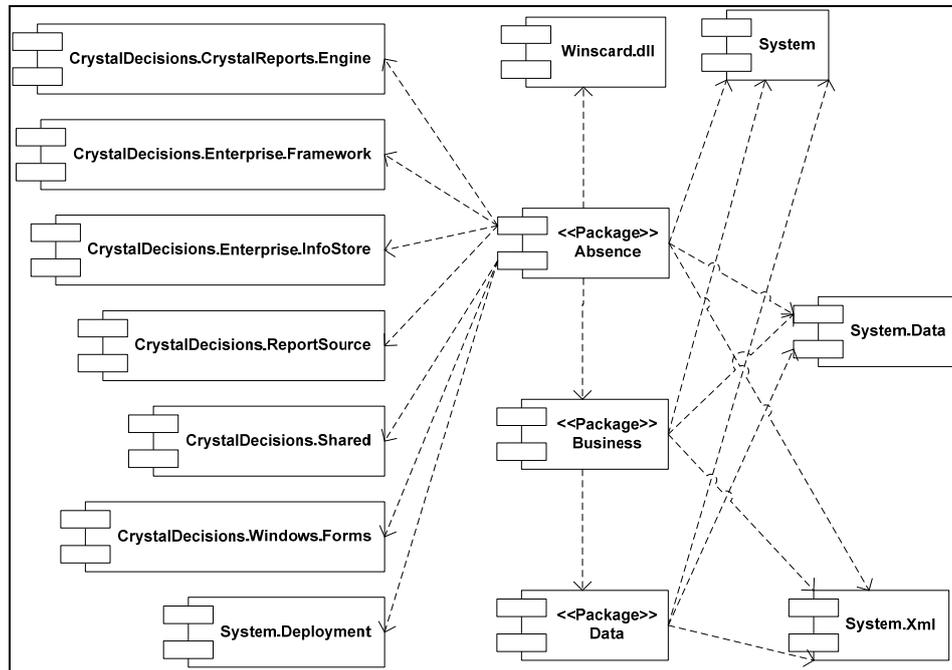
Desain Model

Aplikasi yang dibangun digambarkan dengan menggunakan *Class Diagram* seperti pada Gambar 12.

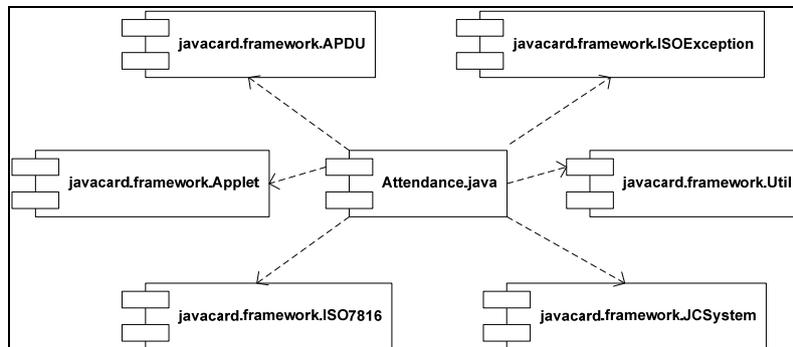


Gambar 12 *Class Diagram*

Pada Gambar 13 dan Gambar 14 akan menggambarkan hubungan komponen perangkat lunak yang dibutuhkan pada aplikasi dan *Smart Card*.



Gambar 13 *Component Diagram* pada Aplikasi



Gambar 14 *Component Diagram* pada *Smart Card*

Kebutuhan Perangkat Lunak

Untuk mengimplementasikan rancangan aplikasi dan basis data yang telah dibuat, diperlukan perangkat lunak dengan spesifikasi tertentu.

Komputer Server

Perangkat lunak pada komputer *server* yang diperlukan untuk implementasi rancangan aplikasi dan basis data yang baru pada *Software Laboratory Center* adalah Microsoft Windows Server 2003 *Enterprise Edition*, Microsoft Visual Studio 2005, MSDN 2005, *Java Runtime Environment 5.0*, Eclipse IDE, Microsoft .Net Framework 2.0., Microsoft SQL Server 2000, Windows *Installer 3.1*.

Komputer Client

Perangkat lunak pada komputer klien yang diperlukan untuk implementasi rancangan aplikasi dan basis data yang baru pada *Software Laboratory Center* adalah Microsoft Windows XP Professional SP2, Microsoft .Net Framework 2.0., Omnikey 5x21, 5x25 PC/SC Driver, Windows Installer 3.1, Java Runtime Environment 5.0.

Kebutuhan Perangkat Keras

Untuk mengimplementasikan rancangan aplikasi dan basis data yang telah dibuat, diperlukan perangkat keras dengan spesifikasi yang ditentukan, yang masing-masing tergantung dari jenis komputer: *server* dan *klien*.

Komputer Server

Spesifikasi perangkat keras pada komputer server yang diperlukan untuk implementasi rancangan aplikasi dan basis data yang baru adalah Processor 1.5 GHz, Memory 1 GB, Harddisk drive dengan kapasitas 8 Gb atau lebih, VGA Card 1024x768 High Color, CD ROM, Keyboard dan Mouse, Monitor.

Komputer Klien

Spesifikasi perangkat keras pada komputer klien yang diperlukan untuk implementasi rancangan aplikasi dan basis data yang baru adalah Processor 1 GHz., Memory 512Mb, Harddisk drive kapasitas 3Gb, VGA Card 1024x768 High Color, CD ROM, Omnikey CardMan 5321 (RFID Reader ISO 14443), Keyboard dan Mouse, Monitor.

HASIL DAN PEMBAHASAN

Evaluasi Waktu

Hasil evaluasi waktu diambil dari 7 buah kelas dengan jumlah mahasiswa yang bervariasi. Rata-rata jumlah mahasiswa yang dihitung dalam evaluasi ini adalah ± 29 orang mahasiswa. Jumlah waktu yang dapat dihemat dengan penggunaan sistem yang baru adalah ± 21 menit, seperti pada Tabel 3.

Tabel 3 Tabel Evaluasi Waktu

No	Rata - rata waktu yang dibutuhkan	Sistem yang sedang berjalan	Sistem yang diusulkan
1.	Pengecekan kelayakan ujian	± 9 menit	± 8 menit
2.	Penandatanganan dokumen kehadiran	± 15 menit	
3.	Penandatanganan keterangan jawaban ujian oleh mahasiswa	± 12 menit	± 9 menit
4.	Pemberian tanda status kelayakan ujian mahasiswa per kelas	± 2 menit	0 menit
5.	Selisih waktu yang dapat di hemat (sistem yang sedang berjalan – sistem yang diusulkan)		± 21 menit

Evaluasi Sumber Daya Manusia

Berdasarkan hasil evaluasi sumber daya manusia yang dibutuhkan, sistem yang sedang berjalan membutuhkan 8 orang dalam melaksanakan 1 transaksi praktikum dan ujian untuk tiap kelasnya. Sedangkan dengan menggunakan sistem yang diusulkan dibutuhkan 5 orang dalam melaksanakan 1 transaksi praktikum dan ujian untuk tiap kelasnya, seperti pada Tabel 4.

Tabel 4 Tabel Evaluasi Sumber Daya Manusia

No	Sistem yang sedang berjalan	Sistem yang diusulkan
1.	1 orang <i>data administrator</i> untuk mencetak dokumen kehadiran praktikum	-
2.	1 orang <i>data administrator</i> untuk memberikan tanda pada dokumen kehadiran ujian mahasiswa yang tidak layak mengikuti ujian baik dikarenakan status pelunasan administrasi ataupun jumlah absensi mahasiswa melebihi batas maksimal	-
3.	1 orang asisten jaga untuk mengisi status kehadiran praktikum mahasiswa ke dalam <i>web</i> kehadiran praktikum	1 orang asisten jaga untuk menyimpan status kehadiran praktikum mahasiswa.
4.	1 orang asisten jaga untuk mengecek kelayakan mahasiswa sebelum mahasiswa memasuki ruang ujian	1 orang asisten untuk mengecek kelayakan ujian mahasiswa.
5.	1 orang asisten jaga untuk mengedarkan dokumentasi kehadiran ujian mahasiswa	-
6.	1 orang asisten korektor untuk mengisi status kehadiran ujian mahasiswa ke dalam <i>web</i> kehadiran.	1 orang asisten jaga untuk menyimpan status kehadiran ujian mahasiswa
7.	1 orang asisten jaga untuk mencetak keterangan file jawaban mahasiswa.	1 orang asisten jaga untuk menyimpan keterangan <i>file</i> jawaban mahasiswa kedalam kartu
8.	1 orang <i>data administrator</i> untuk membuat laporan dispensasi ujian mahasiswa.	1 orang <i>data administrator</i> untuk membuat laporan dispensasi ujian mahasiswa.

Evaluasi Tingkat Kesalahan

Kesalahan pengisian status kehadiran mahasiswa disebabkan karena kelalaian pengentrian status, mahasiswa yang masuk tidak menandatangani dokumen kehadiran. Data ini didapat dari *form* Permintaan Perubahan Status Absensi Mahasiswa pada Semester Ganjil 2008/2009.

Dengan menggunakan sistem kehadiran berbasis *java card*, maka semua kesalahan akibat kelalaian asisten karena kesalahan pengisian status kehadiran tidak terjadi lagi, begitu juga dengan kelalaian mahasiswa yang tidak menandatangani dokumen kehadiran atau kesalahan penandatanganan kolom pada dokumen kehadiran. Kesalahan dapat dihilangkan karena status kehadiran mahasiswa akan ditampilkan secara langsung setelah mahasiswa mendekatkan kartu ke *card reader*, seperti pada

Tabel 5.

Tabel 5 Tabel Evaluasi Tingkat Kesalahan

Pada sistem yang sedang berjalan	Pada sistem yang menggunakan <i>Smart card</i>
195 buah kesalahan	-

SIMPULAN

Simpulan yang diperoleh dari penelitian ini yaitu sistem dapat mempersingkat waktu yang diperlukan dalam pemeriksaan setiap mahasiswa yang akan masuk ke ruang ujian dan pencatatan kehadiran mahasiswa pada saat praktikum maupun ujian; Sistem mengurangi terjadinya kesalahan seperti dalam pengisian status kehadiran mahasiswa pada saat praktikum dan ujian, pemberian tanda bagi mahasiswa yang tidak layak untuk ujian, dan pemberian tanda tangan pada kolom dokumen kehadiran; Sistem kehadiran yang baru ini mempersingkat proses bisnis yang dilakukan seperti pemeriksaan kelayakan ujian mahasiswa, mengurangi antrian pada saat ujian, ketergantungan untuk mendapatkan data status kehadiran mahasiswa dari bagian lain.

Saran untuk penelitian dan pengembangan lebih lanjut yaitu implementasi penggunaan smart Card yang menggunakan teknologi Java Card dapat dikembangkan lebih lanjut, agar Binus Card dapat memiliki fungsi yang lebih selain menjadi alat absensi dan kartu identitas mahasiswa. Contohnya sebagai alat pembayaran di kantin, alat peminjaman buku di perpustakaan, parkir dan lain-lain. Selain itu, penggunaan perancangan struktur database pada *Software Laboratory Center* dan struktur database pada IT Directorate dapat disesuaikan lebih lanjut demi kemudahan dalam pengiriman data.

DAFTAR PUSTAKA

- Bezakova, I., Pashko, O., & Surendran, D. (2000). *Introduction*, from <http://people.cs.uchicago.edu/~dinoj/smartcard>
- Chen, Z. (2000). *Java Card™ Technology for Smart Cards*. USA: Sun Microsystems.
- Ortiz, C. E. (2003). *An Introduction to Java Card Technology - Part 1*, from <http://developers.sun.com/mobility/javacard/articles/javacard1>
- Rankl, W., & Effing, W. (2003). *Smart Card Handbook* (3rd ed.). USA: John Wiley & Sons.