PEMBANGUNAN SUATU MODEL ANTARAMUKA KEBOLEHKENDALIAN-ANTARA UNTUK KAD PINTAR DI DALAM KAMPUS UNIVERSITI

oleh

KHAIRUL ANWAR BIN KAMARUDDIN @ HAMDI

Tesis yang diserahkan untuk
memenuhi keperluan bagi Ijazah
Sarjana Sastera

April, 2008

PENGHARGAAN

Alhamdulillah. Saya panjatkan sepenuh kesyukuran kepada Allah, dengan qudrat dan iradahNya, hasil penyelidikan saya yang berkaitan dengan penggunaan kad pintar di dalam persekitaran kampus telah dapat saya sempurnakan dan terbitkan ke dalam bentuk bahan ilmiah. Dokumen ini dihasilkan sebagai memenuhi syarat kelayakan bagi memperolehi ijazah lanjutan pada peringkat Sarjana Sastera Teknologi Pendidikan.

Saya merakamkan penghargaan yang tidak terhingga kepada Professor Madya Dr. Shukri Sulaiman yang bertugas sebagai pensyarah di Pusat Pengajian Pendidikan Jarak Jauh, Universiti Sains Malaysia. Sungguh banyak budi jasa yang telah dihulurkan oleh beliau sebagai penyelia utama dalam pengajian saya ini dalam pelbagai bentuk: dorongan, pengajaran, nasihat bimbingan dan kepakaran. Tidak kurang juga kepada Professor Madya Dr. Mohamed Ismail Mohamed Ibrahim yang turut membantu saya sebagai penyelia bersama. Hanya Allah sahaja yang mampu membalas bantuan ikhlas daripada kalian berdua.

Selain itu, saya juga menyatakan perasaan terhutang-budi kepada isteri saya serta sahabat-handai yang turut sama memberi dorongan dan sokongan moral kepada saya sepanjang tempoh pengajian saya ini..

JADUAL KANDUNGAN

Muka Surat

SENARAI JADUAL

Muka Surat

SENARAI RAJAH

Muka Surat

SENARAI SINGKATAN

ACL	Access Control Level
APDU	Advanced Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset
COM	Component Object Model
CT-API	Card Terminal API
DES	Data Encryption Standard
DF	Dedicated file
EF	Elementary file
EMV	Europay, MasterCard dan VISA
GSM	Global for System Mobile
ICC	Integrated Circuit Card
IDL	Interface Definition Language
IFD	InterFace Device
ISO	International Standards Organization
KPS	Kad Pintar Serbaguna
OCF	Open Card Framework
PCSC	Personal Computer Smart Card
PS	Pengurus Sumber
RM	Resource Manager
SCSP	SmartCard Service Provider
SDK	Software Development Kit

SENARAI LAMPIRAN

PEMBANGUNAN SUATU MODEL ANTARAMUKA KEBOLEHKENDALIAN-ANTARA UNTUK KAD PINTAR DI DALAM KAMPUS UNIVERSITI

ABSTRAK

Dalam penyelidikan ini, masalah keserasian operasi kad dalam pembangunan sistem perisian pelbagai kad pintar dikaji secara mendalam samada dalam aspek teknikal mahupun aspek pengurusan. Hasil daripada pemerhatian dan perbandingan terperinci ke atas tiga jenis kad yang dipilih: Cryptoflex, Payflex dan Cyberflex, ciri-ciri perbezaan yang jelas dalam sifat operasi di antara kad berkenaan diperolehi. Berasaskan kepada ciri-ciri operasi kad-kad yang dipilih, satu rekabentuk sistem antaramuka yang diberi nama Kad Pintar Serbaguna (KPS) dihasilkan sebagai satu cadangan penyelesaian kepada masalah ini. Ia dibangunkan bagi kegunaan pelbagai jenis kad pintar.

Bagi memperlihatkan keupayaannya, sistem perisian perumah telah dibangunkan, dengan tujuan untuk menyelesaikan masalah pengurusan berkaitan aplikasi kad pintar di dalam sebuah universiti. Pilihan ini dibuat kerana kampus universiti mempunyai bilangan pengguna kad pintar yang besar, melebihi sepuluh ribu orang di kalangan masyarakat kampus dan juga menggunakan pelbagai sistem perisian kad pintar bagi memenuhi keperluan setiap jabatan dan pusat pengajian. Berdasarkan kepada hasil pengujian ke atas beberapa contoh sistem perisian perumah, dapat dibuktikan bahawa sistem antaramuka KPS boleh membantu pembangunan sistem perisian dengan kad pintar yang mana kebergantungan kepada bahan-bahan API yang bercirikan kepelbagaian sifat-sifat pengoperasian kad dapat dikurangkan. Rekabentuk yang sama juga dapat dipakai dalam penghasilan objek antaramuka tambahan bagi suatu contoh kad yang lain, Gemplus MPCOS-

EMV. Dengan andaian bahawa hasil yang sama akan diperolehi bagi sebarang kad yang memenuhi spesifikasi yang sama, adalah dijangkakan rekabentuk KPS dapat dikembangkan bagi menghasilkan satu sistem antaramuka kad pintar yang menyokong penggunaan pelbagai jenis kad.

DEVELOPMENT OF AN INTEROPERABLE INTERFACE MODEL FOR SMART CARDS IN A UNIVERSITY CAMPUS

ABSTRACT

In this research, card interoperability problem in development of multi card software is reviewed thoroughly in both technical and management aspects. Based on detailed observation and comparison on three selected cards: Cryptoflex, Payflex and Cyberflex, marked differences in characteristics of card operation of the samples are collected. Based on selected characteristics of card operation, an interface design named Kad Pintar Serbaguna (KPS) is presented as a proposed solution to the problem. The design is developed for dealing with many kinds of card.

To demonstrate its capability, host software system has been developed, aiming to solve management issue relating to smartcard applications in a university. This selection has been made because university campus has fairly large number of smart card users, more than a ten thousand among citizens, and also has various smart card software systems to fulfill requirement of each department and school. Based on test result on a few samples of host software, it is proved that KPS interface system can assist smart card software developement in a manner that dependency on API resources which consist of diverse characteristics of card operations can be reduced. The same design is also applicable for presenting an additional interface card object of another sample of card, Gemplus MPCOS-EMV. Based on assumption that the same result will be found for any card with the same specification, it is expected that KPS design can be expanded into a card interface system that support usage of many kinds of card.

BAB 1 PENGENALAN

1.0 Apa itu kad pintar?

Dalam dua dekad yang lepas, teknologi kad pintar telah berkembang selari dengan kemajuan dalam teknologi pembuatan cip pemproses mikro (Rankl, 2007). Kad pintar telah mengubah cara manusia menjalankan perniagaan mereka. Ia menjadikan maklumat peribadi dapat dibawa bersama dan dipindahkan ke dalam sistem maklumat dengan selamat. Melalui bentuknya yang nipis serta saiznya yang kecil seperti kad kredit, ia menjadi amat ringan, kecil dan mudah dilentur. Oleh itu, ia dapat disimpan di dalam dompet duit atau poket pakaian dan dijadikan sebagai sebahagian daripada barangan milik peribadi (Mayes, 2007).

Keupayaan sesuatu kad dalam menyimpan dan memproses sesuatu maklumat ditentukan oleh cip ICC (*Integrated Circuit Card*) yang terpasang pada kad berkenaan. Jumlah maklumat yang mampu disimpan di dalamnya boleh mencapai sehingga beratus kali ganda lebih banyak berbanding dengan jumlah maklumat yang dapat disimpan dalam satu kad berjalur magnet. Berdasarkan kepada had keupayaan pada cip ICC, kad boleh dikelaskan kepada dua kategori: kad memori dan kad pemproses mikro. Kad memori hanya mampu menyimpan maklumat sahaja; oleh itu kegunaannya dalam sistem maklumat adalah terhad. Salah satu contoh kegunaan kad memori ialah sebagai kad pra-bayar bagi telefon awam. Sebaliknya, kad pemproses-mikro bukan sahaja mampu menyimpan maklumat tetapi juga mampu memproses maklumat. Oleh itu, kegunaannya lebih luas dalam pelbagai bidang. Sehubungan dengan itu, kad pemproses mikro juga dinamakan sebagai ‘kad pintar’, sesuai dengan ciri-ciri kepintaran yang terkandung di dalamnya (Mayes, 2007; Rankl, 2007).

Columbia Encyclopedia memberikan takrifan yang hampir sama, iaitu kad pintar ditakrifkan sebagai:

> “suatu peranti kecil yang menyerupai bentuk seperti kad kredit tetapi mempunyai pemproses mikro yang tertanam di dalamnya bagi menyimpan dan

memproses maklumat. Kad jalur bermagnet yang menyimpan maklumat dalam jumlah yang amat sedikit (biasanya digunakan untuk mengenalpasti identiti pemilik) dan tidak mempunyai keupayaan diri untuk memproses maklumat, boleh dilihat sebagai kad pintar yang primitif. Kad pintar yang sebenar mempunyai lapan puluh atau lebih kali ganda ruang ingatan dan pemproses mikro membenarkan maklumat dibaca dan dikemaskini pada setiap kali kad itu digunakan".

1.1 Jenis-jenis kad pintar

Pertukaran maklumat antara kad dan komputer terminal dikawal oleh satu modul elektronik yang terdapat di dalam cip ICC. Terdapat dua bentuk antaramuka fizikal pada cip ICC, iaitu: sentuhan dan tanpa-sentuhan. Bagi kad sentuhan, maklumat dalam bentuk denyutan elektrik diterima oleh peranti pembaca melalui sentuhan fizikal pada lapisan luar permukaan cip yang kandungan bahan buatannya merupakan daripada jenis logam pengalir (Rankl, 2007; Kim, 2004).

Manakala bagi kad tanpa-sentuhan, penghantaran maklumat antara peranti pembaca dan kad dibuat dalam bentuk gelombang elektromagnet pada frekuensi tertentu. Satu lingkaran litar elektronik dibina pada bahagian sisi kad dan berfungsi sebagai antenna bagi menerima pancaran gelombang elektromagnet. Keseluruhan cip serta antenna dilitupi oleh kepingan penebat plastik pada kedua-dua sisi permukaan kad dan dilindungi sepenuhnya daripada sentuhan fizikal dengan peranti pembaca. Bagi sesuatu proses pertukaran maklumat berjaya dilakukan, memadai dengan hanya menggandingkan kad kepada peranti kad pada jarak tertentu tanpa menyentuh peranti berkenaan. Kad tanpa-sentuhan boleh dikelaskan kepada tiga jenis berasaskan kepada ciri-ciri fizikal cip ICC sebagaimana yang telah ditetapkan dalam piawaian ISO (*International Standards Organization*). Setiap kad menggunakan jarak penggandingan yang berlainan seperti yang ditunjukkan dalam Jadual 1-1 (Rankl, 2007).

Jadual 1-1 Jenis-jenis kad tanpa sentuhan

Jenis kad	Piawaian ISO	Jarak penggandingan
Kad gandingan dekat (*close coupled*)	ISO 10536	Sehingga 1 sentimeter
Kad *proximity*	ISO 14443	Sehingga 10 sentimeter
Kad *vicinity*	ISO 15693	Sehingga 120 sentimeter

Berbeza daripada modul sentuhan, modul tanpa-sentuhan tidak kelihatan pada permukaan kad. Oleh itu, kad tanpa-sentuhan lebih tahan daripada kerosakan fizikal yang berpunca dari sentuhan langsung berkali-kali pada permukaan kad. Kad yang menggabungkan kedua-dua ciri antaramuka ini, sentuhan dan tanpa-sentuhan, dipanggil kad hibrid. Ia mempunyai satu ruang storan data yang dikongsi bersama oleh kedua-dua modul.

Pada masa kini, terdapat pelbagai kad sentuhan di pasaran yang dikeluarkan oleh pelbagai syarikat pengeluar antaranya ialah: Cryptoflex, Cyberflex dan Payflex oleh Schlumberger[1]; GemClub-Micro, GemSafe, MPCOS/EMV dan GPK oleh Gemplus; Micardo Public, Micardo Elliptic dan JCOP (*Java Card Open Platform*) oleh ORGA Kartensysteme, IBM MFC oleh IBM, dan sebagainya.

Berasaskan kepada sistem pengoperasian dalam cip, kad sentuhan boleh dikelaskan kepada dua kategori iaitu: kad sistem fail dan kad java. Dalam kad sistem fail, aplikasi disimpan dalam fail data dalam direktori tertentu. Operasi ke atas data dikawal oleh sistem pengoperasian kad. Manakala dalam kad java, aturcara (dinamakan *Cardlet*) ditulis dalam bahasa pengaturcaraan Java dan hasil kompilasi ke atas aturcara tersebut disimpan di dalam satu fail di dalam memori kad. Akses ke atas data dikawal oleh aturcara dan ia perlu

[1] Kad Cryptoflex bagi perisian berasaskan penyulitan data dan prasarana kekunci awam; kad Cyberflex bagi perisian berasaskan internet dan Java; kad Payflex bagi perisian berasaskan pembayaran tunai secara elektronik.

dijalankan di dalam memori kad terlebih dahulu sebelum sesuatu operasi data dapat dilaksanakan.

1.2 Kegunaan kad pintar

Elemen utama yang diperolehi daripada kad pintar ialah kebolehpercayaan tentang keselamatan data sensitif yang tersimpan dalam memori kad daripada gangguan luar (BWGCBMMF, 2006; Bakdi, 2006). Kad mampu beroperasi secara terpisah dari sistem pengoperasian komputer terminal untuk tugas-tugas yang melibatkan pengujian ketulenan pengguna, pertukaran kekunci keselamatan, penyulitan data dan tandatangan digital. Ia telah lama digunakan secara meluas di dalam bidang teknologi komunikasi maklumat, terutamanya di dalam urusan-urusan perbankan, perniagaan, pengangkutan awam, telekomunikasi dan perkhidmatan pengguna. Antara sistem-sistem perisian yang menggunakan kad pintar ialah sistem kad kredit, sistem mesin auto-teller, sistem pembayaran elektronik tanpa tunai, sistem komunikasi telefon mudah alih, sistem kad pengenalan diri, sistem kad maklumat kesihatan, sistem pengawasan penggunaan peralatan berharga, sistem pengawasan pintu laluan dan sebagainya (Rankl, 2007).

Melalui gabungan teknologi kad pintar dan biometrik, ciri-ciri keselamatan dan ketulenan data yang lebih baik dapat diperolehi. Salah-satu daripada peranti yang berasaskan gabungan kedua-dua teknologi ini dan amat banyak digunakan ialah peranti pengenalpastian pengguna berasaskan kepada corak pada jari pengguna. Ia bukan sahaja lebih murah dari segi harga jika dibandingkan peranti-peranti biometrik lain, tetapi juga lebih tepat dari segi keunikan data yang mewakili identiti seseorang pengguna. Teknologi seumpama ini amat membantu sistem-sistem perisian yang memerlukan kawalan operasi secara automatik dan jarak jauh seperti sistem kawalan pintu laluan, sistem kawalan penggunaan peralatan berharga dan sistem pengedaran maklumat melalui rangkaian internet.

1.3 Bahagian penting dalam sistem perisian kad pintar

Sistem perisian kad pintar boleh dipecahkan kepada tiga bahagian sistem yang utama iaitu:

a. Aplikasi perumah

b. Antaramuka kad

c. Aplikasi dalaman

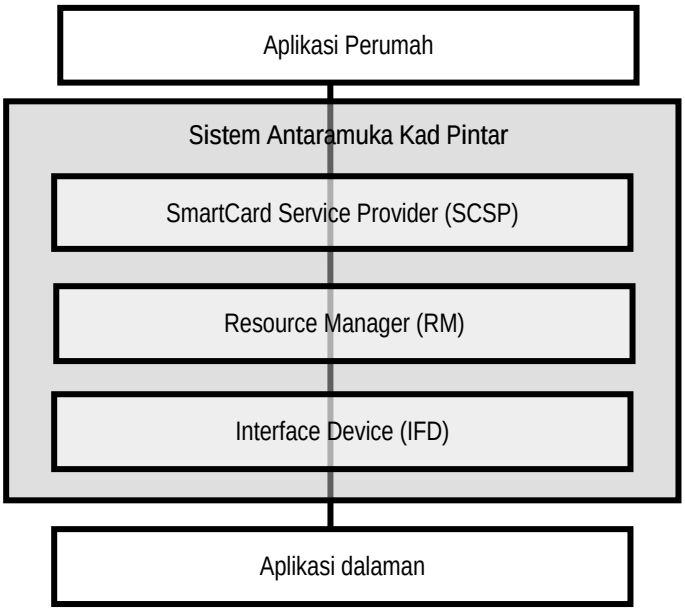
Aplikasi perumah ialah aplikasi yang dipasang pada sistem komputer perumah dan menyediakan perkhidmatan secara langsung kepada pengguna sistem. Aplikasi dalaman ialah aplikasi perkhidmatan yang tersimpan dalam cip memori kad pintar dan dikawal oleh sistem pengoperasian kad. Antaramuka kad menyediakan sejumlah subrutin yang diperlukan oleh sistem perisian perumah. Akses ke atas sumber persisian dan aplikasi dalaman dibuat oleh aplikasi perumah melalui panggilan subrutin yang disediakan dalam bahagian sistem antaramuka kad.

Rekabentuk sesuatu sistem antaramuka kad adalah berbeza bagi persekitaran perkakasan yang berbeza, bergantung kepada ciri-ciri sistem pengoperasian kad pintar, alatan peranti pembaca kad dan sistem pengoperasian komputer yang digunakan. Dalam sesuatu sistem antaramuka kad, terdapat tiga bahagian penting bagi tiga fungsi yang berlainan (seperti yang diperlihatkan dalam Rajah 1-1) :

a. Antaramuka penyedia perkhidmatan kad pintar, *SmartCard Service Provider* (*SCSP*)

b. Antaramuka Pengurus Sumber (PS), *Resource Manager (RM)*

c. Antaramuka peranti pembaca, *InterFace Device* (*IFD*)



Rajah 1-1 Bahagian-bahagian penting dalam sistem perisian kad pintar

Antaramuka IFD menyediakan subrutin bagi kawalan operasi secara langsung ke atas peranti pembaca kad. Oleh kerana setiap jenis peranti pembaca kad mempunyai ciri-ciri operasi yang khusus dan berlainan, setiap jenis peranti pembaca yang digunakan memerlukan satu alatan antaramuka IFD yang tertentu. Biasanya, antaramuka IFD yang sesuai bagi sesuatu peranti pembaca itu akan disediakan oleh syarikat pengeluar yang sama yang mengeluarkan peranti berkenaan.

Antaramuka PS (Pengurus Sumber) menyediakan subrutin bagi mengurus kawalan operasi ke atas sumber persisian yang terdiri daripada pelbagai peranti pembaca dan kad pintar. Berasaskan kepada subrutin dalam antaramuka PS, subrutin tertentu di dalam antaramuka IFD dipanggil. Rekabentuk antaramuka PS adalah berbeza bagi sistem pengoperasian komputer yang berbeza. Contohnya, Winscard keluaran Microsoft Corporation adalah antaramuka PS yang sesuai hanya untuk platform sistem pengoperasian Microsoft Windows sahaja, iaitu untuk keluarga Windows98 dan WindowsNT. Winscard dihasilkan berasaskan kepada spesifikasi PC/SC *(Personal Computer / Smart Card)* dan ia merupakan sebahagian daripada sistem pengoperasian Microsoft Windows. Sistem-sistem

pengoperasian komputer yang lain seperti LINUX, UNIX dan OS2 tidak mempunyai satu bahagian khusus yang menjalankan tugas yang sama. Sebaliknya, sebahagian tugas antaramuka PS dilaksanakan oleh modul-modul tertentu yang bukan sebahagian daripada sistem pengoperasian komputer, seperti JavaCard, BasicCard dan MULTOS.

Antaramuka SCSP menyediakan subrutin bagi menghantar maklumat kepada sistem pengoperasian kad pintar dan menerima maklumbalas daripadanya. Berasaskan kepada subrutin dalam antaramuka SCSP, subrutin tertentu di dalam antaramuka PS dan IFD dipanggil. Melalui hubungan ini, aplikasi dalaman dapat dipasang di dalam kad dan dikawal oleh aplikasi perumah.

1.4 Ketidakseragaman rekabentuk antaramuka SCSP

Sesetengah antaramuka SCSP dihasilkan dalam bentuk modul yang merupakan sebahagian daripada produk industri ‘kit pembangunan perisian’ SDK (*Software Development Kit)*. SDK yang berlainan diperlukan bagi kegunaan dalam persekitaran sistem yang berlainan. Tiada garis-panduan lengkap ditetapkan tentang ciri-ciri rekabentuk antaramuka SCSP yang wajib dipatuhi. Oleh itu, tiada keseragaman dalam rekabentuk antaramuka SCSP dihasilkan dan bentuk sesuatu antaramuka SCSP amat berlainan dengan antaramuka SCSP yang lain.

Antaramuka SCSP yang sesuai bagi sesuatu kad tidak semestinya juga sesuai bagi kad-kad lain kerana ciri-ciri sistem pengoperasian kad dan modul logik mungkin berlainan antara satu kad dengan yang lain.

Umumnya, ciri-ciri sesuatu rekabentuk antaramuka kad adalah berbeza bagi persekitaran sistem yang berbeza, bergantung kepada jenis peranti pembaca, platform sistem pengoperasian komputer dan kad yang digunakan. Sehubungan dengan itu, sesuatu antaramuka yang dipilih untuk sesuatu kad tidak boleh digunakan untuk kad pintar dari jenis

yang lain walaupun kad-kad ini datang daripada satu pengeluar yang sama. Ini dapat dilihat dalam beberapa SDK bagi pembangunan sistem perisian kad yang dikeluarkan oleh syarikat perisian kad yang popular seperti Schlumberger Sema dan Gemplus. Walaupun produk keluaran mereka disasarkan bagi kegunaan dalam persekitaran sistem pengoperasian komputer dengan persisian komputer yang sama, masih terdapat jurang perbezaan yang banyak di antara antaramuka daripada sesuatu produk dengan antaramuka daripada produk yang lain.

Sebagai satu contoh, Schlumberger Sema telah mengeluarkan produk-produk yang berlainan bagi kad dan sistem perisian yang berlainan seperti berikut:

a. Kit Pembangunan Perisian Cryptoflex dengan kad Cryptoflex, sesuai bagi sistem perisian berasaskan kriptografi dan prasarana kekunci awam.

b. Kit Pembangunan Perisian Cyberflex dengan kad Cyberflex, sesuai bagi sistem perisian berasaskan internet dan pengaturcaraan java.

c. WinPractice dengan kad Payflex, sesuai bagi sistem perisian berasaskan pembayaran tunai secara elektronik.

Walaupun ketiga-tiga produk berkenaan disasarkan bagi kegunaan dalam persekitaran sistem pengoperasian Microsoft Windows dengan peranti pembaca jenis yang sama, Schlumberger Reflex, tetapi setiap antaramuka daripada produk berkenaan hanya sesuai digunakan untuk satu jenis kad yang disasarkan itu sahaja.

Oleh itu, tidak menghairankan bagaimana sesuatu sistem yang dibangunkan itu akan terikat kepada penggunaan satu jenis kad pintar sahaja. Keupayaan sesuatu jenis kad yang dipilih untuk satu bahagian dalam sistem berkenaan adalah tidak sesuai untuk kegunaan dalam bahagian yang lain. Masalah ini dapat dilihat dalam sistem-sistem perisian yang

mempunyai jumlah bilangan pemegang kad yang ramai seperti sistem kad pengenalan diri bagi masyarakat sebuah universiti, sistem kad maklumat kesihatan bagi pesakit sebuah hospital dan sistem kad kawalan laluan lebuh raya bagi pengguna kenderaan bermotor. Atas alasan-alasan yang tertentu, suatu kad pintar daripada jenis yang berlainan ingin diintegrasikan dan pada masa yang sama, kad-kad yang sedang beredar di kalangan pengguna masih ingin dikekalkan. Dalam situasi sebegini, sekiranya kad yang dipilih itu tidak sepadan dengan antaramuka yang telah digunakan, kecekapan operasi sistem berkenaan akan berubah. Tambahan pula, seandainya langkah-langkah pengubahsuaian ke atas sistem berkenaan ingin dilaksanakan, ia mungkin akan memerlukan lebih banyak masa dan kos kerana ia akan melibatkan penggunaan beberapa antaramuka kad dengan setiap satu daripadanya mempunyai rekabentuk yang berlainan.

Pelbagai pendekatan telah diambil oleh ramai pembangun perisian dan penyelidik bagi mengatasi masalah keserasian yang terdapat dalam sistem pelbagai kad pintar. Schneier dan Whiting (1998); Daemen dan Rijmen (1998); Anderson et al. (1998) telah melakukan kajian dalam bidang berkaitan dengan ciri-ciri sistem pengoperasian kad bagi menghasilkan spesifikasi sistem pengoperasian kad yang lebih selamat. Manakala, Itoi et al. (2000) dan Hermann et al. (1998) telah melakukan kajian dalam bidang berkaitan dengan sistem antaramuka kad bagi menghasilkan antaramuka yang sesuai dengan pelbagai jenis kad, dan bagi menyokong pembangunan sistem-sistem perisian kad dengan jurang perbezaan rekabentuk yang lebih luas. Hal ini akan dijelaskan secara lebih terperinci dalam BAB 2 TINJAUAN LITERATUR.

Sehubungan dengan itu, satu kajian dijalankan bagi mengenalpasti masalah keserasian operasi yang terdapat dalam kad-kad yang berlainan dan bagi mencari satu pilihan penyelesaian yang boleh dianggap sesuai bagi mengatasi masalah berkenaan.

1.5 Objektif

Objektif penyelidikan ini ialah:

1. Mengenalpasti masalah keserasian operasi yang terdapat dalam jenis kad-kad pintar yang berbeza, berasaskan kepada tiga jenis kad keluaran Schlumberger: Cryptoflex, Cyberflex dan Payflex.

2. Membangunkan satu model sistem antaramuka yang boleh menyelesaikan masalah keserasian operasi kad bagi kad-kad yang terpilih.

3. Menghasilkan satu model keseragaman dalam rekabentuk sistem antaramuka kad yang boleh dijadikan sebagai satu platform untuk pembangunan sistem antaramuka pelbagai jenis kad.

1.6 Skop Kajian

Memandangkan masa kajian dan sumber peralatan yang terhad, kajian ini dihadkan kepada penggunaan beberapa kad sentuhan dari tiga jenis yang berlainan yang dipilih daripada kad-kad keluaran Schlumberger Sema: Cryptoflex, Cyberflex dan Payflex. Pemilihan ini dibuat atas dasar bahawa setiap kad berkenaan mempunyai banyak perbezaan yang jelas di dalam ciri-ciri sistem pengoperasian kad, walaupun ia datang daripada satu pengeluar yang sama. Atas tujuan pemasaran yang tertentu, Schlumberger Sema mensasarkan jenis kad yang berlainan bagi bentuk perisian yang berlainan.

Kajian dilakukan dalam satu persekitaran sistem komputer yang sama, iaitu menggunakan sistem pengoperasian Microsoft Windows 2000 dan peranti pembaca Schlumberger Reflex USB. Adalah diluar skop kajian ini untuk membincangkan masalah ketidakserasian yang timbul dalam aspek-aspek lain seperti bagi persekitaran sistem-sistem pengoperasian komputer yang berlainan dan bagi jenis-jenis peranti pembaca yang berlainan.

BAB 2 TINJAUAN LITERATUR

2.0 Pengenalan

Teknologi kad pintar telah digunakan secara meluas dalam institusi-institusi pengajian tinggi samada di dalam mahupun di luar negara (O'Leary, 2007) . Kini, penggunaan kad pintar bukan sahaja terhad sebagai kad pengenalan diri, tetapi juga dalam pelbagai aplikasi dalam sistem keselamatan, perbankan, kesihatan dan juga pengangkutan (Hendry, 2007). Contohnya, di Universiti Sains Malaysia, teknologi kad pintar digunakan dalam kad matrik pelajar dan kad staf. Ia menawarkan beberapa ciri-ciri tambahan berbanding kad plastik biasa seperti perbankan, laluan keselamatan, maklumat kesihatan, perakam waktu kehadiran, dan perpustakaan. Pelbagai bentuk sistem perisian telah dibangunkan dan diintegrasikan dengan teknologi kad pintar. Isu ketidak-seragaman sistem kad pintar dalam pelbagai aspek yang berbeza dilihat sebagai satu masalah yang sering dihadapi dalam membangunkan sesuatu sistem perisian yang melibatkan pemakaian pelbagai kad pintar (Grimaud et al., 2006).

Dalam kajian ini, tumpuan diberikan kepada isu ketidak-seragaman operasi kad dalam sistem perisian. Berasaskan kepada kajian beberapa penyelidik dalam pembangunan sistem perisian kad pintar, dapat dilihat bagaimana masalah keserasian kad boleh mengakibatkan pelbagai masalah serius dalam penyediaan dan pengendalian sesuatu sistem perisian. Antara masalah-masalah yang timbul adalah seperti berikut: perubahan kecekapan operasi sistem, pertambahan dari segi masa dan kos pembangunan sistem, dan perubahan kekangan terhadap ciri rekabentuk sistem.

Itoi dan Honeyman (1999) mendapati sukar untuk menentukan jenis kad yang sesuai dengan keperluan sistem mereka kerana terdapat ciri-ciri perbezaan di kalangan jenis kad yang telah mereka pilih; walaupun pada dasarnya kesemua kad yang dipilih itu diakui oleh pengeluar kad sebagai telah memenuhi spesifikasi PC/SC. Adalah dijangkakan perbezaan

dalam kecekapan operasi akan terjadi jika sistem yang dibangunkan itu disasarkan untuk pemakaian pelbagai jenis kad. Ini adalah kerana kestabilan dan ciri mesra pengguna adalah berbeza untuk setiap jenis kad dan antaramuka yang berbeza. Bagi sistem yang perlaksanaannya bergantung kepada kadar masa tindak balas sesuatu kad memproses maklumat, kekurangan ini boleh mengakibatkan satu penilaian atau keputusan yang salah dibuat dan dengan itu, boleh menggagalkan operasi sistem berkenaan.

Dalam penyelidikan lain, Itoi et al. (2000) telah membangunkan satu antaramuka berasaskan kepada arahan APDU *(Advanced Protocol Data Unit*) dalam kad untuk kegunaan dalam perisian keselamatan komunikasi internet. Oleh kerana terdapat pelbagai antaramuka untuk kad pintar di pasaran dan tiada satu pun yang dominan, masa yang agak panjang diperlukan bagi mempelajari satu demi satu antaramuka yang ada. Oleh kerana lebih banyak masa dan tumpuan telah digunakan bagi mempelajari dan memahami pelbagai sumber berkenaan, tempoh pembangunan sesuatu sistem menjadi lebih panjang daripada tempoh yang dijadualkan. Kos pembangunan sistem berkenaan juga dijangka meningkat bila lebih banyak tenaga pekerja dan sumber perisian perlu digunakan.

2.1 Piawaian sistem pengoperasian kad

Salah satu langkah pendekatan yang boleh diambil dalam menangani masalah keserasian operasi kad ialah dengan menghasilkan satu rekabentuk sistem pengoperasian kad yang seragam dan sesuai bagi kegunaan pelbagai bentuk sistem. Dalam kata lain, satu spesifikasi yang am dan disepakati oleh pelbagai pengeluar kad perlu dihasilkan. Sehubungan dengan itu, melalui pertubuhan-pertubuhan peringkat antarabangsa yang melibatkan penyertaan daripada pelbagai syarikat perisian dan pengeluar kad terkemuka di dunia, berbagai bentuk spesifikasi piawaian berkaitan dengan sistem pengoperasian kad telah dihasilkan, antaranya ialah ISO7816, EMV, GSM dan CEN796.

2.1.1 Piawaian ISO 7816, EMV dan GSM

Pertubuhan Piawaian Antarabangsa atau ISO (*International Standards Organization*) telah memperkenalkan piawaian ISO 7816 untuk ICC jenis sentuhan. Spesifikasi ini hanya bertumpu pada operasi di tahap rendah sahaja iaitu dari segi saiz fizikal ICC, lokasi dan saiz bahagian sentuhan elektrikal, protokol transmisi dan signal elektronik, dan arahan untuk pengurusan memori dan pertukaran data.

Spesikasi EMV (*Europay, MasterCard and VISA*) telah dikeluarkan secara bersama oleh gabungan syarikat Europay, MasterCard dan VISA pada Disember 1996. Tumpuan diberikan kepada jenis data dan kaedah pengkodan untuk kegunaan dalam industri kewangan bagi pengguna kad kredit. Manakala, industri komunikasi pula mentakrifkan spesifikasi komunikasi yang berbeza, dinamakan GSM (*Global System For Mobile*), untuk sistem komunikasi bagi pengguna telefon mudah-alih.

2.2 Piawaian antaramuka kad

Berasaskan kepada spesifikasi piawaian antarabangsa ISO7816, beberapa antaramuka telah dihasilkan bagi pembangunan pelbagai sistem perisian kad pintar seperti PC/SC, OCF, MUSCLE, CT-API dan lain-lain. Setiap daripada antaramuka ini mempunyai kekuatan dan kelemahan mereka masing-masing.

2.2.1 Spesifikasi PC/SC

Spesifikasi PC/SC telah dikeluarkan pada Disember 1997 oleh kumpulan kerja *PC/SC* yang dianggotai oleh beberapa syarikat kad pintar dan PC terkemuka, antaranya ialah Groupe Bull, Hewlett – Packard, Microsoft, Schlumberger dan Siemens Nixdorf. Ia bertujuan untuk menghasilkan satu piawaian industri bagi kegunaan kad pintar dalam sistem komputer peribadi. Spesifikasi pertama, PC/SC Release 1.0, difokuskan kepada aspek keselamatan data peribadi dan perlindungan storan data yang perlu dipatuhi oleh pengeluar ICC.

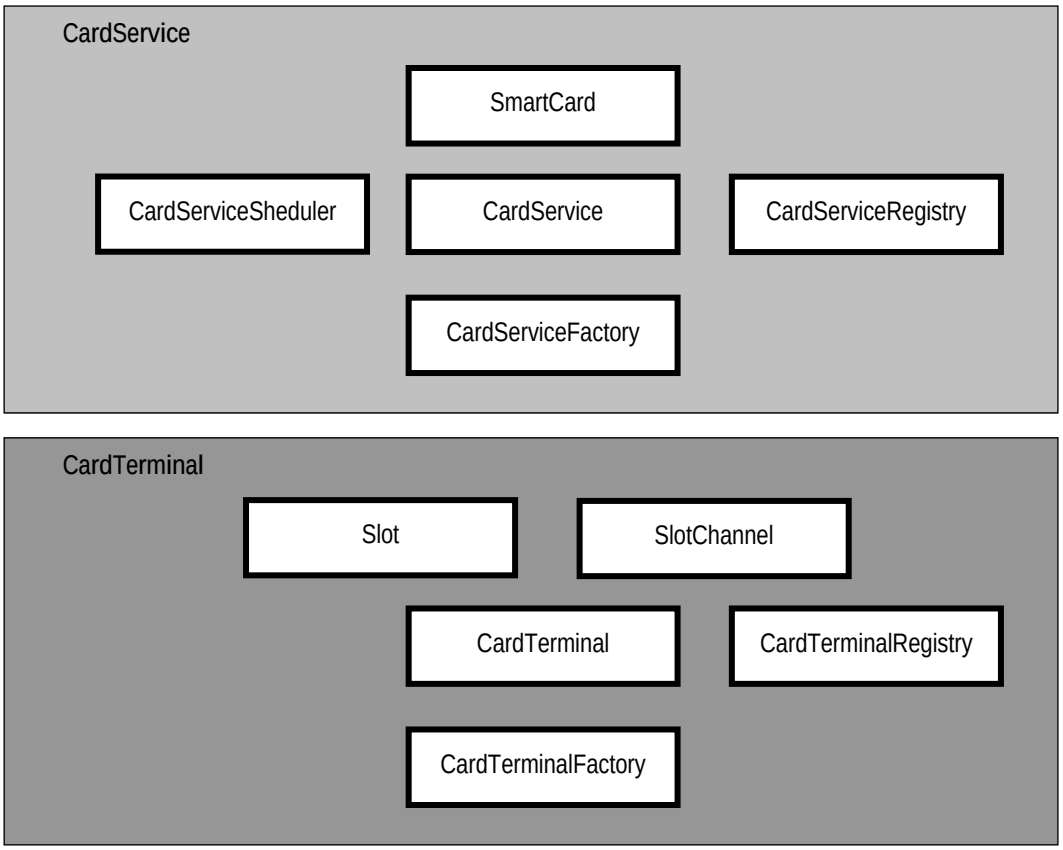
Satu daripada elemen-elemen penting yang dihasilkan ialah antaramuka Pengurus Sumber. Ia bertindak sebagai satu perantara utama yang mengurus hubungan komunikasi antara berbagai sumber perisian dengan sumber persisian kad pintar yang terdapat dalam satu sistem komputer. Antaramuka ini hanya khusus untuk sistem pengoperasian Microsoft Windows sahaja.

Pada masa kini, kerja sedang dibuat untuk mengeluarkan spesifikasi kedua iaitu PC/SC Release 2.0. Tumpuan diberikan kepada tiga aspek: ICC tanpa-sentuhan, mekanisma pemilihan kad oleh sistem perisian, dan antaramuka peranti (*IFD - Inter-Face Device*) untuk peranti pembaca dengan ciri-ciri tambahan seperti panel paparan dan pad pin.

2.2.2 OpenCard Framework (OCF)

Antaramuka OCF telah dibangunkan pada tahun 1998 oleh konsortium OpenCard Framework yang diasaskan bersama oleh Groupe Bull, Dallas Semiconductors, First Access, Gemplus, IBM, Netscape, NCI, Schlumberger, SCM Microsystems, Sun, UbiQ dan VISA. Tumpuan diberikan kepada pembangunan sistem perisian kad pintar dalam bahasa Java. Tidak seperti PC/SC yang hanya boleh digunakan dalam platform Microsoft Windows sahaja, OCF tidak bersandar kepada mana-mana platform. Rekabentuk OCF adalah hampir sama dengan PC/SC iaitu ia turut menyediakan satu antaramuka umum untuk hubungan data dengan peranti pembaca (Hermann et al., 1998).

Rekabentuk antaramuka OCF terbahagi kepada dua komponen utama iaitu: CardService dan CardTerminal. Komponen CardTerminal menyediakan subrutin berkaitan akses kepada peranti pembaca kad pintar dan kad pintar, manakala komponen CardService menyediakan infrastruktur bagi interaksi dengan sistem pengoperasian kad. Rajah 2-1 memperlihatkan kandungan dalam kedua-dua komponen berkenaan.



Rajah 2-1 Komponen utama dalam antaramuka OCF

Peranan yang dimainkan oleh CardTerminal adalah sama seperti peranan yang dimainkan oleh antaramuka Pengurus Sumber dalam PC/SC. Manakala bagi CardService, tiada modul am dalam PC/SC yang disediakan bagi tujuan yang sama. Dalam PC/SC, setiap kad memerlukan antaramuka tertentu yang mungkin berlainan dengan kad-kad yang lain dan ia mungkin datang daripada syarikat-syarikat perisian yang berlainan.

2.2.3 Card Terminal API (CT-API)

CT-API (*Card Terminal - Application Programming Interface*) telah dibangunkan oleh European Union untuk sistem perisian kad kesihatan. Ia mempunyai tahap API yang rendah dan banyak menggunakan parameter berbentuk tatasusunan bait. Oleh itu, ia sesuai untuk persekitaran bahasa pengaturcaraan C. Ia turut menyediakan subrutin asas berkaitan akses kepada peranti pembaca kad pintar. Terdapat sejumlah peranti pembaca yang menyokong pembangunan sistem menggunakan CT-API.

2.2.4 Kekuatan dan kelemahan dalam OCF dan PC/SC

Kekuatan yang dapat dilihat dengan jelas pada kedua-dua senibina OCF dan PC/SC ialah kedua-duanya menyediakan subrutin umum bagi mengawal operasi pelbagai jenis peranti pembaca kad pintar yang dihubungkan dalam satu sistem komputer. Selain itu, kedua-duanya juga turut menyediakan subrutin umum bagi pertukaran maklumat dalam bentuk binari antara sistem pengoperasian kad dan sistem perisian perumah.

Walaupun telah banyak aspek keseragaman dicapai melalui senibina OCF dan PC/SC tetapi masih banyak lagi aspek yang kurang diberi perhatian, terutamanya dalam penyediaan subrutin pada tahap yang lebih tinggi. Antara perkara-perkara yang kurang diberi perhatian ialah: struktur rekod untuk kekunci keselamatan, ciri-ciri atau atribut-atribut yang mentakrifkan keadaan sifat sesuatu fail, dan proses pengurusan ciri-ciri keselamatan ke atas aplikasi dalaman kad (Hermann et al., 1998).

Selain itu, ciri-ciri senibina OCF hanya sesuai bagi pembangunan sistem perisian menggunakan kad Java sahaja, tetapi bukan bagi sistem dengan kad sistem fail. Tidak banyak kemudahan yang disediakan oleh OCF bagi kad sistem fail. Kerumitan akan timbul dalam pembangunan sistem perisian bagi sistem yang memerlukan ciri-ciri terperinci berkaitan pengurusan fail bagi kad sistem fail. Manakala, senibina PC/SC tidak menyediakan satu alatan antaramuka am yang boleh dianggap sesuai bagi kegunaan pelbagai jenis kad sistem fail. Oleh itu, kerumitan akan timbul apabila lebih daripada satu jenis kad sistem fail ingin digunakan di dalam sesuatu sistem perisian.

Akibat daripada kelemahan-kelemahan ini, adalah sukar untuk membangunkan suatu sistem perisian pelbagai kad yang baik jika sumber pengaturcaraan hanya berasaskan kepada sistem antaramuka kad yang telah sedia ada. Satu alatan antaramuka pada tahap yang lebih tinggi diperlukan bagi memperbaiki kelemahan-kelamahan ini.

BAB 3 KAEDAH PENYELIDIKAN

3.0 Pengenalan

Kaedah penyelidikan ini dibahagikan kepada tiga bahagian bagi mencapai tiga bahagian objektif yang berbeza:

1. Mengenalpasti masalah keserasian operasi yang terdapat dalam jenis kad-kad pintar yang berbeza, berasaskan kepada tiga jenis kad keluaran Schlumberger: Cryptoflex, Cyberflex dan Payflex.

2. Membangunkan satu model sistem antaramuka yang boleh menyelesaikan masalah keserasian operasi kad bagi kad-kad yang terpilih.

3. Menghasilkan satu model keseragaman dalam rekabentuk sistem antaramuka kad yang boleh dijadikan sebagai satu platform untuk pembangunan sistem antaramuka pelbagai jenis kad.

3.1 Mengenalpasti masalah keserasian operasi dalam kad

Analisis perbandingan dibuat tentang ciri-ciri persamaan dan perbezaan yang terdapat dalam tiga jenis kad iaitu: Cryptoflex, Cyberflex dan Payflex. Pemerhatian dibuat dengan berpandukan kepada tiga dokumen manual yang diperolehi daripada kit pembangunan perisian keluaran Schlumberger, Schlumberger Cyberflex Access™ Software Development Kit dan juga kit WinPractice, iaitu:

1. Cryptoflex Access Cards Programmer’s Guide

2. Cyberflex Access Cards Programmer’s Guide

3. Reference Manual For Payflex S

Bagi menilai kesahihan maklumat yang terkandung di dalam dokumen berkenaan, ujikaji dijalankan menggunakan beberapa keping kad-kad ujian yang dapat diperolehi dalam kit pembangunan perisian. Ujian dijalankan dengan menggunakan peranti pembaca SchlumbergerSema Reflex USB dalam sistem pengoperasian komputer Microsoft Windows 2000. Aturcara bagi menilai arahan-arahan APDU yang hendak dilaksanakan ke atas kad ujian telah ditulis di dalam bahasa pengaturcaraan Visual C++ menggunakan editor Microsoft Visual Studio Versi 6. Aturcara ini menggunakan fail antaramuka pengurus sumber winscard.lib yang merupakan salah satu komponen dalam perisian Microsoft Platform Software Development Kit.

Hasil pemerhatian yang diperolehi dibincangkan dalam bahagian berasingan, BAB 4 ANALISIS PERBANDINGAN TENTANG PERSAMAAN DAN PERBEZAAN OPERASI DALAM TIGA JENIS KAD.

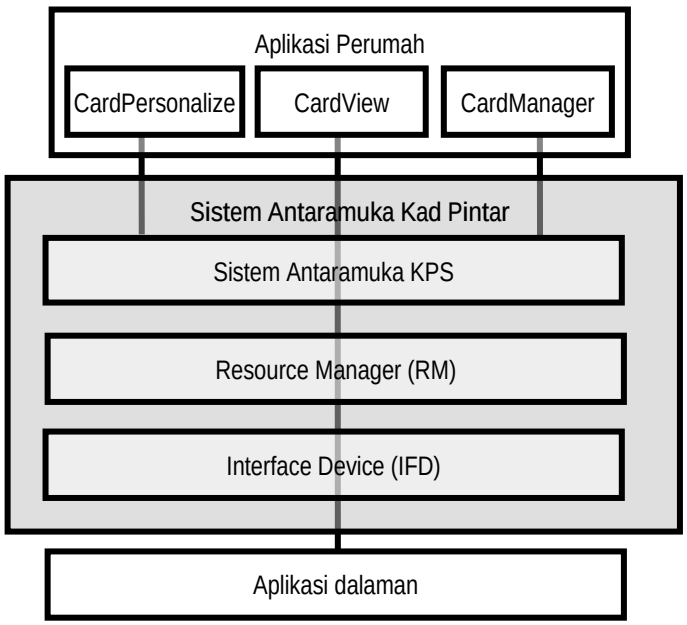
3.2 Membangunkan model sistem antaramuka

Hasil rujukan dalam kaedah 3.1 dijadikan sebagai satu sandaran bagi menghasilkan satu model rekabentuk antaramuka yang diberi nama Antaramuka Kad KPS (Kad Pintar Serbaguna) bagi menyelesaikan masalah keserasian operasi kad untuk tiga jenis kad, iaitu: Cryptoflex, Cyberflex dan Payflex.

Rajah 3-1 memperlihatkan bahagian-bahagian utama dalam model KPS yang terdiri daripada satu sistem antaramuka kad dan tiga contoh aplikasi perumah. Secara ringkasnya, rekabentuk sistem antaramuka KPS yang dibangunkan akan mempunyai ciri-ciri berikut :

a. Rekabentuk sistem adalah berorientasikan objek melalui penggunaan senibina COM *(Component Object Model*). Kelebihan rekabentuk berorientasikan objek berbanding kepada kaedah biasa pengaturcaraan

berprosedur ialah konsep pengaturcaraan ini lebih mudah difahami dan lebih mudah digunakan oleh pengguna.



Rajah 3-1 Bahagian-bahagian penting dalam model KPS

b. Ia mengandungi tahap API (*Application Programming Interface*) yang tinggi dengan subrutin berparameter yang lebih mudah difahami oleh pengguna, disediakan bagi menggantikan subrutin asas yang berasaskan format APDU. Protokol arahan APDU dalam pertukaran maklumat tidak tampak kepada pengguna. Dengan ini pengguna tidak lagi perlu mempelajari protokol arahan APDU yang rumit dan membebankan.

c. Ia boleh diintegrasikan dengan komponen-komponen sistem lain yang ditulis dalam pelbagai jenis bahasa pengaturcaraan (seperti C, C++, Visual Basic, Java, VBScript dan JScript) melalui penggunaan senibina IDL (*Interface Definition Language*).

d. Ia mempunyai objek antaramuka dengan ciri:

   i. am, sesuai untuk kesemua jenis kad

   ii. khas, sesuai untuk jenis kad tertentu sahaja.

Ini menjadikan ia sesuai digunakan untuk pembangunan kedua-dua bentuk sistem perisian, untuk pelbagai jenis kad (am) dan juga untuk satu jenis kad tertentu sahaja (khas).

Tahap keupayaan sistem antaramuka ini boleh dinilai dari segi kecekapan operasi sistem-sistem perisian kad yang dibangunkan dengan bercirikan kepada sifat-sifat operasi dalam ketiga-tiga kad. Model sistem perisian yang dipilih ialah sistem pengenalan diri yang mana kad pintar dilihat sebagai satu media pintar yang menyimpan pelbagai maklumat peribadi dan sebagai tanda pengenalan diri bagi pemegang kad berkenaan. Huraian tentang rekabentuk dan hasil pembangunan sistem dinyatakan dalam bahagian berasingan BAB 5 REKABENTUK DAN IMPLEMENTASI.

Hasil analisa perbandingan dalam BAB 4, satu rumusan telah diperolehi bahawa rekabentuk model antaramuka yang sesuai bagi kegunaan ketiga-tiga jenis kad yang dikaji perlu mempunyai dua bahagian antaramuka: am dan khusus. Satu model antaramuka yang diberi nama Antaramuka Kad KPS (Kad Pintar Serbaguna) dibangunkan dengan berasaskan kepada ciri-ciri am dan khusus yang terdapat dalam sistem pengoperasian kad pada setiap kad berkenaan.

Rekabentuk sistem

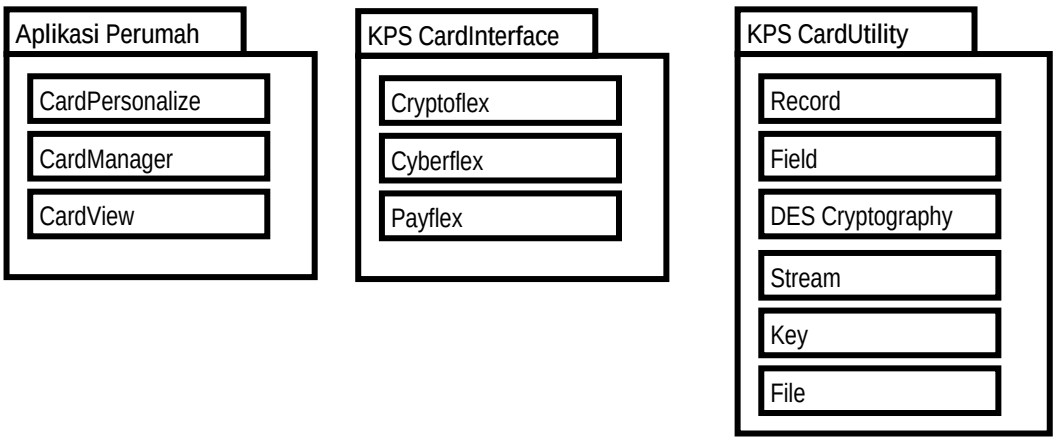
Tiga contoh sistem perisian perumah dibangunkan: CardPersonalize, CardManager dan CardView.

a. CardPersonalize adalah satu sistem perisian ringkas yang memperlihatkan contoh bagaimana seharusnya satu model aplikasi dalaman dapat dibangunkan dan diurus dalam ketiga-tiga jenis kad. Sistem berkenaan dibangunkan di dalam dua bahasa pengaturcaraan yang berlainan iaitu Visual Basic dan Visual C++.

b. CardView adalah sistem perisian yang memproses maklumat yang dibaca daripada aplikasi dalam kad-kad yang berlainan. Ia bertindak sebagai satu pelayan kepada sejumlah sistem perisian perumah yang dipasang dalam satu sistem komputer yang sama.

c. CardManager adalah sistem pengurusan pengeluaran kad pengenalan ahli yang dihubungkan kepada sumber maklumat daripada satu sistem pangkalan data. Ia menyediakan beberapa kemudahan-kemudahan seperti mencetak maklumat ahli pada permukaan plastik kad, menghapuskan sesuatu aplikasi dalaman yang sedia ada, menghasilkan aplikasi baru ke dalam kad, dan memindah maklumat daripada sistem pangkalan data ke dalam aplikasi tersebut.

Selain daripada itu, satu antaramuka tambahan yang diberi nama KPS CardUtility turut dibangunkan untuk menyediakan objek-objek tambahan yang difikirkan perlu dalam sistem perisian kad pintar, antaranya ialah Files, Records dan kryptografi DES (Data Encryption Standard). Ciri-ciri rekabentuk objek-objek berkenaan tiada mempunyai hubungan secara langsung dengan operasi peranti pembaca dan oleh sebab itu, mereka diasingkan daripada sistem antaramuka induk KPS CardInterface. Rajah 3-2 memperlihatkan komponen-komponen utama dalam pakej sistem perisian kad pintar yang akan dibangunkan.



Rajah 3-2 Komponen utama dalam pakej sistem perisian kad pintar KPS

3.3 Menghasilkan satu model keseragaman dalam rekabentuk antaramuka kad

Berasaskan kepada hasil penyelesaian dalam kaedah 3.2 untuk tiga jenis kad yang telah dipilih, satu andaian dibuat bahawa rekabentuk sistem yang sama boleh dikembangkan untuk menghasilkan modul antaramuka bagi jenis kad yang lain. Kaedah pemodelan objek dalam kaedah 3.2 digunakan sebagai satu sandaran dalam rekabentuk antaramuka bagi kad lain.

Untuk setiap kad baru yang ingin diperkenalkan, satu modul antaramuka baru perlu dihasilkan dan ditambah ke dalam sistem yang sedia ada. Apabila sebilangan besar kad baru ditambah, akan timbul suatu keadaan iaitu sejumlah modul antaramuka dipakai untuk pelbagai jenis kad dalam persekitaran sistem komputer yang sama. Keadaan ini memerlukan satu penyelesaian dibuat supaya sistem berupaya mengendalikan hubungan komunikasi antara sistem perisian perumah dengan pelbagai objek antaramuka dalam pelbagai modul. Sistem antaramuka perlu mempunyai ciri-ciri berikut:

a. Mampu mengenalpasti jenis kad yang sedang digunakan.

b. Mampu mengenalpasti jenis objek antaramuka yang sesuai dengan kad tersebut.

c. Mampu mengaktifkan objek antaramuka yang telah dikenalpasti itu yang mungkin disimpan dalam modul-modul yang berlainan.

Untuk menguji keberkesanan sistem, satu model antaramuka NewCardInterface dan satu model kad NewCard dihasilkan dan ditambah ke dalam sistem antaramuka kad yang sedia ada. Satu andaian dibuat, sekiranya kaedah ini boleh dipakai pada model kad yang diuji, kaedah ini seharusnya boleh dikembangkan untuk menghasilkan modul-modul antaramuka bagi kad-kad yang lain. Melalui pengembangan ini, satu sistem antaramuka untuk pelbagai kad dapat dihasilkan. Huraian tentang rekabentuk sistem dan kaedah pengujian yang dibuat dinyatakan dalam BAB 6 MODUL OBJEK ANTARAMUKA AM UNTUK KAD LAIN.

BAB 4 ANALISIS PERBANDINGAN TENTANG PERSAMAAN DAN PERBEZAAN OPERASI DALAM TIGA JENIS KAD

Bahagian ini menghuraikan tentang hasil kajian yang dijalankan bagi kaedah 3.1. Tiga aspek kajian tentang sifat sistem pengoperasian kad yang diberi tumpuan utama ialah:

a. Format arahan APDU (*Application Protocol Data Unit*)
b. Kaedah pengurusan fail
c. Format ACL *(Access Control Level*)

4.0 Ciri-ciri am sistem pengoperasian kad

Ciri-ciri sistem pengoperasian ketiga-tiga jenis kad yang dikaji memenuhi spesifikasi piawaian antarabangsa ISO7816. Spesifikasi ISO7816 menetapkan ciri-ciri berkaitan dengan sistem fail antaranya ialah struktur logik fail, format arahan operasi ke atas fail dan kawalan akses ke atas fail.

4.0.1 Struktur logik fail

Aplikasi kad disimpan di dalam ruangan memori kad. Data disusun di dalam struktur logik (fail) di bawah kawalan sistem pengoperasian kad. Identiti setiap fail dikenalpasti melalui satu integer positif bersaiz 2 bait yang dipanggil id fail. Id sesuatu fail biasanya ditakrifkan dalam format heksadekimal (contohnya 5F20h). Ada dua kategori fail untuk dua fungsi berlainan, iaitu:

a. fail asas EF (*elementary file*) berfungsi menyimpan data. Panggilan lain bagi fail asas ialah fail data.
b. fail dedikasi DF (*dedicated file*) berfungsi menyimpan sejumlah fail asas. Panggilan lain bagi fail dedikasi ialah direktori.

Sama seperti sistem fail MS-DOS, terdapat satu direktori induk yang menyimpan semua direktori lain dan fail data, yang juga dipanggil *direktori akar*. Lazimnya, dalam

setiap kad kosong, terdapat sekurang-kurangnya tiga fail penting yang disediakan oleh pengeluar kad iaitu:

a. Fail induk atau direktori akar, atau singkatannya MF (*Master File*)
b. Fail data kekunci keselamatan
c. Fail data yang mengandungi nombor siri kad

Direktori akar boleh mengandungi sehingga tiga paras subdirektori. Subdirektori tidak boleh dibina di bawah paras yang ketiga, seperti yang ditunjukkan dalam Rajah 4-1.

Terdapat tiga jenis fail data iaitu:

a. Fail jernih (*transparent file*) atau juga dikenali sebagai fail binari, untuk menyimpan sebarang data yang berbentuk binari.
b. Fail rekod berkitar untuk menyimpan rekod dalam satu kitaran. Apabila rekod terakhir telah diisi, data seterusnya akan disimpan dalam rekod pertama.
c. Fail rekod linear untuk menyimpan rekod secara jujukan linear.

Panjang bagi setiap rekod dalam sesuatu fail rekod berkitar adalah tetap, manakala panjang bagi setiap rekod dalam sesuatu fail rekod linear adalah tidak semestinya sama.

4.0.2 Model struktur fail bagi aplikasi dalaman

Terdapat tiga aspek penting yang mempengaruhi rekabentuk sesuatu aplikasi dalaman:

a. ciri pengurusan fail data
b. tahap keselamatan atau perlindungan akses ke atas fail data
c. ciri pengurusan kekunci keselamatan

Data bagi sesuatu aplikasi disimpan dalam fail dalam direktori tertentu dan dilindungi daripada diakses oleh sistem luaran melalui satu kawalan keselamatan oleh sistem