Chapter 1

Sistem Operasi Smartcard

1.1 Pengenalan SmartCard

Smart Card merupakan sebuah kartu plastik yang ditanamkan sebuah chip komputer dan dapat digunanakan utuk penyimpanan dan pertukaran data [5]. Saat ini, smartcard digunakan secara luas pada pemerintahan, perbankan, telekomunikasi, transportasi, hiburan, dll. Smartcard menjadi populer karena menyediakan mobilitas, robustness, serta keamanan bagi penggunanya. Ketahanannya terhadap kerusakan juga menjadikannya sebagai pilihan dalam perangkat komputasi bergerak [2].

Smartcard pada dasarnya merupakan sebuah sistem komputer lengkap, meskipun pada umumnya memiliki kemampuan komputasi yang terbatas. Smartcard memiliki microprosesor, sistem memory, serta IO untuk berkomunikasi dengan perangkat luar. Beberapa smartcard bahkan memiliki coprocessor untuk membantu mikroprosesor utama dalam mengerjakan fungsi-fungsi khusus, seperti kriptografi. [6].

Perbedaan yang paling mendasar antara smartcard dengan komputer biasa seperti PC adalah bahwa smartcard tidak memiliki human-machine interface sendiri sehingga tidak dapat berinteraksi langsung dengan pengguna. Interaksi dengan smartcard hanya dapat dilakukan melalui komputer lainnya yang bertindak sebagai host menggunakan perangkat khusus yang disebut card reader. Komputer yang bertindak sebagai host ini dalam istilah smartcard dinamakan juga sebagai terminal Terminal.

Terminal berkomunikasi dengan smartcard melalui protokol komunikasi khusus. Dua protokol komunikasi yang paling banyak digunakan untuk keperluan ini adalah protokol T=0 dan T=1 [3]. Komunikasi antara terminal dengan smartcard sendiri bersifat master dan slave [1]. Komunikasi diinisiasi oleh terminal dengan mengirimkan pesan Command ke smartcard,

dan smartcard membalas dengan mengirimkan pesan Response kembali ke terminal.

1.1.1 Penggunaan Smartcard

Smartcard telah digunakan pada berbagai bidang yang membutuhkan penyimpanan data yang ringkas.

- Administrasi Kependudukan

  Smartcard telah digunakan sebagai kartu identitas pada banyak negara. Salah satu negara yang mengadopsi smartcard sebagai kartu identitas adalah Indonesia melalui kartu e-KTP.

  Selain kartu identitas, smartcard juga digunakan pada Passport oleh beberapa negara termasuk Indonesia (khusus wilayah Batam).

  Pada beberapa negara, smartcard digunakan sebagai kartu izin mengemudi. Negara yang telah mengadopsi sistem ini misalnya Argentina.

- Keuangan

  Smartcard telah sejak lama digunakan sebagai media untuk melakukan transaksi perbankan (pembayaran) melalui kartu debit/kredit.

  Selain itu juga terdapat pada dompet elektronik yang dapat digunakan pada beberapa toko (merchant) atau *vending machine*. Untuk dompet elektronik ini tidak diperlukan sama sekali sambungan ke bank.

- Telekomunikasi

  Sebagian besar telepon selular menggunakan smartcard untuk identifikasi pengguna melalui k artu SIM.

- Transportasi

  Smartcard banyak digunakan pada sistem transportasi massal diseluruh dunia sebagai media pembayaran. Layanan TransJakarta dan KRL Commuter Jabodetabek telah mulai mengadopsi sistem berbasi smartcard ini.

- Pendidikan

  Smartcard telah digunakan pada beberapa sekolah/perguruan tinggi untuk absensi siswa, sekaligus untuk media pembayaran pada kantin, transportasi, serta layanan umum lainnya. Pemerintahan Kota Jakarta telah menerapkan Kartu Jakarta Pintar sebagai media penyalur bantuan bagi siswa.

- Kesehatan

  Smartcard juga telah digunakan pada bidang kesehatan untuk menyimpan riwayat kesehatan pasien, menggantikan model konvensional menggunakan kertas, menjadikannya lebih ringkas.

- Perkantoran/Hotel

  Smartcard telah banyak diterapkan sebagai kendali akses pada ruang-ruang tertentu pada gedung perkantoran ataupun pada kamar-kamar di Hotel.

1.1.2 Standarisasi Smartcard

Penggunaan smartcard yang terus berkembang dan semakin besar mengharuskan adanya standar yang mengatur penggunaan dan metode-metode yang digunakan pada smartcard. Beberapa standard yang mengatur hal ini diantaranya:

- ISO/IEC 7810

  Mengatur karakteristik fisik dari kartu identifikasi, yang digunakan juga pada smartcard

- ISO 7816

  Mengatur spesifikasi kartu identitas elektronik dengan *contact*. Standard ini terdiri dari sejumlah seri, dimulai dari 7816-1 hingga 7816-15. Penjelasan dari setiap seri ini diberikan pada Tabel 1.1.

- ISO/IEC 14443

  Mengatur spesifikasi kartu identitas elektronik tanpa *contact* atau *proximity card*. Standard ini terdiri dari sejumlah seri, dimulai dari 14443-1 hingga 14443-4. Penjelasan dari setiap seri ini diberikan pada Tabel 1.2.

- GSM 11.11-11-12

  Digunakan sistem telekomunikasi selular digital di Eropa, namun digunakan juga dibelahan dunia lainnya.

- Europay, MasterCard, and Visa (EMV)

  Mengatur penggunaan smartcard untuk sistem pembayaran

- International Airline Transportation Association (IATA) Resolution 791

  Mengatur penggunaan smartcard sebagai tiket elektronik

Seri	Keterangan
7816-1	Karakteristik fisik
7816-2	Dimensi dan lokasi *contact*
7816-3	Antarmuka elektrik dan protokol transmisi
7816-4	Organisasi, Keamanan dan Command untuk pertukaran
7816-5	Registrasi Penyedia Aplikasi
7816-6	Elemen data antar-industri untuk pertukaran
7816-7	Command antar-industri untuk Structured Card Query Language (SCQL)
7816-8	Command untuk operasi keamanan/kerahasiaan
7816-9	Command untuk manajemen kartu
7816-10	Sinyal elektrik dan ATR untuk kartu synchronous
7816-11	Verifikasi personal melalui metode biometrik
7816-12	Antarmuka elektrik dan prosedur operasi untuk USB
7816-13	Command untuk manajemen aplikasi
7816-15	Aplikasi Kriptografi Informasi

Table 1.1: Seri-seri Standard ISO/IEC 7816

Seri	Keterangan
14443-1	Karakteristik fisik
14443-2	Daya Frekuensi Radio dan antarmuka sinyal
14443-3	Initialisasi dan anti-*collision*
14443-4	Protokol Transmisi

Table 1.2: Seri-seri Standard ISO/IEC 14443

- PC/SC

  Mengatur spesifikasi hubungan antara smartcard reader dengan PC yang menjalankan sistem operasi windows

- G7

  Dikeluarkan oleh International Health Organization, mengatur penggunaan smartcard pada bidang kesehatan.

1.2 Pengenalan Sistem Operasi SmartCard

Sebagaimana pada sistem komputer lainnya, smartcard membutuhkan perangkat lunak untuk dapat bekerja. Tanpanya perangkat lunak, smartcard hanyalah sepotong plastik dengan mikroprosesor yang tertanam didalamnya.

Meskipun tidak seperti sistem operasi lengkap layaknya Windows ataupun

Unix, sistem operasi smartcard merupakan bagian yang sangat penting karena sistem operasi ini akan mengendalikan operasi-operasi dasar dari smartcard dan menjamin smartcard melaksanakan fungsinya dengan benar.

1.2.1 Trend dan Perkembangan Sistem Operasi Smartcard

Pada awal pengembangan smartcard di tahun 1980-an, perangkat lunak ini ditanamkan langsung kedalam EEPROM dari smartcard dan proses ini berlangsung pada saat pembuatan semikonduktor. Akibatnya, menjadi sulit (atau bahkan tidak mungkin sama sekali) melakukan perbaikan atau pengembangan apabila ditemukan kesalahan (bugs) atau kerentanan (vulnerability) pada perangkat lunak. Tidak ada pemisahan antara aplikasi dengan sistem operasi sehingga dibutuhkan perangkat lunak khusus untuk setiap aplikasi. Hal ini menyebabkan proses pengembangan aplikasi menjadi sulit dan tidak efisien.

1.2.2 Fungsi-fungsi utama sistem operasi smartcard

Secara umum, sistem operasi smart card bertanggung jawab dalam menangani [6]:

- mengirim dan menerima data dari dan ke smartcard.
- mengendalikan eksekusi command
- mengelola file
- mengelola dan mengeksekusi fungsi-fungsi kriptografi
- mengelola dan mengeksekusi kode program
- mengelola penggunaan kartu

lebih jauh lagi, sistem operasi smart card juga bertanggung jawab pada kendali akses, menjamin integritas data, serta pengelolaan kartu.

1.2.3 Jenis-jenis smartcard berdasarkan command sets

Berdasarkan command sets yang digunakan, sistem operasi smartcard dapat dibagi menjadi dua jenis, yaitu:

- sistem operasi smartcard penggunaan umum (general purpose), menyediakan sets command yang umum
- sistem operasi smartcard penggunaan khusus (dedicated), dengan command yang dirancang khusus hanya untuk suatu aplikasi tertentu

1.2.4 Tantangan dalam perancangan sistem operasi smartcard

Dengan keterbatasan yang dimiliki smartcard, berarti sistem operasinya juga harus dioptimasi sesuai dengan penggunaannya.

- Ruang Penyimpanan (memory) yang kecil

  Smartcard umumnya memiliki ruang penyimpanan (memory) yang kecil. Karenanya, sistem operasi untuk smart card harus dirancang seefisien mungkin untuk menghasilkan kode program dengan ukuran (footprint) yang kecil. Pada smartcard generasi awal, memory ini sangat kecil, hingga sistem operasi-nya harus ditulis dalam bahasa Assembly. Saat ini, memory smartcard telah semakin besar, dan memungkinkan penggunaan bahasa level yang lebih tinggi seperti C atau bahkan Java. Sistem operasi smart card terbaru saat ini umumnya diimplementasikan dalam bahasa C, dan bahasa ini juga yang akan digunakan dalam thesis ini.

- Robust dan reliable

  Selain itu, smart card harus dirancang agar robust and reliable. Hal ini disebabkan smart card seringkali digunakan dalam lingkungan yang tidak aman (sterile) sehingga dapat dengan mudah menyebabkan kerusakan ataupun interferensi pada hardwarenya. Sebagian besar dari sistem operasi smart card yang ada juga disimpan di dalam ROM, sehingga menjadi tidak mungkin (sulit) untuk memperbaikinya apabila terjadi kesalahan setelah manufacture.

- Aman

  Smart card juga seringkali harus digunakan pada domain yang menuntut keamanan tinggi. Untuk itu sistem operasi smart card juga harus dirancang dengan teliti untuk bebas dari celah dan keamanan dan kerentanan dari serangan. security during program execution and protected access to data have the highest priority. Keamanan selama eksekusi program dan akses ke data terproteksi manjadi prioritas utama. Hal ini seringkali mengharuskan rancangan dan implementasi sistem

operasi smartcard menjadi tergantung pada hardware yang digunakan, seperti dalam menangani state EEPROM untuk menjamin integritas dari data yang disimpan. Akibatnya, perancangan smart card OS tidak pernah bisa hardware-independent secara penuh, sebagaimana diinginkan oleh pembuat software.

- Kemampuan Komputasi yang rendah

  Keterbatasan lainnya yang dimiliki smart card adalah kemampuan pemrosesan data dari mikroprosesor yang relatif rendah. Sebaliknya, smartcard diharapkan untuk dapat melayani permintaan dengan segera (tidak lebih dari 5 detik sesuai standar yang banyak digunakan). Untuk itu kode program harus ditulis menggunakan algoritma yang efektif. Bagian yang membutuhkan waktu pemrosesan yang relatif lama biasanya adalah pada algoritma kriptografi. Untuk itu smartcard terbaru biasanya telah dilengkapi dengan co-processor kriptografi.

1.2.5 Sistem Operasi Smartcard - Beberapa Contoh

Tabel 1.3 menampilkan beberap contoh sistem operasi smarcard beserta pembuatnya [6]

Sistem Operasi	**Pembuar**
GemXpresso (Javacard), GPK, MPCOS	Gemplus
STARCOS, STARSIM, STARDC	Giesecke
Devrient	
Multos	Maosco
AuthentIC, SIMphonic	Oberthur
Micardo	Orga
Cyberflex (Javacard), Multiflex, Payflex	Schlumberger
CardOS	Siemens
TCOS	Telesec

Table 1.3: Beberapa contoh sistem operasi smartcard yang banyak ditemui

Hampir semua sistem operasi smartcard bersifat *proprietary*, sehingga sulit untuk mengetahui internal dari sistemnya. Namun beberapa vendor memberikan penjelasan singkat mengenai sistem operasi mereka.

Javacard

MultOS [9]

MULTOS adalah sistem operasi smartcard yang dapat dipakai untuk berbagai aplikasi. MULTOS sendiri adalah standard terbuka yang pengembangannya diawasi oleh MULTOS Consortium. Satu hal yang membedakan MULTOS dari sistem operasi smartcard lainnya adalah bahwa ia mengimplementasikan mekanisme berbasis kriptografi kunci publik yang telah dipatenkan, dimana pembuatan, penerbitan, dan pembaruan seluruh MULTOS berada dibawah kendali penerbit menggunakan sertifikat digital.

Kendali dilakukan melalui Key Management Authority (KMA), sebuah *certificate authority* (CA) khusus. KMA akan memberikan informasi kriptografi yang diperlukan kepada penerbit kartu yang akan mengikat kartu pada penerbit, menginisialisasi penggunaannya, dan menghasilkan sertifikat untuk izin *loading* dan *deleting* aplikasi dibawah kendali penerbit kartu. Pembuat aplikasi dapat meminta dan mem-verifikasi sertifikat kunci publik dari setiap penerbit kartu, dan meng-enkripsi kode aplikasi mereka serta data personalisasi menggunakan kunci tersebut, yang lalu ditanda tangani secara digital menggunakan kunci privat dari pembuat aplikasi. KMA, atas permintaan penerbit kartu, akan menanda tangani kunci publik pembuat aplikasi serta kode aplikasinya, dan membuat sertifikat untuk meng-otorisasi aplikasi pada kartu yang akan diterbitkan. Dengan metode ini, aplikasi menjadi terjaga baik integritasnya maupun kerahasiaannya, dan dapat di-*load* ke kartu tanpa perlu kunci simetrik apapun.

Terdapat mesin virtual (VM) pada implementasi MULTOS yang berfungsi menyediakan:

- Application Runtime Environment
- Memory Management
- Application Loading and Deleting

Bibliography

[1] Chen Yuqiang, Guo Jianlan, Hu Xuanzi, and Liu Liang,"Design and Implementation of Smart Card COS," *Computer Application and System Modelling(ICCASM), 2010 International Conference on*,22-24 Oct. 2010.

[2] Damien Deville, Antoine Galland, Gilles Grimaud, Sebastien Jean,"Smart Card Operating Systems: Past, Present and Future," *5 th NORDU/USENIX Conference, In Proceedings of the*, 2003.

[3] George Selimis, Apostolos Faournaris, George Kostopoulos, and Odysseas Koufopavlou,"Software and Hardware Issue in Smart Card Technology," *Communications Surveys & Tutorial, IEEE*,3rd Quarter 2009.

[4] Heng Guo,"Smart Cards and their Operating Systems."

[5] Mohamed Mohandes,"A Smart Card Management and Application System," *Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on*, 10-12 Dec. 2010.

[6] R. Wolfgang and E. Wolfgang, *Smart Card Handbook*, John Wiley and Sons, 3rd Edition, 2004.

[7] R. Wolfgang, *Smart Card Applications: Design models for using and programming smart cards*, John Wiley and Sons, 2007.

[8] Jorge Ferrari, Robert Mackinnon, Susan Poh, Lakshman Yatawara, *Smart Cards: A Case Study*, IBM International Technical Support Organization, 1998.

[9] ,*MultOS*,, .