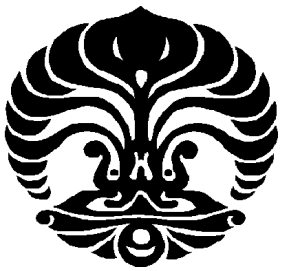
RANCANGAN KEAMANAN DATA SISTEM SMARTCARD KESEHATAN SESUAI KEBUTUHAN DI INDONESIA

Disusun sebagai Laporan Tugas Akhir

Oleh :

Christine Sariasih

1295000113



Fakultas Ilmu Komputer

Universitas Indonesia

Depok

1999

LEMBAR PERSETUJUAN

SKRIPSI	:RANCANGAN KEAMANAN DATA SISTEM SMARTCARD KESEHATAN SESUAI KEBUTUHAN DI INDONESIA.
NAMA	: CHRISTINE SARIASIH
NPM	: 1295000113

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

DEPOK, …….

Mengetahui,

dr Iik Wilarso	Bob Hardian, MKom
Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II

KATA PENGANTAR

Puji dan syukur saya panjatkan kepada Tuhan Yang Maha Kuasa, karena berkat dan anugerah-Nya sehingga saya dapat menyelesaikan tugas akhir dengan judul "Rancangan Kemaanan Data Sistem Smartcard Kesehatan Sesuai Kebutuhan Di Indonesia". Tugas akhir ini merupakan salah satu syarat untuk memperoleh kelulusan untuk mahasiswa Fakultas Ilmu Komputer UI pada jenjang pendidikan tingkat S1.

Selanjutnya saya sampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Bapak dan Mama, yang telah mendidik dan membesarkan saya dengan penuh pengorbanan dan kasih sayang.
2. Bapak FX. Nursalim Hadi Ph.D, selaku pembimbing akademis sejak saya masuk dan menuntut ilmu di Fakultas Ilmu Komputer UI dan pembimbing awal tugas akhir yang telah memberikan arahan dalam mengerjakan tugas akhir ini.
3. Bapak dr. Iik Wilarso dan Bapak Bob Hardian M.Kom, selaku pembimbing tugas akhir yang banyak memberikan arahan dalam mengerjakan tugas akhir ini.
4. Arianto Mukti Wibowo SKom, selaku asisten pembimbing tugas akhir yang telah membimbing saya dalam mengerjakan tugas akhir ini.
5. Bapak Petrus Mursanto, selaku pengganti pembimbing akademis pada akhir masa perkuliahan saya.
6. Bapak Hendrik Makaliwe, Msc, atas dorongan untuk mengambil tugas akhir.
7. B'Posma, Ully, B'Lexy, atas dukungan dan cinta kasihnya.
8. Teman-teman angkatan 95 : Ada, Elis, Dian, Renny, Intan, Ida dan Martha.
9. Teman-teman di Posa Fasilkom : Rotua, Anita, Engel, Martin dan Daniel.
10. Teman-teman Angkatan 98 : Wisnu, Sukma, Rio, Dalton, Kiton, Jeffree, Sandy, Hanna, Anna dan Soetrisno.
11. Segenap staf, dosen, karyawan dan rekan-rekan mahasiswa lain baik di lingkungan Fasilkom UI maupun lingkungan UI yang tidak dapat saya sebutkan satu persatu, atas segala sumbangsih, perhatian dan dukungannya.

Saya menyadari tugas akhir ini masih banyak kekurangannya sehingga saran dan kritik pembaca merupakan masukan yang sangat berguna. Semoga laporan tugas akhir ini

dapat berguna bagi pihak-pihak yang berkepentingan.

Depok, 1999

Penulis

ABSTRAKSI

Informasi rekam medis seseorang merupakan salah satu faktor yang menentukan kualitas pelayanan yang diberikan oleh pusat pelayanan kesehatan kepada pasiennya, oleh sebab itu informasi rekam medis ini harus selalu ada ketika dibutuhkan[PerMen89]. Kerahasiaan informasi rekam medis sangat penting karena informasi ini menjelaskan hubungan yang khusus antara pasien dan dokter, yang wajib dilindungi dari pembocoran sesuai dengan kode etik kedokteran dan peraturan perundangan yang berlaku[PerPem66]. Berdasarkan penelitian sebelumnya, teknologi kartu pintar (*smartcard*) menawarkan kemudahan dan keamanan penyimpanan data karena adanya mekanisme enkripsi data sebelum data tersebut disimpan di dalam memori, serta adanya pin (kode rahasia) yang menjaga data tersebut agar tidak dibaca oleh pihak yang tidak berwenang[ISO7816-95]. *Smartcard* juga dapat dibawa dengan mudah sehingga menunjang ketersediaan data kapan saja ketika dibutuhkan.

Tugas akhir ini bertujuan untuk merancang suatu sistem rekam medis yang sesuai dengan ketentuan-ketentuan rekam medis di Indonesia, menjamin keamanan data, mudah dibawa oleh pemilik, memaksimalkan pelayanan kesehatan untuk kondisi gawat darurat, dan mempercepat serta meningkatkan pelayanan kesehatan rawat jalan pada satu rumah sakit atau bahan rujukan antar rumah sakit.

Untuk mencapai tujuan tersebut, maka penulis akan mempelajari peraturan pemerintah tentang rekam medis dan melakukan observasi lapangan di rumah sakit, mengenal beberapa sistem rekam medis dengan menggunakan *smartcard* yang ada di negara–negara lain sehingga diperoleh sistem *smartcard* kesehatan yang paling aman dari antara sistem-sistem tersebut. Berdasarkan sistem yang paling aman tersebut akan dirancang suatu protokol sistem *smartcard* kesehatan yang sesuai dengan tujuan di atas. Rancangan protokol tersebut akan diuraikan secara jelas dan menitikberatkan pada keamanan data.

Hasil dari tugas akhir ini adalah rancangan suatu sistem *smartcard* kesehatan yang memenuhi peraturan kesehatan Indonesia, menjamin keamanan dan kerahasiaan data, mempercepat dan meningkatkan pelayanan kesehatan, serta dapat digunakan oleh berbagai perangkat lunak aplikasi *smartcard* kesehatan (*interoperability*).

DAFTAR ISI

LEMBAR PERSETUJUAN ..... **ii**

KATA PENGANTAR ..... **iii**

ABSTRAKSI ..... **v**

DAFTAR ISI ..... **vi**

DAFTAR GAMBAR ..... **ix**

DAFTAR TABEL ..... **x**

BAB I PENDAHULUAN **1**

I.1 LATAR BELAKANG MASALAH 1
I.2 TUJUAN PENELITIAN 2
I.3 RUANG LINGKUP DAN PEMBATASAN MASALAH 2
I.3.1 Ruang Lingkup : 2
I.3.2 Pembatasan Masalah : 3
I.4 METODE PENELITIAN 3
I.5 SISTEMATIKA PENULISAN 4

BAB II LANDASAN TEORI **6**

II.1 REKAM MEDIS 6
II.2 KRIPTOGRAFI 7
II.2.1 Kunci Simetris 8
II.2.2 Kunci Asimetris 8
II.2.3 Fungsi *Hash* Satu Arah 8
II.2.4 Tanda Tangan Digital 9
II.2.5 Masalah Pertukaran Kunci Publik 9
II.2.6 Sertifikat Digital 10
II.3 SMARTCARD 10
II.3.1 Jenis Memori Pada *Smartcard* 11
II.3.2 Tipe-tipe *Smartcard* 11
II.3.3 Komunikasi antara *Smartcard* dan Aplikasi 13
II.3.4 Format APDU 14
II.3.5 Serangan Pada *Smartcard* 16

II.3.5.1 Serangan Secara logika 17
II.3.5.2 Serangan Secara Fisik 19
II.3.5.2.1 Dumb Mouse 20
II.3.6 Serangan Pertukaran Pesan Melalui Jaringan Komputer 21
II.4 STANDAR INTEROPERABILITY SMARTCARD KESEHATAN 22
II.4.1 Modul dan Antar Muka Sistem *Smartcard* Kesehatan 23
II.4.2 Secure Socket Layer (SSL) 25

BAB III ANALISIS KEBUTUHAN RANCANGAN SISTEM SMARTCARD KESEHATAN SESUAI KEBUTUHAN DI INDONESIA 28

III.1 ANALISIS KONDISI SISTEM REKAM MEDIS DI INDONESIA 28
III.2 DESKRIPSI UMUM SISTEM SMARTCARD KESEHATAN YANG TELAH DIIMPLEMENTASIKAN 32
III.2.1 Alur Penggunaan Data Rekam Medis 33
III.2.2 Ukuran *Smartcard* 38
III.2.3 Perangkat Lunak Aplikasi 38
III.2.4 Keamanan Smartcard 39
III.2.5 Pencatatan 40
III.2.6 Jenis Aplikasi *Smartcard* Kesehatan 40
III.3 PERBANDINGAN SISTEM SMARTCARD KESEHATAN DI LUAR NEGERI DENGAN KONDISI-KONDISI DI INDONESIA 40
III.4 ANALISIS KEBUTUHAN UMUM *SMARTCARD* KESEHATAN YANG SESUAI KEBUTUHAN DI INDONESIA 50

BAB IV RANCANGAN SISTEM SMARTCARD KESEHATAN SESUAI KEBUTUHAN DI INDONESIA 55

IV.1 SPESIFIKASI RANCANGAN 55
IV.1.1 Solusi Awal 55
IV.1.2 Alur Penggunaan Data Rekam Medis Lapisan Atas 59
IV.1.2.1 Gawat Darurat 59
IV.1.2.2 Bahan Rujukan/Rawat Jalan 61
IV.1.2.3 Pengiriman Data Selesai Proses Pengobatan Ke *Card Centre* 62
IV.1.2.4 Dokter /Rumah Sakit Meminta Data Rekam Medis Ke Rumah Sakit Atau Pasien Meminta Data Rekam Medis Ke Card Centre 64
IV.1.2.5 Pembuatan *Smartcard* Baru/ *Smartcard* Hilang 65
IV.1.3 Konfigurasi Sistem 67
IV.1.4 *Smartcard* Yang Digunakan 73
IV.1.5 Rancangan Pada *Smartcard* 73
IV.1.5.1 Arsitektur Skema Direktori 73
IV.1.5.2 Arsitektur Kemanan *Smartcard* 75
IV.1.5.3 Rancangan Struktur *File* 77

IV.1.5.4 Rancangan Perangkat Lunak Sistem *Smartcard* Kesehatan yang Sesuai Standar *Interoperability* 78
IV.1.6 Rancangan Pengiriman Data Rekam Medis Lewat Jaringan 81
IV.1.7 Kriptanalisis 86
IV.2 ANALISIS SISTEM DENGAN PEMENUHAN KEBUTUHAN DI INDONESIA..... 89
BAB V KESIMPULAN DAN SARAN 92
V.1 KESIMPULAN 92
V.2 SARAN 94

DAFTAR GAMBAR

GAMBAR II.1. CONTOH SERTIFIKAT DIGITAL 10
GAMBAR II.2. BENTUK *SMARTCARD* 11
GAMBAR II.3. DELAPAN TITIK KONTAK 12
GAMBAR II.4. *COMMAND* APDU 15
GAMBAR II.5. RESPON APDU 16
GAMBAR II.6. *DUMB MOUSE* 20
GAMBAR II.7. PENDEKATAN MODULAR UNTUK SISTEM *SMARTCARD* KESEHATAN YANG *INTEROPERABILITY* 23
GAMBAR II.8. SECURITY HANDSHAKE 26
GAMBAR III.1. ALUR PENGGUNAAN DATA UNTUK RAWAT JALAN SISTEM *SMARTCARD* KESEHATAN 36
GAMBAR III.2. ALUR PENGIRIMAN DATA REKAM MEDIS LEWAT JARINGAN KOMPUTER PADA SISTEM *SMARTCARD* KESEHATAN 38
GAMBAR IV.1. INFORMASI DATA LOGIK *SMARTCARD* PROFESIONAL 57
GAMBAR IV.2. INFORMASI DATA LOGIK *SMARTCARD* PASIEN 57
GAMBAR IV.3. DIAGRAM ALUR DATA UNTUK KEADAAN GAWAT DARURAT 60
GAMBAR IV.4. DIAGRAM ALUR DATA UNTUK KEPERLUAN RAWAT JALAN 61
GAMBAR IV.5. DIAGRAM ALUR DATA PENGIRIMAN DATA REKAM MEDIS KE *CARD CENTRE* MELALUI JARINGAN KOMPUTER 63
GAMBAR IV.6. ALUR DATA PENGIRIMAN DATA MELALUI JARINGAN KOMPUTER 64
GAMBAR IV.7. DIAGRAM ALUR DATA PEMBUATAN *SMARTCARD* BARU 66
GAMBAR IV.8. KONFIGURASI SISTEM *SMARTCARD* KESEHATAN 68
GAMBAR IV.9. MEMBAGI SISTEM MENJADI KOMPONEN UNTUK PENGGUNA DAN KARTU 70
GAMBAR IV.10. SKEMA DIREKTORI DI *SMARTCARD* 75
GAMBAR IV.11. DIAGRAM PENGIRIMAN DATA LEWAT JARINGAN 85

DAFTAR TABEL

TABEL III.1. PENJELASAN ELEMEN DIAGRAM ALUR DATA 34
TABEL III.1. HASIL STUDI PERBANDINGAN SISTEM-SISTEM *SMARTCARD* KESEHATAN YANG DIANALISIS 49
TABEL III.1. PENJELASAN SISMBOL-SIMBOL DALAM PROTOCOL SISTEM *SMARTCARD* KESEHATAN SESUAI KEBUTUHAN DI INDONESIA 82

BAB I
PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, tujuan, ruang lingkup dan pembatasan masalah, metode penelitian yang dilakukan, dan sistematika penulisan tugas akhir ini.

I.1 LATAR BELAKANG MASALAH

Rekam medis adalah berkas yang berisi catatan, dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain kepada pasien pada sarana pelayanan pasien[PerMen89]. Informasi rekam medis merupakan suatu informasi penting seseorang yang seharusnya dimiliki oleh orang tersebut setiap saat sehingga dapat tersedia jika dibutuhkan kapan saja dan dimana saja. Informasi ini penting untuk menunjang pelayanan kesehatan yang diberikan dalam hal kecepatan dan keakuratan. Tata kerja rekam medis di rumah sakit bertujuan untuk terlaksananya pengaturan kegiatan rekam medis dengan tepat, cepat dan benar[PerMen89]. Hal penting dari pencatatan informasi rekam medis ini adalah ketersediaannya saat dibutuhkan dan sifat kerahasiaannya. Informasi dalam rekam medis bersifat rahasia karena hal ini menjelaskan hubungan yang khusus antara pasien dan dokter yang wajib dilindungi dari pembocoran sesuai dengan kode etik kedokteran dan peraturan perundangan yang berlaku[PerPem86].

Teknologi *smartcard* menawarkan kemudahan dan keamanan penyimpanan data karena adanya mekanisme enkripsi data sebelum data tersebut disimpan di dalam memori, serta adanya pin (kode rahasia) yang menjaga data tersebut agar tidak dibaca oleh pihak yang tidak berwenang. Setiap *smartcard* telah diprogram oleh perusahaan yang mengeluarkannya atau dilengkapi dengan sistem operasi. Sistem operasi ini menyediakan bahasa/perintah yang dimengerti oleh *smartcard* tersebut.

Keunggulan *smartcard* dalam hal : kemudahan pengaksesan data, keamanan penyimpanan data, perlindungan data dari pihak-pihak yang tidak berwenang, serta fleksibilitas untuk dibawa dengan mudah dalam kegiatan sehari-hari, telah mendorong penggunaan teknologi ini diterapkan di sektor kesehatan untuk menyimpan data rekam medis pasien. Keuntungan yang dapat diperoleh dengan penggunaan *smartcard* kesehatan ini pada proses pengobatan adalah : menyimpan kerahasiaan data pemilik *smartcard*, menyediakan informasi penting dalam keadaan darurat, bahan rujukan, membantu petugas kesehatan melakukan tindakan kesehatan dengan benar dan mengurangi waktu pasien dalam menyelesaikan masalah administrasi di rumah sakit.

Keterbatasan *smartcard* pada saat ini adalah dalam hal memori. Dalam perkembangan ke masa depan, tidak tertutup kemungkinan bahwa jumlah memori yang disediakan dalam *smartcard* akan semakin bertambah. Semakin bertambahnya memori maka harga *smartcard* juga akan semakin bertambah, namun kemampuan *smartcard* dalam hal menyimpan dan mengenkripsi data akan semakin bertambah pula.

I.2 TUJUAN PENELITIAN

Tujuan penelitian tugas akhir ini adalah untuk merancang sistem *smartcard* kesehatan yang sesuai dengan kebutuhan dan peraturan di Indonesia dengan mengacu pada teknologi sistem *smartcard* kesehatan yang sudah diimplementasikan di luar negeri.

I.3 RUANG LINGKUP DAN PEMBATASAN MASALAH

I.3.1 Ruang Lingkup :

Tugas akhir ini melingkupi :

1. Mempelajari peraturan pemerintah Indonesia tentang rekam medis dan observasi lapangan proses penggunaan data rekam medis untuk proses pengobatan di rumah sakit.

2. Mempelajari beberapa aplikasi sistem *smartcard* kesehatan yang diimplementasikan di negara lain.
3. Merancang sistem *smartcard* kesehatan yang sesuai dengan kebutuhan dan peraturan di Indonesia dengan mengacu pada teknologi sistem *smartcard* kesehatan yang sudah diimplementasikan di luar negeri.

I.3.2 Pembatasan Masalah :

Pembatasan masalah pada tugas akhir ini adalah :

1. Teori kriptografi dan teknologi *smartcard* dibahas secara umum, tidak lagi secara rinci karena penelitian terhadap kedua hal tersebut sudah dilakukan pada penelitian-penelitian sebelumnya.
2. Rancangan sistem *smartcard* kesehatan pada tugas akhir ini lebih bertitik berat pada aspek teknologi keamanan data, baik keamanan data yang disimpan dalam *smartcard* maupun keamanan data waktu dikirimkan lewat jaringan komputer. Dengan demikian aspek bisnis dari rancangan tersebut tidak dibahas dalam tugas akhir ini.
3. Tidak mengimplementasi rancangan sistem *smartcard* kesehatan yang dihasilkan.

I.4 METODE PENELITIAN

Penelitian dimulai dengan melakukan observasi terhadap sistem rekam medis di rumah sakit dan mempelajari peraturan-peraturan pemerintah tentang rekam medis di Indonesia. Selanjutnya mempelajari secara umum aplikasi sistem-sistem *smartcard* kesehatan yang telah diimplementasikan di negara lain.

Kemudian penelitian diteruskan dengan mempelajari teknologi *smartcard* dan teori kriptografi yang digunakan *smartcard* untuk menjamin keamanan penyimpanan data dari pihak-pihak yang tidak memiliki otoritas. Selain itu juga mempelajari spesifikasi sistem *smartcard* kesehatan yang *interoperability* yaitu jenis sistem *smartcard* kesehatan yang dapat membaca berbagai sistem *smartcard* kesehatan dari *vendor* yang berbeda. Selanjutnya penelitian dilanjutkan dengan analisis kebutuhan umum yang diperlukan oleh sistem *smartcard* kesehatan di

Indonesia. Berdasarkan analisis kebutuhan umum tersebut ditetapkan kriteria-kriteria suatu sistem *smartcard* kesehatan yang sesuai dengan peraturan dan kebutuhan di Indonesia.

Kriteria-kriteria tersebut digunakan untuk melakukan perbandingan sistem-sistem *smartcard* kesehatan yang ada di luar negeri sehingga didapat suatu sistem *smartcard* kesehatan yang paling mendekati peraturan dan kebutuhan di Indonesia. Sistem ini digunakan sebagai solusi awal untuk merancang protokol sistem *smartcard* kesehatan kesehatan.

Berdasarkan sistem hasil perbandingan dirancang suatu sistem *smartcard* kesehatan yang memenuhi peraturan dan kebutuhan di Indonesia. Teknologi pengamanan data pada *smartcard* dalam sistem ini dianalisis dengan menggunakan teori kriptografi. Transaksi pada sistem ini diuraikan dan dianalisis segi keamanan datanya.

Kemudian diambil kesimpulan rancangan sistem *smartcard* kesehatan apakah sudah dapat memenuhi semua spesifikasi yang sesuai dengan kondisi di Indonesia. Selanjutnya penulis mengajukan saran pengembangan rancangan protokol dalam tugas akhir ini di masa depan atau sebagai langkah penyempurnaan rancangan protokol ini.

I.5 SISTEMATIKA PENULISAN

Sistematika penulisan tugas akhir ini adalah sebagai berikut :

Bab I Pendahuluan -- membahas latar belakang masalah, tujuan penelitian, ruang lingkup dan pembatasan masalah, metode penelitian, dan sistematika penulisan tugas akhir ini.

Bab II Landasan Teori – membahas landasan-landasan teori yang diperlukan untuk merancang sistem *smartcard* kesehatan yang memenuhi spesifikasi kebutuhan di Indonesia. Pertama-tama bab ini membahas tentang definisi rekam medis, setelah itu bab ini membahas secara umum pengenalan terhadap kriptografi dan *smartcard*, dan sebagai bagian terakhir membahas mengenai standar spesifikasi sistem *smartcard* kesehatan yang *interoperability.*

Bab III Analisis Kebutuhan Rancangan Sistem *Smartcard* Kesehatan Sesuai Kebutuhan di Indonesia – menganalisa kebutuhan umum rancangan sistem

smartcard yang memenuhi kebutuhan di Indonesia dengan melakukan observasi ke rumah sakit dan mempelajari peraturan pemerintah tentang rekam medis. Kebutuhan-kebutuhan umum tersebut kemudian digunakan sebagai faktor-faktor perbandingan dalam membandingkan sistem-sistem *smartcard* kesehatan yang sudah diimplementasikan di luar negeri. Dari hasil perbandingan tersebut diperolehlah kesimpulan spesifikasi sistem *smartcard* kesehatan yang sesuai kebutuhan di Indonesia.

Bab IV Rancangan Sistem *Smartcard* Kesehatan Sesuai Kebutuhan di Indonesia – membahas secara rinci rancangan sistem *smartcard* kesehatan sesuai dengan spesifikasi yang didefinisikan di bab sebelumnya. Kemudian dianalisis apakah sistem *smartcard* kesehatan tersebut sesuai dengan kebutuhan di Indonesia.

Bab V Kesimpulan dan Saran Pengembangan – bab ini menyimpulkan hasil penelitian dan saran pengembangan di masa depan terhadap rancangan yang dihasilkan.

BAB II
LANDASAN TEORI

Bab ini menjelaskan hal-hal yang menjadi landasan teori dalam merancang sistem *smartcard* kesehatan di Indonesia. Terlebih dahulu dibahas mengenai definisi rekam medis.

II.1 REKAM MEDIS

Definisi rekam medis adalah keterangan baik yang tertulis maupun terekam, dan memuat informasi yang cukup dan akurat tentang identitas pasien, anamnesis, pemeriksaan, penentuan fisik, perjalanan penyakit, laboratorium, diagnosis, segala pelayanan dan tindakan medis serta proses pengobatan yang diberikan kepada pasien, dan dokumentasi hasil pelayanan; baik yang dirawat inap, rawat jalan maupun pelayanan gawat darurat di suatu sarana pelayanan kesehatan[PerMen89]. Sedangkan definisi e*lektronic medical record* adalah data rekam medis yang diatur oleh suatu badan tertentu seperti : rumah sakit, klinik, atau suatu jaringan komputer sehingga antar badan tersebut dapat saling beroperasi[MRI99].

Electronic medical record[MRI99] harus memiliki fungsi-fungsi penting sebagai berikut :

- Terdapat sistem yang dapat mengidentifikasikan semua informasi pasien yang ada dalam ruang lingkup suatu badan tertentu.
- Menjamin semua informasi pasien tersedia bagi para petugas kesehatan dalam ruang lingkup suatu badan tertentu. Termasuk harmonisasi data, penyimpanan data, teknik data *mining*, mesin antar muka, jaringan, dsb. Hal ini bertujuan agar antar badan yang satu dengan badan yang lain dapat saling beroperasi.
- Mengimplementasikan ketentuan perangkat lunak, struktur dan antar muka sistem sehingga dokter, perawat atau petugas kesehatan lainnya terbiasa menggunakan

komputer untuk memasukkan data atau untuk berinteraksi dengan program dalam mengambil keputusan.

- Membuat keamanan sistem. Jika belum ada hukum nasional, maka badan tersebut harus mendefinisikan ketentuan hak (kerahasiaan, akses data rekam medis dan mengubah informasi pasien).

Keamanan sistem yang harus diimplementasikan :

- Kontrol akses : dapat menggunakan *password* atau *biometric* untuk mengotentikasi dan mengklasifikasikan pengguna sesuai dengan otorisasi mereka dalam mengakses informasi dan menggunakan fungsi tertentu.
- Tanda tangan elektronik : sistem yang memperbolehkan pihak asli (petugas kesehatan atau alat akses data) untuk membubuhkan tanda tangan elektronik terhadap suatu masukan dan mendeteksi masukan-masukan yang telah diubah.
- Integritas data : setelah proses perbaikan, tidak boleh ada informasi yang hilang atau diubah dengan cara apapun, perbaikan dibuat berdasarkan persetujuan.
- Pemeriksaan : pemeriksaan lengkap terhadap akses ke suatu data dan tambahan lain yang dibuat dalam data.
- Ketersediaan : sistem harus dirancang untuk tersedia 24 jam sehari, 7 hari seminggu

II.2 KRIPTOGRAFI

Bagian ini membahas kriptografi yang merupakan alat untuk melakukan pengamanan data dalam sistem *smartcard* kesehatan. Kriptografi (*cryptography*) merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Kritptanalisis (*cryptanalysis)* merupakan ilmu dan seni pembongkaran pesan, data, atau informasi rahasia seperti di atas. Kriptologi (*cryptology*) adalah panduan dari kriptografi dan kriptanalist[Schn96]. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan dalam bahasa sandi (*ciphertext*). Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

Berikut ini adalah hal-hal penting yang dicakup dan sering dibahas dalam teori kriptografi.

II.2.1 Kunci Simetris

Ini adalah jenis kriptografi yang paling umum digunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis. Siapapun yang memiliki kunci tersebut – termasuk pihak-pihak yang tidak diinginkan – dapat membuat dan membongkar rahasia *ciphertext*. Contoh algoritma kunci simetris yang terkenal adalah DES (*Data Encryption Standard*)[Schn96].

II.2.2 Kunci Asimetris

Kunci asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu – dalam hal ini kunci privat – untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (merupakan singkatan penemunya yakni Rivest, Shamir dan Adleman).

II.2.3 Fungsi *Hash* Satu Arah

Fungsi *hash* satu arah (*one-way hash function*) digunakan untuk membuat sidik jari (*fingerprint*) dari suatu dokumen atau pesan M. Pesan M (yang besarnya dapat bervariasi) yang akan di-*hash* disebut *pre-image*, sedangkan outputnya yang memiliki ukuran tetap, disebut *hash-value* (nilai *hash*). Fungsi *hash* dapat diketahui oleh siapapun, tak terkecuali, sehingga siapapun dapat memeriksa keutuhan dokumen atau pesan M tersebut. Tak ada algoritma rahasia dan umumnya tak ada pula kunci

rahasia. Contoh algoritma fungsi *hash* satu arah adalah MD-5 dan SHA. *Message Authentication Code* (MAC) adalah salah satu variasi dari fungsi *hash* satu arah, hanya saja selain *pre-image*, sebuah kunci rahasia juga menjadi input bagi fungsi MAC.

II.2.4 Tanda Tangan Digital

Penandatanganan digital terhadap suatu dokumen adalah sidik jari dari dokumen tersebut beserta *timestamp*-nya dienkripsi dengan menggunakan kunci privat pihak yang menandatangani.

Tanda tangan digital memanfaatkan fungsi *hash* satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja. Keabsahan tanda tangan digital itu dapat diperiksa oleh pihak yang menerima pesan.

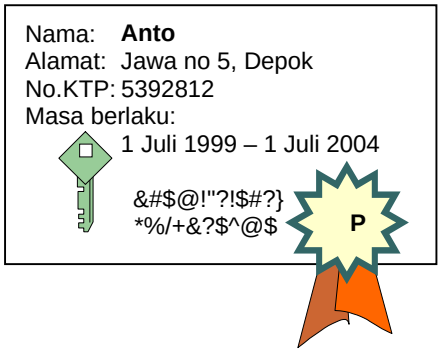
II.2.5 Masalah Pertukaran Kunci Publik

Misalkan ada dua pihak : Anto dan Badu, Anto hendak mengirimkan Badu suatu dokumen rahasia melalui jaringan komputer kepada Badu. Maka sebelumnya Badu harus mengirimkan kunci publiknya kepada Anto agar Anto dapat melakukan enkripsi yang pesannya hanya dapat dibuka oleh Badu. Demikian juga pula sebaliknya, Anto harus mengirimkan kepada Badu kunci publiknya agar Badu dapat memeriksa keaslian tanda tangan Anto pada pesan yang dikirim. Dengan cara ini Anto dapat memastikan pesan itu sampai ke tujuannya, sedangkan Badu dapat merasa yakin bahwa pengirim pesan itu adalah Anto.

Anto dan Badu bisa mendapatkan masing-masing kunci publik lawan bicaranya dari suatu pihak yang dipercaya, misalnya P. Setiap anggota jaringan diasumsikan telah memiliki saluran komunikasi pribadi yang aman dengan P.

II.2.6 Sertifikat Digital

Sertifikat digital adalah kunci publik dan informasi penting mengenai jati diri pemilik kunci publik, seperti misalnya nama, alamat, pekerjaan, jabatan, perusahaan dan bahkan *hash* dari suatu informasi rahasia yang ditandatangani oleh suatu pihak terpercaya. Sertifikat digital tersebut ditandatangani oleh sebuah pihak yang dipercaya yaitu *Certificate Authority* (CA).



Gambar II.1. Contoh sertifikat digital

II.3 SMARTCARD

Smartcard adalah kartu plastik yang berukuran sama dengan kartu kredit yang di dalamnya terdapat *chip* silikon yang disebut *microcontroller*. *Chip* merupakan *integrated circuit* yang terdiri dari prosesor dan memori. *Chip*, seperti layaknya CPU (*Central Processing Unit*) di komputer, bertugas melaksanakan perintah dan menyediakan *power* ke *smartcard*. *Smartcard* merupakan pengembangan dari kartu magnetis, namun berbeda dengan kartu magnetis yang hanya dipakai sebagai tempat penyimpanan data, *smartcard* mempunyai kemampuan untuk memproses dan menginterpretasikan data, serta menyimpan data tersebut secara aman. Apalagi dengan perkembangan algoritma kriptografi, data yang disimpan akan dienkripsi terlebih dahulu, sehingga tidak mudah dibaca oleh pihak yang tidak berwenang/berhak. Hal ini akan mempersulit pemalsuan *smartcard*. Selain perbedaan

dengan adanya *chip*, *smartcard* memiliki kapasitas memori yang lebih besar dari kartu magnetis.

II.3.1 Jenis Memori Pada *Smartcard*

Secara umum ada 3 jenis memori [ISO7816-95] yang digunakan :

1. ROM (*Read Only Memory*), berfungsi untuk menyimpan program utama dan sifatnya permanen.
2. RAM (*Random Access Memory*), berfungsi untuk menyimpan data sementara ketika proses sedang berjalan atau hasil penghitungan selama mengeksekusi perintah. Data yang disimpan di dalamnya akan hilang begitu *smartcard* dicabut (*power* hilang).
3. EEPROM (*Electrically Erasable Programmable Read Only Memory*), berfungsi untuk menyimpan program dan data yang sewaktu-waktu bisa diubah. Seperti halnya *hard disk* pada komputer, jenis memori ini akan tetap menyimpan data meskipun tidak ada *power*(permanen).

II.3.2 Tipe-tipe *Smartcard*

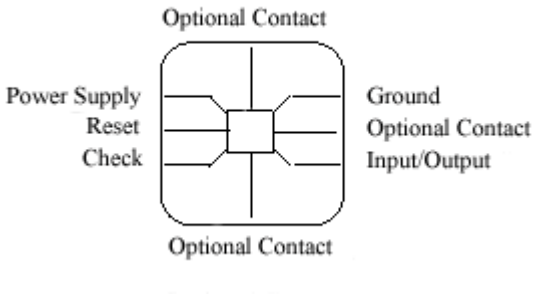
Ada 2 tipe *smartcard*, yaitu *smartcard* yang mempunyai mikroprosesor dan menawarkan kemampuan membaca, menulis dan melakukan penghitungan, seperti mikrokomputer kecil. Yang kedua adalah *smartcard* memori yang tidak mempunyai mikroprosesor dan digunakan hanya untuk tempat menyimpan. *Smartcard* memori menggunakan *security logic* untuk mengatur akses ke memori.

Gambar II.2. Bentuk *smartcard*

Secara komersial, industri membuat *smartcard* dalam beberapa varian, yaitu:

1. ***Memory cards***. *Smartcard* jenis ini hanya berfungsi untuk menyimpan data, tidak mempunyai *processor* atau sistem keamanan yang canggih melainkan hanya perlindungan fisik (karena *smartcard* bersifat *tamper proof*).
2. ***Memory protected cards***. *Smartcard* jenis ini mempunyai sistem keamanan yang lebih canggih daripada *memory cards*, misalnya mekanisme *password* untuk mengakses *smartcard*.
3. ***Microprocessor cards***. *Smartcard* jenis ini mempunyai *processor* sehingga dapat melakukan komputasi walaupun terbatas. Kemampuannya antara lain mengorganisasikan berkas (*file*) yang dilindungi dengan *password*.
4. ***Java cards***. *Smartcard* ini dilengkapi dengan Java Virtual Machine sedemikian hingga dapat dimasukkan berbagai program ke dalamnya.
5. ***Public key cards***. *Smartcard* ini mendukung *public key cryptography* (kriptografi asimetris) sehingga proses enkripsi/dekripsi dapat dilakukan secara internal dan dapat menyimpan *key*.

Pada umumnya, *smartcard* tidak berisi *power supply*, *display* atau *keyboard*. *Smartcard* berinteraksi dengan dunia luar dengan menggunakan antarmuka komunikasi serial melalui 8 titik kontak. Ukuran dan letak dari kontak tersebut didefinisikan didalam ISO 7816, bagian kedua. Gambar berikut menunjukkan kontak di dalam *smartcard*.



Gambar II.3. Delapan titik kontak

Smartcard dimasukkan ke dalam perangkat penerima *smartcard* (*Card Acceptance Device/CAD*), yang dapat dihubungkan dengan komputer. Istilah lain yang digunakan untuk CAD adalah terminal, *reader* dan IFD (*interface device*/perangkat antarmuka). Semuanya mempunyai fungsi dasar, yaitu menyediakan *power* ke *smartcard* dan membangun hubungan pertukaran data

II.3.3 Komunikasi antara *Smartcard* dan Aplikasi

Aplikasi berkomunikasi dengan *reader* (yang kemudian akan berkomunikasi dengan *smartcard*) menggunakan protokol yang standar, yaitu protokol *International Standard Organization* (ISO) 7816. *Smartcard* merupakan *personal hardware* yang harus berkomunikasi dengan perangkat lainnya untuk mengakses perangkat *display* atau jaringan komputer.

Smartcard dapat berkomunikasi dengan *reader* dengan 2 cara, yaitu :

- *contact smartcard* - koneksi dibuat ketika *reader* bersentuhan dengan *chip* yang ada di *smartcard*.
- *contactless smartcard* – dapat berkomunikasi melalui antena, mengurangi keperluan untuk memasukkan dan mengambil *smartcard*. Dengan *contactless*, yang harus dilakukan hanya mendekatkan *smartcard* ke *reader*, dan selanjutnya *smartcard* akan berkomunikasi. *Contactless smartcard* dapat digunakan di dalam aplikasi dimana pemasukan/penarikan *smartcard* tidak praktis dan pertimbangan kecepatan.

Di sisi lain aplikasi ini juga melakukan otentikasi terhadap pemakai. Otentikasi dilakukan terhadap *smartcard* dengan cara mengetahui apakah *smartcard* tersebut asli, dalam arti :

- apakah *smartcard* memang berasal dari perusahaan pemberi layanan aplikasi tersebut.
- Beberapa perusahaan diasumsikan telah menerapkan skenario yang serupa, yaitu memberikan layanan dengan otentikasi menggunakan *smartcard*. Tiap-

tiap perusahaan akan menggunakan kode yang unik untuk menandai *smartcard* yang dikeluarkannya sehingga hanya *smartcard* yang dikeluarkan oleh perusahaan, misal A yang dapat mengakses layanan yang berikan oleh perusahaan A. Hal ini juga dimaksudkan untuk mencegah sembarang *smartcard* dapat menggunakan layanan yang diberikan.

- apakah *smartcard* tersebut tidak ditiru atau digandakan.

  Data yang disimpan di dalam *smartcard* dapat ditiru jika tidak mendapat proteksi yang layak. Jika suatu ketika seorang *attacker* dapat membaca isi *smartcard*, dia bisa meng-*copy* isi(data yang disimpan) *smartcard* ke sembarang *smartcard* sehingga *smartcard* hasil *copy* tersebut dapat digunakan seperti *smartcard* yang asli. Hal ini juga bisa dilakukan oleh si pemegang *smartcard* yang 'nakal' dengan menggandakan *smartcard* yang dimilikinya. Untuk itu pihak pemberi layanan perlu memeriksa apakah *smartcard* yang dipakai benar-benar asli.

  - apakah pemakai benar-benar pemilik *smartcard* yang asli.

  Smartcard bisa hilang atau mungkin dicuri sehingga bisa digunakan oleh orang yang tidak berwenang. Hal ini tentu saja akan sangat merugikan pihak pemberi layanan maupun orang yang mempunyai *smartcard* tersebut. Oleh karena itu perlu mekanisme untuk mengetahui bahwa pemegang *smartcard* adalah orang yang benar-benar berhak.

Dalam rangka mengembangkan aplikasi berbasis *smartcard*, perlu beberapa perangkat: *smartcard reader*, perangkat lunak untuk berkomunikasi dengan *reader* maupun perangkat lunak yang berkomunikasi dengan kartu dan *smartcard*. *Reader* menyediakan *path* untuk aplikasi, untuk mengirim dan menerima *command* dari kartu.

II.3.4 Format APDU

Smartcard tidak berarti tanpa adanya *smartcard reader*, yang berfungsi sebagai perantara komunikasi antara *smartcard* dengan peralatan lain seperti

komputer. Komputer membaca atau menulis data melalui *smartcard reader*, kemudian *smartcard reader* mengubah perintah membaca/menulis tersebut ke dalam bahasa yang dimengerti *smartcard*.

Masing-masing perusahaan menyediakan protokol yang berbeda untuk berkomunikasi dengan *reader*. Komunikasi dengan *smartcard* berdasarkan format APDU (*Application Protocol Data Unit*).

APDU merupakan unit dasar untuk pertukaran paket di dalam *smartcard*. Komunikasi antara kartu dengan *reader* dilakukan dengan APDU[ISO7816-95]. APDU dinyatakan sebagai data paket yang berisi perintah lengkap atau respon yang lengkap dari kartu. Untuk menyediakan fungsionalitas seperti ini, APDU mendefinisikan struktur yang didefinisikan dalam beberapa dokumen ISO 7816.

ISO mendefinisikan standar bagaimana aplikasi berkomunikasi dengan *smartcard*. Sayangnya, ISO tidak mendefinisikan standar untuk berkomunikasi dengan *reader*. Sehingga untuk mengirim perintah ke kartu, pertama pemrogram perlu menemukan *command* yang dimengerti oleh kartu, kemudian membungkus *command* tersebut dengan ISO *command* paket, kemudian dibungkus lagi dengan pembungkus yang diperlukan oleh *reader*.

Model *master-slave* digunakan di mana *smartcard* selalu memainkan posisi yang pasif. Dengan kata lain, *smartcard* selalu menunggu perintah APDU dari terminal. Kemudian *smartcard* mengeksekusi aksi yang ditentukan di dalam APDU dan mengembalikannya ke terminal dengan respon APDU. *Command* APDU dan respon APDU dipertukarkan antara kartu dan terminal.

Gambar di bawah adalah format *command* dan respon APDU. Struktur APDU didefinisikan dalam ISO 7816-4.

Command APDU						
Mandatory Header				*Conditional Body*		
CLA	INS	P1	P2	Lc	Data field	Le

Gambar II.4. *Command* APDU

Header terdiri dari 4 field: *class* (CLA), perintah (INS) serta parameter 1 dan 2 (P1 dan P2). Masing-masing *field* berukuran 1 byte :

- CLA: *class* byte. Di beberapa *smartcard* digunakan untuk mengidentifikasikan aplikasi.
- INS: *Instruction* byte. Byte ini menyatakan kode instruksi/perintah.
- P1 dan P2: Parameter byte. Menyediakan qualifikasi lebih lanjut untuk perintah APDU.
- *Conditional body* terdiri dari 3 *field*, yaitu Lc, datafield dan Le.
- Lc menyatakan jumlah byte di dalam *data field* dari *command* APDU,
- *Data field* menyatakan data yang diperlukan oleh *command* APDU.
- Le menyatakan jumlah maksimal dari byte yang diharapkan di dalam *data field* dari respon APDU.

<table>
<tr><td colspan="3">Respon APDU</td></tr>
<tr><td>Conditional Body</td><td colspan="2">Mandatory Trailer</td></tr>
<tr><td>Data field</td><td>SW1</td><td>SW2</td></tr>
</table>

Gambar II.5. Respon APDU

- Respon APDU terdiri dari *conditional body* dan *mandatory trailer*.
- *Conditional body* berisi *data field* yang menyatakan data yang diperlukan oleh respon APDU.
- *Mandatory trailer* terdiri dari *status byte* SW1 dan SW2 menyatakan status proses dari *command* APDU di dalam kartu.

II.3.5 Serangan Pada *Smartcard*

Serangan terhadap *smartcard* dapat dilakukan terhadap :

a. *Smartcard* magnetik

Serangan terhadap *smartcard* ini adalah dengan menulis kembali informasi yang ada atau membuat *copy* dari *smartcard*.

b. *Smartcard* dengan *microcontroller*

Cara yang lebih umum, menebak kunci yang tepat. Pencarian kunci DES dengan *brute force* (2^{56} = 72.057.594.037.927.936 kemungkinan) membutuhkan 35 jam pada tahun 1995 dan membutuhkan $100,000 perangkat keras[BDHJN96]. Kemampuan menghitung akan bertambah dua kali setiap 9 bulan, dan perangkat lunak 1000 kali lebih lambat dari perangkat keras. Membutuhkan waktu yang lama karena komunikasi yang relatif lambat dengan *smartcard*, dan beberapa *smartcard* hanya akan memperbolehkan beberapa kali tebakan saja. Metode ini akan berarti jika sistem hanya memiliki satu kunci simetris *smartcard* sehingga jika dapat menyerang satu *smartcard*, maka sama saja menyerang semua *smartcard*.

Sistem yang pandai akan menggunakan kunci yang berbeda untuk setiap *smartcard*, contohnya dengan kriptosistem kunci publik.

Di bawah ini dijelaskan beberapa macam penyerangan terhadap *smartcard*

II.3.5.1 Serangan Secara logika

Semua kunci pada *smartcard* disimpan dalam *Electrically Erasable Programmable Read Only Memory* (EEPROM), dan pada kenyataannya operasi tulis ke EEPROM dapat dipengaruhi oleh tegangan dan temperatur yang tidak biasa, informasi dapat terperangkap dengan menaikkan atau menurunkan tegangan yang diberikan ke *microcontroller* .

Sebagai contoh, serangan yang terkenal yaitu *microcontroller* PIC16C84 akan membersihkan *security bit controller* dengan menghapus memori dengan cara menaikkan tegangan VCC ke VPP-0,5V[AK96]. Sebagai contoh yang lain adalah serangan terhadap DS5000 *security processor*. Penurunan tegangan kadang-kadang

dapat membongkar keamanan kunci tanpa menghapus data rahasia. Tegangan rendah dapat memfasilitasi serangan lain, seperti *analogue random generator* digunakan untuk membuat kunci kriptografi akan mengeluarkan keluaran hampir semuanya angka 1 ketika pemberian tegangan direndahkan[AK96].

Untuk alasan-alasan tersebut, beberapa *security processors* mengimplementasikan sensor yang akan mengeluarkan tanda peringatan ketika ada perubahan lingkungan. Bagaimanapun juga, jenis sensor ini selalu mengeluarkan tanda peringatan yang salah akibat dari munculnya fluktuasi ketika *smartcard* diaktifkan dan ketika *smartcard* menstabilkan diri. Oleh sebab itu skema ini tidak biasa digunakan.

Serangan-serangan baru terhadap kriptosistem kunci publik pada alat *tamperproof* muncul untuk mengetahui nilai eksponen pribadi (d) yang disimpan dalam *smartcard*. Eksponen pribadi (d) digunakan untuk membuat kunci privat, oleh sebab itu tidak boleh diketahui oleh pihak lain. Membuka alat *tamperproof* yang tertutup seperti *smartcard* dengan melakukan *external physical effect* (contoh : pengionan atau radiasi *microwave*), memungkinkan seseorang dapat menghasilkan kesalahan bit nilai eksponen pribadi pada lokasi bit sembarang di alat *tamperproof*. Kesalahan dalam lokasi bit sembarang tidak mempengaruhi kode itu sendiri, sebagai contoh program tidak *crash*, dan hanya beberapa nilai operasi yang terkena akibat. Contoh serangan untuk mengetahui nilai d adalah : serangan terhadap skema RSA[BDHJN 96].

Secara garis besar serangan terhadap skema RSA bekerja sebagai berikut : berlaku n=pq adalah produk dari dua bilangan p dan q di RSA, e adalah eksponen yang diketahui secara umum dan d adalah eksponen pribadi yang disimpan di dalam alat *tamperproof*. M adalah sebuah *plaintext*, maka pesan yang terenkripsinya atau *ciphertext* adalah $C = p^{e} \bmod n$. Ditunjukkan representasi biner dari eksponen pribadi sebagai d = d (t-1)| d (t-2)| … | d (I) | … | d (1) | d (0), dimana d (I) bernilai 1 atau 0, adalah bit ke I, t adalah jumlah bit d, dan x|y menunjukkan sambungan x dan y.
Lebih jauh, ditunjukkan C(0)= C, $C(1) = C^{2} \bmod n$, $C(2) = C^{(2\wedge 2)} \bmod n$, …, $C(t-1) = C^{2\wedge(t-1)}$. Diberikan C dan d, *plaintext* M dapat diekspresikan sebagai M = (($C(t-1)^{d(t-}$

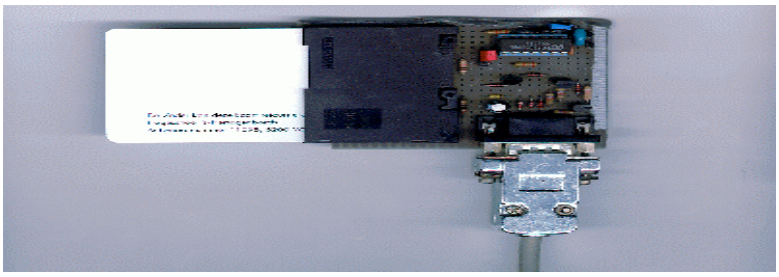
$^{1)}$) (C(t-2) $^{d(t-2)}$) … (C(I) $^{d(I)}$) … (C(1) $^{d(1)}$) (C(0) $^{d(0)}$) mod n. Pada awalnya penyerang secara sembarang memilih suatu *plaintext* (M) dan menghitung *ciphertext* dari M (C). Misalkan salah satu bit dalam representasi biner d berubah dari 1 ke 0 atau sebaliknya, dan posisi bit yang salah bisa dimana saja. Kemudian *smartcard* diminta untuk mendeskripsikan C. Asumsi bahwa d(I) berubah menjadi komplemen d(I)', kemudian *output* dari alat akan menjadi M' = (C(t-1)$^{d(t-1)}$) (C(t-2) $^{d(t-2)}$) … (C(I)$^{d(I)'}$) … (C(1)$^{d(1)}$) (C(0)$^{d(0)}$) mod n. Sejak penyerang memiliki M dan M', penyerang dapat menghitung M'/M = C(I)$^{d(I)'}$/ C(I)$^{d(I)}$ mod n. Tentu saja, jika memiliki M/M' = 1/ C(I) mod n, maka d(I)=1, dan jika M'/M = C(I) mod n, maka d(I)=0. Penyerang dapat menghitung sebelumnya C(I) dan 1/C(I) mod n untuk I = 0,1,…, t-1, dan membandingkan M'/M mod n untuk setiap nilai I dalam menentukan satu bit d. Penyerang menentukan proses di atas berulang-ulang menggunakan pasangan *plaintext*/*ciphertext* yang sama sampai penyerang menemukan cukup informasi untuk memperoleh d.

II.3.5.2 Serangan Secara Fisik

Serangan fisik ini ditujukan bagi sirkuit *chip smartcard*. Sebelum serangan jenis ini dilakukan, sirkut *chip* harus dipindahkan dari bagian plastik *smartcard*. Setelah *chip* berhasil diambil, *chip* dapat diperiksa dan diserang secara langsung.

Contoh serangan fisik yang lain adalah menghapus *security block bit* dengan memfokuskan sinar UV pada EEPROM, penyelidikan operasi sirkuit dengan menggunakan jarum mikro, atau menggunakan mikroskop laser pemotong untuk memeriksa *chip* dan sebagainya. Bagaimanapun juga, serangan ini hanya berlaku pada laboratorium yang canggih karena untuk melakukan serangan membutuhkan biaya yang tinggi.

II.3.5.2.1 Dumb Mouse



Gambar II.6. *Dumb mouse*

Serangan yang tidak dapat dianggap ringan adalah serangan dengan menggunakan *dumb mouse*. *Dumb mouse* adalah *reader* pintar yang kecil, murah, dapat membaca *smartcard* yang sesuai dengan standar ISO 7816-3 dan mungkin juga jenis lain (termasuk *smartcard* memori maupun *smartcard* dengan *microcontroller*), dan menggunakan port serial komputer[Chan99].

Smartcard mengeluarkan beberapa data jika mereka di *reset* atau dimasukkan ke alat pembaca. Ini disebut "*answer to reset*" atau ATR. ATR akan memberitahukan informasi mengenai pembuat *smartcard* (*issuer*) tersebut dan protokol yang seharusnya digunakan untuk berkomunikasi. Untuk menyandikan *byte* dapat menggunakan "*direct convention*" yaitu langsung mengkomplemenkan *bit* atau "*inverse convention*" yaitu *bit* dibalik dan dibaca dari belakang. Protokol yang biasa digunakan disebut T=0 yaitu protokol paling sederhana dan T=1 yaitu protokol lebih kompleks dan memiliki lapisan jaringan tambahan.

Contoh serangan yang dapat dilakukan :

1. Pengujian jenis *smartcard* : *smartcard* magnetik atau *smartcard* dengan *microcontroller*.
2. Lihat dalam ATR : tentukan teknik penyandiannya dan protokol yang digunakan.
3. Menebak instruksi yang digunakan, ada beberapa cara :
    - Coba semua kemungkinan. *Dumb mouse* beroperasi pada 9600 *baud* sehingga walaupun banyak *smartcard*, *dumb mouse* dapat bekerja dua kali lebih cepat. Hal ini berbahaya, karena seseorang dapat mengeksekusi instruksi yang

merusak, mengkosongkan atau mem-*block smartcard*.

- Melakukan *eavesdrop* pada komunikasi sesungguhnya dengan menggunakan alat *login.* Alat *login* dapat terlihat sebagai perpanjangan kawat antara *smartcard* dan terminal. Setiap *byte* yang dikirim dari atau ke *smartcard* dapat diawasi dan membantu untuk mengerti perintah dan protokol. Kesulitan yang ada adalah jika terminal beroperasi dengan kecepatan *baud* yang tidak sesuai standar dan jika terminal menggunakan detektor logam maka penggunaan *smartcard* dengan kawat (alat untuk *login*) tidak mungkin dilakukan.
- Cari manual. Cara yang paling mudah. Tetapi membutuhkan biaya dan terkadang spesifikasi *smartcard* tidak disebarluaskan ke masyarakat.

4. Dengan menggunakan spesifikasi terminal kita mengetahui beberapa perintah. Dengan perintah ini kita dapat memilih *file,* dapat membaca data dalam *file,* dapat memperoleh informasi rahasia dan dapat membaca informasi transaksi.

II.3.6 Serangan Pertukaran Pesan Melalui Jaringan Komputer

Berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi, penyerangan dapat dikategorikan menjadi:

1. *Sniffing*: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekap pembicaraan yang terjadi.
2. *Replay attack*[DHMM96]: Jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.
3. *Spoofing*[DHMM96]: Penyerang – misalnya C – bisa menyamar menjadi A. Semua orang dibuat percaya bahwa C adalah A. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam *Card Acceptance Device* (CAD) – yang benar-benar

dibuat seperti CAD asli – tentu sang penipu bisa mendapatkan PIN pemilik *smartcard*. Pemilik *smartcard* tidak tahu bahwa telah terjadi kejahatan.

4. *Man-in-the-middle*[Schn96]: Jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini, saat A hendak berkomunikasi dengan B, C di mata A seolah-olah adalah B, dan C dapat pula menipu B sehingga C seolah-olah adalah A. C dapat berkuasa penuh atas jalur komunikasi ini, dan bisa membuat berita fitnah.

Kabel koaksial yang sering digunakan pada jaringan sangat rentan terhadap serangan *vampire tap*[Tane89], yakni perangkat keras sederhana yang bisa menembus bagian dalam kabel koaksial sehingga dapat mengambil data yang mengalir tanpa perlu memutuskan komunikasi data yang sedang berjalan. Seseorang dengan *vampire tap* dan komputer jinjing dapat melakukan serangan pada bagian apa saja dari kabel koaksial.

Penyerang juga bisa mendapatkan kunci dengan cara yang lebih tradisional, yakni dengan melakukan penyiksaan, pemerasan, ancaman, atau bisa juga dengan menyogok seseorang yang memiliki kunci itu. Ini adalah cara yang paling ampuh untuk mendapat kunci.

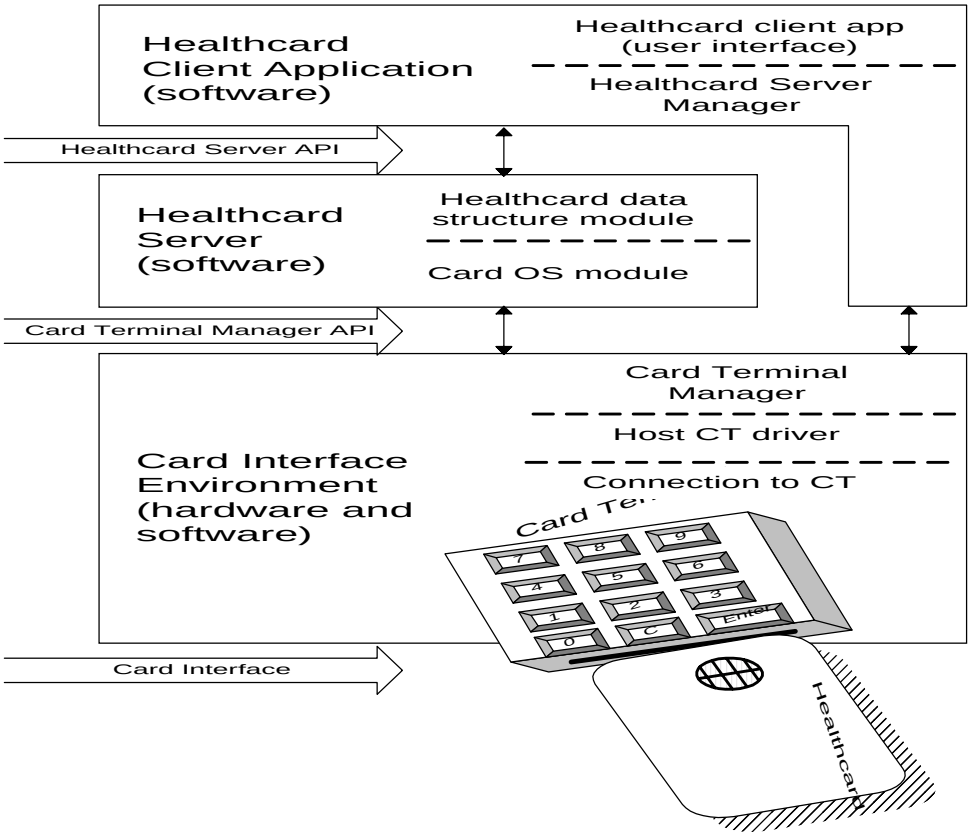
II.4 STANDAR INTEROPERABILITY SMARTCARD KESEHATAN

Interoperability antara sistem *smartcard* kesehatan adalah kemampuan suatu sistem *smartcard* kesehatan untuk membaca, menggunakan, dan mengubah data, yang dikeluarkan oleh sistem *smartcard* kesehatan lain[EUHCI96]. Sistem *smartcard* kesehatan adalah gabungan dari *smartcard* kesehatan dan semua perangkat keras dan perangkat lunak yang digunakan dalam implementasi kesehatan tertentu. Walaupun dua atau lebih proyek menggunakan teknologi yang sama untuk mengimplementasikan fungsi-fungsinya, tetap ada variasi dan ketidaksesuaian pada berbagai implementasi. Oleh sebab itu, sangat penting untuk membangun sistem *smartcard* kesehatan yang *interoperability*.

Standar *interoperability* sistem *smartcard* kesehatan di dunia belum ada yang baku. Oleh karena itu, berbagai organisasi atau *vendor* berusaha untuk membuat standar *interoperability* sistem *smartcard* kesehatan. Pada tugas akhir ini, standar *interoperability* yang digunakan adalah standar dibuat oleh Uni Eropa dan Jepang yaitu EU/G7 *Healthcards* – W7[EUHCI96]. Berikut ini dijelaskan mengenai sistem yang diatur oleh standar *interoperability* EU/G7 *Healthcards* – W7.

II.4.1 Modul dan Antar Muka Sistem *Smartcard* Kesehatan

Sistem *smartcard* kesehatan yang *interoperability* terdiri dari empat komponen dan tiga antar muka, seperti yang terdapat pada gambar di bawah ini :



Gambar II.7. Pendekatan modular untuk sistem *smartcard* kesehatan yang *interoperability*

Komponen modul dan antar muka sistem *smartcard* kesehatan yang *interoperability* adalah sebagai berikut :

1. *Healthcard Client Application*

   Terdiri dari perangkat lunak yang menyediakan antarmuka untuk suatu sistem *smartcard* kesehatan. *Healthcard Client Application* mengakses *smartcard* kesehatan yang *interoperable* dengan menggunakan pelayanan yang disediakan oleh *Healthcard Servers* dan *Card* Terminal *Manager*, pelayanan tersebut adalah *Healthcard Server API* (HS-API) dan *Card* Terminal *Manager API* (CTM-API).

2. *Healthcard Servers*

   Adalah perangkat lunak yang menyediakan akses ke data di dalam *smartcard*-*smartcard* kesehatan yang berbeda melalui suatu antar muka yaitu HS-API. *Healthcard Servers* harus membaca dan memetakan data yang tersimpan di *smartcard* sehingga dapat direpresentasikan dalam bentuk struktur data yang disepakati pada HS-API. *Healthcard Servers* harus menggunakan fungsi-fungsi milik *Card* Terminal *Manager API* untuk mengakses *smartcard* dan mengatur *Card* Terminal.

   Healthcard Servers yang berbeda dapat digunakan untuk setiap *smartcard* kesehatan yang memiliki struktur data yang berbeda. Sebagai alternatif, beberapa *Healthcard Servers* dapat disusun untuk mendukung beberapa bentuk *smartcard* kesehatan. Pengembangan *Healthcard Servers* oleh masing-masing *Healthcard Servers* merupakan tanggung jawab pembuat *smartcard*.

3. *Card Interface Environment*

   Adalah perangkat keras dan lunak yang secara bersama menyediakan *Card* Terminal *Manager API* dan berkomunikasi dengan satu atau lebih *smartcard*.

4. *Healthcard*

   Adalah *smartcard* yang dapat dibaca komputer, diimplementasikan dengan administrasi dan ketetapan pusat pelayanan kesehatan.

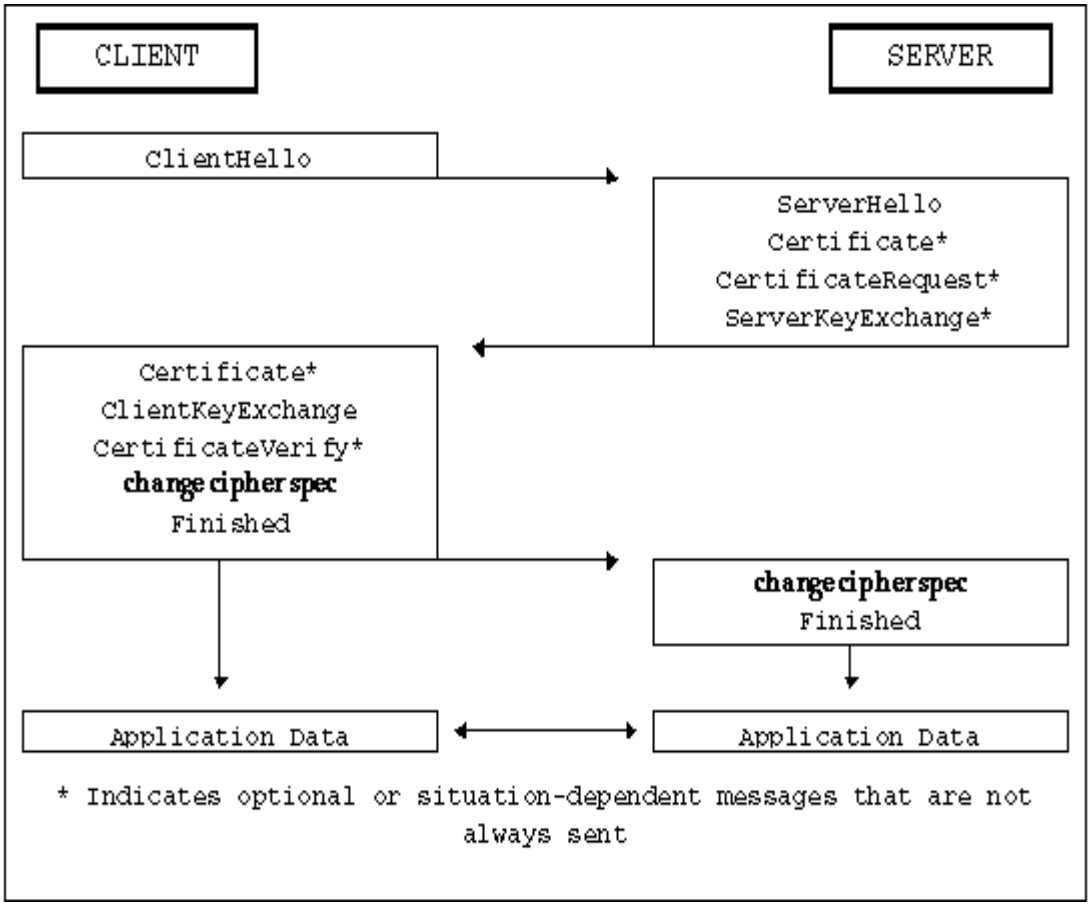
Berikut ini dijelaskan mengenai protokol pengiriman data yang aman lewat jaringan komputer.

II.5 SECURE SOCKET LAYER (SSL)

SSL dapat menjaga kerahasiaan (*confidentiality*) dari informasi yang dikirim karena menggunakan teknologi enkripsi yang maju dan dapat di-*update* jika ada teknologi baru yang lebih bagus. Dengan penggunaan sertifikat digital, SSL menyediakan otentikasi yang transparan antara *client* dengan *server*. SSL menggunakan algoritma RSA untuk membuat tanda tangan digital (*digital signature*) dan amplop digital (*digital envelope*). Selain itu, untuk melakukan enkripsi dan dekripsi data setelah koneksi dilakukan, SSL menggunakan RC4 sebagai algoritma standar untuk enkripsi kunci simetri.

Saat aplikasi menggunakan SSL, sebenarnya terjadi dua sesi, yakni sesi *handshake* dan sesi pertukaran informasi. Berikut akan dijabarkan sebuah skenario yang aman dari sesi *handshake* SSL versi 3.0 [IETF96]:

- *Client* mengirimkan *client hello* yang harus dijawab dengan *server hello*. Tahap ini terjadi kesepakatan atas pengunaan versi protokol, *session ID*, perangkat kriptografi, metoda kompresi.
- *Server* kemudian dapat mengirim sertifikat kepada *client*. Selain itu *server* bisa meminta *client* untuk menunjukkan sertifikatnya – namun tidak harus. *Server* lantas mengirimkan pesan *server hello done,* lalu menunggu jawaban dari *client*.
- Jika *server* meminta sertifikat dengan pesan *certificate request*, maka *client* harus mengirimkan pesan *certificate message* atau *no certificate.*
- Pesan *client key exchange* kini dikirim, dimana pesan yang disandikan itu tergantung dari algoritma kriptografi kunci publik yang disepakati pada tahap pertama. Pesan itu berisi kunci-kunci yang dibuat secara acak oleh *client* untuk keperluan enkripsi dan perhitungan sidik jari (*hash*). Jika memungkinkan, dapat pula disertai tanda tangan digital melalui pengiriman pesan *certificate verify*.
- Akhirnya *server* dan *client* dapat bertukar pesan dengan menyandikannya dengan kunci dan algoritma yang telah disepakati bersama pada level aplikasi.



Gambar II.8. *Security Handshake*

- Guna mencegah serangan yang dilakukan terhadap pesan yang disandikan, *server* dan *client* dapat melakukan *handshake* beberapa kali pada session ID yang sama guna mengubah kunci, namun mereka tidak perlu mengubah parameter komunikasi yang telah disepakati sebelumnya.
- Patut juga dicatat bahwa *client* perlu memeriksa sertifikat yang diterimanya agar lebih yakin bahwa dia sedang berkomunikasi dengan *server* yang diinginkan. Jika *client* tidak memeriksanya, masih ada kesempatan bagi seseorang untuk menyamar menjadi *server* yang seharusnya diajak bicara (masih termasuk serangan *man-in-the-middle*).
- *Client* memeriksa sertifikat digital itu dengan membandingkan tanda tangan CA

(*Certificate Authority*) pada sertifikat digital itu dengan daftar CA yang dimiliki. Biasanya, *browser-browser* seperti Netscape Navigator atau Microsoft Internet Explorer sudah menyertakan sertifikat digital dari CA utama yang terkenal, sehingga memudahkan pemeriksaan sertifikat digital pada koneksi SSL. Penyertaan serfikat digital CA utama pada *browser* akan menghindarkan *client* dari pemalsuan sertifikat CA utama.

BAB III
ANALISIS KEBUTUHAN RANCANGAN SISTEM SMARTCARD KESEHATAN SESUAI KEBUTUHAN DI INDONESIA

Bab ini menganalisis kondisi sistem rekam medis yang berlaku di Indonesia berdasarkan peraturan pemerintah tentang rekam medis dan mengecek peraturan pemerintah tersebut dengan kondisi hasil observasi penggunaan data rekam medis di rumah sakit. Kemudian, dilakukan perbandingan sistem-sistem *smartcard* kesehatan yang ada di luar negeri dengan menggunakan kondisi sistem rekam medis Indonesia. Dari analisis tersebut akan disimpulkan teknologi sistem *smartcard* kesehatan yang paling mendekati dengan kebutuhan di Indonesia. Teknologi sistem *smartcard* kesehatan tersebut digunakan sebagai dasar untuk perancangan sistem *smartcard* kesehatan yang memenuhi kebutuhan di Indonesia.

III.1 ANALISIS KONDISI SISTEM REKAM MEDIS DI INDONESIA BERDASARKAN HASIL OBSERVASI PENGGUNAAN DATA REKAM MEDIS DI RUMAH SAKIT

Pada saat ini sistem rekam medis rumah sakit di Indonesia menggunakan kertas sebagai media penyimpanan data rekam medis para pasiennya. Di luar negeri sudah diimplementasikan sistem rekam medis elektronik dimana *smartcard* digunakan sebagai media penyimpanan rekam medis elektronik seseorang. Tugas akhir ini bertujuan untuk merancang sistem *smartcard* kesehatan yang sesuai dengan kebutuhan di Indonesia, oleh sebab itu lebih dahulu dianalisis kondisi sistem rekam medis di Indonesia berbasis kertas yang ada sekarang. Kondisi-kondisi yang dipilih adalah hasil observasi terhadap penggunaan data rekam medis yang dilakukan di rumah sakit. Kondisi-kondisi tersebut antara lain :

- Kebutuhan 1 : Pihak yang membaca data rekam medis, sesuai dengan hukum/peraturan rekam medis di Indonesia, haruslah pihak yang berwenang. Pihak yang berwenang adalah dokter, tenaga medis (perawat, bidan, tenaga laboratorium klinik, penata rontgen, anestesi, dan lain sebagainya), mahasiswa kedokteran yang sedang melakukan praktek klinik, dan tenaga kesehatan lain yang diberi wewenang khusus oleh direktur rumah sakit atau departemen kesehatan[PerMen89]. Pada saat ini pegawai di rumah sakit dapat mengambil dan membaca data rekam medis asalkan mengembalikan data rekam medis tersebut ke tempat penyimpanannya kembali. Data rekam medis merupakan data sensitif sehingga harus dijaga kerahasiaannya. Pihak yang membaca data rekam medis haruslah mendapat ijin atau sepengetahuan pasien[PerMen89].
- Kebutuhan 2 : Menurut hukum/peraturan rekam medis Indonesia bahwa setiap dokter yang membuat, menambah dan melakukan koreksi terhadap data rekam medis harus menandatangani rekam medis tersebut. Hal ini sangat penting dalam sistem rekam medis di Indonesia karena jika terjadi kesalahan tindakan pengobatan maka pihak yang melakukan diagnosa dapat dituntut secara hukum. Tanda tangan tersebut digunakan sebagai bukti yang tidak dapat disangkal oleh si pembuat diagnosa. Namun pada sistem rekam medis sekarang, tanda tangan dapat dipalsukan dan kemungkinan kerusakan terhadap tanda tangan di kertas dapat terjadi (sebagai contoh : tanda tangan terkena air, kotor, atau kertas tanda tangan robek).
- Kebutuhan 3 : Dokter yang membuat diagnosa harus yakin bahwa data rekam medis yang disimpan dan dibaca kembali tidak diubah oleh pihak yang tidak berwenang. Pihak yang tidak berwenang adalah semua pihak yang tidak berhubungan dengan proses pengobatan pemilik data rekam medis dan pihak lain yang tidak mendapat ijin dari direktur rumah sakit atau departemen kesehatan[PerMen89]. Informasi yang disimpan dalam berkas rekam medis harus merupakan informasi yang benar, agar penggunaan selanjutnya tidak terjadi kesalahan pengobatan, dimana mungkin saja kesalahan tersebut membahayakan jiwa si pemilik data rekam medis. Jika terjadi koreksi pada rekam medis maka

harus diberi paraf oleh pihak yang melakukan koreksi tersebut. Pada sistem sekarang, dokter tidak dapat memastikan bahwa data rekam medis yang dibuatnya atau yang dikoreksinya tidak dapat diubah oleh pihak-pihak lain yang tidak berwenang karena tidak ada prosedur yang membuktikan bahwa data rekam medis sekarang dan data rekam medis asli adalah sama.

- Kebutuhan 4 : Pada sistem rekam medis sekarang tidak menyediakan pencatatan terhadap data rekam medis yang dikoreksi. Seharusnya pihak rumah sakit melakukan pencatatan tersebut sebagai barang bukti sehingga pencatatan ini semakin memperkecil kemungkinan penyangkalan tenaga medis yang melakukan koreksi terhadap data rekam medis.
- Kebutuhan 5 : Rekam medis harus dapat digunakan untuk kepentingan rawat jalan, bahan rujukan dan keadaan gawat darurat setiap saat[PerMen89]. Hukum/peraturan di Indonesia menyatakan bahwa data rekam medis merupakan milik si pasien sehingga pasien tersebut berhak menggunakan data rekam medisnya untuk kepentingannya kapan saja. Pada sistem rekam medis di Indonesia sekarang ini, ketiga hal di atas kurang dapat didukung, sebagai contoh :
    - Untuk meminta data rekam medis sebagai bahan rujukan dari suatu rumah sakit ke rumah sakit lain harus melalui prosedur birokrasi yang cukup panjang dan harus diambil di rumah sakit yang bersangkutan. Serangan penyakit dan kecelakaan bisa terjadi di mana saja oleh sebab itu sangat penting bagi pemilik rekam medis untuk memiliki rekam medisnya di mana saja dan kapan saja.
    - Pada kondisi gawat darurat, dokter atau tenaga medis sulit untuk memperoleh informasi identitas dan sejarah rekam medis pasien. Pada pelaksanaannya pasien gawat darurat tidak akan diberikan tindakan pengobatan lebih lanjut (misalkan operasi, pemberian oksigen) jika tidak memiliki pihak penjamin biaya pengobatan. Hal ini sangat membahayakan kondisi kesehatan pasien gawat darurat..
    - Pada proses rawat jalan, dokter sangat sulit untuk menelusuri sejarah rekam medis pasiennya, terutama pasien yang berobat di berbagai rumah

sakit.

- Antar rumah sakit yang ingin melakukan pertukaran data rekam medis pasien yang sedang dirawatnya, harus mengirimkan pegawainya ke rumah sakit yang bersangkutan untuk mengambil data rekam medis yang dibutuhkan atau mengirimkan resume pengobatan ke pihak rumah sakit yang meminta data melalui jasa pos.
- Dokter yang ingin memeriksa kembali diagnosa yang telah dilakukannya, harus melakukannya di rumah sakit tempat pasien diperiksa.
- Data rekam medis harus lengkap, menurut hukum/peraturan rekam medis di Indonesia maka data rekam medis harus disimpan sekurangnya lima tahun dari pembuatan rekam medis tersebut. Jika mampu, pihak rumah sakit diperbolehkan untuk menyimpan data rekam medis lebih dari lima tahun.

- Kebutuhan 6 : Data rekam medis harus dijamin kerahasiaannya dari pihak yang tidak berwenang[PerPem66]. Data rekam medis merupakan milik si pasien oleh sebab itu pasien berhak untuk merahasiakannya. Setiap penggunaan data rekam medis yang tidak diketahui oleh pasien dan bukan untuk tujuan pengobatan tidak diperbolehkan. Kerahasiaan data rekam medis dapat dilakukan pada hal-hal berikut :
    - Hukum/peraturan rekam medis di Indonesia memperbolehkan bahwa dokter dapat merahasiakan data rekam medis yang dapat memperburuk kondisi kesehatan pasien jika membaca data rekam medis miliknya.
    - Hukum/peraturan rekam medis mengatur bahwa dokter dari suatu poliklinik tidak dapat secara langsung membaca rekam medis dari poliklinik lain yang tidak sesuai dengan pemeriksaan yang dilakukan. Misalkan dokter dari poliklinik gigi tidak dapat membaca data rekam medis milik poliklinik jiwa. Tetapi, dokter dari suatu poliklinik dapat membaca data rekam medis dari poliklinik lain dengan seijin atau sepengetahuan pemilik data rekam medis. Pada sistem sekarang dokter suatu poliklinik dapat langsung membaca data rekam medis dari berbagai

poliklinik lain tanpa seijin atau sepengetahuan pasien.

- Kebutuhan 7 : Rekam medis harus dapat dimengerti dan digunakan oleh berbagai rumah sakit dan dokter. Jadi harus ada standar yang jelas mengenai kode penyakit dan tindakan kesehatan yang disimpan.

III.2 DESKRIPSI UMUM SISTEM SMARTCARD KESEHATAN YANG TELAH DIIMPLEMENTASIKAN

Sebelum membandingkan sistem-sistem *smartcard* kesehatan di luar negeri dengan kondisi-kondisi di Indonesia agar dapat dianalisis apakah sistem tersebut dapat diimplementasikan di Indonesia, terlebih dahulu dideskripsikan sistem *smartcard* kesehatan secara umum. Perancis, Jerman, Amerika serikat, Kanada, Singapura, Hongkong dan negara-negara lain telah mengimplementasikan sistem *smartcard* kesehatan di negaranya sebagai pengganti sistem rekam medis berbasis kertas. Bagian ini mendeskripsikan secara umum sistem-sistem *smartcard* kesehatan yang telah diimplementasikan di luar negeri. Ada lima sistem *smartcard* kesehatan yang dianalisis yaitu sistem *smartcard* kesehatan Motus[Motus99], Oberthur[Oberthur99], Microchart[Microchart99], Orga[Orga99], dan Precis[Precis99]. Dasar pemilihan kelima sistem tersebut adalah karena kelengkapan informasi yang dapat diperoleh dan adanya perbedaan diantara kelima sistem tersebut. Sistem-sistem *smartcard* kesehatan yang sama atau hampir sama tidak diambil sebagai contoh, karena sudah tercakup pada sistem yang terpilih. Pada umumnya kelima sistem *smartcard* kesehatan yang telah diimplementasikan tersebut bertujuan untuk :

- Mengurangi pengisian data dan biaya untuk melakukan tes kesehatan yang sama setiap saat.
- Mengurangi waktu pencarian data rekam medis.
- Meningkatkan komunikasi bagi pasien yang tuna rungu, kurang pendengaran, atau setiap pasien yang kesulitan berkomunikasi.
- Pengingat rutinitas *check up* yang tidak boleh absen. Membantu untuk memonitor

penyakit kronis seperti penyakit jantung atau diabetes.

- Menjaga semua data imunisasi secara permanen dan tersedia setiap waktu.
- Mengurangi kemungkinan terjadinya interaksi obat yang dapat membahayakan jiwa pasien pada waktu pengobatan.
- Memberikan data yang sesuai dan fakta untuk menolong dokter atau tenaga kesehatan membuat keputusan penting secara cepat sehingga meningkatkan pelayanan pengobatan yang diberikan.
- Melakukan pembayaran terhadap klaim asuransi kesehatan sehingga pihak rumah sakit tidak perlu memastikan dahulu sebelum memberikan tindakan pengobatan, bahwa pasien yang sedang dirawat memiliki pihak penjamin biaya pengobatan.

Berikut ini, dijelaskan mengenai alur penggunaan data rekam medis pada sistem *smartcard* kesehatan yang telah diimplementasikan.

III.2.1 Alur Penggunaan Data Rekam Medis

Untuk lebih memperjelas alur penggunaan data rekam medis proses pengobatan sistem *smartcard* kesehatan yang ada secara umum, akan dilengkapi diagram alur data. Tabel berikut ini menjelaskan mengenai elemen-elemen diagram alur data :

Elemen Diagram	Penjelasan
Dokter	Kepala dari setiap kolom pada diagram alur data menunjukkan pihak yang melakukan transaksi
	Kotak menunjukkan proses yang dilakukan oleh pihak tertentu dalam kolom itu
	Panah beserta teks menunjukkan dari dan kemana suatu data dikirimkan.

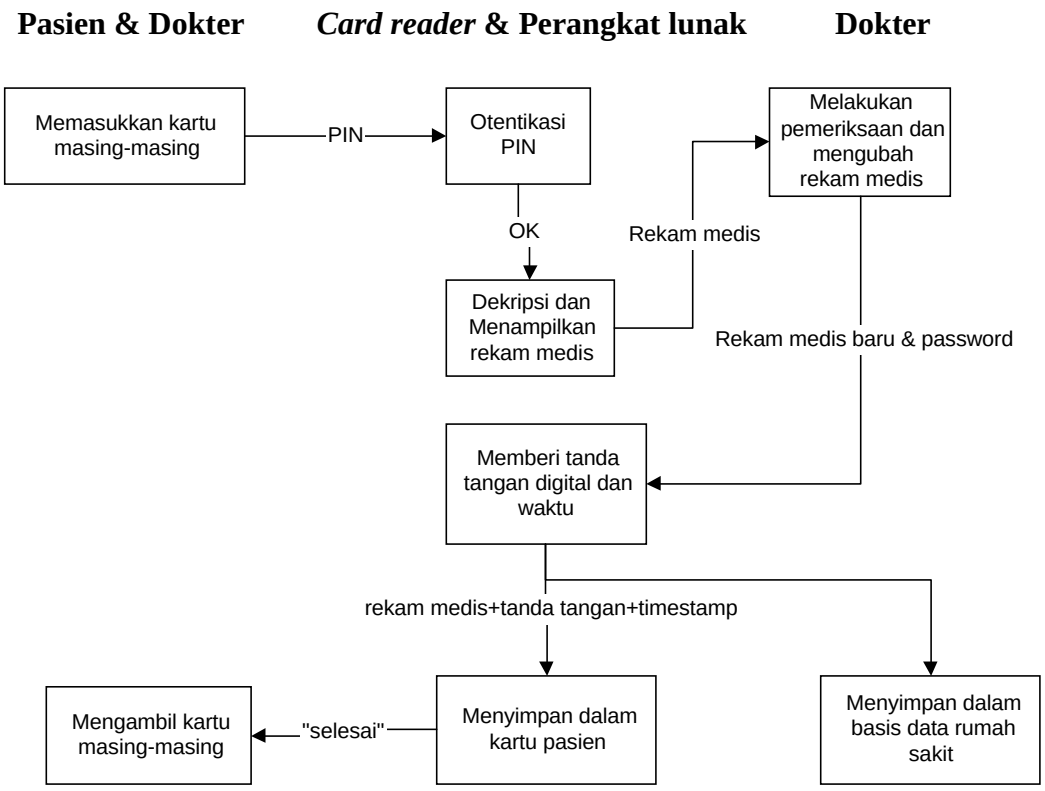
Tabel III.1. Penjelasan elemen diagram alur data

Pada umumnya alur transaksi untuk proses rawat jalan pada kelima sistem tersebut berjalan sebagai berikut :

1. Pasien datang ke tempat pelayanan kesehatan dengan membawa *smartcard*.
2. Pasien memasukkan *smartcard* miliknya ke *card reader* yang terhubung ke komputer. Kemudian ia memasukkan nilai PIN yang hanya diketahui oleh pemilik *smartcard* tersebut.
3. Dokter yang memeriksa akan memasukkan juga *smartcard* profesionalnya ke dalam *card reader* yang terhubung ke komputer. Dokter itu juga memasukkan nilai PIN yang hanya diketahui olehnya.
4. Perangkat lunak aplikasi akan melakukan otentikasi pengguna dengan mengecek apakah nilai PIN yang ada pada *smartcard* sama dengan nilai PIN yang dimasukkannya.
5. Jika nilai PIN benar maka dokter dapat membaca ringkasan sejarah rekam medis pasien dan keterangan alergi terhadap beberapa obat tertentu. Untuk beberapa sistem, data rekam medis di dalam *smartcard* disimpan dalam bentuk terenkripsi

dengan menggunakan kunci publik perangkat lunak aplikasi kesehatan, atau dengan menggunakan kunci simetris perangkat lunak aplikasi kesehatan. Sehingga ketika data tertentu akan dibaca maka data tersebut didekripsi dahulu dengan menggunakan kunci privat perangkat lunak aplikasi kesehatan bagi yang menggunakan mekanisme enkripsi kunci asimetris, atau kunci simetris perangkat lunak aplikasi kesehatan bagi yang menggunakan mekanisme enkripsi kunci simetris. Kemudian data hasil dekripsi ditampilkan pada layar. Tetapi terdapat juga sistem yang tidak melakukan enkripsi terlebih dahulu terhadap data rekam medis yang disimpan di dalam *smartcard*.

6. Dokter melakukan pemeriksaan. Setelah melakukan pemeriksaan dokter akan menambahkan data rekam medis dan tindakan medis lain (misalkan pemeriksaan darah, *rontgen*, pemeriksaan radiologi, dan sebagainya) ke dalam *smartcard*. Sebelum data disimpan, data tersebut dapat dienkripsi dahulu dengan kunci yang dimiliki oleh perangkat lunak aplikasi kesehatan atau data rekam medis tersebut dapat juga tidak dienkripsi.
7. Setelah menambah data rekam medis, dokter menandatangani data rekam medis tersebut dan *time stamp* penambahan data, kemudian tanda tangan tersebut disimpan di dalam *smart card* (tetapi ada beberapa sistem juga yang tidak mendukung tanda tangan digital).
8. Penambahan data rekam medis dicatat dan disimpan dalam basis data rumah sakit.
9. Proses pengobatan selesai, pasien meninggalkan tempat pemeriksaan dengan membawa serta *smartcard* miliknya.



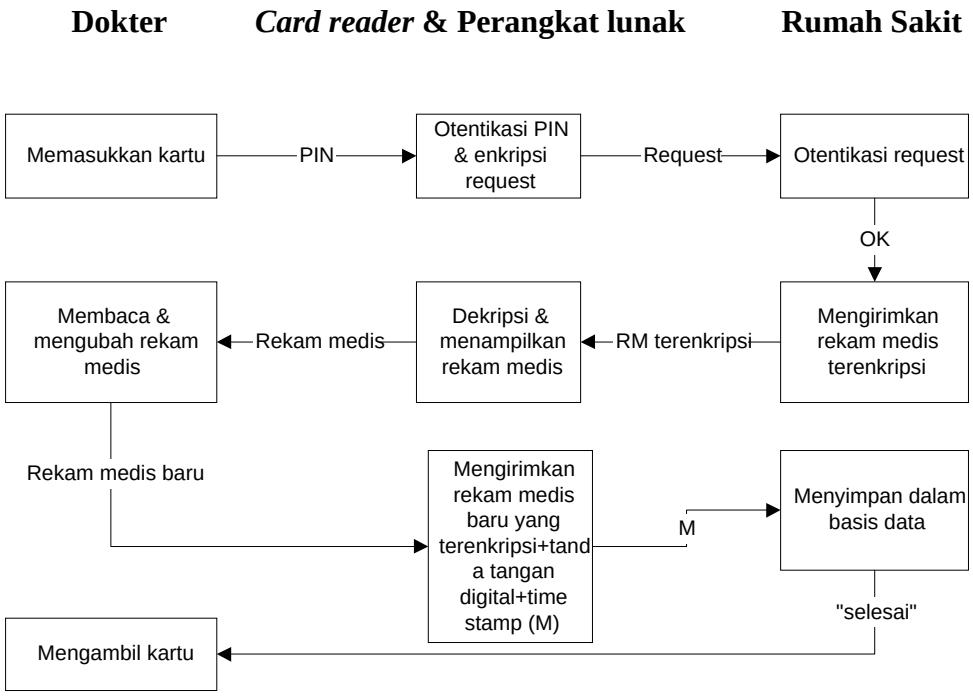
Gambar III.1. Alur penggunaan data untuk rawat jalan sistem *smartcard* kesehatan

Dua sistem *smartcard* kesehatan yang telah diimplementasikan (Motus, Precis) juga menyediakan fasilitas pengiriman data rekam medis melalui jaringan komputer. Fasilitas pengiriman data rekam medis lewat jaringan komputer tersebut ditujukan bagi dokter yang ingin melakukan diagnosa ulang secara *on-line* terhadap data rekam medis yang disimpan di rumah sakit dimana dokter tersebut melakukan tindakan pengobatan. Alur pengiriman data rekam medis lewat jaringan komputer, untuk kedua sistem tersebut pada umumnya berjalan sebagai berikut :

1. Jika dokter ingin melakukan konsultasi dan koreksi terhadap rekam medis pasien-pasiennya secara *on-line,* mereka dapat melakukan koneksi ke jaringan.
2. Koneksi dilakukan dengan memasukkan *smartcard* profesionalnya ke dalam *card*

reader yang terhubung ke komputer dan memasukkan juga nilai PIN miliknya.

3. Sistem akan mengotentikasi *smartcard* dan PIN, jika terbukti bahwa *smartcard* tersebut asli dan nilai PIN sama dengan yang disimpan dalam *smartcard* maka sistem akan membuka koneksi dengan rumah sakit tempat data rekam medis disimpan.
4. Jika pihak peminta data dan rumah sakit sudah dapat saling mempercayai maka data rekam medis yang diminta akan dienkripsi dengan menggunakan kunci sesi yang disepakati oleh kedua pihak. Kunci sesi adalah kunci simetris yang hanya berlaku ketika koneksi berlangsung. Kemudian data terenkripsi tersebut dikirimkan oleh rumah sakit ke peminta data.
5. Data yang telah diterima peminta data akan didekripsi dengan menggunakan kunci sesi tersebut.
6. Jika dokter melakukan koreksi terhadap data maka tanda tangan digital yang juga berisi *timestamp* turut disertakan dalam data. Sebelum data dikirimkan ke rumah sakit, data dienkripsi dengan menggunakan kunci sesi kembali.
7. Data rekam medis yang telah terenkripsi tersebut dikirim ke rumah sakit untuk disimpan di basis data rumah sakit. Koneksi selesai dan kunci sesi tidak berlaku lagi.



Gambar III.2. Alur pengiriman data rekam medis lewat jaringan komputer pada sistem *smartcard* kesehatan

III.2.2 Ukuran Smartcard

Pada umumnya ukuran *smartcard* yang digunakan adalah 8 KB dan 16 KB. Untuk sistem yang menggunakan pasangan kunci privat dan publik membutuhkan *smartcard* dengan memori minimal 16 KB karena untuk menyimpan kunci privat dan tanda tangan digital membutuhkan memori sebesar 2 KB dan komputasi enkripsi/dekripsi yang dilakukan membutuhkan memori yang cukup besar. Data rekam medis yang disimpan disesuaikan dengan kapasitas memori *smartcard*.

III.2.3 Perangkat Lunak Aplikasi

Perangkat lunak aplikasi yang digunakan untuk membaca dan menulis data rekam medis ke dalam *smartcard* haruslah berasal dari pihak yang sama dengan pembuat *smartcard*, jadi *smartcard* dari suatu *vendor* tertentu tidak dapat dibaca

dengan menggunakan perangkat lunak aplikasi dari *vendor* lain. Pihak yang menerbitkan kartu dan layanan aplikasi disebut *card centre*. *Card centre* bertanggung jawab pada semua kartu yang diterbitkannya. Pada kelima sistem ini, data rekam medis pada sistem *smartcard* kesehatan yang berbeda tidak dapat dibaca oleh perangkat lunak aplikasi yang berbeda. Demikian juga rumah-rumah sakit yang mengimplementasikan sistem yang berbeda tidak dapat saling melakukan pertukaran data.

III.2.4 Keamanan Smartcard

Sistem keamanan dalam *smartcard* menggunakan mekanisme enkripsi kunci asimetris atau kunci simetris. Untuk mekanisme enkripsi kunci asimetris menggunakan pasangan kunci privat dan publik, kunci publik boleh diketahui oleh pihak lain sedangkan kunci privat dan algoritma yang digunakan untuk membuat kedua kunci tersebut dirahasiakan. Sedangkan untuk mekanisme kunci simetris, kunci simetris tersebut disimpan dalam perangkat lunak pembuat layanan kartu. Semua informasi rekam medis pasien yang bukan disimpan dalam *smartcard* melainkan yang disimpan di basis data rumah sakit dapat diakses oleh dokter secara *on-line*. Keamanan waktu pengiriman dan penyimpanan informasi dilakukan dengan mengenkripsi setiap data yang dikirim lewat jaringan dengan kunci sesi yang telah disepakati oleh kedua belah pihak. Pengiriman kunci sesi dilakukan dengan mengenkripsi kunci sesi tersebut dengan kunci publik penerima kunci. Hal ini menjamin bahwa hanya penerima kunci yang berwenang yang dapat membuka kunci sesi tersebut, karena hanya pemilik kunci publik saja yang dapat mendekripsi data dengan kunci privat miliknya. Setiap data yang disimpan dalam basis data di *card centre* atau basis data rumah sakit juga dienkripsi dengan menggunakan kunci simetris[Precis99] atau asimetris[Motus99] milik *card centre* atau rumah sakit tersebut sehingga pengakses data rekam medis yang tidak diinginkan, tidak dapat mengerti isi data rekam medis walaupun dia berhasil mendapatkan data rekam medis yang terenkripsi.

III.2.5 Pencatatan

Pencatatan dilakukan terhadap setiap transaksi yang membaca, menambahkan dan koreksi terhadap data rekam medis di dalam *smartcard* atau basis data rumah sakit. Data pencatatan tersebut disimpan di basis data rumah sakit meliputi identitas pengubah, tanggal dan waktu pengaksesan data rekam medis. Untuk keempat sistem *smartcard* kesehatan yaitu Motus, Oberthur, Orga dan Precis menyimpan data rekam medis setiap pemilik *smartcard* baik di basis data rumah sakit yang memberikan tindakan pengobatan maupun basis data di *card centre.* Sedangkan sistem *smartcard* kesehatan Microchart hanya menyimpan data rekam medis pemilik *smartcard* di basis data *card centre.*

III.2.6 Jenis Aplikasi *Smartcard* Kesehatan

Untuk memenuhi segala kebutuhan kesehatan seperti rawat jalan, gawat darurat atau untuk bahan rujukan antar rumah sakit, ada sistem yang menggunakan satu jenis *smartcard* kesehatan yang berisi sejarah rekam medis semua poliklinik untuk semua kebutuhan (gawat darurat, rawat jalan, bahan rujukan), dan ada sistem yang membedakan menjadi beberapa jenis *smartcard* kesehatan sesuai kebutuhan atau sesuai dengan suatu jenis penyakit yang membutuhkan pemeriksaan rutin (misalkan diabetes, jantung, perawatan gigi).

III.3 PERBANDINGAN SISTEM SMARTCARD KESEHATAN DI LUAR NEGERI DENGAN KONDISI-KONDISI DI INDONESIA

Setelah menganalisis kondisi sistem rekam medis di Indonesia dan mengetahui gambaran secara umum sistem *smartcard* kesehatan yang telah diimplementasikan di luar negeri maka akan dilakukan perbandingan sistem-sistem *smartcard* kesehatan yang telah diimplementasikan di luar negeri dengan menggunakan kriteria perbandingan adalah kondisi-kondisi sistem rekam medis di Indonesia. Perbandingan ini bertujuan untuk menganalisis kelayakan sistem *smartcard* kesehatan tersebut dalam memenuhi kebutuhan di Indonesia. Berdasarkan analisis kondisi sistem rekam

medis di Indonesia, deskripsi umum sistem *smartcard* kesehatan yang telah diimplementasikan, dan fungsi-fungsi yang harus dipenuhi oleh *electronic medical record*[MRI99], maka sistem-sistem *smartcard* kesehatan tersebut haruslah mendukung:

- Kebutuhan 1 : Menyediakan proses otentikasi pihak-pihak yang mengakses *smartcard.*

  Kelima sistem *smartcard* kesehatan yang dibandingkan, semuanya menggunakan PIN untuk proses otentikasi. Jika nilai PIN yang dimasukkan sama dengan nilai PIN yang ada di dalam *smartcard* maka pengguna *smartcard* diberi otoritas untuk membaca isi *smartcard* dan memakai fungsi-fungsi dalam *smartcard* yang diwewenangkan kepadanya. Nilai PIN pada setiap *smartcard* kesehatan bernilai unik dan hanya diketahui oleh pemilik *smartcard*. Dengan cara ini dijamin bahwa hanya pemilik *smartcard* yang dapat mengakses data rekam medis.

- Kebutuhan 2 : Tanda tangan digital.

  Untuk memenuhi kebutuhan kedua maka sistem *smartcard* kesehatan harus mendukung tanda tangan digital. Dari kelima sistem *smartcard* kesehatan hanya dua sistem yang mendukung fasilitas penandatanganan digital oleh dokter atau tenaga kesehatan yang membuat, menambah dan melakukan koreksi data rekam medis. Kedua sistem tersebut adalah Motus dan Precis, sedangkan ketiga sistem lainnya, yaitu Microchart, Oberthur, dan Orga, tidak menggunakan fasilitas penandatangan digital. *Smartcard* kesehatan profesional yang dimiliki oleh dokter berisi identitas pribadi, kunci privat, dan kunci publik. Rekam medis yang baru di-*hash* oleh perangkat lunak aplikasi, hasilnya disebut sebagai sidik jari dari rekam medis tersebut. Sidik jari dan *time stamp* dikirimkan ke *smartcard* profesional dokter. Di dalam *smartcard* tersebut, sidik jari dan *time stamp* akan dienkripsi dengan menggunakan kunci privat yang ada di dalam *smartcard*, hasilnya disebut tanda tangan digital. Tanda tangan digital itu kemudian disimpan ke dalam *smartcard* kesehatan pasien. Jika suatu saat keabsahan tanda tangan digital tersebut ingin diperiksa, maka pertama-tama pasien membuat lagi sidik jari

dari data rekam medis asli yang telah ditandatangani. Lalu pasien mendekripsi tanda tangan digital dokter dengan kunci publik dokter tersebut untuk mendapatkan sidik jari yang asli. Pasien kemudian membandingkan kedua sidik jari tersebut. Jika kedua sidik jari tersebut sama, maka dapat diyakini bahwa data rekam medis tersebut ditandatangani oleh dokter yang membuat rekam medis tersebut. Sedangkan pada ketiga sistem *smartcard* kesehatan yang tidak mengikutsertakan tanda tangan digital, untuk membuktikan bahwa seorang tenaga kesehatan telah membuat atau melakukan koreksi data rekam medis maka ketiga sistem ini hanya mencatat setiap tenaga kesehatan yang melakukan login dan kegiatan yang dilakukan oleh tenaga kesehatan tersebut. Jika terjadi kesalahan diagnosa dalam data rekam medis seorang pasien, tidak mudah bagi pihak rumah sakit untuk membuktikan bahwa tenaga kesehatan tersebut telah melakukan kesalahan.

- Kebutuhan 3 : Menjamin keutuhan data rekam medis setelah terjadi proses pengubahan.

  Seperti dijelaskan pada bab sebelumnya bahwa fungsi *hash* satu arah bertujuan untuk meyakinkan bahwa suatu pesan atau dokumen harus utuh, tidak diubah-ubah oleh siapapun juga. Pesan atau dokumen setelah di-*hash* disebut sidik jari. Pada penjelasan sebelumnya bahwa setiap data rekam medis baru atau data rekam medis yang mengalami koreksi pasti disambungkan dengan tanda tangan digital dokter yang bertanggung jawab. Untuk membuktikan bahwa data rekam medis tidak mengalami pengubahan waktu disimpan dalam *smartcard* maka pasien akan membuat sidik jari dari pesan yang disimpan dan kemudian membandingkan dengan sidik jari yang ada pada tanda tangan digital. Jika kedua sidik jari itu identik, maka pasien tersebut dapat yakin bahwa pesan itu utuh tidak diubah-ubah sejak disambungkan dengan tanda tangan digital tenaga kesehatan yang berwenang. Jika data rekam medis tersebut diubah maka akan menghasilkan nilai *hash* yang berbeda. Jaminan dari keamanan sidik jari berangkat dari kenyataan bahwa hampir tidak ada dua *pre-image* yang memiliki nilai *hash* yang sama.

Selain itu, sangat sulit untuk membuat suatu *pre-image* jika hanya diketahui nilai *hash*-nya saja. Kedua sistem *smartcard* kesehatan yang mendukung tanda tangan digital, berarti juga mendukung jaminan keutuhan data setelah terjadi pengubahan. Sedangkan ketiga sistem *smartcard* kesehatan yang tidak mendukung tanda tangan digital, berarti juga tidak mendukung jaminan keutuhan data setelah terjadi pengubahan. Untuk mendukung tanda tangan digital maka dibutuhkan ukuran *smartcard* lebih besar sama dengan 16 KB, harga *smartcard* berukuran 16 KB ke atas relatif mahal pada saat ini. Selain itu dibutuhkan perangkat lunak yang dapat melakukan komputasi cukup rumit. Ketiga sistem yang tidak mendukung tanda tangan digital lebih menitikberatkan pada kemampuan pasar membeli *smartcard* kesehatan tersebut dan mengasumsikan bahwa sedikit pihak yang ingin mengetahui data rekam medis seseorang sehingga keamanan dengan menggunakan nilai PIN sudah cukup aman. *Smartcard* yang digunakan pada ketiga sistem ini jauh lebih murah dibandingkan dengan kedua sistem yang mendukung tanda tangan digital. Tetapi sisi lain, kemungkinan data rekam medis diubah sebelum disimpan dalam *smartcard* lebih tinggi pada ketiga sistem yang tidak mendukung tanda tangan digital ini dibandingkan dua sistem yang mendukung tanda tangan digital. Hal ini tergantung pada kepentingan utama yang ingin dicapai oleh masing-masing sistem.

- Kebutuhan 4 : Menyediakan pencatatan yang dapat dijadikan barang bukti penambahan atau koreksi data rekam medis.

  Kelima sistem *smartcard* kesehatan yang ada melakukan pencatatan terhadap transaksi data rekam medis yang dibaca, dibuat atau dikoreksi. Data-data yang dicatat adalah identitas pengguna, tanggal dan waktu pengaksesan data dan alasan melakukan akses terhadap data. Daftar pencatatan ini disimpan dalam basis data lokal yang aman sehingga tidak ada pihak yang tidak berwenang dapat menghapus bukti pencatatan transaksi pengaksesan data.

- Kebutuhan 5 : Mendukung informasi untuk kebutuhan rawat jalan, bahan rujukan dan keadaan gawat darurat setiap saat.

Untuk memenuhi kebutuhan di atas, kelima sistem *smartcard* kesehatan mendukung hal-hal sebagai berikut :

- Penggunaan *smartcard* untuk menyimpan data rekam medis sehingga mudah untuk dibawa kemana saja. Pasien yang membutuhkan data rekam medis untuk keperluan bahan rujukan atau untuk keperluan lain, tidak perlu datang ke rumah sakit tetapi dapat menggunakan data yang disimpan dalam *smartcard*.
- Dalam keadaan gawat darurat, dokter dapat langsung membaca data rekam medis yang ada di *smartcard*. Di luar negeri untuk memperoleh tindakan pengobatan lebih lanjut (tidak sekedar tindakan pencegahan pertama), pasien gawat darurat tersebut tidak harus memiliki pihak penjamin biaya terlebih dahulu. Kondisi ini berbeda dengan kondisi di Indonesia.
- Pada sistem *smartcard* kesehatan yang ada, penyimpanan data rekam medis pemilik *smartcard* di dalam *smartcard* tergantung pada kapasitas memori *smartcard*, hal ini bertentangan dengan hukum/peraturan rekam medis Indonesia bahwa data rekam medis seseorang harus disimpan sekurangnya lima tahun terhitung dari pembuatan data rekam medis tersebut. Dokter tidak dapat memperoleh data rekam medis yang tidak ada di dalam *smartcard.*
- Sistem *smartcard* kesehatan Motus dan Orga menyediakan beberapa jenis *smartcard* kesehatan untuk kepentingan pengobatan tertentu seperti : *smartcard* kesehatan untuk kondisi gawat darurat, *smartcard* kesehatan untuk asuransi, *smartcard* kesehatan khusus untuk penyakit yang memerlukan pemeriksaan teratur seperti jantung, diabetes, perawatan gigi, dsb. Karena jenis *smartcard* dibedakan maka data rekam medis yang disimpan dalam *smartcard* menjadi lebih lengkap sehingga dapat digunakan untuk bahan rujukan ke rumah sakit lain. Sedangkan ketiga sistem *smartcard* kesehatan yang lain, yaitu, Oberthur, Microchart dan Precis, hanya mengeluarkan satu *smartcard* untuk semua proses pengobatan. Oleh sebab itu data yang disimpan dalam *smartcard* kurang lengkap, lebih berguna digunakan untuk kondisi

gawat darurat dan untuk menghindari interaksi obat yang dapat membahayakan kesehatan pasien, daripada digunakan untuk bahan rujukan antar rumah sakit atau rawat jalan. Hal ini telah mengurangi fungsi data rekam medis menurut hukum/peraturan rekam medis Indonesia, yang mengatur bahwa data rekam medis harus dapat digunakan untuk berbagai keperluan pengobatan. Keuntungan sistem *smartcard* kesehatan dengan satu jenis *smartcard* adalah pemilik *smartcard* tidak perlu memiliki atau membawa banyak *smartcard* dan biaya untuk memiliki *smartcard* kesehatan juga lebih murah. Tetapi kelima sistem tersebut belum dapat menyimpan data rekam medis yang dapat digunakan sebagai bahan rujukan atau rawat jalan minimal lima tahun sesudah data dibuat.

- Sistem *smartcard* kesehatan Motus dan Precis terhubung dengan jaringan komputer sehingga menyediakan fasilitas pengaksesan data rekam medis secara *on-line* oleh dokter yang berwenang kapan saja. Dokter tersebut juga dapat melakukan pemeriksaan atau menambah data rekam medis secara *on-line.* Sedangkan tiga sistem yang lain yaitu Oberthur, Microchart dan Orga, belum mendukung fasilitas jaringan komputer.

- Kebutuhan 6 : Menjamin kerahasiaan data dari pihak yang tidak berwenang.

  - Motus dan Precis : Sistem keamanan kedua sistem ini menggunakan mekanisme enkripsi kunci asimetris, yang menggunakan pasangan kunci privat dan publik. Kelemahan utama kriptografi asimetris adalah proses enkripsi dan dekripsi yang lambat dan mahal. Oleh sebab itu pada sistem Precis data rekam medis dalam *smartcard* dienkripsi dengan menggunakan kunci simetris perangkat lunak aplikasi, sedangkan pada sistem Motus data rekam medis dalam *smartcard* dienkripsi dengan menggunakan kunci privat perangkat lunak aplikasi. Pasangan kunci privat dan kunci publik pemilik *smartcard* pada kedua sistem ini digunakan untuk :

    - **Pesan rahasia**. Jika *A* ingin mengirimkan pesan rahasia untuk *B* maka ia dapat mengenkripsi pesannya dengan kunci publik *B* dan

mengirimnya ke *B.* Hanya *B* yang dapat membaca pesan tersebut karena hanya *B* yang tahu kunci privatnya sendiri. Pesan rahasia ini biasanya merupakan kunci sesi.

- **Sertifikasi**. Jika rumah sakit ingin mengirim data rekam medis ke dokter dan ingin agar dokter tersebut dapat memverifikasi bahwa pesan tersebut memang betul dari rumah sakit, maka rumah sakit dapat mengirimkan dua pesan, yaitu *X* dan *Y*. Dimana X adalah data rekam medis yang dienkrip oleh rumah sakit dengan kunci privatnya. Sedangkan Y adalah data rekam medis yang dienkripsi dengan kunci publik milik dokter. Dokter dapat mendekripsi *Y* dengan kunci privat dokter sendiri sehingga memperoleh data rekam medis. Dokter juga mendekripsi *X* dengan kunci publik rumah sakit, jika hasilnya sama dengan data rekam medis hasil dekripsi Y berarti benar bahwa data rekam medis itu dikirim rumah sakit.
- Jadi mekanisme enkripsi asimetris akan menjamin : proses otentikasi dan otorisasi, melindungi dari serangan *snooping* dan *eavesdropping*, menjaga masuknya penyerang dan pengubahan data oleh pihak yang tidak dapat dideteksi, menjamin keaslian permintaan data dan mencatat bukti permintaan data yang berlangsung melalui penggunaan tanda tangan digital. Tetapi masalah yang ada dengan sistem otentikasi seperti ini adalah masalah keabsahan kunci publik. Masalah keabsahan kunci publik dapat diatasi dengan menggunakan sertifikat digital, namun kelima sistem ini belum mendukung sertifikat digital.

- Microchart : tidak menggunakan mekanisme enkripsi sama sekali. Data hanya dilindungi oleh PIN. Sehingga jika pencuri informasi rekam medis berhasil menyadap data rekam medis yang dikeluarkan oleh perangkat lunak aplikasi maka pencuri tersebut langsung dapat mengerti isi informasi yang disadapnya. Sistem ini sangat tidak aman.
- Oberthur dan Orga : menggunakan mekanisme enkripsi kunci simetris. Kunci

simetris disimpan dalam perangkat lunak aplikasi dan digunakan untuk mengenkripsi data rekam medis sebelum disimpan dalam *smartcard*. Kelemahan utama kriptografi simetris adalah pengirim dan penerima pesan terenkripsi harus tahu kunci yang digunakan dan kunci tersebut harus rahasia. Persoalannya, distribusi kunci rahasia ke banyak pihak tidak mudah karena rentan terhadap pencurian dan manipulasi. Hal ini sangat berbahaya pada sistem *smartcard* Oberthur karena sistem ini menggunakan jaringan untuk mengirimkan data rekam medis antar berbagai pihak. Kelemahan lain lagi adalah jika salah satu pihak (pengirim atau penerima) yang mengetahui kunci tersebut menyalahgunakan kunci, maka dari enkripsinya saja tidak dapat dibuktikan siapa pelaku penyalahgunaan atau penyelewengan itu. Kelebihan kriptografi simetris adalah proses enkripsi dan dekripsi yang cepat dan murah.

- Untuk kelima sistem *smartcard* kesehatan di atas, tindakan-tindakan untuk melakukan pembacaan terhadap data di *smartcard* tanpa sepengetahuan pemilik *smartcard* tersebut adalah sebagai berikut :
  - ***Physical external effect*** : mengubah satu bit nilai d (eksponen pribadi pada mekanisme enkripsi kunci asimetris RSA yang disimpan di dalam *smartcard*) di dalam *smartcard* dari 1 menjadi 0 atau sebaliknya dengan melakukan perubahan tegangan. Dengan adanya *Physical external effect,* maka dapat dilakukan serangan terhadap skema RSA untuk memperoleh nilai d. Dari Nilai d dapat digunakan untuk membuat kunci privat
  - ***Dumb mouse*** *: card reader* yang dapat membaca semua *smartcard* yang mengikuti standar ISO 7816.
  - Untuk mengatasi kedua serangan ini maka *card reader* dan komputer yang terhubung dengan *card reader* tersebut harus dilindungi sehingga tidak ada pihak yang dapat mengisi program atau alat tambahan pada *card reader*. Pengguna hanya dapat memasukkan data-data tertentu melalui *keyboard*, seperti yang dilakukan pada mesin pengambilan uang ATM.

- Pada kelima sistem, dokter tidak dapat merahasiakan data rekam medis pasien di dalam *smartcard* kesehatannya yang kemungkinan dapat memperburuk kondisi pasien tersebut jika mengetahuinya. Hal ini sangat berbahaya bagi proses pengobatan. Demikian juga, dokter dari suatu poliklinik tertentu dapat mengakses informasi rekam medis milik poliklinik-poliklinik lain. Hal ini bertentangan dengan hukum/peraturan rekam medis yang mengatur hal yang sebaliknya.

- Kebutuhan 7 : *Smartcard* dapat diakses oleh semua perangkat lunak aplikasi sistem *smartcard* kesehatan (*interoperability*).

  Kelima sistem *smartcard* kesehatan belum menerapkan standar *interoperability* sehingga untuk mengakses data dalam *smartcard* hanya dapat dengan menggunakan perangkat lunak aplikasi yang dikeluarkan oleh *vendor* yang sama. Hal ini tidak mendukung kebutuhan bahwa data rekam medis dapat digunakan oleh berbagai pihak.

Berikut ini ditampilkan tabel perbandingan kelima sistem *smartcard* kesehatan yang telah diimplementasikan di luar negeri.

III.4 ANALISIS KEBUTUHAN UMUM *SMARTCARD* KESEHATAN YANG SESUAI KEBUTUHAN DI INDONESIA

Berdasarkan perbandingan beberapa teknologi sistem *smartcard* kesehatan di luar negeri yang disesuaikan dengan kondisi sistem rekam medis di Indonesia, diperoleh hasil bahwa sistem *smartcard* kesehatan di luar negeri dapat memenuhi hampir sebagian besar kebutuhan sistem rekam medis di Indonesia. Untuk mengimplementasikan teknologi sistem *smartcard* kesehatan yang telah dibahas di atas di Indonesia, maka beberapa hal yang harus diasumsikan adalah sebagai berikut :

- Masyarakat yang menggunakan *smartcard* kesehatan adalah masyarakat golongan menengah ke atas karena harga *smartcard* yang termurah sekalipun lebih mahal dari kertas dan untuk mengimplementasikan teknologi sistem rekam medis berbasis *smartcard* tidaklah murah. Selain itu, golongan masyarakat menengah ke atas lebih menginginkan kerahasiaan data rekam medis miliknya dan kemudahan-kemudahan yang ditawarkan oleh sistem *smartcard* kesehatan ini, walaupun untuk kedua hal tersebut mereka harus mengeluarkan biaya yang lebih besar dibandingkan dengan sistem rekam medis berbasis kertas yang ada sekarang.
- Rumah sakit yang mengimplementasikan sistem *smartcard* kesehatan adalah rumah sakit yang memiliki kondisi :
  - Sudah terhubung ke jaringan komputer.
  - Memiliki PC dan *card reader* yang terhubung dengan PC tersebut untuk membaca dan menulis data ke/dari *smartcard*.
  - Sumber daya manusia yang dapat menggunakan aplikasi komputer.
  - Memiliki modal keuangan yang cukup untuk mengimplementasikan sistem *smartcard* kesehatan.

Dari perbandingan sistem *smartcard* kesehatan dapat disimpulkan bahwa sistem-sistem yang memenuhi hampir sebagian besar kebutuhan-kebutuhan penggunaan data rekam medis di Indonesia (yaitu memenuhi hal-hal berikut: hanya pihak yang berwenang yang dapat mengakases data di dalam *smartcard* (otentikasi), tanda tangan digital, menjamin pengubahan data tidak dapat dilakukan oleh pihak yang tidak

berwenang (integritas data), pencatatan transaksi, kelengkapan data rekam medis yang disimpan di dalam *smartcard*, mekanisme enkripsi yang digunakan) adalah sistem *smartcard* kesehatan Motus dan sistem *smartcard* kesehatan Precis. Perbedaan utama kedua sistem tersebut adalah :

- Mekanisme enkripsi :
  - Motus : kunci asimetris *smartcard* untuk pertukaran kunci dan kunci asimetris perangkat lunak aplikasi untuk enkripsi data rekam medis.
  - Precis : kunci asimetris *smartcard* untuk pertukaran kunci dan kunci simetris perangkat lunak aplikasi untuk enkripsi data rekam medis.

  Kriptografi simetris kurang aman tetapi proses enkripsi dan dekripsi cepat dan murah. Sedangkan kriptografi asimetris aman tetapi proses enkripsi dan dekripsi lambat dan mahal.
- Kelengkapan data rekam medis dalam *smartcard* :

  Smartcard Motus menyimpan data yang lebih lengkap tetapi dalam beberapa jenis *smartcard* sehingga kurang efisien. Sedangkan *smartcard* Precis menyimpan data rekam medis secara umum saja tetapi efisien karena hanya terdiri dari satu *smartcard*.

Mempertimbangkan kedua hal di atas maka sistem *smart card* kesehatan yang akan diambil sebagai acuan adalah sistem *smartcard* kesehatan yang memadukan kunci asimetris dan simetris untuk keamanannya dan satu jenis *smartcard* kesehatan namun cukup lengkap data rekam medis yang disimpan. Sehingga dalam membuat rancangan *smartcard* kesehatan yang sesuai kondisi di Indonesia, sistem *smartcard* kesehatan perpaduan Motus dan Precis digunakan sebagai acuan.

Kebutuhan-kebutuhan umum *smartcard* kesehatan yang sesuai dengan kondisi di Indonesia, yang dapat didefinisikan dari sistem *smartcard* kesehatan yang telah dibandingkan dan kondisi sistem rekam medis Indonesia, adalah sebagai berikut :

1. Hal-hal yang harus didukung oleh sistem *smartcard* kesehatan :
   - Terdapat c*ard centre* sebagai pihak yang mengeluarkan *smartcard* dan menyimpan data-data sebagai berikut : identitas *smartcard*, identitas pemilik,

data rekam medis dan sertifikat digital. Informasi ini bersifat rahasia dan digunakan jika *smartcard* kesehatan hilang. *Card centre* merupakan basis data terpusat berisi data rekam medis seumur hidup setiap pemilik *smartcard.*

- Pihak-pihak yang membaca informasi dalam *smartcard* dapat diyakini keabsahannya (*authenticity*).
- Informasi dalam *smartcard* hanya boleh diketahui oleh pihak-pihak yang berkepentingan (yaitu pemilik *smartcard*, dokter yang merawat, staf rumah sakit, apoteker), sehingga kerahasiaannya (*confidentiality*) terjamin.
- Pengubahan informasi dalam *smartcard* harus ditandatangani oleh pihak yang dapat melakukan pengubahan yaitu dokter yang merawat. Artinya orang itu adalah benar-benar pihak yang berwenang (*authenticity)* untuk melakukan pengubahan.
- Informasi dalam *smartcard* tidak bisa diubah-ubah oleh pihak-pihak yang tidak berwenang (contoh : pemilik *smartcard*, perusahaan asuransi, staf rumah sakit yang tidak berwewenang), sehingga keutuhannya (*integrity*) terjamin.
- Ada bukti sah yang tidak dapat disangkal (*non-repudiation*) untuk pihak-pihak yang menambah, membuat, atau melakukan koreksi terhadap informasi dalam *smartcard*.
- Dalam keadaan darurat, data rekam medis dalam *smartcard* pasien dapat langsung terbaca.
- Boleh atau tidaknya pasien mengerti akan isi dari pada rekam medis adalah amat tergantung pada kesanggupan pasien untuk mendengar informasi mengenai penyakit yang dijelaskan oleh dokter yang merawatnya, oleh sebab itu tidak semua informasi dalam *smartcard* dapat diakses oleh si pemilik *smartcard*.
- Dokter dari suatu poliklinik tertentu tidak dapat mengakses informasi rekam medis milik poliklinik-poliklinik lain, kecuali apabila informasi rekam medis poliklinik-poliklinik lain tersebut memiliki status dapat dibaca oleh dokter yang merawat dari poliklinik tertentu tersebut[PerMen89]. Sebagai contoh : dokter dari poliklinik THT tidak boleh membaca data rekam medis poliklinik

ginekologi yang tidak berhubungan dengan kebutuhannya.

- Pasien yang kehilangan *smartcard* kesehatannya dapat dengan mudah memperoleh kembali *smartcard* kesehatan baru lengkap dengan data rekam medis yang disimpan dalam *smartcard* yang lama.
- Rumah sakit yang sedang melakukan pengobatan dapat meminta data rekam medis pasiennya kepada rumah sakit lain[PerMen89].
- Dokter dapat mendiagnosa ulang data rekam medis yang dibuatnya secara *on-line* dari mana saja.
- *Smartcard* dapat dibaca oleh segala program aplikasi sistem *smartcard* kesehatan dari berbagai *vendor*[EUHCI96].

2. Kebutuhan pengguna sistem *smartcard* kesehatan yang *interoperability*[EUHCI96] adalah :

a. *Smartcard* kesehatan dokter membutuhkan sistem pengakses kartu yang :

- Mengenali *smartcard* kesehatan secara otomatis dan siap membaca *smartcard* tersebut.
- Membaca data dari *smartcard* yang dikeluarkan oleh sistem *smartcard* kesehatan lain.
- Menampilkan data yang telah dibaca dalam bentuk yang dapat dimengerti pemilik *smartcard*
- Terintegrasi dengan sistem informasi operasional lain yang pemilik gunakan.

b. Pasien membutuhkan *smartcard* kesehatan yang :

- Menyimpan data administrasi dan data gawat darurat yang dibutuhkan.
- Menyiapkan akses *read-only* ke informasi yang *interoperable* yang sesuai melalui berbagai sistem pengaksesan kartu yang *interoperable.*
- Mengamankan informasi penting terhadap pengubahan yang ilegal.
- Melindungi keutuhan informasi yang disimpan terhadap pengubahan yang ilegal.

c. Sistem pengembang dan integrasi membutuhkan :

- Teknologi *smartcard* yang independen.
- Teknologi *Card* Terminal yang independen.

3. Perangkat keras yang dibutuhkan pada sistem *smartcard* kesehatan :
   - *Smartcard* 8KB –16KB
   - *Smartcard reader*
   - PC
   - Modem
4. Perangkat lunak yang dibutuhkan pada sistem *smartcard* kesehatan :
   - Sistem operasi : windows[EUHCI96]
   - Perangkat lunak yang *interoperability* sehingga dapat membaca/menulis data dari/ke *smartcard* dari *vendor* manapun.
5. Teknologi *smartcard* yang digunakan :
   - Teknik enkripsi yang dipakai adalah perpaduan mekanisme asimetris dan simetris[Precis99].
   - Protokol yang digunakan untuk pertukaran data lewat jaringan adalah SSL (*Secure Socket Layer)* karena.protokol ini aman untuk otentikasi *client* dan *server*[SSL99].
   - Mendukung tanda tangan digital[Precis99].
   - Mendukung sertifikat digital[SSL99].
   - Mengacu pada salah satu standar *interoperability* yang ada.

Pada bab berikutnya, penulis mencoba menguraikan rancangan sistem *smartcard* kesehatan yang memenuhi kebutuhan-kebutuhan umum di atas.

BAB IV
RANCANGAN SISTEM SMARTCARD KESEHATAN SESUAI KEBUTUHAN DI INDONESIA

Berawal dari analisis kebutuhan umum untuk sistem *smartcard* kesehatan di Indonesia dan teknologi sistem *smartcard* yang telah ada, pada bab sebelumnya telah disimpulkan bahwa dalam merancang sistem *smartcard* kesehatan Indonesia mengacu pada perpaduan teknologi sistem *smartcard* kesehatan yang telah diimplementasikan yaitu sistem Motus dan sistem Precis. Bab ini menguraikan secara lengkap perpaduan teknologi kedua sistem tersebut dan solusi tambahan untuk memenuhi kebutuhan yang belum terpenuhi oleh kedua sistem tersebut sehingga diperoleh rancangan sistem *smartcard* kesehatan di Indonesia. Kemudian sistem *smartcard* kesehatan sesuai kebutuhan di Indonesia dianalisis apakah sudah memenuhi semua kebutuhan di Indonesia.

IV.1 SPESIFIKASI RANCANGAN

Pertama dijelaskan secara umum mengenai spesifikasi sistem *smartcard* kesehatan yang memenuhi kebutuhan di Indonesia melalui solusi awal. Kemudian solusi awal tersebut dijabarkan lebih rinci, baik dalam rancangan untuk keseluruhan sistem, rancangan untuk *smartcard* dan rancangan protokol pengiriman data lewat jaringan komputer.

IV.1.1 Solusi Awal

Spesifikasi sistem yang sudah ada yang telah memenuhi analisis kebutuhan di Indonesia, dapat digunakan sebagai solusi awal. Solusi-solusi awal tersebut dijabarkan di bawah ini :

1. Penggunaan *password* dan PIN agar pihak-pihak yang membaca informasi dalam

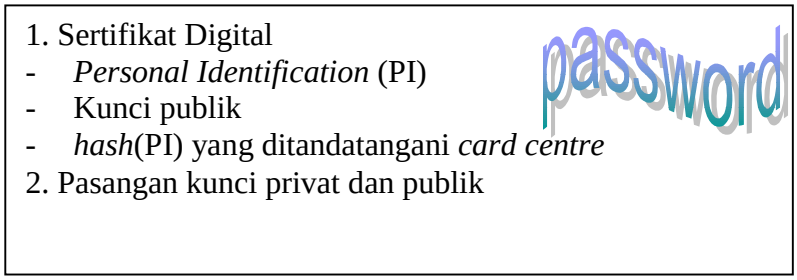
smartcard dapat diyakini keabsahannya.

2. Penggunaan kunci simetris perangkat lunak aplikasi untuk mengenkripsi data rekam medis di dalam *smartcard* agar informasi dalam *smartcard* hanya boleh dibaca oleh pihak-pihak yang berkepentingan.
3. Penggunaan tanda tangan digital untuk menjamin bahwa hanya pihak yang berwenang yang berhak melakukan pengubahan.
4. Penggunaan sidik jari data rekam medis dan tanda tangan digital untuk menjamin bahwa informasi yang disimpan di *smartcard* tidak bisa diubah-ubah oleh pihak-pihak yang tidak berwenang sehingga keutuhan informasi tersebut terjamin.
5. Penggunaan fasilitas pencatatan identitas, waktu dan tanggal, bagi pihak-pihak yang membaca, menambah, melakukan koreksi terhadap data rekam medis. Data pencatatan ini digunakan sebagai bukti sah yang tidak dapat disangkal.
6. Untuk mengatasi pasien yang tidak sadarkan diri atau dalam keadaan darurat maka data rekam medis gawat darurat tidak dilindugi oleh *password* atau PIN.
7. Informasi yang disimpan dalam *smartcard* kesehatan adalah sebagai berikut:
   a. *Smartcard* profesional untuk tenaga medis :
      - Sertifikat digital yaitu berisi sertifikasi dari pihak yang berwenang yang digunakan untuk proses otentikasi pada waktu pengiriman data melalui jaringan komputer. Sertifikasi terdiri dari data pribadi (*personal identity*), serta *hash-value* dari data pribadi dan kunci publik pemilik *smartcard* yang ditandatangani pihak yang berwenang (CA).
      - Pasangan kunci privat dan publik.

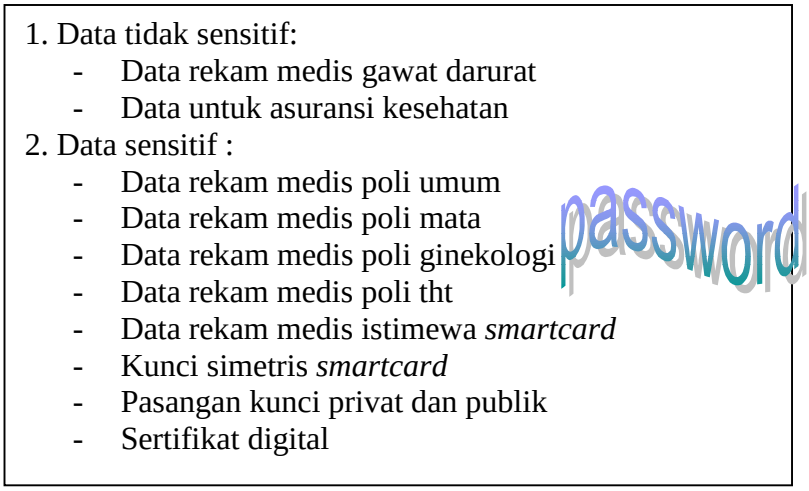
   b. *Smartcard* Pasien :
      - Data tidak sensitif yaitu data yang tidak dilindungi oleh *password* atau PIN yaitu data rekam medis gawat darurat dan data asuransi kesehatan.
      - Data sensitif yaitu data yang dilidungi oleh *password* atau PIN. Bagian data sensitif secara logik terbagi atas direktori-direktori untuk menyimpan data rekam medis, misalnya direktori untuk data rekam medis poli umum,

poli gigi, poli tht, poli mata, data rekam medis rahasia pasien maupun data rekam medis rahasia dokter.

- Pasangan kunci privat dan publik.
- Sertifikat digital.



Gambar IV.1. Informasi data logik *smartcard* profesional



Gambar IV.2. Informasi data logik *smartcard* pasien

Sedangkan identitas pemilik *smartcard* seperti nama, alamat, foto, tanda tangan atau sidik jari, tempat dan tanggal lahir, dapat disimpan di bagian luar/bagian plastik *smartcard.* Hal ini bertujuan untuk menghemat memori *smartcard* sehingga dapat lebih banyak menyimpan data rekam medis.

8. Untuk memudahkan pemilik *smartcard* maka hanya ada satu jenis *smartcard*

kesehatan baik untuk pasien maupun untuk tenaga medis.

9. Agar pasien yang kehilangan *smartcard* kesehatannya dapat dengan mudah memperoleh kembali *smartcard* kesehatan baru lengkap dengan data rekam medis miliknya maka :
   - Setiap jangka waktu tertentu, pihak rumah sakit akan mengirimkan data-data rekam medis baru pasien secara lengkap ke *card centre*. *Card centre* menyimpan data-data rekam medis seluruh pemilik *smartcard* yang dikeluarkannya.
   - Jika pemilik *smartcard* kehilangan *smartcard*nya, maka orang tersebut datang ke *card centre* dan menyatakan identitasnya. Pihak *card centre* akan mengisi kembali *smartcard* yang baru dengan data-data rekam medis dari basis datanya. *Smartcard* yang hilang akan ditandai agar tidak dapat digunakan kembali.
   - Jika pemilik *smartcard* ingin menggunakan data rekam medis miliknya yang tidak terdapat di dalam *smartcard* maka pemilik *smartcard* tersebut dapat menghubungi *card centre.*
10. Untuk mengatasi masalah seorang dokter dari poliklinik tertentu tidak dapat membaca data dari poliklinik lain atau untuk menjaga kerahasiaan suatu data rekam medis pribadi yang tidak diinginkan oleh pemilik *smartcard* terbaca oleh pihak-pihak yang tidak berkepentingan maka data-data rekam medis disimpan dalam direktori-direktori tertentu yang dilindungi dengan sebuah *password* atau PIN tertentu. Dengan adanya *password* atau PIN maka hanya pemilik *smartcard* yang dapat membaca data tersebut.
11. Penggunaan kunci privat dan publik untuk melakukan otentikasi pengiriman data rekam medis lewat jaringan komputer.
12. Penggunaan sertifikat digital untuk menjamin bahwa suatu kunci publik merupakan kunci publik yang sah.
13. Terdapat basis data rekam medis di setiap rumah sakit dan *card centre.* Data-data rekam medis yang disimpan di basis data rumah sakit dan *card centre* tersebut dienkripsi dengan menggunakan kunci simetris masing-masing pihak dan

diasumsikan bahwa penyimpanan kunci simetris tersebut aman.

14. Untuk mengatasi pengiriman dan permintaan data rekam medis oleh pihak-pihak yang berwenang melalui jaringan komputer maka semua rumah sakit yang mengimplementasikan sistem *smartcard* kesehatan harus terhubung ke jaringan komputer.

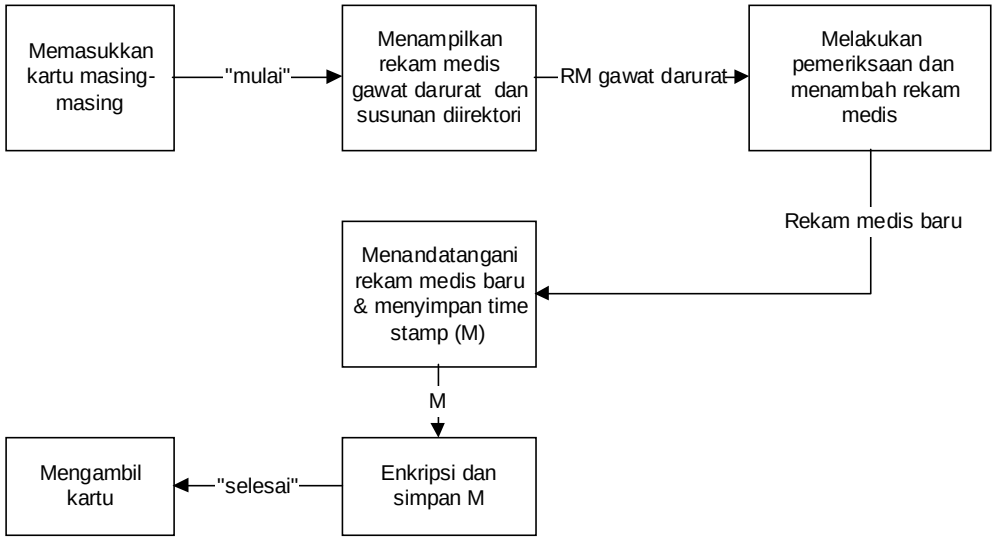
Berdasarkan solusi awal tersebut dan hasil pengamatan lapangan proses pengobatan di Indonesia maka dirancanglah alur data penggunaan rekam medis pada sistem *smartcard* kesehatan di Indonesia secara umum.

IV.1.2 Alur Penggunaan Data Rekam Medis Lapisan Atas

IV.1.2.1 Gawat Darurat

Kemungkinan besar pasien yang datang pada kondisi gawat darurat sulit untuk berkomunikasi, namun pasien tersebut harus mendapat tindakan pengobatan yang cepat dan tepat, oleh sebab itu data rekam medis gawat darurat tidak dilindungi oleh *password* atau PIN tertentu. Selain itu pada data pribadi dalam *smartcard* terdapat pihak asuransi kesehatan yang dapat menjamin biaya pengobatan pasien sehingga pasien gawat darurat tersebut dapat langsung memperoleh tindakan kesehatan selanjutnya seperti operasi, pemberian infus, dan sebagainya. Data rekam medis pada proses ini diambil secara *off-line* dari *smartcard*. Alur penggunaan data pada gawat darurat adalah :

Pasien & Dokter ***Reader*** **& Perangkat lunak** **Dokter**

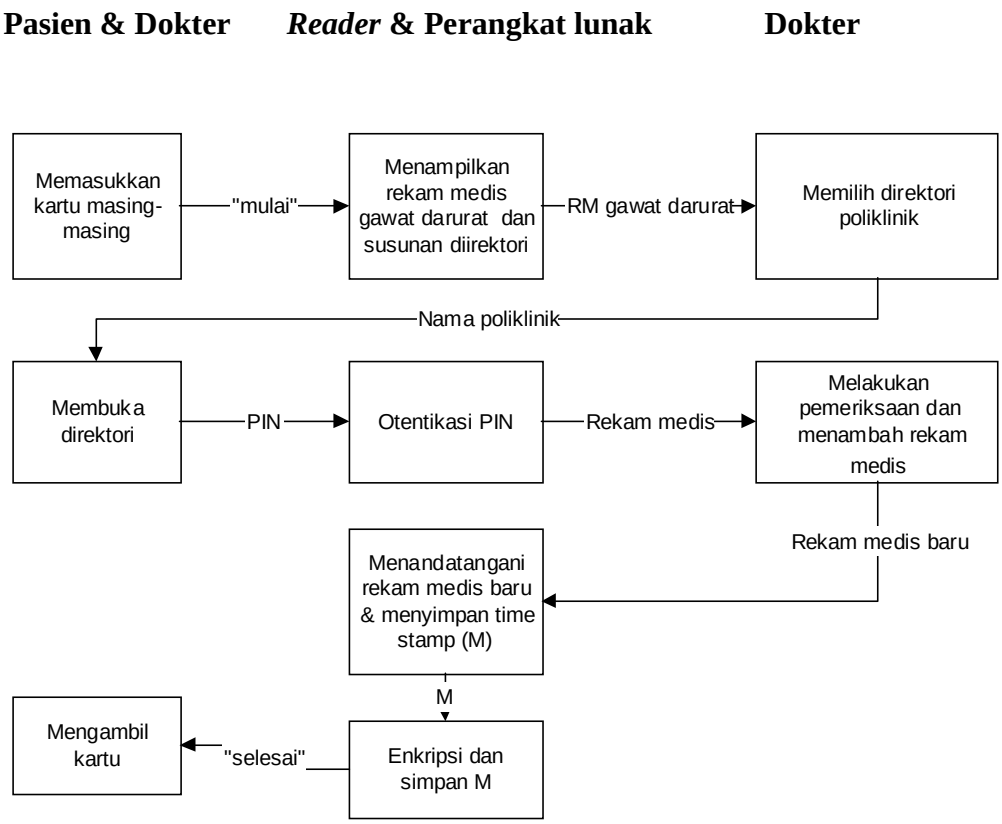


Gambar IV.3. Diagram alur data untuk keadaan gawat darurat

1. Dokter memasukkan *smartcard* miliknya dan *smartcard* milik pasien ke dalam *reader*.
2. Data tentang asuransi kesehatan pemilik *smartcard* dan rekam medis keadaan gawat darurat dapat langsung dibaca tanpa menggunakan *password* dan PIN karena ada kemungkinan untuk keadaan darurat si pasien tidak sadarkan diri.
3. Setelah pemeriksaan, dokter dapat menambah atau mengubah data rekam medis. Kemudian dokter menandatangani data rekam medis tersebut. Data rekam medis baru beserta tanda tangan digital dokter akan dienkripsi dengan menggunakan kunci simetris perangkat lunak aplikasi.
4. Data rekam medis terenkripsi disimpan dalam basis data rumah sakit dan *smartcard* pasien.
5. Pemilik dapat mengambil kembali *smartcard* miliknya. Proses selesai.

IV.1.2.2 Bahan Rujukan/Rawat Jalan

Pasien dapat berobat dari satu rumah sakit ke rumah sakit yang lain, dengan adanya data rekam medis di dalam *smartcard* maka pasien tidak perlu datang ke rumah sakit sebelumnya untuk meminta data rekam medisnya. Data rekam medis pada proses ini diambil secara *off-line* dari *smartcard* karena data rekam medis yang diminta terdapat di dalam *smartcard*. Alur penggunaan data untuk bahan rujukan atau rawat jalan dimana data yang dibutuhkan ada di dalam *smartcard*:



Gambar IV.4. Diagram alur data untuk keperluan rawat jalan

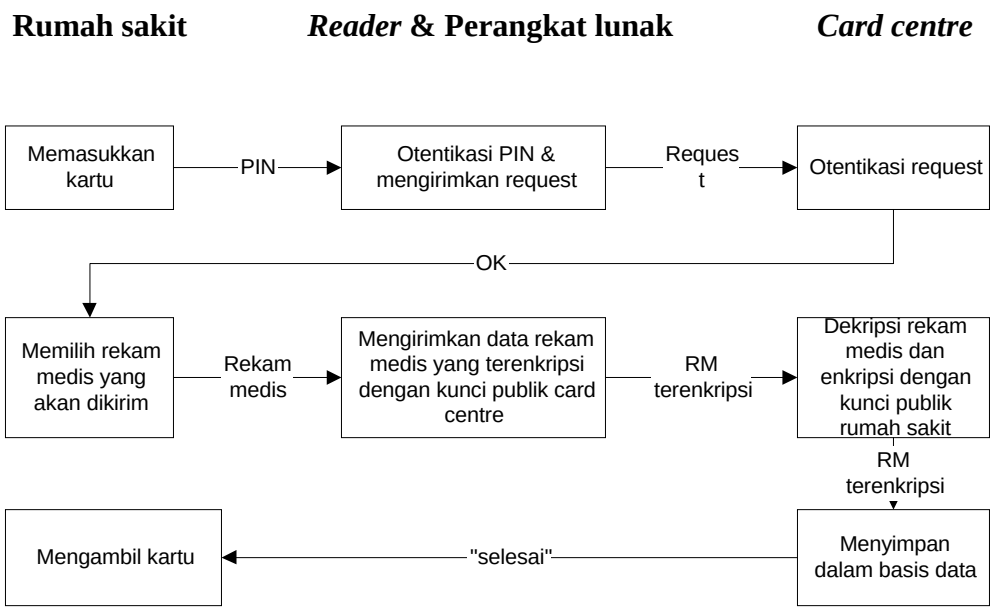
1. Dokter dan pasien di tempat pelayanan kesehatan memasukkan *smartcard* kesehatan miliknya masing-masing ke *reader*.
2. Untuk keperluan rawat jalan, dokter dan pasien harus memberikan *password* atau PIN kepada perangkat lunak sistem *smartcard* kesehatan.

3. Perangkat lunak mengecek nilai *password* atau PIN tersebut sama atau tidak dengan yang ada di dalam *smartcard*. Jika sama maka *smartcard* mengijinkan akses dan menampilkan susunan direktori yang ada di dalam *smartcard*.
4. Untuk masuk ke direktori poliklinik tertentu, misalkan direktori poliklinik gigi, pasien terlebih dahulu harus memasukkan *password* atau PIN tertentu. Jika *password* atau PIN tersebut benar maka data rekam medis di dalam direktori poli gigi dapat dibaca.
5. Jika dibutuhkan untuk mengakses data rekam medis di direktori poliklinik yang lain atau direktori rekam medis yang dirahasiakan oleh pemilik atau direktori rekam medis yang dirahasiakan oleh dokter, atas permintaan dokter yang memeriksa karena data tersebut dibutuhkan untuk menunjang pelayanan kesehatan yang sedang diberikan maka pasien harus terlebih dahulu memasukkan *password* atau PIN.
6. Setelah pemeriksaan selesai, dokter dapat menambah atau mengubah data rekam medis. Data rekam medis baru tersebut beserta tanda tangan digital dokter dienkripsi dengan menggunakan kunci simetris perangkat lunak aplikasi.
7. Data rekam medis terenkripsi disimpan dalam basis data rumah sakit dan *smartcard*.
8. Pemilik dapat mengambil kembali *smartcard* miliknya. Proses selesai.

IV.1.2.3 Pengiriman Data Selesai Proses Pengobatan Ke *Card Centre*

Dalam jangka waktu tertentu, rumah sakit yang terhubung ke *card centre* mengirimkan data rekam medis baru ke *card centre*. Data rekam medis ini digunakan untuk mengisi kembali data-data ke dalam *smartcard* yang baru apabila *smartcard* sebelumnya hilang atau rusak dan juga untuk memberikan informasi rekam medis yang tidak ada di dalam *smartcard* dan diminta oleh pemilik *smartcard*. Proses ini dilakukan secara *on-line* dengan *smartcard* sebagai alat untuk melakukan

otentikasi.Alur pengiriman data selesai proses pengobatan ke *card centre* adalah sebagai berikut :



Gambar IV.5. Diagram alur data pengiriman data rekam medis ke *card centre* melalui jaringan komputer

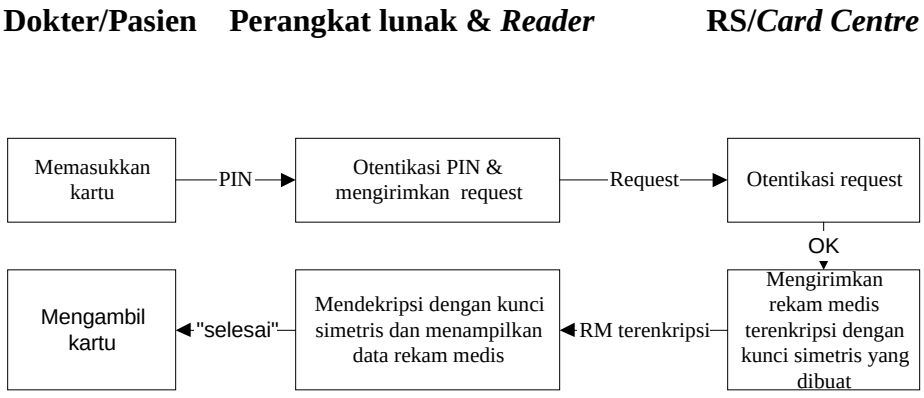
1. Petugas rumah sakit memasukkan *smartcard* profesional miliknya ke *reader* dan memberikan *password* atau PIN kepada perangkat lunak.
2. Perangkat lunak mengecek nilai *password* atau PIN tersebut sama atau tidak dengan yang ada di dalam *smartcard*. Jika sama maka *smartcard* mengijinkan akses.
3. Perangkat lunak akan membuka koneksi ke *card centre.* Kedua belah pihak akan saling mengotentikasikan pihak yang diajak berkomunikasi.
4. Setelah kedua pihak yakin bahwa mereka saling berhubungan dengan pihak yang sah maka perangkat lunak pihak pertama kemudian mengirim data-data rekam medis yang telah dienkripsi dengan menggunakan kunci sesi yang dibuat oleh *card centre.*
5. Oleh *card centre* data-data tersebut disimpan dalam basis data *card centre* dalam

bentuk yang tetap terenkripsi dengan menggunakan kunci simetris miliknya. Data disimpan dalam bentuk terenkripsi untuk menjaga data agar tidak dibaca oleh petugas basis data di *card centre.*

6. Proses selesai.

IV.1.2.4 Dokter /Rumah Sakit Meminta Data Rekam Medis Ke Rumah Sakit Atau Pasien Meminta Data Rekam Medis Ke Card Centre

Dokter dapat meminta data rekam medis ke rumah sakit untuk melakukan diagnosa ulang terhadap data tersebut. Sedangkan pasien dapat meminta data rekam medis yang sudah tidak lagi disimpan di *smartcard* karena keterbatasan memori untuk digunakan bagi keperluan pengobatan atau keperluan pribadi pemilik *smartcard*. Rumah sakit yang sedang merawat seorang pasien dapat juga meminta data pada pihak rumah sakit yang mengadakan pengobatan sebelumnya. Proses ini dilakukan secara *on-line* dengan *smartcard* sebagai alat otentikasi. Alur permintaan data rekam medis ke rumah sakit atau pasien meminta data rekam medis ke *card centre* adalah sebagai berikut :



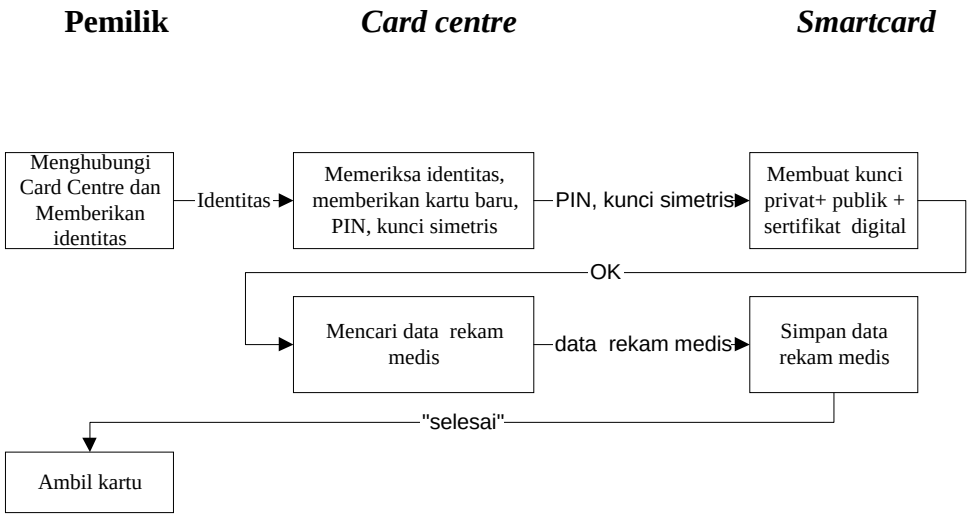
Gambar IV.6. Diagram alur data pengiriman data melalui jaringan komputer

1. Dokter/rumah sakit atau pasien yang hendak meminta data memasukkan *smartcard* miliknya ke *reader* dan memasukkan *password* atau PIN.

2. Perangkat lunak mengecek nilai *password* atau PIN tersebut sama atau tidak dengan yang ada di dalam *smartcard*. Jika sama maka *smartcard* mengijinkan akses.
3. Perangkat lunak dokter atau pasien akan membuka koneksi ke rumah sakit atau *card centre.* Kedua belah pihak akan saling mengotentikasikan pihak yang diajak berkomunikasi.
4. Setelah kedua pihak yakin bahwa mereka saling berhubungan dengan pihak yang sah maka kemudian pihak rumah sakit atau *card centre* yang diminta mengirimkan data-data rekam medis yang telah dienkripsi dengan menggunakan kunci sesi yang dibuat oleh *card centre* atau rumah sakit.
5. Proses selesai. Jika dokter ingin mengirimkan data rekam medis yang mengalami penambahan maka prosesnya sama dengan proses pengiriman data oleh pihak rumah sakit ke *card centre.* Rumah sakit yang meminta data rekam medis dari rumah sakit lain dan mengadakan penambahan pada data rekam medis tersebut maka data rekam medis baru tersebut tidak perlu dikirimkan kepada rumah sakit yang memberikan data karena data rekam medis baru itu telah menjadi milik rumah sakit yang mengadakan penambahan [PerMen89].
6. Dokter/pasien mengambil *smartcard.* Proses selesai.

IV.1.2.5 Pembuatan *Smartcard* Baru/ *Smartcard* Hilang

Proses pembuatan *smartcard* baru atau *smartcard* yang hilang dilakukan secara *off-line*. Alur pembuatan *smartcard* baru atau *smartcard* yang hilang adalah sebagai berikut :

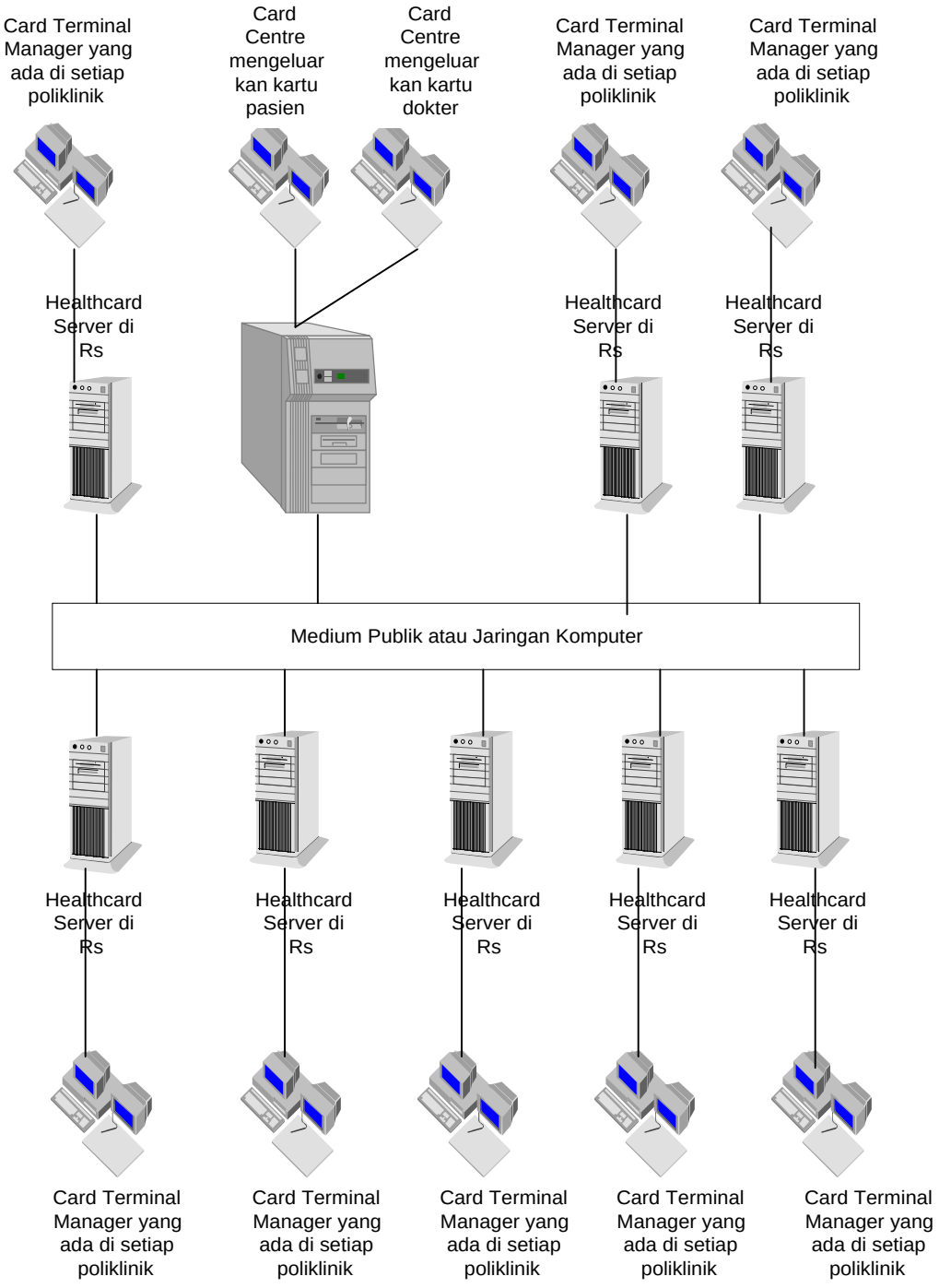


Gambar IV.7. Diagram alur data pembuatan *smartcard* baru

1. Seseorang yang kehilangan *smartcard* pasien atau profesional dapat menghubungi atau datang ke *card centre* untuk melaporkan *smartcard* yang hilang dan meminta *smartcard* yang baru.
2. Orang tersebut akan memberikan identitas dirinya dan *card centre* akan mengecek kebenaran identitas tersebut.
3. Jika identitasnya benar maka orang tersebut akan diberikan *smartcard* baru. Oleh pemilik, *smartcard* baru tersebut akan diisi dengan pasangan kunci privat dan publik *smartcard* dan sertifikat digital miliknya. Kunci privat dan kunci publik dibuat langsung oleh pemilik *smartcard* di dalam *smartcard* sehingga tidak ada pihak yang mengetahui kunci privat dan kunci publik tersebut.
4. Oleh *card centre*, masing-masing *smartcard* diberi *password* atau PIN yang hanya diketahui oleh pemilik *smartcard* tersebut.
5. Untuk *smartcard* pasien, *smartcard* tersebut diisi dengan data rekam medis dari basis data *card centre* dan data asuransi kesehatan miliknya.
6. *Smartcard* yang hilang akan ditandai untuk tidak dapat digunakan kembali. Proses selesai.

IV.1.3 Konfigurasi Sistem

Sesuai dengan solusi awal di atas yaitu sistem penggunaan *smartcard* untuk kesehatan yang *interoperability* maka sistem *smartcard* kesehatan ini disusun dengan menggunakan standar *interoperability* sistem *smartcard* kesehatan yang dikeluarkan oleh EU/G7 *Healthcards* – WG7[EUHCI 96]. Alasan pemilihan standar *interoperability* ini karena standar ini sudah diimplementasikan oleh proyek *DiabCard, CardLink, TrustHealth, Panacea dan Quasi Niere*, disusun berdasarkan standar sistem *smartcard* kesehatan Eropa G7 dan Jepang sehingga penggunaannya menjadi lebih luas dan telah dilakukan penelitian sejak bulan Agustus 1996. Selain itu informasi yang diperoleh oleh penulis mengenai standar *interoperability* ini cukup lengkap. Konfigurasi sistem yang ditunjukkan oleh gambar di bawah menunjukkan infrastruktur yang umum ada antar rumah sakit.

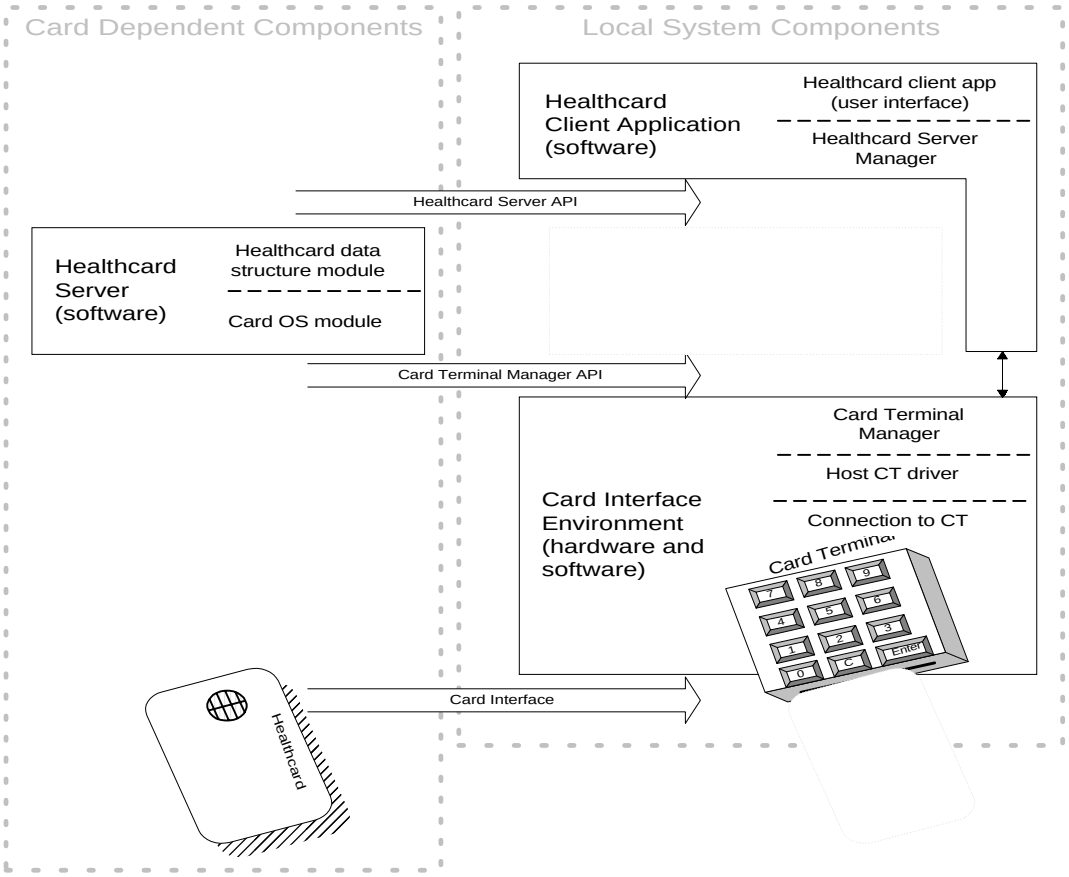


Gambar IV.8. Konfigurasi sistem *smartcard* kesehatan

Secara garis besar sistem dapat digambarkan sebagai berikut :

- Pihak-pihak yang terlibat adalah : dokter, pasien, *card centre* dan rumah sakit.
- *Card centre* dan setiap rumah sakit mempunyai komponen modul dan antarmuka sistem yang diatur oleh standar *interoperability* EU/G7 *Healthcards* – WG7 dan kedua pihak ini juga memiliki basis data rekam medis masing-masing sesuai dengan fungsi dan kebutuhannya. Susunan modul dan antar muka untuk sistem *smartcard* kesehatan yang *interoperability* telah dijelaskan sebelumnya pada bab landasan teori.
- Rumah sakit yang telah memiliki sistem informasi yang terkomputerisasi tetap dapat menggunakan sistem informasinya tersebut. Sistem informasi tersebut ditambahkan sistem *smartcard* kesehatan yang sesuai dengan standar *interoperability* sistem *smartcard* kesehatan EU/G7 *Healthcards* – WG7 [EUHCI96].
- Setiap rumah sakit dan *card centre* terhubung satu sama lain melalui medium publik atau jaringan komputer. Jaringan komputer digunakan jika dibutuhkan pengiriman data dari satu pihak kepada pihak lain secara *on-line*.
- *Card* Terminal mengecek jenis *smartcard* yang digunakan dan me-*load* perangkat lunak *Healthcard Server* yang sesuai dengan jenis *smartcard* dan membaca data dari *smartcard*. Data yang dibaca dari *smartcard* dipetakan sesuai dengan struktur data yang *interoperability* oleh *Healthcard Server* sehingga data tersebut siap digunakan oleh aplikasi dari berbagai *vendor*. Jika data yang sudah *interoperability* tersebut ingin disimpan ke dalam *smartcard*, maka perangkat lunak aplikasi dapat mengubah data yang *interoperability* menjadi data yang sesuai dengan struktur data *smartcard* miliknya.
- Setiap pembacaan, penambahan, dan koreksi terhadap data rekam medis disimpan di dalam basis data oleh pihak rumah sakit melalui fasilitas pencatatan.

Model *Healthcard System* yang *interoperablity* menurut kebutuhannya dapat dibagi menjadi dua bagian, yaitu "*Local System Components"* dan "*Card Dependent Components*".



Gambar IV.9. Pembagian sistem menjadi komponen untuk pengguna dan kartu

a. Kebutuhan untuk *Local System Components* adalah sebagai berikut :

1. Kebutuhan aplikasi *client* -- aplikasi *healthcard client* yang *interoperable* harus :
   - Menyediakan antar muka yang memperbolehkan pengguna meminta sistem untuk membaca sebuah *smartcard* kesehatan.
   - Menampilkan informasi yang dibaca dari *smartcard* kesehatan menggunakan API *Healthcard Server* dalam sebuah bentuk yang dapat dibaca.
   - Memperbolehkan *smartcard* kesehatan yang *interoperable* untuk dinon-aktifkan dan diambil dari *Card* Terminal.
2. Kebutuhan *Card Interface Environment*-- *Card Interface Environment* terdiri

dari kombinasi :

- Satu atau lebih *Card* Terminals (*reader)*
- Perangkat lunak di *Card* Terminal.
- Koneksi ke sistem komputer *host* lokal.
- Perangkat lunak pada sistem komputer *host.*

Card Interface Environment :

- Harus menyediakan *Card* Terminal *Manager API* (CTM-API) yang menyediakan fungsi-fungsi pemanggilan *Card* Terminal *Manager API.*.
- Harus mendukung komunikasi dengan *smartcard* T=0 dan *smartcard* T=1 sesuai ISO7816.
- Memperbolehkan komunikasi transparan antara perintah dan data dari CTM-API ke *smartcard.*

b. Kebutuhan untuk *Card Dependent Components* adalah sebagai berikut :

1. Kebutuhan *smartcard* kesehatan -- sebuah *smartcard* kesehatan yang *interoperable* harus memenuhi :
   - Sesuai dengan ISO 7816 bagian 1 sampai 4.
   - Mendukung akses ke *Card Application Data* sehingga dapat membaca data dari *smartcard*.
   - Memperbolehkan penyimpanan data yang ditandai sebagai "*Mandatory*" (M). Juga memperbolehkan penyimpanan sebanyak-banyaknya terhadap data yang ditandai sebagai "*Recommended*" (R) selama kapasitas *smartcard* memungkinkan dan memenuhi ketetapan-ketetapan perancangan *smartcard*.
   - Memperbolehkan akses *read-only* ke kumpulan data yang *interoperable* tanpa menggunakan alat atau prosedur keamanan tertentu. Informasi yang penulis atau pasien inginkan agar tidak dibaca secara bebas dapat tidak diikutsertakan kumpulan data yang *interoperable* atau dapat diakses dengan menggunakan alat atau prosedur pengamanan yang *interoperable* (akan didefinisikan oleh *smartcard* kesehatan profesional sekarang atau di masa depan yang *interoperable*).

- Mencegah pengubahan ilegal terhadap data *smartcard* kesehatan yang *interoperable.*

2. Kebutuhan *Healthcard Server*—penerbit *smartcard* kesehatan yang *interoperable* harus menyediakan perangkat lunak *Healthcard Server* yang *interoperable* sehingga memperbolehkan akses ke *smartcard* kesehatan yang mereka keluarkan. Perangkat lunak *Healthcard Server* yang *interoperable* memenuhi kebutuhan sebagai berikut *:*

- Harus disediakan dalam bentuk yang dapat dijalankan di Window TM 3.1 (dan versi Window TM berikutnya).
- Harus dapat dikembangkan untuk lingkungan operasi yang biasa digunakan.
- Harus dibuat dapat tersedia luas baik secara gratis atau hanya terkena biaya distribusi untuk penggunaan pada sistem *smartcard* kesehatan yang *interoperable.*

Tugas *Healthcard Server* adalah sebagai berikut :

- Merespon ke fungsi pemanggilan *Healthcard Server API.*
- Berkomunikasi dengan *smartcard* kesehatan melalui CTM-API untuk memperoleh data yang *interoperable* yang diminta.
- Mengembalikan data yang *interoperable* yang dibaca dari *smartcard* ke *Healthcard Server API.*
- Ketika informasi rekam medis gawat darurat dibaca dari *smartcard*, data dalam setiap kategori yang ditandai sebagai *Mandatory* harus ditampilkan. Strukturnya harus sesuai dengan yang telah dispesifikasikan dan tanda yang menunjukkan bahwa data di *smartcard* sudah dibaca.

3. Kebutuhan untuk mengubah *smartcard* -- sistem yang dapat mengubah *smartcard* kesehatan yang *interoperable* seharusnya secara otomatis mengubah rincian otorisasi data ketika data yang lain diubah.
4. Kebutuhan lain -- kebutuhan yang dinyatakan di atas hanya mencakup aspek yang penting untuk *interoperability.* Penerbit *smartcard* kesehatan juga penting untuk memenuhi kebutuhan seperti berikut :

- Perangkat lunak untuk mengeluarkan atau mengubah *smartcard*.
- Struktur data untuk penyimpanan informasi dalam *smartcard*. Hal ini sesuai dengan ENV12018 atau dapat didefinisikan secara lokal.
- Menambahkan nilai perangkat lunak yang menyediakan fasilitas tambahan atau kemampuan lebih tinggi.

IV.1.4 *Smartcard* Yang Digunakan

Dalam sistem ini, perancangan protokol kriptografi dilakukan terhadap *public key cards* tetapi tidak secara spesifik untuk *smartcard* dari suatu *vendor*. Pemilihan *public key cards* adalah karena sistem keamanannya sangat baik karena mendukung kriptografi kunci publik atau kriptografi asimetris dan kriptografi simetris, serta dapat menyimpan kunci di dalam *smartcard.* Namun *smartcard* jenis ini harganya lebih mahal dibandingkan dengan *smartcard memory protected* atau *microprocessor*. Untuk masing-masing pasien dan tenaga medis hanya ada satu jenis *smartcard* kesehatan yaitu *smartcard* kesehatan pasien dan *smartcard* kesehatan profesional.

IV.1.5 Rancangan Pada *Smartcard*

Rancangan sistem *smartcard* kesehatan terbagi atas dua bagian besar yaitu pengiriman data antara aplikasi dan *smartcard* dan pengiriman data melalui jaringan komputer diantara pihak-pihak yang berwenang. Bagian ini menguraikan bagaimana data rekam medis disimpan dalam *smartcard* dan pertukaran pesan yang terjadi antara aplikasi dan *smartcard*.

IV.1.5.1 Arsitektur Skema Direktori

Skema direktori yang di dalam *smartcard* sehingga *file-file* dalam *smartcard* tidak dapat dibaca oleh sembarang pihak adalah sebagai berikut :

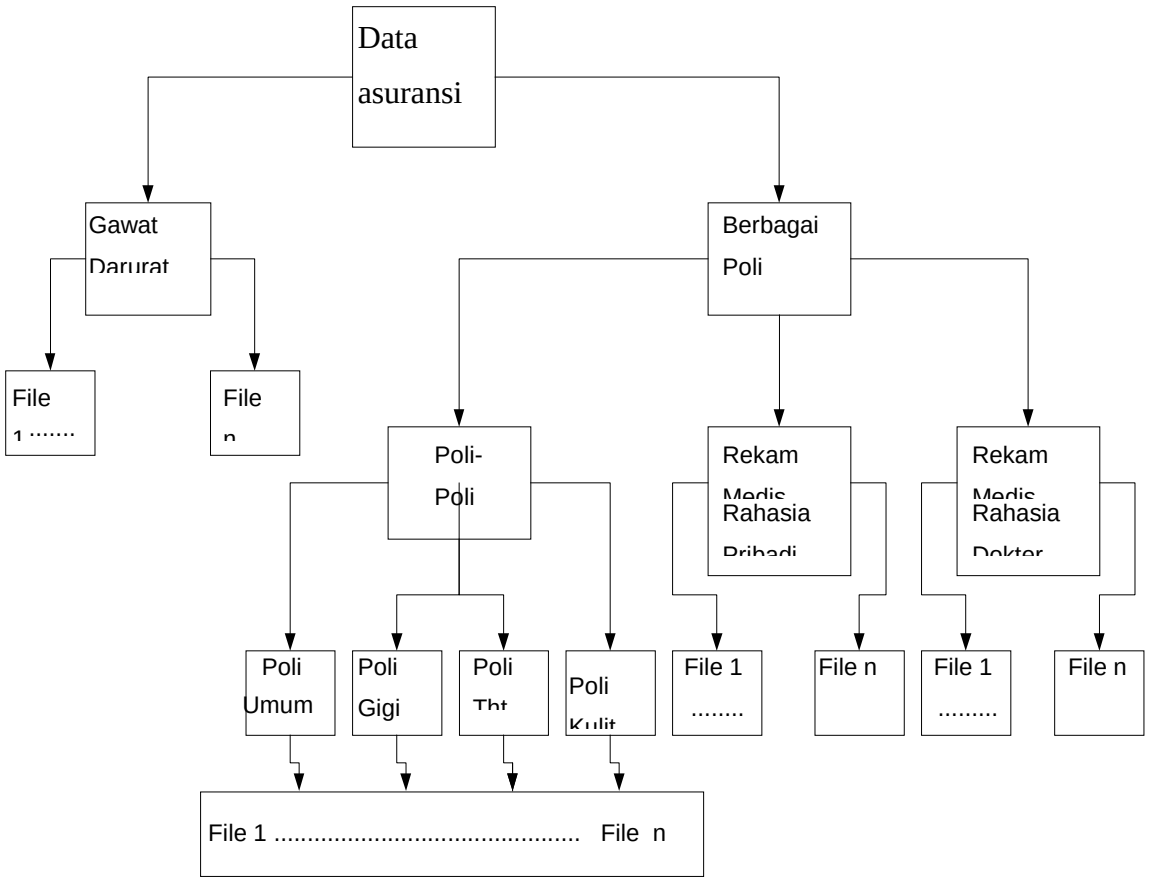
(a) Direktori data asuransi kesehatan : berisi data asuransi kesehatan pemilik *smartcard*. Hak akses : dapat dibaca oleh semua pihak, tidak membutuhkan

password atau PIN pada awal masuk.

(b) **Direktori gawat darurat :** berisi data rekam medis yang diperlukan dalam keadaan darurat . Hak akses : dapat dibaca oleh semua pihak, tidak membutuhkan *password* atau PIN tertentu yang berbeda dengan *password* untuk masuk ke *smartcard*.

(c) **Direktori berbagai poliklinik :** berisi data rekam medis poliklinik-poliklinik yang pernah dikunjungi pemilik *smartcard*, bagian ini terbagi atas beberapa sub direktori. Hak akses : hanya dapat dibaca oleh pemilik *smartcard*, dengan memasukkan *password* atau PIN. Sub direktori-sub direktori di bawahnya adalah:

1) **Direktori poli-poli :** berisi data rekam medis setiap poli yang diperlukan sebagai bahan rujukan. Hak akses : Untuk masuk ke sub direktori-sub direktori masing-masing poli, sebelumnya harus memasukkan *password* atau PIN yang sama dengan *password* atau PIN untuk masuk ke direktori berbagai poli.
2) **Direktori rekam medis rahasia pribadi :** berisi data rekam medis dari semua poli yang dirahasiakan oleh si pemilik *smartcard*. Yang ditampilkan hanya judul-judul dari data rekam medis tersebut. Hak akses : untuk masuk ke direktori ini, sebelumnya harus memasukkan *password* atau PIN yang sama dengan *password* atau PIN untuk masuk ke direktori bahan rujukan.
3) **Direktori rekam medis rahasia dokter :** berisi data rekam medis dari semua poli yang dirahasiakan oleh dokter dari pemilik *smartcard* karena dianggap dapat membahayakan kesehatan pasien. Yang ditampilkan hanya judul-judul dari data rekam medis tersebut. Hak akses : untuk masuk ke direktori ini, sebelumnya harus memasukkan *password* atau PIN yang sama dengan *password* atau PIN untuk masuk ke direktori bahan rujukan. Pemilik *smartcard* disarankan untuk tidak membaca rekam medis ini jika akan membahayakan kesehatannya. Jika rekam medis ini tidak rahasia lagi dapat dipindahkan ke direktori poli yang bersangkutan.



Gambar IV.10. Skema direktori di *smartcard*

IV.1.5.2 Arsitektur Kemanan *Smartcard*

Kunci-kunci yang dibutuhkan oleh *smartcard* untuk menjaga keamanan data :

1. **PIN :** untuk memeriksa apakah pemakai memang pemegang sah dari *smartcard* (otentikasi).
2. **Identitas pemberi layanan atau kode perusahaan :** untuk memastikan agar hanya *smartcard* yang mempunyai kode dari perusahaan tersebut yang bisa menggunakan layanan. Jadi *smartcard* yang dikeluarkan oleh perusahaan pemberi

layanan A tidak dapat digunakan untuk mengakses layanan dari perusahaan B, kecuali jika kedua kode dari perusahaan tersebut di tulis di dalam *smartcard*. Kode perusahaan sama untuk semua *smartcard* dari perusahaan tersebut. Kode perusahaan hanya diketahui oleh perusahaan tersebut dan sulit untuk diketahui oleh pihak lain.

3. **Kunci simetris :** untuk mengenkripsi data dalam *smartcard* supaya tidak bisa dibaca oleh pihak yang tidak berwenang. Kunci simetris ini tidak diketahui oleh pemakai maupun pihak luar, hanya diketahui oleh penerbit kartu atau perangkat lunak aplikasi. Sehingga jika seorang penyerang berhasil memperoleh nilai PIN dan kode perusahaan maka penyerang tersebut tidak dapat melakukan dekripsi data yang ada di dalam *smartcard.*
4. **Pasangan kunci privat dan kunci publik :** untuk membuktikan identitas yang handal pada waktu pemilik *smartcard* menggunakan layanan berupa pengiriman data melalui jaringan komputer. Pasangan kunci privat dan kunci publik ini disimpan di dalam *smartcard* secara terenkripsi dengan menggunakan kunci simetris[Schn96]. Akses baca kunci tersebut dijaga oleh kode perusahaan. Dengan demikian walaupun nilai PIN dan kode perusahaan diketahui, nilai kunci privat dan kunci publik tidak diketahui oleh si penyerang karena si penyerang tidak dapat mengetahui kunci simetris untuk melakukan dekripsi terhadap kunci-kunci tersebut. Kunci publik diketahui oleh umum tetapi disimpan juga di dalam kartu karena kedua kunci tersebut digunakan untuk melakukan verifikasi bahwa kedua kunci tersebut merupakan pasangan kunci yang sebenarnya. Proses verifikasi tersebut adalah :
    - Dekripsi kunci privat dan kunci publik dengan menggunakan kunci simetris sehingga diperoleh nilai kunci privat dan kunci publik.
    - Enkripsi sebuah pesan dengan menggunakan kunci publik.
    - Dekripsi pesan yang terenkripsi tersebut dengan kunci privat.
    - Bandingkan pesan awal dengan pesan yang diperoleh. Jika sama maka kedua kunci tersebut memang pasangan yang sebenarnya.

    Untuk membuktikan kunci publik yang sah maka digunakan sertifikat digital

yang berisi kunci publik tersebut.

Supaya penyerang tidak dapat memasukkan program untuk mencuri data dan menambah alat-alat untuk melakukan *physical external attack* atau membuat sebuah *dumb mouse* maka antara terminal komputer dan *smartcard reader* harus didedikasikan untuk aplikasi *smartcard* tersebut, seperti yang terjadi untuk mesin pengambilan uang ATM.

IV.1.5.3 Rancangan Struktur *File*

Berdasarkan rancangan direktori di atas maka dapat disusun struktur *file* yang ada di dalam *smartcard* berdasarkan standar iso7816-4:

- *File 1* -- berisi informasi data asuransi kesehatan pemilik *smartcard*.
- *File* 2 -- berisi informasi mengenai panjang dari kunci-kunci yang disimpan di *file* lainnya. Hal ini dimaksudkan karena setiap pembacaan data dari *smartcard* memerlukan pendefinisian panjang data yang akan dibaca. *File* ini dijaga oleh kode PIN pemakai.
- *File* 3 -- berisi kunci publik
- *File* 4 -- berisi sebagian kunci privat.
- *File* 5 -- berisi sebagian kunci privat Kunci privat disimpan dalam dua *file* karena panjang maksimum masing-masing *file* dalam *smartcard* adalah 255 *byte* dan panjang kunci privat lebih dari 255 *byte.*

  File 3, 4 dan 5 dijaga oleh kode perusahaan yang mengeluarkan *smartcard* tersebut. Kode ini sama untuk semua *smartcard* yang dikeluarkan oleh perusahaan tersebut. Namun asumsi bahwa kode ini hanya diketahui oleh perusahaan tersebut dan sangat sulit diketahui oleh pihak lain.
- *File* 6 -- berisi *hash* dari data-data yang ada di *file* 3, 4 dan 5 dan nomor seri *smartcard*. Nomor seri adalah data yang ditulis oleh perusahaan penerbit *smartcard* sebelum *smartcard* tersebut ke luar ke pasaran. Hasil *hash* ini digunakan untuk membuktikan apakah *smartcard* yang digunakan asli atau

palsu. *File* ini tidak dijaga oleh *password*, karena walaupun nantinya isi dari *file* ini di-*copy* ke *file* lain, tetapi si pemalsu harus menghitung kembali *hash* karena nomor seri selalu unik untuk setiap *smartcard*.

- *File* 7 -- berisi sertifikat digital, terenkripsi dengan menggunakan kunci simetris perangkat lunak. Akses terhadap file ini dijaga dengan menggunakan PIN.
- *File* 9 … -- berisi direktori-direktori dan *file-file* berisi data rekam medis. Akses terhadap direktori-direktori dijaga oleh PIN.

Panjang masing-masing *file* dapat ditentukan oleh program, dimana panjang maksimum dari suatu file yang diperbolehkan oleh *smartcard* adalah sebesar 255 *byte*. Setiap data rekam medis terbaru harus disimpan ke dalam *smartcard*. Jika memori *smartcard* sudah tidak cukup, maka data rekam medis yang dibuat lebih dahulu akan dihapus dan digantikan dengan data rekam medis terbaru tersebut. Hal ini dilakukan karena pada umumnya data rekam medis terakhir lebih sering digunakan untuk rawat jalan.

IV.1.5.4 Rancangan Perangkat Lunak Sistem *Smartcard* Kesehatan yang Sesuai Standar *Interoperability*

Rancangan perangkat lunak yang diajukan pada sistem ini berdasarkan standar *interoperability* EU/G7 *Healthcards* – WG7. Berikut ini dijelaskan perintah-perintah untuk mengambil data dari *smartcard* dalam sistem *smartcard* kesehatan menurut standar *interoperability* EU/G7 *Healthcards* – WG7.

a. Mengisi *smartcard* baru

1. Periksa apakah ada *card reader* yang terhubung ke komputer.
2. Beri perintah *card reader* untuk menyalakan *power* dari *smartcard.*
3. Ambil data dari pemakai dan buat menjadi kode PIN.
4. Hasilkan kunci publik, kunci privat dan *hash* dari kunci privat, kunci publik dan *serial number*. Karena kita menggunakan *public key card* maka

membangkitkan bilangan acak untuk kunci dan pelaksanaan algoritma RSA dapat dilakukan di dalam *smartcard*. Sehingga kunci privat yang dihasilkan tidak pernah keluar dari *smartcard* karena begitu kunci tersebut dihasilkan di dalam *smartcard* langsung disimpan di dalam *smartcard*.

5. Enkripsi kunci publik, kunci privat dan nilai *hash* dengan menggunakan kunci simetris yang dimiliki oleh perangkat lunak. Komputasi ini dilakukan di dalam *smartcard*.
6. Buat *file* untuk menyimpan kunci privat dan publik yang dihasilkan.
7. Simpan kunci ke *file* di *smartcard*
8. Beri perintah kepada *reader* untuk mematikan *power* dari *smartcard*.

b. Perintah-perintah pada *Healthcard Client Application*

1. Buka hubungan logik dengan *Card* Terminal *Manager* API.
2. Buka hubungan logik dengan slot *smartcard.*
3. Masukkan, Aktifkan, dan *reset smartcard* . Memastikan *smartcard* ada pada slot atau tidak.
4. Memasukkan nilai *password* atau PIN.
5. *Load* dan inisialisasi dari *Healthcard Server.* Ketika sebuah *smartcard* akan diakses, *Healthcard Client Application* me-*load Healthcard Server* yang sesuai dengan *smartcard* dan menginisialisasinya.
6. Inisiatif untuk membaca data *smartcard* yang *interoperability.* Meminta *Healthcard Server* untuk mulai membaca data.
7. Ambil data yang *interoperability* dibaca dari *smartcard.* Setelah baca data selesai, data tersebut siap digunakan oleh *Healthcard Client Application* untuk diproses atau ditampilkan ke *user.*
8. Selesai menggunakan *Healthcard Server.* Setelah komunikasi selesai, *Healthcard Server* selesai digunakan.
9. Non-aktifkan *smartcard* dan ambil *smartcard.* Setelah penggunaan *smartcard* selesai, *Healthcard Client Application* harus meminta *Card* Terminal *Manager* untuk mematikan *smartcard* dan disiapkan untuk diambil.

10. Tutup hubungan logik dengan *Card* Terminal *Manager*.

c. Perintah-perintah pada *Healthcard Server*

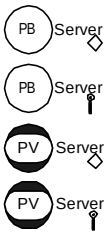
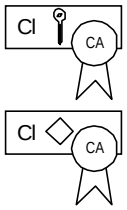
1. Respon untuk inisialisasi. Me-*load* modul *Healthcard Server* yang dipilih sesuai dengan *smartcard* yang dikenali oleh *Healthcard Client Application.*
2. Respon untuk baca data. Setelah *smartcard* dikenali dan pesan inisialisasi disetujui, maka data dari dalam *smartcard* dibaca dan diproses. Perintah-perintah ke *smartcard* disampaikan lewat *Card* Terminal *Manager*. *Healthcard Server* harus memetakan data yang dibaca dari *smartcard* ke struktur *interoperability* EU *Healthcard.*
3. Respon untuk ambil data. Data yang telah sesuai dengan standar *interoperability* siap untuk diambil oleh aplikasi.
4. Respon untuk terminasi. Menutup hubungan logik antara *Healthcard Client Application* dan *Healthcard Server*. Digunakan ketika interaksi dengan *smartcard* tertentu selesai.

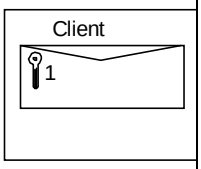
d. Perintah-perintah untuk *Card* Terminal *Manager*

1. Respon untuk membuat tabel *resource* yang diperlukan oleh aplikasi yang dipanggil.
2. Respon untuk mencari referensi ke *resource* yang dipilih.
3. Respon untuk memeriksa apakah *resource* yang dipilih digunakan oleh pihak lain.
4. Respon untuk melepas *resource* yang telah digunakan.
5. Respon untuk membuka hubungan logik dengan *smartcard*.
6. Respon untuk perintah-perintah mengakses *smartcard*.
7. Respon untuk menutup hubungan logik dengan *smartcard*.

IV.1.6 Rancangan Pengiriman Data Rekam Medis Lewat Jaringan

Setelah data rekam medis diubah dalam bentuk struktur data yang sesuai dengan standar *interoperability*, data tersebut siap digunakan oleh aplikasi. Seperti telah dijelaskan sebelumnya bahwa pihak-pihak berwenang dapat meminta data melalui medium publik atau jaringan komputer. Sedangkan medium publik atau jaringan komputer tidak aman dari pihak-pihak yang tidak berwenang oleh sebab itu perlu suatu mekanisme yang membuktikan bahwa pihak yang diajak berkomunikasi adalah pihak yang berwenang. Bagian ini menguraikan alur data otentikasi dua pihak yang akan berkomunikasi. Sebelumnya dijelaskan terlebih dahulu simbol-simbol yang digunakan dalam diagram :

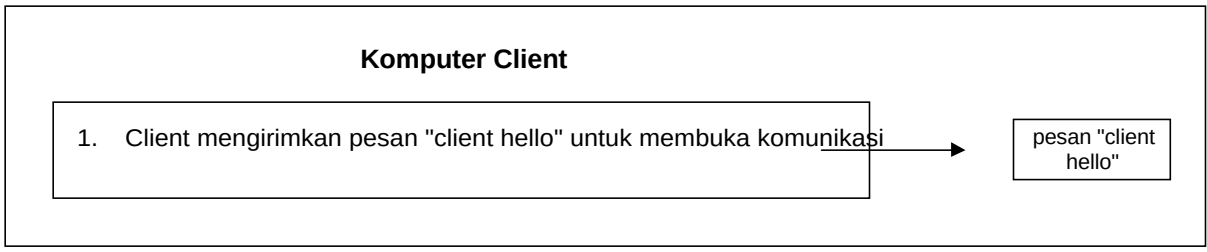
Simbol	Deskripsi
	Ini adalah kunci-kunci kriptografi. • Batang dari kunci menunjukkan pemilik kunci. • Kepala kunci mengindikasikan jenis kunci, apakah itu kunci privat (PV) atau kunci publik (PB). • Kunci dengan gambar intan menunjukkan bahwa kunci itu adalah kunci untuk membuat atau memeriksa tanda tangan digital. Sedangkan kunci dengan simbol kunci pada batangnya mengindikasikan bahwa kunci tersebut adalah kunci pertukaran yang dipergunakan untuk mengenkripsi atau mendekripsi kunci simetris.
	Ini adalah simbol dari tanda tangan digital. Inisial yang ada dalam simbol intan itu menunjukkan siapa yang membuat tanda tangan itu.
	Ini adalah contoh-contoh simbol dar sertifikat digital. • Tanda bukti lingkaran dengan pita menunjukkan siapa yang menandatangani atau mensahkan sertifikat tersebut. • Singkatan pada sertifikat itu mengindikasikan siapa pemilik dari kunci publik yang ada dalam sertifikat itu. • Simbol intan atau kunci dalam sertifikat itu menunjukkan jenis kunci publik apa yang ada dalam sertifikat tersebut. Jika kunci publik untuk memeriksa tanda tangan, maka dipergunakan simbol intan, sedangkan untuk kunci publik pertukaran kunci menggunakan simbol kunci.

	Di samping ini adalah simbol dari kunci simetris. Kunci ini selalu dienkripsi dengan kunci asimetris sebelum dikirim melalui jaringan komputer. Pemberian nomor pada kunci tersebut dimaksudkan untuk memudahkan membedakan satu kunci simetris dengan kunci simetris lainnya, karena dalam protokol ini kunci simetris dibuat dan dipergunakan beberapa kali.
	Ini adalah contoh dari sebuah amplop digital yang lengkap. Data penting ditandatangani secara digital oleh server. Sebuah kunci simetris (#1) dibuat secara acak, kemudian digunakan untuk mengenkripsi data-data aplikasi yang dikirim lewat jaringan komputer. Kunci simetris tersebut lalu dienkripsi dengan kunci publik penerima kunci tersebut.

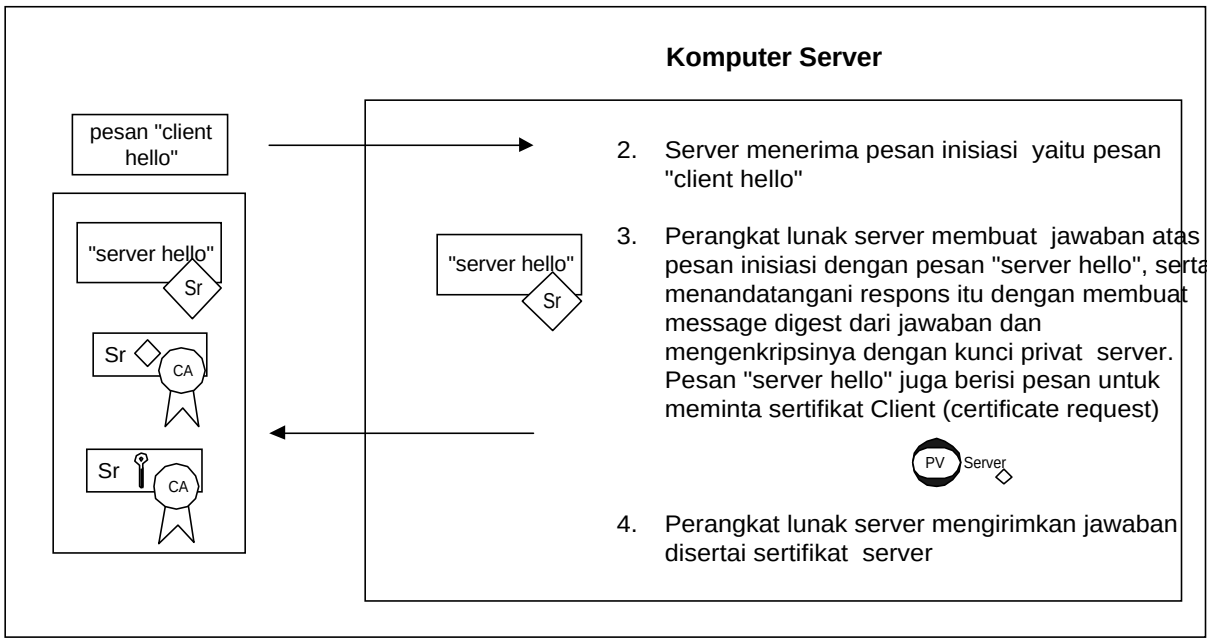
Tabel IV.1. Penjelasan simbol-simbol dalam protokol sistem s*martcard* kesehatan sesuai kebutuhan di Indonesia.

Di bawah ini menguraikan alur data untuk kondisi permintaan data dari pihak *client* ke pihak *server* secara rinci. Pihak yang meminta data disebut *client* sedangkan pihak yang mengirimkan data disebut *server.* Pengiriman data ini dilakukan sesuai dengan protokol *Secure Socket Layer* (SSL).

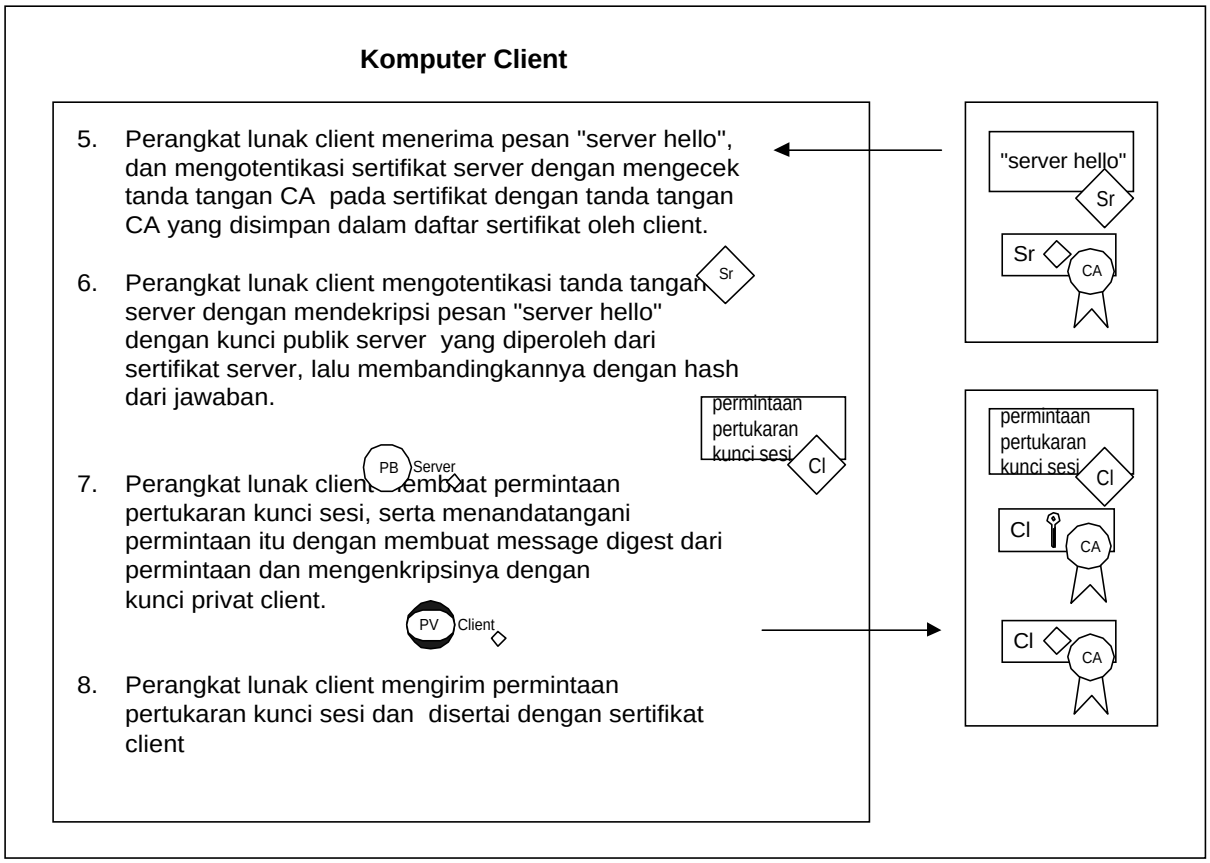
Client : Melakukan inisiasi



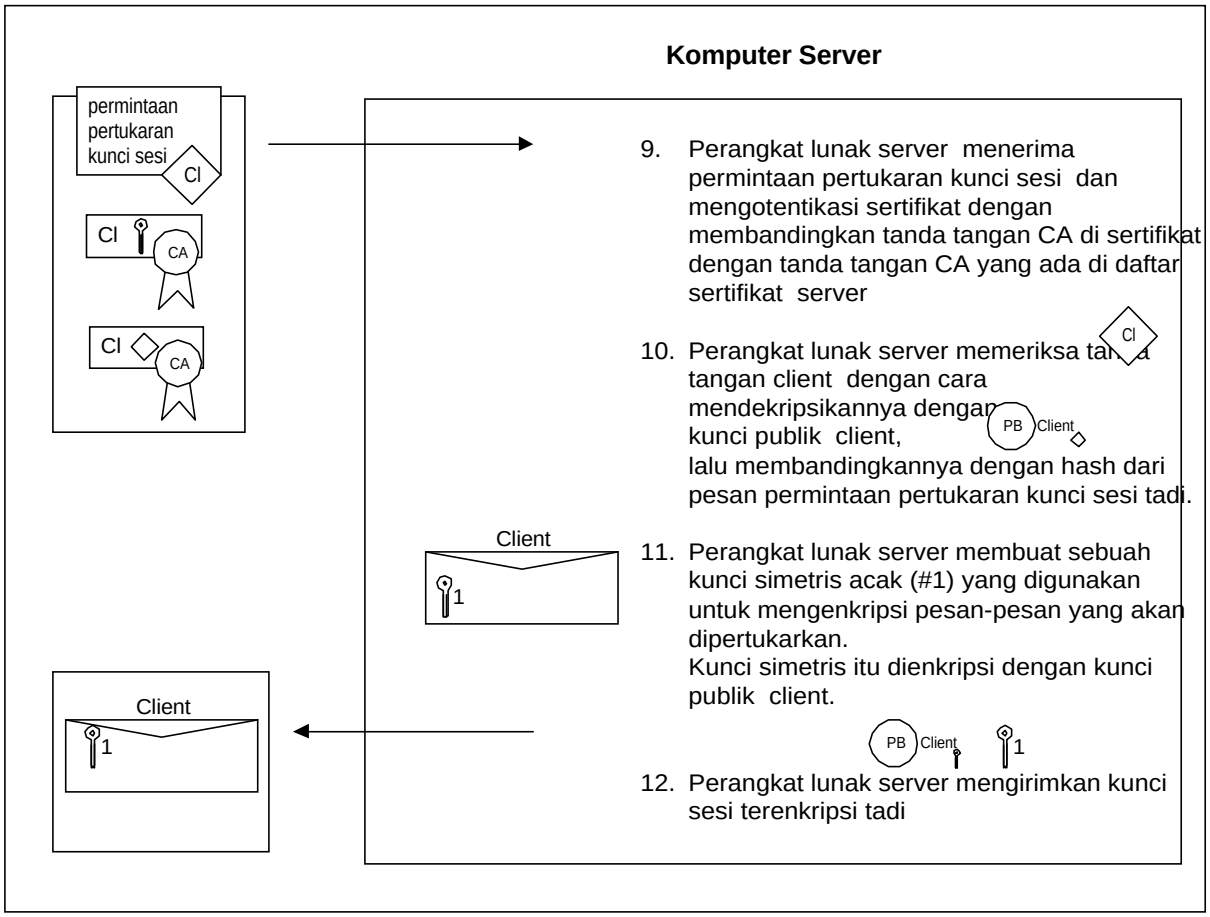
Server : Mengirim sertifikat & permintaan sertifikat Client



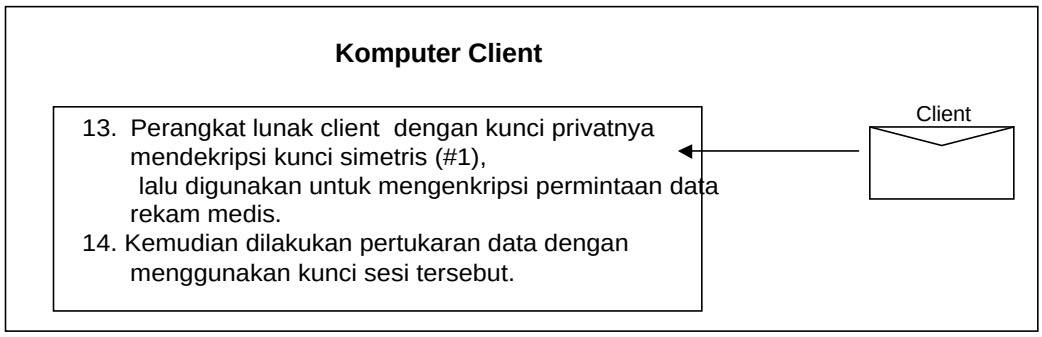
Client : Meminta pertukaran kunci sesi



Server : Mengirim kunci sesi



Client : Mengirim data rekam medis



Gambar IV.11. Diagram pengiriman data lewat jaringan

IV.1.7 Kriptanalisis

Bagian ini membahas analisis kriptografi dari proses pengiriman data dari pihak ke satu ke pihak ke dua. Skenario kriptanalisis adalah sebagai berikut. Misalkan seorang *client* (contoh: dokter), bernama Passy, membuka komunikasi atau melakukan transaksi dengan *server* misalkan *card centre*. Terdapat data (beberapa rahasia dan beberapa tidak rahasia) antara Passy dan *card centre,* yang digunakan untuk menjalankan protokol. Trudy, seorang *user* lain, berusaha untuk membongkar rahasia komunikasi antara Passy dan server. Usaha-usaha itu adalah:

1. ***Eavesdrop***. Yaitu Trudy berusaha mendengarkan untuk mendapatkan informasi dari pesan yang dipertukarkan antara Passy dan *card centre*.
2. **Berinisiasi membuka komunikasi sebagai Passy.** Yaitu Trudy berpura-pura sebagai Passy dan berusaha berkomunikasi dengan *card centre*.
3. **Menunggu di alamat *card centre* dan menerima koneksi dari Passy (*spoofing*)**. Yaitu Trudy berpura-pura sebagai Passy dan mencoba melayani hubungan dengan Passy.
4. **Membaca basis data Passy**. Yaitu Trudy membaca informasi milik Passy.
5. **Membaca basis data *card centre***. Yaitu Trudy membaca informasi milik *card centre*.
6. **Ada diantara jaringan Passy dan *card centre,* kemudian memeriksa dan/atau mengubah pesan dalam pengiriman diantara kedua pihak**. Yaitu Trudy berusaha mengubah pesan yang dipertukarkan antara Passy dan *card centre*.
7. Kombinasi dari usaha-usaha di atas.

Skenario di atas diterapkan pada protokol kriptografi sistem *smartcard* kesehatan untuk melihat kekuatan sistem keamanan. Semua pesan yang melalui jalur komunikasi diamankan dengan menggunakan teknik enkripsi. Semua pesan tersebut tidak ada gunanya bagi Trudy karena ia tidak dapat memperoleh apapun dari pesan

yang terenkripsi. Protokol ini amat mengandalkan keabsahan tanda tangan dari *Certificate Authority* (CA) utama. Jika masing-masing pihak tidak memiliki tanda tangan CA utama yang benar, maka sistem dapat gagal total. Oleh karena, Trudy dapat memberikan tanda tangannya pada setiap sertifikat digital yang seharusnya ditandatangani CA utama yang sebenarnya, ini berarti Trudy bisa memperoleh semua kunci publik yang ada dan dapat digunakan untuk mendekripsi pesan-pesan yang dia terima.

Trudy dapat berpura-pura menjadi Passy hanya jika ia dapat menunjukkan sertifikat digital milik Passy. Tetapi walaupun Trudy berhasil mendapatkan sertifikat Passy dan menggantikannya dengan sertifikat miliknya yang juga telah ditandatangani oleh CA yang sama, *card centre* segera mengetahui bahwa sertifikat digital yang dia peroleh tidak sah. Hal ini disebabkan karena kunci publik di dalam sertifikat yang dikirimkan ke *card centre* tidak dapat digunakan oleh *card centre* untuk mendekripsi pesan yang *card centre* anggap berasal dari Passy. *Card centre* segera mengetahui bahwa ada pihak yang tidak berwenang ikut serta dan langsung membatalkan transaksi pengiriman data selanjutnya. Jadi dalam hal ini, Trudy juga tidak dapat memperoleh informasi apapun juga. Sementara itu, perangkat lunak diasumsikan sebagai perangkat lunak *smartcard* kesehatan yang aman dan tidak dapat berkolusi dengan Trudy. Itu semua artinya menghilangkan kesempatan Trudy untuk berpura-pura sebagai Passy.

Misalkan Trudy berpura-pura sebagai *card centre*. Trudy menerima pesan verifikasi kunci sesi yang dienkripsi dengan kunci publik *card centre*. Trudy tidak akan dapat mendekrip pesan tersebut karena ia tidak mengetahui kunci privat *card centre*. Sementara itu, Passy juga mengharapkan pesan dari *card centre* yang berisi kunci sesi yang dienkripsi dengan kunci privat *card centre*, tetapi Passy tidak akan mendapatkannya karena Trudy tidak dapat memberikan kunci sesi yang dienkripsi dengan kunci privat *card centre*. Itu artinya usaha Trudy untuk berpura-pura sebagai *card centre* juga akan sia-sia.

Trudy tidak akan dapat membaca informasi milik Passy yang tersimpan di

smartcard karena *smartcard* bersifat *tamper-proof*. Jika Trudy berusaha mendapatkan informasi dari *smartcard*, maka *smartcard* akan mudah sekali rusak dan informasi di dalamnya juga akan berubah. Jika Trudy mengembangkan teknologi sendiri untuk membaca atau mendeteksi pulsa elektrik di dalam *smartcard*, seperti yang diuraikan pada bab sebelumnya maka investasi Trudy terlalu besar. Selain itu Trudy juga sukar untuk membaca basis data yang dimiliki oleh Passy atau *card centre* karena data-data yang disimpan di dalam basis data tersebut dienkripsi dengan menggunakan kunci simetris Passy atau *card centre.* Diasumsikan bahwa kunci simetris tersebut tidak diketahui oleh pihak-pihak yang tidak berwenang.

Sistem keamanan di *card centre* diasumsikan sangat baik sehingga sangat sulit bagi Trudy untuk mendapatkan informasi rahasia dari *card centre*. Kalaupun Trudy berhasil mendapatkan informasi rahasia di *card centre* dan berpura-pura sebagai *card centre*, Trudy tetap tidak akan dapat mengakses *smartcard* milik Passy karena *smartcard* tersebut dilindungi *password* atau PIN yang hanya diketahui Passy.

Trudy dapat mengganggu jalur komunikasi antara Passy dan *card centre*. Trudy juga dapat mengubah pesan yang dipertukarkan antara Passy dan *card centre*. Jika hal itu dilakukan baik Passy maupun *card centre* akan segera dapat mengetahui karena jika pesan tersebut diubah baik Passy mapun *card centre* tidak dapat mendekripsi pesan tersebut. Pada akhirnya Trudy tidak akan mendapat hasil apa-apa.

Semua usaha yang dilakukan Trudy di atas tidak mengarah kepada keberhasilan. Oleh karena itu kombinasi dari usaha-usaha itu juga tidak akan menuju keberhasilan.

Dengan penyimpanan kunci privat di dalam *smartcard*, maka kunci privat tersebut tidak diketahui dan diambil baik oleh pemilik *smartcard* itu sendiri atau pihak-pihak lain yang tidak berwenang. Hal ini menyebabkan pemilik *smartcard* tidak dapat mengambil kunci privatnya untuk diumumkan ke masyarakat secara diam-diam atau mengaku bahwa kunci privatnya hilang agar dia dapat menyangkal tanda tangan yang telah dibuatnya[Schn96]. Sebagai contoh : dokter yang membuat

data rekam medis dan telah menandatanganinya, di kemudian hari diketahui bahwa dia telah membuat kesalahan tindakan pengobatan, maka dokter tersebut sukar untuk menyangkal bahwa dia telah menandatangani data rekam medis tersebut karena kunci privatnya sukar dicuri orang atau dia tidak dapat secara diam-diam memberitahukannya ke masyarakat.

IV.2 ANALISIS SISTEM DENGAN PEMENUHAN KEBUTUHAN DI INDONESIA

Setelah merancang sistem *smartcard* kesehatan yang bertujuan untuk memenuhi kebutuhan di Indonesia maka rancangan sistem tersebut akan diperiksa apakah sudah memenuhi kebutuhan-kebutuhan di Indonesia.

- Kebutuhan 1 : Menyediakan proses otentikasi pihak-pihak yang mengakses *smartcard.* Hal ini dipenuhi karena setiap *smartcard* dilindungi oleh nilai *password* atau PIN tertentu yang hanya diketahui oleh pemilik *smartcard.*
- Kebutuhan 2 : Tanda tangan digital. Hal ini dipenuhi dengan penyimpanan pasangan kunci privat dan publik di dalam *smartcard*. Kunci privat ini digunakan untuk membuat tanda tangan digital.
- Kebutuhan 3 : Menjamin keutuhan data rekam medis setelah terjadi proses pengubahan. Hal ini dipenuhi dengan menggunakan fungsi *hash* dan tanda tangan digital sehingga data yang disimpan dapat dibandingkan dengan hasil *hash* pada tanda tangan digital.
- Kebutuhan 4 : Menyediakan pencatatan yang dapat dijadikan barang bukti pembacaan, penambahan atau koreksi terhadap data rekam medis. Hal ini dipenuhi dengan adanya fasilitas pencatatan di pihak rumah sakit dan disimpan dalam basis data rumah sakit tersebut.
- Kebutuhan 5 : Mendukung informasi untuk kebutuhan rawat jalan, bahan rujukan dan keadaan gawat darurat setiap saat. Hal belum sepenuhnya terpenuhi karena keterbatasan memori yang dimiliki oleh *smartcard* untuk menyimpan data. Oleh

sebab itu, jika data rekam medis yang dibutuhkan tidak ada dalam *smartcard*, harus dilakukan hubungan *on-line* ke *card centre*. Hal ini mengurangi fungsionalitas *smartcard* yang bertujuan untuk transaksi *off-line* dan kecepatan untuk memperoleh data rekam medis. Di satu sisi, dengan adanya basis data rekam medis yang terpusat di *card centre* maka pemilik *smartcard* dapat meminta data rekam medis miliknya kapan saja secara *on-line.* Dengan sistem *smartcard* kesehatan ini, pihak rumah sakit dan dokter yang ingin meminta data rekam medis dari suatu rumah sakit dapat memperolehnya secara *on-line* sehingga proses pengobatan menjadi lebih efisien. Dengan adanya data asuransi kesehatan di dalam *smartcard,* maka pasien gawat darurat dapat memperoleh tindakan pengobatan selanjutnya karena pihak asuransi menjamin biaya pengobatan yang akan diberikan.

- Kebutuhan 6 : Menjamin kerahasiaan data dari pihak yang tidak berwenang. Hal ini dijamin dengan adanya pasangan kunci privat dan kunci publik di dalam *smartcard,* kunci simetris di perangkat lunak aplikasi untuk mengenkripsi data, dan sertifikat digital di dalam *smartcard.* Kunci privat, kunci publik dan sertifikat digital digunakan sebagai alat otentikasi untuk kerahasiaan pengiriman data lewat jaringan komputer. Data-data yang disimpan dalam *smartcard* disimpan terenkripsi oleh kunci simetris perangkat lunak yang hanya diketahui oleh penerbit kartu. Selain itu untuk mencegah agar data rekam medis dari berbagai poliklinik tidak dapat langsung terbaca maka penyimpanan data rekam medis terbagi atas direktori-direktori, dimana setiap direktori dilindungi oleh suatu nilai *password* atau PIN tertentu. Untuk mencegah pembongkaran nilai kunci-kunci yang disimpan di dalam kartu dengan melakukan *physical external attack* atau *dumb mouse* maka terminal dan *smartcard reader* dilindungi dengan khusus sehingga pihak-pihak lain tidak dapat memasukkan program ke terminal atau *smartcard reader* untuk mengambil data atau alat-alat lain untuk mengubah tegangan.
- Kebutuhan 7 : *Smartcard* dapat diakses oleh semua perangkat lunak aplikasi

sistem *smartcard* kesehatan (*interoperability*). Hal ini tidak sepenuhnya dipenuhi karena belum ada standar yang baku diantara semua sistem *smartcard* kesehatan di dunia. Namun jika rancangan sistem *smartcard* kesehatan diterapkan pada sistem-sistem *smartcard* kesehatan yang telah mengikuti standar *interoperability* yang dikeluarkan oleh EU/G7 *Healthcards* – WG7, seperti yang telah dibahas sebelumnya, maka rancangan sistem *smartcard* kesehatan tersebut dapat berkomunikasi dengan sistem-sistem *smartcard* yang telah menerapkan standar *interoperability* tersebut.

Pada bab berikutnya akan dibahas kesimpulan dan saran untuk rancangan sistem *smartcard* kesehatan sesuai dengan kebutuhan di Indonesia.

BAB V
KESIMPULAN DAN SARAN

Bab ini menyimpulkan rancangan sistem *smartcard* kesehatan sesuai kebutuhan di Indonesia dan saran-saran pengembangan terhadap rancangan sistem tersebut.

V.1 KESIMPULAN

Dari penelitian yang telah dilakukan dapat ditarik beberapa kesimpulan :

1. Berdasarkan hasil studi perbandingan dari beberapa sistem *smartcard* kesehatan, ditemukan bahwa belum ada sistem *smartcard* kesehatan yang menggunakan sertifikat digital dan yang memenuhi sifat *interoperability.*
2. Rancangan sistem *smartcard* kesehatan sesuai kebutuhan di Indonesia dapat diimplementasikan dengan mengasumsikan hal-hal sebagai berikut :
   - Masyarakat yang menggunakan *smartcard* kesehatan adalah masyarakat golongan menengah ke atas.
   - Rumah sakit yang mengimplementasikan sistem *smartcard* kesehatan adalah rumah sakit yang memiliki kondisi :
     - Sudah terhubung ke jaringan komputer.
     - Memiliki PC dan *card reader* yang terhubung dengan PC tersebut untuk membaca dan menulis data ke/dari *smartcard*.
     - Sumber daya manusia yang dapat menggunakan aplikasi komputer.
     - Memiliki modal keuangan yang cukup untuk mengimplementasikan sistem *smartcard* kesehatan.
3. Sistem *smartcard* kesehatan yang dirancang dalam tugas akhir ini dapat mengatasi masalah :
   a. Otentikasi pihak-pihak yang mengakses *smartcard* dengan menggunakan

password atau PIN yang hanya diketahui oleh pemilik *smartcard.*

b. Keabsahan pihak-pihak yang melakukan pengubahan data dengan memanfaatkan tanda tangan digital.
c. Keutuhan data rekam medis setelah terjadi proses pengubahan dengan menggunakan sidik jari dari data tersebut.
d. Pencatatan yang dapat dijadikan barang bukti pembacaan, penambahan, dan koreksi terhadap data rekam medis.
e. Informasi untuk kebutuhan rawat jalan, bahan rujukan dan keadaan gawat darurat setiap saat. Pada keadaan gawat darurat, pemilik *smartcard* dapat langsung diberikan tindakan pengobatan secara lengkap karena pihak asuransi menjamin biaya pengobatan yang diberikan. Selain itu, pasien tidak perlu lagi datang ke rumah sakit tertentu untuk meminta data rekam medis miliknya. Dokter dan rumah sakit dapat memperoleh data rekam medis dari suatu rumah sakit secara *on-line* sehingga proses pengobatan menjadi lebih efisien.
f. Kerahasiaan data dari pihak yang tidak berwenang, baik data yang disimpan di dalam *smartcard* maupun data yang dikirimkan lewat jaringan komputer.
g. *Interoperability* sistem *smartcard* kesehatan yang sesuai dengan standar *interoperability* oleh EU/G7 *Healthcards* – WG7.

4. Rancangan sistem *smartcard* kesehatan dapat bertahan terhadap :
   - Penggunaan kunci privat dan sertifikat digital oleh pencuri karena kedua data tersebut disimpan di dalam *smartcard*.
   - Serangan-serangan terhadap kerahasiaan data rekam medis yang dikirim melalui jaringan komputer.
5. Rancangan sistem *smartcard* kesehatan dapat ditambahkan pada sistem informasi yang telah ada di rumah sakit. Jadi sistem yang lama tidak langsung terbuang atau tidak dapat digunakan kembali.

V.2 SARAN

Beberapa saran yang dapat diberikan berdasarkan penelitian dalam tugas akhir ini adalah sebagai berikut :

1. Penggunaan standar *interoperability* sistem *smartcard* kesehatan yang baku jika sudah ditentukan standar baku *interoperability* sistem *smartcard* kesehatan di masa yang akan datang.

2. Sistem *smartcard* kesehatan sesuai kebutuhan di Indonesia dapat diterapkan dengan membedakan beberapa jenis pelayanan. Sebagai contoh, terdapat tiga jenis pelayanan yaitu *smartcard* kesehatan *gold, silver,* dan *regular.* Dimana masing-masing jenis *smartcard* memberikan pelayanan yang berbeda. Sebagai contoh *smartcard gold* memberikan keamanan data di dalam *smartcard* yang tinggi dan kemampuan untuk mengakses data lewat jaringan komputer, *smartcard silver* hanya memberikan keamanan data di dalam *smartcard* tetapi tidak dapat meminta data lewat jaringan, sedangkan *smartcard regular* hanya menyimpan data rekam medis gawat darurat dan data asuransi kesehatan tanpa ada pengamanan data di dalam *smartcard.* Pasien dapat menggunakan jenis *smartcard* sesuai kebutuhannya.
3. *Smartcard* kesehatan yang juga menyimpan data rekam medis rawat inap.
4. Seluruh pihak yang mengeluarkan *smartcard* hendaknya bekerja sama dengan pihak asuransi kesehatan sehingga setiap pemilik *smartcard* juga memiliki asuransi kesehatan.
5. Penelitian mengenai rancangan sistem *smartcard* kesehatan sesuai kebutuhan di Indonesia masih dapat dikembangkan dalam hal :
   - Protokol penyerahan sertifikat digital ke pemilik *smartcard*.
   - Implementasi prototip rancangan sistem *smartcard* kesehatan sesuai kebutuhan di Indonesia.

DAFTAR PUSTAKA

[AK96] Ross Anderson, Markus Kuhn. *Tamper Resistance – A Cautionary Note;* Computer Laboratory Cambridge University, and Department of Computer Sciences, Purdue University, 1996.

[BDHJN96] Feng Bao, Robert Deng, Yongfei Han, Albert Jeng, Desai Narasimhalu, Teow Hin Nagir: *New Attacks to Public Key Cryptosystems on Tamperproof Devices;* Information Security Group, Institute of Systems Science, National University of Singapore, 1996.

[Chan99] Chan, Siu-Cheung Charles. *An Overview of Smartcard Security*; 1999.

[DHMM96] Thomas Dawkins, Justin Higgins, Sean Mathias, Joel Millecan, Michael Rice, Paul Tso: *Unlocking Microsoft Internet Information Card centre;* New Riders Publishing, Indianapolis 1996.

[EUHCI96] *Interoperability of Healthcard Systems Part* 3 : Homepage, 1996, http://www.compulink.co.uk/~cic/euhci.htm.

[IETF96] *Internet Engineering Task Force* : *Secure Socket Layer 3.0 Specification*; USA, 1996.

[ISO7816-95] ISO/IEC 7816, *Interindustry Commands for Interchange*, ISO/IEC, 1995.

[Microchart99] Microchart : Homepage, 1999. http://www.cyberspc.mb.ca/~.

[Motus99] Motus: Homepage, 1999. http://www.motus.com.

[MRI99] Medical Records Institute: Homepage, 1999 http://www.medrecinst.com/resources/levels.html.

[Oberthur99] Oberthur: Homepage, 1999. http://www.oberthurkirk.com.

[Orga99] Orga: Homepage, 1999. http://www.orga.com.

[PerMen89] Peraturan Menteri Kesehatan Republik Indonesia Nomor :

749a/MENKES/PER/XII/1989 tentang Rekam Medis/ *Medical Records*.

[PerPem66] Peraturan Pemerintah Nomor 10 tahun 1966 tentang Wajib Simpan Rahasia Kedokteran Presiden Republik Indonesia.

[Precis99] Precis: Homepage, 1999. http://www.precis-scs.com.

[Schn96] Bruce Schneier: *Applied Cryptography, 2nd ed.;* John Wiley & Sons, Inc., New York 1996.

[SSL99] Secure Socket Layer: Homepage, 1999, http://www.verisign.com/repo-sitory/*client*auth/*client*auth.html.

[Tane89] Andrew S. Tanenbaum: *Computer Networks, 2nd ed.;* Prentice-Hall Inc., Englewood Cliffs 1989.