Riset Unggulan Terpadu
Tahun 1998/1999

LAPORAN AKHIR

Judul Penelitian:	**Pengembangan Teknologi dan Aplikasi Teknologi Sekuriti Digital**
Peneliti Utama:	**Dr.Ir. I. Sri Wishnu Brata Prasetya / Ir. FX Nursalim Hadi, PhD**
Lembaga Penanggung Jawab:	**Fakultas Ilmu Komputer Universitas Indonesia**

KANTOR MENTERI NEGARA RISET DAN TEKNOLOGI
DEWAN RISET NASIONAL

Abstrak

Dalam era Internet dan *electronic commerce* saat ini, teknologi sekuriti dengan perangkat kriptografi sangat dibutuhkan, karena Internet merupakan *public network* yang tidak aman. Penelitian yang dilaksanakan antara bulan Juni 1998 sampai dengan Juni 1999 ini bertujuan untuk melakukan transfer teknologi sekuriti digital terutama yang menggunakan perangkat kriptografi, dan juga teknologi *smartcard* (kartu chip). Bahkan sebenarnya, fokus dari penelitian ini adalah pemanfaatan teknologi kriptografi untuk sekuriti digital.

Penelitian ini terbagi menjadi beberapa sub-penelitian. Sub penelitian pertama adalah implementasi protokol *Secure Electronic Transaction* (SET) dari Visa dan MasterCard. Hasilnya adalah berupa *object library* SET dalam Java dan juga aplikasi wallet berbasis Java yang bisa membaca informasi kartu kredit dari *smartcard*. Aplikasi wallet berbasis Java tersebut kami beri nama *SmartWallet.*

Sub penelitan lainnya adalah rancangan kartu kesehatan berbasis *smartcard* (kartu chip). Meskipun sudah ada beberapa produk *health card* luar negeri, rancangan kartu kesehatan dalam penelitian ini disesuaikan dengan peraturan di Republik Indonesia mengenai rekam medis.

Selain itu penelitian ini merancang pula dua protokol pembayaran. Yang pertama adalah protokol pembayaran berbasis *smartcard* dimana konsumen (*cardholder*) dapat membelanjakan ‘uang elektronik’-nya pada *point of sale* (POS) yang tidak memiliki hubungan sama sekali dengan bank saat pembayaran dilakukan. Sistem pembayaran ini juga dapat dimanfaatkan untuk pembayaran di Internet, mencegah / mendeteksi penggandaan uang elektronik, dan uang elektronik bisa kembali meskipun dicuri orang lain. Yang kedua, adalah sistem pembayaran berbasis kartu kredit yang anonimus (tak terlacak), dan mencegah bank-bank berkolusi untuk mengetahui identitas transaksi yang seharusnya tak terlacak itu.

Sub penelitan terakhir adalah kajian mengenai kerangka hukum untuk *digital signature*, sebagai komponen sekuriti yang utama dalam *electronic commerce.* Penelitian ini dilakukan oleh anggota tim yang berasal dari Fakultas Hukum Universitas Indonesia. Hasilnya adalah rekomendasi mengenai konstruksi hukum *digital signature* untuk Indonesia.

Daftar Isi

BAB I

Pendahuluan

A. Latar Belakang Masalah

Sekuriti Digital adalah teknologi yang digunakan untuk melindungi informasi dari pencurian dan pemalsuan lewat tehnik penyandian yang praktis tidak bisa ditembus. Pada saat ini, pertemuan teknologi Internet, Sekuriti Digital, Electronic Commerce dan Smart card bergerak amat cepat dalam mendefinisikan teknologi informasi masal yang baru. Kombinasi keempatnya memungkinkan dikembangkannya komunikasi elektronis pada skala masal dan global, dengan faktor keamanan data (dari pencurian dan pemalsuan) yang tinggi. Ini menjadikan teknologi yang seperti ini strategis nilainya untuk Indonesia di era Internet.

Indonesia memiliki banyak kepentingan untuk mengembangkan sarana komputasi / komunikasi modern demi menunjang pembangunan. Penggunaan Teknologi Informasi tanpa sekuriti sangat berbahaya. Sebaliknya, ekploitasi teknologi sekuriti akan memberi jalan ke berbagai kemungkinan bernilai strategis yang sebelumnya dianggap tidak mungkin. Dalam konteks ini, penting bagi Indonesia untuk mengantisipasi makin pentingnya isu sekuriti dalam tatanan dunia informasi modern.

Menyadari hal itu, Fakultas Ilmu Komputer UI semenjak tahun 1995 telah memberikan perhatian khusus, yaitu berupa seminar, kuliah topik khusus, student project, serta proyek penelitian yang berhubungan dengan sekuriti digital dan electronic commerce.

B. Tujuan Penelitian

Sebagai langkah selanjutnya, usaha diatas perlu diperkuat, yaitu dengan dibentuknya ***Digital Security & Electronic Commerce (DSEC) Special Interest Research Group.*** Secara umum penelitian ditujukan untuk melakukan transfer ilmu dan pengembangan teknologi berbasis sekuriti digital (terutama dengan perangkat kriptografi) dan smart card.

Aplikasi yang paling jelas adalah sistem pembayaran yang standar dan expandable. Hasil yang dicapai diharapkan juga bersifat generik, yaitu karena generalisasi dari protokol pembayaran pada dasarnya mencakup cukup banyak jenis protokol sekuriti yang lain. Artinya, dari *library* yang dihasilkan, dapat dibuat jenis-jenis protokol sekuriti lainnya. Sebagai contoh, sistem sekuriti smartcad bisa dimanfaatkan untuk kartu kesehatan. Penelitan tidak hanya diarahkan pada aspek implementasi protokol sekuriti, namun juga pada aspek teoritis dan perancangan protokol sekuriti.

Memperhatikan bahwa trend dari teknologi electronic commerce yang semakin memanfaatkan teknologi tanda tangan & sertifikat digital, kami juga menyadari bahwa pentinglah artinya eksistensi suatu kerangka hukum bagi tanda tangan digital. Oleh karena itu, salah satu bagian esensial dari kelompok riset kami adalah riset bersama dengan Fakultas Hukum Universitas Indonesia dalam meneliti framework bagi peraturan tanda tangan digital di Indonesia.

C. Ruang lingkup penelitian

Penelitian ini terdiri dari beberapa sub-penelitian:

1. Pengembangan *wallet* dan *library* protokol Secure Electronic Transactioan (SET), beserta pemanfaatan teknologi smartcard dalam SET.

2. Rancangan kartu kesehatan (healtcard) berbasis smartcard yang sesuai dengan peraturan kesehatan di Republik Indonesia.

3. Rancangan sistem pembayaran off-line berbasis smartcard

4. Rancangan protokol kartu kredit anonimus (tak terlacak).

5. Kerangka hukum *digital signature* dalam electronic commerce di Indonesia

BAB II

Pelaksanaan & Hasil-hasil Penelitian

Bab ini memberikan gambaran-gambaran ringkas mengenai output yang dihasilkan oleh sub-sub penelitian yang telah disebutkan di atas.

A. Implementasi Secure Electronic Transaction (SET) Berbasis Java & SmartCard

Internet yang berkembang dengan pesat kini telah dimanfaatkan orang untuk melakukan transaksi perdagangan. Seiring dengan meningkatnya perdagangan elektronik khususnya di internet, meningkat pula jumlah pengguna kartu pembayaran sebagai alat pembayaran yang paling praktis di internet. Peningkatan tersebut diikuti pula dengan peningkatan jumlah penipuan dan kejahatan di internet.

Oleh karena itu, transaksi yang dilakukan harus dapat menjamin keamanan data-data yang dipertukarkan antar pihak-pihak yang berkepentingan. Masalah-masalah umum yang ada pada Sistem Pembayaran di Internet (SPI) antara lain kerahasiaan pesan (*confidentiality*), keutuhan pesan (*integrity*), keabsahan pesan (*authenticity*), dan keaslian pesan (*non repudiation*).

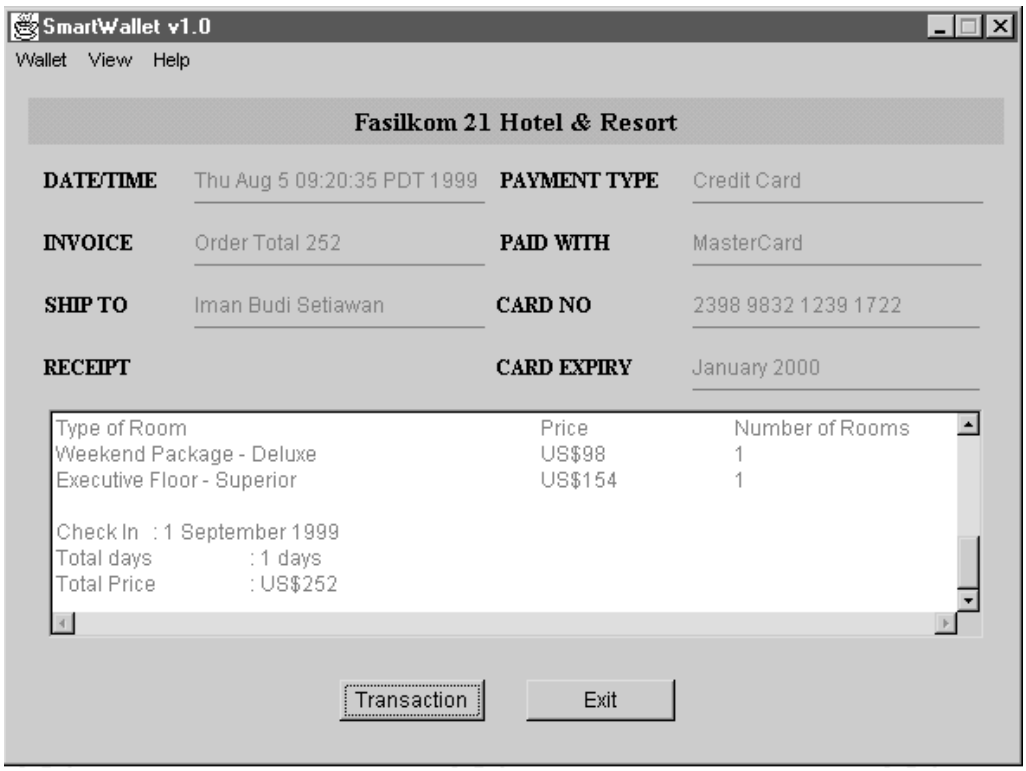
Enkripsi data merupakan solusi yang tepat untuk melindungi data dari usaha-usaha pencurian dan pemalsuan data. Fasilitas enkripsi di Internet yang banyak digunakan orang saat ini adalah *Secure Socket Layer* (SSL) yang didukung oleh dua *browser* terkemuka yaitu Microsoft Internet Explorer dan Netscape Navigator. Namun pada kenyataannya, SSL mempunyai beberapa kelemahan, sehingga tidak terlalu cocok untuk transaksi pembayaran. Oleh karena itu, Visa dan Mastercard mengeluarkan protokol standar yang aman untuk transaksi pembayaran yang disebut *Secure Electronic Transaction* (SET).

Secure Electronic Transaction (SET) adalah sebuah protokol yang khusus dibangun untuk menangani keamanan transaksi kartu pembayaran di Internet. SET menjamin autentisitas, kerahasiaan dan integritas data transaksi yang dikirimkan melalui internet. Saat penelitian dilakukan, di Indonesia belum ada yang mengembangkan dan mengimplementasikan protokol SET. Oleh karena itu dalam penelitian ini dicoba untuk menganalisa dan mengembangkan sendiri protokol SET.

Protokol SET mengatur bagaimana *cardholder* (pemakai kartu pembayaran) dan *merchant* (pedagang) bertransaksi, mengatur bagaimana *merchant* dan *payment gateway* (gerbang pembayaran) melakukan otorisasi kartu pembayaran dan permintaan pembayaran, mengatur bagaimana setiap pihak yang terlibat memiliki suatu sertifikat digital sebagai jaminan atas dirinya.

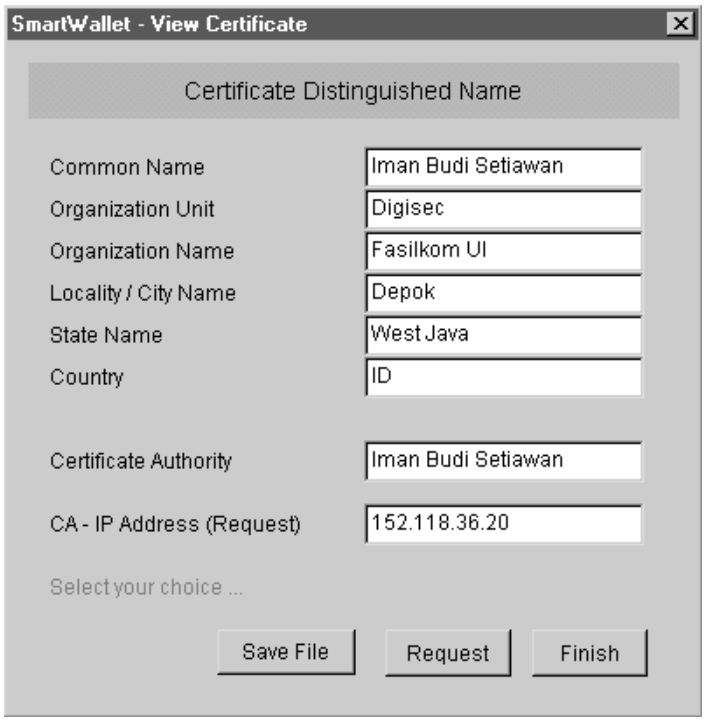
Komponen penelitian protokol SET ini adalah sebagai berikut:

1. Implementasi aplikasi ***wallet*** berbasis Java applet dan smartcard yang kami beri nama "*SmartWallet*". SmartWallet adalah suatu aplikasi yang digunakan oleh *cardholder* untuk melakukan transaksi perdagangan di Internet. SmartWallet digunakan sebagai aplikasi utama untuk melakukan penyimpanan data, autentikasi, permintaan sertifikat ke *certificate authority* (CA), dan transaksi dengan pedagang (*merchant*). Smartcard digunakan cardholder sebagai tempat penyimpanan dan autentikasi data saat melakukan transaksi dengan pedagang. Semua proses di atas menggunakan protokol SET untuk menjamin keamanan data-data selama transaksi.



Gambar 1. Interface pembayaran *SmartWallet*

2. Implementasi sub-protokol ***Purchase Request***, yakni proses pembayaran antara *customer* dengan *merchant.*
3. Implementasi sub-protokol ***Payment Authorization***, yakni proses otorisasi antara *merchant* dengan
4. Implementasi sub-protokol ***Cardholder Registration***, yakni proses permohonan sertifikat digital oleh *cardholder* kepada *certificate authority.*



Gambar 2. Melihat sertifikat digital dengan *SmartWallet*

Penelitian dilakukan dengan mempelajari dan menganalisa spesifikasi SET beserta standar-standar kriptografi pendukungnya, dilanjutkan dengan perancangan dan implementasi objek-objek yang dipakai dalam protokol SET dengan menggunakan Java.

Penelitian dimulai dengan membaca ketiga buku referensi yang dikeluarkan Visa dan Mastercard. Kemudian mempelajari ASN.1, perangkat kriptografi yang dibutuhkan dalam SET, encoding data dalam format DER, dan merancang objek-objek yang akan diimplemetasikan. Lalu dimulailah pembuatan objek-objek tersebut, kemudian melakukan pengujian secara sistematis terhadap kumpulan objek-objek Java yang dihasilkan itu.

Hasil penelitian ini adalah *object library* yang dipakai dalam sub protokol *Purchase Request*, *Payment Authorization*, dan *Cardholder Registration* dalam Java. Selain *object library*, penelitian ini juga membuat *working prototype* "*SmartWallet*".

Peneliti:

Arrianto Mukti Wibowo, I. Arif Priharsanta, Dwinanda Prayudi, Haris Fauzi, Iman Budi Setiawan, Bob Hardian, F.X. Nursalim Hadi.

B. Rancangan Kartu Kesehatan Berbasis Smartcard Sesuai Peraturan Kesehatan Indonesia

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. 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. 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 yang menjaga data tersebut agar tidak dibaca oleh pihak yang tidak berwenang. *Smartcard* juga dapat dibawa dengan mudah sehingga menunjang ketersediaan data kapan saja ketika dibutuhkan.

Penelitian 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.

Dalam penelitan ini, peraturan pemerintah tentang rekam medis dianalisa secara mendalam. Penelitan juga melakukan observasi lapangan di rumah sakit. Selain itu dilakukan pula komparasi beberapa sistem rekam medis dengan menggunakan *smartcard* yang ada di negara-negara lain sehingga diketahuilah sistem *smartcard* kesehatan mana 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 penelitian 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*).

Peneliti:

Christine Sariasih, Iik Wilarso, Arrianto Mukti Wibowo, Bob Hardian, F.X. Nursalim Hadi.

C. Rancangan Protokol Sistem Pembayaran Elektronik Off-Line Berbasis SmartCard (PayCard Off-Line)

Dalam transaksi kartu secara elektronik sehari-hari, seperti dengan kartu debit dan kartu kredit, *merchant* harus terhubung secara on-line (atau *dial-up*) ke bank, agar bisa mengotentikasi *cardholder* dan selanjutnya melakukan otorisasi pembayaran.

Namun, dalam realitanya, banyak sekali kasus dimana pembayaran harus dilakukan manakala *merchant* (atau penerima pembayaran) sangat sulit terhubung on-line ke bank. Contohnya pembayaran di taksi, bis, kereta api, pesawat terbang, kedai-kedai, toko-toko kecil, salesman keliling, dan kedai berjalan (mobile shop).

Penelitian ini bertujuan untuk membuat suatu protokol pembayaran, dimana pembayaran itu bisa dilakukan secara *off-line*, jadi tidak terhubung ke bank saat proses pembayaran dilakukan. Namun, pada saat yang sama tetap menjamin keamanan transaksi dari manipulasi *cardholder* maupun *merchant.*

Cardholder dapat mengambil ‘uang elektronik’ mereka untuk dimasukkan ke dalam smartcard melalui ATM bank atau melalui Internet. Kemudian mereka dapat

memanfaatkan uang dalam *smartcard* mereka untuk berbelanja di *Point Of Sale* (POS)-nya memang tidak memungkinkan terhubung secara langsung pada bank. Selain itu mereka juga bisa melakukan transaksi di Internat dengan aman, bahkan jauh lebih aman dibandingkan dengan transaksi menggunakan SSL. Kemudian, pada selang waktu tertentu (misalnya sehari sekali, pada malam hari), *merchant* menagih 'nota penjualan' dari *cardholder* kepada bank.

Untuk menjamin keamanan transaksi, sistem pembayaran ini menggunakan smartcard serta perangkat kriptografi simetrik dan asimetrik.

Kelebihan-kelebihan lain yang ditawarkan sistem pembayaran yang kami sebut *PayCard Off-Line* ini antara lain mencegah seseorang untuk menduplikasi cek digital-nya, sehingga mencegah *double spending.* Dan juga, kalau smartcard milik *cardholder* itu hilang, maka orang lain tidak dapat menggunakannya, serta *cardholder* dapat mendapatkan lagi 'uang' hilang itu. Jadi, bank dapat menjamin bahwa kalau smartcardnya hilang, uang dalam smartcard itu tidak akan hilang, dan uang yang hilang itu tak dapat dipakai orang lain (***loss tolerant***).

Peneliti:

Arrianto Mukti Wibowo, Raditya Umbas.

D. Rancangan Protokol Kartu Kredit Anonim (Tak terlacak)

Kartu kredit telah lama menjadi sistem pembayaran, bahkan telah diadopsi menjadi sistem pembayaran untuk sistem perdagangan yang memanfaatkan jaringan komputer global. Pada sistem perdagangan seperti itu, sistem pembayaran digital dapat menjadi alternatif selain sistem pembayaran kartu kredit. Pada sistem pembayaran digital, transaksi tidak sekedar melakukan pencatatan atau akunting saja, melainkan diikuti dengan perpindahan data digital sebagai representasi alat pembayaran atau bukti pembayaran, dari satu pihak, misalnya pihak pembeli, ke pihak lain, misalnya pihak penjual. Contoh sistem pembayaran digital adalah uang digital dan kartu kredit digital anonim. Uang digital adalah alat pembayaran secara tunai dalam bentuk digital. Kartu kredit digital anonim adalah alat pembayaran secara tidak tunai atau kredit dalam bentuk digital dimana detil pembayarannya anonim, artinya tidak ada pihak lain kecuali pembayar yang dapat menelusuri hubungan antara identitas pembayar dengan informasi pembayaran. Uang digital yang terkenal adalah uang digital David Chaum dan uang digital Stefan Brands. Kartu kredit digital anonim diusulkan oleh Steven H Low, Nicholas F Maxemchuk, dan Sanjoy Paul. Kartu kredit mereka, dinamakan KK-Low.

KK-Low rentan terhadap kejahatan kolusi. Identitas pembayar dapat ditelusuri dari informasi pembayaran jika ada pihak-pihak tertentu yang berkolusi. Dengan kata lain, kolusi antara pihak-pihak tertentu dapat mengasosiasikan identitas pembayar dengan informasi pembayaran. Hal itu dapat merugikan pembayar karena rahasia pembayarannya diketahui pihak lain. Oleh karena itu, penelitian ini bertujuan membuat kartu kredit digital anonim yang bebas kolusi.

Tujuan tersebut dicapai dengan membuat kartu kredit digital anonim baru, bukan modifikasi terhadap KK-Low. Penyebab kelemahan KK-Low dan teknik menghindari kelemahan itu dipelajari. Juga, uang digital David Chaum dan uang digital Stefan

Brands dipelajari sebagai contoh sistem pembayaran digital. Kemudian, dibuat kartu kredit digital anonim dengan konsep baru.

Penelitian ini menghasilkan kartu kredit digital anonim yang diberi nama SMARTCredit. SMARTCredit berbeda dengan KK-Low karena SMARTCredit berbasis *credential token* sedangkan KK-Low berbasis *fund transfer*. SMARTCredit bersifat bebas kolusi, artinya tidak ada kejahatan kolusi yang dapat merugikan pihak tertentu. Selain itu, SMARTCredit dapat bekerja secara *offline*.

Peneliti:

Deddy D., F.X. Nursalim Hadi.

E. Kerangka Hukum Tanda Tangan Digital Dalam Electronic Commerce Untuk Indonesia

Internet adalah jaringan publik yang global dan murah. Padahal, Internet merupakan jaringan publik yang tidak memiliki fasilitas keamanan yang memadai. Hal ini menimbulkan konsekuensi bahwa semua transaksi yang dilakukan melalui Internet merupakan bentuk transaksi beresiko tinggi.

Kelemahan yang dimiliki oleh Internet sebagai jaringan publik yang tidak aman ini telah dapat diminimalisasi dengan adanya penerapan teknologi penyandian informasi (kriptografi). *Electronic data transmission* dalam e-commerce diamankan dengan melakukan proses enkripsi sehingga menjadi cipher/locked data yang hanya bisa dibaca/dibuka dengan melakukan proses *reversal* yaitu proses dekripsi. Contoh protokol yang memanfaatkan kriptografi adalah protokol SSL, SET, PGP, dsb. Protokol-protokol tersebut digunakan dalam transaksi di Internet.

Perlu digarisbawahi, dengan adanya perkembangan teknologi di masa mendatang, terbuka kemungkinan adanya penggunaan *e-commerce* dalam media selain Internet, seperti misalnya pada jaringan GSM. Bahkan, hasil penyandian, yakni ciphertext / locked data dapat dituliskan / dicetak pada kertas, dan memiliki validitas yang sama dengan data elektronik.

Dalam transaksi *e-commerce*, perangkat kriptografi yang paling sering dipergunakan adalah *digital signature* (tanda tangan digital). Jika pengirim pesan (*message*) membubuhkan tanda tangan digital pada pesan, penerima dapat merasa yakin bahwa setelah ditandatangani pengirim, pesan itu tidak ada yang memanipulasi saat dalam perjalanan.

Sifat yang dimiliki oleh tanda tangan digital adalah:

1. otentik, tak bisa/sulit ditulis/ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatangan tak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya.
2. hanya sah untuk dokumen (pesan) itu saja atau kopinya yang sama persis. Tanda tangan itu tidak bisa dipindahkan ke dokumen lainnya, meskipun dokumen lain itu hanya berbeda sedikit. Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak lagi sah.
3. dapat diperiksa dengan mudah, termasuk oleh pihak-pihak yang belum pernah bertatap muka langsung dengan penandatangan.

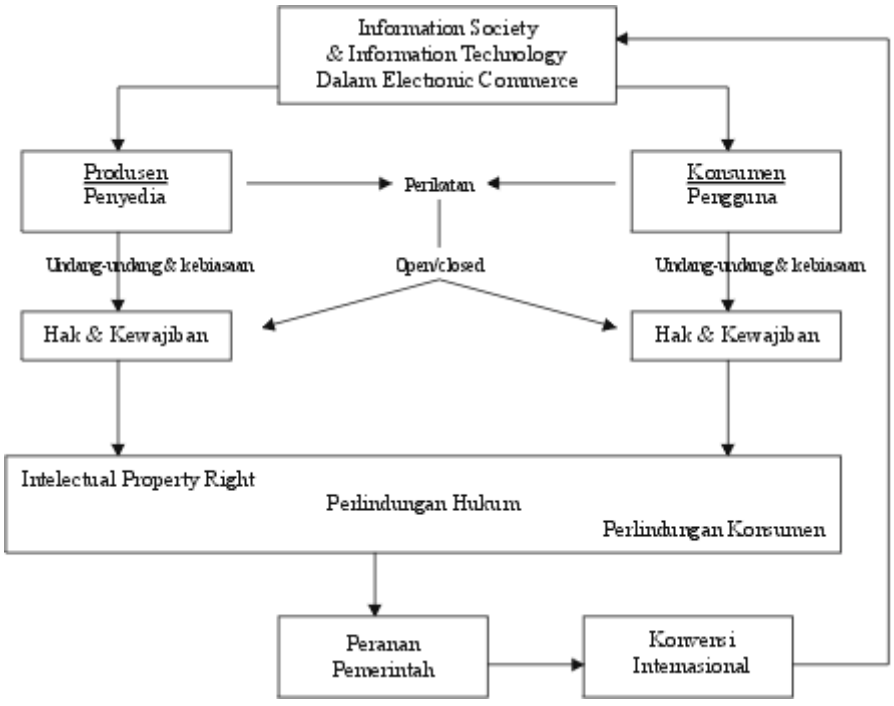
Pada umumnya, tanda tangan digital menggunakan teknik kriptografi kunci publik, kunci simetrik dan sebuah fungsi hash satu arah. Patut dicatat bahwa tanda tangan digital bukanlah tanda tangan dari seseorang yang di-*scan* atau dimasukkan ke komputer menggunakan *stylus* atau *mouse*, tapi merupakan kumpulan dari kalkulasi-kalkulasi matematis untuk menyandikan data, yakni dengan kriptografi. Terminologi lain untuk *digital signature* adalah '*digitally ensured document*', agar maknanya tidak rancu. Jadi dapat diibaratkan sebagai dokumen yang sudah 'dikunci' dan tidak bisa dimanupulasi isinya.

Di negara-negara maju, seperti di Amerika Serikat, beberapa negara bagiannya sudah menerapkan peraturan mengenai *digital signature.* Ada beberapa negara bagian yang membuat peraturan yang sangat komprehensif, tetapi ada juga yang membuat peraturan yang sangat ringkas. Bahkan ada juga negara yang menggabungkannya dengan peraturan mengenai Internet dan informasi multimedia, seperti di Malaysia.

Namun itu bukan berarti bahwa kalau di Indonesia belum ada peraturan mengenai *digital signature*, maka tidak ada hukum yang menangani masalah itu.

Ada sebuah asumsi yang salah, bahwa 'jika belum ada undang-undang tentang sesuatu hal maka dikatakan belum ada hukumnya'. Pemahaman seperti ini sebenarnya adalah tidak tepat, mengingat bahwa hukum berasal dari norma-norma yang telah ada dan berlaku dimasyarakat, sehingga tidak dapat dikatakan terhadap setiap sesuatu hal yang baru yang belum ada undang-undangnya dikatakan belum ada hukumnya.

Apalagi, sebenarnya peraturan-peraturan yang telah ada di Indonesia, sebenarnya bisa diambil sebagai sebagai batu acuan untuk membahas masalah electronic commerce, khususnya penggunaan *digital signature* dalam *electronic commerce*. Oleh karena itu dalam penelitian ini, dibuatlah terlebih dahulu kerangka kajiannya sebagai berikut:



Gambar 3. Kerangka kajian

Dalam penelitan ini, pembahasan dilihat dari berbagai aspek:

1. Aspek Hukum Publik/Pidana
2. Aspek Hukum Perdata, Perikatan/Kontrak, termasuk masalah *Certificate Authority* (CA)
3. Aspek Kontrak Perdagangan Internasional, mencakup pembahasan kontrak internasional berdasarkan UNCSIG, model law *electronic commerce* dan *digital signature* dari UNCITRAL dan GUIDEC, serta penegakan hukumnya.
4. Aspek Hukum Tentang Pembuktian (Acara), menjelaskan tentang bagaimana tanda tangan digital bisa menjada alat bukti yang sah di pengadilan
5. Aspek Asuransi E-Commerce, menjelaskan masalah asuransi perdagangan dan relevansinya dengan perdagangan di Internet. Dibahas pula mengenai *risk analysis* pembobolan kunci kriptografis yang dipergunakan dalam *digital signature.*
6. Aspek Hukum Perlindungan Konsumen
7. Keberlakuan Hukum Hak Atas Kekayaan Intelektual

Hasil penelitan menunjukkan bahwa Indonesia secara mental masih belum siap sedangkan di lain sisi, hal ini sifatnya sangat mendesak. Kalangan masyarakat Indonesia yang selama ini telah melakukan kegiatan dalam ruang lingkup *electronic commerce*, setidak-tidaknya yang mengetahui atau concern mengenai masalah ini hanya terbatas pada kalangan yang selama ini akrab dengan Internet (walaupun telah disebutkan sebelumnya kemungkinan *e-commerce* di luar Internet). Sedangkan kalangan ini hanyalah sebagian kecil dari masyarakat. Selain karena pengguna komputer (yang secara tidak langsung berpengaruh) relatif masih sedikit. Dengan perkataan lain, masyarakat Indonesia harus segera menyiapkan diri menghadapi masalah ini sesegera mungkin, mengingat negara lain sudah menyiapkan diri dalam mensikapi perdagangan secara elektronis, dengan adanya kemudahan-kemudahan yang dibawanya. Oleh karena itu, perlu dipikirkan adanya sosialisasi *e-commerce* kepada seluruh masyarakat Indonesia

Kemudian ada masalah, belum siapnya beberapa peraturan hukum Indonesia. Prinsip yang disarankan untuk dipegang adalah *"Transform the Medium, not the Instrument"*. Kegiatan-kegiatan dalam *e-commerce* secara general masih dapat dikategorikan sebagai tindakan perdagangan/peniagaan biasa, walaupun terdapatnya hal-hal yang signifikan yang membedakannya seperti media elektronik yang menggantikan *paper-based transaction.* Dapat dikatakan beberapa peraturan hukum yang telah ada sekarang ini sudah dapat mencukupi, baik dengan cara melakukan penafsiran secara analogis terhadap tindakan yang ada dalam *e-commerce* (terhadap aturan yang belum ada) maupun melakukan penafsiran ekstentif dengan cara memberlakukan peraturan hukum pada hal-hal yang secara esensi adalah sama (contohnya: listrik dan data elektronik).

Dalam hal-hal yang khusus, sangat perlu dibuat peraturan hukum baru, seperti adanya pengaturan khusus di bidang *digital signature* sebagai mekanisme sekuriti utama untuk *e-commerce*, karena dalam bidang ini tidak dapat dilakukan penafsiran untuk menghindarkan kesalahpengertian mengenai esensi dari *digital signature*.

Perlu diperhatikan lebih lanjut bahwa perangkat hukum di Indonesia khususnya hukum perdata pada dasarnya telah mampu menjangkau permasalahan-permasalahan yang timbul. Hukum perdata ini secara umum. (sec.general: norma sdh mampu, tetapi Indonesia masih membutuhkan pengaturan yang lebih spesifik untuk menjamin kepastian hukum bagi setiap perbuatan hukum perdata khususnya di bidang *electronic commerce.*

Mengenai masalah *digital signature* sebagai alat bukti dalam peradilan, sebenarnya, hakim sesuai dengan ketentuan Pasal 22 Algemene Bepalingen, dilarang menolak untuk mengadili suatu perkara yang belum ada pengaturan hukumnya. Hakim juga dituntut untuk melakukan rechtvinding (penemuan hukum) selain melakukan penafsiran analogis maupun penafsiran ekstentif yang telah dikemukakan di atas.

Peran dari para konsultan hukum yang mewakili pihak yang melakukan suatu perbuatan hukum di bidang ecom sangat besar. Untuk sementara, yang dilakukan mereka adalah mencari norma-norma

Penelitian ini juga merekomendasikan agar dibentuk suatu tim khusus di bidang hukum/regulasi e-commerce sesegera mungkin. Tim khusus ini perlu segera dibentuk untuk mempersiapkan peraturan hukum di bidang e-commerce khususnya Digital Signature. Kedudukan tim ini di bawah beberapa departemen, seperti Sekretariat Negara, Departemen Perdagangan dan Industri, Departemen Kehakiman, Departemen bidang Telekomunikasi, dan beberapa Departemen lainnya yang berkaitan erat dengan masalah ini. Tim khusus ini dapat bekerja secara inter departemen sehingga segala permasalahan dapat dicakup secara luas.

Peneliti:

Arrianto Mukti Wibowo, Edmon Makarim, Leny Helena, Hendra Yuristiawan, Aulia Adnan, Erwin Sundoro, Patricia Gaby K., Leo Faraytody.

BAB III

Anggaran Dan Jadual

A. Anggaran

Catatan:

a. anggaran adalah selama 52 minggu
b. angka dalam ribuan rupiah

Gaji dan Upah

No.	Pelaksana	Jumlah Pelaksana	Jumlah jam / minggu	Honor / jam	Jumlah
1	Peneliti Utama	1	15	8	6240
2	Peneliti 1	1	11	8	4576
3	Peneliti 2	1	4	8	1664
4	Teknisi / peneliti pembantu	12	2.5	4.5	7020
	J U M L A H				19500

Anggaran untuk Bahan

No.	Nama Bahan	Biaya
1	Layanan Intranet & Internet	1200
2	Sewa PC tambahan (2 buah)	6000
2	Cosumables (kertas, tinta, disks, etc) + photocopy	154
	J U M L A H	7354

Anggaran untuk Peralatan

No	Nama Alat	Jumlah barang	Harga satuan	Jumlah Harga
1	Komputer mikro (PC)	2	7000	14000
	J U M L A H			14000

Anggaran untuk Perjalanan

No.	Tujuan	Biaya
1	Pameran Telkom Techno Pre-Emminance 1998 (4 hari)	5900
	J U M L A H	5900

Total pengeluaran adalah: <u>Rp.46.754.000,-</u>

B. Jadual Kegiatan Penelitian

Kegiatan Tahun 1999/2000 (12 bulan):

Nama Kegiatan	1	2	3	4	5	6	7	8	9	10	11	12
1. Penelitian SET												
a. analisis awal												
b. perancangan												
c. impelementasi												
d. uji coba												
2. Penelitian Kartu Kesehatan												
3. Penelitian PayCard Off-line												
4. Penelitian Kartu Kredit Anonim												
5. Penelitian Hukum *Digital Signature*												
a. preliminary research												
b. pengumpulan materi												
c. analisis & sintesis												
6. Penulisan laporan												

BAB IV

Kegiatan-kegiatan Dalam Rangka Penelitian

A. Pembagian Tugas

Penelitia Utama

- Memberikan arahan strategis terhadap penelitian ini
- Mensupervisi kegiatan penelitian
- Melakukan lobbying kepada pihak-pihak luar yang terkait

Peneliti

- Melakukan perancangan yang lebih detail terhadap sub-penelitian
- Melakukan supervisi harian terhadap masalah-masalah yang muncul
- Membantu teknisi memecahkan masalah yang ada

Teknisi / Peneliti Pembantu

- Melakukan implementasi dan coding dari program
- Melakukan maintenance terhadap laboratorium

B. Pertemuan Mingguan

Guna mengkoordinasi riset, maka diadakan hari krida, yakni dimana seluruh anggota riset hadir dan berkumpul. Pada hari krida tersebut, biasanya salah seorang anggota tim peneliti akan melakukan presentasi terhadap apa yang pernah ditelitinya agar pengetahuannya dapat diberikan kepada anggota tim yang lain. Problem diutarakan dihadapan anggota tim yang lain, sehingga bisa dibahas bersama.

1. Untuk tim peneliti dari Fakultas Ilmu Komputer UI, hari krida adalah hari Rabu siang pukul 13.30 sampai 15.00 dimana diskusi dan presentasi dilakukan. Sedangkan pada hari Jum'at pukul 13.30 – 15.00 dilakukan supervisi langsung di hadapan komputer untuk memantau sejauh mana telah diimplementasikan.
2. Untuk tim peneliti dari Fakultas Hukum UI, hari krida untuk diskusi dan prsentasi adalah hari Jum'at pukul 15.00 s/d 17.00, bertempat di Fakultas Hukum UI lantai 2.

C. Pameran

Pada bulan Oktober 1998, tim peneliti diberi kesempatan untuk mewakili Universitas Indonesia dalam pameran Techno Pre-Eminence yang tahun 1998 itu bertemakan E-commerce, yang diselenggarakan Divisi Risti P.T. Telkom di Bandung.

D. Kerjasama Dengan Institusi Lain

Karena kekurangan dana untuk membeli smartcard, maka tim peneliti memutuskan untuk bekerja sama dengan pihak swasta. Dari beberapa perusahaan yang dihubungi, hanya satu, yakni Siemens Indonesia, yang bersedia bekerja sama. Siemens meminjamkan sebuah PC yang sudah dilengkapi dengan smartcard reader. Sayangnya, karena kekuranglengkapan driver dan masalah inkompatibilitas API, smartcard dari Siemens itu tidak dapat dipergunakan oleh *SmartWallet* yang dikembangkan dalam penelitian ini. Akibatnya, implementasi smartcard menggunakan smartcard lama yang telah dimiliki oleh Fakultas Ilmu Komputer, yakni produk dari Alladin.

E. Seminar Mingguan

Fakultas Ilmu Komputer, Universitas Indonesia telah mengembangkan tradisi melakukan seminar mingguan. Setiap peneliti secara bergiliran menjadi pembicara dalam seminar tersebut. Khusus untuk penelitian yang kami lakukan, kami telah mempresentasikan penelitian kami sebanyak dua kali di seminar mingguan.

F. Komunikasi & Penyebaran Hasil Penelitian

Untuk lebih menyebar luaskan hasil penelitian, seluruh hasil-hasil penelitian ini dapat diakses oleh publik melalui Internet di alamat:

http://www.geocities.com/amwibowo/resource.html

Kemudian ternyata, penelitian ini bersamaan waktunya dengan inisiatif dari Masyarakat Telekomunikasi (Mastel) Indonesia untuk membuat kelompok kerja bidang Electronic Commerce. Tim peneliti ikut aktif dalam pokja E-commerce Mastel. Hasil penelitian mengenai kerangka hukum *digital signature* sudah dipresentasikan di hadapan Mastel di Fakultas Ilmu Komputer UI, bulan Juni 1999. Bahkan, dokumen hasil penelitian ini, menjadi salah satu draft untuk direkomendasikan kepada pemerintah.

G. Penulisan artikel populer

Beberapa artikel populer yang dihasilkan dalam periode penelitian ini antara lain:

1. *Mengupas Rahasia Penyandian Informasi*, Infokomputer Internet, IS Wishnu B. Prasetya, Juni 1998.
2. *Mengenal Tanda Tangan & Sertifikat Digital*, Infokomputer Internet, Arrianto Mukti Wibowo, Juni 1998

H. Pengajaran (coursework)

Pada semester I tahun ajaran 1998/1999, yakni bulan September sampai Desember 1999, Fakultas Ilmu Komputer UI juga menyelenggarakan mata kuliah topik khusus “Sekuriti Digital”.

Penutup

Hambatan utama yang dihadapi dalam penelitian ini adalah masalah pendanaan, karena anggaran dipotong sebesar 50% dari proposal awal. Smartcard yang seharusnya dibeli, akhirnya tidak dibeli. Dalam penelitian ini, tim peneliti menggunakan smartcard Alladin yang pernah dibeli dari proyek penelitian sebelumnya. Kemudian, tim peneliti meminta bantuan (pinjaman) dari Siemens Indonesia, sebuah PC dengan smartcard, meskipun akhirnya tidak dapat dipergunakan oleh *SmartWallet* dalam protokol SET, karena masalah ketidakcocokan API.

Meskipun demikian, semua tujuan penelitian dalam proposal (tahun pertama) dapat dilaksanakan, bahkan *melebihi target*, seperti misalnya implementasi wallet dan library SET, yang benar-benar *binary compatible* dengan standar protokol SET. Sub-penelitian yang melebihi target adalah penelitian mengenai kerangka hukum *digital signature* untuk Indonesia, yang tadinya hanya merupakan 'efek sampingan' dari penelitian utama. Bahkan kerangka hukum *digital signature* dari penelitian ini menjadi referensi pertama di Indonesia untuk hukum yang berkenaan dengan masalah *digital signature* dalam *electronic commerce* di Indonesia.

Lembar Pengesahan

Mengetahui

Lembaga Penanggung Jawab

Dekan Fakultas Ilmu Komputer

(Ir. Bagyo Y. Moeliodihardjo, MSc.)

NIP. 130-517-315

Peneliti Utama

(F.X. Nursalim Hadi, PhD.)

NIP. 132-137-885

Telah diperiksa

Tim Pemantau dan Evaluasi

Riset Unggulan Terpadu (RUT)

Ketua

Uhum Tambunan

NIP. 680-000-378