Studi dan Perbandingan Penerapan Protokol Kriptografi Kunci Publik pada Transaksi Elektronik

Elfira Yolanda S – NIM : 13503087

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13087@students.if.itb.ac.id

Abstrak

Sebuah *website* secara otomatis dapat membawa sebuah perusahaan ke pasar global. Perusahaan dapat membuat sebuah toko *online* dan "berdagang" di sana. Transaksi pembelian dan penjualan bukan lagi milik toko yang memiliki bentuk fisik. Seiring dengan makin meluasnya penggunaan internet, penggunaan untuk bisnis pun makin meningkat, salah satunya untuk melakukan transaksi secara elektronik. Transaksi elektronik menguntungkan karena dapat menurangi biaya transaksi bisnis dan dapat memperbaiki kualitas pelayanan kepada pelanggan. Walaupun demikian, sistem transaksi elektronik yang rapuh mudah sekali disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab.

Seperti layaknya sebuah transaksi dagang, transaksi elektronik melibatkan lebih dari satu pihak. Karena tidak memungkinkan pemindahan uang transaksi secara kontan, pemindahan yang terjadi hanya berupa informasi mengenai transaksi yang terjadi saja, termasuk misalnya jumlah potongan yang harus dilakukan pada akun bank tertentu dan penambahan nilai uang pada akun yang lain. Informasi tersebut menjadi amat penting dan dengan demikian menarik serangan-serangan, entah untuk mencuri informasi tersebut atau bahkan memodifikasinya. Kriptografi dapat berperan di dalamnya, salah satunya penerapan kriptografi kunci publik.

Ada dua protokol kriptografi (lengkap dengan infrastruktur kunci publiknya) yang dapat digunakan dalam transaksi elektronik, yaitu *Secure Socket Layer* (SSL) dan *Secure Electronic Transaction* (SET). SSL hadir lebih dahulu dibandingkan SET dan sudah banyak digunakan. SET sendiri dikembangkan oleh kerja sama antara Visa dan MasterCard sejak tahun 1996. Makalah akan mengangkat studi terhadap penerapan kriptografi pada transaksi elektronik dan juga perbandingan terhadap dua protokol kriptografi yang biasa digunakan pada transak elektronik tersebut.

***Kata kunci**: e-commerce, transaksi elektronik, protokol kriptografi, SSL, SET*

1. Pendahuluan

Seiring dengan berkembangnya teknologi informasi, penggunaan internet pun semakin dekat dengan kehidupan sehari-hari. Kegiatan seperti mengirim pesan, mencari informasi, belajar, dan mendapatkan hiburan, semuanya dapat dilakukan dengan menjelajahi dunia maya. Bahkan, saat ini masyarakat bisa memperoleh barang atau yang mereka inginkan melalui internet.

Kegiatan jual beli barang dan jasa di internet bukan suatu yang baru lagi. Masyarakat dapat dengan mudah melihat barang atau jasa yang ditawarkan penjual melalui "etalase" pada website mereka. Transaksi dapat terjadi seperti layaknya transaksi lain, hanya saja dilakukan secara elektronik.

Tidak berbeda dengan transaksi keuangan lain, transaksi elektronik juga melibatkan pertukaran nilai keuangan tertentu. Namun, apabila transaksi lain menggunakan koin, uang kertas, cek atau benda fisik lain sebagai

tanda pertukaran nilai, transaksi elektronik ditandai dengan pertukaran data. Untuk melakukan pertukaran data tersebut, data dapat dikirimkan melalui jaringan internet. Cara tersebut murah, mudah, dan cepat, tapi bukannya tidak ada harga yang harus dibayar. Faktor keamanan menjadi bahan pertimbangan dengan aspek yang berbeda dengan faktor tersebut pada transaksi dunia nyata. Ada kebutuhan untuk menyediakan pengamanan data rahasia, seperti nomor kartu kredit, yang juga berarti kebutuhan untuk menyediakan saluran komunikasi yang aman [7]. Kriptografi memegang peranan penting dalam hal ini dan tujuan dari makalah ini adalah untuk memperlihatkan penerapan protokol kriptografi pada transaksi elektronik.

Struktur penulisan makalah

Untuk memahami perlunya penerapan protokol kriptografi, pada **bagian 2** makalah ini, *e-commerce dan transaksi elektronik*, akan membahas sekilas mengenai e-commerce dan transaksi elektronik. Kedua hal tersebut berkaitan erat dan merupakan asal dari kebutuhan akan keamanan data yang dipertukarkan. Lalu, untuk memenuhi kebutuhan tersebut, ilmu kriptografi digunakan. Pada **bagian 3**, *kriptografi dalam transaksi* elektroni*k*, istilah-istilah yang berkaitan dengan sentuhan kriptografi yang ada pada transaksi elektronik akan dibahas. Secara spesifik, makalah ini mengangkat dua protokol kriptografi yang pernah dan masih digunakan untuk melakukan transaksi elektronik. Keduanya akan diberikan pada **bagian 4**, *Secure Socket Layer* (SSL), dan kemudian **bagian 5**, *Secure Electronic Transaction* (SET). Sebagai penutup, makalah ini akan menyajikan *perbandingan SSL dan SET* pada **bagian 6** serta ***kesimpulan*** yang bisa ditarik dari penerapan kedua protokol kriptografi tersebut dalam transaksi elektronik.

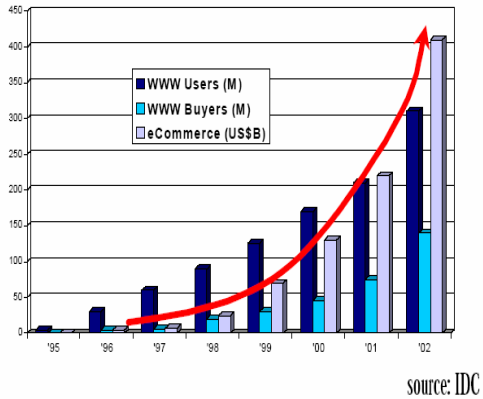
2. E-*commerce* dan transaksi elektronik

E-commerce, istilah yang lazim untuk *electronic commerce*, mengacu pada berbagai kegiatan bisnis, baik menyangkut barang maupun jasa, yang berlangsung secara *online* [4]. Tidak ada kegiatan bisnis yang berlangsung tanpa transaksi. Transaksi yang terjadi pada e-commerce disebut transaksi elektronik. Bab kedua dari makalah ini dikhususkan untuk membahas kedua istilah yang tidak dapat dipisahkan tersebut, untuk memberikan gambaran awal yang jelas mengenai celah awal masuknya kriptografi pada kedua istilah itu.

2.1. *E-commerce*

Saat ini belum ada definisi *e-commerce* yang disepakati bersama sehingga sering terjadi kerancuan. Ada yang mengatakan bahwa *e-commerce* adalah web site yang digunakan untuk berdagang (semacam *storefront*), ada yang dimaksud *e-commerce* adalah *Electronic Data Interchange* (EDI), dan seterusnya [12]. Sebagai cantoh, berikut ini adalah definisi *e-commerce* diambil dari [11]:

E-Commerce is a dynamic set of technologies, applications, and business process that link enterprises, consumers, and communities through electronic transactions and the electronic exchange of goods, services, and information.
(E-commerce adalah himpunan dinamis dari teknologi, aplikasi, dan bisnis proses yang menghubungkan perusahaan, konsumen, dan berbagai komunitas melalui transaksi elektronik dan pertukaran barang, layanan, maupun informasi secara elektronik)



Gambar 1 Pertumbuhan e-commerce menurut IDC

Untuk memperjelas, makalah ini memberikan batasan e-commerce pada kegiatan bisnis yang dilakukan secara *online*. Dengan pengertian seperti itu, e-commerce menunjukkan perkembangan yang luar biasa. **Error! Reference source**

not found.menunjukkan peningkatan yang terjadi pada jumlah pengguna internet, jumlah pembeli melalui internet, dan nilai uang (dalam US dollar) yang terlibat dalam e-commerce sejak tahun 1995 sampai tahun 2002.

Bisnis yang dijalankan secara *online* biasanya memiliki elemen-elemen sebagai berikut:

- Mengiklankan produk perusahaan
- Menawarkan produk tersebut
- Menjual produk
- Mengeluarkan tagihan
- Menerima pembayaran
- Memverifikasi informasi pembayaran pada pihak terkait, dan
- Mengantarkan pesanan

Kegiatan-kegiatan tersebut bisa saja menyertakan persetujuan kontrak tertentu, pengaturan untuk pengantaran barang, dan ketentuan pajak serta layanan penjualan pasca pembelian yang disediakan. Sejauh ini tidak ada perbedaan berarti dengan kegiatan bisnis biasa.

Yang menjadi pembeda adalah seluruh kegiatan yang disebutkan di atas dilakukan tanpa pertukaran fisik atau kontak fisik langsung antar partisipan kegiatan. Yang memungkinkan itu semua terjadi tentu teknologi yang dikenal dengan jaringan internet, baik publik maupun privat. Bahkan, saat ini, jaringan internet tidak hanya menghubungkan komputer saja, tetapi juga alat-alat teknologi lain seperti *Personal Digital Assistance* (PDA) atau telepon genggam. Asalkan memiliki kemampuan untuk terhubung dengan jaringan internet, *e-commerce* dapat berlangsung.

Perkembangan yang terjadi bukan hanya pada media *e-commerce*, tetapi juga pada jenis *e-commerce* itu sendiri. *E-commerce* tidak lagi sebatas kegiatan bisnis antara perusahaan penjual dan masyarakat umum sebagai pembeli. Berikut merupakan beberapa jenis *e-commerce*:

- *Business to- Consumer* (B2C)
- *Business-to-Business* (B2B)
- *Consumer-to-Consumer* (C2C)
- *Business-to-Government* (B2G)
- *Mobile commerce* (*m-commerce*)

2.1.1. Business to Consumer (B2C)

Tipe *e-commerce* yang satu ini adalah yang paling umum dan dikenal. Ada perusahaan yang menjual kepada konsumen. Produk yang ditawarkan amat bervariasi. Cerita sukses jenis *e-commerce* B2C pernah terjadi untuk bisnis perumahan (*real estate*), perjalanan / wisata, pelelangan barang, dan bisnis perbankan. Sedangkan *e-commerce* yang menawarkan produk yang memerlukan "sentuhan tambahan" atau kegiatan mencoba langsung seperti pakaian dan barang-barang mewah biasanya tidak berkembang.

2.1.2 Business to Business (B2B)

Jika *e-commerce* B2C menekankan pada pemasaran dan penjualan produk perusahaan, jenis B2B difokuskan pada pemenuhan kebutuhan perusahaan. Contoh yang paling dapat menjelaskan adalah kegiatan bisnis yang terjadi antar perusahaan, misalnya antara perusahaan dengan *supplier* dan *distributor*-nya (yang merupakan perusahaan lain dengan kegiatan bisnisnya sendiri). Biasanya B2B dilakukan untuk *supply chain management* (SCM) dan sistem perusahaan-perusahaan yang terkait di dalamnya diintegrasikan.

2.1.3 C2C e-commerce

Berikut merupakan contoh e-commerce C2C:

- Pelelangan barang, contoh: eBay. Situs ini memfasilitasi pelelangan barang secara real-time.
- Sistem *peer-to-peer*, contoh: Napster. Situs ini memungkinkan penggunanya untuk saling berbagi data.

2.1.4 Business-to-government e-commerce (B2G)

E-commerce B2G berarti penggunaan internet untuk memenuhi kebutuhan sektor publik, misalnya perusahaan negara. Biasanya pihak sektor publik atau pemerintahan-lah yang membuat situs e-commerce, beserta segala peraturan yang berkaitan dengan transaksi yang dapat terjadi. Bagaimanapun juga, jumlah situs e-commerce jenis ini paling sedikit.

2.1.5 Mobile Commerce (m-commerce)

M-commerce hadir karena keberadaan teknologi nirkabel (wireless). Presentase

pemanfaatan m-commerce melalui laptop/notebook dan telepon genggam relatif seimbang. Keuntungan terbesar jenis ini terletak pada karakter mobilitas yang tinggi sehingga akses dapat dilakukan kapan saja dan di mana saja. Karakter tersebut juga mengakibatkan peningkatan layanan yang dapat dihadirkan pada m-commerce, misalnya pembayaran tagihan dengan pulsa telepon genggam atau pengiriman notifikasi saat jumlah akun di bank mulai mendekati batas bawah yang ditentukan.

2.2. Transaksi elektronik

Transaksi elektronik yang dimaksud dalam makalah ini adalah transaksi yang melibatkan pertukaran nilai keuangan. Ada nilai uang yang berkurang dan bertambah pada pihak tertentu. Dengan demikian, transaksi seperti yang terjadi pada *data sharing* yang dilakukan di Napster (lihat poin 2.1.3), meskipun juga terdapat pertukaran di dalamnya, tidak termasuk hitungan.

Pertukaran nilai keuangan berarti ada kegiatan pembayaran di dalamnya. Ada banyak cara pembayaran yang mendukung transaksi elektronik dan *e-commerce*, di antaranya:
- kartu pembayaran elektronik (baik debit maupun kredit)
- *E-wallets /e-purses* (dompet elektronik)
- *Smart cards*
- pembayaran nirkabel (*Wireless payments*)
- *Stored-value card payments*
- *Loyalty cards*
- *Person-to-person payment methods*
- Pembayaran elektronik pada kios-kios khusus.

Makalah ini hanya akan mengambil jenis pembayaran kartu kredit pada transaksi elektronik karena cara ini adalah cara yang populer untuk pembayaran barang, informasi, maupun layanan yang didapat melalui internet (*e-commerce*) [6].

Berkaitan dengan pembayaran kartu kredit, ada beberapa pertanyaan yang menjadi perhatian, seperti:

a. Apakah kartu kredit masih valid atau tidak?
b. Apakah pengguna kartu kredit saat itu merupakan pemegang kartu yang sah?
c. Apakah penjual yang menawarkan produk benar dapat menangani transaksi kartu kredit?
d. Apakah keterangan yang berkaitan dengan kartu kredit saat transaksi terjamin aman dan tidak akan bocor kepada pihak yang tidak berkepentingan?
e. Apakah sistem pembayaran kartu kredit tersebut menerima banyak jenis kartu kredit atau hanya kartu tertentu saja?
f. Apakah sistem pembayaran yang ada mudah digunakan oleh pemegang kartu?
g. Apakah sistem pembayaran menguntungkan si penjual atau malah menghabiskan dana yang besar untuk biaya implementasi dan pemeliharaannya?
h. Apakah sistem dapat dengan mudah dikembangkan?

Meskipun tidak membentuk keseluruhan dari proses pembayaran kartu kredit, pertanyaan yang menyangkut keamanan dalam transaksi cukup mendominasi. Hal ini tidak berbeda jauh dengan pembayaran pada transaksi elektronik.

Pembayaran pada transaksi elektronik pada dasarnya sama dengan pembayaran kartu kredit, hanya saja tanpa kehadiran fisik kartunya. Seperti yang telah disinggung pada bagian 1, sebagai pengganti kehadiran kartu, ada informasi berkaitan dengan kartu kredit yang dipertukarkan.

Perbedaan lainnya adalah proses pembayaran yang terjadi pada sisi penjual berlangsung secara otomatis. Minimnya peranan manusia sebenarnya membawa keuntungan tersendiri, yakni penanganan banyak transaksi dapat dilakukan lebih cepat dan lebih murah. Tetapi, keuntungan yang dapat membuka peluang lebih lebar pada *e-commerce* juga membuat celah dari segi keamanan.

Dalam melakukan pembayaran pada transaksi elektronik, baik pembeli maupun penjual bisa menjadi pihak pelaku kejahatan. Penjual tidak benar-benar mempunyai produk yang ditawarkan dan hanya ingin mengambil uang pembeli atau pembeli yang

menggunakan kartu palsu untuk mendapatkan produk yang diinginkan. Dengan kondisi seperti ini, kepercayaan terhadap semua pihak harus dipertanyakan dan suatu bentuk mekanisme pengamanan diperlukan.

3. Kriptografi dalam transaksi elektronik

Menilik kembali pertanyaan- pertanyaan yang harus diperhatikan pada bagian 2.2, ada aspek-aspek kriptografi yang menjadi isu penting pada transaksi elektronik. Aspek-aspek kriptografi yang dimaksud adalah:

- **Autentikasi pelaku transaksi atau keabsahan pelaku transaksi (*authenticity*),** yang menjamin bahwa pihak penjual dan pembeli adalah pihak yang berhak melakukan transaksi elektronik.
- **Autentikasi data atau keaslian data, yang** mencakup kerahasiaan (*confidentiality*) dan integritas data (*integrity*), yang menjamin data yang dikirim sepanjang transaksi tidak diketahui oleh pihak lain yang tidak berwenang, apalagi sampai berubah.
- **Anti penyangkalan (*non-repudiation*)**, yang menjamin bahwa pengirim tidak dapat menyangkal bahwa dialah yang mengirim data.

Ketiga aspek kriptografi tersebut menjadi kebutuhan yang tidak terelakkan dalam sebuah transaksi elektronik. Untuk transaksi non-elektronik, solusi yang dapat diambil adalah sebagai berikut, untuk masing-masing aspek:

- *Autentikasi pelaku*, dengan kehadiran fisik atau menghadirkan notaris
- *Kerahasiaan data*, dengan menggunakan amplop.
- *Integritas data*, dengan tanda tangan
- *Anti penyangkalan*, dengan tanda tangan, atau bukti tertulis.

Sedangkan untuk transaksi elektronik, berikut adalah langkah-langkah yang dapat diambil:

- *Autentikasi pelaku*, dengan tanda tangan digital dan atau sertifikat digital.
- *Kerahasiaan data*, dengan melakukan enkripsi.
- *Integritas data*, dengan tanda tangan digital atau fungsi hash.
- *Anti penyangkalan*, dengan tanda tangan digital.

Seperti yang dapat dilihat, langkah-langkah tersebut merupakan bagian dari penerapan ilmu kriptografi. Selain langkah-langkah di atas, kriptografi juga memiliki sesuatu yang juga dapat menjadi solusi keamanan transaksi elektronik, yaitu **protokol kriptografi**.

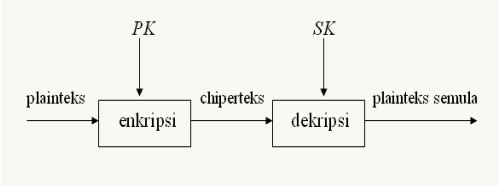
Bagian 3 dari makalah ini akan mengangkat sentuhan kriptografi yang dapat masuk dalam sebuah transaksi elektronik, antara lain sistem kriptografi kunci publik, tanda tangan digital, sertifikat digital, dan protokol kriptografi.

3.1. Sistem Kriptografi Kunci-Publik

Sampai akhir tahun 1970, hanya ada sistem kriptografi simetri. Karena sistem kriptografi simetri menggunakan kunci yang sama untuk enkripsi dan dekripsi, maka hal ini mengimplikasikan dua pihak yang berkomunikasi saling mempercayai.

Ide dasar dari sistem kriptografi kunci-publik adalah bahwa kunci kriptografi dibuat sepasang, satu kunci untuk enkripsi dan satu kunci untuk dekripsi.

Kunci untuk enkripsi bersifat publik (tidak rahasia) – sehingga dinamakan kunci publik (*public-key*) – sedangkan kunci dekripsi bersifat rahasia – sehingga dinamakan kunci rahasia (*private key* atau *secret key*). Kunci-kunci ini dipilih sedemikian sehingga – secara praktek – tidak mungkin menurunkan kunci rahasia dari kunci publik.



Gambar 2 Skema sistem kriptografi kunci publik

Sistem kriptografi kunci-publik cocok untuk kelompok pengguna di lingkungan jaringan komputer. Setiap pengguna jaringan mempunyai kunci publik dan kunci rahasia yang bersuaian. Kunci publik, karena tidak rahasia, biasanya disimpan di dalam

basisdata kunci yang dapat diakses oleh pengguna lain. Jika ada pengguna yang hendak berkirim pesan ke pengguna lainnya, maka ia ia perlu mengetahui kunci publik penerima pesan melalui basisdata kunci ini lalu menggunakannya untuk mengenkripsi pesan. Hanya penerima pesan yang berhak yang dapat mendekripsi pesan karena ia mempunyai kunci rahasia.

Dengan sistem kriptografi kunci publik, tidak diperlukan pengiriman kunci rahasia melalui saluran komunikasi khusus sebagaimana pada sistem kriptografi simetri.

Meskipun kunci publik diumumkan ke setiap orang di dalam kelompok, namun kunci publik perlu dilindungi agar otentikasinya terjamin (misalnya tidak diubah oleh orang lain) [2].

Keamanan sistem kriptografi kunci publik terletak pada dua hal:

1. Sulitnya menurunkan kunci rahasia dari kunci publik.
2. Sulitnya menurunkan plainteks dari cipherteks.

Kelemahan sistem kriptografi kunci publik di antaranya:

1. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri, karena enkripsi dan dekripsi melibatkan operasi perpangkatan yang besar.
2. Ukuran cipherteks lebih besar daripada plainteks (bisa dua sampai empat kali ukuran plainteks).
3. Karena kunci publik diketahui secara luas dan dapat digunakan setiap orang, maka cipherteks tidak memberikan informasi mengenai otentikasi pengirim.

Sistem kriptografi kunci publik pada transaksi elektronik

Kelemahan sistem kriptografi kunci publik seperti yang disebutkan di atas berpengaruh pada penerapannya pada transaksi elektronik. Sistem ini tidak diterapkan untuk mengenkripsi langsung data yang dikirimkan pada transaksi elektronik, tetapi untuk mengenkripsi kunci sistem enkripsi simetris. Kunci sistem enkripsi simetris sendiri dibutuhkan karena data yang dikirim dienkripsi menggunakan algoritma simetris.

3.2. Tanda Tangan Digital

Sejak berabad-abad lamanya, tanda tangan (sidik yang ditulis tangan) digunakan untuk membuktikan otentikasi dokumen kertas (misalnya surat, piagam, ijazah, buku, karya seni, dan sebagainya).

Fungsi tanda tangan pada dokumen kertas juga diterapkan untuk otentikasi pada data dijital seperti pesan yang dikirim melalui saluran komunikasi dan dokumen elektronis yang disimpan di dalam memori komputer.

Tanda tangan pada data digital ini disebut tanda tangan digital (*digital signature*). Yang dimaksud dengan tanda tangan digital bukanlah tanda tangan yang di-digitasi dengan alat *scanner*, tetapi suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan (Hal ini kontras dengan tanda tangan pada dokumen kertas yang bergantung hanya pada pengirim dan selalu sama untuk semua dokumen).

Dengan tanda tangan digital, maka integritas data dapat dijamin, disamping itu ia juga digunakan untuk membuktikan asal pesan (keabsahan pengirim dan anti-penyanggahan).

Hanya sistem kriptografi kunci-publik yang cocok dan alami untuk pemberian tanda tangan digital. Hal ini disebabkan karena skema tanda tangan digital berbasis sistem kunci-publik dapat menyelesaikan masalah *non-repudiation* (baik penerima dan pengirim pesan mempunyai pasangan kunci masing-masing) [2].

3.3. Sertifikat digital

Penggunaan kriptografi kunci public mungkin membantu menjaga kerahasiaan data (*confidentiality*), tapi tidak menyumbangkan apapun untuk menyelesaikan masalah otentikasi. Seseorang dapat mengaku menjadi orang lain dengan memberikan kunci publik miliknya sendiri. Orang yang berkomunikasi dengan penipu ini dapat mengira bahwa dia berkomunikasi dengan orang yagn

identitasnya telah dicuri. Sertifikat digital hadir untuk menjadi jawaban permasalahan tersebut.

Badan yang mengeluarkan sertifikat digital adalah *Certification Authority* (CA). CA biasanya adalah institusi keuangan (seperti bank) atau institusi yang terpercaya. Sertifikat digital adalah dokumen digital yang berisi informasi sebagai berikut:

- nama subjek (perusahaan/individu yang disertifikasi)
- kunci publik si subjek
- waktu kadaluarsa sertifikat (*expired time*)
- informasi relevan lain seperti nomor seri sertifikat, dll [2]

CA akan menandatangani dokumen digital tersebut dengan menggunakan kunci privat CA. Hasilnya, jika seseorang mencoba untuk menyamar menjadi orang lain dan memberikan kunci publik yang salah, pihak lain tidak akan tertipu karena dapat memverifikasi kunci publik tersebut. Verifikasi kunci public yang palsu akan menghasilkan nilai hash yang tidak serupa dengan nilai hash yang dikeluarkan oleh CA. Perlu diingat, sertifikasi digital tidak rahasia, tersedia secara publik, dan disimpan oleh CA di dalam *certificate repositories*, selain tentu dimiliki oleh pemegang sertifikat itu sendiri.

Waktu kadaluarsa sertifikat dimaksudkan agar subjek mengganti pasangan kunci publik-kunci privatnya secara periodik. Subjek dapat mengetahui status sertifikatnya dalam *Certificate Revocation List* (CRL) yang dikeluarkan CA secara periodik. CRL berisi nomor seri digital sertifikat yang ditarik.

Tanda tangan dan sertifikat digital untuk transaksi elektronik

3.4. Protokol kriptografi

Protokol adalah aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, yang dibuat untuk menyelesaikan suatu kegiatan. Sedangkan protokol kriptografi adalah protokol yang menggunakan kriptografi.

Orang yang berpartisipasi dalam protokol kriptografi memerlukan protokol tersebut misalnya untuk:
- berbagi komponen rahasia untuk menghitung sebuah nilai,
- membangkitkan rangkaian bilangan acak,
- meyakinkan identitas orang lainnya (otentikasi), dll

Protokol kriptografi dibangun dengan melibatkan beberapa algoritma kriptografi.

Sebagian besar protokol kriptografi dirancang untuk dipakai oleh kelompok yang terdiri dari 2 orang pemakai, tetapi ada juga beberapa protokol yang dirancang untuk dipakai oleh kelompok yang terdiri dari lebih dari dua orang pemakai (misalnya pada aplikasi *teleconferencing*) [2].

Protokol kriptografi untuk transaksi elektronik

Ada dua jenis protokol kriptografi yang dapat diterapkan pada transaksi elektronik, yaitu **protokol untuk komunikasi** dan **protokol kriptografi khusus untuk transaksi keuangan**.

Protokol kriptografi untuk komunikasi tidak hanya ditujukan untuk komunikasi dalam sebuah transaksi elektronik melainkan juga segala jenis komunikasi yang terjadi pada jaringan internet. Contoh protokolnya adalah SSL, SHTTP, IP/Sec, dan sebagainya. Di antara protokol-protokol itu, yang digunakan secara luas untuk komunikasi dalam transaksi elektronik adalah SSL. Untuk lebih detail, protokol ini akan dibahas pada bagian 4 makalah.

Protokol-protokol seperti iKP, Milicent, NetCheque, SEPP, SET, SIPS, dan STT memang didesain khusus untuk implementasi transaksi elektronik yang aman, khususnya transaksi yang menggunakan kartu kredit. Protokol SET yang dibangun oleh Visa dan MasterCard adalah protokol yang sering dipakai dalam transaksi elektronik selain SSL. Bagian 5 makalah akan mendeskripsikan protokol ini lebih detail.

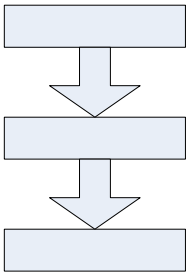
4. *Secure Socket Layer* (SSL)

SSL adalah protokol yang menyediakan layanan komunikasi yang aman di internet. Protokol SSL dibangun oleh Netscape Communication Corporation. Untuk komunikasi online, SSL memungkinkan jalur komunikasi antara penggunanya terenkripsi menggunakan teknologi kriptografi kunci publik. SSL sudah sampai pada versi ketiganya sebelum berganti nama menjadi TLS atau *Transport Layer Security*. Perbedaan TLS dengan versi paling baru SSL sendiri tidak begitu banyak jika dibandingkan dengan perbedaan antara SSL versi 3.00 dengan versi sebelumnya. Oleh karena itu, makalah ini menggunakan istilah SSL.

4.1. SSL sebagai protokol komunikasi internet

Secure Socket Layer atau biasa disingkat SSL adalah salah satu protokol kriptografi untuk komunikasi melalui internet, yang artinya SSL berisi aturan untuk menjamin komunikasi yang terjadi aman. Pendekatan keamanan pada SSL berupa lapisan protokol yang terpisah.

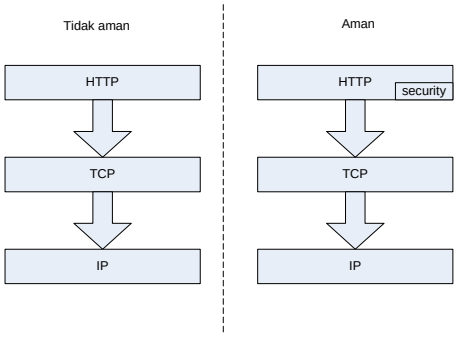
Selain pendekatan keamanan seperti pada SSL, ada pendekatan atau cara-cara lain untuk mengamankan komunikasi internet. Sebagaimana diketahui, arsitektur protokol internet terdiri atas lapisan protokol yang yang masing-masing menggunakan layanan yang disediakan oleh protokol di bawahnya. **Gambar 3 Lapisan protokol pada arsitektur internet**menunjukkan beberapa lapisan protokol yang ada. *Hypertext Transfer Protocol* (HTTP) merupakan protokol aplikasi dan berada pada lapisan paling atas. HTTP mengerti detail interaksi yang terjadi antara *browser* dan *web servers*. Lapisan *Transmission Control Protocol* (TCP) merupakan protokol yang bertugas memberikan layanan untuk HTTP dan menjamin komunikasi dapat terjadi. TCP dibangun di atas layanan IP atau *Internet Protocol*, yang bertanggung jawab untuk mengantarkan pesan melalui jaringan, atau dikenal dengan istilah *routing*.



Gambar 3 Lapisan protokol pada arsitektur internet

Pendekatan keamanan komunikasi pada jaringan internet lainnya akan dibahas sekilas di bawah ini:

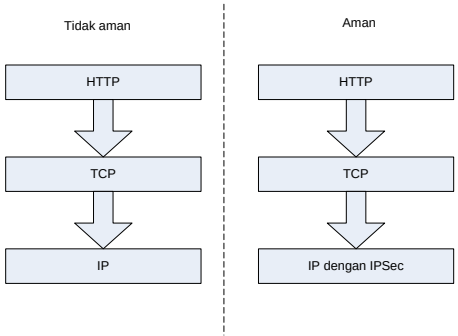
a. di dalam lapisan aplikasi
   Layanan keamanan dengan pendekatan ini ditempatkan pada lapisan aplikasi bersama dengan protokol aplikasi, yaitu HTTP. Protokol HTTP yang sudah dilengkapi fitur keamanan biasa disebut HTTPS. Karena ditempatkan pada lapisan aplikasi, pendekatan ini kurang begitu fleksibel. Untuk tiap protokol aplikasi lain (misalnya *Net News Transfer Protocol*/NTTP dan *File Transfer Protocol*/FTP), fitur keamanan yang baru harus dibuat dan diletakkan bersama dengan protokol masing-masing.



Gambar 4 Pendekatan keamanan melalui lapisan aplikasi

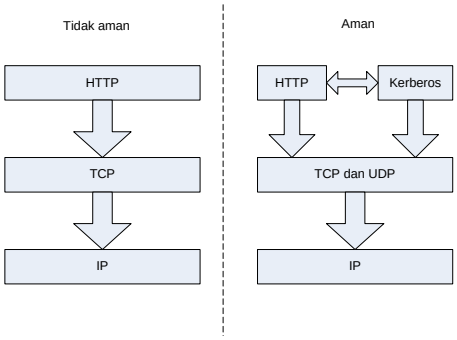
b. terintegrasi pada lapisan inti
   Berbeda dengan HTTPS, pendekatan ini menempatkan layanan keamanannya pada lapisan paling bawah, yaitu lapisan IP (IPSec). Dengan demikian, berbeda degan pendekatan sebelumnya, tidak peduli protokol aplikasi apa yang digunakan,

fitur keamanan dapat berjalan dengan baik. Tetapi, karena layanan keamanan terletak pada lapisan yang dalam, pendekatan ini tidak memungkinkan interaksi antara fitur keamanan dan aplikasinya. Sebagai contoh, aplikasi yang tidak membutuhkan fitur keamanan mau tidak mau akan mendapatkannya.



Gambar 5 Pendekatan keamanan yang terintegrasi pada lapisan IP

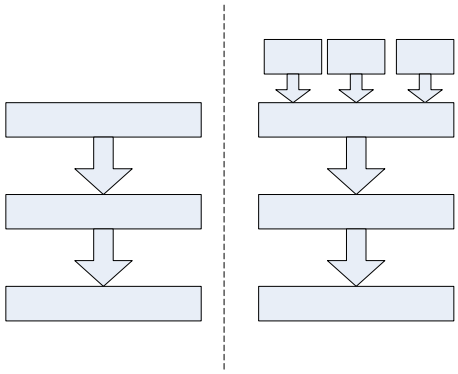
c. sebagai protokol paralel
Contoh yang paling populer dari pendekatan ini adalah protokol Kerberos yang dibangun oleh Massachusetts Institute of Technology (MIT). Protokol Kerberos merupakan protokol aplikasi dan bertindak sebagai alat yang menyediakan layanan keamanan untuk protokol lain. Yang perlu dicatat adalah, Kerberos sendiri bukan merupakan solusi keamanan yang lengkap [15]. Protokol ini tidak memiliki akses pada informasi yang ditukarkan oleh pihak yang berkomunikasi sehingga Kerberso tidak dapat menyediakan layanan enkripsi dan dekripsi.



Gambar 6 Pendekatan keamanan dengan protokol yang paralel

d. sebagai lapisan protokol terpisah
Perancang SSL memang memutuskan untuk menciptakan lapisan khusus untuk menangani keamanan. Sebagai akibatnya, lapisan baru ditambahkan dalam arsitektur protokol internet. Hal ini berarti dibutuhkan perubahan pada lapisan di atas dan di bawah SSL.

Perubahannya sendiri hanya berpengaruh bagi HTTP walaupun tidak terlalu banyak, karena HTTP tetap menjalankan fungsinya seperti biasa, kecuali layanan yang digunakan sekarang berasal dari SSL. Sedangkan untuk TCP, keberadaannya tidak berubah dan layanan milik lapisan ini digunakan oleh SSL. Sebagai ganti perubahan tersebut, ada keuntungan yang diperoleh. Protokol aplikasi yang dapat merasakan layanan keamanan bukan saja HTTP, seperti tampak pada **Gambar 7 Pendekatan keamanan dengan lapisan protokol terpisah**.



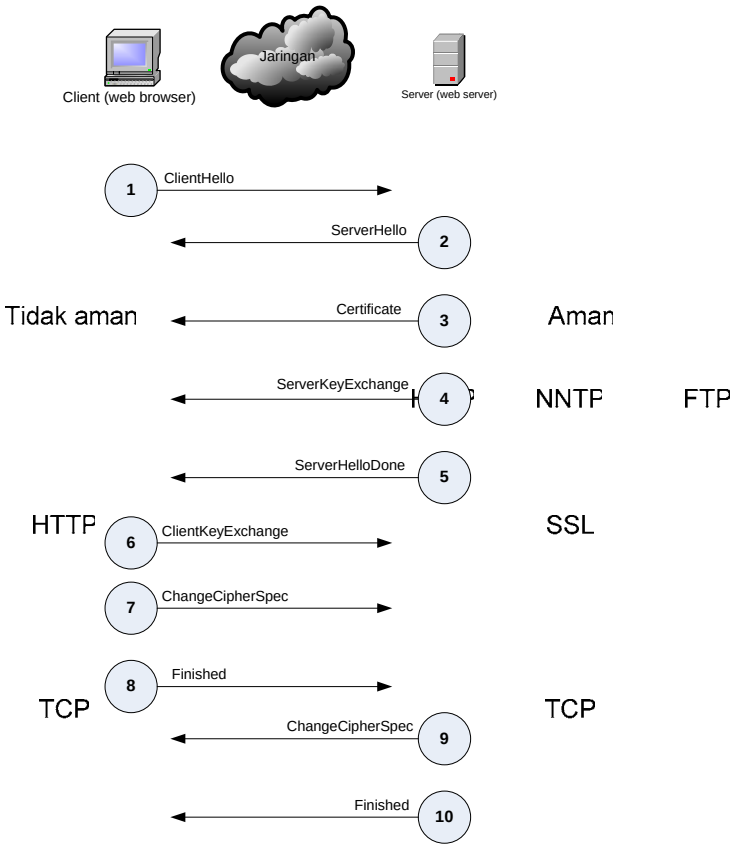
Gambar 7 Pendekatan keamanan dengan lapisan protokol terpisah

4.2. Operasi SSL

Client-Server
Protokol ini melibatkan dua partisipan. Yang satu akan berperan sebagai *client*, yang lain sebagai *server*. Seperti kebanyakan sistem *client-server*, masing-masing pihak mempunyai fungsi dan aksi yang berbeda. Dalam penggunaan SSL pada umumnya, yakni untuk melakukan *web browsing* yang aman, *web browser* bertindak sebagai *client* dan *web site* adalah *server*-nya [15].

Protokol komunikasi
Sebagai protokol komunikasi, SSL bertugas mendirikan sebuah saluran berkomunikasi yang aman antara *client* dan *server*-nya. Pihak yang berkomunikasi akan menggunakan saluran tersebut untuk bertukar data secara rahasia. SSL juga memungkinkan kedua pihak yang berkomunikasi untuk memeriksa integritas data, dan kalau diperlukan, untuk memeriksa keabsahan pihak yang sedang berkomunikasi satu sama lain.

Langkah-langkah operasi SSL dapat dilihat pada **Gambar 9 Langkah-langkah operasi protokol SSL**.Tiap langkah yang tercantum menunjukkan pesan yang dikirimkan oleh *client* atau *server*.



Gambar 8 Langkah-langkah operasi SSL

4.2.1. *ClientHello*

Pihak *client* selalu mengawali komunikasi SSL dengan mengirimkan pesan *ClientHello*. *Client* menggunakan pesan ini untuk meminta server memulai negosiasi layanan keamanan. Pesan *ClientHello* memuat:

a. *Version*, versi SSL yang dapat digunakan
b. *RandomNumber*, angka 32 byte yang dibangkitkan secara acak untuk kalkulasi kriptografi
c. *SessionID*, nomor identitas sesi
d. *CipherSuites*, daftar layanan kriptografi yang dapat dilakukan *client*, termasuk algoritma kriptografi dengan ukuran kuncinya. Algoritma kriptografi ini akan digunakan untuk mengenkripsi data yang dikirim sepanjang client dan server berkomunikasi (catatan: bukan pada saat bernegosiasi melalui protokol SSL). Algoritma kriptografi yang digunakan

merupakan **algoritma kriptografi simetri.**

e. *ComprressionMethod*, daftar metode kompresi data. Kompresi data biasa dilakukan sebelum data dienkripsi.

4.2.2. ServerHello

Reaksi pertama yang diberikan oleh *server*. Isi pesan *ServerHello* mirip dengan *ClientHello*, hanya saja pesan ini memuat pilihan *server* terhadap tiap nilai.

4.2.3. *Certificate*

Pesan ini menunjukkan niat baik *server* untuk mengidentifikasikan dirinya. *Server* mengirimkan sertifikat kunci publik yang disertai dengan sertifikat kunci publik CA, yang nantinya akan diperiksa oleh *client*.

4.2.4. *ServerKeyExchange*

Pesan kedua dari *server* ini berisi kunci publik yang akan digunakan client untuk mengenkripsi kunci enkripsi untuk sepanjang sesi komunikasi. Pesan ini ditanda-tangani menggunakan kunci privat pasangan kunci publik yang tercantum pada sertifikat yang telah dikirim sebelumnya. Tujuannya adalah untuk meyakinkan *client* kalau *server* benar memiliki kunci privat yang sesuai dengan kunci yang tercantum pada sertifikat yang dikirim.

4.2.5. *ServerHelloDone*

ServerHelloDone menandai akhir dari negosiasi awal oleh *server*.

4.2.6. *ClientKeyExchange*

Client kemudian mengirimkan kunci untuk algoritma kriptografi simetri yang dipilih untuk sepanjang komunikasi. Kunci komunikasi ini dienkripsi menggunakan kunci publik yang dikirim *server* pada pesan *ServerKeyExchange.*

4.2.7. ChangeChiperSpec

Pesan ini merupakan tanda diaktifkannya saluran komunikasi dengan fitur-fitur kriptografi yang telah disepakati sebelumnya. Semua pesan yang dikirimkan setelah pesan ini harus dienkripsi menggunakan kesepakatan yang telah terjadi sebelumnya. Perpindahan pada saluran komunikasi yang aman sangat kritikal. Oleh karena itu, pihak mana pun yang mengirimkan pesan ini harus tahu informasi keamanan yang akan digunakan secara lengkap.

4.2.8. *Finished*

Pesan terakhir ini menandakan negosiasi berjalan lancar dan sukses. Selain itu, ada dua manfaat yang diberikan oleh pesan ini. Pertama, pesan ini dapat berfungsi sebagai tanda awal dimulainya saluran komunikasi yang aman karena isi pesan ini dienkripsi dengan fitur kriptografi untuk sesi komunikasi ini. Kedua, pesan ini merangkum dan mengirimkan seluruh hasil kesepakatan atas fitur kriptografi seperti informasi kunci, isi dari pesan SSL yang dipertukarkan sebelumnya, dan nilai khusus yang menandakan pengirim pesan ini (*client* atau *server*).

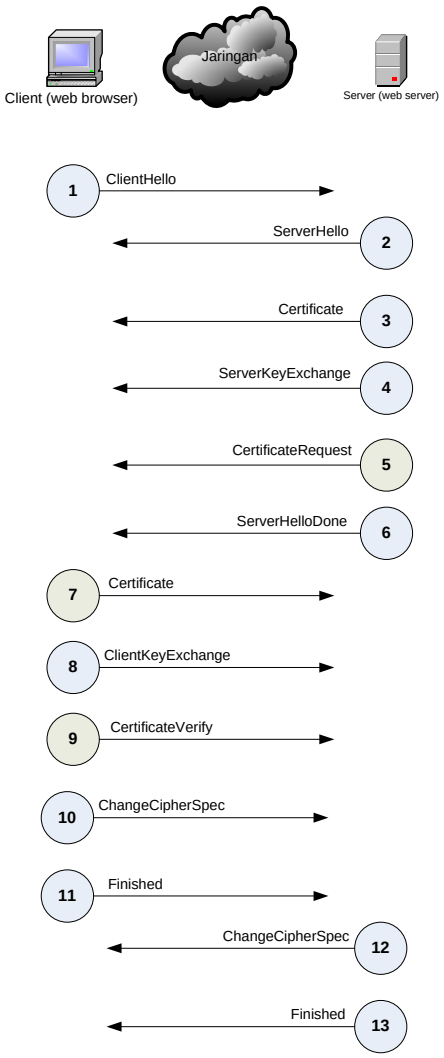
4.2.9. *ChangeChiperSpec dan Finished*

Kedua pesan penutup oleh *server* ini tidak berbeda dengan pesan yang sama yang dikirimkan oleh *client*. Pesan *Finished* dari *server* sekaligus menutup negosiasi *client-server*.

Langkah-langkah di atas memisahkan enkripsi dari proses otentikasi. Proses otentikasi dibantu oleh sertifikat digital. Kegunaan kunci publik yang tercantum dalam sertifikat itu sendiri hanyalah untuk mengenkripsi kunci saluran komunikasi yang sebenarnya, bukan untuk mengenkripsi data sepanjang komunikasi terjadi. Pemisahan seperti ini memang diperlukan karena sebagian besar algoritma kunci publik dirancang untuk memberikan tanda tangan, bukan untuk proses enkripsi (lihat bagian 3.1 – kelemahan sistem kriptografi kunci publik).

Kemudian, proses otentikasi yang terjadi sendiri baru dari segi *server*. SSL juga menyediakan mekanisme untuk melakukan otentikasi *client*. Prosesnya hampir sama, dapat dilihat pada **Gambar 9 Langkah-langkah operasi protokol SSL yang melibatkan otentikasi *client***Langkah atau pesan yang berbeda adalah pesan *CertificateRequest* oleh server dan

Certificate serta *CertificateVerify* oleh *client*.



Gambar 9 Langkah-langkah operasi protokol SSL yang melibatkan otentikasi *client*

Pesan *CertificateRequest* dikirimkan oleh *server* jika merasa otentikasi *client* dibutuhkan. Yang perlu menjadi perhatian adalah spesifikasi SSL mengharuskan permintaan otentikasi *client* dikirimkan setelah *server* menunjukkan identitasnya terlebih dahulu (melalu pesan *Certificate* dan *ServerKeyExchange*). Pesan *CertificateRequest* berisi daftar tipe sertifikat dan daftar nama *Certificate Authorities* yang diterima oleh *server*. Pesan ini akan direspon oleh *client* dengan mengirimkan pesan *Certificate* yang identik dengan pesan *Certificate* yang dikirimkan oleh *server*.

Mengirimkan kunci publiknya pada pesan *Certificate* tidaklah cukup untuk membuktikan identitas *client*. *Client* harus terbukti memiliki kunci privat yang benar. Oleh karena itu, pesan *CertificateVerify* dikirimkan. Isi pesan ini adalah informasi kunci yang terdapat dalam pesan *ClientKeyExchange* dan pesan-pesan SSL sebelumnya. Pesan ini ditandatangani menggunakan kunci privat *client* sehingga pihak *server* dapat melakukan verifikasi menggunakan kunci publik yang diterima sebelumnya.

5. *Secure Electronic Transaction* (SET)

Pada tahun 1996, Visa dan MasterCard membangun protocol SET. Protokol ini dirancang untuk menyediakan transaksi elektronik yang dapat dipercaya. Keamanan diberikan pada seluruh pihak yang terlibat dalam transaksi elektronik. SET merupakan sebuah *open standard*, yang saat ini ditangani oleh SETCo LLC [6].

Empat komponen SET

SET merupakan protokol yang melibatkan banyak pihak. Ada empat komponen yang terlibat di dalam SET, yaitu:

a. pembeli yang merupakan pemegang kartu kredit
b. penjual
c. *Certificate Authority* (CA)
   Pihak yang berwenang untuk mengeluarkan sertifikat digital (lihat bagian 3.3).
d. *Payment Gateways*
   Pihak yang bertugasi memproses kartu pembayaran (dalam hal ini kartu kredit) dan pembayaran transaksi. Biasanya *Payment Gateways* dijalankan oleh pihak yang mengeluarkan kartu kredit atau biasa disebut ***issuer***, yakni bank.

Untuk komunikasi yang terjadi antar komponen, SET menyediakan perangkat lunak khusus untuk masing-masing komponen.

5.1. SET Business Plan

Pihak issuer yang sebagai perancang SET menetapkan tujuh kebutuhan bisnis yang harus dipenuhi SET sebagai protokol transaksi elektronik. Kebutuhan tersebut tertuang dalam *SET business plan* yang menyatakan bahwa SET seharusnya:

a. Memungkinkan kerahasiaan informasi pembayaran dan informasi transaksi.
b. Menjamin integritas semua data yang terkirim
c. Menyediakan otentikasi terhadap pembeli sebagai pemegang kartu kredit untuk akun kartu pembayaran yang sah
d. Menyediakan otentikasi terhadap penjual yang mampu melayani transaksi elektronik melalui hubungannya dengan sebuah institusi keuangan yang terkait
e. Menjamin penggunaan layanan keamanan dan rancangan sistem terbaik untuk melindungi seluruh pihak yang terlibat transaksi
f. Menghindari ketergantungan terhadap mekanisme keamanan lain dan mencegah penggunaan mekanisme lain tersebut
g. Memfasilitasi dan mendukung pengugunaan perangkat lunak dan penyedia jaringan yang bervariasi.

Untuk memenuhi tujuh kriteria tersebut, SET memiliki langkah-langkah operasi yang akan dibahas pada bagian selanjutnya.

5.2. Langkah-langkah Operasi SET

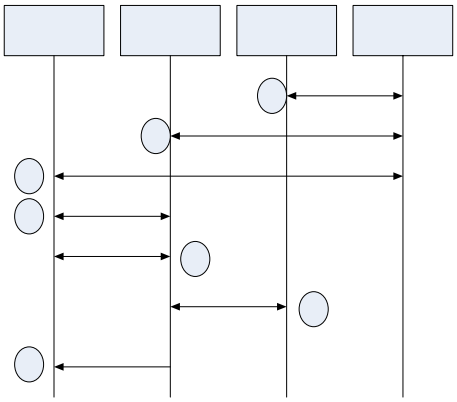
5.2.1. Mendapatkan sertifikat digital

SET menginginkan otentikasi yang jelas terhadap semua pihak yang berpartisipasi dalam transaksi elektronik. Karena itu, seperti yang terlihat pada Gambar 10 Langkah-langkah operasi SET, langkah 1 sampai 3, pihak pembeli, penjual, dan Payment Gateway berhubungan dengan CA untuk mengajukan permohonan sertifikat.

Pesan awal dikirimkan oleh pembeli melalui paket perangkat lunak yang khusus dikeluarkan oleh SET. Pesan ***CInitReq*** menandakan apa yang pembeli inginkan, melakukan registrasi sertifikat digital, atau jika pembeli telah memiliki sertifikat, mendapatkan sertifikat tersebut.

Pihak CA akan merespon dengan memberikan pesan ***CInitRes*** yang berisi form pendaftaran atau sertifikat digital milik pembeli dan CRL, sehingga pembeli mengetahui jika sertifikatnya sudah kadaluwarsa.

Proses yang dialami oleh penjual dan *Payment Gateway* tidak berbeda dengan proses mendapatkan sertifikat digital untuk pembeli.



Gambar 10 Langkah-langkah operasi SET

5.2.2. Melakukan transaksi pembelian

Setelah pembeli menetapkan hati dan memilih produk yang akan dibeli, proses transaksi pembelian pun dimulai. Pada saat pembeli menekan tombol beli, pada saat itu juga perangkat lunak di pihak pembeli, yang biasa dipanggil (*wallet*) mengirimkan pesan ***PInitReq*** kepada penjual. Pesan ini memberitahukan kepada penjual akan terjadi transaksi pembelian. Penjual merespon melalui pesan PInitRes yang berisi sertifikat yang berisi kunci public penjual dan *Payment Gateways* (langkah 4).

Berikutnya, pihak pembeli memasukkan instruksi pembayaran (*payment instruction/PI*) dan informasi pembelian (*order information/OI*). informasi pembelian berisi keterangan mengenai produk yang dibeli. Sedangkan instruksi pembayaran berisi informasi keuangan seperti data kartu kredit dan total harga yang harus dibayar. Informasi pembayaran dienkripsi menggunakan **kunci publik *Payment Gateway*** dan informasi pembelian dienkripsi

dengan **kunci publik penjual**. Dengan cara ini, semua pihak hanya mendapatkan informasi yang mereka butuhkan saja. Kedua informasi tersebut dikirim dalam satu pesan ***PReq.***

Bagian yang cukup rumit adalah pemakaian *dual digital signature* untuk pesan ini. Setelah informasi pembayaran dan informasi pembelian masing-masing di-*hash* oleh pembeli dan dijadikan satu. Hasil *hash* gabungan itu kemudian di-hash sekali lagi. Hasilnya menjadi *dual signature* khas SET. *Dual signature* digunakan untuk menunjukkan ada dua *item* dalam satu pesan tersebut sehingga tidak ada informasi yang dapat hilang di tengah perjalanan.

Setelah mendapatkan pesan *Preq*, penjual dapat mendekripsi informasi pembelian dan mengekstrak informasi pembayaran. Tanda tangan yang diberikan sekaligus menjadi bukti keabsahan pembeli. Transaksi hanya dilanjutkan bila verifikasi sertifikat pembeli berhasil. Jika transaksi berlanjut, penjual akan mengirimkan ***PRes*** yang berisi kode mengenai langkah-langkah yang dilakukan penjual sebelum meresponi transaksi lebih lanjut.

Pihak penjual mempunyai hak untuk menunda transaksi. Apabila ini terjadi, pembeli dapat mencoba untuk melanjutkan transaksi dengan mengirimkan ***InqReq*** yang berisi identitas transaksi yang tertunda. Pesan ***InqRes*** akan dikirimkan jika penjual hendak melanjutkan transaksi kembali (langkah 5). Pesan *InqReq* mungkin saja dikirimkan berulang kali sebelum penjual memberikan respon.

5.2.2. Pengesahan transaksi

Untuk mengesahkan transaksi, penjual mengirim ***AuthReq*** kepada *Payment Gateway*. Pesan ini berisi informasi pembelian yang telah di-*hash* oleh penjual dan pesan *PReq* yang dikirimkan oleh pembeli. *Payment Gateway* dapat mendekripsikan informasi pembayaran dan membandingkan nilai *hash* informasi pembelian dan nilai *hash* yang dikirimkan penjual. Apabila terjadi kecocokan, *Payment Gateway* yakin jika pembeli dan penjual telah sepakat mengenai pembelian yang dilakukan.

Tugas *Payment Gateway* yang lain adalah melakukan pengesahan transaksi sesuai dengan kebijakan yang dimiliki oleh *issuer* kartu kredit.

Jika segalanya sudah beres, *Payment Gateway* memberikan pesan ***AuthRes*** untuk penjual (langkah 6). Setelah mendapat izin tersebut, penjual melakukan langkah terakhir untuk menutup pembelian yang telah dilakukan.

6. Perbandingan SSL dan SET

6.1. Implementasi SSL untuk transaksi elektronik

Dapat dikatakan SSL merupakan protokol kriptografi yang paling dominan untuk pembangunan *e-commerce*. Saat ide e-commerce mencuat, SSL terlebih dahulu ada. SSL memang lahir hampir bersamaan dengan keluarnya *browser* pertama (*NSCA Mosaic*). Hanya selang delapan bulan setelah *NSCA Mosaic* keluar, *Netscape Communication* menyelesaikan rancangan SSL versi 1.0. Tidak lama setelah itu, tepatnya lima bulan kemudian, *Netscape* mengeluarkan *browser* mereka, *Netscape Navigator*, yang didukung oleh SSL versi 2.0. Hal tersebut menunjukkan bahwa komunikasi merupakan aspek penting dalam internet dan keamanannya tidak dapat dilepaskan begitu saja.

Pemakaian yang mudah

Begitu e-commerce muncul, komunikasi juga tidak lepas, bahkan semakin penting karena informasi yang ditukarkan menjadi makin vital. Karena pengamanan terhadap komunikasi telah tersedia dan dapat langsung digunakan, SSL sangat membantu. Hal itu menjelaskan dominasi SSL sebagai protokol kriptografi untuk transaksi elektronik.

Pemakaian SSL untuk transaksi elektronik dapat dikatakan lebih kepada pembajakan teknologi yang sudah ada dari pada pendekatan sistematis kepada transaksi elektronik yang aman [13]. Pemakaiannya pun tidak berbeda dengan langkah operasi SSL seperti biasa. Ada keuntungan yang diraih dari segi ini, yaitu tidak ada tambahan apa pun yang disediakan oleh pembeli

(pemegang kartu kredit) dan penjual. Penjual cukup mengaktifkan layanan SSL pada *web server*-nya.

Otentikasi *client*
Sayangnya, penggunaan SSL bukan cara yang ampuh untuk mengamankan transaksi elektronik. Kekurangan SSL dalam hal ini dikarenakan dua hal. Pertama, kebutuhan yang vital dalam sebuah transaksi elektronik yaitu otentikasi pengguna, khususnya pembeli. Otentikasi pembeli dalam transaksi elektronik menuntut jaminan kalau nomor kartu kredit yang diberikan dalam transaksi benar-benar dimiliki oleh si pembeli. Sebaliknya, tidak tersedianya fasilitas untuk memenuhi kebutuhan tersebut disebabkan protokol SSL sendiri tidak merasa memerlukannya.

Seperti yang dibahas pada bagian 4.2, SSL memang menyediakan mekanisme otentikasi *client*, yang dalam kasus transaksi elektronik berarti si pembeli. Penjual, yang menyediakan *server*, bisa saja menuntut otentikasi *client* pada setiap komunikasi yang dibangun di atas SSL. Client diharuskan memberikan sertifikat digital. Namun, bila ditilik lebih lanjut, yang menjadi client dalam komunikasi SSL adalah *web browser*.

Dampak dari kenyataan tersebut adalah, sertifikat digital dari client terikat dengan perangkat lunak, yakni *web browser*. Dalam sebuah transaksi elektronik, pihak yang ingin dibuktikan keabsahannya adalah orangnya, pembelinya, bukan perangkat lunaknya.

Dari segi SSL sendiri, otentikasi client jarang digunakan. Mengingat bahwa tujuan awal protokol ini bukan sebagai protokol pembayaran elektronik, otentikasi tidak ditujukan pada manusianya secara langsung.

Bukan protokol khusus transaksi elektronik
Ada dampak lain penggunaan protokol komunikasi umum untuk transaksi elektronik. Yang menjadi perhatian dalam protokol SSL adalah menyediakan saluran komunikasi yang aman. Protokol ini tidak mengatur apa yang terjadi selanjutnya dengan data pembayaran yang diberikan. Masalah yang dapat timbul dari hal ini adalah pihak penjual dapat menggunakan data kartu kredit pembeli sewenang-wenang, misalnya dengan mempublikasikannya.

Terakhir, minimnya jumlah pihak yang terlibat dalam komunikasi SSL mungkin tidak membawa kerumitan. Tetapi, transaksi elektronik sebagian besar menggunakan kartu kredit. Kehadiran kartu kredit melambangkan ada pihak lain yang berperan di dalamnya, bank. Dengan SSL, bank sebagai pihak yang mengeluarkan kartu kredit, tidak mengetahui apa pun. SSL hanya melibatkan pembeli dan penjual. Dengan demikian, transaksi elektronik yang terjadi seolah-olah dibatasi oleh karakteristik awal protokol.

6.2. Implementasi SET untuk transaksi elektronik

Sebagai protokol yang dirancang khusus, implementasi SET untuk transaksi elektronik dilakukan sesuai dengan langkah-langkah operasi yang ada di dalamnya. SET memenuhi kebutuhan transaksi elektronik yang kurang dapat dipenuhi oleh protokol SSL, seperti otentikasi pembeli.

Tiap langkah operasi SET dirancang untuk memenuhi tujuh kriteria yang dicetuskan dalam *SET Business Plan* untuk menciptakan transaksi elektronik yang aman. Misalnya dengan langkah operasi SET dalam melakukan transaksi pembelian, data keuangan yang merupakan data yang penting tidak akan sampai kepada tangan yang tidak berwenang.

Untuk menjawab keabsahan pengirim pesan dalam tiap langkah transaksi elektronik, SET mengharuskan tiap partisipan memiliki sertifikat digital yang valid. Poin ini memiliki nilai tambah untuk SET karena tingkat rasa keamanan tentu meningkat.

Di balik semua keuntungan tersebut, SET yang melibatkan banyak pihak tentu mendatangkan kerumitan dalam implementasinya. Keterlibatan banyak pihak memerlukan kerja sama yang baik. Belum lagi setiap pihak harus bersedia memiliki sertifikat digital yang valid.

Begitu juga dengan perangkat lunak khusus yang perlu dipasang untuk kepentingan komunikasi antar partisipan. *Maintanance* perangkat lunak akan menjadi masalah tersendiri. Kerepotan yang ditimbulkan oleh SET menyebabkan kurang populernya protokol ini untuk transaksi elektronik, selain faktor usianya yang lebih mudah dibandingkan SSL.

Perbandingan yang lebih lengkap antara protokol SET dan SSL disajikan dalam tabel pada **Lampiran**.

7. Kesimpulan

Tidak dapat dipungkiri *e-commerce* semakin berkembang. Tingkat nilai mata uang yang terlibat dalam jenis bisnis ini semakin meninggi. Keterkaitannya dengan nilai keuangan, seperti layaknya transaksi bisnis lain, menyebabkan aspek yang ada di dalamnya patut diperhatikan.

Hal lain yang perlu menjadi perhatian adalah perbedaan transaksi yang terjadi dalam e-commerce dengan transaksi biasa. Transaksi dalam e-commerce disebut transaksi elektronik. Pembayarannya pun dilakukan secara elektronik. Meskipun tetap menggunakan kartu kredit, keberadaan fisik kartunya sendiri tidak ada. Yang diambil dari kartu kredit tersebut hanyalah data yang kemudian dipertukarkan dengan pihak yang berkepentingan.

Kriptografi masuk karena pertukaran data tersebut amat penting untuk diamankan. Berbagai penerapan ilmu kriptografi diimplementasikan, termasuk penerapan protokol kriptografi. Protokol yang paling dominan untuk transaksi elektronik adalah SSL dan SET.

Kedua protokol memiliki kelebihan dan kekurangannya masing-masing. Keunggulan SSL terletak pada kemudahan penggunaannya, sedangkan SET pada layanan keamanan yang lebih memuaskan. Kekurangan yang dimiliki keduanya berada pada sektor yang berbeda, namun tidak menjadikan keduanya tidak dapat dipakai sebagai protokol dalam transaksi elektronik.

Secara keseluruhan, kedua protokol ini, SSL dan SET, masih layak menjadi protokol kriptografi untuk transaksi elektronik.

DAFTAR PUSTAKA

[1] Madhu Gayathri. *Secure Electronic Transaction (SET)*

[2] Rinaldi Munir. 2004. *Bahan Kuliah IF5054 Kriptografi*. Departemen Teknik Informatika, Institut Teknologi Bandung

[3] Onno W Purbo dan Aang Arif Wahyudi. 2001. Mengenal eCommerce. PT Elex Media Computindo, Jakarta

[4] A. Koponen. *E-commerce, Electronic Payments*. Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory.
http://www.tml.tkk.fi/Opinnot/T-09.7510/2006/reports/E-commerce.pdf
(diakses tanggal 19 Desember 2006)

[5] Maurizio Dècina. 2001 *Internet Security & E-commerce*. Politecnico di Milano/CEFRIEL**.**
http://www.forumti.it/fti/downloads/internet%20security%20e-commerce.pdf
(diakses tanggal 19 Desember 2006)

[6] Richard Jewson. 2001. *E-payments: Credit Cards on the Internet*. Aconite.
http://cnscenter.future.co.kr/resource/security/ecommerce/Epayments_Whitepaper.pdf
(diakses tanggal 19 Desember 2006)

[7] Rasika Amarasiri and Gihan Dias. *Techniques For Secure Electronic Transactions*.
http://www.bsys.monash.edu.au/people/ramarasiri/Techniques%20for%20Secure%20Electronic%20Transactions.pdf
(diakses tanggal 19 Desember 2006)

[8] Report Dr. Cetin Kaya Koc Juthamas Pongnukit Witit Tingthanathikul. *Analysis of E-commerce Security ECE*. Oregon State University.
http://islab.oregonstate.edu/koc/ece4

78/05Report/Pong-Ting.pdf
(diakses tanggal 19 Desember 2006)

[9] Mustafa A. Ally. 2001. *The Integration of SET in Australian Based Internet Payment System Products: A System Developer's Perspective*. University of Southern Queensland, Faculty of Business and Commerce Department of Information Systems

[10] Michael Fritscher, Oliver Kump. *Security And Productivity Improvements – Sufficient For The Success Of Secure Electronic Transaction?* Department of Information Systems Vienna University of Economics and Business Administration
http://nm.wu-wien.ac.at/research/publications/FrKu.pdf
(diakses tanggal 19 Desember 2006)

[11] David Baum, "Business Links," *Oracle Magazine*, No. 3, Vol. XIII, May/June, 1999, pp. 36-44

[12] Budi Rahardjo. 1999. *Mengimplementasikan Electronic Commerce di Indonesia*. PPAU Mikroelektronika – ITB

[13] Shane Balfe and Kenneth G. Paterson. 2006. *Augmenting Internet-based Card Not Present Transactions with Trusted Computing: An Analysis*. Royal Holloway, University of London

[14] Laurence H. Loeb. 1998. *Secure Electronic Transaction: introduction and technical reference*. Artech House..

[15] Stephen A. Thomas. 2000. *SSL and TLS Essentials*. Wiley Computer Publishing.

LAMPIRAN

Aspek yang dibandingkan	SSL	SET
Tipe protokol	Komunikasi	Transaksi elektronik
Partisipan	*web browser* (pembeli) dan *web server* (penjual)	Pembeli, penjual, CA, Payment Gateway
Otentikasi	Penjual	Semua partisipan
Kemudahan penggunaan	Cukup mudah, cukup dengan mengaktifkan layanan SSL.	Membutuhkan perangkat lunak khusus SET dan sertifikat untuk tiap partisipan
privasi	Kurang. Pihak penjual dapat mengetahui data kartu pembayaran pengguna	Bagus. Data hanya sampai pada pihak yang berkepentingan.
Efisiensi	bagus	Kurang karena terlalu banyak sentuhan kriptografi yang diberikan.
Maintance sistem	Mudah. Kemunculan versi baru dari SSL biasanya turut dimasukkan dalam versi baru dari *web browser*.	Sulit. Kemunculan versi baru dari perangkat lunak yang digunakan mengharuskan pembaharuan dilakukan di tiap komputer partisipan.

Tabel 1 Perbandingan SSL dan SET dalam transaksi elektronik