



KARAKTERISTIK DARI BEBERAPA SISTEM PERDAGANGAN DI INTERNET

Objektif :

- Mengenal dan memahami berbagai jenis sistem perdagangan di internet
 - Mampu melakukan transaksi pada berbagai jenis sistem perdagangan di internet
-

Pada bab ini dibahas karakteristik dari beberapa Sistem perdagangan di Internet (SPI). Maksud dari pembahasan yang dilakukan ialah agar didapatkan informasi dan gambaran yang lebih jelas dari sistem-sistem perdagangan yang saat ini ada di Internet.

Walaupun tidak semua dari sistem perdagangan yang ada di Internet saat ini dapat dibahas, tapi diharapkan beberapa contoh SPI yang dibahas dapat mewakili Sistem transaksi perdagangan di Internet yang ada saat ini.

Beberapa contoh Sistem Perdagangan di Internet yang akan dibahas di bab ini meliputi : toko elektronik di situs web dengan forms html; kupon elektronik sederhana; cybercash; netchex; dan visa/mastercard Secure Electronic Transaction (Set).

4.1 TOKO ELEKTRONIK DI SITUS WEB DENGAN FORMS HTML

Saat ini toko elektronik di situs web semacam ini merupakan salah satu Sistem Perdagangan di Internet yang paling banyak dijumpai. Toko elektronik semacam ini menggunakan tag `<forms..>` pada HTML dan pemrograman di sisi Server (CGI, ASP, dan sejenisnya). Modifikasi terakhir SPI ini memanfaatkan fasilitas sistem keamanan SSL (*Secure Socket Layer*), tetapi tidak mengubah alur transaksi.

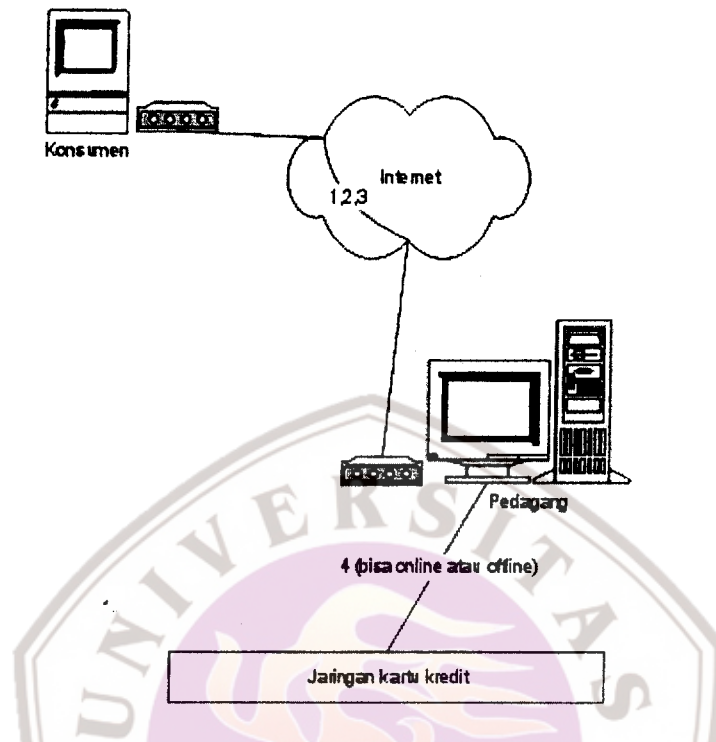
Perangkat Lunak

Cukup dengan program *browser* biasa tanpa kemampuan enkripsi, konsumen dapat berbelanja di toko elektronik ini. Pedagang juga tidak perlu menggunakan *web server* dengan fasilitas enkripsi untuk mengimplementasikan toko elektroniknya. Akan tetapi tentunya jika ingin menggunakan fasilitas keamanan SSL, baik *browser* konsumen maupun *web server* pedagang harus menunjang SSL pula.

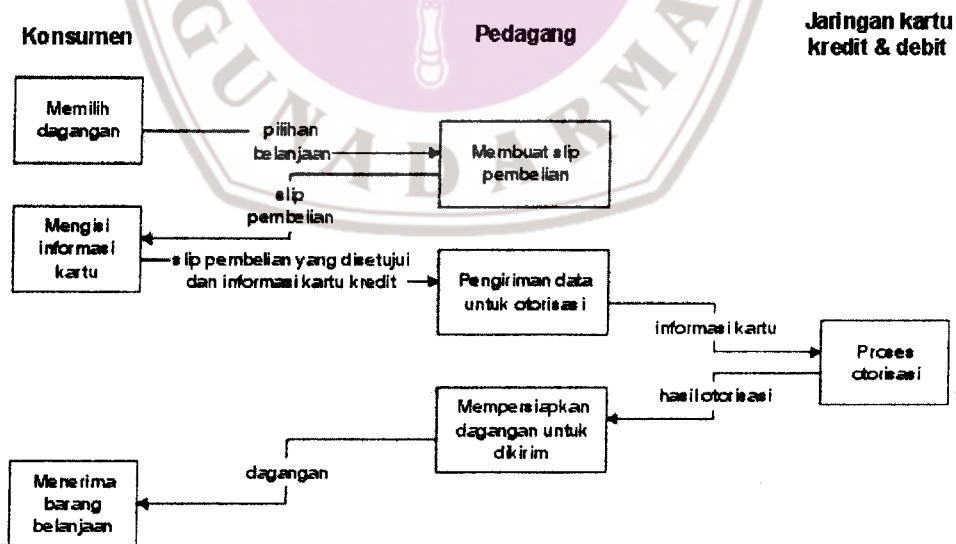
Alur Transaksi

1. Konsumen dengan menggunakan *browser* memilih barang yang akan dibelinya pada halaman Situs web pedagang.
2. Setelah harga ditotal, kemudian konsumen mengetikkan informasi kartu kreditnya pada *form* slip pembelian yang disediakan dalam toko elektronik (situs web si pedagang) itu.
3. Informasi kartu kredit itu dikirim ke *web server* pedagang bersama informasi pembelian lainnya sebagai parameter pada URL.

- Informasi kartu kredit beserta informasi pembelian di-parse (dibaca) dengan program CGI, untuk selanjutnya diproses sama seperti proses transaksi kartu kredit *mail order / telephone order (MOTO)*.



Gambar 4.1 Diagram topologi transaksi toko elektronik sederhana



Gambar 4.2 Diagram alur data transaksi toko elektronik sederhana

Klasifikasi

Skenario SPI ini tak berbedanya dengan *mail order / telephone order (MOTO)*, yang disebut dengan *card not present transaction*. Hal ini memang diperkenankan oleh sebagian besar lembaga pengelola kartu kredit. Konsumen akan ditagih seperti biasa. Sedangkan pedagang tentunya menagih ke *acquirer* seperti halnya transaksi MOTO. Penggunaan kartu kredit sebagai alat pembayaran langsung mengindikasikan bahwa ini bukan sistem pembayaran *peer-to-peer*.

Sistem sederhana ini umumnya hanya menerima kartu kredit, karena otorisasi nomor kartu kredit tidak perlu *on-line*, meskipun kini umumnya lebih banyak pedagang yang menggunakan sistem otorisasi *on-line*. Memang relatif sulit untuk membuat sendiri sebuah toko elektronik yang melakukan otorisasi *on-line* langsung ke lembaga pengelola kartu kredit, jika tidak membeli paket perangkat lunak yang sudah jadi. Jika tidak ada otorisasi *on-line*, sistem ini kurang cocok untuk menjual barang-barang yang bisa di-*download* segera lewat Internet, karena jika nomor kartu tersebut tidak lagi sah, maka pedagang akan dirugikan. Memang ada pemecahannya, yakni mengirim barang digital itu menggunakan surat elektronik, setelah nomor kartu itu diotorisasi. Jelas pada SPI ini, terlihat pihak mana yang menjadi pedagang dan konsumen. Transaksi ini derajat keanonimitasnya juga sangat rendah, karena pedagang dapat dengan mudah mengetahui informasi kartu kredit konsumen. Seperti halnya transaksi kartu kredit biasa, pada skenario ini keterlacakan transaksi juga tinggi.

Keamanan dan Serangan

Pada dasarnya, tidak ada fasilitas keamanan pada skenario transaksi SPI ini. Jika pedagang tidak menggunakan *web server* yang terjamin keamanannya (*secure*), maka seluruh kelemahan pada protokol TCP/IP dan HTTP, termasuk *web spoofing*, akan dimiliki pula oleh SPI yang sederhana ini. Penyerang dengan mudah bisa mendapatkan informasi kartu kredit.

Pada beberapa pedagang, terkadang toko elektronik mereka juga sudah menggunakan *web server* dari Netscape yang mendukung SLL. Dengan cara ini, informasi transaksi dan informasi kartu kredit menjadi lebih sulit untuk disadap. Patut diperhatikan disini, komunikasi yang aman hanya dari konsumen ke pedagang. Pedagang pada akhirnya tetap dapat membaca informasi kartu kredit milik konsumen.

Kepercayaan dan Penipuan

Karena pedagang mendapatkan seluruh informasi kartu kredit milik konsumen, maka konsumen harus percaya kepada pedagang bahwa nomor tersebut tidak akan dipergunakan dua kali. Selain itu, karena tidak ada jaminan keotentikan pedagang (apakah pedagang itu ada atau hanya toko yang dibuka oleh orang tak bertanggung jawab), maka konsumen menanggung resiko ditipu.

Di sisi lain, jika pedagang tidak melakukan otorisasi sebelum mengirimkan barang dagangannya kepada konsumen, maka pedagang menanggung resiko tertipu oleh konsumen. Karena itu dalam kasus seperti ini pedagang umumnya menjual barang-

barang yang harus dikirim lewat pos, agar ada kesempatan untuk melakukan otorisasi secara konvensional.

Prospek di masa depan

Meskipun banyak diimplementasikan oleh pedagang dengan mudah, namun meningkatnya kesadaran konsumen akan perlunya keamanan dalam transaksi perdagangan di Internet, maka mungkin membuat para pedagang beralih ke skenario lain yang lebih aman. Alternatif lain tampaknya penggunaan SSL untuk jaminan keamanan dalam bertransaksi menjadi suatu keharusan.

4.2 KUPON ELEKTRONIK SEDERHANA

Sistem Perdagangan Internet yang kedua ialah dengan menggunakan Kupon Elektronik..Kupon itu sebenarnya hanya sederet 'janji' (*promise*) yang ditandatangani pedagang dan harus dilaksanakan oleh pedagang. Dalam skenario SPI ini, sebenarnya secara hukum pedagang mengedarkan semacam 'uang elektronik' yang nilainya dijamin oleh sang pedagang itu sendiri

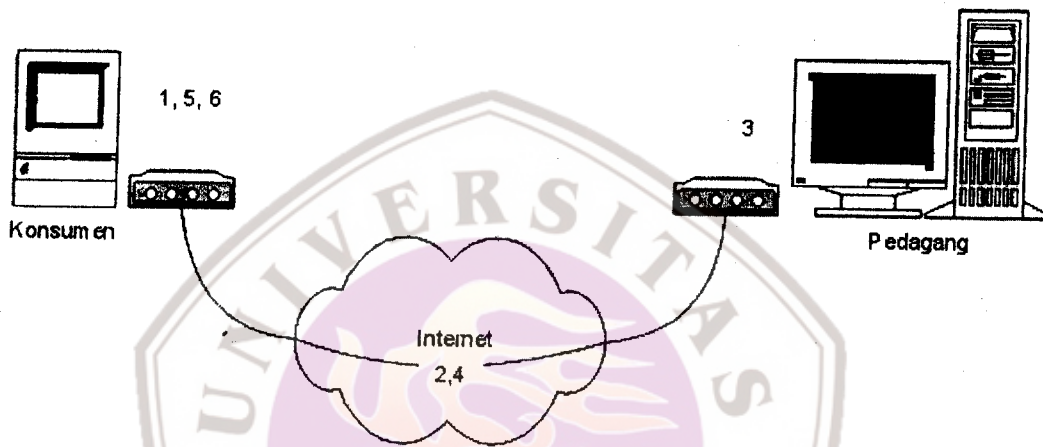
Perangkat Lunak

Pedagang dapat 'mencetak' kupon ini dengan menggunakan aplikasi surat elektronik seperti PGP atau PEM. Untuk memeriksa keabsahan kupon, konsumen perlu memiliki perangkat lunak yang memiliki fasilitas pengecekan keabsahan, (tergantung apakah itu PGP atau PEM). Konsumen dapat mengirimkan kembali kupon itu dengan surat elektronik atau program *browser* biasa. Jika dikirim dengan *browser*, maka tentunya pedagang harus menggunakan suatu program di sisi server (CGI,ASP,dsbnya) untuk mem-*parse* kupon dari parameter URL.

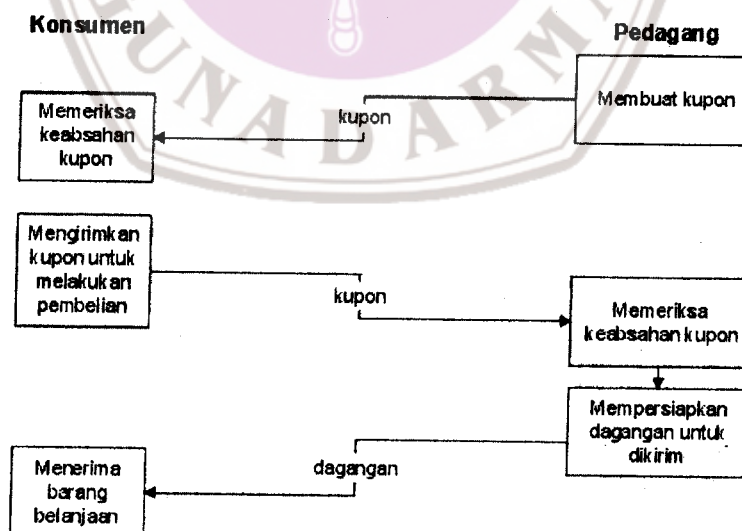
Alur Transaksi

1. Pertama-tama, pedagang harus 'mencetak' kupon dan menandatangani dengan kunci privat miliknya terlebih dahulu. Jika menggunakan sertifikat, maka sertifikat itu ikut disatukan bersama kupon yang sudah ditandatangani tadi.
2. Kupon tersebut kemudian diedarkan. Ada banyak cara mengedarkannya. Mungkin dapat dikirim langsung kepada orang yang memang sudah menjadi anggota suatu perkumpulan tertentu - katakanlah sebagai hadiah ulang tahun. Atau bisa saja konsumen itu telah membayar dimuka kepada pedagang (tidak peduli dengan cara apa dia membayar), kemudian pedagang memberikan kepada konsumen itu setumpuk kupon yang dapat dipergunakan sewaktu-waktu.
3. Konsumen perlu memeriksa keabsahan kupon dengan menggunakan kunci publik pedagang sebelum dipergunakan. Jika menggunakan sertifikat digital, konsumen juga menelusuri sertifikat yang diberikan untuk memastikan keabsahannya.
4. Jika sudah saatnya kupon dipergunakan, konsumen mengembalikan kupon itu kepada pedagang. Hal ini bisa dilakukan dengan menggunakan surat elektronik atau *browser*. Pada *browser* yang akan mengirimkannya sebagai parameter pada URL, konsumen menyisipkan kupon yang dimilikinya melalui *form* yang disediakan toko elektronik pedagang. Bersama kupon yang dikirimkan kembali itu,

- dapat saja disertakan alamat dimana pedagang dapat mengirimkan 'dagangannya'.
5. Pedagang yang menerima kupon itu, kemudian memeriksa kembali keabsahannya dengan membuat sidik jari dari isi kupon itu, lalu membandingkannya sidik jari hasil dekripsi tanda tangan yang ada pada kupon. Hal ini dilakukan untuk mencegah kemungkinan pihak konsumen mengubah isi perjanjian. Pedagang juga memeriksa nomor seri dari kupon itu, untuk mencegah pembelanjaan ganda (*double spending*).
 6. Setelah diperiksa keabsahannya, pedagang berkewajiban menjalankan apa yang telah tertera dalam perjanjian.



Gambar 4.3 Diagram topologi transaksi kupon elektronik



Gambar 4.4 Diagram alur data transaksi kupon elektronik

Klasifikasi

Skenario SPI ini dapat tergolong pada transaksi *pre-paid* (dibayar dimuka), karena konsumen harus memiliki dulu 'kupon'. Kupon elektronik ini cocok untuk penjualan komoditas yang dapat ditransfer secara digital, begitu selesai melakukan otentikasi kupon – jika terbukti masih absah – pedagang langsung dapat mengirimkan dagangannya. Pedagang tidak perlu otorisasi dahulu kepada pihak ketiga seperti pada transaksi kartu kredit atau kartu debit, karena kupon itu dikeluarkan dan dijamin sendiri oleh pedagang yang bersangkutan. Pencatatan identitas konsumen yang diberi kupon akan membuat transaksi pada skenario ini terlacak dengan mudah.

Keamanan dan Serangan

Penggunaan enkripsi asimetris memang membuat skenario transaksi ini cukup aman, namun bukan berarti tidak ada celah. Pada PGP, pengiriman kunci publik pedagang kepada konsumen masih dapat diserang dengan teknik *man-in-the-middle*. Jadi ada baiknya jika konsumen benar-benar merasa yakin dahulu bahwa kunci publik pedagang benar-benar otentik. Setelah menerima kupon pun, konsumen harus menjaganya baik-baik, baik mengenkripsi ulang kupon tersebut dengan *password* atau disimpan dalam perangkat keras yang bisa dikunci.

Pencatatan dan pemberian nomor seri pada kupon dapat mencegah pembelanjaan ganda. Mungkin terpikir bahwa kupon elektronik itu dapat dipergunakan sebagai alat tukar antarkonsumen secara *off-line*. Sebenarnya memang bisa, namun karena pihak konsumen pemberi kupon masih dapat menyimpan kopi dari kupon yang diberikan, maka dikhawatirkan pihak pemberi kupon membelanjakan kopi kupon yang telah diberikan. Karena itu tidaklah tepat jika kupon-kupon itu dipertukarkan antarkonsumen.

Jika pembuatan kupon ditujukan hanya untuk salah seorang konsumen saja, maka pedagang dapat mencantumkan identitas sang konsumen sebagai pengguna yang sah dalam kupon elektronik yang dibuatnya. Hal ini akan membuat pemakaian kupon terlacak. Pedagang dapat menolak kupon yang akan digunakan oleh konsumen yang identitasnya tidak sesuai dengan apa yang ada di kupon, dengan dugaan bahwa kupon itu telah dicuri.

Kepercayaan dan Penipuan

Nilai dari kupon sangat tergantung dari kepercayaan konsumen kepada pedagang, karena pedaganglah yang menjamin nilai kupon elektronik itu. Jadi kasusnya mirip sekali dengan uang yang diedarkan oleh bank sentral. Rakyat mempercayai uang yang diedarkan bank sentral karena dengan uang Rp.500,- misalnya, sebotol minuman bisa dibeli. Demikian pula dengan kasus kupon elektronik ini. Sebuah kupon harus bernilai sesuatu, tidak harus dalam nilai mata uang, namun bisa saja dengan ukuran point yang ditetapkan sendiri oleh pedagang. Dengan kupon bernilai 5 point misalnya, konsumen berhak men-*download* program permainan terbaru dari pedagang.

Konsumen harus benar-benar percaya terhadap catatan pedagang atas kupon-kupon yang telah dipergunakan, dan saat penyerahan kupon kembali, pedagang tidak

berbohong bahwa terjadi *double spending*. Pedagang harus jujur kepada konsumen bahwa kupon tersebut sudah pernah dipergunakan atau belum.

Konsumen juga harus percaya bahwa pedagang adalah pihak yang jujur, karena tidak ada lembaga yang mengawasi pedagang yang berkewajiban menyerahkan dagangan jika sudah saatnya. Namun jika menggunakan sertifikat, masih mungkin ada lembaga dilapisan atas yang berani menjamin kejujuran pedagang.

Pencatatan

Tanpa perangkat lunak khusus, pencatatan hanya dilakukan di *web server* pedagang saja. Yang dicatat *web server* pastilah nomor seri yang sudah dikeluarkan dan yang sudah 'dilaksanakan', namun dapat pula ditambah dengan data tambahan mengenai transaksi pembelian yang diberikan konsumen saat pengembalian kupon.

Penerimaan Pembayaran dan Biaya Transaksi

Kupon itu dapat diberikan secara gratis kepada konsumen sebagai bonus, atau juga bisa dijual kepada konsumen. Masalah penjualan kupon itu berada di luar cakupan masalah kupon elektronik. Jadi sebenarnya saat kupon itu berada di tangan konsumen, pedagang sudah menerima 'pembayaran', dan saat menerima kembali kupon itu pedagang harus menjalankan kewajibannya sesuai yang tertera dalam kupon. Boleh dikatakan pula bahwa tidak ada biaya transaksi, karena tidak ada pihak ketiga yang menjadi perantara.

Prospek di masa depan

Proses pencetakan kupon ini memang relatif canggih dari sisi keamanan namun cukup sederhana untuk diimplementasikan pedagang. Sistem ini memiliki kelemahan dimana konsumen memerlukan beberapa langkah yang relatif rumit untuk dapat memanfaatkan kupon elektronik itu jika tidak disediakan perangkat lunak khusus untuk kupon itu. Meskipun proses enkripsi yang dilakukan lebih menjamin kerahasiaan, namun proses tersebut menambah lagi beban yang harus dilakukan oleh konsumen, terutama saat pengembalian kupon.

4.3 CYBERCASH

CyberCash adalah sebuah perusahaan di Internet yang menyediakan jasa pembayaran transaksi yang aman bagi para pedagang dan konsumen. CyberCash tidak menyediakan satu macam pembayaran saja, namun dua macam cara pembayaran, yakni dengan menggunakan kartu kredit dan CyberCoin. Sudah ada beberapa perusahaan yang mendukung skenario transaksi CyberCash, misalnya CompuServe, CheckFree dan beberapa bank pendukung.

Salah satu tujuan awal SPI ini adalah bagaimana konsumen dapat menggunakan kartu kredit milik mereka untuk pembelian barang-barang yang berharga murah (*micropayments*) di Internet. Kartu kredit biasa tidak mungkin digunakan untuk transaksi yang nilainya kurang dari nilai (harga) minimum pembelian. Ini cukup

penting, karena banyak barang-barang 'murah' yang ditawarkan di Internet seperti aneka macam foto, berita, jurnal, artikel, hasil riset, lagu dan sebagainya. Selain itu, juga memudahkan pembayaran *pay-per-view*, misalnya untuk *video-on-demand*.

Perangkat Lunak

CyberCash menggunakan sebuah perangkat lunak yang harus di-*download* (disebut *wallet*, yang dalam bahasa Indonesia berarti dompet) ke dalam *hard disk* konsumen terlebih dahulu. *Wallet* tersebut nanti akan dijalankan oleh *browser* saat konsumen melakukan transaksi. *Wallet* tersebut dapat di-*download* tidak saja dari CyberCash, namun juga dari CompuServe, CheckFree dan beberapa situs lainnya. Meskipun ada sedikit perbedaan, namun semuanya kompatibel dengan skenario transaksi CyberCash.



Gambar 4.5 Tampilan menu utama wallet dari CyberCash

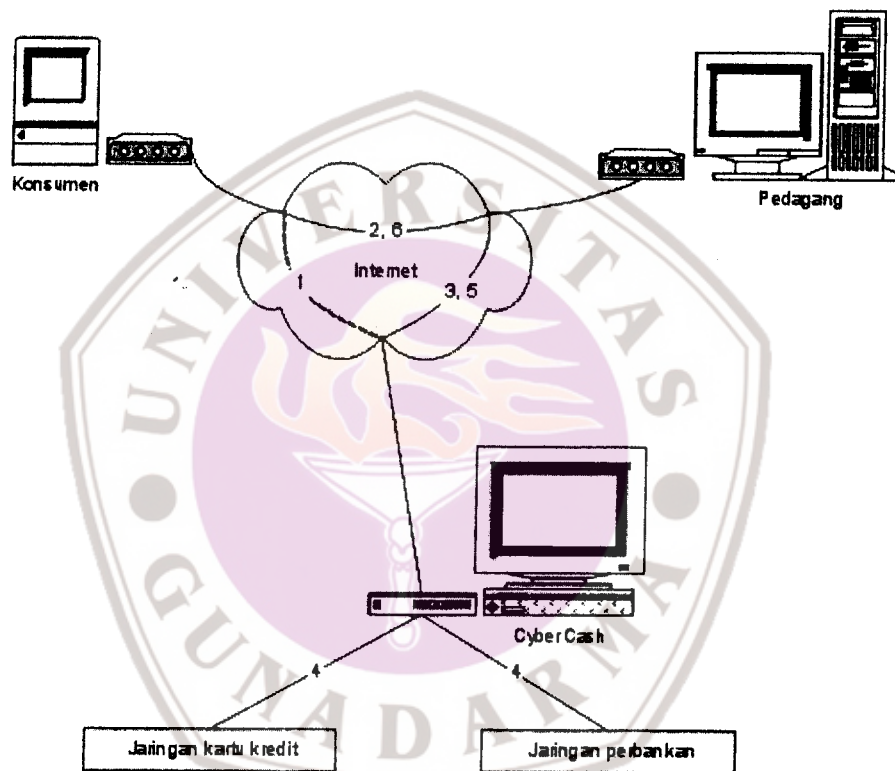
Seperti dalam kenyataan sehari-hari, sebelum melakukan transaksi, konsumen harus mengisi dompet dengan alat pembayaran, baik itu dengan *kartu kredit* atau *uang*. Demikian pula dengan *wallet*. *Wallet* itu harus diisi kartu kredit dulu. Dalam skenario CyberCash, informasi kartu kredit dipertalikan secara elektronik dengan *wallet*.

Selain itu konsumen juga dapat mengisi *wallet*-nya dengan uang elektronik yang diedarkan oleh CyberCash dengan istilah CyberCoin. Konsumen dapat membeli sejumlah CyberCoin dengan menggunakan kartu kredit, atau dengan menggunakan rekening bank yang telah dimiliki sebelumnya pada sebuah bank yang ikut berpartisipasi dalam skenario transaksi CyberCash. Rekening bank dari konsumen tersebut harus dipertalikan dahulu dengan program *wallet* yang dipergunakan

konsumen yang bersangkutan, sehingga setiap kali konsumen menggunakan *wallet*, program *wallet* tadi sudah tahu rekening bank siapa yang dipergunakan. Sejumlah uang yang sama dengan CyberCoin yang dibeli, akan didebit dari rekening bank sang konsumen.

Pedagang dalam skenario SPI ini menggunakan perangkat lunak Secure Merchant Payment System (SMPS) yang disediakan oleh CyberCash. Perangkat lunak ini seolah-olah bertindak sebagai *point-of-sale* (POS) dari pedagang, yang menghubungkan antara konsumen dengan CyberCash. Pedagang, seperti halnya konsumen, juga harus mendaftarkan diri terlebih dahulu kepada CyberCash.

Alur transaksi

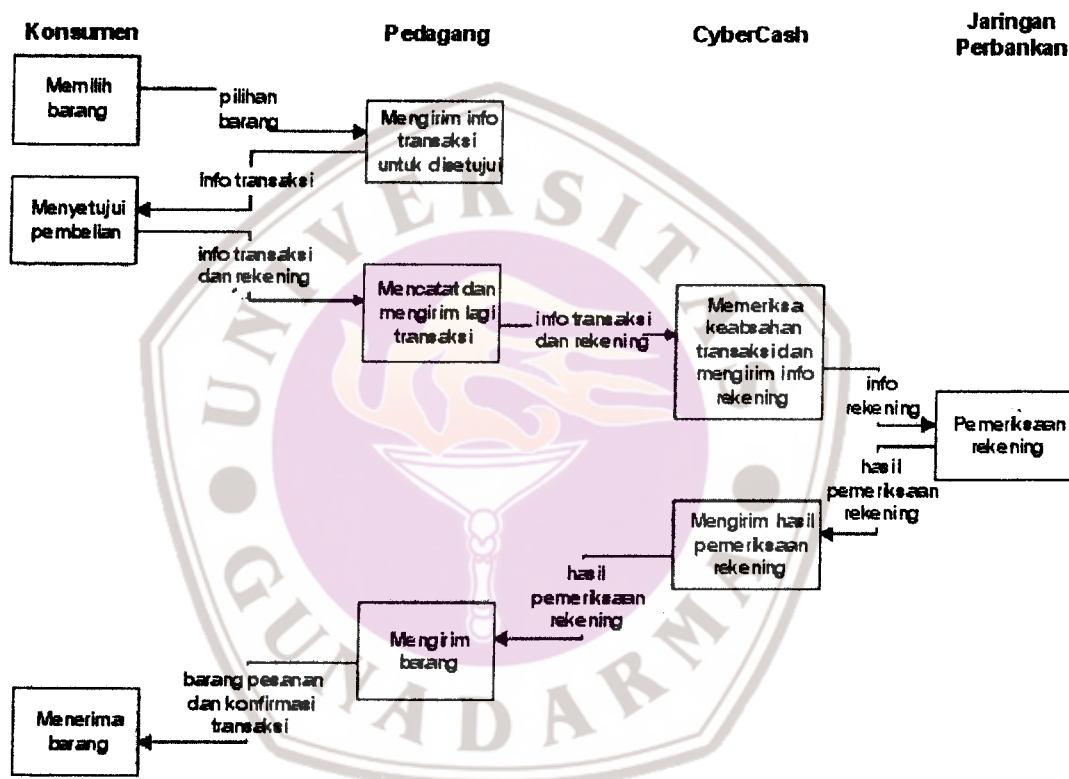


Gambar 4.6 Diagram topologi transaksi CyberCash

Alur transaksi dengan CyberCoin

1. Seperti sudah dijelaskan di atas, konsumen harus mengisi *wallet*-nya dengan CyberCoin terlebih dahulu. Tentunya hal ini dilakukan kalau konsumen sudah mendaftarkan diri ke CyberCash dan juga telah mempertalikan *wallet*-nya dengan kartu kredit atau rekening banknya.
2. Konsumen memilih barang yang akan dibelinya di *homepage* pedagang. Setelah dipilih, *web server* pedagang menginstruksikan agar *browser* konsumen menjalankan program *wallet*. Jika setuju dengan tawaran yang diajukan

- pedagang, konsumen menekan tombol pembayaran [Pay]. *Wallet* kemudian akan mengirim informasi pembayaran kepada pedagang.
3. Pedagang akan menambahkan informasi tambahan pada transaksi itu dan mengirimkannya ke pelayan (*server*) CyberCash. CyberCash hanya memiliki rekapitulasi dari transaksi, sedangkan detail transaksi tetap disimpan oleh pedagang.
 4. CyberCash akan memeriksa jumlah CyberCoin yang dimiliki konsumen pada rekening bank yang bersangkutan melalui jaringan perbankan.
 5. Jika ternyata rekening bank milik konsumen masih mencukupi untuk transaksi itu, maka CyberCash akan menginstruksikan pedagang untuk mengirim barang belanjaan konsumen.
 6. Konsumen menerima barang kirimannya.

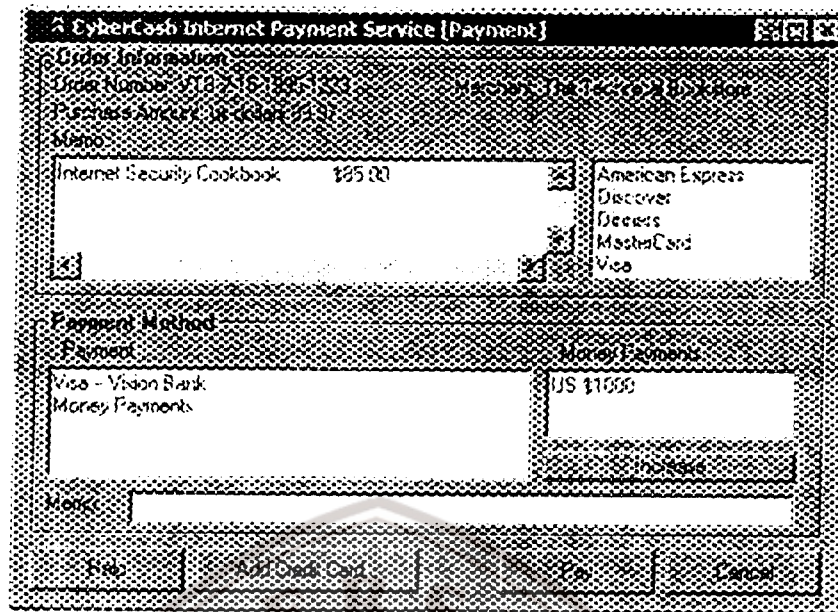


Gambar 4.7 Diagram alur data transaksi CyberCash dengan CyberCoin

Alur transaksi dengan kartu kredit

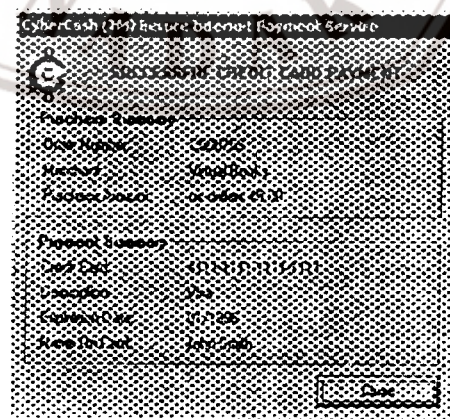
1. Konsumen harus mempertalikan kartu kredit miliknya dengan program *wallet* yang dipergunakan olehnya. Informasi kartu kredit tersebut tentunya dienkrpsi dengan *password*. Hal ini cukup hanya dilakukan satu kali.
2. Konsumen memilih barang yang akan dibelinya di situs web pedagang, dan memilih metoda pembayaran dengan [CyberCash]. Setelah dipilih, *web server* pedagang menginstruksikan agar *browser* konsumen menjalankan program *wallet*. Program *wallet* akan menampilkan *dialog box* pembayaran, yang berisi detail transaksi. Konsumen kemudian harus memilih kartu kredit mana yang akan dipergunakannya. Jika setuju, konsumen menekan tombol pembayaran [Pay].

Wallet kemudian akan mengirim informasi pembayaran kepada pedagang. Pedagang tidak bisa melihat informasi kartu kredit, karena informasi kartu kredit yang terenkripsi itu hanya bisa dibuka oleh CyberCash.

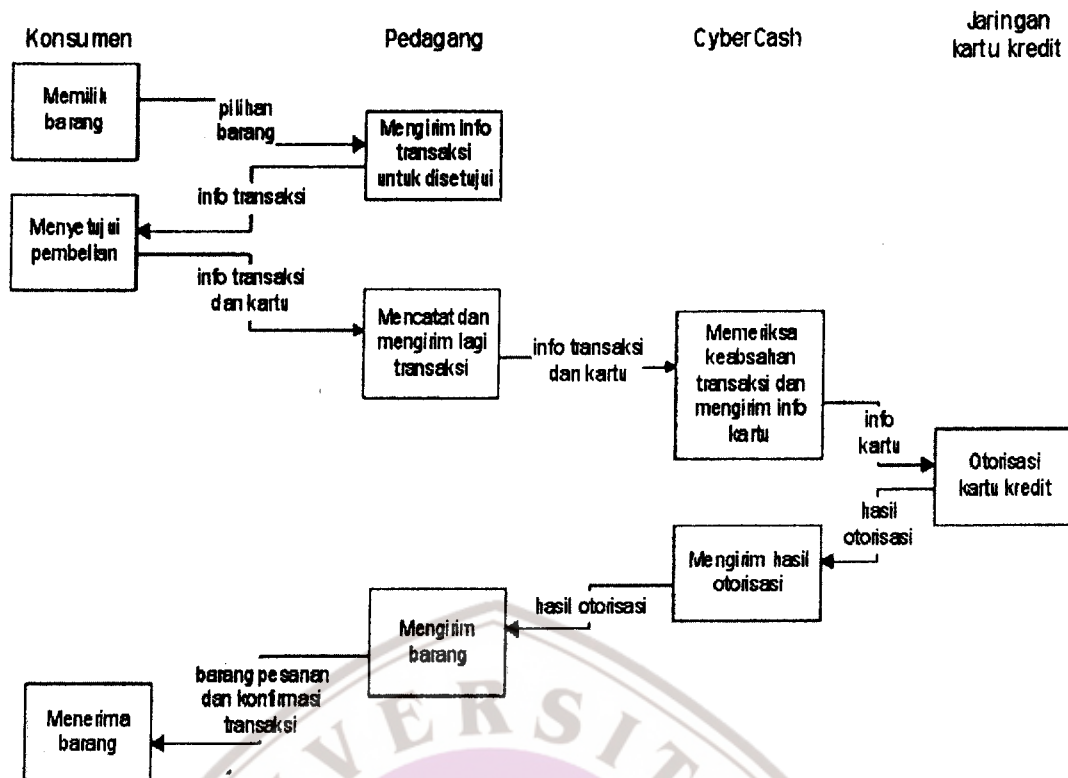


Gambar 4.8 Dialog box pembayaran CyberCash

3. Pedagang akan menambahkan informasi tambahan pada transaksi itu dan mengirimkannya ke pelayan CyberCash. Perhatikan bahwa CyberCash hanya memiliki rekapitulasi dari transaksi, sedangkan detail transaksi tetap disimpan oleh pedagang.
4. CyberCash akan memeriksa proses otorisasi dengan lembaga pengelola kartu kredit melalui jaringan kartu kredit.
5. CyberCash akan mengirimkan hasil otorisasi kepada pedagang, yang kemudian akan diteruskan ke program *wallet* konsumen.
6. Jika otorisasi disetujui, maka pedagang kemudian berkewajiban mengirimkan barang belanjaan kepada konsumen



Gambar 4.9 Pesan konfirmasi pembayaran pada transaksi dengan CyberCash



Gambar 4.10 Diagram alur data transaksi CyberCash dengan kartu kredit

Klasifikasi

CyberCash adalah salah satu perusahaan penyelenggara SPI yang menyediakan lebih dari satu macam cara pembayaran, yakni dengan menggunakan kartu kredit maupun dengan CyberCoins. Seperti telah diutarakan di atas, untuk membeli CyberCoins – uang elektronik dari CyberCash – konsumen dapat menggunakan kartu kredit atau transfer dari rekening banknya. Jadi CyberCoins termasuk dalam alat pembayaran dengan sistem *pre-paid*. Karena pedagang tidak tahu dari mana uang itu berasal, tetapi CyberCash mengetahui pemakaiannya, maka transaksinya bersifat *pseudo-anonim*. Ini disebabkan karena CyberCoin tidak termasuk dalam kategori uang elektronik dengan sistem *token* – dimana uang itu sendiri yang berpindah – namun termasuk ke dalam kategori *network money*, dimana bank melakukan pendebitan dan pengkreditan secara *on-line*. Kedua metoda pembayaran tersebut membutuhkan otorisasi *on-line*, dan jelas pedagang terbedakan dengan konsumennya. CyberCoins cocok untuk transaksi *micropayments*.

Keamanan dan Serangan

Enkripsi yang dipergunakan untuk enkripsi informasi adalah dengan RSA 768-bit, dan enkripsi simetris DES 56-bit. Kunci privat disimpan di dalam *hard disk* milik konsumen dan diproteksi dengan *password* dari *wallet*. Dalam waktu dekat, CyberCash berencana untuk meningkatkan panjang kunci asimetrisnya menjadi 1024 bit.

Karena belum menggunakan sertifikat digital, maka tentunya saat pendaftaran konsumen secara *on-line* ke CyberCash, penyerang masih bisa mengganti kunci publik yang sedang dipertukarkan. Jika berhasil, penyerang akan mendapatkan informasi kartu kredit atau rekening bank. Saat pertukaran kunci publik antara konsumen dengan pedagang, juga dapat dilakukan serangan untuk menukar kunci-kunci yang sedang dipertukarkan. Jika berhasil, maka penyerang dapat mengganti data transaksi seperti alamat tujuan pengiriman barang. CyberCash kini sedang bekerjasama dengan VeriSign untuk menyediakan fasilitas sertifikat digital dalam skenario transaksinya.

Kepercayaan dan Penipuan

Pertama, konsumen jelas harus yakin kepada CyberCash bahwa perangkat lunak *wallet* yang dipergunakan dan gerbang pembayaran CyberCash akan menjamin kerahasiaan konsumen, jadi tidak membocorkan informasi transaksi dan kartu kredit kepada pihak lain yang tidak perlu. Konsumen mempercayai bahwa CyberCash tidak akan menyalahgunakan informasi kartu kredit atau rekening banknya. Kedua, pedagang juga harus mempercayai pencatatan informasi kartu kredit konsumen yang dilakukan oleh CyberCash, karena akan dibutuhkan saat penagihan oleh pedagang kepada *acquirer*. Pedagang tidak bisa berkolusi dengan CyberCash untuk membuat transaksi fiktif atas nama seorang konsumen, karena transaksi itu tidak sah kalau tidak ditandatangani dengan kunci privat milik konsumen.

Pencatatan

Patut dicatat bahwa CyberCash tidak menerima detail transaksi, hanya sebagian data transaksi yang perlu saja. Detail transaksi (tapi tidak termasuk informasi kartu kredit atau rekening bank) dicatat oleh pedagang. Informasi kartu kredit atau rekening bank milik konsumen tidak diketahui oleh pedagang, karena pedagang menerimanya dalam bentuk terenkripsi. Pencatatan juga dilakukan dalam *wallet* yang digunakan oleh konsumen, sehingga memudahkan konsumen untuk mengawasi pengeluarannya.

Penerimaan Pembayaran dan Biaya Transaksi

Setelah otorisasi kartu kredit dan pengiriman, sebuah transaksi dapat langsung ditagih oleh pedagang kepada *acquirer*. Proses penagihan itu dapat dilakukan saat konsumen masih terhubung ke pedagang atau belakangan. CyberCash, yang memegang informasi kartu dari setiap transaksi, memberikan pula pelayanan *capture* kepada *acquirer*.

Untuk transaksi dengan CyberCoins, jika komputer konsumen sudah menerima barang belanjanya yang dikirim secara digital, maka barulah bank akan mengkredit rekening bank pedagang. Pendebitan rekening bank konsumen dan pengkreditan rekening bank pedagang tentunya dilakukan melalui jaringan privat perbankan, jadi tidak melalui Internet.

Pedagang akan membayar kepada bank sejumlah biaya untuk setiap transaksi yang menggunakan CyberCoin. Hal ini dilakukan karena bank adalah pihak yang sesungguhnya menyediakan rekening khusus untuk CyberCoin secara *on-line*. Besar

biaya transaksi tersebut bukanlah dalam bentuk prosentase dari transaksi atau suatu nilai tetap tertentu, melainkan digolongkan berdasarkan peringkat nilai transaksi. Pada gilirannya, bank dan lembaga pengelola kartu kredit juga akan membayar kepada CyberCash yang menyediakan teknologi dan jasa *payment server*.

Prospek di masa depan

Kini CyberCash bekerjasama dengan Netscape untuk mengintegrasikan metoda pembayaran yang dirancangnya ke dalam *browser* dan *web server* dari Netscape. Dalam waktu dekat, CyberCash juga akan meluncurkan sistem transaksi yang sanggup melakukan pembayaran *peer-to-peer*. Selain itu CyberCash juga sudah menyatakan dukungannya terhadap protokol SET yang diusulkan oleh VISA dan MasterCard. Meskipun harus menggunakan perangkat lunak tambahan yang harus di-*download* sebelum berbelanja, namun mengingat kemampuannya untuk menangani berbagai macam pembayaran, prospek CyberCash cukup cerah di masa depan. Di masa depan CyberCash juga akan menyediakan fasilitas untuk pembayaran *peer-to-peer*.

4.4 NET1 NETCHEX

Sesuai dengan namanya, NetChex adalah suatu cara untuk menuliskan cek elektronik melalui Internet. NetChex tidak mengirimkan data sensitif seperti nomor rekening bank melalui Internet, melainkan menggunakan *shadow account*, yakni berkorelasi dengan informasi konsumen beserta informasi rekening sesungguhnya. NetChex menyimpan pangkalan data berisi rekening bank asli dan *shadow account*-nya. NetChex menjadi perpanjangan tangan dari rekening bank konsumen yang sudah ada. Proses kliring tetap dilakukan secara konvensional.

Konsumen (pemberi cek) dan pedagang yang menerima cek harus memiliki dahulu *shadow account* di gerbang pembayaran NetChex. Pada skenario awal, NetChex secara fisik mencetak cek tersebut dan mengirimnya lewat pos. Kini NetChex telah terhubung langsung ke jaringan privat antarbank, sehingga dapat memerintahkan pembayaran dari satu bank ke bank lain secara elektronik.

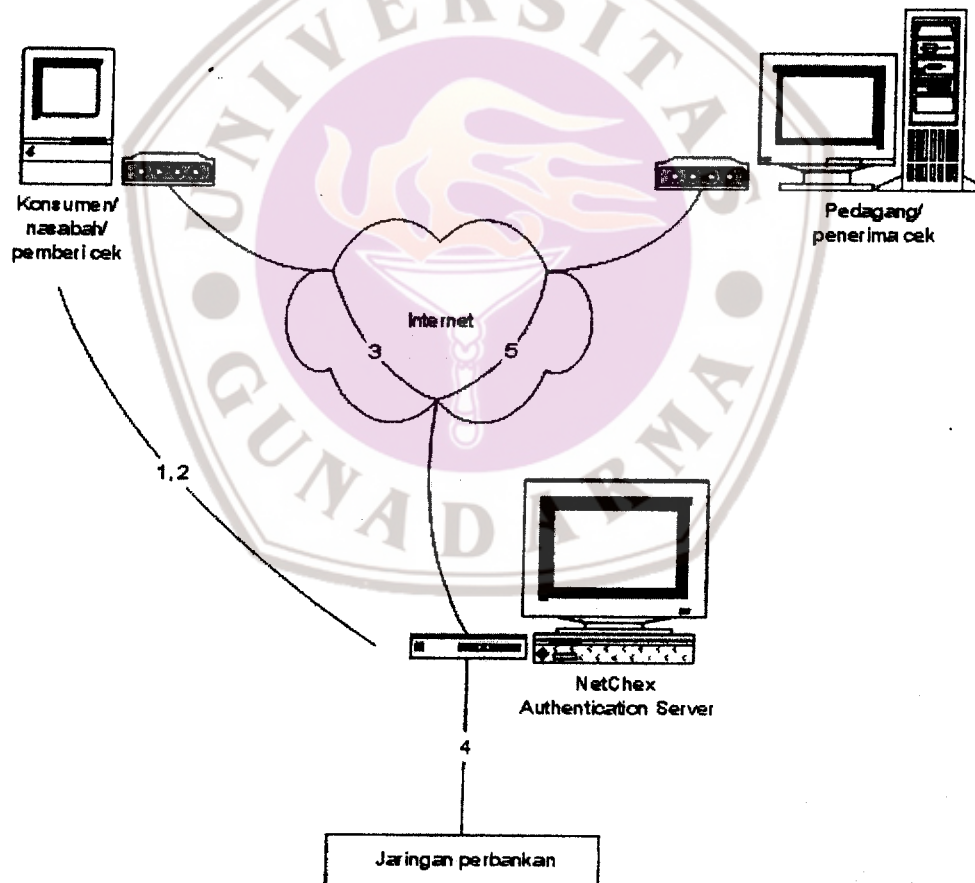
Perangkat Lunak

Konsumen menggunakan perangkat lunak klien (*client software*) khusus yang perlu di-*download*. Perangkat lunak itu berguna untuk menuliskan cek elektronik yang akan ditransmisikan ke NetChex Authentication Server (NCAS) yang dapat dianggap sebagai gerbang pembayarannya. Pedagang tidak memerlukan perangkat lunak khusus.

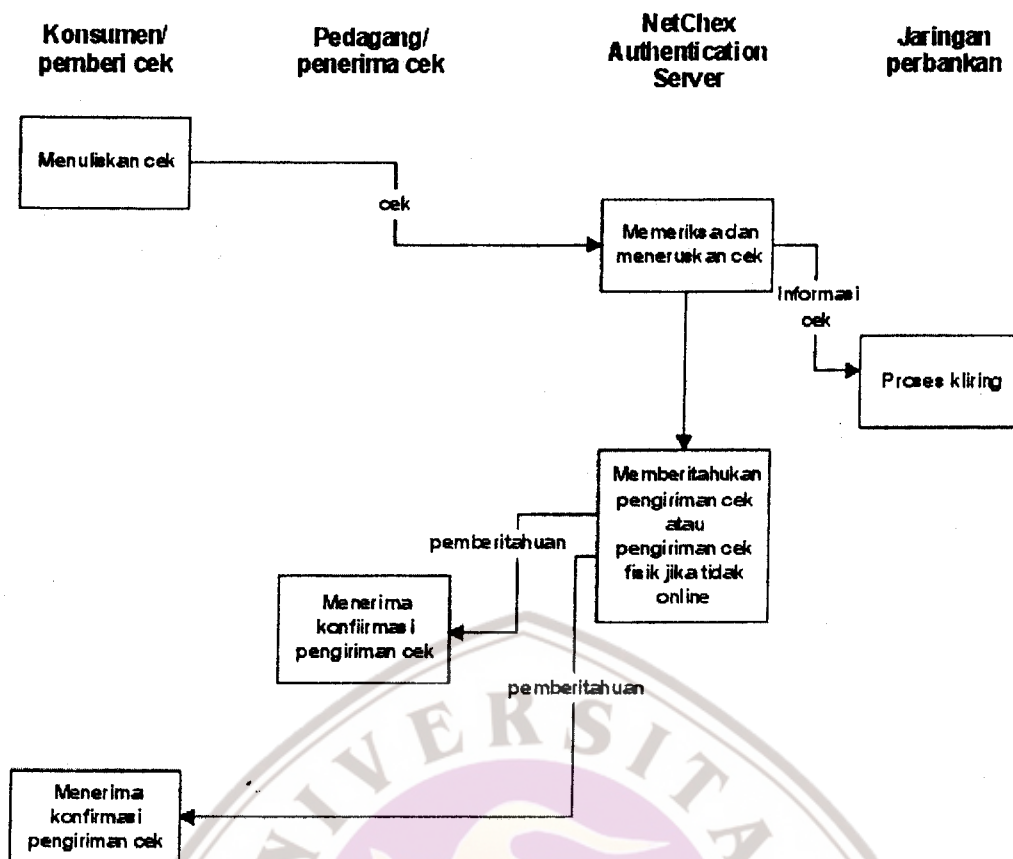
Uniknya saat instalasi, perangkat lunak klien NetChex yang tersedia gratis itu, membuat sidik jari dari konfigurasi komputer konsumen, sehingga perangkat lunak klien NetChex itu tidak bisa dikopi untuk dipergunakan pada komputer-komputer lain. Namun demi fleksibilitas, memang ada fasilitas tambahan dari NetChex untuk menduplikasi perangkat lunak klien NetChex pada komputer kedua.

Alur Transaksi

1. Konsumen men-*download* perangkat lunak NetChex. Untuk menyelesaikan proses instalasi pada komputernya, konsumen mendaftarkan diri dahulu kepada NetChex dengan mengirimkan identitas diri dan informasi rekening banknya melalui pos atau faksimili.
2. NetChex akan memberikan jawaban konfirmasi dalam waktu 24 jam. Jika disetujui, konsumen akan ditelpon oleh NetChex. Konsumen akan diberikan kode khusus untuk menyelesaikan proses instalasi perangkat lunak klien NetChex. Konsumen diberi *shadow account* oleh NetChex.
3. Konsumen dengan perangkat lunak klien NetChex bisa menuliskan cek elektronik kepada siapa saja dengan menggunakan *shadow account*-nya. Cek elektronik itu dikirim kepada NetChex Authentication Server. NetChex memeriksa keabsahan cek elektronik yang dikirim konsumen.
4. Informasi dalam cek elektronik itu dikirim oleh NetChex melalui jaringan privat ke bank yang bersangkutan untuk proses kliring lebih lanjut.
5. Jika pedagang memiliki surat elektronik, maka pedagang diberitahu oleh NetChex mengenai pembayaran cek itu melalui surat elektronik. Konsumen yang mengirimkan cek juga dikirimi surat elektronik yang berisi informasi transaksi.



Gambar 4.11 Diagram topologi transaksi NetChex



Gambar 4.12 Diagram alur data transaksi NetChex

Klasifikasi

NetChex tergolong sistem pembayaran debit. Transaksi dengan NetChex dapat dilacak, namun informasi rekening nasabah hanya diketahui oleh NetChex Authentication Server. Perlu diperhatikan bahwa skenario yang ditawarkan oleh NetChex adalah sistem *peer-to-peer*, dimana konsumen dapat membayar kepada siapa saja yang memiliki account bank di Amerika Serikat, sekalipun orang yang menerima pembayaran itu tidak memiliki akses ke Internet. Dalam sistem ini meskipun dilakukan proses otentikasi oleh NetChex secara *on-line*, namun proses kliring pada saat ini pasti memerlukan proses minimal satu hari. Ini disebabkan karena prosedur kliring di rumah kliring yang memang memakan waktu lama. Rekening bank pedagang baru dapat dikredit setelah proses kliring itu selesai. Barang dagangan yang di-*download* dengan segera tidak cocok menggunakan skenario SPI ini.

Kemanan dan Serangan

Fasilitas keamanan yang ditawarkan oleh NetChex di Internet terbilang cukup canggih. Pertama, data sensitif seperti informasi rekening bank dari konsumen tidak pernah dikirim di Internet. Kedua, informasi transaksi juga dienkripsi dengan kunci asimetris dinamis yang dibuat setiap kali terjadi transaksi, dimana kunci itu dibuat dengan mengambil informasi transaksi terakhir dan informasi saat pendaftaran. Jadi

andaikan seorang penyerang berhasil mendapatkan kunci privat dari suatu transaksi, itu tidak berarti berhasil mendapatkan kunci privat selanjutnya, karena kunci privat selanjutnya akan dibuat ulang. Ketiga, penulisan cek hanya bisa dilakukan dari komputer yang dimana perangkat lunak klien NetChex di-*install* pertama kali saat pendaftaran.

Kepercayaan dan Penipuan

Konsumen harus mempercayai NetChex yang menyimpan pangkalan data yang berisi hubungan antara *shadow account* dengan informasi rekening yang asli. Pada saat pendaftaran melalui faksimili atau pos, konsumen juga harus mempercayai NetChex agar tidak menyalahgunakan informasi jati diri dan informasi rekening bank milik konsumen.

Pedagang juga sebaiknya tidak melepas barang dagangannya dahulu sebelum proses kliring selesai, agar tidak tertipu oleh cek kosong.

Pencatatan

Konsumen dapat melihat cek elektronik apa saja yang pernah ditulisnya dengan menggunakan perangkat lunak klien NetChex. Tentunya seperti biasa, cek yang ditulisnya itu juga muncul pada laporan bulanan dari bank.

Penerimaan Pembayaran dan Biaya Transaksi

Pedagang atau penerima cek akan dikredit rekening banknya setelah proses kliring cek tersebut selesai.

Prospek di masa depan

NetChex dapat dilihat sebagai salah satu pengembangan (*extension*) fasilitas perbankan di Internet. Jika sudah terhubung ke bank, sebenarnya banyak hal yang bisa dilakukan, bukan cuma sekedar untuk menulis cek saja. Mungkin selanjutnya sistem dapat dikembangkan untuk *telebanking*.

4.5 VISA/MASTERCARD SECURE ELECTRONIC TRANSACTION (SET)

Dua raksasa kartu kredit dunia, Visa dan MasterCard, bekerja sama membuat suatu standar. Kini, sebagian besar penyedia jasa pelayanan pembayaran di Internet telah setuju untuk mengikuti standar SET. Menurut spesifikasi SET, ada beberapa kebutuhan bisnis yang perlu ditangani:

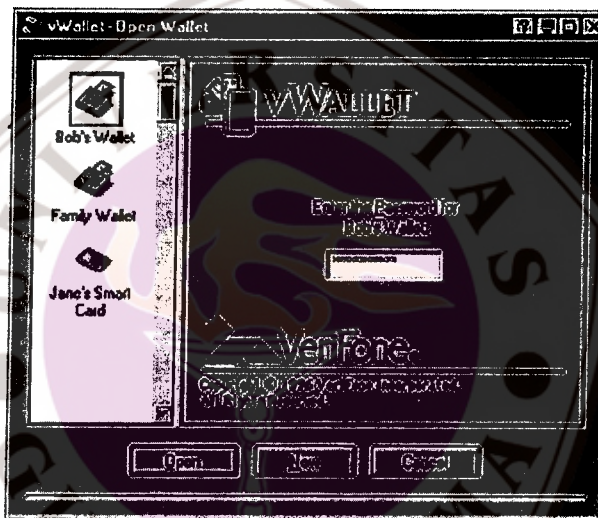
1. Keamanan pengiriman informasi pemesanan dan pembayaran.
2. Integritas data dalam setiap transaksi.
3. Otentikasi bahwa seorang konsumen adalah seorang pemegang kartu (*cardholder*) yang valid pada suatu perusahaan penyelenggara pembayaran tertentu (misalnya: Visa atau MasterCard).
4. Otentikasi bahwa seorang pedagang memang benar-benar bisa menerima jenis pembayaran tersebut.

5. Menyediakan suatu sistem pembayaran yang tidak terikat kepada suatu protokol perangkat keras atau perangkat lunak tertentu, dengan kata lain dapat bekerja dengan berbagai macam perangkat lunak dan berbagai penyedia jasa.

Banyak perusahaan *developer* yang sudah menyatakan dukungannya terhadap SET bagi produk/produk penunjang sistem perdagangan Internet mereka, seperti Microsoft, IBM, Netscape, SAIC, GTE, Open Market, CyberCash, Terisa Systems and VeriSign. Bahkan kini perusahaan penyelenggara *charge card* seperti American Express, akhirnya menyatakan dukungannya untuk SET. Tampaknya SET, (ataupun derivasinya) akan menjadi standar di masa depan.

Perangkat Lunak

SET tidak hanya dirancang untuk transaksi pada Web saja, namun juga bisa dipergunakan pada media lainnya. Pedagang dapat saja menyebarkan katalog dalam CD-ROM. Setelah konsumen memilih barang yang akan dibelinya dari katalog CD-ROM itu, konsumen kemudian dapat melakukan pembayaran dengan protokol SET, baik itu dengan *browser* atau surat elektronik.



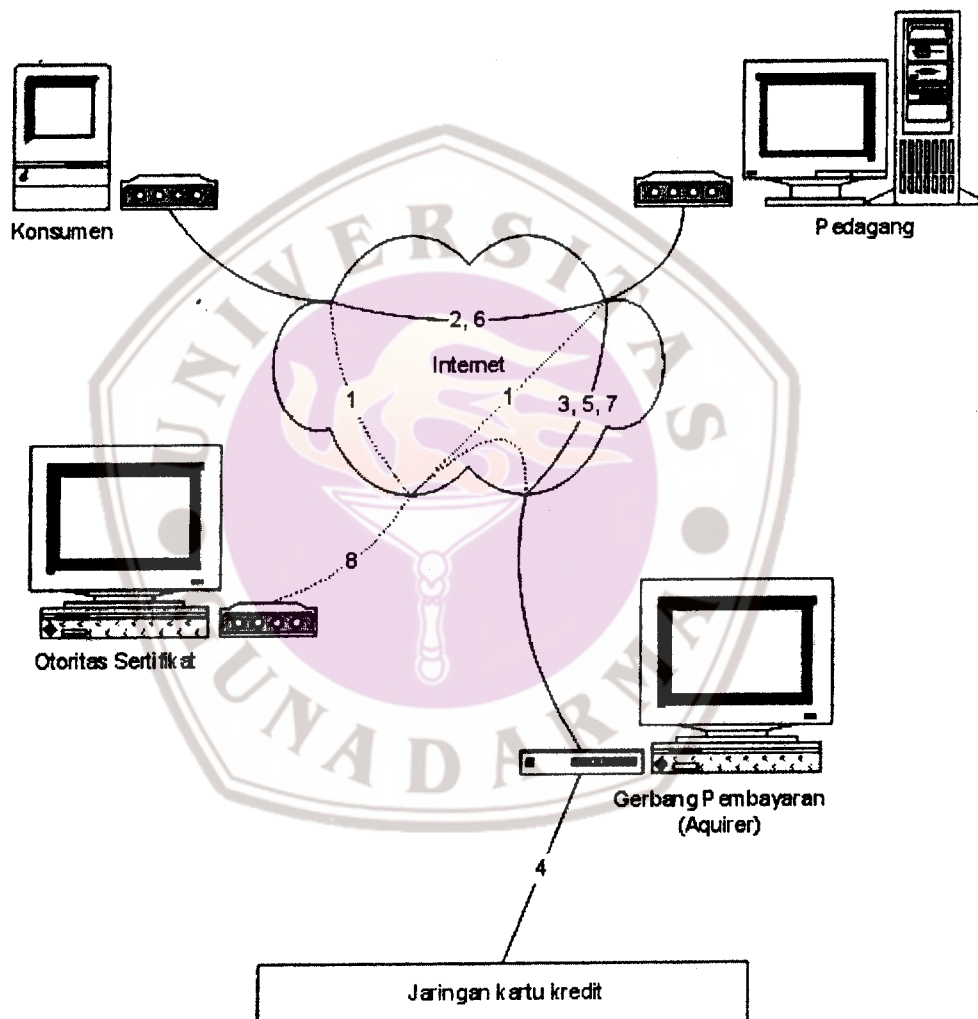
Gambar 4.13 Tampilan vWallet dari Verifone

VeriFone telah meluncurkan suatu program kecil yang mirip dengan program *wallet* CyberCash, yang dinamakan *vWallet*. Program ini adalah program aplikasi pertama bagi klien untuk mendukung skenario transaksi SET. *vWallet* juga dapat dirancang agar di masa depan dapat menunjang teknologi pembayaran lainnya seperti uang elektronik dan cek elektronik

Alur Transaksi

1. Untuk melakukan transaksi SET, konsumen dan pedagang harus mendapatkan sertifikat terlebih dahulu dari otoritas sertifikat (OS). Konsumen dalam langkah ini harus mengetikkan *personal account number* (PAN) dan informasi jati dirinya. Pedagang dalam langkah ini juga harus memberikan informasi jati dirinya kepada OS.

2. Konsumen kemudian dapat mulai berbelanja. Jika sudah memilih barang apa yang hendak dibeli, konsumen membuat *order instruction* (OI) dan *payment instruction* (PI). Konsumen menyerahkan OI dan PI kepada pedagang. PI tidak bisa dibaca oleh pedagang karena dienkripsi dengan kunci publik gerbang pembayaran (*payment gateway*).
3. Setelah pedagang memproses OI, maka pedagang melakukan otorisasi PI melalui gerbang pembayaran. Seringkali *acquirer* bertindak sebagai gerbang pembayaran.
4. Gerbang pembayaran melakukan otorisasi kartu kredit dengan *issuer* melalui jaringan privat kartu kredit.
5. Jika otorisasi disetujui, maka gerbang pembayaran menginstruksikan pedagang untuk menyerahkan barang dagangannya kepada konsumen.
6. Konsumen menerima barang dagangannya.

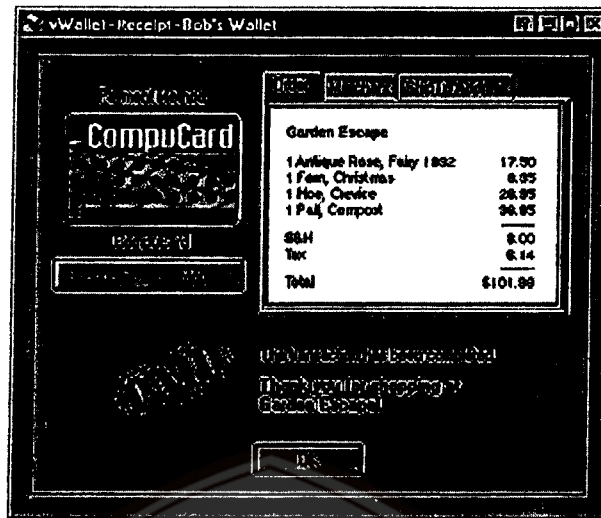


Gambar 4.14 Diagram topologi protokol SET

7. Pedagang kemudian dapat memperoleh pembayarannya dengan melakukan proses *capture* melalui gerbang pembayaran pula. Langkah ini sering di-*batch*,

sehingga akan ada tenggang waktu antara permintaan pembayaran (*payment capture*) dengan proses otorisasi.

8. Setiap melakukan komunikasi, setiap pihak yang terlibat dalam transaksi dapat melakukan otentikasi sertifikat digital pihak yang lain dengan menghubungi OS.



Gambar 4.15 Dialog box konfirmasi pembayaran dengan ewallet

Klasifikasi

Berdasarkan skenario di atas, terlihat bahwa sistem perdagangan di Internet dengan skenario SET dijalankan secara *on-line*. Protokol SET dapat mendukung sistem pembayaran dengan kartu kredit, *charge card* dan kartu debit. Namun kini memang belum ada bank pengelola kartu debit yang menyatakan dukungannya terhadap protokol SET. Tentunya, transaksi dengan protokol SET ini terlacak. Pada skenario SET, transaksi tidak dapat dilakukan antarkonsumen (*peer-to-peer*), namun harus antara konsumen dengan pedagang. Konsumen dapat dilihat jati dirinya oleh pedagang, karena pedagang dan konsumen saling memeriksa sertifikat digital yang dipertukarkan. Meskipun begitu, informasi kartu konsumen tidak dapat diketahui pedagang. Protokol SET tidak cocok untuk transaksi *micropayments*.

Keamanan dan Serangan

Inti dari keamanan dalam protokol SET adalah penggunaan sertifikat digital. Secara teoritis, tanpa *brute-force attack*, sertifikat digital dapat bertahan terhadap serangan *man-in-the-middle* dan juga *replay attack*. Hal ini disebabkan karena siapapun yang ingin melakukan pemeriksaan dapat memastikan apakah kunci publik yang diterimanya sah atau tidak. Seperti sudah dijelaskan sebelumnya, bagian yang rentan adalah saat pemberian sertifikat digital OS utama kepada pihak-pihak lain yang memerlukan seperti kepada para pengembang perangkat lunak untuk SET.

Sertifikat konsumen tidak memiliki informasi kartu konsumen, yakni *personal account number* (PAN) dan tanggal kadaluarsanya, namun berisi *hash* dari PAN, tanggal kadaluarsa dan sebuah angka rahasia yang hanya diketahui konsumen (*personal identification number / PIN*). Jadi jika pedagang memeriksa sertifikat milik seorang

konsumen, maka pedagang meskipun dapat melihat jati diri konsumen namun pedagang tetap tidak dapat melihat informasi kartunys. Seorang penyerang yang memiliki sertifikat seorang konsumen juga tidak dapat menggunakannya tanpa mengetahui informasi kartu dan PIN. Informasi kartu dan PIN dalam skenario SET dikirimkan dalam bentuk terenkripsi kepada gerbang pembayaran untuk pemeriksaan. Gerbang pembayaran tidak hanya memeriksa keabsahan sertifikat digital milik konsumen, tapi juga memeriksa apakah *hash* dari informasi kartu dan angka rahasia tadi sesuai dengan nilai *hash* yang ada dalam sertifikat.

Ukuran kunci yang dipergunakan dalam SET amat panjang, yang dapat dikategorikan *hard encryption*. Semua kunci berukuran 1024 bit, kecuali OS utama menggunakan ukuran kunci 2048 bit. Kunci sepanjang ini sulit dipecahkan dengan *brute-force-attack*.

Penggunaan sertifikat digital sebagai sarana pengamanan komunikasi memang membuat SPI yang menggunakan protokol SET menjadi sistem yang aman. Namun muncul pula masalah bagaimana menyimpan kunci privat dari sertifikat digital yang bersangkutan. Dalam implementasi awalnya, mungkin kunci itu disimpan dalam *hard disk* dengan pengamanan dienkripsi ber-*password*, namun pengembangan yang lebih jauh adalah dengan menyimpan sertifikat digital dan kunci privat itu di dalam *tamper-proof device* seperti kartu chip.

Protokol SET juga menggunakan suatu perangkat kriptografi baru, yakni tanda tangan pesan ganda (*dual signature*). Dengan menggunakan tanda tangan pesan ganda, gerbang pembayaran saat melakukan otorisasi dapat memastikan bahwa PI yang diterimanya memang benar berhubungan dengan suatu OI tertentu, namun gerbang pembayaran tetap tidak tahu isi OI tersebut.

Kepercayaan dan Penipuan

Karena mengandalkan sertifikat digital, maka tentunya pihak-pihak yang bertransaksi mengandalkan kepercayaan mereka terhadap OS yang menerbitkan sertifikat digital. Sama halnya dengan transaksi menggunakan kartu kredit, tentunya konsumen harus mempercayai lembaga keuangan pengelola kartu kredit yang melakukan otorisasi.

Untuk pemeriksaan sertifikat digital, pihak-pihak yang bertransaksi juga membutuhkan informasi dari OS mengenai sertifikat siapa saja yang dibatalkan. Tentunya OS yang menyimpan daftar sertifikat terbatalan ini harus dipercayai oleh pihak-pihak yang melakukan transaksi.

Pencatatan

Skenario protokol SET tidak menspesifikasi pencatatan yang dilengkapi dengan tanda tangan digital dari pihak-pihak yang melakukan transaksi. Namun dalam implementasinya, pencatatan dapat dilakukan di perangkat lunak klien yang dipergunakan oleh konsumen dan juga di *web server* pedagang.

Penerimaan Pembayaran dan Biaya Transaksi

Spesifikasi SET tidak menjelaskan mengenai biaya tambahan atas transaksi. Namun, jika pihak *acquirer* sendiri yang menjadi gerbang pembayaran, tentunya boleh dikatakan tidak ada biaya tambahan. Jadi hampir tidak ada bedanya karena dalam transaksi kartu kredit *on-line* yang biasa, pedagang akan melakukan otorisasi itu melalui *acquirer* juga.

Seperti sudah dijelaskan di atas, karena perubahan sistem dimana pedagang tidak mendapatkan informasi kartu kredit, maka memang ada perubahan prosedur penagihan ke *acquirer*.

Prospek di masa depan

Suatu *pilot project* SET telah berhasil dilakukan di Jepang pada awal tahun 1997. Implementasi SET saat ini menggunakan *hard disk* sebagai media untuk menyimpan kunci privat. Meskipun dilindungi oleh *password*, namun tetap kurang aman. Oleh karena itu, diusulkan untuk menggunakan kartu chip untuk menyimpan kunci privat. IBM kini juga mengembangkan protokol SET menjadi superSET

4.6 TABEL PERBANDINGAN SPI

Dari analisis beberapa SPI di atas, umumnya SPI menggunakan gerbang pembayaran sebagai pihak yang dipercaya dalam suatu skenario transaksi. Dalam suatu skenario transaksi SPI di suatu titik tertentu pasti ada satu pihak (biasanya konsumen) yang harus mempercayai pihak lain.

Mengingat Internet tidak aman, maka sebenarnya yang dilakukan oleh banyak SPI adalah berusaha merahasiakan informasi-informasi penting dari pihak-pihak yang tidak perlu mengetahuinya. Banyak SPI yang menggunakan kriptografi kunci simetris / asimetris pada skenario transaksinya, dan ada SPI yaitu Net1 NetChex yang menggunakan *shadow account* sebagai sarana untuk proses otentikasi. Meskipun sudah lama Netscape menjual *web server* dengan fasilitas SSL, protokol SET dari Visa/MasterCard-lah mempopulerkan penggunaan sertifikat digital untuk klien dalam suatu transaksi.

Tabel 4.1 Tabel Perbandingan karakteristik dari SPI yang dibahas

	Forms HTML	Kupon PGP	CyberCash	NetChex	SET
Cara pembayaran	Netif	USSD	Netif/Netif	Netif	Netif
Keterlacakan transaksi	teridentifikasi	teridentifikasi	pseudo-anonim	teridentifikasi	pseudo-anonim
Status pihak yang bertransaksi	pedagang/pembeli	pedagang/pembeli	pedagang/pembeli	pedagang/pembeli	pedagang/pembeli
Waktu konfirmasi keabsahan transaksi	off-line; on-line	on-line	on-line	on-line; off-line	on-line
Perangkat lunak	browser, SSL, SSI	Netif PGP, browser	Netif	Netif	Netif
Kerahasiaan transaksi	tidak ada atau SSL	kunci asimetris dan simetris	DES dan RSA	kunci simetris; asimetris	amplop digital
Keutuhan transaksi	SHA-1, MD5	Integrity	DES, MD5, hash	MD5	MD5, SHA-1
Keabsahan konsumen	nomor kartu yang sah	nama pada kupon	kunci asimetris RSA	shadow account; sidik jari komputer klien	sertifikat digital
Keabsahan pedagang	MD5, SHA-1, SSL	Integrity	MD5, SHA-1, RSA	MD5, SHA-1	Integrity
Pencatatan transaksi	web server pedagang	web server pedagang/penerbit kupon	klien dan server pedagang & CyberCash	web server & klien	klien, pedagang, gerbang pembayaran
Pembukuan transaksi	tidak ada	tidak ada/tercatat digital	MD5	MD5	MD5, SHA-1
Kepercayaan konsumen	pedagang	penerbit kupon	CyberCash	NetChex	otoritas sertifikat