

Author:



M Taufiq Ismail - A.2005.1.30028

Malangkecewara College of Economics
Terusan Candi Kalasan, Blimbing - Malang

Email: opic-s@plasa.com

Peran Kriptografi sebagai bagian keamanan jaringan dalam *Electronic Commerce*

M Taufiq Ismail – A.2005.1.30028

Malangkecewara College of Economics
Terusan Candi Kalasan, Blimbing - Malang

Email: opic-s@plasa.com

Abstrak

Komunikasi jaringan telah mengalami perkembangan yang signifikan dalam 25 tahun terakhir. Dan saat ini jaringan tidak hanya dinikmati segelintir kalangan, namun telah menjadi sesuatu yang esensial bagi setiap orang. Jaringan pun tidak hanya digunakan untuk berkomunikasi namun sudah mulai digunakan dalam perdagangan yaitu menjadi bagian dari mata rantai perdagangan (e-Commerce).

Hal itu tentu saja tidak serta merta diterima masyarakat. Aspek keamanan masih menjadi salah satu masalah dalam perkembangan e-Commerce. Problem otentifikasi, non-repudiation, kerahasiaan serta integritas data antara mobile device dan web server mendorong para ahli untuk menggunakan teknik-teknik kriptografi. Aplikasi seperti Public Key Infrastructure (PKI), dan Wireless Transport Layer Security (WTLS), merupakan salah satu contoh penggunaan kriptografi untuk mendukung E-commerce. Oleh karena itu pada makalah ini akan dibahas mengenai permasalahan keamanan yang ada pada mobile commerce dan pemanfaatan kriptografi sebagai solusi untuk permasalahan tersebut pada platform yang umum digunakan untuk mengembangkan aplikasi mobile commerce. Pembahasan ini akan meliputi kajian bagaimana solusi tersebut dapat menjamin keamanan pada aplikasi mobile commerce, bagaimana penggunaannya dan kelemahannya serta usulan yang dapat digunakan untuk mengatasinya.

keyword : Business Information Systems, e-commerce, Managing IT: Security and Ethical Challenges, Managing IT: Security and Ethical Challenges

1. Pendahuluan

E-commerce merupakan proses bisnis yang dijalankan melalui melalui elektronik, misalnya transaksi jual-beli barang dan jasa secara *online*. Bisnis proses ini mungkin dalam bentuk B2B (*Business to Business*) maupun B2C (*Business to Customer*). Defenisi ini, tidak membatasi jenis alat yang digunakan oleh *end user* untuk memperoleh akses ke internet.

Bentuk lain dari E-commerce adalah *mobile commerce* yang memanfaatkan perangkat *mobile* atau terminal untuk melakukan transaksi bisnis melalui jaringan telekomunikasi *mobile*. Transaksi bisnis ini tidak hanya terbatas pada layanan yang hanya melibatkan komunikasi, transaksi dan hiburan, tetapi juga memungkinkan terjadinya transfer uang. Perangkat yang digunakan bisa berbentuk telepon seluler maupun PDA.

Bahkan karena jumlah pengguna telepon seluler di berbagai negara lebih banyak dari jumlah pengguna internet, maka layanan *m-commerce* semakin banyak dikembangkan karena memiliki potensi yang sangat besar. Semakin tinggi penetrasi telepon seluler dan perangkat *mobile* lainnya semakin banyak jumlah calon pelanggan yang dapat dijangkau. Selain itu, dengan sifat perangkat yang *mobile* maka aplikasi *mobile* dapat digunakan kapan dan dimana pun. Oleh karena itu, terutama pada pasar B2C. Contoh aplikasi yang telah dikembangkan adalah *mobile banking*, aplikasi untuk transaksi saham, pelelangan barang dan lain sebagainya.

Akan tetapi, kesuksesan dari aplikasi ini sangat bergantung pada jaminan keamanan teknologi yang dimanfaatkan. Hal ini cukup penting, mengingat pengguna tidak akan menggunakan aplikasi *e commerce* yang belum sepenuhnya aman. Aspek keamanan pada aplikasi *e commerce* meliputi keamanan system jaringan serta keamanan data yang disimpan pada server.. Contoh penerapan kriptografi pada aplikasi *electronic commerce* adalah *Public Key Infrastructure* (PKI),

2. Aspek keamanan *electronic commerce*

Terdapat beberapa ancaman keamanan pada aplikasi *electronic commerce* yaitu:

- a. Kurangnya kesadaran pengguna akan resiko keamanan. Biasanya pengguna tidak begitu peduli mengenai aksinya misalnya tidak menggunakan pin pada telepon seluler.
- b. Pencurian informasi personal yang mungkin tidak disadari pengguna. Hal ini dapat terjadi melalui pencurian perangkat *electronic commerce*,, *network sniffing* dan sebagainya.
- c. Adanya virus dan aplikasi yang tidak jelas sumbernya dan mungkin

berbahaya .

d. Transmisi nirkabel. Hal ini mengakibatkan sinyal transmisi dapat ditangkap oleh siapapun dengan bebas. Penyadap dapat mencoba menginterpretasi data, memodifikasi pesan, menahan pesan bahkan mencegah pesan sampai kepada pengguna

e. Serangan *man-in-the-middle-attack*, dimana penyerang dapat mengintersepsi komunikasi antar dua pihak kemudian "menyerupai" salah satu pihak dengan cara bersikap seolah-olah ia adalah salah satu pihak yang berkomunikasi (pihak yang lainnya tidak menyadari kalau dia berkomunikasi dengan pihak yang salah).

f. Penyerang yang dapat mengintersepsi komunikasi, dapat saja menyimpan pesan tertentu kemudian mengirimkannya kembali di lain waktu. Hal ini memungkinkan penyerang untuk mencoba meyakinkan server bahwa dia adalah seorang pengguna yang terotentikasi.

Sedangkan hal-hal yang perlu diperhatikan pada aplikasi *electronic commerce* dari sudut pandang keamanan adalah sebagai berikut:

a. Aplikasi menyediakan layanan yang berdasarkan pendaftaran (*subscription*). Untuk mendaftar user dapat memberikan informasi seperti nomor kartu kredit atau informasi lainnya. Aplikasi harus melindungi informasi ini karena akan di proses di *client* dan akhirnya sampai ke *server*. Jika informasi pelanggan tersebut memenuhi persyaratan yang dibutuhkan maka pelanggan akan terdaftar dan informasi tersebut akan tersimpan pada basis data di *server* yang juga harus dilindungi keamanannya.

b. Pengguna yang sudah terdaftar dapat meminta informasi atau permintaan tertentu dari layanan yang didaftarnya. Oleh karena itu pengguna membutuhkan cara tertentu untuk membuktikan identitasnya kepada *server* sehingga dapat diverifikasi dengan menggunakan informasi yang tersimpan pada basis data di *server*.

c. Permintaan informasi dari *client* dan respon dari *server* mungkin saja mengandung informasi yang sifatnya sensitif. Contohnya jika seorang pengusaha melakukan transaksi bisnis yang menyangkut rahasia perusahaan dengan memanfaatkan *server*, maka pengusaha tersebut tidak mau orang lain mengetahui isi pesan selama transaksi dilakukan. Dengan kata lain kerahasiaan informasi harus dijaga.

Aspek keamanan pada aplikasi *electronic commerce* dengan berbagai ancaman keamanan seperti yang telah dijelaskan diatas dapat diatasi dengan kriptografi karena kriptografi menyediakan beberapa aspek keamanan berikut :

Kerahasiaan (*confidentiality*)

Layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya. Layanan ini umumnya direalisasikan dengan cara mengenkripsi pesan menjadi bentuk yang tidak dapat dimengerti.

Integritas Data (*data integrity*)

Layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain aspek keamanan ini dapat diungkapkan sebagai pertanyaan :

“Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?”.Istilah lain yang serupa dengan *data integrity* adalah otentikasi pesan (*message authentication*). Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubstitusian data lain kedalam pesan yang sebenarnya.

Otentifikasi (*authentication*)

Otentifikasi adalah layanan yang untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan : “Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar? ”.

Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan.

Nirpenyangkalan (*Nonrepudiation*)

Nirpenyangkalan adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan

Menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

3. Kriptografi dan aplikasinya

Kriptografi adalah studi teknik matematis untuk keamanan informasi seperti kerahasiaan, integritas, dan otentifikasi. Kriptografi mengacak pesan sehingga tidak dapat dipahami [Al-Ba]. Berikut ini adalah beberapa teknik kriptografi dan aplikasinya yang dapat digunakan dalam menjamin keamanan pada *e-commerce*.

Teknik kriptografi

Kriptografi dapat menyediakan aspek keamanan kerahasiaan, integritas, otentikasi dan nirpenyangkalan. Salah satu teknik kriptografi yang sudah lama dikenal adalah kriptografi kunci simetris yang menggunakan kunci rahasia yang sama untuk mengenkripsi dan mendekripsi pesan. Dengan demikian, dua pihak yang saling berkomunikasi harus saling mempercayai dan merahasiakan kunci rahasia yang digunakan. Hal ini mengakibatkan timbulnya permasalahan bagaimana cara mendistribusikan kunci. Contoh algoritmanya RC4, RC5 untuk *stream cipher* dan AES, IDEA untuk *block cipher*. Untuk mengatasi permasalahan distribusi kunci tersebut berkembanglah teknik kriptografi kunci public yang memungkinkan pengguna berkomunikasi secara aman tanpa perlu berbagi kunci rahasia. Pada teknik ini digunakan dua buah kunci yaitu kunci publik dan kunci privat. Kunci publik tidak rahasia dan digunakan untuk mengenkripsi pesan, sedangkan kunci privat bersifat rahasia dan digunakan untuk mendekripsi pesan.

Infrastruktur Kunci Publik (*Public Key Infrastructure*)

Pada sistem kriptografi kunci publik terdapat permasalahan dalam distribusi kunci publik yang juga disebut dengan *man-in-the-middle-attack*. Untuk lebih jelasnya, misalkan Alice dan Bob mengirim kunci publiknya masing-masing melalui saluran komunikasi. Orang ditengah misalnya Carol, memutus komunikasi antara Bob dan Alice lalu ia berpura-pura sebagai salah satu pihak (Alice atau Bob). Carol (yang menyamar sebagai Alice) mengirimkan kunci publiknya kepada Bob (Bob percaya itu adalah kunci publik milik Alice), dan Carol (yang menyamar sebagai Bob) mengieimkan kunci publiknya kepada Alice (Alice percaya itu adalah kunci publik milik Bob). Selanjutnya Carol mendekripsi pesan dari Bon dengan kunci privatnya, menyimpan salinannya, lalu mengenkripsi pesan tersebut dengan kunci publik Alice dan mengirim cipherteks tersebut kepada Alice. Alice dan Bob tidak dapat mendeteksi keberadaan Carol.

Serangan yang mirip dengan *man-in-the-middle attack* dan umum terjadi pada kunci publik tanpa identitas adalah penyamaran (*impersonation attack*). Seseorang yang memiliki kunci public orang lain dapat menyamar seolah-olah dia adalah pemilik kunci tersebut.

Contohnya dalam aplikasi *e-commerce* pemesanan tiket dengan dengan sistem pembayaran menggunakan kartu kredit. Pelanggan mengirimkan informasi kartu kredit melalui *website* agen perjalanan *online*. Selama pengiriman, informasi kartu kredit tersebut dilindungi dengan cara mengenkripsinya dengan kunci publik agen perjalanan *online*. Bagaimana pelanggan memastikan *website* tersebut memang benar milik agen

perjalanan *online* dan bukan milik pihak lain yang menyamar dengan tujuan untuk mencuri informasi kartu kredit. Karena terdapat permasalahan tersebut, maka dalam penerapan kriptografi kunci public dibutuhkan pendukung yang dinamakan infrastruktur kunci publik (PKI).

PKI adalah sebuah pengaturan yang menjamin penggunaan kunci publik bagi pihak-pihak yang terlibat dengan sistem penggunaan sistem keamanan. PKI juga mengikat kunci publik dengan identitas pengguna. Dengan PKI, setiap pengguna dapat mengotentikasi satu sama lain. Informasi di dalam sertifikat yang dikeluarkan oleh PKI digunakan untuk enkripsi dan dekripsi pesan antara pihak-pihak yang berkomunikasi. Komponen PKI adalah pengguna (pemohon sertifikat dan pemakai sertifikat), sertifikat digital, CA (*Certification Authority* yaitu pihak yang mengeluarkan sertifikat digital) dan direktori untuk menyimpan sertifikat digital dan CRL (*Certificate Revocation List* berisi nomor seri sertifikat digital yang ditarik/ sudah kadaluarsa dan dianggap tidak sah).

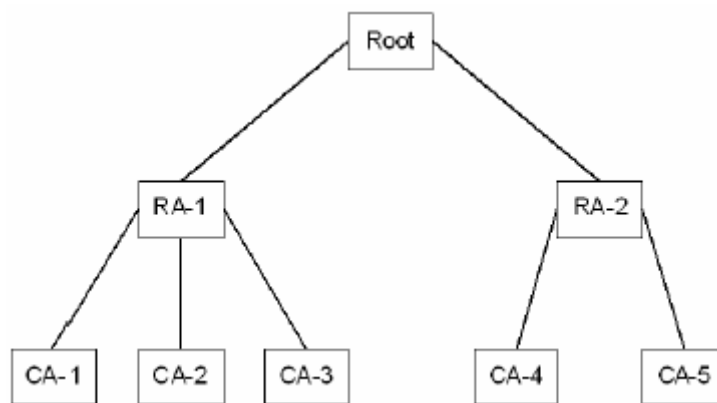
Seringkali CA adalah institusi keuangan (seperti bank) atau institusi terpercaya. PKI menyediakan cara penstrukturan komponen-komponen ini dan mendefinisikan bermacam-macam dokumen dan protokol. Sertifikat digital adalah dokumen digital yang berisi informasi name subjek (perusahaan / individu yang disertifikasi), kunci publik subjek, waktu kadaluarsa sertifikat (*expired time*), algoritma yang digunakan untuk menandatangani sertifikat dan informasi relevan lain seperti nomor seri sertifikat dan lain sebagainya. Standar untuk sertifikat telah disetujui oleh ITU (*International Telecommunication United*) dan dinamakan X.509. [HAM01]

Sertifikat digital tidak rahasia dan tersedia secara publik dan disimpan oleh CA pada direktori (*certificate repositories*). Salinan sertifikat ini dimiliki juga oleh pemohon sertifikat. Contoh sebuah sertifikat digital: Sebuah agen perjalanan *online* membawa kunci publiknya dan mendatangi CA untuk meminta sertifikat digital. CA mengeluarkan sertifikat digital dan menandatangani sertifikat tersebut dengan cara mengenkripsi nilai *hash* dari kunci publik agen perjalanan *online* (atau nilai *hash* dari sertifikat digital keseluruhan) dengan menggunakan kunci privat CA. Jadi sertifikat digital mengikat kunci publik dengan identitas pemilik kunci publik.

Supaya sertifikat digital ini dapat diverifikasi maka kunci publik CA harus diketahui secara luas. Seseorang yang memiliki kunci publik CA dapat menverifikasi bahwa tanda tangan digital di dalam suatu sertifikat sah. Contoh penggunaan sertifikat digital: Agen perjalanan *online* meletakkan salinan sertifikat digital di *website* miliknya sehingga dapat diakses oleh pengunjung *website* tersebut. Misalkan seorang pelanggan ingin membeli tiket melalui *website* agen perjalanan tersebut, dan komunikasi antara *website* agen perjalanan dengan pelanggannya berhasil diintersepsi pihak ketiga sehingga *request* dari pelanggan masuk ke *website* agen perjalanan palsu yang dibuat oleh pihak ketiga. Pihak ketiga ini meletakkan sertifikat digitalnya pada *website* palsu, tetapi ketika pelanggan membaca sertifikat digital tersebut dia langsung paham bahwa dirinya sedang tidak berkomunikasi dengan agen perjalanan asli karena identitas agen perjalanan tidak terdapat pada sertifikat tersebut. Misalkan pihak ketiga tersebut

berhasil mengubah *website* agen perjalanan dan mengganti kunci publik milik agen perjalanan pada sertifikat digital.

Ketika pelanggan meng*hash* sertifikat digital tersebut dia memperoleh nilai *hash* yang tidak sama dengan nilai *hash* yang dihasilkan jika tanda tangan digital diverifikasi dengan kunci publik CA. Pihak ketiga tidak memiliki kunci privat CA sehingga pelanggan dapat meyakini apakah dia memperoleh kunci publik agen perjalanan yang asli atau tidak. Adanya waktu kadaluarsa pada sertifikat digital dimaksudkan agar pengguna mengubah kunci publik dan kunci privat pasangannya secara periodik dan jika kunci privat berhasil diketahui pihak lain sebelum waktu kadaluarsa habis maka sertifikat digital harus ditarik. CA mengeluarkan daftar sertifikat digital yang ditarik secara periodik dengan mengeluarkan CRL. Protokol OCSP (*Online Certificate Status Protocol*) memungkinkan pemeriksaan sertifikat secara *real time* sehingga lebih efisien dari pada pemeriksaan CRL secara tradisional. Tentunya tidak mungkin hanya ada satu CA untuk melayani sertifikat digital dari seluruh dunia.



Hierarki CA dalam PKI

Pada level tertinggi terdapat *root* yang merupakan *root certificate authority*, yaitu *Internet Policy Registration Authority* (IRPA). Root mensertifikasi CA level satu (RA / *Registry Authorities*) menggunakan kunci privat *root* (*root key*). RA bertindak sebagai *policy creation authority*, yaitu organisasi yang membuat kebijakan untuk memperoleh sertifikat digital. Sebuah RA mungkin mencakup beberapa area seperti negara bagian, negara atau benua. RA menandatangani sertifikat digital untuk CA di bawahnya dengan menggunakan kunci privat RA. CA menandatangani sertifikat digital untuk individu atau organisasi dengan menggunakan kunci privat CA. Selain itu, CA bertanggung jawab untuk otentikasi sertifikat digital, sehingga CA harus memeriksa informasi secara hati-hati sebelum mengeluarkan sertifikat digital

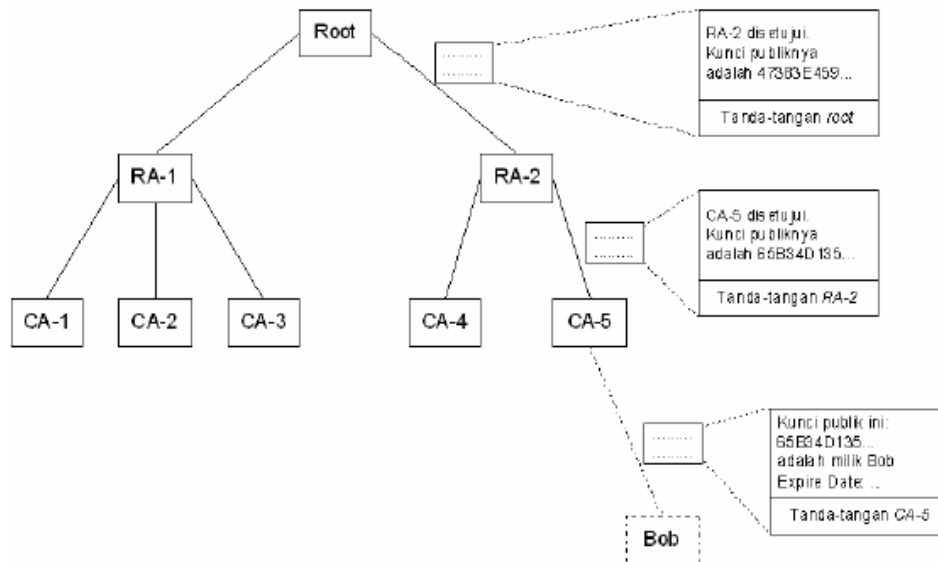
Verifikasi sertifikat digital dilakukan dari daun menuju akar (*root*). Misalkan pelanggan memerlukan kunci publik agen perjalanan online untuk melakukan pemesanan tiket, lalu

dia mencari dan menemukan sertifikat agen perjalanan tersebut ditandatangani oleh CA-5. Pelanggan kemudian menandatangani CA-5 dan meminta bukti legitimasi CA-5. CA-5 merespon dengan memperlihatkan sertifikat digital yang diperoleh dari RA-2, di dalamnya ada kunci publik CA-5 yang ditandatangani oleh RA-2.

Dengan menggunakan kunci publik CA-5, pelanggan dapat memverifikasi sertifikat digital agen perjalanan yang ditandatangani oleh CA-5 dan mendapatkan hasil bahwa sertifikat tersebut sah. Langkah berikutnya, pelanggan mendatangi RA-2 dan meminta bukti legitimasi RA-2.

RA-2 merespon dengan memperlihatkan sertifikat digital yang diperoleh dari *root*, di dalamnya terdapat kunci publik RA-2 yang ditandatangani oleh *root*.

Pelanggan memverifikasi sertifikat digital RA-2 dengan menggunakan kunci public *root* dan mendapatkan hasil bahwa sertifikat digital tersebut sah. Pelanggan akhirnya yakin bahwa dia sudah memiliki kunci publik agen perjalanan. Rantai sertifikat yang menuju ke *root* disebut *chain of trust* atau *certification path*



Contoh rantai sertifikat digital

Tanda Tangan Digital (*Digital Signature*)

Salah satu aplikasi kriptografi kunci publik, yang dapat memberikan aspek keamanan adalah tanda tangan digital. Penandatanganan pesan dapat dilakukan dengan dua cara, yaitu dengan mengenkripsi pesan atau dengan cara menggunakan fungsi *hash* dan kriptografi kunci publik

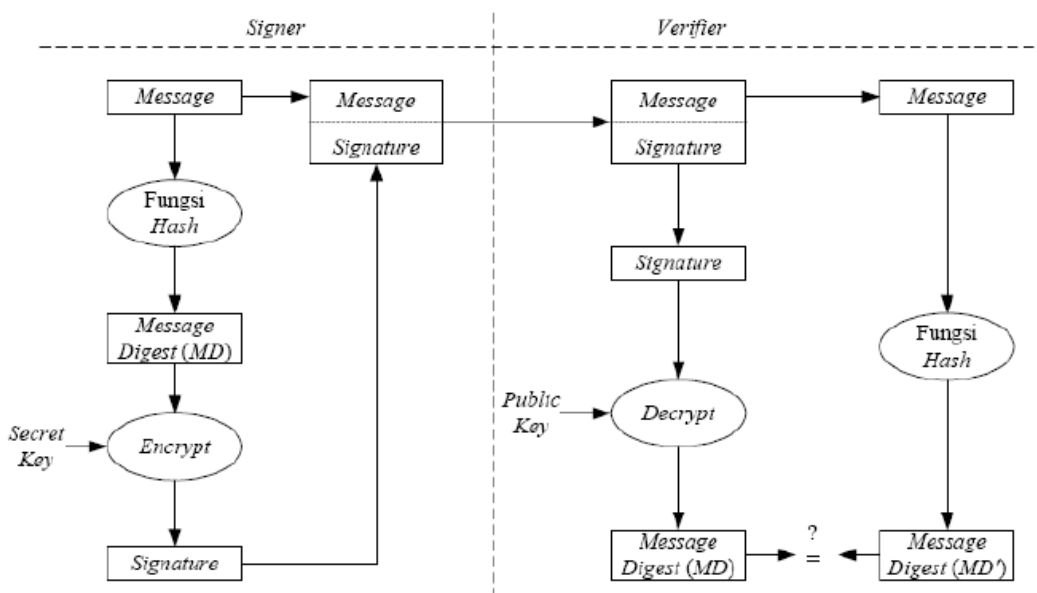
Penandatanganan pesan dengan cara mengenkripsinya menggunakan kriptografi kunci publik dapat memberikan fungsi kerahasiaan pesan, otentikasi, dan nirpenyangkalan. Kerahasiaan pesan tentunya terjamin karena setelah dienkripsi pesan tidak dapat

diketahui maknanya. Agar dapat menjamin otentikasi maka pesan dienkripsi dengan kunci privat

karena sifatnya rahasia. Dengan demikian, kebenaran pihak-pihak yang berkomunikasi dan kebenaran sumber pesan dapat dijamin. Agar tanda-tangan digital dapat memberikan fungsi integritas data maka tanda tangan digital memanfaatkan fungsi *hash*. Fungsi *hash* adalah fungsi yang menerima masukan *string* dan menghasilkan *string* keluaran yang disebut dengan nilai *hash*. Jika *string* masukan dari fungsi *hash* diubah maka akan dihasilkan nilai *hash* yang berbeda. Dengan demikian fungsi integritas pesan dapat diberikan oleh fungsi *hash*. [Cole]

Langkah-langkah pemberian tanda tangan digital adalah sebagai berikut:

- Pesan yang diubah terlebih dahulu menjadi *message digest MD*.
- Message digest MD* dienkripsikan dengan algoritma kunci publik menggunakan kunci rahasia (*SK*) pengirim menjadi tanda tangan digital
- Pesan *M* disambung (*append*) dengan tanda tangan digital *S*.



Otentifikasi tanda tangan digital menggunakan fungsi hash

Selanjutnya,

langkah-langkah untuk melakukan otentikasi adalah sebagai berikut:

a. Tanda tangan digital *S* didekripsi dengan menggunakan kunci publik (*PK*) pengirim pesan, menghasilkan *message digest* semula, yaitu *MD*.

b. Pesan *M* diubah menjadi *message digest MD'* menggunakan fungsi *hash* satu arah yang sama dengan fungsi *hash* yang digunakan oleh pengirim.

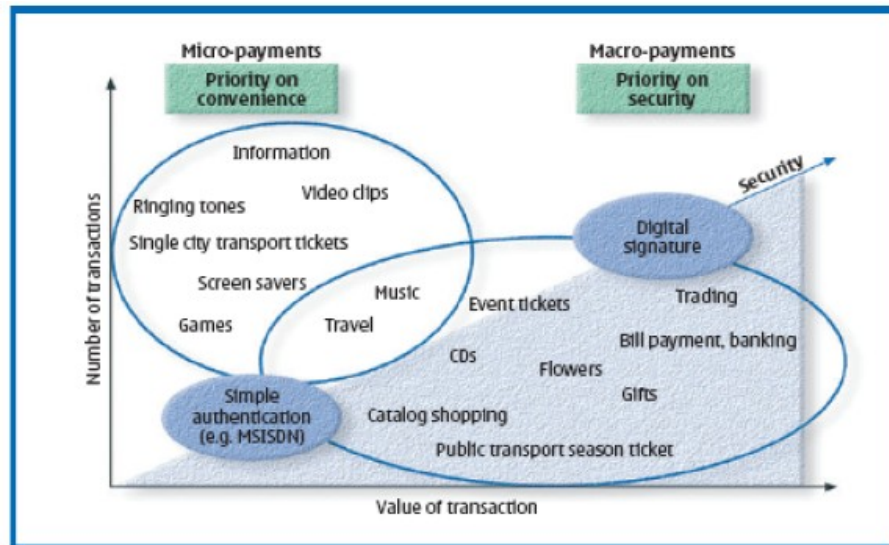
c. Jika $MD' = MD$, berarti pesan yang diterima otentik dan berasal dari pengirim yang benar. Apabila pesan M yang diterima sudah berubah maka MD' yang dihasilkan dari fungsi *hash* berbeda dengan MD semula. Ini berarti pesan tidak asli lagi. Apabila pesan M tidak berasal dari orang yang sebenarnya maka MD akan berbeda dengan MD' karena kunci publik yang digunakan oleh penerima pesan tidak berkoresponden dengan kunci privat pengirim. Andaikan pengirim pesan M menyangkal telah mengirim pesan, maka sangkalan tersebut dapat dibantah dengan cara berikut: jika ia tidak mengirim pesan, berarti ia tidak mengenkripsi MD dengan kunci privatnya. Faktanya kunci publik yang berkoresponden dengan kunci privat pengirim akan menghasilkan $MD=MD'$ ini berarti MD memang benar dienkripsi oleh pengirim karena hanya pengirimlah yang mengetahui kunci privatnya sendiri.

4. Hambatan Penerapan kriptografi pada e-commerce

Secara umum hambatan penerapan kriptografi pada e-commerce hampir tidak ada. Satu-satunya hambatan ialah jika kita mulai berbicara tentang mobile commerce di mana jaringan nirkabel memiliki beberapa batasan

Pada jaringan kabel terdapat beberapa asumsi yaitu *client* memiliki kemampuan komputasi, *bandwith*, *latency* yang tinggi dan tempat penyimpanan yang cukup. Hal ini bertolak belakang dengan perangkat nir kabel yang memiliki bandwith terbatas, kemampuan komputasi terbatas, memiliki sumber tenaga berupa baterai. Oleh karena itu, banyak aplikasi kriptografi pada jaringan kabel yang harus dioptimasi supaya berjalan dengan efisien pada perangkat nir kabel tetapi harus *compatible* dengan aplikasi pada jaringan kabel. Karena adanya keterbatasan kemampuan komputasi maka algoritma kriptografi yang dapat digunakan pada aplikasi *mobile commerce* menjadi terbatas bergantung dari karakteristik algoritma tersebut.

Keterbatasan *bandwith* juga membatasi ukuran pesan. Keterbatasan yang keempat adalah ruang penyimpanan yang terbatas pada perangkat seperti telepon seluler dan PDA.



Berbagai aplikasi pada tingkat keamanan yang berbeda

5. Kriptografi pada teknologi pendukung *Mobile commerce*

SIM Application Toolkit (SAT)

SIM misalnya pada GSM menyimpan data personal pemilik kartu dan dapat diimplementasikan dalam bentuk kartu cerdas (*smart card*) yang sering disebut kartu SIM. *SIM toolkit* merupakan spesifikasi SIM dan fungsionalitas terminal yang memungkinkan SIM mengendalikan perangkat *mobile* untuk beberapa fungsi tertentu. *SIM Application Toolkit (SAT)* digunakan untuk membuat aplikasi *mobile commerce* berbasis *ShortMessage Service (SMS)*.

Dalam sistem berbasis SAT komunikasi antara *mobile client* dan penyedia layanan dilakukan melalui SMS. SMS digunakan untuk mengidentifikasi dan mengotorisasi pembayaran. Pengguna diidentifikasi dan diotentikasi oleh layanan otentikasi GSM sehingga operator seluler GSM bertindak sebagai perantara antara *mobile client*, *server* untuk pembayaran, dan penjual layanan. SAT menyediakan layanan kerahasiaan, otentikasi, *message replay protection*, integritas, tetapi tidak menjamin nirpenyangkalan. Hal ini adalah yang menjadi faktor kelemahan utama pada aplikasi *mobile commerce* berdasarkan SAT.

Selain tidak mampu menjamin nirpenyangkalan, SAT juga memiliki kelemahan karena penggunaan kode PIN pada perangkat *mobile client*. Kode PIN ini biasanya berupa angka 4 digit yang dapat ditebak dengan relatif mudah oleh pencuri perangkat *mobile*.

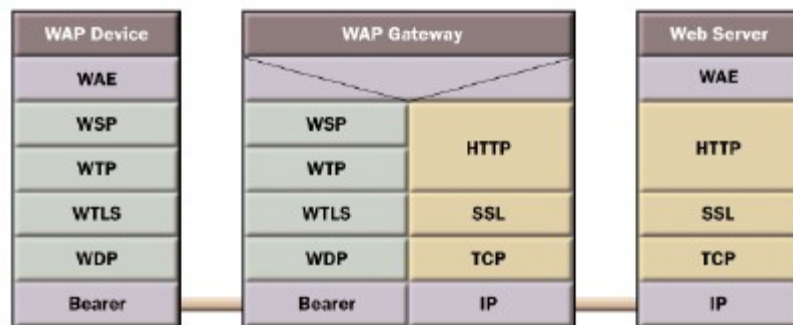
Pada SIM kebutuhan keamanan dapat mengatasi masalah keamanan umum pada *transport Layer* seperti *peer authentication*, integritas pesan, deteksi balasan dan integritas urutan, bukti penerimaan dan kerahasiaan pesan. Setiap pesan dari aplikasi

dibagi ke dalam paket yang masing-masing dijamin keamanannya dengan melindungi isi pesan dan menambahkan *header* untuk keamanan. Akan tetapi, nirpenyangkalan tidak didukung sehingga harus diimplementasikan pada level aplikasi.

Pengirim dan penerima pesan diidentifikasi sehingga penyerang tidak dapat mencoba memalsukan kecuali jika mengkloning kartu SIM. Jadi pesan SMS dapat digunakan untuk otentikasi. Lebih jauh lagi data SMS dienkripsi untuk menjamin kerahasiaan data. Meskipun demikian, perlindungan ini berakhir pada jaringan, tidak ada keamanan *end-to-end* dan operator seluler dan infrastrukturnya harus dipercaya ketika tidak ada lagi perlindungan terhadap pesan SMS.

Wireless Application Protocol (WAP)

WAP digunakan secara luas oleh piranti mobile untuk mengakses internet. Karena dirancang untuk tampilan dan sistem kecil dengan bandwidth terbatas, WAP tidak didesain untuk menampilkan data berkapasitas besar. WAP digunakan untuk browsing jaringan melalui TV dan dalam tampilan otomotif. Mengacu pada keterbatasan memori dan prosesor yang peralatan mobile, WAP membutuhkan lebih sedikit overhead ketimbang TCP/IP.



Arsitektur WAP 1.x

WAP versi 1.x menggunakan protokol WTLS untuk menjamin keamanan pesan dari perangkat *mobile* ke *WAP gateway*. *WAP gateway* akan mentransformasikan pesan dalam format WAP ke dalam TCP/IP, meneruskan data ke jaringan kabel dan berkomunikasi dengan *web server* yang diakses oleh perangkat *mobile*.

a. WPKI (Wireless Public Key Infrastructure)

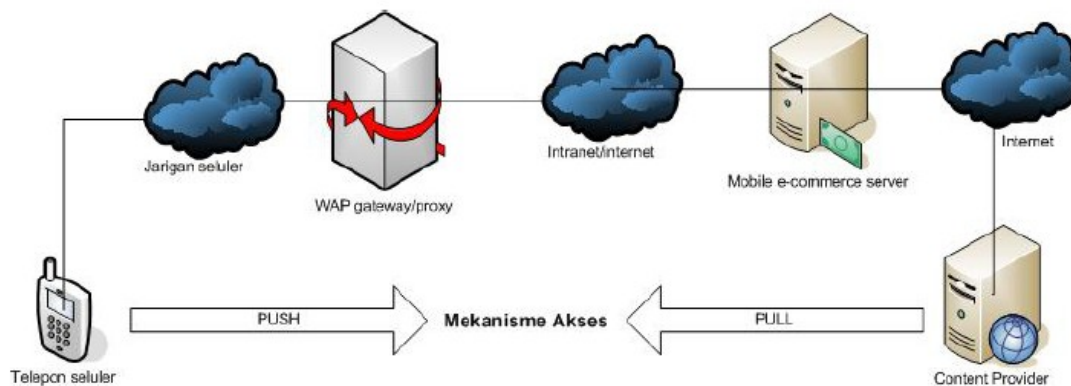
WPKI merupakan ekstensi dari PKI, yang dibuat khusus untuk jaringan nirkabel. WPKI memerlukan komponen yang sama dengan PKI yang telah dijelaskan sebelumnya. Namun pada WPKI, *registration authority* (RA) diimplementasikan berbeda dan terdapat entitas baru yaitu PKI Portal. PKI Portal dapat seperti sistem pada dua jaringan seperti halnya *WAP gateway*. PKI Portal berfungsi sebagai RA dan bertanggung jawab untuk

menterjemahkan pesan dari *client* kepada RA dan berinteraksi dengan CA pada jaringan kabel. RA mevalidasi aplikasi, apakah permintaannya untuk memperoleh sertifikat digital dikabulkan atau ditolak.

b. WTLS (*Wireless Transport Layer Security*)

Protokol WTLS merupakan protokol yang mendukung WPKI dan didesain untuk menjamin keamanan komunikasi dan transaksi melalui jaringan nirkabel. Seperti dapat dilihat pada arsitektur WAP 1.X, WTLS terdapat pada *transport Layer* antara WAP *client* pada perangkat *mobile* dengan WAP *server* pada WAP *gateway*. WTLS menyediakan fungsionalitas yang mirip dengan fungsi *Layer* keamanan pada internet yaitu TLS/SSL. WTLS dibuat berdasarkan TLS dan dioptimasi untuk komunikasi nirkabel, mendukung *datagram*, memiliki protokol *handshake* yang dioptimasi dan memiliki mekanisme *dynamic key refreshing*. [HAM01]

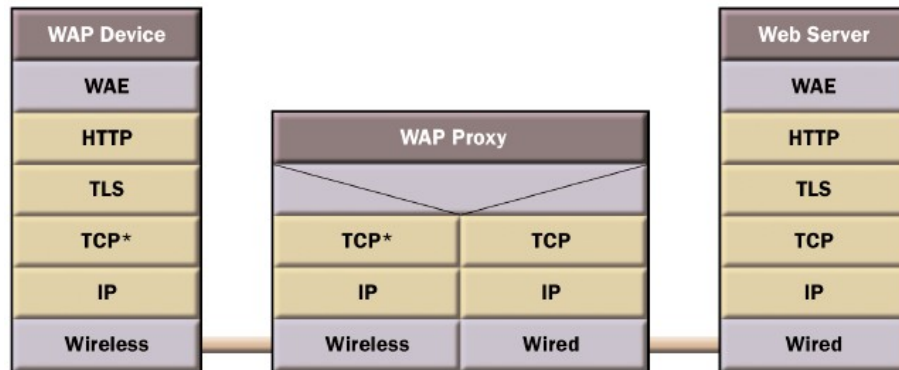
Dynamic key refreshing merupakan sebuah mekanisme yang memungkinkan pengubahan kunci enkripsi dan otentikasi dalam rentang waktu tertentu. Hal ini akan mengurangi kemungkinan *eavesdropper* mendekripsi pesan karena kunci yang berbeda digunakan pada sebuah sesi.



Contoh arsitektur *mobile commerce* yang memanfaatkan WAP 1.x

Pada gambar di atas ketika terjadi transaksi yang melibatkan data rahasia seperti nomor *credit card*, *password*, alamat, data ditransmisikan lewat jaringan, sehingga pertukaran informasi ini harus dijamin keamanannya. Ada beberapa bagian dimana masalah keamanan memiliki peran penting yaitu bagian yang berhubungan dengan komunikasi lewat jaringan nirkabel, keamanan *gateway*, koneksi ke *server*, dan masalah keamanan aplikasi yang berjalan di *server*. Keamanan komunikasi lewat jaringan nirkabel dijamin oleh *Layer* WTLS. *Gateway* umumnya merupakan milik operator seluler sehingga pengembang tidak memiliki kontrol terhadap komponen ini. Peran dari WAP *gateway* adalah menghubungkan jaringan nirkabel dengan jaringan IP. Dengan demikian, data terenkripsi dari jaringan nirkabel akan di dekripsi pada *gateway*, kemudian dienkripsi kembali dengan memanfaatkan SSL untuk dikirim melalui internet. Pada rentang waktu yang singkat terdapat data plainteks pada *gateway*.

Karena adanya ancaman keamanan pada WAP *gateway* seperti yang telah dijelaskan di atas, maka pada versi 2.0 WAP menggunakan WAP TLS *profile*. Dengan adanya TLS *tunneling* ini maka dimungkinkan keamanan end-to-end antara *client* dan *server*.



Arsitektur WAP 2.0

Pada WAP, keamanan dijamin lewat protokol WTLS (pada WAP 1.x) dan WAP TLS *Profile* (pada WAP 2.0). Protokol ini menyediakan layanan keamanan integritas data, kerahasiaan dan otentikasi. Salah satu persoalan keamanan pada WAP 1.x yang dikenal dengan “WAP *gap*” disebabkan oleh adanya saat dimana pesan berada dalam bentuk plaintext pada Wap *gateway* ketika sedang dikonversi. Namun, hal ini sudah diatasi pada WAP 2.0.

6. Kesimpulan dan Saran

Pada makalah ini telah coba diuraikan beberapa teknik kriptografi pada electronic commerce sehingga memungkinkan komunikasi yang aman. Berikut ini adalah kesimpulan yang diambil dan beberapa usulan yang mungkin dapat digunakan untuk mengatasi kelemahan yang ada:

- a. Untuk penerapan kriptografi pada e-commerce hampir bisa dikatakan tidak ada hambatan yang signifikan. Satu-satunya hambatan ialah jika kita mulai berbicara tentang mobile commerce di mana jaringan nirkabel memiliki beberapa batasan
 - 1 b. Penerapan kriptografi pada aplikasi mobile commerce memanfaatkan aplikasi kriptografi pada jaringan kabel, tetapi diadaptasi dan dioptimasi sehingga dapat berjalan secara efisien pada aplikasi mobile commerce. Bentuk adaptasi/optimasi misalnya implementasi kriptografi pada perangkat keras misalnya smart card,
 - 2 c. Tingkat jaminan keamanan yang diimplementasikan hendaknya disesuaikan dengan nilai dari transaksi yang dilakukan karena dalam menjamin keamanan ini sering kali dibutuhkan resource yang relatif besar. Aplikasi mobile commerce yang melibatkan

nilai transaksi yang kecil dapat dikembangkan dengan SAT sedangkan pada aplikasi yang nilai transaksinya besar dapat dikembangkan menggunakan Wap 2.0 dengan penggunaan teknik kriptografi yang sesuai.

3 d. Umumnya pada aplikasi mobile commerce masih terdapat kurangnya otentikasi yang lengkap. Perangkat mobile dan server umumnya mengotentikasi dirinya masing-masing, tetapi pengguna biasanya tidak perlu membuktikan dirinya kepada telepon seluler. Oleh karena itu, seharusnya sebelum menggunakan aplikasi pengguna harus diotentikasi, hal ini penting karena perangkat mobile sering kali hilang atau dicuri. Dengan demikian, akses yang tidak terotorisasi pada data yang disimpan oleh aplikasi mobile commerce pada device dapat dicegah.

e. Pada jaringan nirkabel terdapat beberapa kekurangan yaitu *client* memiliki kemampuan komputasi, *bandwith*, *latency* yang rendah dan tempat penyimpanan yang relative kecil. Kemampuan komputasi yang terbatas mengakibatkan terbatasnya jenis algoritma yang dapat dilakukan. Oleh karena itu, algoritma yang digunakan harus membutuhkan biaya komputasi yang kecil, tetapi tetap dapat memberikan jaminan keamanan yang dibutuhkan. Keterbatasan *bandwith* juga membatasi ukuran pesan. Hal ini mengakibatkan sertifikat pada aplikasi seperti *mobile commere* sedikit berbeda dan pengiriman rantai sertifikat misalnya url sertifikat tidak dilakukan. Karena adanya keterbatasan *latency* pada jaringan nirkabel, maka protokol kriptografi yang diterapkan sebaiknya memiliki jumlah pesan dan pertukaran pesan yang lebih sedikit. Dan tentang ruang penyimpanan yang terbatas, dalam menerapkan kriptografi kode yang dibutuhkan harus diminimumkan misalnya memanfaatkan kode yang dioptimasi untuk *platform* perangkat *mobile*.

Daftar Referensi

[HAM01] Paper “**PKI Solution for Mobile Systems**” by Hammarstedt, Christian dan Jonas Stewen. 2001.. Växjö University . Diakses tanggal 20 April 2009

[Cole]Cole, Krutz, and Conley . 2005. **Network Security Bible**.Wiley Publishing, Inc., Indianapolis, 2005

[Al-Ba]Paper ”**A Novel Security Model Combining Cryptography and Steganography**” by H. Al-Barhmtoshy*, E. Osman** and M. Ezzat**Diakses tanggal 20 April 2009

Presentation “CH-2: Conventional Encryption: Classical Techs.ppt” by H. Yoon Diakses tanggal 20 April 2009