Analisis Penerapan Manajemen Kunci pada Kriptografi di Aplikasi *m-commerce*

Gahayu Handari Ekaputri [1)]

1) Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung Jl.Ganesa 10 Bandung, Indonesia. Email: if14031@students.if.itb.ac.id

Abstract – *Kriptografi sudah kian berkembang dan makin banyak diterapkan pada berbagai aplikasi di dunia nyata, salah satunya adalah aplikasi m-commerce. m-commerce merupakan suatu media untuk melakukan transaksi keuangan yang diaplikasikan pada suatu perangkat bergerak. Pada saat ini perkembangan m-commerce semakin meningkat, karenanya dibutuhkan suatu kriptografi yang dapat mengamankan setiap transaksi yang terjadi melalui m-commerce ini.*

Kekuatan sistem kriptografi sendiri secara total bergantung pada keamanan kunci. Oleh karena itu, kunci perlu dilindungi selama fase daur hidupnya. Daur hidup kunci dimulai dari saat pembangkitan kunci (generation) hingga ketika kunci tidak diperlukan lagi untuk kemudian dihancurkan (destruction). Secara umum, daur hidup kunci terdiri dari pembangkitan, penyebaran, penyimpanan, penggunaan, perubahan, dan penghancuran kunci.

Makalah ini membahas tentang analisis penerapan manajemen kunci tersebut di m-commerce. Kajian ini meliputi bagaimana pembangkitan kunci dilakukan pada m-commerce, dilanjutkan dengan bagaimana mekanisme penyebaran kunci dilakukan pada m-commerce, penyimpanan kunci, pemakaian kunci, perubahan dan bagaimana penghancuran kunci dilakukan pada aplikasi m-commerce

Kata Kunci*: kriptografi, kunci, m-commerce, manajemen kunci*

1. PENDAHULUAN

Kian hari, penetrasi penggunaan telepon seluler saat ini semakin tinggi, serta diproyeksikan masih memiliki tingkat pertumbuhan yang tinggi pula. Tercatat saat ini terdapat 1 Miliar pengguna di seluruh dunia, dan 28 Juta pengguna di Indonesia. Sehingga merupakan suatu langkah yang tepat apabila selanjutnya banyak entitas bisnis,perbankan, dan finansial yang kemudian mencoba untuk memberdayakan telepon seluler sebagai suatu media transaksi yang baru. [6]

Aplikasi *e-commerce* juga kian berkembang seiring dengan kemajuan teknologi yang ada, khususnya internet. *E-commerce* saat ini semakin banyak diimplementasikan pada perangkat *mobile* seperti telepon seluler,mengingat semakin tingginya jumlah pengguna selular saat ini, sehingga diharapkan pengguna *e-commerce* pun menjadi semakin besar. Aplikasi *e-commerce* ini karena diimplementasikan pada suatu perangkat *mobile* sering disebut dengan *mobile commerce* atau *m-commerce*. Aplikasi ini banyak dikembangkan dengan memanfaatkan berbagai *platform* seperti Wap, *i-mode* dan Java *Mobile Edition*.

Pada aplikasi seperti ini, masalah keamanan yang muncul meliputi bagaimana menjamin keamanan otentikasi, nirpenyangkalan, kerahasian serta integritas data transaksi antara perangkat *mobile* dan *web server* dan juga keamanan data yang tersimpan pada perangkat *mobile*. Untuk mengatasi masalah ini telah dikembangkan solusi keamanan yang memanfaatkan kriptografi seperti *Wireless Public Key Infrastructure* (PKI), *Wireless Transport Layer Security* (WTLS), penggunaaan kriptografi pada level aplikasi atau pada perangkat keras.[5]

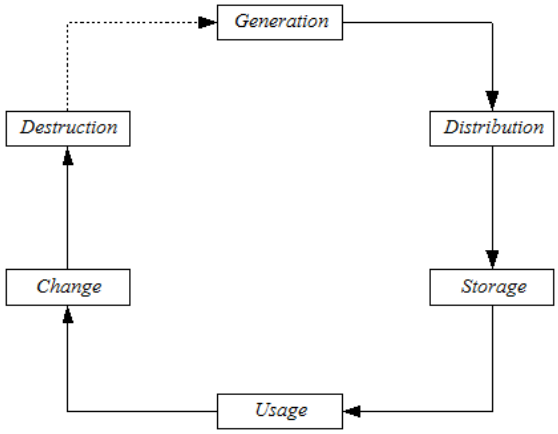
Seiring dengan besarnya laju arus informasi, kriptografi telah kian berkembang, dan banyak sekali aplikasi kehidupan yang memanfaatkan kriptografi sebagai teknik untuk menjamin keamanan informasi. Kriptografi telah diterapkan dalam mekanisme kerja berbagai aplikasi dalam kehidupan sehari-hari, seperti anjungan tunai mandiri, komunikasi telepon seluler, *e-commerce* di internet, kartu cerdas, *pay* TV, dan lainnya. Pada makalah ini yang akan dibahas adalah penerapan kriptografi pada aplikasi *m-commerce*, khususnya pada penerapan manajemen kunci di dalamnya.

Manajemen kunci dipilih sebagai topik bahasan karena tidak dipungkiri, bahwa keamanan dari kriptografi bergantung pada keamanan kunci, dimana sebagaimana diketahui bahwa kunci juga memiliki suatu fase kehidupan. Fase kehidupan inilah yang menjadi penting untuk dibicarakan dan disebut dengan manajemen kunci. Manajemen kunci berlangsung dari bagaimana suatu kunci dibangkitkan, didistribusikan, disimpan, digunakan, diubah, hingga kunci tersebut dihancurkan. Karenanya perlu dianalisis bagaimana penerapan manajemen kunci tersebut dalam aplikasi *m-commerce*.

2. LANDASAN TEORI

2.1. Manajemen Kunci

Seperti sudah disebutkan sebelumnya, kekuatan sistem kriptografi secara total bergantung pada keamanan kunci. Kunci adalah parameter yang digunakan utnuk melakukan transformasi enkripsi dan dekripsi. Karenanya, kunci perlu dilindungi selama fase daur hidupnya.Daur hidup kunci sendiri dimulai dari pembangkitan kunci (*generation*) sampai kunci tidak diperlukan lagi untuk kemudian dihancurkan (*destruction*). Secara garis besar, daur hidup kunci digambarkan sebagai berikut: [1]



Gambar 1 Daur hidup kunci

Tujuan manajemen kunci adalah menjaga keamanan dan integritas kunci pada semua fase di dalam daur hidupnya. Pada umumnya setiap kunci akhirnya diganti dengan kunci lain. Jadi, keseluruhan fase membentuk siklus (lingkaran) karena penghancuran kunci biasanya diikuti dengan penggantiannya dengan kunci baru (garis putus-putus). [1]

Masalah utama yang muncul pada tahapan pembangkitan kunci adalah bagaimana membuat kunci yang tidak dapat diprediksi. Pada algoritma kunci-publik, pembangkitan kunci merupakan masalah tersendiri, karena pembangkitan kunci membutuhkan perhitungan matematis yang rumit. Selain itu, pembangkitan bilangan prima yang besar juga dibutuhkan untuk membentuk kunci. Oleh karena itu, pada algoritma kunci-publik dibutuhkan program khusus untuk membangkitkan kunci. Pembangkitan kunci pada algoritma simetri jauh lebih mudah daripada pembangkitan kunci pada algoritma kunci-publik. Karena kunci simetri umumnya terdiri dari rangkaian bit atau rangkaian karakter, maka setiap pengguna dapat membangkitkan kuncinya sendiri.

Pada tahapan penyebaran kunci, protokol kriptografi dapat digunakan untuk mendistribusikan kunci. Sementara pada tahapan penyimpanan kunci, kunci harus disimpan di tempat yang aman yang tidak memungkinkan pihak lawan untuk mengaksesnya. Oleh karena itu, penyimpanan kunci mungkin memerlukan perlindungan secara fisik. Selain perlindungan secara fisik, kunci juga dapat disimpan di dalam *smart card* yang hanya dapat dibaca dengan menggunakan suatu kode rahasia tertentu.

Pada tahapan penyimpanan kunci, kunci sebaiknya disimpan tidak dalam bentuk jelas. Ada dua solusi alternatif untuk masalah ini. Pertama, kunci disimpan dengan mengenkripsinya dengan menggunakan kunci lain. Kedua, kunci dipecah menjadi beberapa komponen, setiap komponen disimpan di tempat terpisah.

Pada tahapan penggunaan kunci, supaya setiap kunci mempunyai penggunaan yang unik, maka kita perlu membeli label pada setiap kunci. Dalam hal ini label menspesifikasikan penggunaan kunci. Kunci sebaiknya diubah secara periodik dan teratur. Sistem kriptografi harus mempunyai kemampuan untuk mengubah kunci. Kunci diubah secara teratur untuk membatasi lama keberadaanya dan mengurangi nilainya dimata penyerang. Setiap kunci seharusnya diubah jauh sebelum dapat ditemukan dengan cara *exhaustive search*.

Pada fase penghancuran kunci, Kunci yang tidak dibutuhkan lagi seharusnya dihancurkan dengan cara yang aman, sehingga ia tidak mungkin ditemukan kembali secara fisik maupun secara elektronik.

2.2. Aplikasi Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara mengenkripsinya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. [1] Terdapat empat hal penting yang menjadi aspek keamana yang disediakan oleh kriptografi. Keempat hal tersebut adalah kerahasiaan, integritas data, otentikasi, dan nirpenyangkalan. Suatu sistem kriptografi harus menjamin keempat hal tersebut ada dan terjaga.[2]

Dapat dikatakan bahwa kehidupan saat ini sudah dikelilingi oleh kriptografi, mengingat akan pentingnya menjaga sekuritas dari suatu informasi tertentu. Terdapat berbagai contoh penerapan kriptografi dalam kehidupan sehari-hari, seperti Anjungan Tunai Mandiri, dimana setiap transaksi keuangan yang terjadi di dalamnya harus berlangsung secara rahasia dari orang-orang yang tidak berhak mengetahuinya sehingga perlu mendapatkan perlindungan kriptografi; komputer di laboratorium atau kantor, dimana perlu terdapat mekanisme otentikasi tertentu untuk menjamin hanya orang yang berhak yang dapat mengaksesnya, dan ini memerlukan kriptografi di dalamnya; telepon selular, mengingat pesan yang dikirimkan oleh pengirim merupakan pesan rahasia yang memang ditujukan hanya untuk penerima, karenanya terdapat kriptografi untuk memastikan hanya orang yang berhak yang menerima panggilan pesan tersebut, dan pesan tersebut diterima

secara utuh; aplikasi internet khususnya untuk perdagangan yang sering disebut sebagai aplikasi *e-commerce*, aplikasi ini memerlukan kriptografi untuk mencegah terjadinya nirpenyangkalan juga keamanan dari setiap transaksi perdagangan yang terjadi di internet, mengingat semakin luasnya internet dan semakin hebatnya bagaimana informasi dapat mengalir melalui teknologi internet ini.

2.3. *m-commerce*

m-commerce merupakan proses transaksi yang dilakukan dengan menggunakan perangkat mobile. *M-commerce* merupakan subset dari *e-commerce*, dan didefinisikan sebagai proses transaksi yang dilakukan secara elektronik, baik melalui internet, smart card maupun perangkat mobile melaui jaringan seluler. Pada umumnya, perangkat pengguna yang digunakan pada proses *m-commerce* antara lain *Handphone, Personal Digital Assistant*, atau *Smartphone.* [4]

M-commerce menciptakan kesempatan untuk memberikan layanan baru pada konsumen, mengingat penggunaan perangkat mobile yang kian tinggi *M-commerce* merupakan semua transaksi (yang memiliki niai uang) baik secara langsung maupun tidak langsung melalui jaringan komunikasi nirkabel.

Fitur yang ditawarkan dalam *m-commerce* adalah: [3]

- *Mobility* : pengguna memakai perangkat mobile yang memungkinkan terjadinya transaksi dengan mobilitas tinggi
- *Broad reachability* : pengguna dapat diakses dan mengakses transaksi kapan pun
- *Ubiquity*: pengaksesan informasi yang lebih mudah dalam lingkungan sistem waktu nyata
- *Convenienc*e: ukuran dan berat perangkat yang menyimpan data dan memiliki koneksi internet membuat pengguna nyaman.
- *Localization of products and services*: mengetahui dimana pengguna berada pada waktu tertentu (diterapkannya *location based services*)

Berbagai aplikasi dalam *m-commerce* telah dikelaskan dalam suatu kelas tertentu yang dapat dilihat pada gambar berikut:[4]

Class of Applications	Examples
Mobile financial applications (B2C, B2B)	Banking, brokerage, and payments for mobile users
Mobile advertising (B2C)	Sending user-specific and location-sensitive advertisements to users
Mobile inventory management (B2C, B2B)	Location tracking of goods, boxes, troops, and people
Proactive service management (B2C, B2B)	Transmission of information related to distributing components to vendors
Product locating and shopping (B2C, B2B)	Locating/ordering certain items from a mobile device
Wireless reengineering (B2C, B2B)	Improvement of business services
Mobile auction or reverse auction (B2C)	Services for customers to buy or sell certain items
Mobile entertainment services (B2C)	Video-on-demand and other services to a mobile user
Mobile office (B2C)	Working from traffic jams, airport, and conferences
Mobile distance education (B2C)	Taking a class using streaming audio and video
Wireless data center (B2C, B2B)	Information can be downloaded by mobile users/vendors
Mobile music/music-on-demand (B2C)	Downloading and playing music using a mobile device

Gambar 2 Kelas Aplikasi *m-commerce*

m-commerce juga memiliki beberapa kekurangan: [6]

- Keterbatasan perangkat.
- Tingkat keberagaman perangkat, jaringan dan sistem operasi yang sangat tinggi, membutuhkan standardisasi *platform*.
- Tingginya kehilangan/pencurian perangkat
- Bertambahn tingkat kerawanan terhadap sekuritas ketika data ditransfer melalui *air interface*.

Tahapan proses pada *m-commerce* dapat dibedakan menjadi 4 tahap sebagai berikut: [6]

1. Set-up dan Konfigurasi

Proses ini termasuk instalasi aplikasi khusus pada perangkat yang akan digunakan pada *m-commerce*. Selain itu, untuk beberapa sistem *m-commerce* proses ini juga melibatkan proses pembelian atau penambahan nilai uang pada aplikasi tersebut.

2. Inisiasi Pembayaran

Pada tahap ini informasi pembayaran dikirimkan melalui jaringan seluler kepada *merchant*.

3. Authentikasi

Pada tahap ini diperiksa apakah pengguna memang berhak melakukan transaksi, serta memenuhi persyaratan finansial tertentu. Pada sebagian sistem pembayaran, proses ini melibatkan otentikasi berdasarkan *SIM Card.*

4. Penyelesaian Pembayaran

Proses ini dilakukan ketika pengguna telah berhasil di-otentikasi, demikian juga transaksi itu sendiri telah berhasil diotentikasi.

2.4.Kriptografi pada *m-commerce*

Penerapan kriptografi pada jaringan nirkabel yang merupakan lingkungan aplikasi *m-commerce* digunakan, lebih sulit dari pada penerapan kriptografi pada jaringan kabel karena terdapat berbagai batasan. Oleh karena itu, banyak aplikasi kriptografi pada jaringan kabel yang harus dioptimasi supaya berjalan dengan efisien pada perangkat nir kabel tetapi harus sesuai dengan aplikasi pada jaringan kabel.

Karena adanya keterbatasan kemampuan komputasi maka algoritma kriptografi yang dapat digunakan pada aplikasi *m-commerce* menjadi terbatas bergantung dari karakteristik algoritma tersebut. Oleh karena itu, algoritma yang digunakan harus membutuhkan biaya komputasi yang kecil, tetapi tetap dapat memberikan jaminan keamanan yang dibutuhkan.

Karena adanya keterbatasan *latency* yang tinggi pada jaringan nirkabel, maka protokol kriptografi yang diterapkan sebaiknya memiliki jumlah pesan dan pertukaran pesan yang lebih sedikit. Hal ini dapat dilihat pada penggunaan WTLS kelas 3 yang menggunakan *handshake* sebagai permintaan sertifikat (berbeda dengan SSL).

Keterbatasan *bandwith* juga membatasi ukuran pesan. Hal ini mengakibatkan sertifikat pada aplikasi seperti m-commere sedikit berbeda dan pengiriman rantai

sertifikat misalnya url sertifikat tidak dilakukan. Keterbatasan berikutnya adalah ruang penyimpanan yang terbatas pada perangkat seperti telepon seluler dan PDA. Oleh karena itu, dalam menerapkan kriptografi kode yang dibutuhkan harus diminimumkan misalnya memanfaatkan kode yang dioptimasi untuk platform perangkat mobile. Solusi lainnya adalah mengurangi ukuran kunci dan menyimpan sertifikat pada *client*. [5]

3. ANALISIS PENERAPAN MANAJEMEN KUNCI PADA *M-COMMERCE*

Kunci memegang peranan yang sangat penting pada suatu sistem kriptografi. Manajemen kunci yang meliputi fase pembangkitan kunci hingga penghancuran kunci tentunya juga menentukan keamanan dari suatu sistem kriptografi. *M-commerce* sebagai salah satu contoh aplikasi kriptografi, tentunya menerapkan manajemen kunci di dalamnya, untuk menjamin kekuatan dari sistem kriptografinya. Berikut ini adalah analisis mengenai bagaimana manajemen kunci diaplikasikan pada *m-commerce*, yang dijelaskan untuk masing-masing tahapan pada daur hidup kunci.

3.1. Fase Pembangkitan Kunci (*Key Generation*)

Masalah utama yang muncul pada pembangkitan kunci adalah bagaimana membuat kunci yang tidak dapat diprediksi. Kriptografi pada aplikasi *m-commerce* ini umumnya menggunakan algoritma kunci publik. Karena itu diperlukan suatu program khusus untuk membangkitkan kunci. Data yang akan dikirim akan dikompresi, kemudian di-hash dengan MAC (fungsi hash satu arah yang menggunakan kunci rahasia dalam pembangkitan nilai hash). Selanjutnya data yang telah ditambah dengan nilai hash dienkripsi dan ditransmisikan.

Dilihat dari teknologi jaringan *mobile*, keamanan pada GSM menggunakan IMSI (kode internasional pelanggan) dan Ki (kunci yang digunakan untuk authentikasi) yang disimpan di SIM Card. Enkripsi *air interface* menggunakan kunci simetris yang diturunkan dari Ki. Untuk UMTS, menggunakan kunci enkripsi yang lebih panjang.

Pada *SIM Application Toolkit* (SAT) digunakan untuk membuat aplikasi *m-commerce* berbasis *Short Message Service* (SMS), penyedia layanan menempatkan kunci enkripsi pada SIM sebelum diberikan kepada pengguna. Hal ini memastikan kunci rahasia tidak pernah dikirim melalui saluran komunikasi.

3.2. Fase Pendistribusian Kunci (*Key Distribution*)

Ketika pengguna menggunakan kunci untuk melindungi informasi yang disimpan di dalam *storage*, maka tidak ada kebutuhan untuk menyebarkan kunci, contohnya pada SAT.

Untuk melakukan pendistribusian kunci dilakukan dalam suatu protokol kriptografi. Protokol kriptografi yang digunakan dalam *m-commerce* adalah dengan menggunakan *session key*. Contohnya adalah dengan menggunakan RSA, Diffie-Hellman, dan DFEC (Diffie-Hellman Elliptic Curve).

Contoh protokol pertukaran kunci dengan menggunakan algoritma Diffie-Hellman adalah sebagai berikut:

a. Pelanggan memilih bilangan bulat acak yang besar x , dan mengirim hasil perhitungannya kepada agen perjalanan *online*:

$$X = g^x \bmod n$$

b. Agen perjalanan online menghitung bilangan bulat acak yang besar dan mengirim hasil perhitungan berikut kepada pelanggan:

$$Y = g^y \bmod n$$

c. Pelanggan menghitung

$$K = Y^x \bmod n$$

d. Agen perjalanan *online* menghitung:

$$K = X^y \bmod n$$

3.3. Fase Penyimpanan Kunci (*Key Storage*)

Pada SAT kunci disimpan pada perangkat *mobile* nya, di SIM *card. Wireless Indentity Module(WIM)* digunakan pada fungsi yang berhubungan dengan WTLS /WAP TLS dan keamanan pada level aplikasi dengan menyimpan dan memproses informasi seperti kunci rahasia dan sertifikat yang dibutuhkan untuk memberikan layanan otentikasi dan nirpenyangkalan.Untuk mencegah pengubahan, WIM diimplementasikan sebagai suatu perangkat lunak pada kartu cerdas yang berdasarkan *microprocessor*.

Pada Java ME terdapat penyimpanan data pada tempat penyimpanan permanen melalui *record store* atau pada *file resource* aplikasi yang digunakan untuk menyimpan sertifikat dijital atau kunci. Kunci disimpan dalam bentuk yang terpotong-potong, dan ketika akan digunakan akan digabungkan kembali.[7]

3.4. Fase Penggunaan Kunci (*Key Usage*)

Pada SAT terdapat memiliki kelemahan karena penggunaan kode PIN pada perangkat *mobile client*. Kode PIN ini biasanya berupa angka 4 dijit yang dapat ditebak dengan mudah oleh pencuri perangkat *mobile*.

Wireless Public Key Infrastructure(WPKI). WPKI merupakan ekstensi dari PKI(*Public Key Infrastructure*), yang dibuat khusus untuk jaringan nirkabel. WPKI memerlukan komponen yang sama dengan PKI, yaitu. pengguna (pemohon sertifikat dan pemakai sertifikat), sertifikat dijital, CA (*Certification Authority* yaitu pihak yang mengeluarkan sertifikat dijital, biasanya adalah institusi keuangan atau institusi terpercaya lain), direktori untuk menyimpan sertifikat dijital dan CRL (*Certificate Revocation List* berisi nomor seri sertifikat dijital ynag ditarik/ sudah kadaluarsa dan dianggap tidak sah).

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

3.5. Fase Perubahan Kunci (*Key Change*)

Protokol WLTS (*Wireless Transport Layer Security*) merupakan protokol yang mendukung WPKI dan didesain untuk menjamin keamanan komunikasi dan transaksi melalui jaringan nirkabel. WTLS dibuat berdasarkan TLS dan dioptimasi untuk komunikasi nirkabel, mendukung datagram, memiliki protokol *handshake* yang dioptimasi dan memiliki mekanisme *dynamic key refreshing*.

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. Seberapa sering kunci diubah ditentukan saat melakukan *handshake*.

3.6. Fase Penghancuran Kunci (*Key Destruction*)

Kunci yang sudah digunakan akan dihancurkan. Pada Java ME kunci yang sudah digunakan akan dihapus dari tempat penyimpanannya dengan menggunakan *garbage collector*. [7] Untuk kunci-kunci yang disimpan dalam bentuk *smart card*, dihancurkan dengan dihapus atau ditimpa.

4. KESIMPULAN

Terdapat beberapa kesimpulan yang diambil dari pembuatan makalah analisis penerapan manajemen kunci pada kriptografi di aplikasi *m-commerce* ini, yaitu:

1. Kriptografi saat ini telah menjadi sangat penting dan berkembang. Dengan pembuatan makalah ini semakin membuat penulis memahami tentang konsep kriptografi
2. Keamanan sistem kriptografi bergantung pada keamanan dalam menjaga kunci, disepanjang daur hidupnya
3. *M-commerce* merupakan salah satu varian *e-commerce* yang diaplikasikan pada suatu perangkat mobile sekaligus merupakan salah satu contoh penerapan aplikasi kriptografi, yang saat ini semakin berkembang mengingat jumlah penggunaan telepon selular yang semakin meningkat dari hari ke harinya
4. Fase pembangkitan kunci di *m-commerce* umumnya memakai program khusus, mengingat algoritma kunci publik yang digunakan dalam sistem kriptografinya. Namun ada juga yang sudah diletakkan di dalam kartu SIM, yaitu SAT.
5. Fase pendistribusian kunci di *m-commerce* adalah dengan menggunakan *session key* untuk kunci yang tidak disimpan dalam perangkat *mobile*
6. Fase penyimpanan kunci di *m-commerce* ada yang disimpan pada perangkat *mobile*, atau pada WIM
7. Fase penggunaan kunci di *m-commerce* adalah dengan menggunakan WPKI yang mendukung pemakaian algoritma kunci publik
8. Fase perubahan kunci di *m-commerce* adalah dengan menggunakan *dynamic key refreshing* yang disediakan oleh protokol WLTS
9. Fase penghancuran kunci di *m-commerce* adalah dengan menghapus atau menimpa kunci yang sudah tak berguna.

DAFTAR REFERENSI

[1] Munir, Rinaldi. *Diktat Kuliah IF5054 Kriptografi.* Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung. 2006

[2] Bishop, David. *Introduction to Cryptography with Java Aplets*. Jones and Batrlet Publisher. 2002

[3] *M-commerce and Security*, http://www.certification.tn/Conference/presentationPKI/Session5/CERT%20M%20commerce.ppt, diakses tanggal 3 Januari 2008

[4] *Mobile Commerce*, http://sunny.umcrookston.edu/courses/mgmt/bbrorson/0304/fall/online/3270/PPT_08.ppt, diakses tanggal 3 Januari 2008

[5] Sembiring, Krisantus. *Studi Penerapan Kriptografi pada Mobile Commerce.* Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung. 2006

[6] Purnama, Indra. *Aspek Security pada Penerapan m-commerce di Indonesia*. Magister Teknik Teknologi Informasi, Departemen Teknik Elektro, Institut Teknologi Bandung. 2005

[7] *MIDP Application Security.* http://developers.sun.com/techtopics/mobility/midp/articles/security/, diakses tanggal 3 Januari 2008