PENGGUNAAN MOBILE PUBLIC KEY INFRASTRUKTUR UNTUK MENGAMANKAN TRANSAKSI MOBILE PAYMENT

Fajar Baskoro , Rahdian Seto Hananto K
Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS), Surabaya, 60111, Indonesia
E-mail :fajarbaskoro@gmail.com, transmoment@gmail.com

ABSTRAK

Perangkat komunikasi mobile memainkan peran yang sangat penting dalam kehidupan sehari-hari, Cara pembayaran non-fisik mungkin memang telah banyak dipandang orang sebagai cara pembayaran yang paling aman dan praktis, dengan adanya cara pembayaran yang dapat dilakukan dengan perangkat mobile maka proses pembayaran non fisik dapat dilakukan secara lebih luas.

Aplikasi mobile payment ini dibuat untuk memudahkan pengguna dalam bertransaksi dengan aman secara online dengan menggunakan media handphone, aplikasi dibangun dengan menggunakan teknologi Java 2 Micro Edition yang dirancang agar mudah digunakan. Aplikasi ini menggunakan keamanan berbasis Secure socket Layer (SSL). yang menginplementasikan koneksi melalui secure http (https) untuk mengamankan saluran komunikasi antara aplikasi klien dan server dalam proses transfer data transaksi.

Hasil dari penelitian ini adalah aplikasi mobile yang dapat digunakan pengguna untuk melakukan transaksi finanasial secara elektronik untuk kelompok masyarakat yang tidak memiliki rekening bank, secara cepat, aman dan mudah digunakan dimana pun dan kapanpun.

Kata Kunci: mobile public key, system pembayaran, security

1. PENDAHULUAN

Jumlah penggunaan piranti mobile meningkat dengan sangat cepat, Seiring dengan meningkatnya penggunaan piranti mobile, maka terbuka alternatif-alternatif baru yang lebih memudahkan dalam melakukan berbagai transaksi bisnis.

Cara pembayaran non-fisik mungkin memang telah banyak dipandang orang sebagai cara pembayaran yang paling aman dan praktis, sehingga tidaklah mengherankan jika jenis cara pembayaran ini semakin marak berkembang. Dimulai dari pembayaran melalui Credit Card, Giro, Cheque, kemudian Kartu Debit, dan terus berkembang, sehingga kini melalui ponsel pun pembayaran dapat dilakukan melalui mobile payment.

Jaminan keamanan terhadap M-Commerce akan menjadi kunci penambahan tingkat funsionalitas telepon selular. Setidaknya ada empat hal yang harus selalu diperhatikan untuk menjamin transaksi yang aman, yakni autentication, confidentiality, integrity, dan non-repudiation. Authentication berkaitan dengan masalah verifikasi identitas dari pihak-pihak yang terlibat dalam komunikasi untuk memastikan bahwa mereka adalah orang yang sesuai dengan apa yang diklaim. Confidentiality adalah bagaimana menjamin bahwa hanya pengirim dan penerima pesan yang seharusnya yang bisa membaca isi pesan. Integrity berkaitan dengan penjaminan isi pesan dantransaksi tidak berubah, baik secara tidak sengaja maupun sebaliknya. Non-repudiation adalah bagaimana menyediakan mekanisme yang dapat digunakan untuk menjamin salah satu pihak yang terlibat dalam transaksi tidak bias menyanggah bahwa mereka tidak pernah terlibat dalam transaksi tersebut.

Maka pembuatan sistem yang diharapkan dapat memberikan rasa aman dan efisiensi dalam bertransaksi, dengan aplikasi J2ME dan WEB, diharapkan dapat diterapkan dalam usaha meningkatkan penjualan.

1.1 M-Commerce

M-commerce atau mobile commerce sering disebut juga dengan m-business atau pervasive computing. M-commerce merupakan pengembangan dari e-commerce yang menggunakan jaringan wireless atau mobile telecommunication.

Secara karakteristik m-commerce terdiri dua bagian yaitu mobility dan board reachability. Kata mobile menerangkan bahwa aktifitas tersebut dilakukan dengan cell phone atau perangkat teknologi lainnya yang bersifat mobile seperti PDA (personal digital assistant), sehingga para penggunanya dapat melakukan berbagai aktifitas e-commerce dimana saja. Sedangkan kata board reachibility menjelaskan bahwa apapun aktifitasnya dan dimanapun mereka berada para pengguna m-commerce tersebut dapat menjangkau atau memiliki informasi yang dia butuhkan secepatnya.

Secara umum, aktifitas dari m-commerce dibagi menjadi 12 kategori yaitu, mobile financial, mobile advertising, mobile inventory management, proactive service management, product locating and shopping, wireless reengineering, mobile auction or reverse auction, mobile entertainment services, mobile office, mobile distance education, wireless data centre dan mobile music.

Dari kedua belas kategori diatas dalam perkembangannya dapat digabung menjadi beberapa aktifitas yang disesuaikan menurut aktifitasnya seperti financial application; marketing, advertisement and customer service; enterprise application; B2B and supply chain; individual consumer; location-based dan non-internet applications. Beberapa dari kategori tersebut telah dikembangkan di Indonesia, terutama oleh para pengembang dan provider mobile phone.

Financial application merupakan salah satu contoh utama dari m-commerce. Beberapa contoh dari aplikasi ini seperti mobile banking, m-brokerage services, wireless electronic payment systems, micro payments, wireless web wallet dan bill payment.

Aplikasi mobile banking sudah banyak digunakan berbagai bank di Indonesia, para customer dari bank tersebut dapat melakukan aktifitas perbankan seperti cek account balance, transfer, pembayaran tagihan listrik, air, telepon, kartu kredit, dengan menggunakan cell phone mereka.

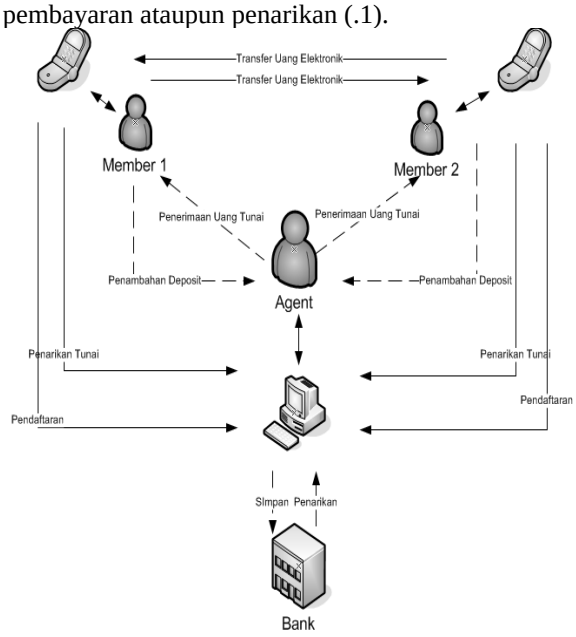
Sedangkan wireless electronic payment systems adalah sebuah aplikasi yang digunakan untuk aktifitas pembayaran makanan dan minuman di tempat tertentu atau pembayaran pencucian mobil otomatis dengan hanya mengirim SMS dari GSM handset ke nomor tertentu. Biaya dari aktifitas tersebut akan diambil dari besar harga pulsa yang ada untuk GSM prabayar atau ditambahkan ke biaya pulsa yang akan dibayar oleh para pengguna GSM abondemen. Sedangkan aplikasi dari micropayments sebenarnya hampir mirip dengan aktifitas wireless electronic payment, bedanya, para pengguna harus menelepon nomor tertentu dan membayar waktu telepon tersebut seharga biaya yang dibutuhkan. Hal tersebut juga tidak jauh berbeda dengan wireless web wallet, aplikasi ini digunakan untuk pembayaran online, penggunanya menggunakan sebuah virtual wallet (dompet online).

2. ANALISIS KEBUTUHAN DAN PERANCANGAN SISTEM

2.1 DESKRIPSI UMUM

Aplikasi yang dibangun dalam penelitian ini adalah system pembayaran berbasis mobile yang di aplikasikan dalam proses Transfer Uang Elektronik dalam transaksi keseharian dengan menggunakan aplikasi j2me, dimana dalam proses transaksi tersebut diperlukan tingkat keamanan agar tidak terjadi kesalahan pengiriman data ataupun terjadi perubahan data yang di timbulkan selama proses transaksi dilakukan, dengan adanya perangkat lunak ini diharapkan dapat memberikan alternative pilihan dalam bertransaksi dengan aman dan mudah.

Aplikasi menggunakan model debit prabayar dimana user menambahkan uang elektronik pada agent yang berfungsi sebagai perwakilan layanan pelanggan untuk menerima dan melayani penarikan uang tunai dari user . User yang telah terdaftar sebagai member dapat mempergunakan fitur – fitur yang terdapat pada aplikasi mobile seperti informasi saldo, pembayaran transaksi untuk member yang lain, melakukan penarikan uang tunai pada agent serta melihat histori transaksi yang dilakukan baik pembayaran ataupun penarikan (.1).



Gambar 1. Deskripsi Umum Sistem

2.2 PENGGUNA

Klasifikasi pengguna dalam perangkat lunak ini dibedakan menjadi dua kategori yaitu pengguna web server dan pengguna mobile device :

Pengguna Web Base:

1. Administrator

   Bagian administrasi mengurusi masalah-masalah yang berhubungan dengan pengaturan data administrasi dan memonitor data member dan agent.
2. Agent

   Bagian yang melayani pendaftaran member serta melakukan penambahan uang elektronik (deposit) dan melayani penarikan tunai.
3. Klien Member

   Bagian yang digunakan oleh member untuk mengubah data administrasi serta melihat informasi transaksi secara lebih detil dan terperinci.

Pengguna Perangkat Mobile:

1. Klien (member)

   Bagian yang melakukan proses transaksi meliputi, Penambahan uang elektronik, Pembayaran Transaksi Melalui Proses Tranfer uang elektronik, Penerimaan Transaksi , Histori Pembayaran, Penarikan uang tunai, Histori penarikan uang, Menerima dan mengirim Pesan

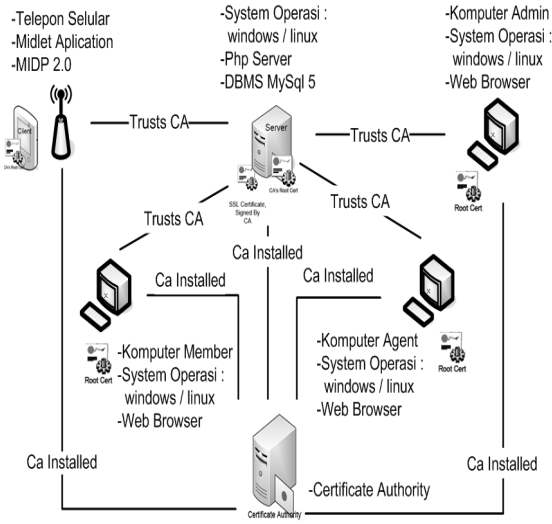
   Terdapat dua tipe member dalam menggunakan aplikasi yaitu

Member Pengirim Transaksi : User yang melakukan proses tranfer uang elektronik kepada user penerima.

Member Penerima Transaksi : User yang menerima proses transfer dari user pengirim transaksi.

3. ARSITEKTUR SISTEM

Aplikasi Sistem yang dikembangkan adalah aplikasi berbasis web dan mobile yang dikembangkan dengan menggunakan bahasa pemrograman Php dan sebuah aplikasi klien yang dikembangkan dengan teknologi J2ME. Versi Php yang dikembangkan adalah versi 5.x.x. Sedangkan untuk databasenya menggunakan MySql versi 5.x. Untuk aplikasi Midlet menggunakan Konfigurasi dan profil MIDP 2.0 dan CLDC 1.1.

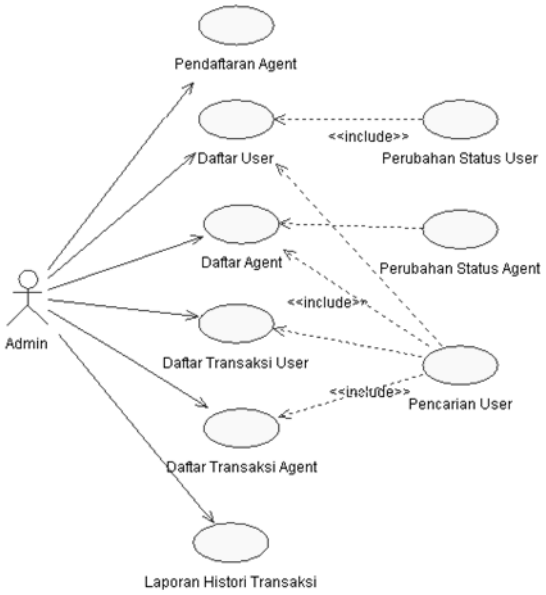


Gambar 1 Arsitektur Sistem

Pada gambar 2 arsitektur sistem diatas terdapat dua tipe client yaitu komputer client dan mobile device client. client tersebut terhubung oleh server yang memerlukan kepercayaan saat berhubungan, untuk menjamin kepercayaan pada masing-masing diperlukan suatu Certificate Authority yang berfungsi untuk memberikan bukti atau verifikasi kepada client bahwa server yang dituju telah diverifikasi keberadaanya dengan benar sesuai dengan identitas alamat server tersebut, hal ini dapat dilakukan dengan cara menginstall CA Root certifikat di client ataupun di server. Root certifikat digunakan untuk memberitahukan bahwa komputer saling mengetahui dan mempercayai. menempatkan certifikat pada client dan server akan membuat hubungan saling percaya antara client dan CA ataupun server dengan CA, ketika CA mengeluarkan setifikat dan menandatangani dengan menggunakan private key, sertifikat tersebut akan di install pada server, sehingga client yang berhubungan dengan server dapat membuktikan bahwa tanda tangan CA dengan menggunakan Root certificate public key, dengan cara ini client akan tahu kalau server dapat dipercaya karena telah mendapat persetujuan atau tanda tangan dari CA yang terpercaya.

Proses verifikasi CA pada client dan server dengan menggunakan sertifikat SSl, proses kerja pengamanan menggunakan SSL , mempunyai kesamaan dalam menggunakan spesial tipe dari 2 kunci. jika suatu pembuka kunci di kunci menggunakan kunci A maka untuk membukanya dengan kunci B, dan sebaliknya salah satu kunci tersebut dinamakan public key dan satunya lagi dinamakan private key. publik key dapat digunakan oleh semua orang tetapi private key hanya diketahui oleh satu orang proses ini dikenal dengan kriptografi kunci publik

Setelah hubungan saling percaya telah terpenuhi dengan bantuan CA maka proses pengiriman data dan penerimaan data antara client dan server dapat dilakukan dengan menggunakan jalur SSL.



Gambar 3 Use Case Fungsionalitas Web Server Admin

Semua session pada SSL dimulai dengan sebuah pesan Client Hello. Pesan ini dikirim oleh client kepada server yang ingin dituju untuk berkomunikasi. Pesan ini berisi versi SSL dari client, sebuah bilangan acak yang akan digunakan selanjutnya pada penurunan kunci, dan juga sebuah kumpulan ciphersuite offer. Offer ini merupakan penanda yang menunjukkan cipher dan algoritma hash yang ingin digunakan oleh client. Pada saat membangun koneksi inisial, server memilih sebuah offer yang ingin digunakan, dan menyampaikan kembali offer tersebut kepada client bersama dengan certificate dan sebuah bilangan acak yang dimilikinya. Client kemudian melakukan verifikasi server menggunakan sertifikat dan mengekstraksi kunci publik server. Dengan menggunakan kunci publik, client mengenkripsi rahasia premaster,

sebuah nilai acak yang akan digunakan untuk membangkitkan kunci simetri, dan mengirim pesan terenkripsi tersebut kepada server, yang kemudian mendekripsi pesan menggunakan kunci privatnya.

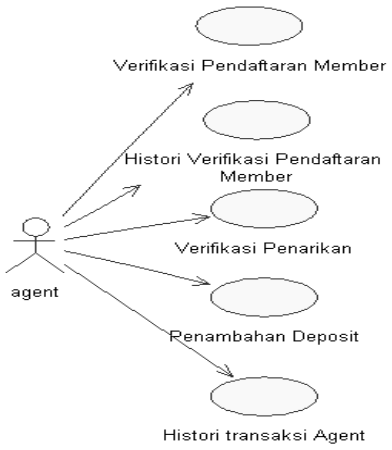
Setelah server menerima rahasia premaster dari client, server dan client sama-sama membangkitkan kunci simetri yang sama menggunakan rahasia premaster dan juga bilangan acak yang telah dipertukarkan sebelumnya.

Spesifikasi use case yang ada di Sistem Mobile Payment secara umum dapat dilihat pada gambar 3.

Use case ini digunakan untuk melakukan pengaturan user ,

- Melakukan Pencarian Daftar User Member dan Agent
- Melihat Daftar User Member dan Agent
- Melihat Detil Data User Member dan Agent
- Melakukan Perubahan Status User Member dan Agent
- Melihat Daftar transaksi user
- Melihat Daftar transaksi agent

Gambar 4 merupakan use case yang digunakan oleh agent untuk melayani transaksi yang dilakukan oleh member.



Gambar 4. Use Case Fungsionalitas Web Server Agent

Terdapat beberapa fungsionalitas web server untuk Agent yaitu:

a. Verifikasi / Persetujuan Pendaftaran Calon Member
b. Histori Verifikasi / Persetujuan Pendaftaran Member
c. Penambahan Deposit / Uang Elektronik
d. Histori transaksi

4. IMPLEMENTASI SISTEM

Sistem ini dikembangkan dengan dua teknologi. Yang pertama adalah untuk bagian server. Bagian server merupakan aplikasi dengan berbasis web dengan bahasa pemrograman Php. Web server yang digunakan adalah XAMPP versi 1.6.4. Bagian yang kedua adalah aplikasi klien yang berupa aplikasi J2ME. Pengembangan aplikasi klien ini menggunakan Netbeans 5.5 dan WTK 2.5.1. Spesifikasi masing-masing aplikasi dapat dilihat pada tabel berikut:

Tabel 1 Teknologi yang digunakan untuk aplikasi server

Teknologi	*Versi*	*Spesifikasi*
Webserver	XAMPP 1.6.4	- Apache 2.2.6 - MySQL 5.0.45 - PHP 5.2.4
Sistem Database	MySQL 5.0.45	
Bahasa Pemrograman	PHP 5.2.4	

Aplikasi Web dibangun sesuai dengan rancangan yang telah dibuat sebelumnya. Aplikasi ini bertindak sebagai jalur akses bagi pihak admin, agent ataupun member. Selain itu juga sebagai server yang berkomunikasi dengan aplikasi klien dengan menggunakan koneksi https. Karena aplikasi server merupakan aplikasi yang dikembangkan dengan basis web maka bentuk komunikasinya adalah *request – respon*. Server akan menerima permintaan dari klien kemudian memberikan balasan sesuai dengan yang diminta oleh klien.

Pembuatan aplikasi J2ME adalah aplikasi yang berjalan pada konfigurasi MIDP 2.0 dan CLDC 1.1. konfigurasi ini sebelumnya harus ditentukan pada WTK sebagai emulator

Implementasi HTTPS pada aplikasi j2me menggunakan sertifikat ssl X.509.

Tabel 2. Teknologi yang digunakan untuk aplikasi klien

Teknologi	*Versi*	*Spesifikasi*
Software	WTK 2.5.1 + skin emulator SE K750	- MIDP 2.0 - CLDC 1.1
Editor	NetBeans Versi 5.5 Mobiliti tool 5.5	

Gambar dibawah ini adalah tampilan menu utama dari aplikasi J2ME.

Gambar 5. Menu Utama Aplikasi J2ME

5. UJI COBA

Uji coba dilakukan untuk melihat jalannya aplikasi, baik aplikasi yang berbasis web maupun aplikasi klien yang berbasis J2ME. Uji coba ini dijalankan sesuai dengan sekenario yang ditentukan dalam scenario uji coba.

Tabel 3 Lingkungan Uji Coba

Perangkat Server	*Host* : https://www.transmoment.web.id/ Sistem Operasi : Linux *Web Server*: Apache versi 2.2.6 (Unix) PHP versi 5.2.5 Basis Data : MySQL versi 5.0.45
Perangkat Klien	*Prosesor* : Intel(R) Pentium (R) 4 (2.81 Ghz) Memori : 512 MB Sistem Operasi : Microsoft Windows XP SP2. Web Browser: Mozilla/5.0 Firefox/2.0.0.11 Ponsel : MIDP 2.0, CLDC 1.1 - Nokia N80 (GPRS class 10, 352x416 pixel, MIDP 2.0, CLDC 1.1) - LG KG300 (GPRS class 8, 240 x 320 pixel, MIDP 2.0, CLDC 1.1)
CA	*Equifax Secure Global eBusiness CA-1*

Skenario uji coba yang akan dilakukan adalah sebagai berikut:

I. Skenario pengujian member dan agent
   1. konfigurasi member
   2. pendaftaran member dan verifikasi agent
   3. Penambahan saldo member oleh agent
   4. Melakukan proses transfer antar member
   5. Melihat penerimaan tranfer
   6. Melakukan penarikan dan melihat histori penarikan
   7. melihat dan mengirim Pesan
   8. Pendaftaran member web site
   9. melakukan proses perubahan data password
   10. Melihat histori transkasi member
   11. Melihat histori transaksi agent

II. Skenario Pengujian Administrator untuk member dan agent
   1. login
   2. melihat daftar user
   3. melakukan perubahan aktifasi member
   4. melaukan perubahan aktifasi agent
   5. melihat histori member
   6. melihat histori agent

6. PENUTUP

6.1 KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, maka dapat disimpulkan beberapa hal sebagai berikut :

1 Sistem Transkasi Mobile Payment telah berhasil diimplementasikan Secara Online dengan menggunakan teknologi Open Source berbasis web yang menggunakan PHP dan Mysql

2 Sistem yang telah dibangun dapat memberikan kemudahan dan keamanan untuk melakukan proses transaksi elektronik dengan menggunakan mobile device.

6.2 SARAN

Beberapa hal yang diharapkan dapat dikembangkan pada masa mendatang adalah sebagai berikut:

1. Sistem dapat melayani pembayaran untuk penerima transaksi tanpa mendaftar sebagai member .
2. Sistem dapat melayani proses pembayaran pada sistem e–commers.
3. Terdapat Data Perolehan data pada setiap transaksi yang telah dilakukan oleh user yang didapat dari sistem applikasi

PUSTAKA

Anonymous. Build Brilliant Client/Server Apps with J2ME, PHP, and MySQL http://www.devx.com

Anonymous. PHP Interacting with J2ME http://DevBuilder.org

DevBuilder.org.2007 PHP Interacting with J2ME.

DuBois, Paul. October 2002. MySQL Cookbook. O'Reilly.

Lacava, Alessandro. Obtaining Wireless News with J2ME and PHP. http://www.alessandrolacava.com/blog/2006/04/18/obtaining-wireless-news-with-j2me-and-php

Sklar, David. June 2004. Learning PHP 5. O'Reilly.

Yu Feng. Network Programming with J2MEWirelessDevices. http://www.wirelessdevnet.com/channels/java/features/j2me_http.phtml

Sds OMahony, D. & Peirce, M. & Tewari, H., *Electronic Payment Systems for ECommerce*, Artech House, United States, 1997, 254 pages Referensi

Stallings William, *Cryptography and Network Security Principles and Practices, Fourth Edition.* 2005. Prentice Hall.

Stallings William, *Cryptography and Network Security Principles and Practices, Fourth Edition.* 2005. Prentice Hall. Studi Pener Penerapan Kriptografi pada Mobile Commerce, diakses tgl: 4/nov/2008 jam:05:30 http://krisantus.com/wp-content/uploads/2008/03/makalah-055.pdf

Kajian dan Implementasi Sistem Keamanan Data pada Ponsel Berbasis J2ME Menggunakan Profile MIDP 1.0, diakses tgl: 5/nov/2008 jam:21:45 http://www.cert.or.id/~budi/courses/ec7010/2003/report-antonius.pdf

Penggunaan Mobile Public Key Infrastruktur Untuk Mengamankan Transaksi Mobile Payment, diakses Tgl: 5/nov/2008 , jam:21:45 http://www.cert.or.id/~budi/courses/ec7010/dikmenjur-2004/taukhid-report.pdf

Penggunaan Mobile Public Key Infrastruktur Untuk Mengamankan Transaksi Mobile Payment, diakses Tgl: 5/nov/2008 , jam:21:45 http://www.cert.or.id/~budi/courses/ec7010/dikmenjur-2004/taukhid-report.pdf

Analisis Keamanan Mobile Payment System Berbasis PKI, diakses tgl: 8/nov/2008 jam:08:30 http://www.cert.or.id/~budi/courses/ec7010/dikmenjur-2004/taukhidwisnubroto-report.pdf

Analisis Keamanan Mobile Payment System Berbasis PKI, diakses tgl: 8/nov/2008 jam:21:00 http://www.cert.or.id/~budi/courses/ec7010/dikmenjur-2004/taukhidwisnubroto-report.pdf

An Architecture for Mobile Payments, diakses tgl :8/nov/2008 jam:21: 30 http://yb1zdx.arc.itb.ac.id/data/OWP/library-ref-eng/ref-eng-2/network/m-banking/04-Bled1.pdf