Penggunaan *Smart Card* sebagai Tiket Jalan Tol

Tantri Saraswati[1] , Alvernia Nareswari N.[2], dan Novitarini[3]
Program Studi Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132
E-mail : *if12008@students.if.itb.ac.id*[1] ,*if12011@students.if.itb.ac.id*[2] ,
if12019@students.if.itb.ac.id[3]

Abstrak

Kelancaran jalan tol merupakan kebutuhan penting bagi masyarakat kota besar. Salah satu hal yang dapat mengganggu kelancaran jalan tol yaitu antrian pengguna untuk melakukan transaksi pembayaran pada gerbang tol. Solusi dari permasalahan ini adalah pembangunan sistem ticketing otomatis dengan memanfaatkan teknologi *smart card*. *Smart card* dapat didefinisikan sebagai sebuah kartu kecil dengan *integrated circuit* yang *embedded* dengannya. *Smart card* dapat digunakan untuk menyimpan data dan dapat disisipi dengan sejumlah aplikasi yang berbeda. Hal ini memungkinkan *smart card* digunakan sebagai multitiket dalam sistem *ticketing* otomatis. Dengan demikian, untuk setiap penyedia jasa dapat dibuat program tertentu untuk mendebet nilai sesuai kebijakan perusahaan. Hal ini juga akan memudahkan proses *revenue sharing.* Keamanan sistem diimplementasikan dengan menggunakan aspek kriptografi. Aspek kriptografi dalam implementasi *smart card* berkaitan dengan enkripsi data yang disimpan dalam *smart card* dan otentikasi pengguna dengan *server*. Salah satu algoritma yang dapat dimplementasikan untuk melakukan otentikasi pengguna *smart card* dan *server* adalah algoritma *Elliptic Curve Cryptography (ECC)*. Algoritma kunci-publik ini mampu mencapai tingkat keamanan yang optimal dengan masukan *digit* kunci yang lebih sedikit dari algoritma kunci-publik lain.

***Kata kunci**: smart card, jalan tol, tiketing, Elliptic Curve Cryptography (ECC)*

1. Pendahuluan

Penggunaan jalan tol di kota-kota besar telah menjadi hal yang tidak dapat dipisahkan dari kehidupan masyarakat sehari-hari. Hal ini menyebabkan kelancaran jalan tol menjadi kebutuhan yang sangat penting bagi pengguna. Salah satu hal yang dapat mengganggu kelancaran jalan tol yaitu antrian pengguna untuk melakukan transaksi pembayaran pada gerbang tol.

Pada sebagian besar kota, mekanisme pembayaran tiket tol masih dilakukan secara manual. Pada saat pengguna memasuki gerbang tol, pengguna akan diberi tiket berupa kartu oleh petugas yang kemudian akan diserahkan kembali pada petugas yang berada di gerbang keluar. Kartu inilah yang kemudian dijadikan sebagai bukti perjalanan pengguna. Jumlah yang harus dibayar oleh pengguna pun dihitung berdasarkan kartu ini. Selain itu, penyedia jasa tol juga menyediakan kartu berlangganan bagi pengguna yang sering menggunakan tol. Pembayaran untuk kartu berlangganan ini dilakukan dimuka dengan nilai nominal tertentu sesuai kebutuhan.

Dewasa ini, muncul kecenderungan untuk melakukan privatisasi sektor transportasi publik. Salah satu dari transportasi publik yang telah banyak diprivatisasi adalah jalan tol. Dalam suatu kota, mungkin terdapat beberapa jalan tol yang dikelola oleh penyedia jasa yang berbeda-beda.

2. Rumusan Masalah

Dari deskripsi diatas, dapat dirumuskan beberapa masalah sebagai berikut:

1. Mekanisme *ticketing* manual dapat menghambat perjalanan pengguna jalan karena harus berhenti diawal untuk mengambil tiket dan diakhir untuk melakukan pembayaran.
2. Apabila jumlah gerbang tol cukup banyak, dibutuhkan sumber daya manusia yang banyak pula untuk menjadi petugas tiket. Hal ini dapat meningkatkan biaya operasional jalan tol.
3. Apabila pengguna hendak berlangganan beberapa jalan tol yang dilewati, pengguna harus memiliki kartu berlangganan untuk setiap tol. Hal ini tentunya akan sangat merepotkan pengguna.
4. Mekanisme *ticketing* manual memperbesar kemungkinan terjadinya *ticket fraud*.

Permasalahan-permasalahan tersebut dapat diatasi dengan penggunaan *smart card* sebagai pengganti karcis tol.

3. Teori Pendukung

Smart card, sering disebut pula sebagai chip card atau integrated circuit(s) card(ICC), dapat didefinisikan sebagai kartu seukuran kantong (dapat lebih kecil lagi) dengan integrated circuit yang embedded dengannya. Ada dua jenis ICCs, yaitu memory card dan microprocessor card. Memory card hanya terdiri dari non volatile memory storage dan mungkin terdiri dari fitur kemanan pula. Sedangkan memory card terdiri dari memory dan komponen microprocessor.

Smart card sering dipersepsikan sebagai sebuah microprocessor dengan ukuran sebesar kartu kredit dengan beragam property tamper-resistant (seperti crypto-processor yang aman, file system yang aman, serta fitur lainnya yang dapat dimengerti manusia awam) dan menyediakan layanan keamanan (informasi rahasia dalam memori). Tidak semua chip card memiliki microprocessor (contohnya memory cards). Oleh karena itu, tidak semua chip card dianggap sama dengan *smart card*.

Smart card tampak seperti kartu kredit tetapi memiliki fungsi yang mirip dengan komputer. *Smart card* berbeda dengan magnetic strip card biasa dalam hal pemrosesan dan penyimpanan data. *Smart card* dapat berfungsi sebagai penyimpan data, pembuat kalkulasi, pemroses data, pengatur file, dan eksekusi algoritma enkripsi. Dengan demikian *smart card* memungkinkan untuk mewujudkan suatu aplikasi yang canggih dan portable dalam pemrosesan data. *Smart card* telah terbukti lebih terpercaya dibandingkan dengan magnetic strip cards.

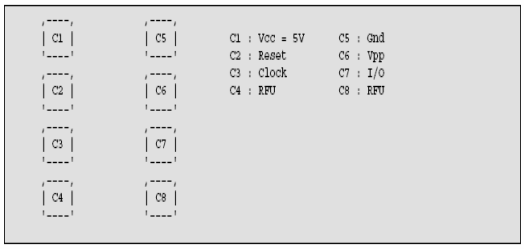
Smart card lebih sukar untuk di-clone daripada kartu tradisional lainnya, informasi yang disimpan dalam *smart card* lebih kompleks. Informasi tersebut dapat pula di-update

Smart card dapat dikategorikan dalam dua jenis, yaitu :

Contact *Smart card*

Contact *smart card* memiliki sebuah chip emas yang berukuran sekitar 0.5 inchi di bagian depan, tidak seperti kartu kredit yang memiliki magnetic strip di bagian belakang. Contact *Smart card* membutuhkan aplikasi *smart card* reader untuk membaca dan menulis data dari dan ke dalam chip tersebut.

Standar PIN koneksi berdasarkan ISO7816:



- I/O : masukan atau keluaran dari serial data ke integrated circuit dalam card
- Vpp : voltage masukan (opsional digunakan)
- Gnd (voltage referensi)
- CLK : clocking atau sinyal waktu (optional digunakan)
- RST : digunakan sendiri oleh *smart card* (sinyal reset yang tersedia pada antarmuka device) atau kombinasi dengan sirkuit control reset internal (opsional digunakan). Jika reset

internal tersedia maka voltage harus tersedia pada Vcc
- Vcc : masukan power supply (opsional digunakan

Contactless *Smart card*

Contacless *Smart card* tampak seperti kartu kredit plastik dengan chip computer dan antenna coil di dalamnya. Contacless *smart card* dapat ditulis dan dibaca hanya dengan didekatkan pada antenna luar. Contactless *Smart card* digunakan bila membutuhkan transaksi yang harus diproses dengan cepat.

Dua kategori tambahan lainnya merupakan turunan dari kedua tipe yang telah dijelaskan sebelumnya. Kedua kategori tersebut adalah Combi Card dan Hybrid Card.

Hybrid card memiliki dua chips, masing-masing merepresentasikan antarmuka contact dan contactless. Kedua chip tersebut tidak saling berhubungan, tetapi untuk sebagian besar aplikasi digunakan secara bersamaan dalam melayani kebutuhan consumer dan card issuer. Berbeda dengan Hybrid Card, Combi card hanya memiliki sebuah chip yang merepresentasikan antarmuka contact dan contactless.

Chip yang digunakan pada kedua jenis kategori tersebut di atas dapat dikategorikan ke dalam dua bagian, yaitu: chip microprocessor dan chip memory.

Chip memory dapat dilihat sebagai floppy disk kecil dengan layanan keamanan(optional). Memory card dapat menyimpan 103 hingga 16000 bits data. Memory card lebih murah bila dibandingkan dengan chip microprocessor, hanya saja fasilitas keamanan yang dimiliki pun lebih sedikit. Keamanan memory card bergantung pada keamanan yang diberikan card reader saat pemrosesan data

Chip microprocessor dapat menambahkan, menghapus, ataupun memanipulasi informasi yang tersimpan dalam memory. Chip microprocessor dapat dianggap sebagai miniature computer dengan input/ouput port, sistem operasi, dan hard disk

Platform *smart card*:

Microsoft Windows Card

Keunggulan yang dimiliki oleh Microsoft Windows Card bila dibandingkan dengan *Smart card* dengan platform lainnya, antara lain :
- Microsoft memiliki ISV partner yang banyak sehingga memudahkan dalam pendistribusian *smart card* miliknya.
- Dominasi platform windows, yang mendukung *smart card* juga mem`ercepat penerimaan *smart card* dengan platform Microsoft.
- Platform Microsoft juga kompatibel dengan bahasa C++, Visual Basic dan developer object oriented lainnya.
- Platform Microsoft terintegrasi dengan arsitektur Microsoft lainnya, seperti Windows NT dan /internet Explorer.
- Microsoft telah menyediakan sebuah *smart card* reader sebagai komponen yang direkomendasikan pada spesifikasi PC99.
- Microsoft telah mendemonstrasikan komitmennya dalam teknologi *smart card*. Hal ini mengindikasikan bahwa Microsoft akan meningkatkan platform *smart card* yang dimilikinya melalui revisi berulang kali.

Java

Java based *smart card* dapat menjalankan multiple aplikasi yang aman. Bahasa java banyak dipergunakan oleh developer perangkat lunak. Dengan demikian Java based *smart card* pun dapat digunakan luas oleh berbagai developer perangkat lunak. Sementara java berusaha untuk menyederhanakan pengembangan card applet, distribusi yang aman terhadap applet tersebut tidak diuji pada berbagai jaringan dengan provider yang berbeda.

Java memperbolehkan mendownload code executable code ke dalam card, sehingga isi dari *smart card* dapat dimodifikasi sesukanya. Hal ini dapat meningkatkan fleksibilitas sekaligus mengurangi tingkat keamanan penggunaan kartu.

MULTOS

MULTOS merupakan platform independent pertama yang memperbolehkan adanya

interoperability. Pada mulanya MULTOS hanya dipergunakan di bidang financial, oleh karena itu platform MULTOS kurang diterima oleh bidang industri lainnya. Selain itu, MULTOS hanya dapat diimplementasikan dengan bahasa pemrograman tingkat rendah bernama MEL, yang tidak banyak digunakan di kalangan developer perangkat lunak, akibatnya MULTOS semakin kurang diterima.

4. Analisis

4.1. Kapabilitas Smart Card

Beberapa kapabilitas yang mendukung penggunaan *smart card* dalam *toll ticketing* antara lain:

1. *Smart card* dapat digunakan untuk menyimpan data. Dalam sistem *ticketing* otomatis, *smart card* dapat digunakan untuk menyimpan data pribadi pemilik dan besar nominal harga tiket yang dibeli oleh pengguna. Nilai inilah yang nantinya akan didebet untuk membayar jasa tol.
2. *Smart card* dapat digunakan untuk melakukan verifikasi identitas dengan menampilkan *buit-in* PIN, data demografi, foto, maupun data biometrik pemilik yang disimpan dalam kartu. Untuk melakukan verifikasi, dapat diimplementasikan proses verifikasi otomatis dengan menggunakan *card reader*. Hal ini dapat membatasi penggunaan kartu oleh orang yang tidak berhak. Kapabilitas *smart card* ini memenuhi kebutuhan sistem *ticketing* otomatis untuk menyediakan tiket yang bersifat individual dan tidak dapat digunakan orang lain.
3. *Smart card* dapat diintegrasikan dengan sistem *global positioning system*. Hal ini menyebabkan keberadaan *smart card* dapat dilacak. Dalam sistem *ticketing* otomatis, hal ini berguna untuk melakukan *tracking* kilometer yang telah dilalui oleh pengguna.
4. *Smart card* dapat memproses. Kapabilitas ini dapat digunakan untuk memproses data posisi dari GPS menjadi jumlah kilometer yang telah dilalui pengguna. Karena proses penghitungan harga jasa tol didasarkan pada jumlah kilometer yang dilalui dan jumlah kilometer yang dilalui dihitung secara otomatis, resiko terjadinya *ticket fraud* sangat kecil.
5. *Smart card* dapat diprogram dan disisipi dengan berbagai aplikasi. Hal ini memungkinkan *smart card* digunakan sebagai multitiket dalam sistem *ticketing* otomatis. Dengan demikian, untuk setiap penyedia jasa dapat dibuat program tertentu untuk mendebet nilai sesuai kebijakan perusahaan. Hal ini juga akan memudahkan proses *revenue sharing.*
6. *Smart card* menyediakan mekanisme *access control*. Data dengan kepentingan berbeda dapat diatur agar hanya dapat diakses oleh aplikasi yang berkepentingan. Hal ini akan berguna untuk mengimplementasikan multitiket dalam sistem *ticketing* otomatis.
7. Untuk menjamin keamanan, *smart card* memiliki mekanisme dimana kartu dan terminal dapat saling melakukan otentikasi dengan memanfaatkan algoritma kriptografi kunci publik.

Berdasarkan uraikan diatas, dapat dilihat bahwa *smart card* dapat digunakan sebagai tiket dalam implementasi sitem *ticketing* otomatis.

4.2. Keuntungan Smart Card

Dengan mengimplementasikan *smart card* untuk sistem *ticketing* otomatis, diperoleh beberapa keuntungan sebagai berikut:

1. Menurunkan biaya perawatan untuk gerbang tol.
   Sistem *ticketing* otomatis menggunakan *smart card* tidak memerlukan lagi adanya gerbang tol dan gardu tol karena pembayaran dilakukan secara otomatis dengan mendebet nilai yang tersimpan pada *smart card* pengguna.
2. Mengurangi waktu transaksi yang diperlukan untuk melayani pelanggan.
   Waktu transaksi akan berkurang karena pelanggan tidak perlu dilakukan penerimaan pembayaran secara langsung dengan uang tunai pada gerbang tol
3. Mengefisienkan jumlah tenaga kerja manusia yang diperlukan.

Dalam sistem baru ini, tidak diperlukan lagi tenaga kerja manusai untuk memberikan karcis dan menerima pembayaran di setiap gerbang tol, maka jumlah tenaga kerja manusia yang dipekerjakan dapat dikurangi.

4. Meningkatkan kualitas pelayanan terhadap pengguna.

Perjalanan pengguna tidak perlu lagi terhambat karena harus mengambil tiket dan melakukan pembayaran. Sistem ini juga memudahkan pengguna karena pembayaran tiket tol dilakukan dengan mendebet nilai kartu secara otomatis. Pembayaran otomatis juga lebih memudahkan bagi para penyandang cacat

4.3. Analisis Resiko

Terdapat beberapa hal penting yang harus diperhatikan dalam pengembangan sistem yang menggunakan *smart card*:

1. *Smart card* harus mampu mengenali pemilik informasi pribadi yang tersimpan didalamnya.
2. *Smart card* harus mampu mengidentifikasi proses penggunaan informasi yang tersimpan
3. Komputasi yang dilakukan *smart card* harus menggunakan aturan proteksi privasi yang telah tersedia
4. *Smart card* hanya menyimpan informasi pelanggan yang berguna dan relevan
5. Pengembang *smart card* tidak menyewakan dan menjual data yang telah terkumpul tanpa persetujuan pelanggan
6. *Smart card* mampu memproteksi personal data pelanggan terhadap *data loss* atau penggunaan yang tidak terautorisasi [*Smart card* Tutorial]

5. Desain Sistem

5.1. Alur Kerja Sistem

Pelanggan dapat memperoleh *smart card* dengan mendaftar pada pihak penyedia jasa. Setelah memenuhi persyaratan, pelanggan akan memperoleh *smart card* dengan nilai nominal tertentu yang dibayarkan di muka. Oleh karena itu, pihak penyedia jasa sebaiknya bekerja sama dengan instansi keuangan tertentu.

Pembayaran jasa tol digunakan dengan cara mendebet nilai nominal yang terdapat pada *smart card* berdasarkan biaya yang harus dibayar ketika menggunakan jasa tol. Untuk mengisi ulang *smart card* pelanggan dapat menyetorkan sejumlah uang sesuai dengan nilai nominal yang diinginkan kepada instansi keuangan yang terkait.

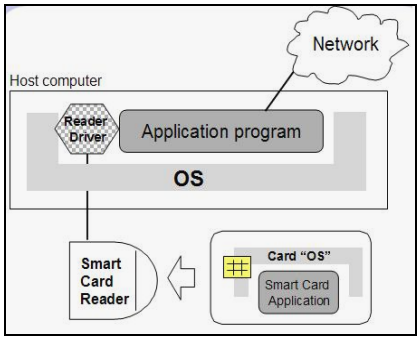
Jika pelanggan kehilangan *smart card* miliknya, pelanggan cukup melaporkan kepada pihak penyedia jasa tol. Pihak penyedia jasa kemudian akan memblokir *smart card* yang hilang tersebut untuk mencegah penggunaan *smart card* oleh pihak yang tidak berhak. Pelanggan dapat memperoleh *smart card* baru sebgai pengganti *smart card* yang hilang dengan memenuhi beberapa persyaratan tertentu sesuai dengan kebijakan pihak penyedia jasa tol.

Untuk menggunakan jasa tol dengan memanfaatkan *smart card*, pelanggan dapat melakukan langkah-langkah berikut:

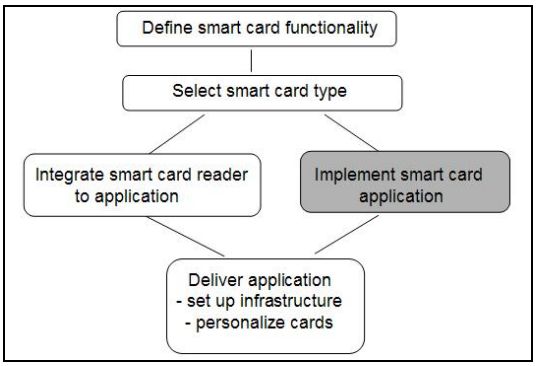
1. Saat memasuki gerbang tol, pelanggan menggesekkan *smart card* pada card reader yang tersedia untuk melakukan otentikasi
2. Jika otentikasi berhasil, portal pada gerbang akan terbuka sehingga pelanggan dapat meneruskan perjalanan
3. Pada saat pelanggan akan keluar dari jalan tol, pelanggan harus menggesekkan kembali *smart card* pada card reader yang tersedia untuk pendebetan nilai nominal pada *smart card* sebagai pembayaran jasa tol.

Untuk mengatasi perbedaan kebijakan antara penyedia-penyedia jasa tol, setiap penyedia jasa tol dapat menyisipkan aplikasi pada *smart card* sesuai dengan kebijakan masing-masing perusahaan.

Komponen aplikasi *smart card* dapat dilihat pada gambar berikut.



Langkah-langkah penambahan penggunaan *smart card* dalam aplikasi sistem *ticketing* otomatis untuk jasa tol dapat dilihat pada gambar berikut.



5.2. Keamanan Sistem

Keamanan sistem diimplementasikan dengan menggunakan aspek kriptografi. Aspek kriptografi dalam implementasi *smart card* berkaitan dengan enkripsi data yang disimpan dalam *smart card* dan otentikasi pengguna dengan *server*.

Dalam implementasi *smart card*, data yang disimpan dienkripsi dengan menggunakan algoritma enkripsi tertentu. Sedangkan untuk melakukan otentikasi pengguna dengan *server* digunakan mekanisme sebagai berikut:

1. Komputer *server* mengirimkan suatu nilai atau string (yang disebut *challenge*) ke kartu.
2. Kartu menandatangani string dengan menggunakan kunci privat yang tersimpan didalamnya.
3. Tanda tangan tersebut diverifikasi oleh mesin dengan menggunakan kunci publik pemilik kartu

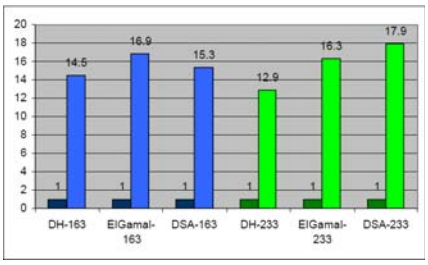
Pembangkitan tanda-tangan digital merupakan operasi yang secara komputasi memiliki *cost* yang paling besar. Kebanyakan *smart card* masih menggunakan mikrokontroler 8 bit. Penggunaan algoritma kunci publik berbasis aritmetika modulo dengan digit operan yang panjang seperti RSA dan DSA pada prosesor tersebut dapat menyebabkan lamanya waktu pemrosesan yang dibutuhkan. Oleh karena itu, perlu dilakukan pemilihan algoritma kriptografi kunci publik yang tepat.

Salah satu algoritma kriptografi kunci-publik yang dapat digunakan untuk mengatasi permasalahan di atas adalah *Elliptic Curve Cryptography* (ECC). Kekuatan algoritma ECC terletak pada sulitnya memecahkan *Elliptic Curve Discrete Logarithm Problem* (ECDLP).

Operasi dasar ECC adalah *point multiplication* yang didefinisikan pada *finite field operation*. Seluruh kurva eliptik yang telah distandarisasi didefinisikan dalam *field* bilangan bulat prima (GF(p)) maupun *field* polinomial biner ($GF(2^m)$). Dalam implementasi algoritma ECC pada *smart card* , kurva eliptik hanya didefinisikan pada *field* bilangan bulat prima karena multiplikasi pada *field* polinomial biner tidak didukung oleh mikroprosesor 8 bit dan dapat mengakibatkan turunnya performansi.

Algoritma kunci publik seperti El Gamal dan DSA dapat dimodifikasi sehingga menjadi varian dari algoritma ECC. Dengan modifikasi ini, panjang kunci yang tadinya berkisar 1024-2048 bit dapat berkurang menjadi 163-233 bit. Pengurangan panjang kunci ini tidak mempengaruhi keamanan algoritma kriptografi.

Untuk lebih meningkatkan efisiensi pemrosesan, algoritma dikodekan dan dioptimisasi dengan menggunakan bahasa *assembly*. Peningkatan kecepatan pemrosesan untuk berbagai algoritma setelah dioptimisasi dapat dilihat pada grafik di bawah ini:



Varian algoritma ECC yang dapat digunakan dalam *smart card* adalah algoritma ECC *digital signature*. Algoritma ini memiliki parameter kunci publik dan kunci privat yang sama dengan algoritma El Gamal. Dalam implementasinya, dibutuhkan sebuah fungsi bijektif

$$f : G \rightarrow \{0, \ldots, \#G - 1\}$$

Fungsi ini tidak bersifat rahasia dan dapat disebarluaskan. Protokol otentikasi dengan menggunakan algoritma ini adalah sebagai berikut:

1. *Server* membangkitkan *string* acak m dan mengirimkannya pada pemilik kartu.
2. Kartu membangkitkan bilangan asli acak $k \in \{1,...,\#G-1\}$ dan hitung $a = g^k$
3. Kartu menghitung nilai b dari persamaaan
$$f(m) = -xf(a) + kb(\text{mod } \#G)$$
4. Kartu mengirimkan *string* m dan tanda-tangan digital (a,b) pada *server.*
5. *Server* menerima *string* m dan tanda-tangan (a,b) dan mengambil duplikat kunci publik pengguna (g,h).
6. *Server* menghitung
$$u = f(m)b^{-1} (\text{mod } \#G)$$
$$v = f(a)\, b^{-1} (\text{mod } \#G)$$
$$w = g^u h^v$$
7. *Server* melakukan verifikasi apakah tanda-tangan digital sesuai dengan *string* acak yang telah dikirim pada awal proses dengan persamaan
$$w = g^u h^v = g\text{^}f(m)b^{-1}\, g^{vx} = g\text{^}f(m)b^{-1} + xf(a)b^{-1}$$
$$= g\text{^}((f(m)+xf(a))b^{-1}) = g\text{^}kbb^{-1} = g^k = a$$

7. Kesimpulan

Smart card dapat digunakan untuk pembayaran jasa tol. Penggunaan *smart card* dalam *ticketing* meningkatkan pelayanan terhadap pelanggan jasa tol. Untuk menjamin keamanan sistem perlu dilakukan pemilihian algoritma kriptografi yang tepat sehungga tidak hanya aman namun juga memiliki performansi yang sesuai dengan kebutuhan dan keterbatasan mikroprosesor *smart card*.

Algoritma kriptografi *Elliptic Curve Cryptography* (ECC) dapat digunakan dalam proses otentikasi penggunan *smart card* dan *server*. Hal ini disebabkan untuk tingakat keamanan yang sama, algoritma kunci-publik ini membutuhkan jumlah *digit* kunci yang lebih sedikit daripada algoritma kunci-publik lainnya.

[1] A.D Woodbury, D.V BaileyCITU, P. Christof. *Elliptic Curve Cryptography on Smart Cards without Coprocessor.* http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/woodburybaileypaarcardis.pdf Diakses tanggal 6 Januari 2006, pukul 13.00

[2] CITU, *Framework for Information Age Government: Smart Card*. http://www.govtalk.gov.uk/documents/smart_cards_framework_v1-0.pdf. Diakses tanggal 4 Januari 2006, pukul 18.00

[3] J. Hurd, *Elliptic Curve Cryptography: A Case Study in Formalization Using a Higher Order Logic Theorem Prover*, Oxford University, 2005

[4] K. Fukushima, *Elliptic Curve Cyptography Network Security Algorithm* http://palms.ee.princeton.edu/PALMSopen/fiskiran02workload-presentation-with-reference.pdf Diakses tanggal 6 Januari 2006, pukul 13.00

[5] Soon-Yong Choi and Andrew B. Whinston, *Enabling Smart Commerce in the Digital Age*, Center for Research in Electronic Commerce, 1998.
[6] Wikipedia, *Smart Card*, *http://en.wikipedia.org/wiki/Smart_card*
Diakses tanggal 4 Januari 2006, pukul 18.00
[7] *Smart Card White Paper*, *http://www.acersupport.com/library/smartcardwp.pdf*
Diakses tanggal 4 Januari 2006, pukul 18.00