PERANCANGAN SURAT TANDA NOMOR KENDARAAN ELEKTRONIK MENGGUNAKAN SMART CARD DAN SECURE ACCESS MODULE

M. Amin Haris[1], Junartho Halomoan[2], Estananto[3], Fernando Hasudungan[4],

[1, 2, 3, 4]Fakultas Teknik Elektro, Universitas Telkom
[1]amin.haris3323@gmail.com,[2]junartho.halomoan@gmail.com, [3]Estananto@gmail.com, [4]fhasudungan2501@gmail.com

Abstrak

Keamanan merupakan salah satu faktor yang harus dipertimbangkan pada berkas-berkas penting. Surat Tanda Nomor Kendaraan (STNK) merupakan salah satu berkas berharga yang paling sering digunakan hampir setiap hari. Oleh karena itu dibutuhkan sistem keamanan ekstra pada STNK dibanding sistem konvensional saat ini. *Smart card* adalah salah satu solusi yang efektif untuk mengatasi hal tersebut. *Smart card* dapat menyimpan data-data pada STNK seperti pajak, informasi kendaraan, informasi kepemilikan, dan lain-lain. Untuk meningkatkan keamanannya, digunakan *Secure Access Module* (SAM) yang memiliki fitur otentikasi dan algoritma kriptografi. Dengan demikian, usaha pengambilan data pada *smart card* secara ilegal dapat dicegah. Sistem ini diharapkan dapat meningkatkan keamanan pada STNK yang lebih baik dibanding sistem konvesional saat ini.

Kata Kunci: ***Smart Card*, *Secure Access Module, STNK***

Abstract

Security is one of the important factor that should be considered for important documents. STNK is one of important license card that we used the most. Therefore, system with extra security is necessary for STNK, compared with conventional system today. Smart card is one of the most effective solution to solve the problem. Smart card can save the STNKs data such as tax, vehicles information, owners information, etc from unauthorized access. To enhance the security, Secure Access Module (SAM) is used because having authentication and cryptographic algorithm features. The benefit of this security is an illegal data retrieval from the smart card can be prevented. With this new system, the security level in STNKs data is expected to be better compared to conventional system today.

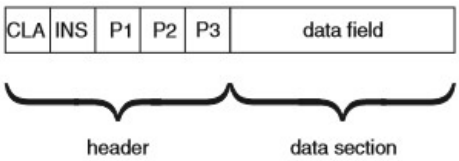
Key Words*: *Smart Card*, *Secure Access Module, STNK

1. Pendahuluan

Bentuk kepemilikan benda berharga yang sah ialah adanya berkas-berkas kepemilikan yang sah. Salah satu contoh berkas yang sering kita jumpai ialah Surat Tanda Nomor Kendaraan (STNK). STNK tentunya harus memiliki tingkat keamanan yang tinggi agar tidak terjadi kejadian yang tidak diinginkan seperti adanya STNK palsu. Saat ini, STNK masih menggunakan sistem konvensional yang masih rentan terjadi penyalinan data pada STNK palsu [**?**].

STNK palsu biasanya ditemukan pada kendaraan curian. Kasus STNK palsu telah banyak terjadi dengan cara menghapus identitas STNK yang sudah mati dengan menggunakan kertas pasir (amplas), lalu dilakukan pengetikan ulang pada STNK palsu tersebut [1]. Selain itu, terdapat pula metode lain dalam menjalankan aksi tersebut, misalkan menggunakan sebuah aplikasi di internet yang dapat mencari gambar STNK, kemudian data STNK dari gambar tersebut dihapus dan diganti dengan data kendaraan yang baru dengan menggunakan sebuah alat *press hologram* [2].

Untuk mengatasi masalah tersebut, dibutuhkan sebuah sistem dengan tingkat keamanan yang lebih tinggi. *Smart card* merupakan solusi dari permasalahan sistem konvensional tersebut. *Smart card* ditujukan untuk menggantikan STNK berbasis kertas sebagai media penyimpanan data-data pada STNK. Untuk meningkatkan tingkat keamanan, digunakan *Secure Access Module* (SAM) yang memiliki fitur otentikasi serta algoritma kriptografi yang tersedia *built-in* pada kartu. SAM akan mengenkripsi data STNK dengan algoritma keamanan beserta *keywords* yang akan disimpan pada SAM, sehingga usaha pengambilan data



Gambar 1. Struktur C-APDU.

secara ilegal sulit dilakukan [3].

Penelitian ini dimaksudkan untuk merancang STNK elektronik berbasis *smart card* dan SAM mengganti sistem STNK konvensional berbasis kertas. Diharapkan data-data penting pada STNK dapat lebih terjamin tingkat keamanannya.

2. Tinjauan Pustaka

Smart card merupakan sebuah kartu plastik yang memiliki sebuah chip di dalamnya. Chip tersebut mengandung sistem operasi tersendiri yang dapat melakukan proses komputasi dengan algoritma tertentu terhadap proses pengisian maupun pembacaan data. Secara umum *smart card* dapat dikategorikan menjadi *contact smart card* dan *contactless smart card* [4] .

SAM merupakan sebuah modul fisik yang berperan sebagai sistem pengamanan data terhadap komunikasi *smart card*. Secara umum, SAM merupakan *contact smart card* yang menggunakan sistem operasi tersendiri yang berfokus dalam pengamanan data. Oleh karena itu, *smart card* dan SAM memiliki karakteristik yang sama dan diatur dalam standar ISO/IEC 7816. Dalam menjalankan proses pengamanannya, SAM telah dilengkapi dengan algoritma kriptografi yang telah diatur pada sistem operasi dan dapat langsung dipanggil dalam pengisian maupun pembacaan data pada smart card [5].

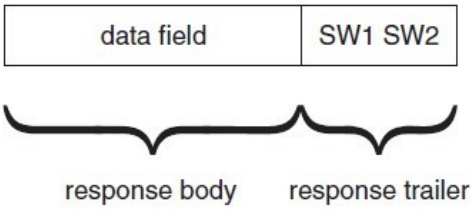
APDU (*Application Protocol Data Unit*) merupakan jenis komunikasi yang digunakan *smart card* untuk berinteraksi dengan *reader*. C-APDU (*Command APDU*) merupakan APDU yang dikirim dari *reader* ke *smart card* dengan format tertentu dan R-APDU (*Response APDU*) merupakan APDU balasan yang dikirim dari *smart card* ke *reader* [6] [7].

Gambar 1 adalah struktur C-APDU. Header C-APDU terdiri dari:

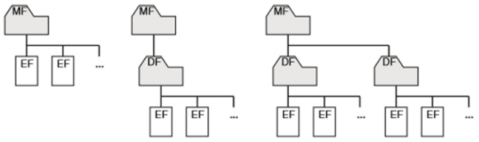
1. *Class of instruction* (CLA) CLA mengidentifikasi kategori C-APDU dari setiap smart card.
2. *Instruction code* (INS) INS merupaan instruksi spesifik dari C-APDU.
3. Parameter 1 dan 2 (P1 dan P2). Parameter yang menyediakan kualifikasi lebih lanjut untuk C-APDU.
4. Parameter 3 (P3). Parameter yang menyatakan panjang data *field* pada C APDU.

Data section C-APDU:

1. *Data Field* menyatakan data yang diperlukan oleh C-APDU. Ukuran maksimal data *field* adalah 255 *byte*.



Gambar 2. Struktur R-APDU.



Gambar 3. Manajemen *File Smart card*.

Gambar 2 menunjukkan struktur R-APDU. R-APDU terdiri dari 2 *field*:

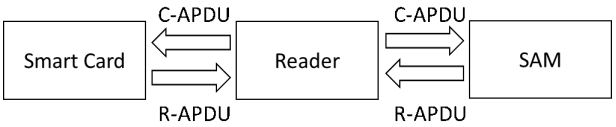
1. *Response Body Response body* berisi data *field* tertentu yang selanjutnya akan ditampilkan sebagai R-APDU.
2. *Response Trailer* Terdiri dari *Status Word* 1 (SW1) dan *Status Word* 2 (SW2). SW1 dan SW2 menunjukkan hasil kondisi dari eksekusi C-APDU terhadap data-data yang dieksekusi.

Gambar 3 merupakan manajemen *file smart card*. Di dalam sistem operasi *smart card* diperlukan manajemen *file* untuk memberikan akses perintah tertentu seperti *read, write*, membuat *file*, menghapus *file*, dan lain-lain. Dasar dari manajemen *file* ialah *Master File* (MF). Pada setiap aplikasi atau suatu grup data akan tersimpan pada *Dedicated File* (DF). Pada setiap MF atau DF dapat menyimpan data masing-masing pada *Elementary File* (EF).

Pada saat proses penulisan data berlangsung, pertama-tama diwajibkan untuk mengatur *management file* dengan urutan dimulai dari MF, DF, dan ke EF [8]. Namun, apabila kita sudah berada pada EF dan ingin berpindah ke EF lain yang berada pada DF yang sama, maka kita tidak perlu kembali ke DF sebelumnya dan cukup langsung memberi perintah untuk berpindah ke EF selanjutnya [9].

3. Perancangan Sistem

Perancangan sistem ini bertujuan untuk menggantikan STNK konvensional berbasis kertas menjadi STNK berbasis *smart card*. Data-data pada STNK konvensional akan dialihkan ke *smart card* dengan menimbang peraturan tentang STNK pada UU no.22 tahun 2009 pasal 68 ayat 2 yang berbunyi:Surat Tanda Nomor Kendaraan Bermotor sebagaimana



Gambar 4. Alur Komunikasi *Smart card* dan SAM.

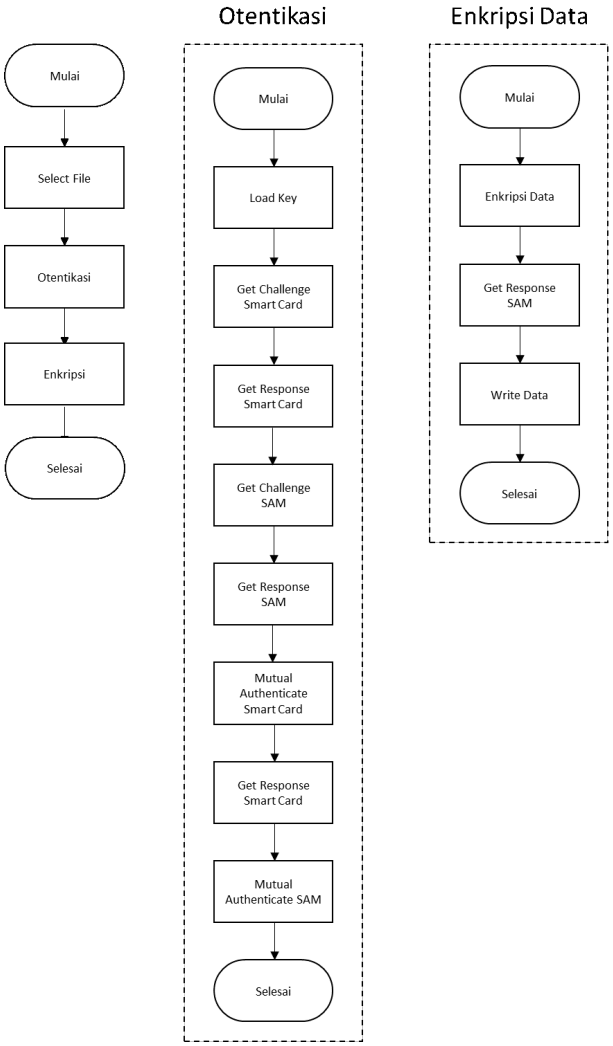
dimaksud pada ayat (1) memuat data kendaraan bermotor, identitas pemilik, nomor registrasi kendaraan bermotor, dan masa berlaku. Adapun data-data STNK tersebut mencakup:

1. Nama Pemilik : 32 karakter
2. Alamat Pemilik : 128 karakter
3. Merk / Tipe : 25 karakter
4. Jenis / Model : 16 karakter
5. Tahun Pembuatan : 9 karakter
6. Warna Kendaraan : 25 karakter
7. Isi Silinder : 8 karakter
8. Nomor Rangka / NIK : 20 karakter
9. Nomor Mesin : 12 karakter
10. Nomor BPKB : 9 karakter
11. Bahan Bakar : 16 karakter
12. Warna TNKB : 8 karakter
13. Kepemilikan Keberapa : 8 karakter
14. Nomor Registrasi : 10 karakter
15. Kode NJKB : 10 karakter
16. Masa Berlaku : 20 karakter
17. Biaya Pajak : 16 karakter

Setiap data pada STNK kemudian akan dituliskan kedalam *smart card* dalam bentuk bilangan heksadesimal dimana satu bilangan heksadesimal, akan dinyatakan sebesar 1 *byte* untuk setiap karakter dengan rentang 00 - FF. Sehingga jumlah data maksimal yang dibutuhkan untuk informasi pada STNK ialah sebanyak 372 *bytes*. Data data yang akan ditulis dalam *smart card* mengikuti format ASCII yang nantinya akan dikonversi kedalam bentuk heksadesimal.

STNK elektronik pada penelitian ini dirancang dengan menggunakan contact *smart card* disertai dengan modul pengaman berupa SAM. Pada dasarnya SAM merupakan *contact smart card*, oleh karena itu *smart card* dan SAM yang digunakan memiliki spesifikasi yang identik. *Smart card* dan SAM yang digunakan memiliki memori sebesar 32 KB dengan menggunakan protokol T = 0 sesuai dengan standar ISO/IEC 7816. Sementara pada SAM digunakan algoritma kriptografi 3DES yang sudah tersedia *built-in* pada kartu sehingga dapat langsung dipanggil dengan menggunakan perintah enkripsi pada APDU. Gambar 4 memaparkan alur komunikasi *smart card* dan SAM.

Komunikasi pada STNK elektronik berbasis *smart card* bersifat *half duplex*. Hal tersebut dikarenakan *smart card* dan SAM merupakan komponen yang hanya bekerja apabila diberi perintah oleh *reader*. Komunikasi



Gambar 5. Diagram Alir Penulisan Data STNK.

hanya akan terjadi apabila *reader* memberikan perintah C-APDU terlebih dahulu yang kemudian akan direspon dengan R-APDU baik pada *smart card* maupun pada SAM. Gambar 5 menunjukkan diagram alir penulisan data STNK.

Pada implementasinya, penggunaan EF untuk masing masing informasi data STNK dinilai kurang efektif karena untuk melakukan proses enkripsi data pada EF yang berbeda memakan cukup banyak waktu. Sehingga, untuk mempercepat waktu respon sistem hanya digunakan 1 EF dimana untuk masing masing informasi yang disimpan pada *smart card* disesuaikan dengan *field map* nya.

Secara keseluruhan terdapat dua tahap yang dilakukan pada saat penulisan *smart card* yaitu tahap otentikasi dan tahap enkripsi data. Tahap otentikasi terjadi ketika SAM dan *Smart Card* saling berkomunikasi sebagai berikut:

Otentikasi

1. Mulai :

   Memulai proses otentikasi.

2. *Load Key* :

   Memuat kunci sebagai penanda perintah dan jenis *file* yang akan dieksekusi pada SAM.

3. *Get Challenge Smart card* :

   Meminta STNK elektronik agar mengirimkan bilangan Heksadesimal secara acak yang akan diinteraksikan dengan SAM.

4. *Get Challenge* SAM :

   Mencocokkan hasil *Get Challenge Smart* Card pada SAM yang selanjutnya akan dipakai dalam proses otentikasi.

5. *Mutual Authenticate Smart card* :

   Melakukan proses otentikasi dari hasil *Get Challenge* SAM pada STNK Elektronik.

6. *Mutual Authenticate* SAM :

   Melakukan proses otentikasi dari hasil *Mutual Authenticate Smart card* pada SAM.

7. *Get Response Smart card* :

   Mengambil hasil eksekusi STNK elektronik pada proses sebelumnya.

8. *Get Response SAM* :

   Mengambil hasil eksekusi SAM pada proses sebelumnya.

9. Selesai :

   Mengakhiri proses Otentikasi.

Enkripsi:

1. Mulai :

   Memulai proses enkripsi data.

2. Enkripsi Data :

   Melakukan proses enkripsi data pada SAM dengan algoritma kriptografi 3DES.

3. *Write Data* :

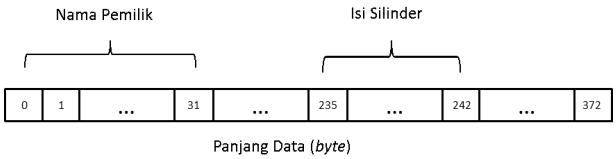
   Melakukan proses penulisan data STNK pada *smart card.*

4. *Get Response* SAM :

   Mengambil hasil eksekusi SAM pada proses sebelumnya.

5. Selesai :

   Mengakhiri proses enkripsi data.



Gambar 6. *Field Map* STNK.

Dalam proses penulisan data, data-data STNK akan disimpan dalam 1 EF yang sama untuk mendapatkan waktu respon yang lebih cepat dibanding dengan menyimpan tiap jenis informasi STNK pada EF yang berbeda-beda. Akan tetapi proses penulisan dengan algoritma kriptografi pada SAM dapat membuat waktu respon menjadi semakin lama untuk melakukan proses penulisan dan enkripsi untuk setiap jenis informasi STNK.

Oleh karena itu, diperlukan suatu aturan dalam penulisan data STNK sesuai dengan urutan dan jumlah karakter pada tiap jenis informasi (*field map*) yang bertujuan untuk mempercepat waktu respon penulisan data.

Waktu respon dapat dioptimalkan dengan meminimalisir proses enkripsi pada penulisan data STNK. Hal tersebut dapat dilakukan dengan merancang *field map*, sehingga hanya diperlukan dua kali proses enkripsi data.

Field map dirancang dengan menggabungkan seluruh data sesuai dengan urutannya dan kemudian dipotong menjadi dua bagian yang terdiri dari 235 *bytes* dan 137 *bytes*. Sehingga proses penulisan dan enkripsi data hanya dilakukan dua kali sehingga perancangan *field map* ini dapat mengoptimalkan waktu respon secara signifikan.

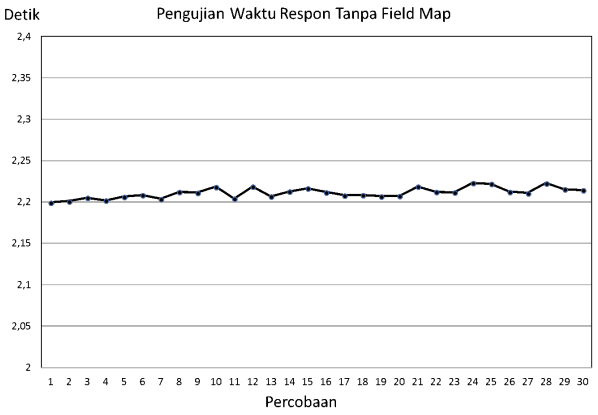
4. Pengujian dan Analisa

Pengujian penulisan data STNK elektronik dilakukan dalam dua kondisi yaitu dengan menggunakan *field map* yang telah dirancang dan pengujian tanpa menggunakan *field map*. Pengujian penulisan data STNK elektronik menggunakan jumlah data maksimal sebesar 372 *bytes* yang telah dirancang sebelumnya. Pengujian dilakukan sebanyak 30 kali percobaan agar mendapatkan hasil yang akurat.

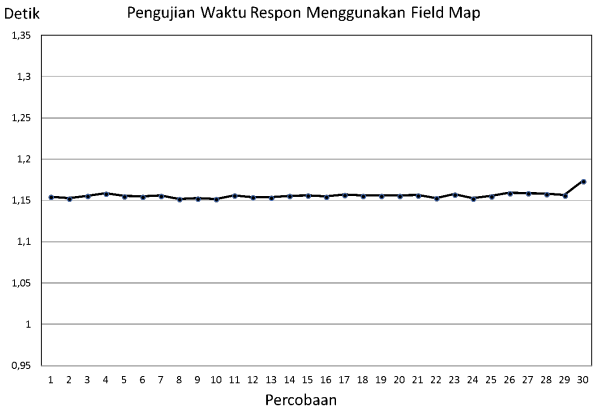
Gambar 6 menggambarkan *field map* STNK. Pada percobaan pertama, pengujian waktu respon dilakukan tanpa menggunakan *field map* yang telah dirancang. Berdasarkan hasil pengujian penulisan data STNK elektronik tanpa menggunakan *field map*, maka nilai rata rata dari 30 kali percobaan dapat dengan menggunakan persamaan (1).

$$\overline{X} = \frac{\sum_{Xi}}{n}, \tag{1}$$

$\overline{X}$ = Mean



Gambar 7. Pengujian Waktu Respon Tanpa *Field map.*



Gambar 8. Pengujian Waktu Respon Menggunakan *Field map.*

$\sum X_i$ = Pengujian

n = Jumlah Pengujian

Dengan menggunakan persamaan 1, diperoleh nilai *mean* dengan percobaan sebanyak 30 kali senilai 2.211186179 detik. Hal ini menunjukkan bahwa penulisan data STNK elektronik mendapatkan hasil yang presisi dengan rentang nilai antara 2.223145008 - 2.199508905 detik.

Pada percobaan pertama, pengujian waktu respon dilakukan dengan menggunakan *field map* yang telah dirancang.

Berdasarkan hasil pengujian penulisan data STNK elektronik dengan menggunakan *field map*, maka kita dapat mengambil nilai rata rata dari 30 kali percobaan dengan menggunakan persamaan (1).

Nilai *mean* dengan percobaan sebanyak 30 kali senilai 1.156134764 detik. Hal ini menunjukkan bahwa penulisan data STNK elektronik mendapatkan hasil yang presisi dengan rentang nilai antara 1.17377615 detik hingga 1.151909113 detik.

Berdasarkan pengujian yang dilakukan terhadap waktu respon, maka dapat disimpulkan bahwa penggunaan *field map* pada proses penulisan data STNK elektronik dapat meningkatkan waktu respon hingga dua kali lipat, dibandingkan dengan proses penulisan tanpa menggunakan *field map*.

Gambar 7 menunjukkan pengujian waktu respon tanpa *field map*, sedangkan Gambar 8 menunjukkan pengujian waktu respon menggunakan *field map*.

5. Kesimpulan

STNK elektronik telah dirancang menggunakan *smart card* serta SAM sebagai modul keamanan dengan menggunakan algoritma kriptografi yang dapat langsung dipanggil dengan instruksi APDU.

Proses penulisan data STNK elektronik dapat dioptimalkan dengan mengatur *field map* pada *smart card* dan dapat meningkatkan waktu respon hingga dua kali lipat dengan rata-rata waktu respon senilai. 1.156134764 detik.

Dengan demikian perancangan STNK elektronik berbasis *smart card* dan *secure access module* dapat menggantikan STNK konvensional berbasis kertas.

Daftar Pustaka

[1] D. I. Ramadhan, "Detiknews," *Polda Jabar Bongkar Praktik Pemalsuan STNK Bermotor*, 2017.

[2] A. Prakasa, "Detiknews," *Polisi Bekuk 4 Sindikat Pemalsu STNK Beromzet Ratusan Juta*, 2017.

[3] W. Rankl and W. Effing, *Smart card handbook*. John Wiley & Sons, 2004.

[4] W. Yu, M. Mao, B. Wang, and X. Liu, "Implementation evaluation of beijing urban master plan based on subway transit smart card data," in *2014 22nd International Conference on Geoinformatics*. IEEE, 2014, pp. 1–6.

[5] W. Rankl, "Smart card applications," *Design Models forusing and programming smart cards, Springer-Verlag*, 2007.

[6] B. R. Hermanto, T. R. Mengko, A. Indrayanto, and T. Rahman, "Application protocol data unit implementation in e-health smart card for health and medical data record," in *2013 3rd International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering (ICICI-BME)*. IEEE, 2013, pp. 396–398.

[7] M. F. F. Khan, Y. Takeshi, I. So, M. Bessho, and K. Sakamura, "A secure and flexible electronic-ticket system," in *2009 33rd Annual IEEE International*

Computer Software and Applications Conference, vol. 1. IEEE, 2009, pp. 421–426.

[8] N. V. Bustillo, D. I. Cendana, and T. D. Palaoag, "E-purse transit pass: The potential of public transport smart card system in the philippines," in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*. IEEE, 2017, pp. 2786–2790.

[9] V. G. Martínez, L. H. Encinas, A. M. Muñoz, M. Á. Mariño, and D. A. Guardeño, "A comparative study of three spanish egoverment smart cards," *Logic Journal of the IGPL*, vol. 25, no. 1, pp. 42–53, 2017.