Jurnal Teknik Elektro Vol. 8 No. 2 ISSN 1411 - 0059
Juli - Desember 2016

Perancangan Emulator KTP Elektronik Berbasis *Java Card* untuk Mendukung Pengujian Fungsionalitas Pembaca KTP Elektronik Industri Nasional

Wahyu Cesar[1] dan Fito Wigunanto[2]

Badan Pengkajian dan Penerapan Teknologi (BPPT) Puspiptek
Serpong, 15314, Indonesia
wahyu.cesar@bppt.go.id [1], fito.wigunanto@bppt.go.id [2]

Abstrak— Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 34 Tahun 2014 menerangkan bahwa pengujian teknologi perlu dilakukan terhadap perangkat pembaca KTP elektronik dalam rangka verifikasi kesesuaian terhadap spesifikasi teknis serta verifikasi fungsionalitas dan kinerja perangkat pembaca KTP-el. Pengujian fungsionalitas merupakan bagian penting dari proses *Quality Control* produk yang akan dijual/ dipasarkan oleh industri. Oleh karena itu proses pengujian ini pasti akan selalu dilakukan oleh seluruh industri yang akan memproduksi perangkat pembaca KTP elektronik. Dalam rangka mendukung tahapan pengujian fungsionalitas pembaca KTP elektronik terintegrasi diperlukan suatu rancangan model emulator KTP elektronik yang dapat mengemulasikan kinerja keseluruhan serta memenuhi aspek keamanan KTP-el. Dalam penelitian ini akan dilakukan perancangan piranti lunak dasar kartu cerdas nirkontak (*contactless smart card*) yang mengacu pada standar SNI ISO/IEC 14443 dengan berbasis teknologi *Java Card* yang memodelkan sistem KTP elektronik (emulator KTP-el). Tujuan dari penelitian ini adalah untuk memberikan solusi teknologi dengan melakukan perancangan emulator KTP elektronik untuk mendukung proses produksi perangkat pembaca KTP-el yang sedang dilakukan oleh industri nasional, khususnya pada fase pengujian kemampuan fungsionalitas produk. Pada penelitian ini akan dihasilkan suatu perangkat emulator ini diharapkan mampu mengemulasikan seluruh fungsi dan kinerja KTP-el dengan tujuan agar dapat mempermudah industri dalam melakukan pengujian fungsionalitas produk, untuk memastikan bahwa perangkat tersebut mampu untuk melakukan pembacaan data KTP-el dengan baik.

Kata kunci— *Quality Control, contactless smart card, Java Card,* emulator KTP-el

I. PENDAHULUAN

Referensi [1] menyatakan perlu dilakukan pengujian teknologi pembaca KTP elektronik terintegrasi oleh setiap industri yang akan memproduksi perangkat tersebut, oleh sebab itu industri terkait sangat membutuhkan banyak sampel KTP-el dan *Security Access Module* (SAM) untuk mendukung kelancaran proses produksi perangkat pembaca KTP-el, khususnya digunakan untuk menguji fungsionalitas produk akhir yang mereka hasilkan. Karena mereka memiliki kendala keterbatasan sampel SAM dan KTP-el, hingga saat ini industri nasional masih mengalami hambatan dalam proses produksi perangkat pembaca KTP-el. Untuk mengatasi kendala tersebut, maka diperlukan penelitian untuk merancang suatu alat yang memiliki kemampuan untuk mengemulasikan seluruh fungsi dan kinerja dari KTP elektronik, sehingga dapat dijadikan sebagai model emulator untuk pengujian.

Membuat rancangan emulator KTP elektronik merupakan salah satu solusi yang dapat mengatasi kendala yang sedang dialami oleh industri nasional pada saat ini. Emulator KTP-el akan dirancang dengan kemampuan mengemulasikan kinerja keseluruhan sistem dan transaksi KTP-el dengan pembaca, yang memenuhi seluruh aspek keamanan KTP elektronik.

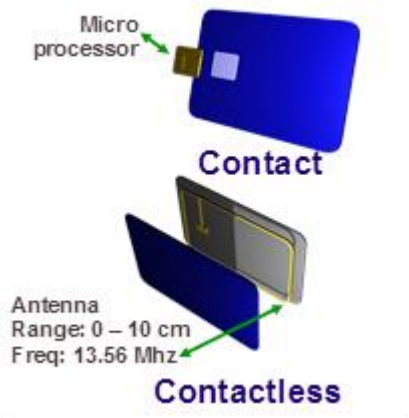
Perangkat emulator KTP-el diharapkan memiliki kemampuan dan fungsi yang sama persis dengan KTP elektronik dengan tujuan agar dapat memenuhi seluruh tahapan uji fungsionalitas produk. Tahap pengujian fungsionalitas ini merupakan bagian penting dari proses *Quality Control* produk yang akan dijual/ dipasarkan oleh industri. Sehingga proses ini pasti selalu akan dilakukan oleh seluruh industri nasional yang akan memproduksi perangkat pembaca KTP-el. Tahapan uji ini dilakukan dengan tujuan untuk memverifikasi fungsi dan kesesuian kinerja dari perangkat tersebut.

Perangkat emulator KTP elektronik ini akan dirancang dan diimplementasi dengan menggunakan kartu cerdas nirkontak (*contactless smart card*) yang berbasis kode yaitu *Java Card* dengan tujuan agar lebih fleksibel dalam menerima *command* atau perintah spesifik yang digunakan pada KTP elektronik *Production*.

Tujuan dari penelitian ini antara lain untuk menawarkan solusi teknologi dengan melakukan perancangan dan implementasi emulator KTP elektronik untuk mendukung proses produksi perangkat pembaca KTP-el yang hingga saat ini sedang dilakukan oleh industri nasional, khususnya dalam hal menguji kemampuan fungsionalitas produk. serta sebagai

salah satu bentuk dukungan dari sebuah instansi teknis milik pemerintah, dalam hal ini BPPT, terhadap penerapan suatu teknologi yang relatif baru di Indonesia. Diharapkan hasil dari kegiatan ini dapat bermanfaat bagi bangsa dan negara, serta berdampak positif bagi penguatan Negara Kesatuan Republik Indonesia (NKRI).

Sasaran utama dari penelitian ini yaitu menghasilkan desain piranti lunak pada kartu cerdas nirkontak berbasis *Java Card* yang dapat memodelkan seluruh sistem KTP elektronik (emulator KTP-el) dengan menggunakan jenis kartu cerdas nirkontak *Java Card* yang mengacu pada standar SNI ISO/IEC 14443 Tipe A dan Tipe B. Dan juga memodelkan sistem Secure Access Module KTP-el (emulator SAM KTP-el) dengan menggunakan jenis kartu cerdas kontak *Java Card* yang keduanya akan diemulasikan dengan hasil rancangan prototipe perangkat pembaca KTP-el terintegrasi yang telah dikembangkan oleh industri nasional.



Gambar 1. Bentuk fisik kartu cerdas

Kartu cerdas *Java Card* adalah teknologi yang telah matang, baik dari sisi standar, ketersediaan, dan implementasi, serta banyak digunakan untuk keperluan pengelolaan data kependudukan secara elektronik (eID) di seluruh dunia. Apabila dibandingkan dengan teknologi sejenis lainnya, misalnya *bar code* dan *magnetic stripe*, *Java Card* memiliki banyak kelebihan, seperti kapasitas penyimpanan data yang besar (dalam satuan Kilo Byte) dan menawarkan fitur-fitur keamanan, multi aplikasi, efisiensi, interoperabilitas, otentikasi, manajemen identitas, manajemen data, dan lain sebagainya. Kombinasi antara teknologi *Smart card* dan biometrik akan menghasilkan sebuah perangkat untuk keperluan manajemen identitas yang sangat dapat dipercaya.

Referensi [2] menyatakan pada jenis antarmuka yang digunakan untuk berkomunikasi dengan perangkat pembaca (*reader*), kartu cerdas dapat diklasifikasikan menjadi:

1) Kartu Cerdas Kontak (*Contact Smart Card*). *Smart card* jenis ini memiliki area kontak yang terlihat pada permukaan kartu. Harus dimasukkan ke dalam *reader* untuk melakukan transaksi data. Umumnya digunakan untuk keperluan identifikasi personal, transaksi finansial, dan pengendalian akses ke program aplikasi pada komputer.

2) Kartu Cerdas Nirkontak (*Contactless Smart Card*). *Smart card* jenis ini menggunakan gelombang frekuensi radio (*radio frequency*, RF) untuk melakukan transaksi data. *Smart card* dan *reader* dilengkapi dengan antena. Jarak transaksi berkisar sampai dengan 10 cm. Umumnya digunakan untuk keperluan identifikasi personal, pengendalian akses fisik, dan keperluan yang membutuhkan proses cepat.

3) Kartu Cerdas Hybrid (*Smart Card Hybrid*). Memiliki dua buah *chip*, satu dengan antarmuka kontak dan satu dengan antarmuka nirkontak. Kedua *chip* tersebut umumnya tidak saling berhubungan.

4) Kartu Cerdas Dual-Interface (*Smart Card Dual-Interface Chip*). Memiliki sebuah *chip* dengan antarmuka kontak dan nirkontak. Transaksi dapat dilakukan dengan menggunakan *reader* kontak maupun nirkontak.

Dengan menyesuaikan dokumen spesifikasi teknis KTP elektronik yang dikeluarkan oleh Kementrian Dalam Negeri Republik Indonesia yang disebutkan bahwa kartu cerdas yang digunakan untuk KTP elektronik adalah jenis kartu cerdas nirkontak dan harus mengacu pada standar SNI ISO/IEC 14443 tipe A atau tipe B. Selain itu, terdapat beberapa kriteria lainnya, seperti penggunaan SAM dalam proses otentikasi data secara dua arah (metode *Mutual Authentication*), pengamanan komunikasi antara *Smart card* dan *reader* (metode *Secure Messaging*), serta pengamanan data yang disimpan dalam *chip* (metode *Encrypted Data*). Seluruh kriteria tersebut harus dapat dipenuhi oleh perangkat emulator yang akan dirancang ini agar dapat menguji seluruh fungsi elektronik dari KTP-el (Gambar 2) yang seharusnya mampu dilakukan oleh perangkat pembaca KTP-el untuk dijadikan acuan bagi industri nasional terkait.

Gambar 2. Fungsi elektronik KTP-el

Kartu cerdas nirkontak KTP-el menerapkan struktur *file* seperti dalam standar SNI ISO/IEC 7816-4 yang serupa dengan struktur *folder* pada sistem operasi komputer. Secara umum struktur *file* pada kartu cerdas dapat dibagi menjadi dua kategori [3]. Kategori pertama adalah *file* yang selalu diasosiasikan dengan sebuah aplikasi, yang disebut dengan *Dedicated Files* (DF). Kategori kedua adalah *file* yang menyimpan data aktual, yang disebut dengan *Elementary File* (EF). Sebuah DF bertindak sebagai tempat untuk memuat DF lainnya atau EF yang secara logis menjadi milik sebuah aplikasi. Sedangkan EF dapat dibagi menjadi EF yang digunakan untuk menyimpan data pengguna dan EF yang

digunakan oleh sistem operasi untuk keperluan internal, misalnya untuk menyimpan kunci rahasia dan kode program. Di atas DF dan EF terdapat sebuah *Master File* (MF). *File* ini secara implisit akan terpilih setelah komunikasi dengan kartu cerdas diulang. *File* ini adalah sebuah DF jenis khusus, dan mengindikasikan batas memori yang tersedia untuk *file*. Setiap kartu cerdas harus memiliki sebuah MF.

II. METODE

Perangkat KTP elektronik hanya mampu menerima perintah dalam format Application Protocol Data Unit (APDU) mengacu pada standar SNI ISO/IEC 7816-4 yang dilakukan oleh program aplikasi menggunakan teknologi frekuensi radio (*Radio Frequency*/RF). Selanjutnya, program aplikasi akan menerima balasan dari *Smart card* KTP-el yang diberikan dalam format APDU pula.

APDU yang digunakan pada transaksi antara kartu cerdas KTP-el dan program aplikasi (terminal) dapat dibagi menjadi dua kategori [3] yaitu:

- APDU perintah (*command*). APDU ini merupakan perintah yang diberikan oleh program aplikasi komputer ke kartu cerdas nirkontak, melalui perangkat *reader*. APDU ini berisi header yang bersifat wajib (CLA, INS, P1, P2) dengan panjang masing-masing 1 byte, dan data dengan panjang 0 sampai dengan 256 byte [3].
- APDU balasan (*response*). APDU ini merupakan balasan dari kartu cerdas nirkontak terhadap perintah yang diberikan oleh program aplikasi komputer. APDU ini berisi status transaksi dengan panjang 2 byte, dan data dengan panjang 0 sampai dengan 256 byte [3].

Struktur lengkap dari sebuah APDU perintah adalah sebagai berikut:

1 byte	1 byte	1byte	1 byte	1 byte	0~256 byte	1 byte
CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**
←	***Header* wajib**	→	←	**Opsional**		→

Keterangan:

CLA : Menyatakan jenis perintah yang diberikan, misalnya *proprietary* atau terbuka.

INS : Menyatakan kode instruksi yang mengacu pada standar SNI ISO/IEC 7816-4, misalnya kode 'B0' (READ BINARY) untuk mendapatkan data dalam bentuk biner dari kartu cerdas nirkontak.

P1 : Menyatakan offset (MSB) dari *file* tempat data yang ditransaksikan.

P2 : Menyatakan offset (LSB) dari *file* tempat data yang ditransaksikan.

Lc : Menyatakan panjang data yang ada di dalam APDU.

Data : Data di dalam APDU perintah.

Le : Menyatakan panjang data yang diminta dari kartu cerdas nirkontak.

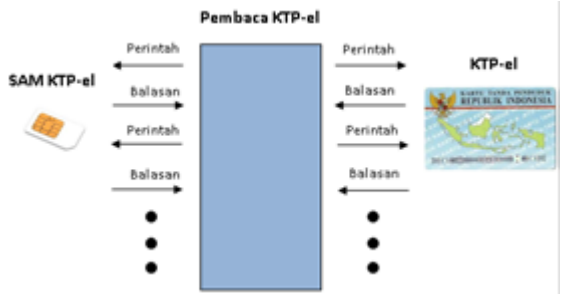
Sedangkan struktur lengkap dari sebuah APDU balasan adalah sebagai berikut:

2 byte	n byte
Status	**Data**

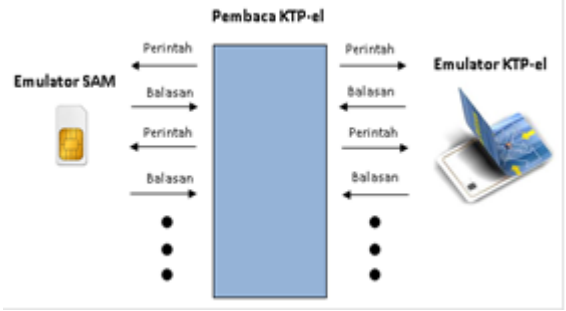
Transaksi membaca data dari kartu cerdas KTP-el, atau menyimpan data ke dalam kartu cerdas KTP-el, dapat diawali dengan proses autentikasi dua arah (*mutual authentication*). Proses ini menggunakan metode umpan balik (*challenge*/*response*) untuk menguji keabsahan dari perangkat *reader* dan kartu cerdas nirkontak yang melakukan transaksi.

Perangkat emulator KTP-el akan dirancang dengan mengacu terhadap standar SNI ISO/IEC 14443 Tipe A/B, dan akan melakukan komunikasi dengan perintah protokol standar SNI ISO/IEC 7816-4. Jenis kartu cerdas yang akan digunakan sebagai emulator KTP-el menggunakan teknologi *Java Card*. Teknologi *Java Card* pada dasarnya merupakan *platform* kartu cerdas yang aplikasinya berbasis pemrograman java (java *programming*) yang dalam hal ini disebut Applet. Kelebihan teknologi *Java Card* dari jenis *smart card* yang lain adalah *platform* aplikasinya lebih fleksibel karena berbasis kode program (*code programmable*), sehingga pengembang aplikasi dapat dengan mudah memprogram sistem kerja dari kartu cerdas tersebut sesuai kebutuhan.

Applet yang akan dikembangkan pada perangkat emulator KTP-el dan emulator SAM KTP-el menggunakan format protokol APDU. APDU perintah (*command*) dan balasan (*response*) yang dikerjakan oleh perangkat emulator akan disamakan atau disesuaikan dengan APDU perintah dan balasan yang dilakukan pada KTP elektronik dan SAM *Production*.



Gambar 3. Mekanisme transaksi pembacaan data pada KTP-el *Production*



Gambar 4. Mekanisme transaksi pembacaan data dengan emulator KTP-el

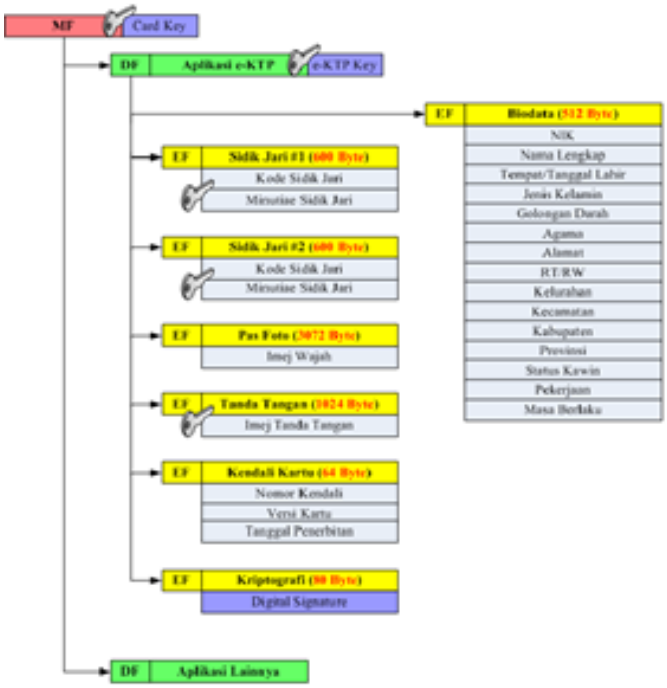
Pengujian teknologi perlu dilakukan terhadap perangkat pembaca KTP elektronik dalam rangka verifikasi kesesuaian terhadap spesifikasi teknis serta verifikasi fungsionalitas dan kinerja perangkat pembaca KTP-el [1]. Pada mekanisme transaksi dengan emulator KTP-el dan emulator SAM seperti terlihat pada Gambar 4. Emulator KTP-el dirancang untuk tidak memiliki perbedaan seluruh tahapan APDU perintah (*command*) maupun balasan (*response*) seperti halnya yang dikerjakan oleh KTP-el dan SAM *Production* (Gambar 3). Mekanisme uji fungsionalitas KTP-el dapat dilakukan hanya dengan mengganti KTP-el dan SAM *Production* dengan perangkat emulator KTP-el dan emulator SAM maka seluruh proses mekanisme transaksi pembacaan data KTP-el dapat dilakukan dengan baik, sehingga dapat memudahkan proses pengujian fungsionalitas perangkat pembaca KTP-el oleh industri.

Tabel I menunjukan detail tahapan mekanisme transaksi pembacaan data KTP elektronik yang dapat dijadikan acuan perancangan emulator KTP-el.

TABEL I. PROSEDUR PEMBACAAN DATA KTP-EL

No.	*Command*	*Destination*
1.	Open Access SAM KTP-el	SAM
2.	Get UID Type A	KTP-el
3.	Select DF KTP-el	KTP-el
4.	Select EF Photograph	KTP-el
5.	Read Photograph	KTP-el
6.	Get UID Type B	KTP-el
7.	Select EF Card Control	KTP-el
8.	Read Card Control	KTP-el
9.	Reset SAM	SAM
10.	Get Challenge	KTP-el
11.	SAM Calculate Challenge	SAM
12.	External Authenticate	KTP-el
13	Internal Authenticate	SAM
14.	Select EF Digital Signature with Secure Messaging	KTP-el
15.	Read Digital Signature with Secure Messaging	KTP-el
16.	SAM Start Digital Signature Automatic Verification	SAM
17.	SAM Retrieve Digital Signature	SAM
18.	Select EF Biodata with Secure Messaging	KTP-el
19.	Read Biodata with Secure Messaging	KTP-el
20.	SAM Retrieve Photograph	SAM
21.	SAM Perform Automatic Dechipering	SAM
22.	Select EF Signature with Secure Messaging	KTP-el
23.	Read Signature with Secure Messaging	KTP-el
24.	Select EF Minutiae #1 with Secure Messaging	KTP-el
25.	Read Minutiae #1 with Secure Messaging	KTP-el
26.	Select EF Minutiae #2 with Secure Messaging	KTP-el
27.	Read Minutiae #2 with Secure Messaging	KTP-el
28.	SAM Stop Digital Signature Automatic Verification	SAM
29.	SAM Verify Digital Signature	SAM

Pengelompokan data kependudukan pada emulator KTP-el mengikuti tata cara pengelompokan data KTP-el *Production* yaitu mengacu terhadap standar The International Civil Aviation Organization (ICAO) dalam menentukan grup data (*Data Group*, DG) untuk passpor elektronik (*ePassport*), ICAO menyampaikannya dalam Doc 9303 tentang *Logical Data Structure* (LDS). Ilustrasi pengelompokan data kependudukan pada KTP-el seperti yang diperlihatkan pada Gambar 5.



Gambar 5. Pengelompokan data kependudukan pada KTP elektronik

Perancangan emulator model kartu cerdas KTP-el menggunakan sebuah kartu cerdas nirkontak dengan teknologi yang berbasis kode (*code base*). Proses perancangan emulator ini dengan cara membentuk sebuah aplikasi (applet) yang ditempatkan di dalam ruang kartu cerdas nirkontak JCOP (*Java Card Open Platform*) yang dapat berfungsi untuk mengemulasikan seluruh fungsi dari KTP elektronik. Rancangan keseluruhan fungsi pada emulator model kartu cerdas KTP-el mengacu SNI ISO/IEC 7816-4.

Dengan teknologi berbasis *Java Card* Open *Platform* (JCOP) dirancang suatu applet yang dapat memenuhi seluruh tahapan prosedur pembacaan data KTP elektronik (Tabel I) dan juga dirancang applet emulator SAM yang dapat mengimplementasikan seluruh fungsi dari SAM KTP-el *Production*.

Lingkup tahapan kegiatan penelitian yang dilakukan untuk menghasilkan perangkat emulator KTP-el adalah sebagai berikut:

1. Merancang kunci akses kendali keamanan dan menentukan algoritma kriptografi untuk mekanisme otentikasi dua arah emulator KTP-el dan emulator SAM.
2. Membuat aplikasi data kependudukan yang serupa dengan KTP-el mulai dari struktur data hingga format penyimpanan data, dan menerapkannya pada kartu cerdas nirkontak *Java Card* yang akan dirancang menjadi perangkat emulator KTP-el.
3. Melakukan penyimpanan data Biodata, Photo, Tanda Tangan Digital, Minutiae Sidik Jari dan *Digital Signature* pada kartu cerdas *Java Card* yang akan dirancang menjadi perangkat emulator KTP-el
4. Membuat aplikasi SAM pada kartu cerdas kontak *Java Card* dengan fitur yang serupa dengan SAM KTP-el *Production*, namun dengan kunci yang berbeda.
5. Melakukan pengujian proses pembacaan data dengan menggunakan prototipe perangkat pembaca KTP-el yang dikembangkan BPPT dengan emulator KTP-el dan SAM.
6. Melakukan pengujian fungsionalitas produk perangkat pembaca KTP-el yang dikembangkan industri nasional dengan menggunakan hasil rancangan perangkat emulator KTP-el dan SAM.

Emulator KTP-el diharuskan dapat memenuhi seluruh tahapan metode uji fungsionalitas perangkat pembaca KTP-el agar mampu mengetahui kemampuan program aplikasi pada perangkat pembaca KTP elektronik tersebut. Referensi [4] menyatakan Butir-butir metode uji fungsionalitas perangkat pembaca KTP-el adalah sebagai berikut:

- Pengujian fungsi melakukan verifikasi keabsahan KTP Elektronik
- Pengujian fungsi membaca data KTP Elektronik
- Pengujian fungsi melakukan verifikasi keabsahan data KTP Elektronik
- Pengujian fungsi menampilkan data KTP Elektronik
- Pengujian fungsi melakukan aktifasi KTP Elektronik

III. HASIL DAN PEMBAHASAN

Hasil rancangan emulator model kartu cerdas KTP-el dengan menggunakan kartu cerdas nirkontak dengan teknologi yang berbasis kode (*code base*) yaitu dalam bentuk suatu aplikasi (applet) yang ditempatkan di dalam ruang memori EEPROM kartu cerdas nirkontak JCOP (*Java Card Open Platform*) yang mampu mengemulasikan seluruh fungsi dari KTP elektronik. Rancangan keseluruhan fungsi pada emulator kartu cerdas KTP-el mengacu SNI ISO/IEC 7816-4.

Sistem keamanan hasil rancangan emulator kartu cerdas KTP-el menggunakan algoritma kriptografi Triple DES (*Data Encryption Standard*) untuk proses otentikasi dua arah dan SHA-256 (*Secure Hash Algorithm*) untuk mekanisme digital signature. Informasi mengenai kunci kriptografi kartu cerdas sangat dijaga ketat dan terkendali. Oleh karena itu, dalam artikel ini hanya disampaikan sebuah contoh diversifikasi kunci kriptografi sederhana dengan menggunakan tata cara yang ditentukan sendiri sebagai model proses diversifikasi kunci emulator KTP-el. Rumus dasar untuk melakukan diversifikasi kunci kriptografi sederhana emulator KTP-el adalah sebagai berikut:

Diversified Key = enc(*key*, *data*)

Algorithm : AES-128

Mode : Cipher Block Chaining (CBC)

Contoh proses penurunan kunci kriptografi emulator KTP-el (dalam byte heksadesimal):

MASTER KEY = F6128D09A0636A5EFE18B6BF937FF69F
MF KEY = enc(MASTER KEY, MF INFO)
MF INFO = Hex (“Multiapplication”) = 4D756C74696170706C69636174696F6E
MF KEY = DE73055D8F003329A6D408C151A5B8FB
DF KEY = enc(MF KEY, DF INFO)
DF INFO = Hex(“BPPTCardeID_____”) = 42505054436172646549445F5F5F5F5F
DF KEY = 4A0917FB496827DC4D5D1BF928D42EC1
EF KEY = enc(DF KEY, EF INFO)
- *Read Key*:
EF INFO = Hex(02740030329157) + Hex(“eID_____”) + Hex(1) = 027400303291576549445F5F5F5F5F01
EF KEY = 3EE5FF70757211BCA38B49F5310CE3A7
- *Write Key:*
EF INFO = Hex(02740030329157) + Hex(“eID_____”) + Hex(2) = 027400303291576549445F5F5F5F5F02
EF KEY = 8AF4336502D74E14A2BED79F5AE3D9AB

Pembuatan model aplikasi (applet) pada kartu cerdas JCOP menggunakan bahasa pemrogramman Java yang dioperasikan dengan menggunakan JCOP *tools* untuk keperluan installasi applet pada *Java Card*. Selain itu juga digunakan *smart card reader* untuk proses installasi applet tersebut.

Pembuatan model emulator SAM KTP-el juga menggunakan JCOP jenis kontak yang *programmable code*. JCOP *tools* juga digunakan untuk keperluan installasi applet emulator SAM.

Gambar 6. Proses installasi Applet *Java Card* menggunakan *smart card reader*

Perintah-perintah untuk melakukan komunikasi dengan emulator kartu cerdas KTP-el adalah perintah-perintah standar SNI ISO/IEC 7816-4. Berikut ini adalah beberapa perintah yang digunakan:

- **GET CHALLENGE**

Perintah GET CHALLENGE digunakan untuk mendapatkan bilangan acak (*random number*) dari emulator kartu cerdas KTP-el. APDU perintah-respons GET CHALLENGE adalah seperti yang diperlihatkan pada Tabel II.

TABEL II. APDU PERINTAH GET CHALLENGE

Kode	Nilai
CLA	'00'
INS	'84'
P1	'00'
P2	'00'
Lc	-
Data	-
Le	'08'

- **EXTERNAL AUTHENTICATE**

Perintah EXTERNAL AUTHENTICATE digunakan untuk mendapatkan akses administrasi dari kartu cerdas KTP-el. APDU perintah EXTERNAL AUTHENTICATE adalah seperti yang diperlihatkan pada Tabel III.

TABEL III. APDU PERINTAH EXTERNAL AUTHENTICATE

Kode	Nilai
CLA	'00'
INS	'82'
P1	'00'
P2	'00'
Lc	'18'
Data	*Authentication Data*
Le	-

- **SELECT FILE**

Perintah SELECT *FILE* digunakan untuk memilih *Dedicated File* (DF) atau *Elementary File* (EF) pada kartu cerdas KTP-el. APDU perintah SELECT *FILE* adalah seperti yang diperlihatkan pada Tabel IV.

TABEL IV. APDU PERINTAH SELECT FILE

Kode	Nilai
CLA	'00'
INS	'A4'
P1	'00'
P2	'00'
Lc	*Data Length*
Data	*File* ID
Le	-

- **READ BINARY**

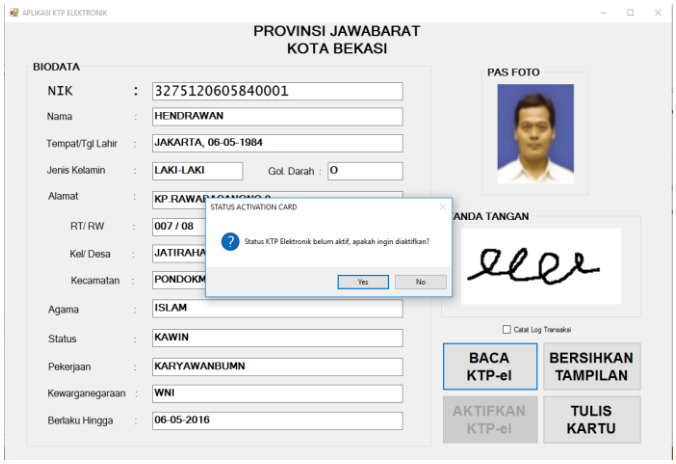
Perintah READ BINARY digunakan untuk membaca data *Elementary File* (EF) pada kartu cerdas KTP-el. APDU perintah untuk READ BINARY adalah seperti yang diperlihatkan pada Tabel V.

TABEL V. APDU PERINTAH READ BINARY

Kode	Nilai
CLA	'00'
INS	'B0'
P1	Parameter P1
P2	Parameter P2
Lc	-
Data	-
Le	*Data Length*

Parameter P1 dan P2 pada APDU perintah READ BINARY merupakan parameter alamat memori (*memory address*) EEPROM dari *chip Smart card* sebagai informasi alamat data yang akan dibaca oleh terminal aplikasi. Hasil respon pembacaan data akan diterima dalam format bilangan heksadesimal yang akan diikuti dengan informasi status transaksi (SW1SW2) yang pada umumnya apabila transaksi APDU berhasil adalah '9000', namun apabila transaksi APDU mengalami kesalahan maka informasi status transaksi (SW1SW2) dapat dilihat pada dokumen SNI ISO/IEC 7816.

Emulator kartu cerdas KTP-el dan emulator SAM telah dirancang untuk memenuhi seluruh prosedur tahapan pembacaan data KTP-el (Tabel I), sehingga proses pembacaan data KTP-el oleh perangkat pembaca KTP-el dapat diemulasikan oleh emulator tersebut. Gambar 7 menunjukan contoh hasil pembacaan data KTP-el dengan menggunakan emulator kartu cerdas KTP-el menggunakan data *dummy*.



Gambar 7. Tampilan hasil pembacaan data *dummy* dari emulator KTP-el

Pembacaan data dari emulator KTP-el dilakukan melalui proses otentikasi dua arah (*mutual authentication*), pengamanan komunikasi transaksi APDU (*secure messaging*) antara emulator KTP-el dan SAM, pengamanan penyimpanan data (*encrypted data*), verifikasi keabsahan data dengan melalui proses verifikasi *digital signature*, dan juga melalui proses verifikasi sidik jari seperti halnya pada prosedur pembacaan data KTP elektronik *Production* yang sah.

Emulator KTP-el dirancang untuk dapat memenuhi seluruh tahapan metode uji fungsionalitas perangkat pembaca KTP-el agar mampu mengukur kemampuan program aplikasi dari perangkat pembaca KTP elektronik hasil pengembangan industri nasional. Pada Tabel II merupakan butir-butir pengujian fungsionalitas perangkat pembaca KTP elektronik yang mampu dipenuhi oleh perangkat emulator kartu cerdas KTP-el.

Hasil implementasi emulator kartu cerdas KTP-el dapat memenuhi butir–butir pengujian fungsionalitas perangkat pembaca KTP Elektronik. Tabel VI menunjukan contoh hasil pengujian fungsionalitas pembacaan data KTP Elektronik yang mampu dipenuhi oleh perangkat emulator KTP-el yang diujikan pada prototipe perangkat pembaca KTP-el terintegrasi hasil pengembangan tim KTP Elektronik BPPT. Hasil pengujian tersebut diperlihatkan pada Gambar 8.

Gambar 8. Hasil pengujian fungsionalitas pembacaan data KTP Elektronik pada prototipe perangkat pembaca KTP-el BPPT menggunakan emulator KTP-el

TABEL VI. PENGUJIAN FUNGSIONALITAS PEMBACA KTP-EL YANG MAMPU DIPENUHI EMULATOR KTP-EL

Pengujian	Butir Pengujian	Indikator
Verifikasi keabsahan KTP Elektronik	• Otentikasi dua arah (*Mutual Authentication*) • Komunikasi teramankan (*Secure Messaging*)	Berhasil atau tidaknya transaksi pembacaan data dengan SAM KTP Elektronik yang sah
Pembacaan data KTP Elektronik	• Pembacaan seluruh data KTP-el Tipe A • Pembacaan seluruh data KTP-el Tipe B	Berhasil atau tidaknya membaca seluruh data pada KTP-el Tipe A dan B
Verifikasi keabsahan data KTP Elektronik	• Verifikasi prosedur pembacaan data KTP-el • Verifikasi *Digital Signature* KTP-el oleh SAM KTP-el yang sah	Berhasil atau tidaknya melakukan verifikasi *Digital Signature* KTP-el dengan status heksadesimal 2 byte “0010” dari SAM KTP-el yang sah
Menampilkan data KTP Elektronik	• Pembacaan data KTP-el secara lengkap dan sesuai prosedur • Menampilkan data KTP Elektronik secara lengkap	Berhasil atau tidaknya menampilkan hasil dari proses pembacaan data KTP-el secara lengkap dan sesuai prosedur
Aktifasi KTP Elektronik	• Melakukan aktifasi KTP-el sesuai prosedur	Berhasil atau tidaknya proses aktifasi KTP-el dengan SAM sah

IV. SIMPULAN DAN SARAN

Dari hasil kegiatan penelitian ini maka dapat disimpulkan bahwa:

1. Perancangan emulator KTP-el sangat dibutuhkan untuk mengatasi keterbatasan sampel KTP-el dan SAM (*Secure Access Module*) *Production* yang dimiliki oleh industri nasional yang secara langsung akan berdampak positif untuk mendukung kelancaran proses produksi perangkat pembaca KTP-el.
2. Emulator KTP Elektronik sangat bermanfaat untuk mendukung proses pengujian fungsionalitas perangkat pembaca KTP-el.
3. Emulator KTP Elektronik dan SAM dapat diimplementasikan menggunakan kartu cerdas *Java Card* yang berbasis *Open Platform* (JCOP).
4. KTP Elektronik dapat juga diimplementasikan menggunakan kartu cerdas yang berbasis kode (*code base*) dengan model multiaplikasi (*multi-applet*) yang memiliki kemampuan dan kapasitas memori yang jauh lebih besar.
5. Emulator KTP-el dan SAM dapat memberikan solusi teknologi kepada pihak industri nasional sebagai pengembang perangkat pembaca KTP-el agar dapat melakukan akselerasi proses produksi perangkat tersebut.

Saran dari hasil kegiatan penelitian ini adalah sebagai berikut:

1. Diharapkan dari hasil pengembangan emulator KTP-el dan SAM ini dapat dimanfaatkan dengan baik oleh industri nasional untuk meningkatkan kualitas produk serta mempercepat proses produksi Perangkat Pembaca KTP-el.
2. Diharapkan agar KTP Elektronik generasi berikutnya dapat memanfaatkan kartu cerdas yang berbasis kode *Java Card* Open *Platform* (JCOP) sehingga lebih memudahkan untuk melakukan proses multiaplikasi.
3. Diharapkan agar hasil perancangan emulator KTP-el dan SAM ini dapat menjadi cikal bakal terbentuknya standard interoperabilitas *chip smart card* KTP Elekronik Indonesia yang mungkin disediakan oleh berbagai vendor *chip* di seluruh dunia.
4. Diharapkan agar dari hasil penelitian ini dapat dimanfaatkan untuk pengembangan KTP elektronik generasi berikutnya yang lebih bersifat *programmable*, multiaplikasi dan berbasis *open platform*.

Semoga dari hasil penelitian ini dapat mendorong pengembangan KTP Elektronik Indonesia yang lebih optimal kedepannya dan arah pemanfaatan KTP-el dapat lebih bersifat multifungsi untuk keperluan lain, seperti transaksi keuangan, asuransi, pajak, kesehatan, parkir, dan lain sebagainya.

UCAPAN TERIMA KASIH

Ucapan terimakasih ditujukan kepada Kementrian Riset Teknologi dan Pendidikan Tinggi (RistekDikti) selaku penyandang dana dalam penelitian ini melalui kegiatan Insentif Riset Sistim Inovasi Nasional (SINas) tahun 2016 pada judul penelitian “Perancangan Perangkat Emulator KTP Elektronik untuk Mendukung Proses Produksi Pembaca KTP Elektronik Industri Nasional” dengan nomor kontrak penelitian 036. Semoga hasil penelitian ini dapat bermanfaat bagi perkembangan teknologi Negara Kesatuan Republik Indonesia.

REFERENSI

[1] Kementrian Dalam Negeri Republik Indonesia, 2014, Lampiran Permendagri No.34 Tahun 2014, Tentang Spesifikasi Teknis Perangkat Pembaca Kartu Tanda Penduduk Elektronik.

[2] Wolfgang Rankl dan Wolfgang Effing, 2003, *Smart card Handbook 3th Edition*, John Wiley & Sons.

[3] International Standard, 2005, ISO/IEC 7816-4 Organization, Security and *Command*s for Interchange.

[4] Dwidharma Priyasta, 2013, *Rekomendasi Standar Perangkat Pembaca KTP Elektronik Mandiri*, Bagian 4: Program Aplikasi KTP Elektronik.