p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

PENGEMBANGAN METODE UJI KESESUAIAN PERILAKU KARTU CERDAS TERHADAP KTP ELEKTRONIK

Dwidharma Priyasta
Pusat Teknologi Elektronika (PTE), Badan Pengkajian dan Penerapan Teknologi (BPPT)
Gedung Teknologi 3 Kawasan Puspiptek, Jl. Raya Puspiptek, Tangerang Selatan, Banten 15314
dwidharma.priyasta@bppt.go.id

Abstrak

Makalah ini melaporkan hasil pengembangan sebuah metode uji untuk mengukur kesesuaian perilaku sebuah kartu cerdas (*smart card*) terhadap KTP Elektronik. Tujuannya adalah untuk memastikan kemampuan dari kartu cerdas tersebut sebagai tempat bagi aplikasi KTP Elektronik. Metode uji ini memuat skenario-skenario pengujian yang menerapkan standar-standar ISO/IEC 7816-4, ICAO Doc 9303 dan ISO/IEC 9797-1. Metode uji ini telah diterapkan pada sebuah sistem sederhana yang terdiri dari sebuah pembaca kartu cerdas (*smart card reader*) dan program aplikasi komputer yang kemudian dicobakan ke blangko KTP Elektronik dan ke produk-produk kartu cerdas lainnya. Hasil uji coba memperlihatkan bahwa metode uji ini 100% akurat dan andal.

Kata Kunci: metode uji, KTP Elektronik

Abstract

This paper reports on the development of a test method for measuring the behavior of a smart card against the national electronic identity cards. The goal is to determine the ability of the smart card as a place for the national electronic identity card application. This test method contains test scenarios that apply ISO/IEC 7816-4, ICAO Doc 9303 and ISO/IEC 9797-1 standards. This test method had been applied to a simple system consisting of a smart card reader and a computer application program which was then tried out on the national electronic identity cards and other smart card products. The result shows that this test method is 100% accurate and reliable.

Keywords: test method, the national electronic identity cards

PENDAHULUAN

Kartu cerdas yang menggunakan sistem operasi *native* memiliki perilaku bawaan yang diberikan oleh produsen kartu cerdas tersebut. Perilaku ini terkait dengan status siklus hidup, sistem berkas, perintah-perintah dan prosedur keamanan yang diterapkan pada kartu cerdas dan akan dimiliki oleh setiap aplikasi yang ada di dalamnya. Perilaku ini harus dipahami oleh setiap pembaca kartu cerdas yang ingin berkomunikasi (operasi baca/tulis) dengan kartu cerdas tersebut.

Perilaku sebuah kartu cerdas umumnya berbeda berdasarkan sistem operasinya. Kartu cerdas dengan sistem operasi A akan memiliki perilaku yang berbeda dari kartu cerdas dengan sistem operasi B. Tetapi hal ini tidak menutup peluang adanya produk-produk kartu cerdas dengan sistem operasi berbeda yang memiliki perilaku selaras. Sebagai contoh adalah KTP Elektronik.

KTP Elektronik saat ini menggunakan dua produk kartu cerdas nirkontak (*contactless smart card*) dengan sistem operasi *native* yang berbeda. Kedua sistem operasi menerapkan standar-standar ISO/IEC 7816-4, ICAO Doc 9303 dan ISO/IEC 9797-1. Sebuah pembaca KTP Elektronik dapat menggunakan prosedur yang sama saat melakukan komunikasi dengan kedua kartu cerdas tersebut karena keduanya memiliki perilaku yang sesuai, sehingga dapat diberi aplikasi KTP Elektronik yang sama.

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Seiring dengan kemajuan pesat di bidang teknologi kartu cerdas, misalnya prosesor yang semakin cepat, jenis memori baru, dan sistem operasi multiaplikasi, membuat teknologi yang ada pada KTP Elektronik pun perlu untuk di-perbarui. Hal lain yang dapat menjadi dasar perlu dilakukannya pembaruan adalah dalam rangka memenuhi kebutuhan di masa depan.

Kompatibilitas adalah kata kunci dalam sebuah pembaruan teknologi. Dalam hal ini, kartu cerdas berteknologi baru yang menjadi kandidat harus dapat digunakan di sistem yang telah ada tanpa syarat. Dengan kata lain, para kandidat tersebut harus memiliki perilaku yang sesuai, agar dapat menjadi tempat bagi aplikasi KTP Elektronik. Karena itu, perlu disiapkan adanya sebuah alat uji yang dapat digunakan untuk memastikan kesesuaian perilaku yang diinginkan.

Tujuan dan Sasaran

Kegiatan ini bertujuan untuk membantu Program KTP Elektronik milik pemerintah dalam memastikan produk-produk kartu cerdas yang sesuai dengan aplikasi KTP Elektronik. Sasaran kegiatan adalah sebuah metode uji untuk mengukur kesesuaian perilaku sebuah kartu cerdas terhadap KTP Elektronik. Metode uji ini memuat skenario-skenario pengujian yang dapat diterapkan pada sebuah alat uji berupa pembaca kartu cerdas dan program aplikasi komputer. Metode uji ini melengkapi metode uji standar ISO/IEC 10373-6 yang telah digunakan untuk mengukur kesesuaian kinerja sebuah kartu cerdas terhadap Peraturan Menteri Dalam Negeri Republik Indonesia tentang KTP Elektronik.

Pendekatan Pemecahan Masalah

Secara garis besar, metode uji yang menjadi sasaran kegiatan dihasilkan melalui langkah-langkah berikut ini:

a. Mempelajari standar-standar dan informasi teknis yang terkait dengan KTP Elektronik.
b. Mengidentifikasi perilaku KTP Elektronik.
c. Merumuskan skenario-skenario pengujian yang akan dituangkan di dalam metode uji.
d. Menerapkan metode uji ke sebuah sistem sederhana.
e. Melakukan uji coba penerapan metode uji.
f. Melakukan analisis hasil uji coba.

METODE

KTP Elektronik mengacu pada standar-standar umum untuk kartu cerdas. Di tahap awal kegiatan, beberapa standar yang harus dipelajari dan relevansinya dengan metode uji yang dikembangkan adalah sebagai berikut:

a. **ISO/IEC 7816-4** menetapkan status siklus hidup, sistem berkas, perintah-perintah dan prosedur keamanan yang dapat diterapkan pada sebuah kartu cerdas. Standar ini men-jadi referensi saat penyusunan skenario-skenario pengujian dan penentuan perintah-perintah yang harus diujikan.
b. **ICAO Doc 9303** menjelaskan tentang Basic Access Control dan Secure Messaging yang disertai dengan contoh-contoh riil. Standar ini menjadi referensi saat mendeskripsikan urutan perintah dalam sebuah komunikasi yang mensyaratkan keamanan. Standar ini juga menjadi referensi untuk istilah-istilah teknis terkait keamanan yang dimuat oleh metode uji.
c. **ISO/IEC 9797-1** menentukan algoritme Message Authentication Code (MAC) yang menggunakan sebuah kunci dan blok sandi berukuran *n*-bit untuk menghitung sebuah MAC berukuran *m*-bit. Standar ini menjadi referensi untuk memahami peranan MAC sebagai sebuah elemen yang hadir dalam komunikasi yang mensyaratkan keamanan.

Berikutnya adalah melakukan identifi-kasi perilaku KTP Elektronik melalui produk kartu cerdas yang saat ini digunakan sebagai blangko KTP Elektronik. Beberapa hal yang dilakukan adalah sebagai berikut:

a. Mempelajari dokumen teknis kartu cerdas tersebut.
b. Mempelajari perilaku kartu cerdas tersebut dengan cara mengirimkan perintah-perintah yang berlaku berdasarkan dokumen teknis, lalu mencermati respons yang diberikan oleh kartu cerdas.

   Perintah-perintah dikirimkan dalam konstruksi Application Protocol Data Unit (APDU) berikut ini:

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

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

Keterangan:
- **CLA** : menyatakan jenis perintah (antarindustri atau *proprietary* atau lainnya).
- **INS** : menyatakan kode perintah dalam heksadesimal, misalnya 'B0' untuk mendapatkan data dari kartu cerdas (READ BINARY).
- **P1-P2** : menyatakan parameter-parameter yang terkait, misalnya *offset* dari sebuah data.
- **Lc** : menyatakan panjang elemen Data.
- **Data** : Data dengan panjang *n* byte.
- **Le** : menyatakan panjang data yang diminta untuk diberikan oleh kartu cerdas.

Sedangkan kartu cerdas merespons dengan konstruksi APDU berikut ini:

	n byte	2 byte
	Data	**Status**
←	Opsional →	← Wajib →

Keterangan:
- **Data** : Data dengan panjang *n* byte.
- **Status** : menyatakan status komunikasi.

APDU perintah dikondisikan untuk memuat dua kategori skenario berikut ini:

- Skenario APDU perintah normal, yang akan direspons oleh kartu cerdas dengan APDU respons berkode status ’9000’.
- Skenario APDU perintah berisikan eror, yang akan direspons oleh kartu cerdas dengan APDU respons berkode status eror, seperti yang disampaikan dalam standar ISO/IEC 7816-4.

Keduanya berlaku di dua siklus hidup kartu cerdas, yaitu di Initialization state dan di

Operational state. Berdasarkan hal tersebut, maka skenario-skenario pengujian dibagi ke dalam dua kelompok besar yang mengacu pada status siklus hidup kartu cerdas.

Secara garis besar, perilaku sebuah KTP Elektronik dapat diteliti berdasarkan elemen-elemen yang turut serta membentuk perilaku tersebut. Dalam proses ekstraksi perilaku KTP Elektronik seperti yang diper-lihatkan pada Gambar 1, peran dari masing-masing elemen dapat diperiksa dengan cara berikut ini:

- Siklus hidup, sistem berkas dan perintah diperiksa berdasarkan pada ketetapan standar ISO/IEC 7816-4.
- Prosedur keamanan diperiksa berdasar-kan pada ketentuan ICAO Doc 9303 dan ketetapan standar ISO/IEC 9797-1.

Tahap selanjutnya adalah merumuskan seluruh skenario pengujian berdasarkan hasil identifikasi perilaku KTP Elektronik. Sebuah skenario pengujian memiliki kerangka seperti yang diperlihatkan di dalam Tabel 1. Kerangka seperti ini mengikuti cara metode uji standar ISO/IEC 10373-6 mendeskripsikan sebuah skenario pengujian parameter digital dari kartu cerdas nirkontak.

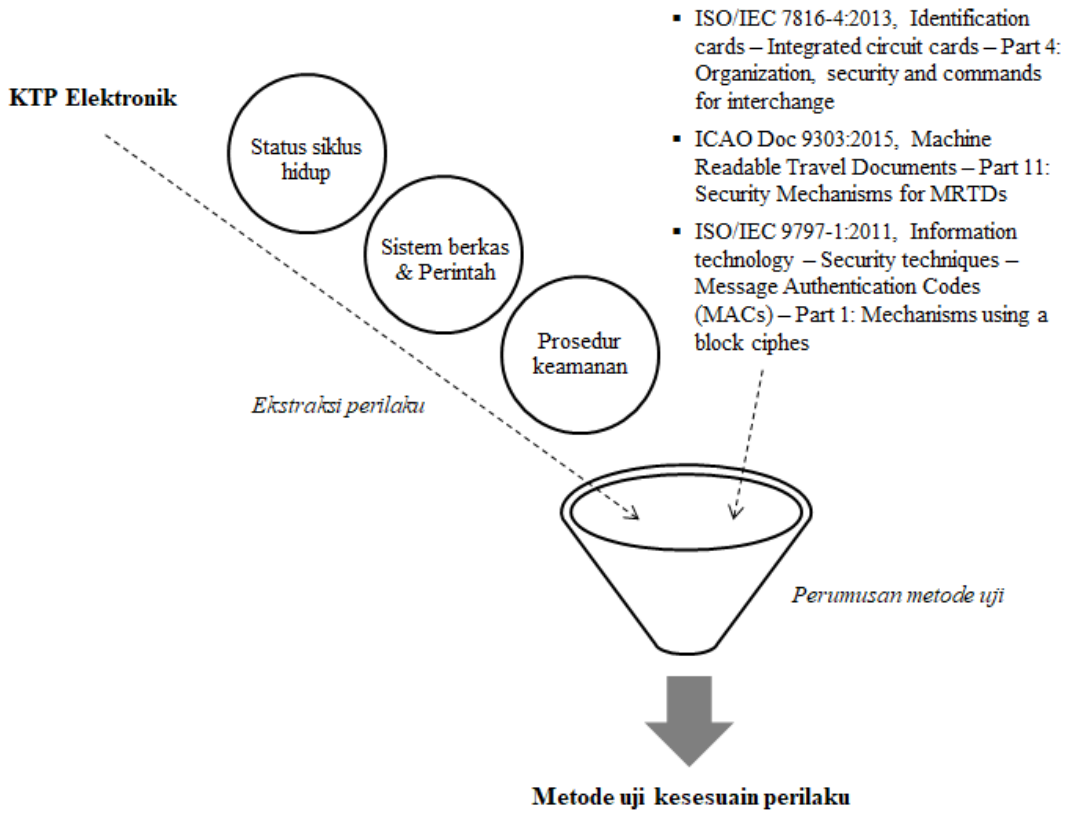
Tabel 1. Kerangka skenario pengujian

Siklus hidup	**Alat uji**		**Kartu cerdas**
Operational state	[PERINTAH]	⟶	
		⟵	[RESPONS]

Keterangan: Bagian dengan [ ] bersifat dinamis.

Kegiatan diakhiri dengan melakukan uji coba penerapan skenario-skenario pengujian pada sebuah sistem sederhana yang terdiri dari pembaca kartu cerdas dan komputer dengan sistem operasi MS Windows yang mendukung pembuatan program aplikasi berbasiskan Java. Sistem ini nantinya dapat dikembangkan lebih lanjut menjadi sebuah alat uji kesesuaian peri-laku kartu cerdas terhadap KTP Elektronik.

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek



Gambar 1. Ilustrasi proses ekstraksi perilaku KTP Elektronik

III. HASIL DAN PEMBAHASAN

Isi dari metode uji kesesuaian perilaku kartu cerdas terhadap KTP Elektronik disusun dalam struktur berikut ini:

- Dibagi ke dalam dua kelompok besar yang mengacu pada status siklus hidup.
- Masing-masing siklus hidup memuat butir-butir pengujian yang menerapkan perintah-perintah standar seperti yang diperlihatkan di dalam Tabel 2.
- Setiap butir pengujian memuat skenario-skenario APDU perintah normal dan APDU perintah berisikan eror.

Ada 56 skenario pengujian yang telah didefinisikan. Tetapi dalam makalah ini hanya dibahas 2 skenario pengujian saja.

Pertama adalah External Authenticate di Initialization state seperti yang diperlihatkan di dalam Tabel 3. Tujuan dari skenario pengujian ini adalah dalam rangka memastikan perilaku kartu cerdas terhadap perintah tersebut. Di sini dirancang terjadinya komunikasi antara alat uji dan kartu cerdas melalui pertukaran kode-kode dalam heksadesimal. Uraiannya adalah sebagai berikut:

[1] Alat uji memberi perintah GET CHALLENGE berdasarkan ketetapan standar ISO/IEC 7816-4 (INS=’84’) dan meminta respons dengan panjang 8 byte. APDU perintah yang disampaikan adalah ’00-84-00-00-08’.
[2] Kartu cerdas memberi respons RND.ICC berupa sebuah bilangan acak 8 byte.
[3] Alat uji memberi perintah EXTERNAL AUTHENTICATE (INS=’82’) dan meminta respons status perintah tersebut. APDU perintah yang disampaikan adalah ’00-82-00-00-Lc-Data. Dalam hal ini, isi dari elemen Data adalah data autentikasi yang diperoleh dengan cara mengenkripsi RND.ICC.
[4] Kartu cerdas akan memberi respons SW1-SW2 dengan kode status ’9000’, apabila berlangsung sesuai dengan ketentuan.

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Tabel 2. Rangkuman butir-butir pengujian

Siklus hidup	Butir pengujian
Initialization state	GET CHALLENGE
	EXTERNAL AUTHENTICATE
	CREATE FILE
	SELECT FILE
	UPDATE BINARY
	READ BINARY
	ACTIVATE FILE
	CHANGE REFERENCE DATA
Operational state	GET CHALLENGE
	MUTUAL AUTHENTICATE
	SELECT FILE
	UPDATE BINARY
	READ BINARY

Tabel 3. External Authenticate di Initialization state (normal)

Siklus hidup	Alat uji		Kartu cerdas
Initialization state	GET CHALLENGE	⟶	
		⟵	RND.ICC || SW1-SW2: ’9000’
	EXTERNAL AUTHENTICATE	⟶	
		⟵	SW1-SW2: ’9000’

Kedua adalah Mutual Authenticate di Operational state seperti yang diperlihatkan di dalam Tabel 4, dengan uraian sebagai berikut:

[1] Alat uji memberi perintah GET CHALLENGE berdasarkan ketetapan standar ISO/IEC 7816-4 (INS=’84’) dan meminta respons dengan panjang 8 byte. APDU perintah yang disampaikan adalah ’00-84-00-00-08’.

[2] Kartu cerdas memberi respons RND.ICC berupa sebuah bilangan acak 8 byte.

[3] Alat uji memberi perintah MUTUAL AUTHENTICATE (INS=’82’) dan menunggu respons berisi data sebesar 40 byte. APDU perintah yang disampaikan adalah ’00-82-00-00-28-Data-28. Dalam hal ini, isi dari elemen Data (sebesar 40 byte) diperoleh berdasarkan ketentuan ICAO Doc 9303 berikut ini:

$$S = RND.IFD \,||\, RND.ICC \,||\, K.IFD$$
$$Data = enc(S) \,||\, MAC$$

RND.IFD adalah sebuah bilangan acak 8 byte dan K.IFD adalah sebuah kunci acak 16 byte yang dibangkitkan oleh alat uji. Sedangkan MAC adalah nilai MAC dari enc(S) yang dihitung berdasarkan standar ISO/IEC 9797-1.

[4] Kartu cerdas akan memberi respons data sebesar 40 byte dan SW1-SW2 dengan kode status ’9000’, apabila berlangsung sesuai dengan ketentuan.

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Tabel 4. Mutual Authenticate di Operational state (normal)

Siklus hidup	Alat uji		Kartu cerdas
Operational state	GET CHALLENGE	⟶	
		⟵	RND.ICC || SW1-SW2: '9000'
	MUTUAL AUTHENTICATE	⟶	
		⟵	enc(RND.ICC || RND.IFD || K.ICC) || MAC || SW1-SW2: '9000'

Pengujian untuk mengukur keakuratan dan keandalan dari metode uji dilakukan dalam bentuk penerapan metode uji ke sebuah sistem sederhana. Sistem tersebut terdiri dari pembaca kartu cerdas dan program aplikasi khusus yang melaksanakan seluruh skenario pengujian yang disampaikan oleh metode uji. Sistem tersebut diperlihatkan pada Gambar 2.

Program aplikasi yang disebutkan di atas dibuat berbasiskan bahasa pemrograman Java pada NetBeans IDE 8.2 dengan JDK 1.8.0_45. Program aplikasi ini akan memberikan informasi bahwa:

- hasil eksekusi sebuah skenario pengujian berakhir dengan **tanda sukses**, yang berarti memiliki perilaku yang **sesuai** dengan KTP Elektronik pada bagian yang sedang diukur, dan
- hasil eksekusi sebuah skenario pengujian berakhir dengan **tanda gagal**, yang berarti memiliki perilaku yang **tidak sesuai** dengan KTP Elektronik pada bagian yang sedang diukur.

Program aplikasi ini akan dikembangkan lebih lanjut dalam rangka menghasilkan sebuah alat uji sesungguhnya.

Sistem tersebut di atas telah dicobakan ke blangko KTP Elektronik dan ke produk-produk kartu cerdas lainnya. Tujuan dari uji coba adalah sebagai berikut:

- Untuk memperbaiki kesalahan-kesalahan rancangan sebuah skenario pengujian.

  Sebuah contoh kasus diberikan pada Gambar 3. Dapat dilihat bahwa skenario pengujian yang telah disampaikan di dalam Tabel 4 harus mengalami perubahan saat diterapkan. Sebuah perintah SELECT FILE harus diberikan mendahului perintah GET CHALLENGE. Hal ini membuat isi dari metode uji harus direvisi. Kejadian seperti ini hanya dapat diketahui dari mencobakan metode uji ke kartu cerdas sesungguhnya.

- Untuk membuktikan bahwa metode uji ini akurat dan andal.

  Informasi pada Gambar 3 merupakan hasil dari mencobakan skenario pengujian Mutual Authenticate di Operational state ke blangko KTP Elektronik. Hasil percobaan berakhir dengan tanda sukses, seperti yang seharusnya.

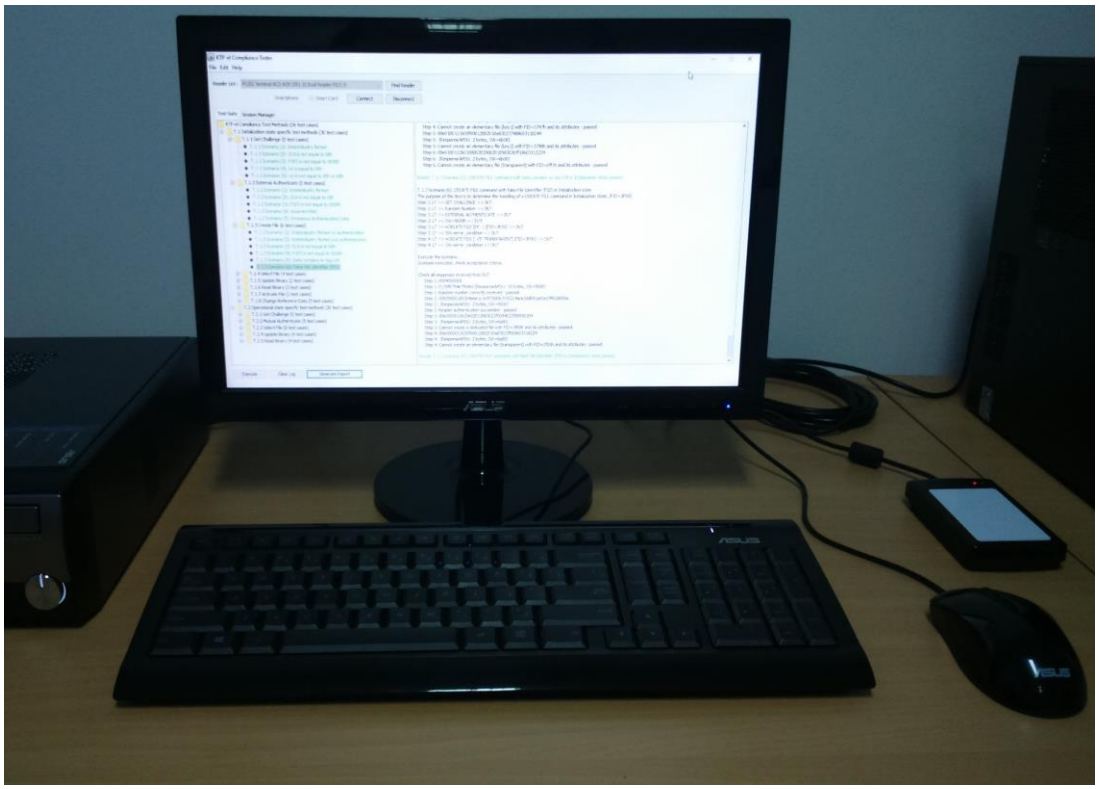
  Hasil yang sama juga diperoleh saat mencobakan skenario pengujian di atas ke kartu cerdas lain yang diketahui memiliki perilaku yang sesuai. Kedua hasil tersebut akan menjadi salah satu bukti pendukung untuk menarik kesimpulan bahwa metode uji yang dihasilkan akurat dan andal.

  Sebuah bukti lain diperlihatkan pada Gambar 4. Dalam kasus ini, skenario pengujian Mutual Authenticate di Operational state dicobakan ke kartu cerdas yang telah diketahui memiliki perilaku yang berbeda dari KTP Elektronik. Hasil percobaan ini adalah seperti yang sudah diprediksi, harus berakhir dengan tanda kegagalan.

- Untuk memenuhi ketentuan bahwa sebuah metode uji harus divalidasi terlebih dahulu sebelum dapat dijadikan sebagai referensi sebuah lingkup pengujian yang diakreditasi oleh Komite Akreditasi Nasional (KAN).

Sebagai penutup, metode uji terkait telah ditulis ke dalam sebuah Dokumen Teknis di Pusat Teknologi Elektronika, BPPT.

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

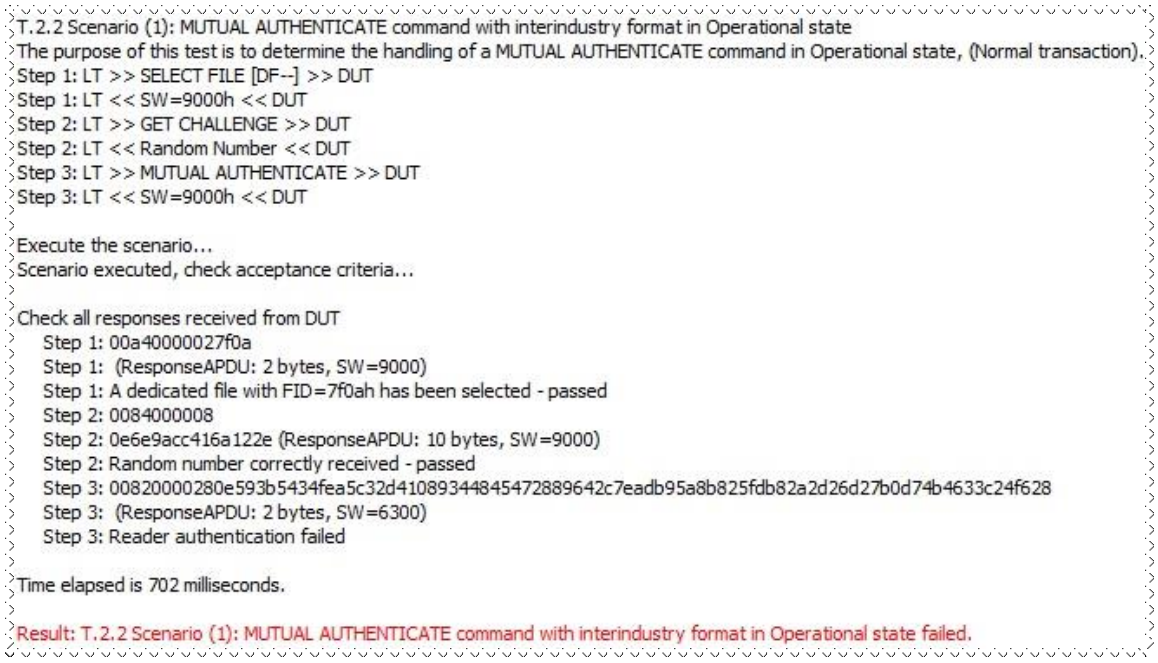


Gambar 2. Sistem yang menerapkan metode uji

```
T.2.2 Scenario (1): MUTUAL AUTHENTICATE command with interindustry format in Operational state
The purpose of this test is to determine the handling of a MUTUAL AUTHENTICATE command in Operational state, (Normal transaction).
Step 1: LT >> SELECT FILE [DF--] >> DUT
Step 1: LT << SW=9000h << DUT
Step 2: LT >> GET CHALLENGE >> DUT
Step 2: LT << Random Number << DUT
Step 3: LT >> MUTUAL AUTHENTICATE >> DUT
Step 3: LT << SW=9000h << DUT

Execute the scenario...
Scenario executed, check acceptance criteria...

Check all responses received from DUT
    Step 1: 00a40000027f0a
    Step 1:  (ResponseAPDU: 2 bytes, SW=9000)
    Step 1: A dedicated file with FID=7f0ah has been selected - passed
    Step 2: 0084000008
    Step 2: 715de7e05cdd6d33 (ResponseAPDU: 10 bytes, SW=9000)
    Step 2: Random number correctly received - passed
    Step 3: 0082000028f70ab444f4fa1711528e350e9e979fe568769ef130eb85cb2a9755e115b05ef3193609420e8e2f2628
    Step 3: d7fff70a6a83b72a1c6b78dc836c085cb9c5f83206a2cd5aecd3dc68d7c69e11650901ed14d056d9 (ResponseAPDU: 42 bytes, SW=9000)
    Step 3: Reader authentication succeeded - passed

Time elapsed is 6648 milliseconds.

Result: T.2.2 Scenario (1): MUTUAL AUTHENTICATE command with interindustry format in Operational state passed.
```

Gambar 3. Hasil penerapan Mutual Authenticate di Operational state (normal)

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek



Gambar 4. Hasil uji coba metode uji ke kartu cerdas yang tidak sesuai

IV. SIMPULAN DAN SARAN

Kegiatan ini telah menghasilkan sebuah metode uji yang ditujukan untuk mengukur kesesuaian perilaku kartu cerdas terhadap KTP Elektronik. Metode uji tersebut dikembangkan dalam rangka memastikan kesesuaian sebuah kartu cerdas sebagai tempat bagi aplikasi KTP Elektronik. Hal ini sangat dibutuhkan oleh para produsen kartu cerdas yang ingin berkontribusi dalam program nasional KTP Elektronik.

Metode uji yang telah dihasilkan dapat diimplementasikan ke dalam sebuah program aplikasi komputer yang akan menjadi bagian dari sebuah alat uji. Sebuah kartu cerdas yang mampu melewati seluruh skenario pengujian yang ada di dalam metode uji secara berurutan dan lengkap dapat dianggap mampu menjadi tempat bagi aplikasi KTP Elektronik.

Metode uji yang telah dihasilkan harus terus-menerus divalidasi dan disempurnakan keakuratannya. Berbagai produk kartu cerdas yang diprediksi akan mampu menjadi tempat bagi aplikasi KTP Elektronik harus dicobakan ke alat uji yang menerapkan metode uji ter-sebut. Selanjutnya produk-produk kartu cerdas yang telah lulus uji harus dicobakan di sistem sesungguhnya yang dikelola oleh Kementerian Dalam Negeri Republik Indonesia.

DAFTAR PUSTAKA

Kementerian Dalam Negeri Republik Indonesia. 2011. *Peraturan Menteri Dalam Negeri Republika Indonesia Nomor 6 Tahun 2011 Tentang Standar dan Spesifikasi Perangkat Keras, Perangkat Lunak dan Blangko KTP Berbasis NIK Secara Nasional*

International Organization for Standardization (ISO), International Electrotechnical Commission (IEC). 2013. *ISO/IEC 7816-4:2013 Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*

International Civil Aviation Organization (ICAO). 2015. *ICAO Doc 9303 Machine Readable Travel Documents – Part 11: Security Mechanisms for MRTDs*

International Organization for Standardization (ISO), International Electrotechnical Commission (IEC). 2011. *ISO/IEC 9797-1:2011 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*