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

PENGEMBANGAN ALAT UJI KESESUAIAN PERILAKU KARTU CERDAS TERHADAP KTP ELEKTRONIK

Dwidharma Priyasta[1], Wahyu Cesar[2]
[1]Pusat Teknologi Elektronika (PTE), BPPT
[2]Pusat Teknologi Industri Pertahanan dan Keamanan (PTIPK), BPPT
Gedung Teknologi 3 Kawasan Puspiptek, Jl. Raya Puspiptek, Tangerang Selatan, Banten 15314
dwidharma.priyasta@bppt.go.id

Abstrak

Saat ini alat uji yang digunakan untuk mengukur kesesuaian kinerja sebuah kartu cerdas (*smart card*) terhadap Peraturan Menteri Dalam Negeri Republik Indonesia tentang KTP Elektronik mengacu pada standar ISO/IEC 10373-6. Akan tetapi alat uji ini tidak dapat digunakan untuk memastikan bahwa sebuah kartu cerdas mampu menjadi tempat bagi aplikasi KTP Elektronik. Kepastian ini sangat dibutuhkan oleh para produsen kartu cerdas yang ingin berkontribusi dalam program nasional KTP Elektronik. Makalah ini melaporkan hasil pengembangan sebuah alat uji yang dapat digunakan untuk memeriksa kesesuaian perilaku sebuah kartu cerdas sebagai tempat bagi aplikasi KTP Elektronik. Alat uji ini berupa sebuah pembaca kartu cerdas (*smart card reader*) dan sebuah program aplikasi komputer. Alat uji ini menerapkan skenario-skenario pengujian dari sebuah metode uji tentang KTP Elektronik yang telah dikembangkan di Pusat Teknologi Elektronika – Badan Pengkajian dan Penerapan Teknologi (BPPT). Sebuah kartu cerdas yang dapat melewati seluruh butir pengujian yang ada pada alat uji secara berurutan dan lengkap dapat dianggap mampu menjadi tempat bagi aplikasi KTP Elektronik.

Kata Kunci: alat uji, KTP Elektronik

Abstract

Currently the test tool used for measuring the performance of a smart card against the Regulation of the Minister of Home Affairs of the Republic of Indonesia on national electronic identity card is based on the ISO/IEC 10373-6 standard. However, the test tool cannot be used to assure whether a smart card can be a place for the national electronic identity card application. This assurance is needed by the smart card ven-dors who want to contribute in the national electronic identity program. This paper reports on the development of a test tool that can be used to check the conformity of the behaviour of a smart card as a place for the national electronic identity card application. This test tool consist of a smart card reader and a computer application program. This test tool implements test scenarios from a test method for the national identity cards which has been developed in Pusat Teknologi Elektronika – Badan Pengkajian dan Penerapan Teknologi (BPPT). A smart card that could pass through all the test items on the test tool in sequence and complete can be considered capable of becoming a place for the national electronic identity card application.

Keywords: test tool, the national electronic identity cards

PENDAHULUAN

KTP Elektronik yang ada saat ini menggunakan kartu cerdas jenis nirkontak untuk menyimpan biodata, tanda tangan, pas foto dan *minutiae* sidik jari dari seluruh penduduk wajib KTP. Spesifikasi teknis dari kartu cerdas KTP Elektronik ditetapkan dalam Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 6 Tahun 2011. Sampai saat tulisan ini dibuat, belum ada perubahan terhadap peraturan menteri tersebut.

Pengujian untuk mengukur kesesuaian kinerja sebuah kartu cerdas terhadap peraturan

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

menteri yang tersebut di atas dapat dilakukan dengan menggunakan alat uji yang menerapkan standar ISO/IEC 10373-6. Alat uji tersebut terdiri dari beberapa perangkat keras seperti yang diperlihatkan pada Gambar 1. Sedangkan standar ISO/IEC 10373-6 memuat prosedur pengujian untuk kartu cerdas jenis nirkontak yang memiliki jangkauan komunikasi paling jauh 10 cm terhadap perangkat pembacanya.

Seluruh parameter pengujian yang digunakan dalam standar ISO/IEC 10373-6 berasal dari sebuah seri standar tentang kartu cerdas jenis nirkontak berikut ini:

1. ISO/IEC 14443-1:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics
2. ISO/IEC 14443-2:2010 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface
3. ISO/IEC 14443-3:2011 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision
4. ISO/IEC 14443-4:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol

Keempat bagian dari seri standar ISO/IEC 14443 yang tersebut di atas tidak membahas tentang ketentuan perilaku dari sebuah kartu cerdas agar dapat menjadi tempat bagi aplikasi kartu cerdas lainnya. Sudah tentu hal ini adalah sangat logis, karena segala sesuatu yang terkait dengan sebuah aplikasi akan menjadi bersifat spesifik dan tidak dapat dijadikan sebagai standar yang berlaku umum. Karena itu, dalam rangka memastikan apakah sebuah kartu cerdas dapat sesuai sebagai tempat bagi aplikasi KTP Elektronik, perlu dikembangkan sebuah alat uji yang menerapkan sebuah metode uji baru.

Tujuan dan Sasaran

Tujuan dari kegiatan yang disampaikan adalah untuk menghasilkan sebuah perangkat yang dapat digunakan untuk memastikan kesesuaian sebuah kartu cerdas sebagai tempat bagi aplikasi Elektronik. Sedangkan sasaran kegiatan adalah dihasilkannya sebuah alat uji yang dapat digunakan untuk memeriksa perilaku sebuah kartu cerdas, dalam rangka memastikan kesesuaian dari kartu cerdas tersebut sebagai tempat bagi aplikasi KTP Elektronik.

Alat uji yang menjadi sasaran kegiatan akan menerapkan sebuah metode uji yang telah dikembangkan di Pusat Teknologi Elektronika – Badan Pengkajian dan Penerapan Teknologi (BPPT) tentang kesesuaian perilaku sebuah kartu cerdas terhadap KTP Elektronik. Alat uji ini akan digunakan untuk melayani seluruh industri kartu cerdas yang ingin berkontribusi dalam program nasional KTP Elektronik.

Pendekatan Pemecahan Masalah

Secara garis besar, sasaran kegiatan akan dihasilkan melalui langkah-langkah berikut ini:

1. Mengkaji ulang metode uji kesesuaian perilaku kartu cerdas terhadap KTP Elektronik.
2. Melakukan pengembangan alat uji dengan mengikuti ketentuan sebuah proses siklus hidup perekayasaan perangkat lunak yang baik (SDLC), yang meliputi aktivitas:
   a. pendefinisian kebutuhan (*requirements definition*),
   b. penetapan spesifikasi kebutuhan (*requirements specification*),
   c. analisis dan perancangan (*analysis and design*),
   d. penerapan (*implementation*), dan
   e. pengujian hasil (*testings*).

METODE

Pertama adalah melakukan kaji ulang metode uji kesesuaian perilaku terhadap KTP Elektronik di bagian-bagian penting yang terkait dengan penerapannya. Topik utama adalah tentang skenario pengujian dan standar-standar yang harus dijadikan sebagai referensi.

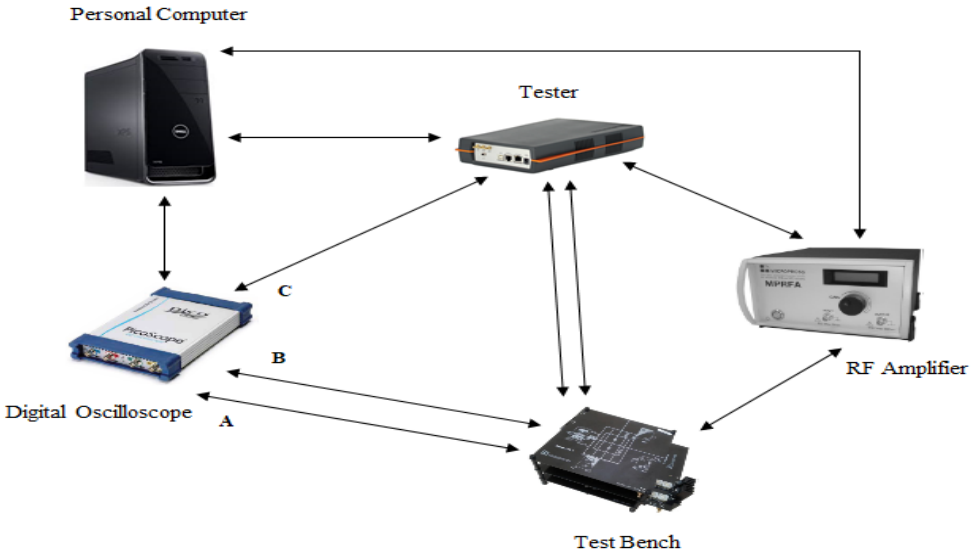
Penerapan dari sebuah skenario pengujian harus mengikuti sebuah kerangka seperti yang diperlihatkan di dalam Tabel 1.

Tabel 1. Kerangka skenario pengujian

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

Keterangan: Bagian dengan [ ] bersifat dinamis.

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



Gambar 1. Alat uji kartu cerdas jenis nirkontak berdasarkan standar ISO/IEC 10373-6 (Sumber : *Microprоss SAS)*

Sedangkan beberapa standar yang harus dijadikan se-bagai referensi dalam penerapan metode uji kesesuaian perilaku terhadap KTP Elektronik ke sebuah alat uji 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 menjadi referensi saat menerapkan seluruh perintah yang harus dilaksanakan di dalam sebuah skenario pengujian.

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

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 →

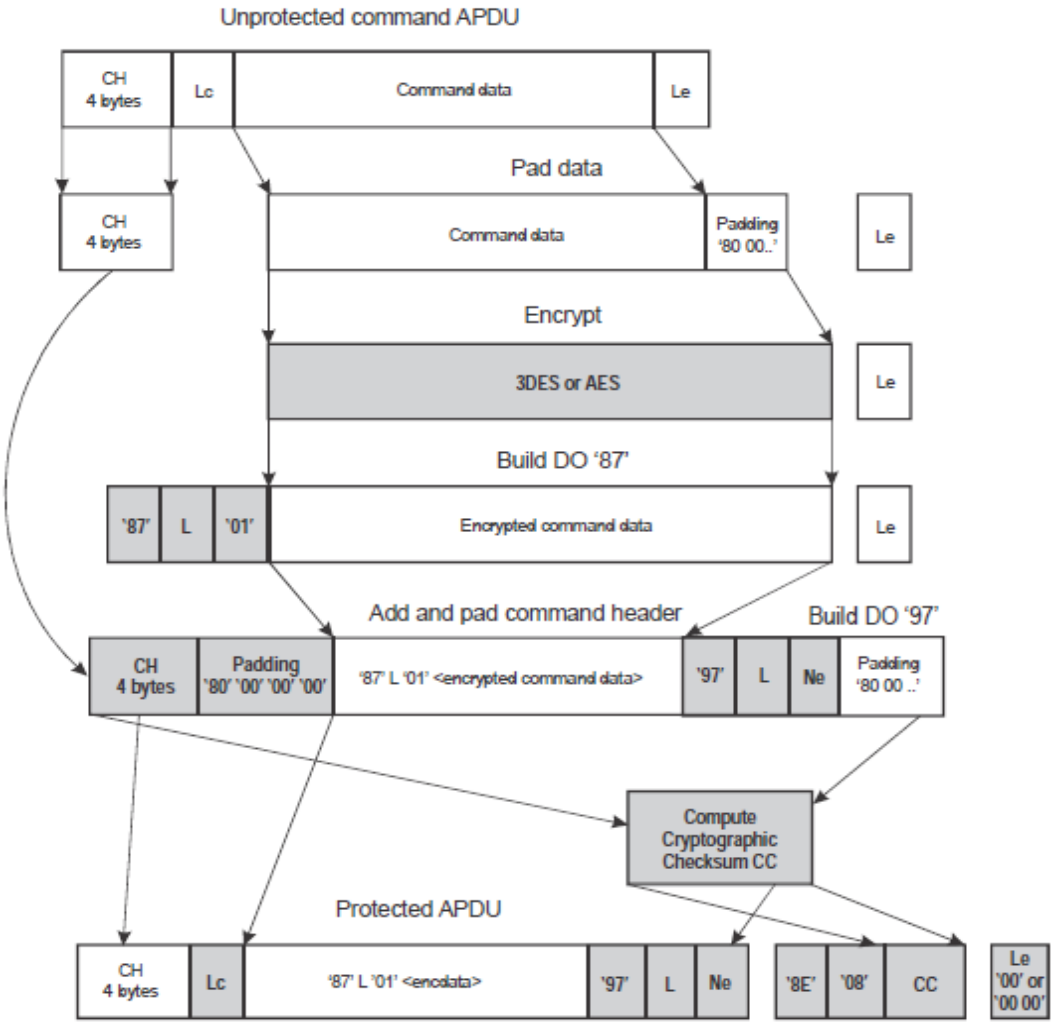
Keterangan:
Data : Data dengan panjang *n* byte.
Status : menyatakan status komunikasi.

b. **ICAO Doc 9303** menjelaskan tentang Basic Access Control dan Secure Messaging yang disertai dengan contoh-contoh riil. Standar ini menjadi referensi saat menerapkan perintah-perintah dalam sebuah komunikasi yang mensyaratkan keamanan. Misalnya pada saat harus menerapkan sebuah APDU perintah dalam format Secure Messaging, seperti yang diperlihatkan pada Gambar 2.

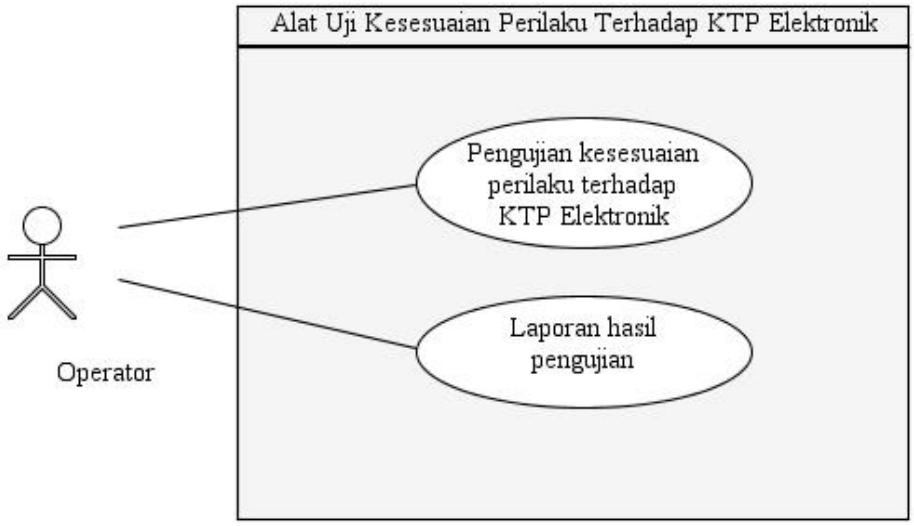
c. **ISO/IEC 9797-1** menentukan algoritme Message Authentication Code (MAC) yang menggunakan sebuah kunci dan blok sandi berukuran *n*-bit untuk menghitung sebuah MAC berukuran *m*-bit. Standar ini menjadi referensi saat menerapkan penghitungan MAC sebagai *cryptographic checksum*.

Berikutnya adalah mendefinisikan kebutuhan akan alat uji kesesuaian perilaku terhadap KTP Elektronik, dan menetapkan spesifikasi kebutuhan yang meliputi persyaratan fungsional dan persyaratan arsitektur dari perangkat keras dan perangkat lunak. Dalam makalah ini, persyaratan fungsional disampaikan dalam bentuk diagram Use Case, seperti yang diperlihatkan pada Gambar 3. Sedangkan arsitektur dari perangkat keras dan perangkat lunak diperlihatkan pada Gambar 4.

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

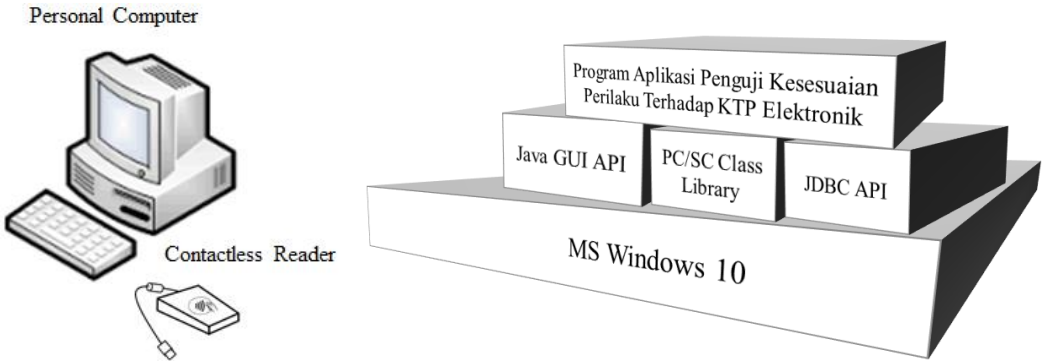


Gambar 2. Pembentukan sebuah APDU dalam format Secure Messaging (*Sumber: ICAO Doc 9303*)



Gambar 3. Diagram Use Case dari persyaratan fungsional

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



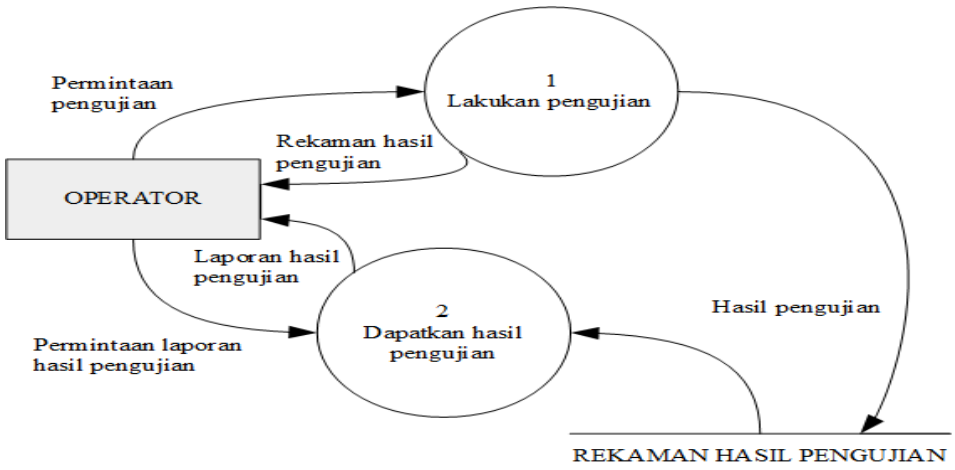
Gambar 4. Arsitektur dari perangkat keras dan perangkat lunak

Tahap selanjutnya adalah menguraikan secara teknis servis yang diberikan oleh alat uji dan merancang antarmuka dari program aplikasi yang digunakan oleh pengguna. Uraian teknis dari servis yang diberikan oleh alat uji disampaikan dalam bentuk diagram aliran data (DFD) level 0 seperti yang diperlihatkan pada Gambar 5. Sedangkan perancangan antarmuka pengguna dilakukan seperti yang diperlihatkan pada Gambar 6.

Terkait dengan dilaksanakannya sebuah skenario pengujian, terdapat dua kategori hasil pengujian, yaitu **Passed** dan **Failed**. Rekaman hasil pengujian disampaikan kepada pengguna dalam bentuk seperti berikut ini:

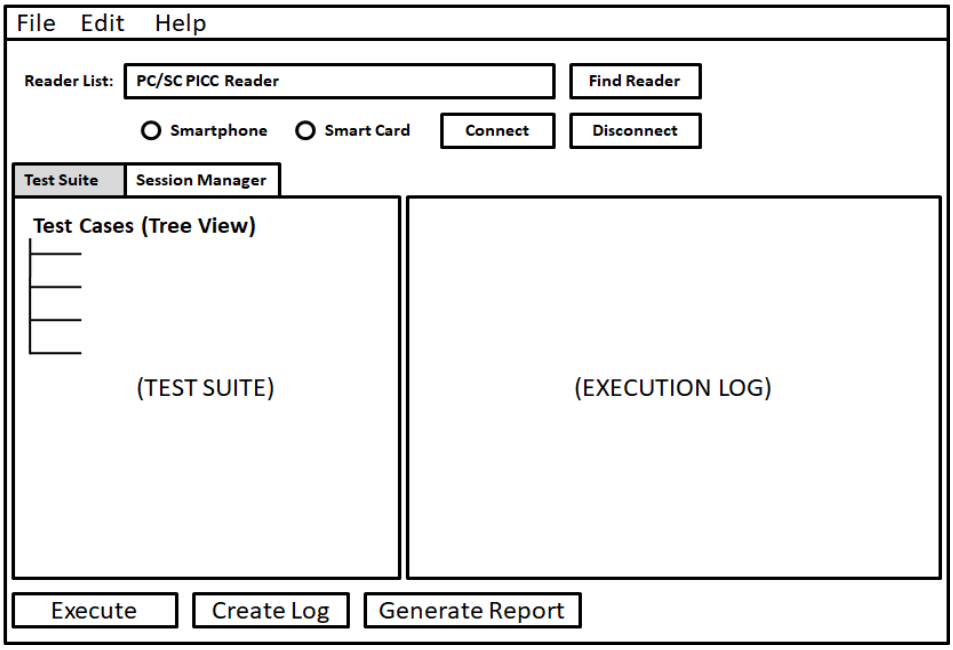
```
T.2.1 Scenario (1): GET CHALLENGE
command with interindustry format in
Operational state
Step 1: LT >> SELECT FILE [DF-] >> DUT
Step 1: LT << SW=9000h << DUT
Step 2: LT >> GET CHALLENGE >> DUT
Step 2: LT << Random Number << DUT
Execute the scenario...
Scenario executed, check acceptance
criteria...

Check all responses received from DUT:
   Step 1: 00a40000027bfe00
   Step 1: (Response APDU: 2 bytes,
SW=9000)
   Step 1: A dedicated file with
FID=7bfe has been selected - passed
   Step 2: 0084000008
   Step 2: 8fbb735d49c12260 (Response
APDU: 10 bytes, SW=9000)
   Step 2: Random number correctly
received - passed

Time elapsed is 2219 milliseconds.

Result: T.2.1 Scenario (1): GET
CHALLENGE command with interindustry
format in Operational state passed.
```

Kegiatan diakhiri dengan melakukan uji coba penerapan alat uji ke beberapa produk kartu cerdas jenis nirkontak.



Gambar 5. DFD level 0 dari uraian teknis servis yang diberikan oleh alat uji

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

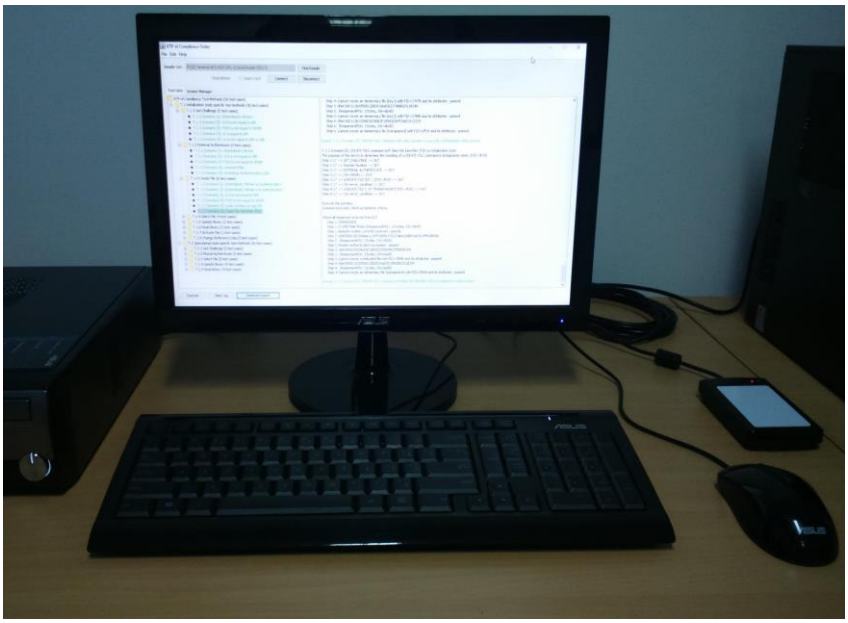


Gambar 6. Sebuah rancangan antarmuka pengguna alat uji

HASIL DAN PEMBAHASAN

Realisasi dari alat uji kesesuaian perilaku terhadap KTP Elektronik adalah seperti yang diperlihatkan pada Gambar 7. Alat uji ini memuat 56 skenario pengujian yang dikelompokkan ke dalam 13 butir pengujian. Alat uji ini telah dicobakan ke 4 produk kartu cerdas yang dipilih, yaitu:

- satu produk kartu cerdas yang saat ini digunakan sebagai blangko KTP Elektronik (disebut dengan produk **A**),
- satu produk kartu cerdas yang dapat melakukan emulasi KTP Elektronik (disebut dengan produk **B**), dan
- dua produk kartu cerdas dengan perilaku yang berbeda dari KTP Elektronik (disebut dengan produk **C** dan **D**).



Gambar 7. Alat uji kesesuaian perilaku terhadap KTP Elektronik

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

Rangkuman hasil pengujian dari produk A adalah seperti yang diperlihatkan di dalam Tabel 2. Persentase keberhasilan adalah 100%. Hasil ini sudah semestinya terjadi, karena alat uji yang digunakan memang ditujukan untuk menguji kesesuaian terhadap produk tersebut.

Tabel 2. Hasil pengujian produk A

Hasil	Jumlah skenario	Persentase
Passed	56	100%
Failed	0	0%
TOTAL	56	100%

Rangkuman hasil pengujian dari produk B adalah seperti yang diperlihatkan di dalam Tabel 3. Hasil ini sudah dapat diprediksi dari awal, karena produk B memiliki perilaku yang sesuai dengan KTP Elektronik.

Tabel 3. Hasil pengujian produk B

Hasil	Jumlah skenario	Persentase
Passed	56	100%
Failed	0	0%
TOTAL	56	100%

Sementara itu, rangkuman hasil pengujian dari produk C adalah seperti yang diperlihatkan di dalam Tabel 4. Persentase keberhasilan hanya 17,86%. Hasil ini sudah semestinya terjadi, karena produk C tidak memiliki perilaku yang sesuai dengan KTP Elektronik.

Tabel 4. Hasil pengujian produk C

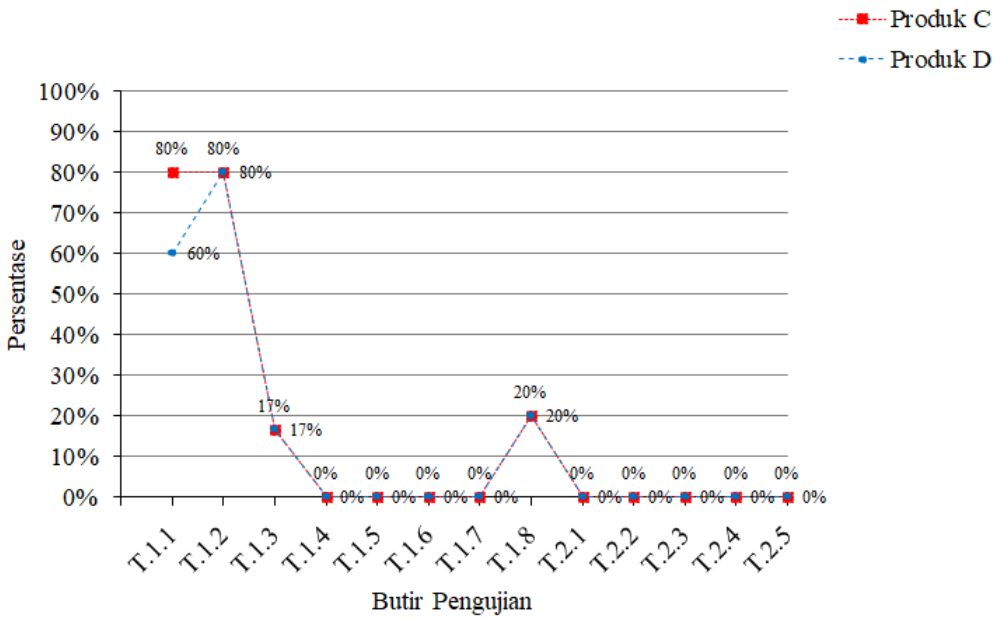
Hasil	Jumlah skenario	Persentase
Passed	10	17,86%
Failed	46	82,14%
TOTAL	56	100%

Sedangkan rangkuman hasil pengujian dari produk D adalah seperti yang diperlihatkan di dalam Tabel 5. Persentase keberhasilan hanya 16,07%. Hasil ini pun sudah semestinya terjadi, karena produk D tidak memiliki perilaku yang sesuai dengan KTP Elektronik.

Tabel 5. Hasil pengujian produk D

Hasil	Jumlah skenario	Persentase
Passed	9	16,07%
Failed	47	83,93%
TOTAL	56	100%

Untuk mendapatkan informasi terperinci mengenai butir pengujian yang dapat dipenuhi maupun yang tidak dapat dipenuhi oleh produk C dan D, dengan kata lain informasi mengenai persentase kesesuaian kedua produk tersebut terhadap KTP Elektronik, data pada Gambar 7 dapat digunakan sebagai referensi.



Gambar 7. Persentase keberhasilan produk C dan D per butir pengujian

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

Berdasarkan data pada Gambar 7, terlihat bahwa produk C maupun D berpeluang untuk memenuhi butir pengujian T.1.1 dan T.1.2. Hal seperti ini dapat saja terjadi, meskipun secara umum kedua produk tersebut memiliki perilaku yang berbeda dari KTP Elektronik. Peluang untuk menghasilkan beberapa perilaku yang sama dimungkinkan dengan keberadaan standar yang dapat dijadikan sebagai referensi bersama oleh para produsen cip maupun pengembang sistem operasi kartu cerdas. Standar tersebut adalah ISO/IEC 7816-4. Oleh karena itu, dapat dinyatakan di sini bahwa hal tersebut tidak terkait sama sekali dengan keandalan dari alat uji yang telah dihasilkan.

SIMPULAN DAN SARAN

Kegiatan ini telah menghasilkan sebuah alat uji untuk memeriksa kesesuaian perilaku sebuah kartu cerdas terhadap KTP Elektronik. Hal ini perlu dilakukan dalam rangka memastikan kemampuan dari kartu cerdas tersebut sebagai tempat bagi aplikasi KTP Elektronik. Cara ini sangat dibutuhkan oleh para produsen kartu cerdas yang ingin berkontribusi dalam program nasional KTP Elektronik.

Sebuah kartu cerdas yang mampu melewati seluruh butir pengujian yang ada pada alat uji secara berurutan dan lengkap dapat dianggap mampu menjadi tempat bagi aplikasi KTP Elektronik. Hal ini telah dibuktikan melalui beberapa kali uji coba yang telah dilakukan.

Alat uji ini harus terus ditingkatkan keandalannya. Salah satu caranya adalah melalui kegiatan layanan pengujian kepada para mitra yang kartu cerdasnya diprediksi mampu menjadi tempat bagi aplikasi KTP Elektronik. Semakin banyak produk kartu cerdas yang diuji, semakin bertambah pula keandalan dari alat uji yang telah dihasilkan.

DAFTAR PUSTAKA

Pusat Teknologi Elektronika - BPPT. 2018. *Dokumen Teknis: Kartu cerdas KTP Elektronik – Metode uji – Bagian 1: Karakteristik perilaku*

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*