LAMPIRAN
PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA
NOMOR 2 TAHUN 2014
TENTANG
PERSYARATAN TEKNIS KARTU CERDAS KONTAK (*CONTACT SMART CARD*)

PERSYARATAN TEKNIS KARTU CERDAS KONTAK (*CONTACT SMART CARD*)

Ruang lingkup persyaratan teknis kartu cerdas meliputi:

BAB I : Ketentuan Umum
1. definisi;
2. konfigurasi;
3. singkatan; dan
4. istilah.

BAB II : Persyaratan Teknis Kartu Cerdas Kontak (*Contact Smart Card*).

BAB III : Kelengkapan Pengujian Kartu Cerdas Kontak.

BAB IV : Pelaksanaan Pengujian.

BAB I
KETENTUAN UMUM

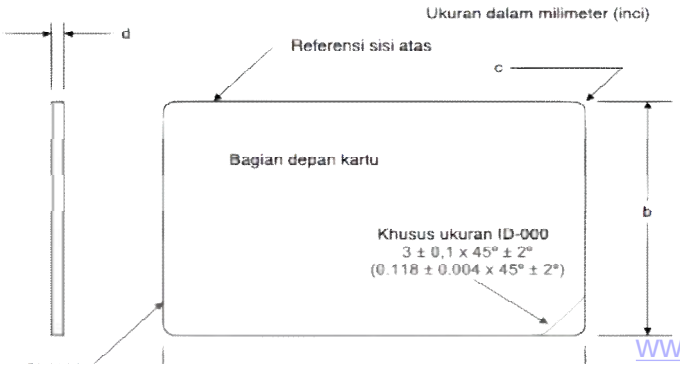
1. Definisi

Kartu cerdas kontak (*contact smart card*) adalah sebuah perangkat yang memiliki satu atau lebih cip rangkaian terintegrasi (*integrated circuit chip*/IC *chip*) yang terbentuk dari komponen prosesor, memori, dan antarmuka komunikasi dan bersifat konduktif.

2. Konfigurasi

2.1. Ukuran Kartu

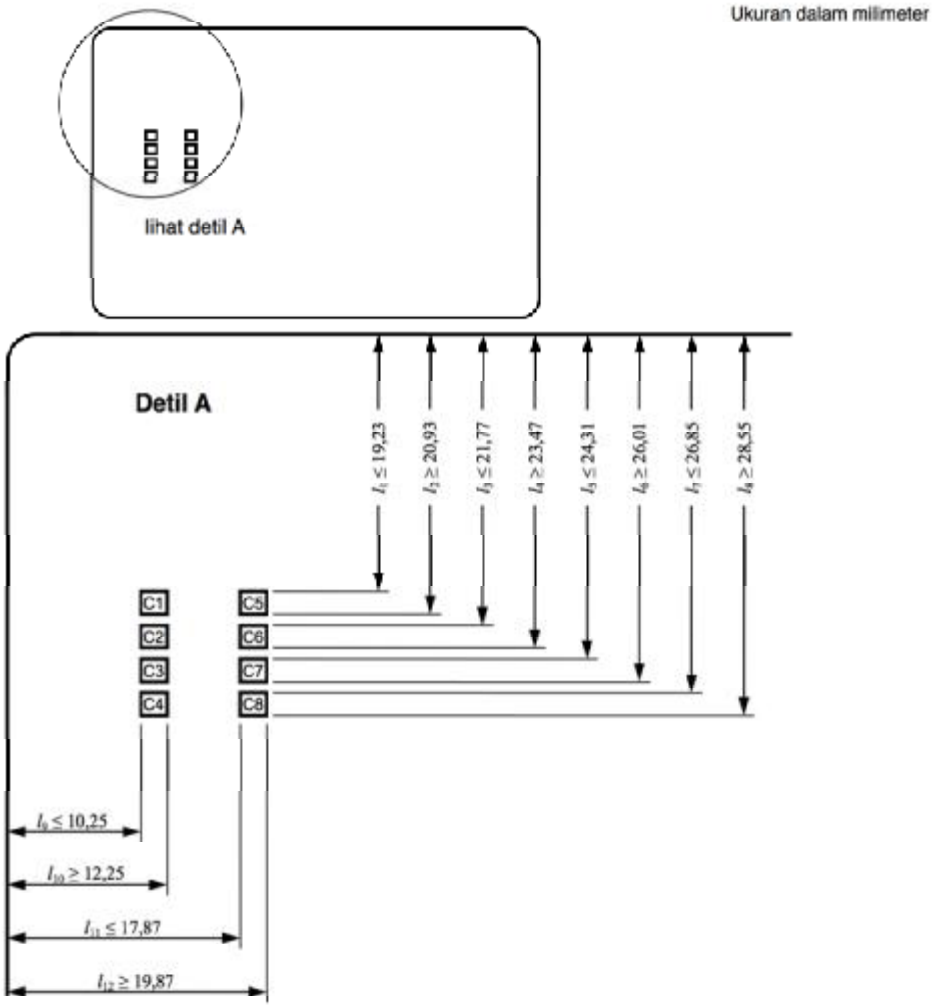
Gambar 1. Ukuran kartu (ISO/IEC 7810:2003)



	a		b		c		d	
	maks	min	maks	min	maks	min	maks	min
ID-1 Unused card	85,72 (3,375)	85,47 (3,365)	54,03 (2,127)	53,92 (2,123)	3,48 (0,137)	2,88 (0,133)	0,84 (0,033)	0,68 (0,027)
ID-1 Returned card	85,90 (3,382)	85,47 (3,365)	54,18 (2,133)	53,92 (2,123)	3,48 (0,137)	2,88 (0,133)	0,84 (0,033)	0,68 (0,027)

Tabel 1. Ukuran kartu (ISO/IEC 7810:2003)

2.2. Posisi Elemen Kontak



Gambar 2. Posisi kontak dalam kartu cerdas kontak (*contact smart card*) (ISO/IEC 7816-2:2007)

Keterangan gambar:

C1

*Input*catu daya.

C2

Reset sinyal *input*.

C3

Input sinyal *clock*.

C5

Ground (tegangan referensi).

C6

Pemrograman tegangan input .

C7

Input dan *output*data serial (half-duplex).

C4, C8

Dua kontak sisanya AUX1 dan AUX2 masing, dan digunakan untuk antarmuka dan penggunaan lainnya.

3. Singkatan

3-DES	:	*Triple DES*
A	:	*Ampere*
AES	:	*Advanced Encryption Standard*
CPU	:	*Central Processing Unit*
DES	:	*Data Encryption Standard*
ECDSA	:	*Elliptic Curve Digital Signature Algorithm*
EEPROM	:	*Electrically Eraseable Programmable Read-Only Memory*
eV	:	*electro Volt*
F	:	*Farad*
Gy	:	*Gray*
IDEA	:	*International Data Encryption Algorithm*
IEC	:	*International Electrotechnical Commission*

ISO	:	*International Organization for Standardization*
k	:	*kilo*
m	:	*mili*
p	:	*pico*
PC	:	*Polycarbonate*
PET	:	*Polyethylene Terephthalate*
PVC	:	*Polyvinyl Chloride*
RAM	:	*Random-Access Memory*
ROM	:	*Read-Only Memory*
RSA	:	*Ron Rivest, Adi Shamir and Leonard Adleman*
SHA-1	:	*Secure Hash Algorithm version* 1
SHA-256	:	*Secure Hash Algorithm 256 bits*
V	:	*Volt*
µ	:	*micro*

4. Istilah

Anti-tearing	:	fitur untuk melindungi konten dari memori jika kartu keluar dari area transaksi sebelum transaksi selesai
Barcode	:	grafik berbentuk batang yang digunakan untuk mewakili sistem kode nomor pengidentifikasian
Crypto co-processor	:	sebuah modul perangkat keras yang terdiri dari sebuah prosesor untuk keperluan proses enkripsi dan proses terkait lainnya
Digital signature	:	skema matematika untuk memastikan keaslian dari sebuah pesan atau dokumen digital
Electromagnetic compatibility	:	kemampuan perangkat atau sistem elektronik untuk beroperasi dekat dengan perangkat elektronik lainnya tanpa mengalami penurunan performa

Embossing	:	desain yang dicap ke dalam substrat untuk menghasilkan dekoratif mengangkat atau indentasi permukaan masing-masing
Guilloche	:	dekorasi pola dengan garis-garis terjalin, biasanya berbentuk melingkar atau oval yang biasa dibuat dengan mengunakan teknik percetakan berkualitas tinggi
Hash	:	sebuah algoritma yang merubah sekumpulan karakter ke dalam sebuah nilai yang merepresentasikan kumpulan karakter tersebut namun dalam karakter yang jumlahnya tetap dan lebih sedikit dari jumlah karakter asli
Kinegram	:	suatu bentuk gambar bergerak yang dibuat dengan menggeser pola bergaris
Laser engraving	:	penerapan teknologi laser untuk membuang sebagian dari permukaan bahan untuk mengukir atau menandai objek
Logging	:	proses pencatatan rentetan peristiwa dan atau data yang terjadi dalam sebuah sistem atau perangkat
Moduliertes merkmal	:	fitur *machine-readable modulated* yang ditambahkan ke kartu pada tahap manufaktur untuk mencegah pemalsuan
Signature panel	:	tempat pembubuhan tanda tangan pemilik kartu
Thermochrome display	:	sebuah panel atau area yang berubah warna berdasarkan temperatur

BAB II

PERSYARATAN TEKNIS KARTU CERDAS KONTAK

(*CONTACT SMART CARD)*

1. Persyaratan Fisik

   Persyaratan fisikkartu cerdas kontak (*contact smart card*) wajib memenuhi ketentuan sebagai berikut:

   a. Material kartu cerdas kontak (*contact smart card*) dapat terbuat dari

bahan PVC atau PET atau PC;
b. Dimensi kartu cerdas kontak (*contact smart card*) sesuai dengan gambar 1 dan tabel 1.

2. Persyaratan Pelabelan

Persyaratan pelabelan kartu cerdas kontak (*contact smart card*) wajib menyertakan satu atau lebih dari teknologi pelabelan diantaranya sebagai berikut :

a. Identitas kartu;
b. *Signature panel*;
c. *Embossing*; dan/atau
d. *Laser engraving*.

3. Persyaratan Keamanan Fisik

Persyaratan keamanan fisik kartu cerdas kontak (*contact smart card*) dapat menyertakan satu atau lebih dari teknologi keamanan fisik diantaranya sebagai berikut :

a. *Guilloche*;
b. Hologram;
c. *Kinegram*;
d. Penanda ultraviolet;
e. *Moduliertes Merkmal*;
f. *Barcode*; dan / atau
g. *Thermochrome Display*.

4. Persyaratan KetahananKartu Cerdas Kontak (*Contact Smart Card*)

Persyaratan ketahanan kartu cerdas kontak (contact smart card)wajib memenuhi ketentuan sebagai berikut:

a. Daya tahan fisik kartu terhadap pengelupasan lapisan tertentu pada kartu sesuai dengan ketentuan IS0/IEC 10373-1;
b. Daya tahan fisik kartu terhadap pelintiran pada kartu sesuai dengan ketentuan IS0/IEC 10373-1;
c. Daya tahan fisik kartu terhadap tekukan sesuai dengan ISO/IEC 10373-1.

5. Persyaratan Ketahanan Cip

Persyaratan ketahanan cip kartu cerdas kontak (*contact smart card*)wajib memenuhi ketentuan sebagai berikut:

a. Cip kartu cerdas kontak (*contact smart card*) tidak boleh rusak oleh tegangan listrikstatissebesar2000 V yang berasal dari kapasitor 100 pF dengan resistansi 1500 Ohm;

b. Resistensi cipyang diukur di antara dua titik dari pin tidak boleh lebih dari (maksimum) 0,5 Ohm, dengan nilai dari 50 µA sampai dengan 300 mA;
c. Kartu wajib dapat terus berfungsi setelah menerima radiasi sinar-X sebesar 70 keV sampai dengan 140 keV di setiap permukaan manapun, dengan dosis kumulatif 0,1 Gy per tahun;
d. Persyaratan *electromagnetic compatibility* sesuai SNI CISPR 22:2012 dan/atau standar EMC internasional yang setara;
e. Kartu cerdas kontak (*contact smart card*)wajib dapat bekerja dengan baik pada kisaran suhu antara -25°C sampai dengan 70°C;
f. Ruang penyimpanan data dengan durabilitas baca/tulis paling rendah 100.000 kali.

6. Persyaratan Komponen Cip Kartu Cerdas Kontak (*Contact Smart Card*)

Persyaratan komponen cipkartu cerdas kontak (*contact smart card*)wajib memenuhi ketentuan paling sedikit sebagai berikut:

a. CPU: Arsitektur 8 bit;
b. RAM:256 *Bytes*;
c. EEPROM:1 Kilo *Bytes*;
d. ROM:1 Kilo *Bytes*.

7. Persyaratan Keamanan Data

Kartu cerdas kontak (*contact smart card*)wajib memenuhi persyaratan keamanan data yang memiliki :

a. *Cryptoco-processor*yang mendukung teknologi kriptografi, antara lain:
   1) Algoritma simetrik (contoh: DES, 3-DES, IDEA, dan AES);
   2) Algoritma asimetrik (contoh: RSA);
   3) Fungsi *hash* (contoh: SHA–1 dan SHA–256);
   4) *Digital signature*(contoh: ECDSA, RSA-2000);
   5) Pembangkit bilangan acak (*random number generator*);
   6) Proses otentikasi dua arah dengan menggunakan mekanisme umpan balik (*mutual authentication*).
b. Fitur yang dapat menjaga keamanan transaksi dan akses data;
c. Mekanisme untuk mengamankan transaksi dan akses data;
d. Fituruntuk menyimpan informasi tentang seluruh perubahan yang dilakukan oleh suatu transaksi;
e. Fituruntuk mempersingkat waktu *logging* dan pemulihan;
f. Fitur *anti-tearing*.

8. Persyaratan Struktur Data

Struktur data pada kartu cerdas kontak (*contact smart card*) wajib mendukung pembentukan *Master File* (MF), *Dedicated File* (DF), dan *Elementary File* (EF) seperti yang didefinisikan dalam dokumen ISO/IEC 7816-4.

9. Persyaratan *Command Set*

   Command set padakartu cerdas kontak (*contact smart card*)wajib sesuai dengan ISO/IEC 7816-4 klausul 5.1.2.

BAB III
KELENGKAPAN PENGUJIAN KARTU CERDAS KONTAK
(*CONTACT SMART CARD*)

Kartu cerdas kontak (*contact smart card*) yang akan diuji wajib dilengkapi dengan:

1. Identitas kartu cerdas kontak (*contact smart card*)

   Identitas penerbit dan nomor seri cip.

2. Dokumen manual aplikasikartu cerdas kontak (*contact smart card*)

   Dokumen dalam bahasa Indonesia dan/atau bahasa Inggris.

BAB IV
PELAKSANAAN PENGUJIAN

Pengujian kartu cerdas kontak (*contact smart card*) dilaksanakan sesuai ketentuan peraturan perundang-undangan.

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA

TIFATUL SEMBIRING