LAMPIRAN : PERATURAN MENTERI DALAM NEGERI
NOMOR : 6 Tahun 2011
TANGGAL : 21 Januari 2011

SPESIFIKASI PERANGKAT KERAS, PERANGKAT LUNAK DAN
BLANGKO KTP BERBASIS NIK SECARA NASIONAL

A. SPESIFIKASI PERANGKAT KERAS DAN PERANGKAT LUNAK

1. *Chip*
   a. Struktur Data dalam *Chip* meliputi:
      1) Biodata penduduk wajib KTP dengan ukuran rekaman paling rendah 0,5 *Kilo Bytes*;
      2) Tanda tangan penduduk wajib KTP dengan format digital yang dikompresi dengan ukuran rekaman paling rendah 0,5 *Kilo Bytes*;
      3) Pas photo dengan format digital yang dikompresi dengan ukuran rekaman paling rendah 3 *Kilo Bytes*;
      4) Kode keamanan dengan rincian:
         a) *Minutiae* per sidik jari dengan ukuran paling rendah 0,4 *Kilo Bytes* dan dapat diverifikasi 1:1 dengan referensi format INCITS 378 MIN:A;
         b) Format *minutiae* sidik jari berdasarkan standar ANSI, INCITS atau *Proprietary* yang sudah diuji dalam hal *interoperabilitas* oleh NIST;
         c) Tanda tangan elektronik *(Digital Signature)* berdasarkan standar *Elliptic Curve Digital Signature Algorithm* paling rendah 256 *bit* atau RSA 2048 *bit* dan *Hash Algorithm* SHA-256.

   b. Memori *(Memory)* terdiri dari beberapa hal sebagai berikut:
      1) Ukuran EEPROM paling rendah 8 *Kilo Bytes* untuk menyimpan biodata, tanda tangan, pas photo dan *minutiae* sidik jari telunjuk tangan kanan dan sidik jari telunjuk tangan kiri penduduk yang bersangkutan;
      2) Daya tahan penulisan memori *(Write Endurance)* paling rendah 100.000 kali;
      3) Daya tahan penyimpanan data (Data *Retention*) paling singkat 10 tahun;
      4) Pengaturan penyimpanan data *(Data Organization)* menggunakan *Flexible File System*.

   c. Frekuensi Radio *(Radio Frequency)* terdiri dari beberapa hal sebagai berikut:
      1) Berdasarkan standar ISO 14443 A/B;
      2) Frekuensi dengan kisaran 13,56 MHz ± 7 KHz;
      3) Kecepatan transfer data *(Baudrate)* paling rendah 100 *Kilo Bit*/detik;
      4) Memiliki sifat frekuensi tidak bertabrakan *(anti collision)*;
      5) Jarak pengoperasian pembacaan dan penulisan *(Operating Distance)* paling jauh 100 mm;
      6) Kekuatan medan pengoperasian *(Operating Field Strength)* dari 1,5 A/M sampai dengan 7,5 A/M.

   d. Keamanan *(Security)* terdiri dari beberapa hal sebagai berikut:
      1) Pembangkit Bilangan Acak *(Random Number Generator)* berdasarkan standar AIS-31 (P2)/FIPS 140-2;
      2) Mendukung autentikasi dua arah antara *smart card reader/writer* dan *chip*;
      3) *Access Conditions* diterapkan per file;
      4) Algoritma Keamanan *(Security Algorithm)* bersifat simetris *(symmetric)* berdasarkan algoritma: 3DES dengan panjang kunci 168 *bit*, AES 128 *bit*, atau setara;

5) Memenuhi syarat ketunggalan transaksi *(anti tear), supported by chip*;
6) Memiliki perangkat keras *crypto co-processor*;
7) e-KTP didukung dengan pengamanan melalui Sistem Manajemen Kunci *(Key Management System).*

e. Lain-lain meliputi hal sebagai berikut:
1) *Chip* adalah *smart card nirsentuh* yang berbasis CPU *(microcontroller chip)* dan menggunakan Sistem Operasi *(Operating System)* terbuka;
2) *Electro Static Discharge* paling rendah ESD 2 kV;
3) Bekerja dengan baik pada suhu *(Temperature)* dari - 25ºC sampai dengan 70ºC;
4) Memerlukan pasokan daya *(Voltage)* dari 2,7 Volt sampai dengan 3,6 Volt.

2. *Reader/Writer Chip* pada Blangko Kartu terdiri dari beberapa hal sebagai berikut:
a. Berdasarkan standar ISO 14443 A dan B;
b. Frekuensi dengan kisaran 13,56 MHz ± 7 KHz;
c. Kecepatan transfer data *(Baudrate)* paling rendah 100 *Kilo Bit*/detik;
d. Memiliki *Secure Access Module* (SAM) yang dilengkapi dengan *crypto processor* yang sesuai dengan kebutuhan *chip*;
e. Mendukung autentikasi dua arah antara *smart card reader/writer* dan *chip*.

3. *Automated Fingerprint Identification System* (AFIS), terdiri dari:
a. Perangkat server, terdiri dari beberapa hal sebagai berikut:
1) *Platform* perangkat server berbentuk *rack mounted* atau *blade*;
2) Kinerja *(Performance)* perangkat server bersifat *upgradeable* dan *scalable*;
3) Sistem operasi *(Operating System)* berbasis *Linux/Unix/Windows* atau yang setara;
4) Pangkalan Data *(Database)* berbasis standard RDBMS *(Relational Database Management System)*, seperti *MySQL, Oracle, MS SQL Server* atau setara;
5) Perangkat lunak *(Software)* tersedia bagi AFIS Server dan AFIS *Workstation*;
6) Kinerja perangkat lunak *(Software)* server dapat mendukung gugusan *(cluster)* dan dapat berskala sesuai dengan jumlah prosesor *(scalable to number of processors)*.

b. Klien, terdiri dari beberapa hal sebagai berikut :
1) *Platform* perangkat keras berbasis PC;
2) Sistem operasi *(Operating System)* berbasis *Linux/Unix/Windows* atau yang setara;
3) Pangkalan Data *(Database)* berbasis standard RDBMS, seperti *MySQL, Oracle, MS SQL Server* atau setara;
4) Perangkat lunak *(software)* tersedia bagi AFIS PC;
5) Perangkat lunak *(software)* klien dapat mendukung verifikasi secara *realtime*.

c. Sistem AFIS terintegrasi dengan biodata, tanda tangan, pas photo dan *minutiae* sidik jari telunjuk tangan kanan dan sidik jari telunjuk tangan kiri pada *chip* dan SIAK serta terkonsolidasi dengan pusat data kependudukan.

d. Pemindai Sidik Jari *(Fingerprint Scanner)* :
1) Pemindai hidup *(Live scanner)* berbasis optik, pemindai satu jari *(one finger scanner)*;
2) Pemindai dengan kemampuan resolusi *(scanner resolution)* paling rendah 356 x 292 *pixels* 500 dpi;
3) *Driver* berbasis *Linux/Windows* atau yang setara.