SALINAN

MENTERI DALAM NEGERI
REPUBLIK INDONESIA

PERATURAN MENTERI DALAM NEGERI REPUBLIK INDONESIA
NOMOR 76 TAHUN 2020
TENTANG
PERANGKAT PEMBACA DAN PENULIS SERTA PERANGKAT PEMBACA
KARTU TANDA PENDUDUK ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI DALAM NEGERI REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk mendukung dan menyelenggarakan administrasi kependudukan terhadap pemanfaatan data dan dokumen kependudukan, perlu didukung dengan perangkat pembaca dan penulis kartu tanda penduduk elektronik dan/atau perangkat pembaca kartu tanda penduduk elektronik;

b. bahwa Peraturan Menteri Dalam Negeri Nomor 34 Tahun 2014 tentang Spesifikasi Perangkat Pembaca Kartu Tanda Penduduk Elektronik sudah tidak sesuai lagi dengan kebutuhan administrasi kependudukan sehingga perlu diganti;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, serta untuk melaksanakan ketentuan Pasal 5 huruf j Peraturan Pemerintah Nomor 40 Tahun 2019 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, perlu menetapkan Peraturan

Menteri Dalam Negeri tentang Perangkat Pembaca dan Penulis serta Perangkat Pembaca Kartu Tanda Penduduk Elektronik;

Mengingat : 1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 124, Tambahan Lembaran Negara Republik Indonesia Nomor 4674), sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 262, Tambahan Lembaran Negara Republik Indonesia Nomor 5475);
3. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);
4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
5. Peraturan Pemerintah Nomor 40 Tahun 2019 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 102,

Tambahan Lembaran Negara Republik Indonesia Nomor 6354);

6. Peraturan Presiden Nomor 11 Tahun 2015 tentang Kementerian Dalam Negeri (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 12);
7. Peraturan Menteri Dalam Negeri Nomor 102 Tahun 2019 tentang Pemberian Hak Akses dan Pemanfaatan Data Kependudukan (Berita Negara Republik Indonesia Tahun 2019 Nomor 1611);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI DALAM NEGERI TENTANG PERANGKAT PEMBACA DAN PENULIS SERTA PERANGKAT PEMBACA KARTU TANDA PENDUDUK ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Administrasi Kependudukan adalah rangkaian kegiatan penataan dan penertiban dalam penerbitan dokumen dan data kependudukan melalui pendaftaran penduduk, pencatatan sipil, pengelolaan informasi administrasi kependudukan serta pendayagunaan hasilnya untuk pelayanan publik dan pembangunan sektor lain.
2. Penduduk adalah warga negara Indonesia dan orang asing yang bertempat tinggal di Indonesia.
3. Kartu Tanda Penduduk Elektronik yang selanjutnya disebut KTP-el adalah kartu tanda Penduduk yang dilengkapi cip yang merupakan identitas resmi Penduduk sebagai bukti diri yang diterbitkan oleh instansi pelaksana.
4. Perangkat Pembaca dan Penulis KTP-el yang selanjutnya disebut *Card Encoder* adalah alat pembaca dan penulis data elektronik dalam bentuk basis data yang tersimpan di dalam pusat data dan/atau pusat data cadangan ke dalam cip KTP-el.

5. Perangkat Pembaca KTP-el yang selanjutnya disebut *Card Reader* adalah alat pembaca data elektronik yang tersimpan di dalam cip KTP-el.
6. Kartu *Secure Access Module* yang selanjutnya disebut Kartu SAM adalah unit perangkat kartu cerdas yang berfungsi membaca dan/atau menulis basis data di dalam cip KTP-el yang diamankan menggunakan mekanisme algoritma kriptografi tertentu.
7. Sidik Jari adalah hasil reproduksi tapak jari tangan Penduduk yang terdiri atas kumpulan alur garis halus dengan pola tertentu yang sengaja diambil melalui proses perekaman Sidik Jari oleh petugas untuk kepentingan kelengkapan data Penduduk dalam basis data kependudukan.
8. Pengguna adalah lembaga negara, kementerian/lembaga pemerintah nonkementerian, dan/atau badan hukum Indonesia yang memerlukan informasi data kependudukan sesuai dengan bidangnya.
9. Data Balikan adalah data yang bersifat unik dari masing-masing lembaga Pengguna yang telah melakukan akses data kependudukan.
10. Produsen *Card Encoder* adalah badan hukum Indonesia yang melakukan kegiatan produksi untuk menghasilkan produk *Card Encoder*.
11. Produsen *Card Reader* adalah badan hukum Indonesia yang melakukan kegiatan produksi untuk menghasilkan produk *Card Reader.*
12. Produsen Blangko KTP-el adalah badan hukum Indonesia yang melakukan kegiatan produksi untuk menghasilkan produk blangko KTP-el.
13. Satuan Kerja Pelaksana adalah perangkat daerah kabupaten/kota, unit pelaksana teknis, desa/kelurahan, dan perwakilan Republik Indonesia di luar negeri yang bertanggung jawab dan berwenang melaksanakan pelayanan dalam urusan Administrasi Kependudukan.
14. Prepersonalisasi adalah proses pembuatan struktur *file* pada cip saat proses pembuatan kartu cerdas.

15. Personalisasi adalah proses memasukkan data *file* ke dalam kartu cerdas yang telah dilakukan Prepersonalisasi.
16. Kementerian adalah kementerian yang menyelenggarakan urusan pemerintahan dalam negeri.
17. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan dalam negeri.
18. Direktorat Jenderal yang selanjutnya disingkat Ditjen adalah Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian.
19. Direktur Jenderal yang selanjutnya disingkat Dirjen adalah Direktur Jenderal Kependudukan dan Pencatatan Sipil Kementerian.

BAB II
KOMPONEN DAN JENIS PERANGKAT

Pasal 2

(1) Komponen *Card Encoder* dan *Card Reader* terdiri atas:
    a. perangkat keras; dan
    b. perangkat lunak.
(2) Spesifikasi komponen *Card Encoder* dan *Card Reader* sebagaimana dimaksud pada ayat (1), tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 3

(1) *Card Encoder* untuk perangkat keras sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf a, terdiri atas:
    a. perangkat komputasi; dan
    b. perangkat pembaca dan penulis kartu cerdas.
(2) Perangkat keras sebagaimana dimaksud pada ayat (1), dapat disertai perangkat verifikasi berupa perangkat pemindai Sidik Jari.
(3) Perangkat pembaca dan penulis kartu cerdas sebagaimana dimaksud pada ayat (1) huruf b menggunakan Kartu SAM dan/atau melalui koneksi kode kunci jaringan tertutup yang disesuaikan.

Pasal 4

(1) C*ard Reader* untuk perangkat keras sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf a, terdiri atas:
   a. perangkat komputasi; dan
   b. perangkat pembaca kartu cerdas.
(2) Perangkat keras sebagaimana dimaksud pada ayat (1) dapat disertai perangkat verifikasi berupa perangkat pemindai Sidik Jari dan/atau perangkat pemindai foto wajah.
(3) Perangkat pembaca kartu cerdas sebagaimana dimaksud pada ayat (1) huruf b menggunakan Kartu SAM atau dapat melalui koneksi kode kunci pada jaringan tertutup dan/atau terbuka yang disesuaikan memenuhi kaidah keamanan teknologi informasi dan komunikasi.

Pasal 5

(1) *Card Encoder* untuk perangkat lunak sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf b berupa aplikasi penulis dan pembaca KTP-el.
(2) *Card Reader* untuk perangkat lunak sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf b berupa aplikasi pembaca KTP-el.

Pasal 6

(1) Jenis *Card Encoder* terdiri atas:
   a. Prepersonalisasi blangko KTP-el;
   b. Personalisasi KTP-el; dan
   c. gabungan Prepersonalisasi dan Personalisasi KTP-el.
(2) *Card Encoder* Prepersonalisasi blangko KTP-el sebagaimana dimaksud pada ayat (1) huruf a merupakan perangkat yang digunakan oleh Produsen Blangko KTP-el sesuai dengan fungsinya.
(3) *Card Encoder* Personalisasi KTP-el sebagaimana dimaksud pada ayat (1) huruf b merupakan perangkat yang digunakan oleh Satuan Kerja Pelaksana sesuai dengan fungsinya.

(4) *Card Encoder* gabungan Prepersonalisasi dan Personalisasi KTP-el sebagaimana dimaksud pada ayat (1) huruf c merupakan perangkat proses penulisan data ke dalam cip KTP-el yang terintegrasi atau terpisah dengan perangkat komputasi utama yang digunakan oleh Satuan Kerja Pelaksana sesuai dengan fungsinya.

(5) Dalam hal terdapat kondisi tertentu gabungan Prepersonalisasi dan Personalisasi KTP-el sebagaimana dimaksud pada ayat (4) digunakan oleh Menteri melalui Dirjen untuk pencetakan masal dan pengujian cip KTP-el.

(6) Kondisi tertentu sebagaimana dimaksud pada ayat (5) dilakukan untuk mendukung percepatan pelayanan Administrasi Kependudukan.

Pasal 7

Card Encoder sebagaimana dimaksud dalam Pasal 6 ayat (2) sampai dengan ayat (4) memiliki fungsi untuk:

a. menuliskan data digital ke dalam cip KTP-el;
b. memastikan KTP-el diterbitkan oleh Satuan Kerja Pelaksana yang berlaku di seluruh wilayah Negara Kesatuan Republik Indonesia;
c. memastikan data Penduduk yang dibaca dari cip KTP-el merupakan data yang benar dan sah;
d. membantu otentikasi visual keabsahan data yang tercetak pada KTP-el;
e. memastikan keabsahan kepemilikan KTP-el dengan memanfaatkan kode keamanan untuk menjamin dokumen kependudukan merupakan milik orang yang bersangkutan dengan metode verifikasi Sidik Jari secara elektronik; dan
f. memastikan data Penduduk dari cip KTP-el dapat diakses dan ditampilkan sesuai sertifikasi keamanan untuk kepentingan pelayanan administrasi pemerintahan dan pelayanan publik.

Pasal 8

(1) Jenis *Card Reader* terdiri atas:
    a. tingkat pertama dengan hanya menggunakan autentikasi cip KTP-el;
    b. tingkat kedua dengan menggunakan autentikasi cip KTP-el dan menerapkan 1 (satu) perangkat verifikasi sebagaimana dimaksud dalam Pasal 4 ayat (2); dan
    c. tingkat ketiga dengan menggunakan autentikasi cip KTP-el dan menerapkan paling sedikit 2 (dua) perangkat verifikasi sebagaimana dimaksud dalam Pasal 4 ayat (2).
(2) Jenis *Card Reader* tingkat pertama sebagaimana dimaksud pada ayat (1) huruf a merupakan perangkat pembaca data digital pada cip KTP-el untuk pembuktian keabsahan elemen data tercetak pada KTP-el.
(3) Jenis *Card Reader* tingkat kedua sebagaimana dimaksud pada ayat (1) huruf b merupakan perangkat pembaca data digital pada cip KTP-el, perangkat pemindai Sidik Jari, dan/atau perangkat pemindai foto wajah untuk pembuktian keabsahan elemen data tercetak pada KTP-el.
(4) Jenis *Card Reader* tingkat ketiga sebagaimana dimaksud pada ayat (1) huruf c merupakan perangkat pembaca data digital pada cip KTP-el, perangkat pemindai Sidik Jari, perangkat pemindai foto wajah, dan/atau perangkat lainnya untuk pembuktian keabsahan elemen data tercetak pada KTP-el dan pembuktian KTP-el.
(5) Jenis *Card Reader* sebagaimana dimaksud pada ayat (2), sampai dengan ayat (4) digunakan oleh Pengguna dan Satuan Kerja Pelaksana sesuai dengan fungsinya.
(6) Jenis *Card Reader* sebagaimana dimaksud pada ayat (1) terdiri atas perangkat:
    a. terintegrasi dengan perangkat komputasi utama; dan
    b. terpisah dengan perangkat komputasi utama.

Pasal 9

Card Reader sebagaimana dimaksud dalam Pasal 8 ayat (2), sampai dengan ayat (4) memiliki fungsi untuk:

a. memastikan KTP-el diterbitkan oleh Satuan Kerja Pelaksana yang berlaku di seluruh wilayah Negara Kesatuan Republik Indonesia;
b. memastikan data Penduduk yang dibaca dari cip KTP-el merupakan data yang benar dan sah;
c. membantu otentikasi visual keabsahan data yang tercetak pada KTP-el;
d. memastikan keabsahan kepemilikan KTP-el dengan memanfaatkan kode keamanan untuk menjamin dokumen kependudukan merupakan milik orang yang bersangkutan dengan metode verifikasi Sidik Jari secara elektronik; dan
e. memastikan data Penduduk dari cip KTP-el dapat diakses dan ditampilkan sesuai sertifikasi keamanan untuk kepentingan pelayanan administrasi pemerintahan dan pelayanan publik.

Pasal 10

(1) Jenis *Card Reader* tingkat pertama, tingkat kedua, dan tingkat ketiga sebagaimana dimaksud dalam Pasal 8 ayat (2) sampai dengan ayat (4), data disimpan setelah diverifikasi dan disetujui Penduduk sebagai pemilik data yang bersangkutan.
(2) Pengguna yang menggunakan *Card Reader* wajib memberikan Data Balikan kepada Ditjen sesuai dengan ketentuan peraturan perundang-undangan.
(3) Data Balikan sebagaimana dimaksud pada ayat (2) berupa *file excel spreadsheet, comma separated values*, dan *dump file* atau bentuk format data lainnya yang diberikan secara langsung, surat elektronik, dan/atau melalui aplikasi paling lama 6 (enam) bulan sekali.

Pasal 11

(1) Pemanfaatan *Card Reader* dan/atau integrasi *Card Reader* pada perangkat pembaca kartu cerdas multi kartu lainnya, melalui:
    a. cip KTP-el difungsikan untuk menyimpan data atau aplikasi selain data KTP-el;

b. pembacaan KTP-el dalam bentuk token keamanan, telepon pintar, atau bentuk teramankan lainnya; dan
c. pemanfaatan lainnya.

(2) Dalam hal pemanfaatan *Card Reader* dan/atau integrasi *Card Reader* pada perangkat pembaca kartu cerdas multi kartu lainnya sebagaimana dimaksud pada ayat (1), selanjutnya dilakukan pengembangan mekanisme dan prosedur pengelolaan kunci keamanan aplikasi dan/atau Kartu SAM dari masing-masing data atau aplikasi di dalam cip KTP-el.

BAB III
PENGUJIAN TEKNIS DAN SERTIFIKASI

Pasal 12

(1) Pengujian teknis dilakukan terhadap perangkat keras dan perangkat lunak sebagaimana dimaksud dalam Pasal 2.
(2) Pengujian teknis perangkat keras dan perangkat lunak sebagaimana dimaksud pada ayat (1) untuk memastikan kesesuaian spesifikasi teknis.
(3) Pengujian teknis perangkat keras dan perangkat lunak sebagaimana dimaksud pada ayat (2) dilakukan oleh lembaga pengujian teknis.
(4) Lembaga pengujian teknis sebagaimana dimaksud pada ayat (3) yaitu:
    a. lembaga pemerintah nonkementerian yang membidangi urusan pemerintahan di bidang pengkajian dan penerapan teknologi sesuai dengan ketentuan peraturan perundang-undangan; dan
    b. lembaga pemerintah nonkementerian yang membidangi urusan pemerintahan di bidang keamanan siber dan sandi negara sesuai dengan ketentuan peraturan perundang-undangan.
(5) Pengujian teknis oleh lembaga sebagaimana dimaksud pada ayat (4) dilakukan berdasarkan perjanjian kerja sama dengan Menteri melalui Dirjen.

Pasal 13

(1) Produsen *Card Encoder* dan/atau Produsen *Card Reader* wajib mengajukan surat permohonan pengujian teknis kepada Dirjen.
(2) Proses pengajuan pengujian teknis sebagaimana dimaksud pada ayat (1) tidak dipungut biaya.
(3) Dirjen menerbitkan surat persetujuan pengujian teknis *Card Encoder* dan/atau *Card Reader*.
(4) Surat persetujuan pengujian teknis *Card Encoder* dan/atau *Card Reader* sebagaimana dimaksud pada ayat (2) sebagai dasar dilakukan pengujian Produsen *Card Encoder* dan/atau Produsen *Card Reader* oleh lembaga pengujian teknis.
(5) Dalam hal *Card Encoder* dan/atau *Card Reader* telah sesuai dengan spesifikasi, lembaga pengujian teknis menerbitkan surat keterangan hasil pengujian.
(6) Surat keterangan hasil pengujian sebagaimana dimaksud pada ayat (5) disampaikan kepada Menteri melalui Dirjen.
(7) Dirjen melaporkan proses dan hasil sebagaimana dimaksud pada ayat (1) sampai dengan ayat (6) kepada Menteri.

Pasal 14

(1) Selain memenuhi persyaratan teknis, *Card Encoder* dan/atau *Card Reader* wajib memenuhi tingkat komponen dalam negeri paling rendah 30% (tiga puluh persen) sesuai dengan ketentuan peraturan perundang-undangan.
(2) Untuk meningkatkan penggunaan produk dalam negeri, terhitung sejak tanggal 1 Januari 2024 tingkat komponen dalam negeri wajib memenuhi sebesar 55% (lima puluh lima persen) sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 15

(1) Produsen *Card Encoder* dan/atau Produsen *Card Reader* yang akan mengajukan sertifikasi perangkat keras wajib menyampaikan surat permohonan pengajuan sertifikasi kepada Dirjen.

(2) Proses pengajuan sertifikasi sebagaimana dimaksud pada ayat (1) tidak dipungut biaya.
(3) Ditjen menerbitkan surat persetujuan pengajuan sertifikasi *Card Encoder* dan/atau *Card Reader*.
(4) Surat persetujuan pengajuan sertifikasi *Card Encoder* dan/atau *Card Reader* sebagaimana dimaksud pada ayat (2) disampaikan kepada kementerian yang menyelenggarakan urusan pemerintahan di bidang perindustrian sebagai dasar dilakukannya sertifikasi *Card Encoder* dan/atau *Card Reader*.
(5) Kementerian yang menyelenggarakan urusan pemerintahan di bidang perindustrian menerbitkan sertifikat tingkat komponen dalam negeri.
(6) Sertifikat sebagaimana dimaksud pada ayat (5) disampaikan kepada Dirjen.
(7) Dirjen melaporkan hasil sertifikasi sebagaimana dimaksud pada ayat (6) kepada Menteri.

Pasal 16

(1) Produsen *Card Encoder* dan/atau Produsen *Card Reader* yang memiliki surat keterangan hasil pengujian dan sertifikat tingkat komponen dalam negeri sebagaimana dimaksud dalam Pasal 13 ayat (5) dan Pasal 15 ayat (5), selanjutnya dilakukan inventarisasi dan ditetapkan oleh Dirjen atas nama Menteri.
(2) Produsen *Card Reader* yang telah ditetapkan sebagaimana dimaksud pada ayat (1) melaporkan setiap penggunaan *Card Reader* kepada Dirjen meliputi:
    a. jumlah *Card Reader* yang telah dilakukan Personalisasi dan aktivasi;
    b. Pengguna dan/atau Satuan Kerja Pelaksana yang menggunakan *Card Reader*;
    c. posisi *Card Reader* semula dan perpindahannya; dan
    d. status aktif atau tidak aktif *Card Reader*.
(3) Dirjen melaporkan penggunaan *Card Reader* sebagaimana dimaksud pada ayat (2) kepada Menteri.

BAB IV

KARTU *SECURE ACCESS MODULE* DAN/ATAU KODE KUNCI

Pasal 17

(1) *Card Encoder* dan/atau *Card Reader* yang telah mendapat surat keterangan hasil pengujian dan/atau sertifikat diberikan Kartu SAM dan/atau koneksi kode kunci kepada Produsen *Card Encoder* dan/atau Produsen *Card Reader* sebagaimana dimaksud dalam Pasal 16 ayat (1) sebagai bentuk pengaman.
(2) Kartu SAM dan/atau koneksi kode kunci sebagaimana dimaksud pada ayat (1) terdapat pada perangkat pembaca dan penulis kartu cerdas dan perangkat pembaca kartu cerdas.

Pasal 18

(1) Kartu SAM sebagaimana dimaksud dalam Pasal 17 ayat (2) dilakukan Prepersonalisasi dan Personalisasi oleh Dirjen.
(2) Kartu SAM sebagaimana dimaksud pada ayat (1) digunakan pada:
    a. perangkat pembaca dan penulis kartu cerdas oleh Produsen *Card Encoder* untuk pengajuan Prepersonalisasi blangko KTP-el;
    b. perangkat pembaca dan penulis kartu cerdas dan/atau perangkat pembaca kartu cerdas oleh Satuan Kerja Pelaksana untuk Personalisasi KTP-el; dan
    c. perangkat pembaca kartu cerdas atas permintaan Pengguna untuk pemanfaatan data kependudukan berupa pembacaan KTP-el.
(3) Kartu SAM sebagaimana dimaksud pada ayat (1) dilakukan pengujian fungsi sesuai dengan standar operasional prosedur Prepersonalisasi dan Personalisasi Kartu SAM dengan pendekatan kendali mutu.
(4) Dirjen melaporkan Prepersonalisasi dan Personalisasi sebagaimana dimaksud pada ayat (1) kepada Menteri.

Pasal 19

(1) Produsen Blangko KTP-el menyampaikan pengajuan Kartu SAM untuk Prepersonalisasi blangko KTP-el sebagaimana dimaksud dalam Pasal 18 ayat (2) huruf a kepada Menteri melalui Dirjen setelah mendapat surat perintah kerja.
(2) Produsen Blangko KTP-el sebagaimana dimaksud pada ayat (1) yang telah selesai melaksanakan perjanjian kerja dengan Dirjen wajib melaporkan serta mengembalikan Kartu SAM kepada Menteri melalui Dirjen.
(3) Dalam hal telah selesainya perjanjian sebagaimana dimaksud pada ayat (2), akses untuk memproduksi blangko KTP-el terputus secara otomatis melalui sistem.

Pasal 20

(1) Satuan Kerja Pelaksana menyampaikan pengajuan Kartu SAM untuk Personalisasi KTP-el sebagaimana dimaksud dalam Pasal 18 ayat (2) huruf (b) kepada Dirjen.
(2) Kartu SAM yang diterima secara baik dan rusak dilaporkan kepada Dirjen.
(3) Kartu SAM untuk perangkat pembaca dan penulis kartu cerdas dan/atau perangkat pembaca kartu cerdas yang rusak dan/atau terkunci oleh sistem, wajib dilakukan pemusnahan.
(4) Pemusnahan sebagaimana dimaksud pada ayat (3) dilakukan dengan cara dibakar, digunting, dan/atau dihancurkan dengan alat penghancur Kartu SAM.
(5) Pemusnahan sebagaimana dimaksud pada ayat (4) merupakan tanggungjawab:
    a. Dirjen;
    b. Kepala Dinas Kependudukan dan Pencatatan Sipil Kabupaten/Kota; dan
    c. pejabat di perwakilan Republik Indonesia di luar negeri yang menangani urusan Administrasi Kependudukan.
(6) Pemusnahan sebagaimana dimaksud pada ayat (5) huruf a dan huruf b disaksikan paling sedikit oleh aparat pengawas internal pemerintah dan aparat penegak hukum.

(7) Pemusnahan sebagaimana dimaksud pada ayat (5) huruf c disaksikan paling sedikit oleh 2 (dua) orang pejabat yang ditunjuk oleh kepala perwakilan.
(8) Pemusnahan sebagaimana dimaksud pada ayat (6) dan ayat (7) dibuatkan berita acara pemusnahan.
(9) Dirjen melaporkan pengajuan Kartu SAM sebagaimana dimaksud pada ayat (1) kepada Menteri.

Pasal 21

Produsen *Card Reader* menyampaikan pengajuan Personalisasi Kartu SAM kepada Menteri melalui Dirjen terhadap perangkat pembaca kartu cerdas atas permintaan Pengguna sebagaimana dimaksud dalam Pasal 18 ayat (2) huruf c.

Pasal 22

(1) Menteri melalui Dirjen menugaskan unit kerja pada Direktorat Fasilitasi Pemanfaatan Data dan Dokumen Kependudukan melakukan Prepersonalisasi dan Personalisasi Kartu SAM sebagaimana dimaksud dalam Pasal 18, Pasal 19, dan Pasal 21 untuk menghasilkan *file* konfigurasi.
(2) Untuk mendapatkan *file* konfigurasi sebagaimana dimaksud pada ayat (1), Produsen Blangko KTP-el, Satuan Kerja Pelaksana, dan/atau Pengguna melakukan permohonan aktivasi atas pengajuan Kartu SAM kepada Dirjen.
(3) Permohonan aktivasi sebagaimana dimaksud pada ayat (2) dengan menyampaikan data meliputi:
    a. tipe komponen perangkat;
    b. jumlah unit;
    c. nomor Kartu SAM dan nomor hasil Personalisasi;
    d. alamat Produsen Blangko KTP-el, Satuan Kerja Pelaksana, dan/atau Pengguna;
    e. koordinat; dan
    f. informasi lain yang dibutuhkan.

(4) Dirjen melaporkan permohonan aktivasi atas pengajuan Kartu SAM sebagaimana dimaksud pada ayat (2) kepada Menteri.

Pasal 23

(1) Dalam hal dilakukan pengujian teknis *Card Reader* dan keperluan sosialisasi, Produsen *Card Reader* menyampaikan permohonan peminjaman Kartu SAM kepada Dirjen.
(2) Menteri melalui Dirjen menerbitkan surat persetujuan peminjaman Kartu SAM *Card Reader* yang disampaikan kepada Produsen *Card Reader*.
(3) Produsen *Card Reader* menyampaikan surat persetujuan peminjaman Kartu SAM sebagaimana dimaksud pada ayat (2) kepada lembaga pengujian teknis.
(4) Kartu SAM *Card Reader* sebagaimana dimaksud pada ayat (2) disimpan oleh lembaga pengujian teknis.
(5) Produsen *Card Reader* yang telah selesai melakukan pengujian teknis wajib mengembalikan Kartu SAM kepada lembaga pengujian teknis dan melaporkan pengembalian Kartu SAM kepada Dirjen.
(6) Dirjen melaporkan permohonan peminjaman Kartu SAM dan pengembalian Kartu SAM sebagaimana dimaksud pada ayat (1) dan ayat (5) kepada Menteri.

Pasal 24

(1) Kode kunci sebagaimana dimaksud dalam Pasal 17 ayat (2) berupa *end to end* algoritma kriptografi untuk *Card Encoder* dan *Card Reader*.
(2) Kode kunci berupa *end to end* algoritma kriptografi untuk *Card Encoder* dan *Card Reader* sebagaimana dimaksud pada ayat (1), digunakan tanpa Kartu SAM atau dapat dalam bentuk teknologi aplikasi multi Kartu SAM terintegrasi dengan menggunakan jaringan tertutup.
(3) Kode kunci berupa *end to end* algoritma kriptografi untuk *Card Reader* sebagaimana dimaksud pada ayat (2) dapat menggunakan jaringan terbuka.

Pasal 25

(1) Kode kunci untuk *Card Encoder* diajukan oleh Satuan Kerja Pelaksana dan/atau Produsen Blangko KTP-el kepada Menteri melalui Dirjen untuk dilakukan aktivasi konfigurasi.
(2) Kode kunci untuk *Card Reader* diajukan oleh Satuan Kerja Pelaksana atau Pengguna kepada Dirjen untuk dilakukan aktivasi konfigurasi.
(3) Menteri melalui Dirjen menugaskan unit kerja pada Direktorat Fasilitasi Pemanfaatan Data dan Dokumen Kependudukan untuk melakukan aktivasi konfigurasi sebagaimana dimaksud pada ayat (1) dan ayat (2).
(4) Aktivasi konfigurasi sebagaimana dimaksud pada ayat (1) dan ayat (2) dilakukan pengujian fungsi sesuai dengan standar operasional prosedur aktivasi konfigurasi yang dilakukan oleh Dirjen atas nama Menteri.
(5) Dirjen melaporkan kode kunci *Card Reader* sebagaimana dimaksud pada ayat (2) kepada Menteri.

Pasal 26

(1) Kode kunci sebagaimana dimaksud dalam Pasal 25 dapat dikembangkan untuk peningkatan manfaat KTP-el, verifikasi, dan validasi kepemilikan KTP-el kepada Pengguna.
(2) Pemberian kode kunci sebagaimana dimaksud pada ayat (1) dilakukan oleh Dirjen.
(3) Verifikasi dan validasi kepemilikan KTP-el sebagaimana dimaksud pada ayat (1) berupa identifikasi data kependudukan, identitas cip KTP-el, lokasi pembacaan data, dan data lainnya yang dibutuhkan.
(4) Verifikasi dan validasi kepemilikan KTP-el sebagaimana dimaksud pada ayat (3) menggunakan sistem seluler elektronik (*electronic mobile system*).
(5) Dirjen melaporkan pemberian kode kunci *Card Reader* sebagaimana dimaksud pada ayat (2) kepada Menteri.

Pasal 27

Ketentuan sebagaimana dimaksud dalam Pasal 19 ayat (1), Pasal 20 ayat (1), Pasal 21, dan Pasal 25 ayat (1) dilakukan melalui sistem informasi berbasis aplikasi yang disediakan oleh Kementerian.

BAB V

PENGAWASAN

Pasal 28

(1) Pengawasan *Card Encoder* dan/atau *Card Reader* dilakukan terhadap kesesuaian antara standar produk *Card Encoder* dan/atau *Card Reader* dengan kondisi faktual.
(2) Kesesuaian sebagaimana dimaksud pada ayat (1) paling sedikit meliputi:
    a. komponen *Card Encoder* dan/atau *Card Reader* yang dilakukan pengujian teknis dengan kondisi faktual; dan
    b. jumlah *Card Encoder* dan/atau *Card Reader* yang digunakan oleh Pengguna sama dengan jumlah Kartu SAM yang dikeluarkan oleh Dirjen.
(3) Pengawasan sebagaimana dimaksud pada ayat (1) dilakukan sesuai kebutuhan dalam hal adanya:
    a. laporan tertulis dari masyarakat, lembaga, dan/atau pihak lainnya;
    b. temuan dari lembaga pemerintah, lembaga pemerintah nonkementerian, dan/atau pihak lainnya;
    c. dugaan penyalahgunaan produk *Card Encoder* dan/atau *Card Reader*; dan
    d. kebutuhan lainnya.
(4) Dirjen melaporkan jumlah *Card Encoder* dan/atau *Card Reader* dan Kartu SAM sebagaimana dimaksud pada ayat (2) huruf b kepada Menteri.

Pasal 29

(1) Pengawasan sebagaimana dimaksud dalam Pasal 28 ayat (1) dilakukan oleh Menteri melalui Dirjen.

(2) Menteri melalui Dirjen dalam melakukan pengawasan sebagaimana dimaksud pada ayat (1) melibatkan pihak:
   a. lembaga pemerintah nonkementerian yang membidangi urusan pemerintahan di bidang pengkajian dan penerapan teknologi;
   b. lembaga pemerintah nonkementerian yang membidangi urusan pemerintahan di bidang keamanan siber dan sandi negara; dan/atau
   c. tenaga ahli perseorangan yang memiliki keahlian bidang auditor teknologi.

(3) Pelibatan dilakukan dengan mengajukan surat permohonan dari Dirjen atas nama Menteri kepada pihak sebagaimana dimaksud pada ayat (2).

Pasal 30

(1) Dalam hal pengawasan sebagaimana dimaksud dalam Pasal 28 ayat (3) terbukti, tim melaporkan kepada Menteri melalui Dirjen untuk dikenakan sanksi administratif.

(2) Dalam hal pengawasan sebagaimana dimaksud dalam Pasal 28 ayat (3) tidak terbukti, tim melaporkan kepada Dirjen hasil pengujian teknis telah sesuai dengan kondisi faktual.

BAB VI
SANKSI ADMINISTRATIF

Pasal 31

Pengguna yang melanggar ketentuan Pasal 10 ayat (2) dikenakan sanksi administratif berupa pencabutan hak akses pemanfaatan data melalui perangkat *Card Reader.*

Pasal 32

(1) Produsen *Card Encoder* dan/atau Produdsen *Card Reader* yang melanggar ketentuan Pasal 13 ayat (1) dan Pasal 15 ayat (1) dikenakan sanksi administratif berupa *Card Encoder* dan/atau *Card Reader* tidak dapat digunakan oleh Pengguna dan Satuan Kerja Pelaksana.

(2) *Card Encoder* dan/atau *Card Reader* sebagaimana dimaksud pada ayat (1) dapat digunakan kembali dengan menggunakan mekanisme proses pengajuan dari awal sebagaimana dimaksud dalam Pasal 13 ayat (1) dan Pasal 15 ayat (1).

Pasal 33

(1) Produsen Blangko KTP-el yang tidak mengembalikan Kartu SAM sebagaimana dimaksud dalam Pasal 19 ayat (2), dikenakan sanksi administratif secara bertahap berupa:
   a. teguran tertulis untuk melaporkan dan mengembalikan Kartu SAM kepada Ditjen paling lama 2 (dua) minggu; dan
   b. pengambilan secara langsung Kartu SAM dari Produsen Blangko KTP-el oleh Ditjen.

(2) Dalam hal Kartu SAM sebagaimana dimaksud pada ayat (1) huruf b akan digunakan kembali, dengan menggunakan mekanisme proses pengajuan dari awal sebagaimana dimaksud dalam Pasal 19 ayat (1).

Pasal 34

Satuan Kerja Pelaksana yang melanggar ketentuan Pasal 20 ayat (2), dikenakan sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan yang mengatur mengenai pelaporan penyelenggaraan Administrasi Kependudukan.

Pasal 35

(1) Produsen *Card Encoder* dan/atau Produsen *Card Reader* yang melanggar ketentuan Pasal 23 ayat (5), dikenakan sanksi administratif secara bertahap berupa:
   a. teguran tertulis untuk melakukan pengembalian Kartu SAM kepada lembaga pengujian teknis dan melaporkan pengembalian Kartu SAM kepada Dirjen paling lama 2 (dua) minggu; dan
   b. pencabutan surat keputusan menjadi Produsen *Card Encoder* dan/atau Produsen *Card Reader* disertai

penarikan Kartu SAM dan/atau pemutusan akses kode kunci.

(2) Sanksi sebagaimana dimaksud pada ayat (1) dilakukan oleh Menteri melalui Dirjen.

Pasal 36

(1) Produsen *Card Encoder* dan/atau Produsen *Card Reader* yang melanggar ketentuan Pasal 30 ayat (1), dikenakan sanksi administratif berupa pencabutan surat keputusan menjadi Produsen *Card Encoder* dan/atau Produsen *Card Reader* disertai penarikan Kartu SAM dan/atau pemutusan akses kode kunci.

(2) Sanksi sebagaimana dimaksud pada ayat (1) dilakukan oleh Menteri melalui Dirjen.

BAB VII

PENDANAAN

Pasal 37

(1) Pendanaan *Card Encoder* dan/atau *Card Reader* di lingkungan Kementerian dibebankan pada anggaran pendapatan dan belanja negara.

(2) Pendanaan *Card Encoder* dan/atau *Card Reader* di lingkungan provinsi dibebankan anggaran pendapatan dan belanja daerah provinsi.

(3) Pendanaan *Card Encoder* dan/atau *Card Reader* di lingkungan kabupaten/kota dibebankan anggaran pendapatan dan belanja daerah kabupaten/kota.

BAB VIII

KETENTUAN PENUTUP

Pasal 38

Pada saat Peraturan Menteri ini mulai berlaku, Peraturan Menteri Dalam Negeri Nomor 34 Tahun 2014 tentang Spesifikasi Teknis Perangkat Pembaca Kartu Tanda Penduduk

Elektronik (Berita Negara Republik Indonesia Tahun 2014 Nomor 590), dicabut dan dinyatakan tidak berlaku.

Pasal 39

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 30 Desember 2020

MENTERI DALAM NEGERI
REPUBLIK INDONESIA,

ttd

MUHAMMAD TITO KARNAVIAN

Diundangkan di Jakarta
pada tanggal 30 Desember 2020

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

WIDODO EKATJAHJANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2020 NOMOR 1776

Salinan sesuai dengan aslinya
Kepala Biro Hukum,

R. Gani Muhamad, SH, MAP
Pembina Utama Muda (IV/c)
NIP. 19690818 199603 1001

LAMPIRAN
PERATURAN MENTERI DALAM NEGERI REPUBLIK INDONESIA
NOMOR 76 TAHUN 2020
TENTANG PERANGKAT PEMBACA DAN PENULIS SERTA PERANGKAT PEMBACA KARTU TANDA PENDUDUK ELEKTRONIK

SPESIFIKASI KOMPONEN *CARD ENCODER* DAN *CARD READER*

I. SPESIFIKASI TEKNIS PERANGKAT PEMBACA DAN PENULIS KTP-el (*CARD ENCODER*)

A. SPESIFIKASI TEKNIS PERANGKAT PEMBACA DAN PENULIS KTP-el TERPISAH

1. SPESIFIKASI TEKNIS PERANGKAT KERAS :

a. *Smart Card Reader*

1)	Standar	:	SNI ISO/IEC 14443.
2)	Frekuensi	:	13,56 MHz ± 7 KHz.
3)	*Baudrate* [kbit/s]	:	106, 212, 424, 848 kbps.
4)	Kuat Medan Operasi	:	dari 1,5 A/m (rms) sampai dengan 7,5 A/m (rms).
5)	Jarak transaksi	:	maksimum 10 cm.
6)	*Slot Secure Access Module* (SAM)	:	mendukung paling sedikit 1 slot SAM, (SAM ditanam di dalam *smart card reader*).
7)	Keamanan	:	Memiliki mekanisme perlindungan keamanan terhadap SAM.
8)	*Interface*	:	USB
9)	Otentikasi	:	mendukung otentikasi dua arah antara *smart card reader* dan cip
10)	Protokol	:	T=0, T=1, dan T=CL.
11)	Komunikasi dengan Komputer (*Host Protocol*)	:	*personal computer/smart card* (PC/SC) pada windows atau linux.
12)	Lain-lain	:	*software development kit.*

b. *Secure Access Module* (SAM) pada *Smart Card Reader*

1)	Cip	:	*smart card* kontak (*contact smart card*) berbasis *microprocessor*.
2)	Standar	:	SNI ISO/IEC 7816 (protokol T=1).
3)	*Instruction Set*	:	SNI ISO/IEC 7816-4.
4)	Kapasitas EEPROM	:	paling rendah 32 KB.
5)	Daya tahan penyimpanan data	:	paling singkat 10 tahun.
6)	*Crypto Co-Processor*	:	memiliki *Crypto Co-Processor* yang mendukung algoritma penyandian 3-Key Triple-DES (3KTDEA) dengan panjang kunci paling rendah 168-bit, algoritma hash SHA256 serta mendukung *Digital Signature* dengan menggunakan ECDSA 256-bit dengan *point curve* secp256r1.
7)	Pembangkit Bilangan Acak	:	standar FIPS 140-2 atau AIS-31 (P2).
8)	Sertifikasi Keamanan	:	memiliki sertifikasi keamanan dengan tingkat jaminan keamanan paling rendah *Common Criteria* EAL5+ atau FIPS 140-2 (atau standar FIPS yang lebih terbaru) paling rendah tingkat 4.
9)	*Mutual Authentication*	:	mendukung proses otentikasi dua arah antara *smart card* dan *reader* dengan mekanisme umpan-balik (*mutual authentication*).
10)	*Anti Cloning*	:	memiliki proteksi terhadap penggandaan secara ilegal (*anti cloning*).
11)	Model/Fungsi	:	dengan fungsi baca tulis.

2. SPESIFIKASI TEKNIS PERANGKAT LUNAK

a. Perangkat Lunak Aplikasi *Card Encoder*

Tersedia dalam bentuk aplikasi *Graphical User Interface* (GUI) dan dalam bentuk *Software Development Kit* (SDK) yang memiliki:

1) Fitur/Fungsi:
   a) menuliskan data ke dalam cip KTP-el.
   b) melakukan verifikasi keabsahan cip KTP-el.
   c) membaca data KTP-el (rekaman biodata, pas photo, tanda tangan dan Sidik Jari) dari cip KTP-el).
   d) melakukan verifikasi keabsahan data KTP-el.
   e) menampilkan data KTP-el (rekaman biodata, pas photo, tanda tangan).
   f) melakukan aktivasi cip KTP-el.
   g) menyimpan riwayat transaksi.
   h) mampu mengirimkan hasil pembacaan data KTP-el (rekaman biodata, pas photo, tanda tangan) ke perangkat komputasi eksternal.
   i) indikator berhasil atau tidaknya sebuah transaksi (visual berupa layar LCD atau setara, atau audio berupa *buzzer* atau setara).
2) Fitur indikator untuk verifikasi Sidik Jari:

   Indikator audio atau visual pada perangkat pemindai Sidik Jari (*fingerprint scanner*) atau perangkat lunak aplikasi untuk mengindikasikan suatu kejadian (*event*) atau informasi:
   a) jari yang akan dipindai.
   b) penempatan Sidik Jari untuk dipindai.
   c) pemindaian Sidik Jari.
   d) berhasil atau gagal verifikasi Sidik Jari.
   e) pemindaian ulang Sidik Jari.

   Fitur indikator untuk verifikasi wajah:

   Indikator audio atau visual pada perangkat pemindai wajah atau perangkat lunak aplikasi untuk mengindikasikan suatu kejadian atau informasi:
   a) pemindaian wajah.
   b) berhasil atau gagal verifikasi wajah.
   c) pemindaian ulang wajah.

3) *Supported Operating System*: Windows atau Linux.
4) *Pembacaan* data dari dalam cip KTP-el melalui Kartu *Secure Access Module* (SAM) fisik atau Kode Kunci secara daring.
5) Standar ekstraktor *minutiae* dan pemadan *minutiae* (*matcher*) untuk verifikasi Sidik Jari:

   Hasil pemadanan (*Matching Results*) pernah masuk dalam sepuluh besar dari *National Institute of Standars and Technology Internal Report* (NISTIR), Amerika Serikat mulai tahun 2003 sampai dengan sekarang.

   Catatan: ekstraktor dan pemadan *minutiae* dapat terintegrasi dengan *fingerprint scanner* atau berupa piranti lunak di perangkat komputasi/*Personal Computer*.

   Standar untuk verifikasi wajah:

   Hasil pemadanan (*Matching Results*) pernah masuk dalam sepuluh besar dari *National Institute of Standars and Technology Internal Report* (NISTIR), Amerika Serikat mulai tahun 2003 sampai dengan sekarang.
6) Kemampuan pemadan *minutiae* (*matcher*):

   Pemadanan *minutiae* dengan membandingkan terhadap *minutiae* dari cip KTP-el dengan *Standar Minutiae*: SNI ISO/IEC 19794-2.
7) Kinerja akurasi sistem verifikasi Sidik Jari secara keseluruhan (algoritma ekstraktor dan algoritma pemadan *minutiae*):

   False Rejection Rate (FRR) 3% atau lebih rendah dan pada *False Acceptance Rate* (FAR) 0,01%.

   Catatan: ekstraktor dan pemadan *minutiae* dapat terintegrasi dengan *fingerprint scanner* atau berupa piranti lunak di perangkat komputasi/*personal computer*.

   Kinerja akurasi sistem verifikasi wajah akan diatur standarnya setelah dilakukan riset atau uji awal sebagai dasar pengujian teknis dan PoC.
8) Kinerja transaksi KTP-el:

   Durasi pembacaan data dan verifikasi Sidik Jari atau verifikasi wajah hingga pemberitahuan hasilnya kepada Pengguna tidak lebih atau sama dengan 15 detik.
9) Keamanan:

a) memiliki mekanisme pengamanan logikal (*logical protection*) terhadap data; dan
b) memiliki keamanan akses terhadap aplikasi dan perangkat komputer di mana aplikasi diinstal.

10) Tersedia *Software Development Kit*.
11) Kode Kunci adalah metode yang digunakan selain menggunakan Kartu SAM secara fisik. Penggunaan Kode Kunci setelah dilakukan *Proof of Concept* (PoC) dan memenuhi standar keamanan informasi.

B. SPESIFIKASI TEKNIS PERANGKAT PEMBACA DAN PENULIS KTP-EL TERINTEGRASI

1. SPESIFIKASI TEKNIS PERANGKAT KERAS

a. Smart Card Reader

1)	Standar	:	SNI ISO 14443 A and B.
2)	Frekuensi	:	13,56 MHz ± 7 KHz.
3)	Baudrate	:	paling rendah 100 kbps.
4)	Kuat Medan Operasi	:	dari 1,5 A/m (rms) sampai dengan 7,5 A/m (rms).
5)	Jarak transaksi	:	maksimum 10 cm.
6)	Inisialisasi dan anti *collision*	:	SNI ISO/IEC 14443-3.
7)	*Bit rate*	:	bit rate untuk melakukan komunikasi dengan KTP-el pada saat proses inisialisasi dan anticollision = fc/128 (~106 kbit/s). bit rate untuk melakukan komunikasi dengan KTP-el setelah proses inisialisasi dan anticollision bernilai salah satu dari rumusan berikut ini: — fc/128 (~106 kbit/s), — fc/64 (~212 kbit/s), — fc/32 (~424 kbit/s), — fc/16 (~848 kbit/s).
8)	Protokol Komunikasi	:	T = CL

9)	Slot *Secure Access Module* (SAM)	:	mendukung paling rendah 1 slot SAM.
10)	Otentikasi	:	mendukung otentikasi dua arah antara *smart card reader* dan cip.
11)	Lain - lain	:	*software development kit.*

b. *Secure Access Module* (SAM) pada *Smart Card Reader*

1)	Cip	:	*smart card* kontak (*contact smart card*) berbasis *microprocessor*.
2)	Standar	:	SNI ISO 7816 (protokol T=1).
3)	*Instruction set*	:	SNI ISO 7816-4.
4)	*Kapasitas* EEPROM	:	paling rendah 32 KB.
5)	Daya tahan penyimpanan data	:	paling singkat 10 tahun.
6)	*Crypto Co-Processor*	:	memiliki *Crypto Co-Processor* yang mendukung algoritma penyandian 3-Key Triple-DES (3KTDEA) dengan panjang kunci paling rendah 168-bit, algoritma *hash* SHA256 serta mendukung *Digital Signature* dengan menggunakan ECDSA 256-bit dengan *point curve* secp256r1.
7)	Pembangkit bilangan acak	:	standar FIPS 140-2 atau AIS-31 (P2).
8)	Sertifikasi keamanan	:	memiliki sertifikasi keamanan dengan tingkat jaminan keamanan paling rendah *Common Criteria* EAL5+ atau FIPS 140-2 paling rendah tingkat 4.
9)	*Mutual authentication*	:	mendukung proses otentikasi dua arah antara *smart card* dan *reader* dengan mekanisme umpan-balik (*mutual authentication*).
10)	*Anti cloning*	:	memiliki proteksi terhadap penggandaan secara illegal (*anti cloning*).
11)	*Model*/fungsi	:	dengan fungsi Baca Tulis (*Read Write*).

c. Fingerprint Scanner

1)	Tipe sensor	:	berbasis *Optic*, apabila akan digunakan tipe sensor selain berbasis *optic* (*capacitive, ultrasonic* dan lain-lain) perlu dilakukan riset/penelitian awal untuk mendukung prosedur pengujian dan *Proof of Concept* (PoC). diperlukan data dukung awal seperti minimum 3.000 sampel yang sama atau hasil perekaman sesuai tipe sensor selain *optic* tersebut.
2)	Luas permukaan sensor	:	bagi tipe sensor *optic*, paling rendah *one fingerprint scanner* dengan dimensi paling rendah 15,2 mm x 20,3 mm (atau paling rendah setara dengan sensor jenis FAP 20). bagi tipe sensor selain *optic* akan disesuaikan berdasarkan hasil riset awal sebagaimana catatan nomor (1).
3)	Resolusi	:	paling rendah 500 dpi (± 10 dpi).
4)	Citra keluaran	:	Paling rendah 8 bit skala abu-abu (8-*bit gray scale image*).
5)	Standar sensor	:	FBI IQS Compliant, Sertifikasi PIV (*Personal Identifikasi Verification*).
6)	Standar *minutiae* Sidik Jari	:	SNI ISO/IEC 19794-2.
7)	*Supported operating system*	:	*windows* atau *linux* atau *android* atau *embedded* OS atau setara.
8)	Lain-lain	:	*software development kit*.

d. Perangkat Komputasi

1)	Processor	:	paling rendah 16-bit yang dapat diprogram ulang (*reprogrammable*).
2)	*Memory*	:	1) paling sedikit 128 *Kilobytes* untuk program. 2) paling sedikit 256 *Kilobytes*

untuk data.

3) paling sedikit 20 *Megabytes* untuk menyimpan data riwayat transaksi.

3) *Display*/layar tampilan : 1) jenis layar sentuh *monochrome* atau berwarna atau layar *monochrome* atau berwarna dengan papan tombol. Resolusi Paling rendah 320 x 240@60 Hz. Atau

2) layar *monochrome* teks atau

3) tanpa layar, tetapi dengan indikasi visual/audio terhadap otentisitas cip dan data, serta sukses/gagal verifikasi Sidik Jari.

4) Antar muka : 1) antarmuka RF untuk menerima transaksi KTP-el.

2) antarmuka pemindaian Sidik Jari untuk menerima transaksi verifikasi Sidik Jari 1:1 (*one-to-one matching*).

3) antarmuka Serial atau USB atau *ethernet* untuk keperluan pemrograman ulang aplikasi dan pengambilan data dan riwayat transaksi.

4) bagian antarmuka pemasok daya listrik AC dan/atau baterai kering dan/atau jenis lainnya.

5) Supported *operating system* : *windows* atau *linux* atau *android* atau *embedded* OS atau setara.

e. Karakteristik Fisik Perangkat Terintegrasi

Keamanan perangkat : mekanisme pengamanan fisik (*tamper resistant*).

f. Catu Daya

Asal catu daya : catu daya tersedia dari listrik AC

dan/atau baterai kering dan/atau jenis lainnya.

g. Printer : *card encoder* terintegrasi pada perangkat Prepersonalisasi Blangko KTP-el atau Printer pada proses Personalisasi/pencetakan KTP-el.

2. SPESIFIKASI TEKNIS PERANGKAT LUNAK

a. Fitur/fungsi :

1) melakukan penulisan data ke dalam cip KTP-el.
2) melakukan verifikasi keabsahan cip KTP Elektonik.
3) membaca data KTP-el (rekaman biodata, pas photo, tanda tangan dan Sidik Jari dari cip KTP-el).
4) melakukan verifikasi keabsahan data KTP-el.
5) melakukan verifikasi keabsahan pemilik KTP-el melalui verifikasi Sidik Jari (dan/atau foto wajah)
6) menampilkan data KTP-el (rekaman biodata, pas photo, tanda tangan).
   Catatan : data yang ditampilkan bergantung pada jenis layar tampilan grafik /teks.
7) melakukan aktivasi cip KTP-el.
8) menyimpan riwayat transaksi.
9) mampu mengirimkan hasil pembacaan data KTP-el (rekaman biodata, pas photo, tanda tangan) ke perangkat komputasi eksternal.
10) indikator berhasil atau tidaknya sebuah transaksi (visual dan/atau *buzzer* dan/atau lampu LED).

b.	fitur indikator untuk verifikasi Sidik Jari	:	1) jari yang akan dipindai. 2) penempatan Sidik Jari untuk dipindai. 3) pemindaian Sidik Jari. 4) sukses/gagal verifikasi Sidik Jari. 5) pemindaian ulang Sidik Jari.
c.	Fitur indikator untuk verifikasi wajah:	:	1) wajah yang akan dipindai. 2) penempatan wajah untuk dipindai. 3) pemindaian wajah. 4) berhasil atau gagal verifikasi wajah. 5) pemindaian ulang wajah.
d.	*Supported operating system*	:	*windows* atau *linux* atau *android* atau RTOS atau *embedded* OS atau setara.
e.	Pembacaan data dari dalam cip KTP-el melalui	:	*Secure access module* (SAM) dan/atau kode kunci.
f.	Standar ekstraktor *minutiae* dan pemadan *minutiae* (*matcher*)	:	hasil pemadanan (*matching results*) pernah masuk dalam sepuluh besar dari *National Institute of Standars and Technology Internal Report* (NISTIR), Amerika Serikat mulai tahun 2003 sampai dengan sekarang. Catatan: Ekstraktor dan pemadan *minutiae* dapat terintegrasi dengan *Fingerprint scanner* atau berupa piranti lunak di perangkat komputasi.
g.	Kemampuan pemadan *minutiae* (*matcher*)	:	pemandanan *minutiae* dengan membandingkan terhadap *minutiae* dari cip KTP-el dengan Standar *Minutiae*: SNI ISO/IEC 19794-2.
h.	Kinerja akurasi sistem verifikasi Sidik Jari secara keseluruhan (algoritma ekstraktor dan algoritma	:	*false rejection rate* (FRR) 3 % atau lebih rendah dan pada *false acceptance rate* (FAR) 0,01 %

pemadan *minutiae*)
Catatan :

Ekstraktor dan pemadan minutiae dapat terintegrasi dengan fingerprint scanner atau berupa piranti lunak di perangkat komputasi.

Selanjutnya, kinerja akurasi sistem verifikasi wajah akan diatur standarnya setelah dilakukan riset atau uji awal sebagai dasar pengujian teknis dan PoC.

i. Kinerja transaksi KTP-el : durasi pembaca data dan verifikasi Sidik Jari, kurang dari 15 detik.
j. Keamanan data : Mekanisme pengamanan non fisik *(logical protection*) terhadap data dan aplikasi.
k. Kode kunci : kode kunci adalah metode yang digunakan selain menggunakan Kartu SAM secara fisik. Penggunaan Kode Kunci setelah dilakukan *Proof of Concept* (PoC) dan memenuhi standar keamanan informasi.
l. Lain - lain : *software development kit*.

II. SPESIFIKASI TEKNIS PERANGKAT PEMBACA KTP-el (*CARD READER*)

A. SPESIFIKASI TEKNIS PERANGKAT PEMBACA KTP-el TERINTEGRASI

1. SPESIFIKASI TEKNIS PERANGKAT KERAS

a. *Smart Card Reader*

1) Standar : SNI ISO 14443 A and B.
2) Frekuensi : 13,56 MHz ± 7 KHz.
3) Baudrate : paling rendah 100 kbps.
4) Kuat medan operasi : dari 1,5 A/m (rms) sampai dengan 7,5 A/m (rms).
5) Jarak transaksi : maksimum 10 cm.
6) Inisialisasi dan anti collision : SNI ISO/IEC 14443-3.
7) Bit rate : *bit rate* untuk melakukan komunikasi dengan KTP-el pada saat proses inisialisasi dan anticollision = fc/128 (~106 kbit/s).

bit rate untuk melakukan komunikasi dengan KTP-el setelah proses inisialisasi dan anticollision bernilai salah satu dari rumusan berikut ini:
— fc/128 (~106 kbit/s),
— fc/64 (~212 kbit/s),
— fc/32 (~424 kbit/s),
— fc/16 (~848 kbit/s).

8) Protokol komunikasi : T = CL
9) Slot secure access module (SAM) : mendukung paling rendah 1 slot SAM.
10) Otentikasi : mendukung otentikasi dua arah antara *smart card reader* dan cip.
11) Lain - lain : *software development kit*.

b. *Secure Access Module* (SAM) pada *Smart Card Reader*

1) Cip : *smart card* kontak (*contact smart card*) berbasis *microprocessor*.
2) Standar : SNI ISO 7816 (protokol T=1).
3) Instruction Set : SNI ISO 7816-4.
4) Kapasitas EEPROM : paling rendah 32 KB.
5) Daya tahan penyimpanan data : paling singkat 10 tahun.
6) Crypto Co-Processor : memiliki *Crypto Co-Processor* yang mendukung algoritma penyandian 3-Key Triple-DES (3KTDEA) dengan panjang kunci paling rendah 168-bit, algoritma *hash* SHA256 serta mendukung Digital Signature dengan menggunakan ECDSA 256-bit dengan *point curve* secp256r1.
7) Pembangkit bilangan acak : standar FIPS 140-2 atau AIS-31 (P2).
8) Sertifikasi keamanan : memiliki sertifikasi keamanan dengan tingkat jaminan keamanan paling rendah *Common Criteria* EAL5+ atau FIPS 140-2 paling rendah tingkat 4.

9)	Mutual authentication	:	mendukung proses otentikasi dua arah antara *smart card* dan *reader* dengan mekanisme umpan-balik (*mutual authentication*).
10)	Anti cloning	:	memiliki proteksi terhadap penggandaan secara ilegal (*anti cloning*).
11)	Model/fungsi	:	hanya dengan fungsi Baca (*Read*).

c. *Fingerprint scanner*

1)	Tipe sensor	:	berbasis *Optic*, apabila akan digunakan tipe sensor selain berbasis *optic* (*capacitive, ultrasonic* dan lain-lain) perlu dilakukan riset/penelitian awal untuk mendukung prosedur pengujian dan *Proof of Concept* (PoC). Diperlukan data dukung awal seperti minimum 3.000 sampel yang sama atau hasil perekaman sesuai tipe sensor selain *optic* tersebut.
2)	Luas permukaan sensor	:	bagi tipe sensor *optic*, paling rendah *one fingerprint scanner* dengan dimensi paling rendah 15,2 mm x 20,3 mm (atau paling rendah setara dengan sensor jenis FAP 20). bagi tipe sensor selain *optic* akan disesuaikan berdasarkan hasil riset awal sebagaimana catatan nomor (1).
3)	Resolusi	:	paling rendah 500 dpi (± 10 dpi).
4)	Citra keluaran	:	paling rendah 8 bit skala abu-abu (8-*bit gray scale image*).
5)	Standar sensor	:	FBI IQS *Compliant*, sertifikasi PIV (*Personal Identifikasi Verification*).
6)	Standar minutiae Sidik Jari	:	SNI ISO/IEC 19794-2.
7)	Supported Operating System	:	*windows* atau *linux* atau *android* atau e*mbedded* OS atau setara.
8)	Lain-lain	:	*software development kit*.

d. *Perangkat* Komputasi

1) *Processor*	:	paling rendah 16-bit yang dapat diprogram ulang (*reprogrammable*).
2) *Memory*	:	1) paling sedikit 128 *Kilobytes* untuk program. 2) paling sedikit 256 *Kilobytes* untuk data. 3) paling sedikit 20 *Megabytes* untuk menyimpan data riwayat transaksi.
3) *Display/layar tampilan*	:	1) jenis layar sentuh *monochrome* atau berwarna atau layar *monochrome* atau berwarna dengan papan tombol. Resolusi Paling rendah 320 x 240@60 Hz atau 2) layar *monochrome* teks atau 3) tanpa layar, tetapi dengan indikasi visual/audio terhadap otentisitas cip dan data, serta sukses/gagal verifikasi Sidik Jari.
4) *Antar* muka	:	1) antarmuka RF untuk menerima transaksi KTP-el. 2) antarmuka pemindaian Sidik Jari untuk menerima transaksi verifikasi Sidik Jari 1:1 (*one-to-one matching*). 3) antarmuka Serial atau USB atau ethernet untuk keperluan pemrograman ulang aplikasi dan pengambilan data dan riwayat transaksi. 4) bagian antarmuka pemasok daya listrik AC dan/atau baterai kering dan/atau jenis lainnya.
5) *Supported*	:	*windows* atau *linux* atau *android* atau

operating system		*embedded* OS atau setara.

e. Karakteristik Fisik Perangkat Terintegrasi

Keamanan perangkat	:	mekanisme pengamanan fisik (*tamper resistant*).

f. Catu daya

Asal catu daya	:	catu daya tersedia dari listrik AC dan/atau baterai kering dan/atau jenis lainnya.

2. SPESIFIKASI TEKNIS PERANGKAT LUNAK

a. Fitur/fungsi	:	1) melakukan verifikasi keabsahan cip KTP Elektonik. 2) membaca data KTP-el (rekaman biodata, pas photo, tanda tangan dan Sidik Jari dari cip KTP-el). 3) melakukan verifikasi keabsahan data KTP-el. 4) melakukan verifikasi keabsahan pemilik KTP-el melalui verifikasi Sidik Jari. 5) menampilkan data KTP-el (rekaman biodata, pas photo, tanda tangan). *Catatan : data yang ditampilkan bergantung pada jenis layar tampilan grafik /teks.* 6) melakukan aktivasi cip KTP-el. 7) menyimpan riwayat transaksi. 8) mampu mengirimkan hasil pembacaan data KTP-el (rekaman biodata, pas photo, tanda tangan) ke perangkat komputasi eksternal. 9) indikator berhasil atau tidaknya sebuah transaksi (visual dan/atau *buzzer* dan/atau lampu LED).
b. Fitur indikator untuk verifikasi Sidik Jari	:	1) jari yang akan dipindai. 2) penempatan Sidik Jari untuk

dipindai.

3) pemindaian Sidik Jari.
4) sukses/gagal verifikasi Sidik Jari.
5) pemindaian ulang Sidik Jari.

c. *Supported operating system* : *windows* atau *linux* atau *android* atau RTOS atau *embedded* OS atau setara.

d. *Pembacaan* data dari dalam cip KTP-el melalui : *secure access module* (SAM) dan/atau kode kunci.

e. *Standar* ekstraktor *minutiae* dan pemadan *minutiae* (*matcher*) : hasil pemadanan (*matching results*) pernah masuk dalam sepuluh besar dari *National Institute of Standars and Technology Internal Report* (NISTIR), Amerika Serikat mulai tahun 2003 sampai dengan sekarang.

Catatan:
ekstraktor dan pemadan *minutiae* dapat terintegrasi dengan *fingerprint scanner* atau berupa piranti lunak di perangkat komputasi.

f. Kemampuan *pemadan minutiae (matcher)* : pemadanan *minutiae* dengan membandingkan terhadap *minutiae* dari cip KTP-el dengan Standar *Minutiae*: SNI ISO/IEC 19794-2.

g. Kinerja akurasi system verifikasi Sidik Jari secara keseluruhan (algoritma ekstraktor dan algoritma pemadan *minutiae*) : *false rejection rate* (FRR) 3 % atau lebih rendah dan pada *false acceptance rate* (FAR) 0,01 %

Catatan :

Ekstraktor dan pemadan minutiae dapat terintegrasi dengan *fingerprint scanner* atau berupa piranti lunak di perangkat komputasi.

h. Kinerja transaksi KTP-el : durasi pembaca data dan verifikasi Sidik Jari, kurang dari 15 detik.

i. Keamanan data : mekanisme pengamanan non fisik

(logical protection) terhadap data dan aplikasi.

j. Kode kunci : kode kunci adalah metode yang digunakan selain menggunakan Kartu SAM secara fisik. Penggunaan Kode Kunci setelah dilakukan *Proof of Concept* (PoC) dan memenuhi standar keamanan informasi.

k. Lain - lain : *software development kit*.

B. SPESIFIKASI TEKNIS PERANGKAT PEMBACA KTP-el TERPISAH (UNTUK RISET DAN KAJIAN)

1. SPESIFIKASI TEKNIS PERANGKAT KERAS

a. *Smart Card Reader*

1)	Standar	:	SNI ISO/IEC 14443.
2)	Frekuensi	:	13,56 MHz ± 7 KHz.
3)	*Baudrate* [kbit/s]	:	106, 212, 424, 848 kbps.
4)	Kuat medan operasi	:	dari 1,5 A/m (rms) sampai dengan 7,5 A/m (rms).
5)	Jarak transaksi	:	maksimum 10 cm.
6)	*Slot secure access module* (SAM)	:	mendukung paling sedikit 1 slot SAM, (SAM ditanam di dalam *smart card reader*).
7)	Keamanan	:	memiliki mekanisme perlindungan keamanan terhadap SAM.
8)	*Interface*	:	USB
9)	Otentikasi	:	Mendukung otentikasi dua arah antara *smart card reader* dan cip
10)	Protokol	:	T=0, T=1, dan T=CL.
11)	Komunikasi dengan komputer	:	*personal computer/smart card* (PC/SC) pada *windows* atau *linux*.
12)	CPU	:	paling rendah 16-bit *processor*.
13)	*Program memory*	:	paling rendah 64 *Kbytes*.
14)	*Data memory*	:	paling rendah 20 *Kbytes*.

15) Lain-lain : *software development kit.*

b. *Secure Access Module* (SAM) pada *Smart Card Reader*

1) Cip : *smart card* kontak (*contact smart card*) berbasis microprocessor.
2) Standar : SNI ISO/IEC 7816 (protokol T=1).
3) *Instruction Set* : SNI ISO/IEC 7816-4.
4) Kapasitas EEPROM : paling rendah 32 KB.
5) Daya tahan penyimpanan data : paling singkat 10 tahun.
6) *Crypto Co-Processor* : memiliki *Crypto Co-Processor* yang mendukung algoritma penyandian 3-Key Triple-DES (3KTDEA) dengan panjang kunci paling rendah 168-bit, algoritma hash SHA256 serta mendukung *Digital Signature* dengan menggunakan ECDSA 256-bit dengan *point curve* secp256r1.
7) Pembangkit bilangan acak : SP 800-140D, SNI ISO/IEC 18031
8) Sertifikasi keamanan : memiliki sertifikasi keamanan dengan tingkat jaminan keamanan paling rendah *Common Criteria* EAL5+ atau FIPS 140-2 (atau standar FIPS yang lebih terbaru) paling rendah tingkat 4.
9) *Mutual authentication* : mendukung proses otentikasi dua arah antara *smart card* dan *reader* dengan mekanisme umpan-balik (*mutual authentication*).
10) *Anti cloning* : memiliki proteksi terhadap

penggandaan secara ilegal (*anti cloning*).

11) Model/fungsi : hanya dengan fungsi baca (*Read*).

c. *Fingerprint Scanner*

1) Tipe : optic *base,* paling rendah *one fingerprint scanner*, dengan dimensi paling rendah 15,2 mm x 20,3 mm (atau paling rendah setara dengan sensor jenis FAP 20) atau *ten fingerprint scanner* atau *slap* atau 4+4+2.

Catatan: apabila akan digunakan tipe sensor selain berbasis *optic* (*capacitive, ultrasonic* dan lain-lain) perlu dilakukan riset/penelitian awal untuk mendukung prosedur pengujian dan *Proof of Concept* (PoC).

Diperlukan data dukung awal seperti minimum 3.000 sampel yang sama atau hasil perekaman sesuai tipe sensor selain *optic* tersebut.

2) Resolusi : paling rendah 500 dpi.

3) Citra keluaran : paling rendah 8 bit skala abu-abu (8-*bit gray scale image*).

4) *Supported operating system* : *windows* atau *linux*.

5) Standar sensor : FBI *Compliants*, IQS EFTS.

6) Standar *minutiae* : SNI ISO/IEC 19794-2.

7) *Software development kit* : tersedia *software development kit*.

8) *Power supply* : *power supply* melalui kabel USB atau yang disesuaikan.

d. *Personal Computer*

1)	*Processor*	:	intel-based x86 atau setara.
2)	*Memory*	:	mendukung pengoperasian sistem operasi (*operating system*), aplikasi pelindung keamanan (misalnya, anti virus) dan aplikasi Pembaca KTP-el.
3)	*Hard disk*	:	mendukung pengoperasian sistem operasi (*operating system*), aplikasi pelindung keamanan (misalnya, anti virus) dan aplikasi Pembaca KTP-el.
4)	Monitor	:	dapat menampilkan data KTP-el (biodata, pas photo dan tanda tangan).
5)	USB port	:	paling sedikit 4 buah.
6)	*Operating System*	:	*windows/linux*.

e. *Camera*

Perlu dilakukan riset/penelitian awal untuk mendukung prosedur pengujian dan *Proof of Concept* (PoC) atas kebutuhan *Facial Recognition* (FR).

Dalam rangka FR tersebut diperlukan data dukung awal minimum sebagai standar spesifikasi pengujian FR yang akan ditentukan kemudian.

2. SPESIFIKASI TEKNIS PERANGKAT LUNAK

Perangkat lunak aplikasi pembaca KTP-el tersedia dalam bentuk aplikasi *Graphical User Interface* (GUI) dan dalam bentuk *Software Development Kit* (SDK) yang memiliki:

a. Fitur/fungsi:

1) melakukan verifikasi keabsahan cip KTP-el.
2) membaca data KTP-el (rekaman biodata, pas photo, tanda tangan dan Sidik Jari) dari cip KTP-el).
3) melakukan verifikasi keabsahan data KTP-el.
4) melakukan verifikasi keabsahan pemilik KTP-el melalui

verifikasi Sidik Jari.

5) menampilkan data KTP-el (rekaman biodata, pas photo, tanda tangan).
6) melakukan aktivasi cip KTP-el.
7) menyimpan riwayat transaksi.
8) mampu mengirimkan hasil pembacaan data KTP-el (rekaman biodata, pas photo, tanda tangan) ke perangkat komputasi eksternal.
9) indikator berhasil atau tidaknya sebuah transaksi (visual berupa layar LCD atau setara, atau audio berupa *buzzer* atau setara).

b. Fitur indikator untuk verifikasi Sidik Jari :

indikator audio atau visual pada perangkat pemindai Sidik Jari (*fingerprint scanner*) atau perangkat lunak aplikasi untuk mengindikasikan suatu kejadian atau informasi:

a) jari yang akan dipindai.
b) penempatan Sidik Jari untuk dipindai.
c) pemindaian Sidik Jari.
d) berhasil atau gagal verifikasi Sidik Jari.
e) pemindaian ulang Sidik Jari.

Fitur indikator untuk verifikasi wajah :

Indikator audio atau visual pada perangkat pemindai wajah (*Facial Recognition*) atau perangkat lunak aplikasi untuk mengindikasikan suatu kejadian (*event*) atau informasi:

a) pemindaian wajah.
b) berhasil atau gagal verifikasi wajah.
c) pemindaian ulang wajah.

c. *Supported operating system*: *windows atau linux*.

d. Pembacaan data dari dalam cip KTP-el melalui Kartu *Secure Access Module* (SAM) fisik atau Kode Kunci secara daring.

e. Standar ekstraktor *minutiae* dan pemadan *minutiae* (*matcher*) untuk verifikasi Sidik Jari:

Hasil pemadanan (*matching results*) pernah masuk dalam sepuluh besar dari *National Institute of Standars and Technology Internal Report* (NISTIR), Amerika Serikat mulai tahun 2003 sampai dengan sekarang.

Catatan: ekstraktor dan pemadan *minutiae* dapat terintegrasi

dengan *fingerprint scanner* atau berupa piranti lunak di perangkat komputasi/*Personal Computer*.

Standar untuk verifikasi wajah:

Hasil pemadanan (*matching results*) pernah masuk dalam sepuluh besar dari *National Institute of Standars and Technology Internal Report* (NISTIR), Amerika Serikat mulai tahun 2003 sampai dengan sekarang.

f. Kemampuan pemadan *minutiae* (*matcher*):

Pemadanan *minutiae* dengan membandingkan terhadap *minutiae* dari cip KTP-el dengan *Standar Minutiae*: SNI ISO/IEC 19794-2.

g. Kinerja akurasi sistem verifikasi Sidik Jari secara keseluruhan (algoritma ekstraktor dan algoritma pemadan *minutiae*):

false rejection rate (FRR) 3% atau lebih rendah dan pada *false acceptance rate* (FAR) 0,01%.

Catatan: ekstraktor dan pemadan *minutiae* dapat terintegrasi dengan *fingerprint scanner* atau berupa piranti lunak di perangkat komputasi/*personal computer*.

Kinerja akurasi sistem verifikasi wajah akan diatur standarnya setelah dilakukan riset atau uji awal sebagai dasar pengujian teknis dan PoC.

h. Kinerja transaksi KTP-el:

Durasi pembacaan data dan verifikasi Sidik Jari atau verifikasi wajah hingga pemberitahuan hasilnya kepada Pengguna tidak lebih atau sama dengan 15 detik.

i. Keamanan:

a) memiliki mekanisme pengamanan logikal (*logical protection*) terhadap data; dan
b) memiliki keamanan akses terhadap aplikasi dan perangkat komputer di mana aplikasi diinstal.

j. Tersedia *software development kit*.

k. Kode kunci

Kode kunci adalah metode yang digunakan selain menggunakan Kartu SAM secara fisik. Penggunaan Kode Kunci setelah dilakukan *Proof of Concept* (PoC) dan memenuhi standar keamanan informasi.

III. PENJELASAN

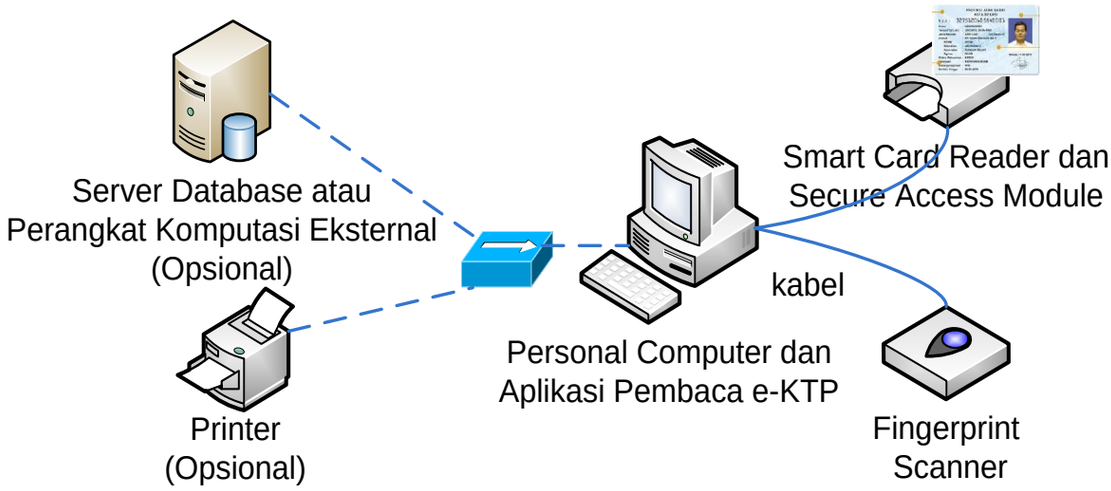
Card Encoder dan/atau *Card Reader*

Card Encoder dan *Card Reader* terdiri atas perangkat keras yaitu perangkat komputasi, perangkat pembaca dan/atau penulis kartu cerdas (*smart card reader*), dan dapat disertai perangkat pemindai Sidik Jari (*fingerprint scanner*) atau pemindai wajah serta printer; dan perangkat lunak yaitu aplikasi pembaca dan/atau penulis KTP-el. Perangkat keras dan perangkat lunak tersebut dapat berupa:

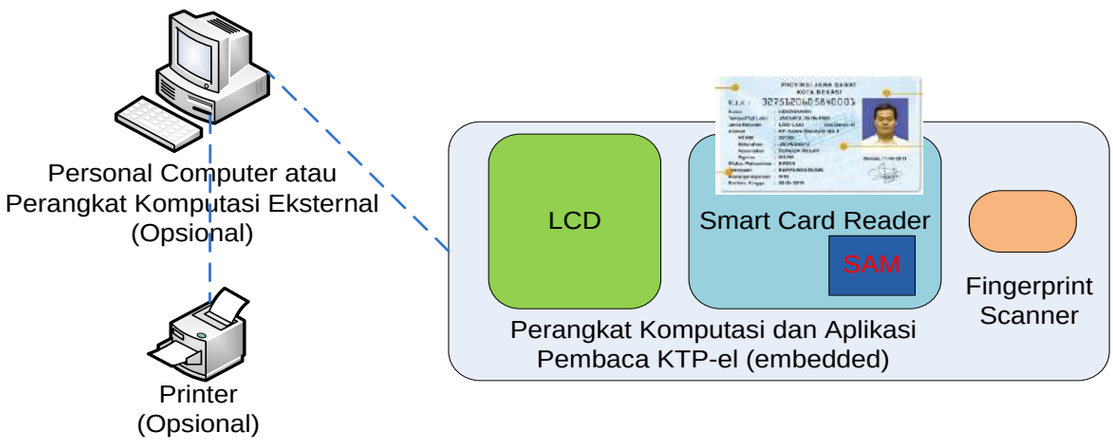
1. berdiri sendiri secara terpisah yang masing-masing harus terhubung dengan perangkat komputer seperti terlihat pada Gambar 1, sebagaimana yang telah diterapkan pada pelayanan perekaman KTP-el di Satuan Kerja Pelaksana untuk *Card Encoder*, atau
2. terintegrasi menjadi sebuah Perangkat Pembaca KTP-el yang mandiri tanpa harus terhubung dengan perangkat komputer, seperti terlihat pada Gambar 2, yang diterapkan pada pelayanan publik di Instansi Pemerintah, Pemerintah Daerah, Lembaga Perbankan, dan Swasta yang berkaitan dengan dan tidak terbatas pada Perizinan, Usaha, Perdagangan, Jasa Perbankan, Asuransi, Perpajakan dan Pertanahan, dll untuk *Card Reader*.

Card Encoder memiliki fitur menuliskan data ke dalam cip KTP-el dalam proses pencetakan Blangko KTP-el dan pencetakan KTP-el. Sedangkan *Card Reader* memiliki fitur untuk pembacaan KTP-el dan mengirimkan data hasil pembacaan KTP-el tersebut. Satuan Kerja Pelaksana dan Pengguna Serta Produsen *Card Encoder* dan/atau Produsen *Card Reader* wajib menjamin kerahasiaan, keutuhan dan kebenaran data yang diperoleh dari hasil penulisan dan/atau pembacaan data cip KTP-el oleh *Card Encoder* dan/atau *Card Reader*.

Dalam rangka pengkajian dan pengembangan *Card Encoder* dan *Card Reader,* Kementerian melalui Ditjen melibatkan lembaga pemerintah nonkementerian yang memiliki tugas dan fungsi pengkajian dan penerapan teknologi dan lembaga pemerintah nonkementerian yang memiliki tugas dan fungsi keamanan siber dan sandi negara.



Gambar 1. Perangkat Pembaca dan/atau Penulis KTP Elektronik (Terpisah)



Gambar 2. Perangkat Pembaca KTP Elektronik Terintegrasi

Card Reader memanfaatkan dua faktor otentikasi untuk verifikasi otentikasi keabsahan KTP-el, keabsahan data pada cip KTP-el dan keabsahan kepemilikan KTP-el. Secara standar *best practice* internasional untuk otentikasi identitas, faktor otentikasi yang digunakan terhadap KTP-el adalah otentikasi terhadap keabsahan cip pada kartu KTP-el ("Apa yang Anda miliki" - "*what you have*") dan otentikasi terhadap kepemilikan kartu KTP-el, yaitu otentikasi karakteristik khas biometrik Penduduk berupa Sidik Jari dan/atau foto wajah ("Apa karakteristik khusus Anda yang melekat" - "*what you are*"). Berdasarkan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah menjadi Undang-Undang Nomor 24 Tahun 2013, dalam KTP-el disediakan ruang untuk memuat kode keamanan dan rekaman elektronik. Rekaman elektronik menyimpan data elektronik Penduduk yang dapat dibaca secara elektronik dengan alat pembaca dan sebagai pengaman data kependudukan.

Alat identifikasi pada *Data Center* menggunakan rekaman Sidik Jari, iris mata dan wajah, sedangkan alat identifikasi dalam KTP-el menggunakan rekaman Sidik Jari dan/atau foto wajah. Sidik Jari Penduduk yang disimpan di dalam cip KTP-el adalah Sidik Jari telunjuk kanan dan Sidik Jari telunjuk kiri. Dalam rangka implementasi teknis di lapangan, terdapat mekanisme di aplikasi perekaman KTP-el, jika Sidik Jari telunjuk kanan dan/atau Sidik Jari telunjuk kiri, memiliki kualitas yang kurang baik, sehingga berpotensi gagal verifikasi Sidik Jari, maka Sidik Jari yang lain yang memiliki kualitas yang baik untuk verifikasi Sidik Jari akan disimpan di dalam cip KTP-el.

Card Reader akan memastikan/mengotentikasi keabsahan KTP-el, dan keabsahan data cip KTP-el serta keabsahan kepemilikan KTP-el Penduduk yang memastikan dokumen kependudukan sebagai milik orang tersebut. Data rekaman biodata, pas photo dan tanda tangan dari cip akan ditampilkan di layar tampilan dan/atau dapat ditampilkan di sistem informasi/komputer Instansi Pengguna, setelah sukses verifikasi Sidik Jari secara elektronik. Verifikasi Sidik Jari secara elektronik yaitu pemadanan antara Sidik Jari yang dipindai pada saat verifikasi oleh Perangkat Pembaca KTP-el dan Sidik Jari yang tersimpan di dalam cip. Apabila Sidik Jari yang dipindai identik dengan Sidik Jari yang tersimpan di dalam cip, maka verifikasi Sidik Jari sukses dalam rangka memastikan KTP-el sebagai milik orang tersebut.

Secara prinsip, data rekaman biodata, pas photo dan tanda tangan dari cip akan ditampilkan di layar tampilan dan/atau dapat disimpan di sistem informasi/komputer Instansi Pengguna, setelah sukses verifikasi Sidik Jari secara elektronik, serta Penduduk pemilik KTP-el dan Pengguna Perangkat Pembaca KTP-el memperoleh informasi tentang tentang keabsahan kartu KTP-el dan proses verifikasi Sidik Jari berhasil atau tidak.

Mekanisme dan prosedur tertentu berlaku apabila terjadi suatu kegagalan dalam verifikasi Sidik Jari, walaupun Penduduk benar sebagai pemilik KTP-el tersebut.

Perangkat Pembaca KTP-el Terintegrasi, terdiri atas:

1. Perangkat Keras
    a. perangkat komputasi.
    b. perangkat pembaca kartu cerdas (s*mart card reader*).
    c. *secure access module* (SAM).
    d. perangkat pemindai Sidik Jari (*fingerprint scanner*).

e. layar tampilan grafik, atau layar tampilan teks, atau indikator audio/ visual terhadap keabsahan KTP-el dan sukses verifikasi Sidik Jari.

2. Perangkat Lunak

aplikasi pembaca KTP-el.

Perangkat Pembaca KTP-el Terintegrasi ini mengintegrasikan semua komponen perangkat keras dan perangkat lunak. Perangkat Pembaca KTP-el Terintegrasi ini dapat dioperasikan secara mandiri, di mana hasil pembacaan biodata, foto wajah dan tanda tangan, serta hasil verifikasi Sidik Jari secara elektronik dapat ditampilkan secara aman di layar tampilan yang terintegrasi di perangkat tersebut. Perangkat ini memiliki fitur yang dapat dikoneksikan ke perangkat komputer (*personal computer*) Instansi Pengguna untuk mengambil data dan/atau mencetak hasil pembacaan data tersebut.

Fungsi dari Perangkat Pembaca KTP-el (*Card reader*) adalah sebagai berikut:

1. memastikan bahwa KTP-el Penduduk menggunakan Cip KTP-el yang sah yang diterbitkan oleh Satuan Kerja Pelaksana melalui mekanisme kriptografi yang diimplementasikan dalam Kartu SAM KTP-el atau mekanisme kriptograsi lainnya yang ditetapkan oleh Ditjen Dukcapil;
2. memastikan bahwa data Penduduk yang dibaca dari cip KTP-el adalah data yang benar dan sah, sesuai yang diterbitkan oleh Satuan Kerja Pelaksana melalui mekanisme kriptografi yang diimplementasikan dalam Kartu SAM KTP-el atau mekanisme kriptograsi lainnya yang ditetapkan oleh Ditjen Dukcapil;
3. membantu otentikasi visual keabsahan data yang tercetak pada permukaan KTP-el dengan cara membandingkan secara visual terhadap data yang diperoleh dari hasil pembacaan cip KTP-el melalui mekanisme kriptografi yang diimplementasikan dalam Kartu SAM KTP-el atau mekanisme kriptograsi lainnya yang ditetapkan oleh Ditjen Dukcapil;
4. memastikan keabsahan kepemilikan KTP-el dengan memanfaatkan autentikasi diri yang memastikan kebenaran kepemilikan dokumen kependudukan KTP-el dengan metode verifikasi Sidik Jari dan/atau verifikasi wajah secara elektronik dan mekanisme kriptografi yang

diimplementasikan dalam Kartu SAM KTP-el atau mekanisme kriptograsi lainnya yang ditetapkan oleh Ditjen Dukcapil;

5. memastikan bahwa data Penduduk dari cip KTP-el dapat diakses dan ditampilkan untuk kepentingan pelayanan administrasi pemerintahan dan pelayanan publik melalui jalur/mekanisme yang teramankan sesuai kaidah/standar keamanan teknologi informasi dan komunikasi.

Pengguna yang menggunakan *card reader* KTP-el untuk pelayanan publik akan memanfaatkan fungsi – fungsi yang tersedia di *card reader* KTP-el tersebut.

Fungsi – fungsi yang tersedia di *card reader* sesuai dengan Permendagri No. 102 Tahun 2019 tentang Pemberian Hak Akses dan Pemanfaatan Data Kependudukan, dalam pasal 26, dimana tujuan penyediaan setiap unit pelayanan publik dalam menyediakan *card reader KTP-el* adalah untuk:

a. mendeteksi keaslian KTP-el untuk mencegah kejahatan akibat pemalsuan KTP-el; dan
b. melakukan verifikasi dan validasi kepemilikan KTP-el untuk mencegah penyalahgunaan KTP-el yang bukan miliknya.

Verifikasi dan validasi kepemilikan KTP-el dilakukan oleh *card reader* KTP-el dengan verifikasi Sidik Jari secara elektronik.

Dalam hal pemanfaatan operasional lapangan terkait dengan kebutuhan pelayanan publik secara masal yang membutuhkan waktu yang cepat, atau kebutuhan pelayanan publik secara masal pada kondisi khusus tertentu, dimana pemanfaatan fungsi verifikasi Sidik Jari dan/atau verifikasi lainnya secara elektronik kurang optimal untuk dilaksanakan, maka verifikasi dan validasi kepemilikan KTP-el dapat dilakukan secara visual oleh petugas dengan memanfaatkan tampilan foto wajah, yang diakses *card reader* secara aman dari dalam cip KTP-el. Foto wajah yang tersimpan di dalam cip KTP-el lebih aman dan lebih "*tamper resistant*" dibandingkan dengan foto wajah yang tercetak di permukaan KTP-el.

Pada saat situasi kebutuhan pelayanan secara masal kembali ke kondisi normal, maka dapat kembali menggunakan verifikasi secara elektronik yang disediakan sesuai tingkatan *Card Reader*-nya.

Hal tersebut dituangkan dalam suatu dokumen kajian risiko keamanan penggunaan Perangkat Pembaca KTP-el (*Card Reader*) dan petunjuk

operasional lapangan dari Pengguna yang mana proses penyusunan dan *proof of concept* berkoordinasi dengan Ditjen Dukcapil Kemendagri.

Kartu *Secure Access Module* (SAM) dan/atau Kode Kunci

KTP-el dilengkapi dengan cip yang menyimpan biodata, pas photo, tanda tangan dan Sidik Jari Penduduk yang bersangkutan. Cip pada KTP-el dilindungi dengan teknik keamanan informasi melalui *Secure Access Module* (SAM) dan/atau Kode Kunci untuk dapat membaca rekaman biodata, pas photo, tanda tangan dan Sidik Jari Penduduk atau data lainnya sesuai perkembangan inovasi penyimpanan data pada cip KTP-el.

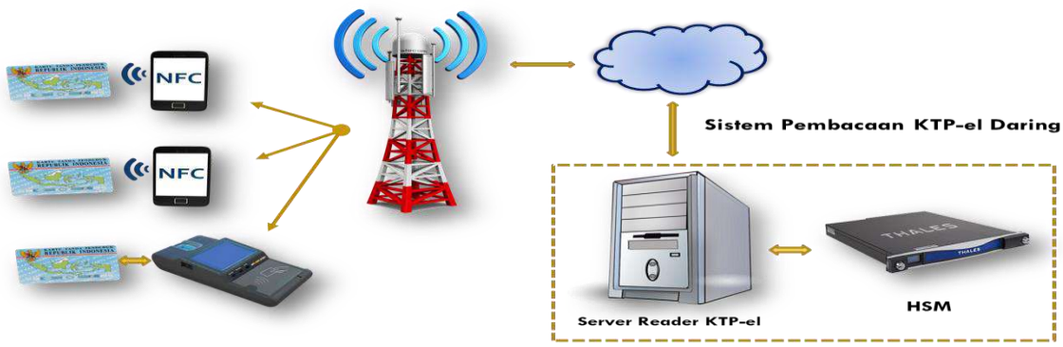
Dalam rangka pembacaan KTP-el oleh perangkat pembaca, KTP-el tidak perlu disisipkan atau digesekkan ke dalam suatu slot dari perangkat pembaca. Hal ini dikarenakan teknologi cip pada KTP-el berbasis kartu cerdas (*smart card*) bertipe nirkontak (*contactless chip)*, yaitu cip *smart card* yang mampu berkomunikasi dengan perangkat pembaca (*card reader*) tanpa harus kontak langsung secara fisik melainkan menggunakan gelombang radio dengan frekuensi 13,56 MHz, sesuai dengan standar nasional/internasional, seperti SNI ISO/IEC 14443 dan standar internasional lainnya yang mengatur keamanan teknologi/informasi. Dalam pemenuhan standar tersebut, Kementerian melalui Ditjen melibatkan lembaga pemerintah nonkementerian yang memiliki tugas dan fungsi pengkajian dan penerapan teknologi dan lembaga pemerintah nonkementerian yang memiliki tugas dan fungsi keamanan siber dan sandi negara.

Untuk dapat melakukan pembacaan dan/atau penulisan KTP-el melalui perangkat Pembaca KTP-el, perangkat pembaca tersebut harus dilengkapi dengan *Secure Access Module* (SAM) dan/atau Kode Kunci. SAM dan/atau Kode Kunci tersebut disediakan oleh Satuan Kerja Pelaksana dan/atau Pengguna dengan mengacu pada spesifikasi teknis yang telah ditetapkan oleh Kementerian Dalam Negeri. Kemudian setelah SAM dan/atau Kode Kunci tersebut tersedia, Satuan Kerja Pelaksana dan/atau Pengguna mengajukan permohonan agar SAM dipersonalisasi dan/atau Kode Kunci tersebut diberikan oleh Kementerian Dalam Negeri melalui sistem informasi berbasis aplikasi *file management* (SIFILMA). Kementerian Dalam Negeri kemudian akan melakukan verifikasi terhadap SAM dan/atau kode yang diajukan untuk dipersonalisasi dan/atau diaktivasi apakah sesuai dengan

spesifikasi teknis yang telah ditetapkan dan mempertimbangkan permohonan pengajuan Personalisasi tersebut. SAM yang telah dipersonalisasi dan/atau Kode Kunci yang telah diaktivasi kemudian dapat digunakan oleh *Card Encoder* dan/atau *Card Reader* untuk melakukan penulisan dan/atau pembacaan secara teramankan terhadap cip KTP-el.

Pengguna yang menggunakan Perangkat Pembaca KTP-el terintegrasi untuk pelayanan administrasi pemerintahan dan/atau pelayanan publik, dapat memanfaatkan data hasil pembacaan data dari cip KTP-el melalui Perangkat Pembaca (*Card Reader*) KTP-el untuk disimpan di sistem informasi Pengguna dalam rangka kebutuhan pemrosesan data lebih lanjut. Khusus data Sidik Jari Penduduk, pemanfaatan hanya dipergunakan untuk kepentingan verifikasi (pencocokan) Sidik Jari secara elektronik oleh Perangkat Pembaca KTP-el (*Card Reader*), sehingga data Sidik Jari tidak boleh disimpan di sistem informasi Pengguna.

Selanjutnya, penggunaan Kartu SAM dan/atau Kode Kunci dapat dioperasionalkan ke depan melalui jaringan komunikasi data secara tertutup dan/atau terbuka sesuai yang diatur di dalam batang tubuh Peraturan Menteri ini.



Gambar 3. Ilustrasi *Secure Access Module* dan/atau Kode Kunci Dalam Jaringan KTP-el (SAM *Online* KTP-el)

Berdasarkan gambar di atas, dijelaskan beberapa hal sebagai berikut:

1. *card encoder* dan/atau *card reader* digantikan oleh sebuah *server encoder/reader* KTP-el daring;
2. server *encoder/reader* KTP-el daring terhubung dengan KTP-el melalui *encoder/reader smartcard*;
3. bisa dihubungkan dengan banyak (multi) SAM melalui banyak (*multi*) *reader smartcard*;
4. aplikasi NFC di *smartphone* hanya berfungsi sebagai *proxy* untuk pembacaan Kartu KTP-el;
5. otentikasi dan verifikasi Pengguna KTP-el melalui *fingerprint*, *face recognition* atau data lainnya yang tersimpan dalam memori KTP-el.

Pengujian Teknis dan Sertifikasi

Bagi pengembang dan/atau industri nasional yang berencana untuk mengembangkan produk *Card Encoder* dan/atau *Card Reader*, akan memerlukan informasi dan akses terhadap mekanisme pembacaan cip KTP-el. Dalam rangka melindungi keamanan transaksi dan komunikasi dengan KTP-el, Kementerian berwenang untuk menetapkan kebijakan tentang pemanfaatan terhadap mekanisme pembacaan cip KTP-el.

Lembaga pengujian teknis akan menindaklanjuti kebijakan tersebut dengan suatu kebijakan dan prosedur teknis dalam rangka memberikan asistansi atau dukungan teknis kepada pengembang dan/atau industri nasional agar dapat mengembangkan produk *Card Encoder* dan/atau *Card Reader* dengan tetap mempertimbangkan aspek keamanan KTP-el. Pengembang dan/atau industri nasional dengan kualifikasi kemampuan

teknis tertentu, serta yang bersedia untuk menandatangani perjanjian kerahasiaan terhadap perlindungan mekanisme penulisan dan/atau pembacaan cip KTP-el atau perjanjian *Non Disclosure Agreement* (NDA) dengan lembaga pengujian teknis, akan diberikan asistansi implementasi mekanisme penulisan dan/atau pembacaan cip KTP-el pada produk *Card Encoder* dan/atau *Card Reader*.

Pengujian teknologi perlu dilakukan terhadap Perangkat Pembaca KTP-el dalam rangka verifikasi kesesuaian terhadap spesifikasi teknis serta verifikasi fungsionalitas dan kinerja Perangkat Pembaca KTP-el. Perangkat pembaca KTP-el yang telah lulus dari pengujian teknologi adalah perangkat yang layak untuk digunakan oleh Pengguna.

Pengadaan Perangkat Pembaca KTP-el memprioritaskan produksi dalam negeri sesuai dengan ketentuan yang berlaku dalam bentuk sertifikat Tingkat Komponen Dalam Negeri (TKDN). Sertifikat Tingkat Komponen Dalam Negeri (TKDN) mengacu pada ketentuan peraturan perundang-undangan yang berlaku.

Integrasi *Card Reader KTP-el* dengan Card Reader Multi Kartu

Seiring dengan kemajuan teknologi, perangkat pembaca kartu cerdas (kartu dengan cip) dapat mengoperasikan lebih dari satu aplikasi pembaca kartu dalam rangka pembacaan beberapa kartu cerdas secara aman (perangkat pembaca multi kartu cerdas). Dengan demikian, dalam operasional lapangan, satu perangkat pembaca kartu cerdas dapat difungsikan untuk membaca beberapa kartu cerdas. Salah satu latar belakang kebutuhan untuk sharing satu perangkat adalah dalam rangka efisiensi dan efektifitas. Seiring dengan kemajuan teknologi, *card reader* dapat terintegrasi dalam suatu perangkat pembaca multi kartu cerdas, dengan instalasi aplikasi pembaca KTP-el dan aplikasi pembaca kartu lainnya pada satu perangkat komputasi secara aman. Masing – masing aplikasi pembaca beroperasi dan berfungsi secara aman dengan dilindungi oleh SAM dan/atau Kode Kunci yang terkait. SAM KTP-el berupa kartu SAM, sedangkan SAM kartu lain disesuaikan dengan persyaratan keamanan kartu lain tersebut. Sebagai ilustrasi operasional di lapangan, *Card Reader* KTP-el yang telah terintegrasi dengan *card reader* multi kartu, digunakan dalam membaca kartu KTP-el dan kartu lain, semisal, kartu perbankan atau kartu kepesertaan suatu lembaga.

KTP-el Multiguna dengan *Card Reader* Multi Kartu

Seiring dengan kemajuan teknologi dan peningkatkan kapasitas memori dan fitur kartu KTP-el, fungsi dari KTP-el secara bertahap dapat ditingkatkan dengan menambahkan data dan/atau aplikasi di cip KTP-el. Ruang memori di dalam satu cip dapat dipartisi secara aman untuk penyimpanan data dan/atau aplikasi dari pemilik data dan/atau aplikasi yang berlainan. Data perorangan pada cip KTP-el dapat disesuaikan dan /atau ditambahkan, baik berupa data dari *database* kependudukan nasional, Data Balikan, maupun data dari instansi mitra pemanfaat cip KTP-el, secara aman sesuai dengan persyaratan keamanan. Hal tersebut berlaku pula untuk penambahan aplikasi KTP-el maupun aplikasi dari instansi mitra pemanfaat cip KTP-el.

Pembacaan data dan/atau aplikasi dari cip KTP-el yang telah berisi data KTP-el dan data dan/atau aplikasi lain dilakukan oleh suatu *Card Reader* yang dilengkapi dengan SAM terkait. Bila pembacaan dilakukan terhadap data KTP-el maka SAM terkait adalah SAM dan/atau Kode Kunci KTP-el, bila pembacaan dilakukan terhadap data lain di cip KTP-el, maka dilakukan oleh SAM dan/atau Kode Kunci terkait data tersebut. Ketentuan mengenai masing – masing SAM mengacu pada persyaratan Keamanan Teknologi Informasi.

Referensi terkait penambahan fungsi KTP-el dan penyesuaian dan/atau penambahan data adalah pada penjelasan pasal 64 ayat (6) dari Undang-Undang No. 24 Tahun 2013 tentang Perubahan atas Undang-Undang No. 23 Tahun 2006 tentang Administrasi Kependudukan, dimana Pasal 64 ayat (6) disebutkan bahwa dalam KTP-el sebagaimana dimaksud pada ayat (1) tersimpan cip yang memuat rekaman elektronik data perseorangan.

Penjelasan Pasal 64 ayat (6) sebagai berikut:

a. Fungsi KTP-el ditingkatkan secara bertahap menjadi KTP-el multiguna.
b. Data perseorangan yang dimuat dalam cip akan disesuaikan dengan kebutuhan.

*Card reade*r KTP-el dengan Bentuk Perangkat (*Form Factor*) Tertentu

Seiring dengan kemajuan teknologi, bentuk dari perangkat pembaca kartu cerdas dapat pula berupa perangkat telepon pintar (*smart phone*), komputer tablet, dan lain lain. Telepon pintar dengan teknologi *Near Field Communication* (NFC) dapat berfungsi untuk membaca kartu KTP-el dengan

suatu metode pengamanan berupa SAM atau berupa aplikasi, sesuai dengan persyaratan keamanan teknologi informasi.

Pengelolaan SAM dan/atau Kode Kunci KTP-el dan SAM dan/atau Kode Kunci Data/Aplikasi Lain di KTP-el Multiguna

Seiring dengan kemajuan teknologi dan peningkatan fungsi KTP-el secara bertahap dengan peningkatan memori dan fitur pada cip KTP-el, cip KTP-el akan memuat data perorangan tambahan dari data KTP-el saat ini maupun sebagai data tambahan dari Instansi mitra/Pengguna pemanfaat cip KTP-el. Selain itu cip KTP-el juga akan memuat aplikasi tambahan. Setiap data dan aplikasi akan memiliki SAM dan/atau Kode Kunci dan persyaratan keamanan tertentu dengan suatu standar keamanan teknologi informasi yang berlaku. Maka diperlukan mekanisme dan prosedur pengelolaan kunci keamanan aplikasi dan/atau SAM dan/atau Kode Kunci dari masing – masing data/aplikasi di dalam cip KTP-el.

MENTERI DALAM NEGERI
REPUBLIK INDONESIA,

ttd

MUHAMMAD TITO KARNAVIAN

Salinan sesuai dengan aslinya
Kepala Biro Hukum,

R. Gani Muhamad, SH, MAP
Pembina Utama Muda (IV/c)
NIP 19690818 199603 1001