PEKELILING KEMAJUAN PENTADBIRAN AWAM
BILANGAN 3 TAHUN 2015

DASAR PERKHIDMATAN
PRASARANA KUNCI AWAM KERAJAAN
[GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)]

JABATAN PERDANA MENTERI
MALAYSIA
23 OKTOBER 2015

Diedarkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN
62502 PUTRAJAYA

No. Tel. : 03-8000 8000
No. Faks: 03-8888 3721

Ruj. Kami: MAMPU.600–1/3/4 (4)
Tarikh: 23 Oktober 2015

Semua Ketua Setiausaha Kementerian

Semua Ketua Jabatan Persekutuan

Semua Setiausaha Kerajaan Negeri

Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri

Semua Pihak Berkuasa Tempatan

PEKELILING KEMAJUAN PENTADBIRAN AWAM
BILANGAN 3 TAHUN 2015

DASAR PERKHIDMATAN
PRASARANA KUNCI AWAM KERAJAAN
[GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)]

TUJUAN

Pekeliling Kemajuan Pentadbiran Awam ini bertujuan untuk menjelaskan kepada ketua-ketua jabatan kerajaan mengenai dasar perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)] bagi memantapkan tahap keselamatan data dan maklumat sistem teknologi maklumat dan komunikasi (ICT) kerajaan dalam menyokong inisiatif perkhidmatan digital kerajaan.

LATAR BELAKANG

2. Prasarana Kunci Awam [Public Key Infrastructure (PKI)] ialah gabungan perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi memastikan data dan maklumat transaksi urus niaga secara dalam talian selamat. Prasarana Kunci Awam (PKI) membolehkan data serta maklumat dilindungi dari aspek kerahsiaan, integriti dan kebolehsediaan. Sebarang transaksi atau aktiviti terhadap data dan maklumat tidak boleh disangkal melalui pengesahan jejak audit.

3. Selaras dengan Akta Tandatangan Digital 1997 dan Peraturan-Peraturan Tandatangan Digital 1998, Prasarana Kunci Awam (PKI) telah mula dilaksanakan pada tahun 2002 dalam pelaksanaan projek-projek Kerajaan Elektronik (EG). Bagi menyelaras pelaksanaan Prasarana Kunci Awam (PKI) di agensi sektor awam, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri (JPM) telah menyediakan perkhidmatan Prasarana Kunci Awam (PKI) secara berpusat yang dikenali sebagai perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI).

PELAKSANAAN

4. Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) diurus tadbir dan dipantau pelaksanaannya oleh Jawatankuasa Pelaksanaan Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI).

5. Semua sistem ICT kerajaan yang memerlukan kemudahan Prasarana Kunci Awam (PKI) hendaklah menggunakan perkhidmatan

Prasarana Kunci Awam Kerajaan (GPKI). Pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI) ini berpandukan kepada **Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)]** seperti dalam Lampiran. Dasar ini menjelaskan kaedah kepada agensi dalam pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI) di sektor awam yang melibatkan dua aspek utama, iaitu:

(i) Kaedah pelaksanaan teknikal bagi aspek penggunaan sijil digital yang merangkumi tatacara pelaksanaan penilaian risiko, panduan penentuan penggunaan sijil digital dan keperluan teknikal; dan

(ii) Tadbir urus dan tatacara operasi merangkumi aspek pengurusan, pengendalian dan pelaksanaan operasi Prasarana Kunci Awam Kerajaan (GPKI) di semua peringkat pelaksanaan termasuk pengeluaran sijil digital.

PEMAKAIAN

6. Pekeliling ini terpakai kepada semua Kementerian, Jabatan Persekutuan, Pejabat Setiausaha Kerajaan Negeri, Badan Berkanun dan Pihak Berkuasa Tempatan. Pemakaian pekeliling ini tertakluk pada penerimaan oleh pihak berkuasa masing-masing.

TARIKH BERKUAT KUASA

7. Pekeliling ini berkuat kuasa mulai tarikh pekeliling dikeluarkan.

PERTANYAAN

8. Sebarang pertanyaan mengenai pekeliling ini boleh dikemukakan kepada:

Unit Pemodenan Tadbiran dan Perancangan Pengurusan
Malaysia (MAMPU)
Jabatan Perdana Menteri
Aras 5, Blok B2
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
No. Telefon : 03 - 8000 8000
No. Faksimile : 03 - 8000 8001
E-mel : gpki@mampu.gov.my

"**BERKHIDMAT UNTUK NEGARA**"

TAN SRI DR. ALI HAMSA
Ketua Setiausaha Negara

Lampiran Pekeliling Kemajuan Pentadbiran Awam

Bilangan 3 Tahun 2015

DASAR PERKHIDMATAN
PRASARANA KUNCI AWAM KERAJAAN
[GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)]

KANDUNGAN

TUJUAN

Dasar ini bertujuan untuk menjelaskan Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)] kepada agensi sektor awam bagi memantapkan tahap keselamatan data dan maklumat bagi sistem teknologi maklumat dan komunikasi (ICT) kerajaan.

LATAR BELAKANG

2. Perkhidmatan Prasarana Kunci Awam Kerajaan merupakan salah satu perkhidmatan keselamatan ICT bagi memantapkan tahap keselamatan data dan maklumat bagi sistem ICT kerajaan. Selaras dengan Akta Tandatangan Digital 1997 dan Peraturan-peraturan Tandatangan Digital 1998, perkhidmatan ini merangkumi tiga tujuan penggunaan, iaitu pengesahan identiti (identity authentication), tidak boleh disangkal (non-repudiation) melalui tandatangan digital (digital signature) dan penyulitan maklumat (information encryption).

3. Dalam konteks perkhidmatan awam Malaysia, Prasarana Kunci Awam Kerajaan (GPKI) yang digunakan dalam pelaksanaan projek-projek Kerajaan Elektronik (EG) sejak tahun 2002 adalah untuk memastikan keselamatan data dan maklumat, selaras dengan Akta Tandatangan Digital 1997. Sejak pelaksanaan pada tahun 2002, Prasarana Kunci Awam Kerajaan (GPKI) telah digunakan dengan lebih meluas dalam pelbagai sistem ICT kerajaan. Walau bagaimanapun, pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI) terbahagi kepada dua pendekatan, iaitu secara berpusat di Unit Pemodenan Tadbiran dan

Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri (JPM) dan atas inisiatif berasingan di agensi sektor awam.

4. Selaras dengan itu, Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan ini digubal berserta dengan dua garis panduan, iaitu Garis Panduan Operasi Perkhidmatan Prasarana Kunci Awam Kerajaan dan Garis Panduan Teknikal Perkhidmatan Prasarana Kunci Awam Kerajaan. Dasar ini hendaklah dibaca bersekali dengan kedua-dua garis panduan tersebut supaya dapat membantu agensi dalam pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI).

TAKRIFAN

5. Takrifan yang digunakan dalam dasar ini adalah seperti yang berikut:

(i) **Prasarana Kunci Awam [Public Key Infrastructure (PKI)]** ialah satu set perkakasan, perisian, individu, teknologi, polisi, dan tatacara yang perlu bagi mencipta, mengurus, mengedar, mengguna, menyimpan dan membatalkan pemerakuan digital;

(ii) **Portal GPKI** ialah laman web yang menyampaikan maklumat mengenai perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) dan juga menyediakan kemudahan perkhidmatan dalam talian pemohonan sijil digital kepada pejawat awam. Portal ini boleh dicapai melalui URL https://gpki.mampu.gov.my;

(iii) **Agensi sektor awam** ialah agensi yang merangkumi Kementerian, Jabatan Persekutuan, Badan Berkanun Persekutuan, Kerajaan Negeri, Badan Berkanun Negeri dan Pihak Berkuasa Tempatan;

(iv) **Agensi pusat** ialah agensi sektor awam yang bertanggungjawab untuk menyelaras dan memantau pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI) secara keseluruhan serta memberikan khidmat nasihat bagi penggunaan teknologi Prasarana Kunci Awam (PKI) bagi sistem ICT kerajaan dan mentadbir Portal GPKI;

(v) **Agensi pelaksana** ialah agensi sektor awam yang memiliki aplikasi dan bertanggungjawab mengurus, menyelaras dan mentadbir sistem aplikasi yang menggunakan perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI);

(vi) **Pihak Berkuasa Pemerakuan Berlesen [Licensed Certification Authority (CA)]** ialah pihak yang bertanggungjawab mengeluarkan sijil digital yang sah berdasarkan Akta Tandatangan Digital 1997 dan Peraturan-Peraturan Tandatangan Digital 1998;

(vii) **Pihak Berkuasa Pendaftaran [Registration Authority (RA)]** ialah pihak yang dilantik oleh Pihak Berkuasa Pemerakuan Berlesen (CA) bagi menjalankan kerja semakan permohonan dan mengesahkan pengeluaran sijil digital sebelum dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA);

(viii) **Pentadbir Portal GPKI** ialah Pentadbir (Admin*)*, Subpentadbir (Sub Admin*)* dan Pegawai Diberi kuasa (Authorised Personnel*)*;

(ix) **Pentadbir (Admin)** ialah pegawai di agensi pusat yang menguruskan perkhidmatan GPKI dan mentadbir Portal GPKI serta melantik dan mengurus Subpentadbir (Sub Admin)*;*

(x) **Subpentadbir (SA)** ialah pegawai di agensi pelaksana yang dilantik untuk mengurus pelantikan dan permohonan Pegawai Diberi Kuasa (Authorised Personnel*)*;

(xi) **Pegawai Diberi Kuasa (AP)** ialah pegawai di agensi sektor awam yang dilantik bagi mengenal pasti dan mengurus permohonan pengguna di agensi masing-masing;

(xii) **Pentadbir Pelayan (PS)** ialah pegawai agensi pelaksana yang mentadbir pelayan yang mengandungi sistem ICT kerajaan;

(xiii) **Sijil digital** ialah sijil yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) untuk mengesahkan tanpa penafian identiti pengguna atau pelayan;

(xiv) **Sijil digital pengguna** ialah sijil yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) yang mengandungi maklumat berkenaan dengan identiti pelanggan dan kunci persendirian pelanggan dan ditandatangani pelanggan;

(xv) **Sijil digital pelayan** ialah sijil yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) untuk mengesahkan identiti organisasi kepada pengguna supaya maklumat transaksi dihantar tanpa masalah pemintasan data semasa transaksi dilakukan, data penggodaman, atau pemalsuan mesej. Sijil digital dimuatkan dalam pelayan di agensi pelaksana untuk mengesahkan identiti organisasi kepada pengguna bagi memastikan keselamatan data dan maklumat sistem aplikasi supaya maklumat transaksi dihantar tanpa masalah pemintasan data semasa transaksi dilakukan, data penggodaman, atau pemalsuan mesej. Protokol Lapisan Soket Selamat (SSL) digunakan untuk menyulitkan maklumat yang dihantar melalui internet. Sijil digital pelayan SSL membolehkan pelayan web mewujudkan sesi SSL dengan pelayar web;

(xvi) **Medium sijil digital** ialah perkakasan atau perisian yang digunakan untuk menyimpan sijil digital pengguna. Beberapa medium yang digunakan adalah seperti yang berikut:

(a) **Kad Pintar**, iaitu kad yang mengandungi cip kriptografi untuk menyimpan sijil digital bagi melaksanakan fungsi Prasarana Kunci Awam (PKI). Kad ini dihubungkan kepada komputer pengguna mengunakan pembaca kad pintar;

(b) **Token**, iaitu sebuah perkakasan yang mengandungi cip kriptografi untuk menyimpan sijil digital bagi melaksanakan fungsi Prasarana Kunci Awam (PKI). Perkakasan ini

berbentuk seperti pemacu mudah alih dan dihubungkan kepada komputer pengguna mengunakan port USB; dan

(c) **Sijil Perisian [software certificate (softcert)]** yang terdiri daripada:

(1) **Sijil digital muat turun (download certificate)**, iaitu fail yang mengandungi sijil digital, kunci peribadi (private key) bagi pengesahan identiti, penyulitan data dan tandatangan digital. Sijil digital yang dijana boleh dimuat turun ke medium storan perkakasan pengguna dan lokasi sijil digital tidak tertakluk pada satu-satu komputer; dan

(2) **Sijil digital perayauan (roaming certificate)**, iaitu fail yang mengandungi sijil digital, kunci peribadi (private key) bagi pengesahan identiti, penyulitan data dan tandatangan digital. Sijil digital disimpan dalam pelayan yang berpusat di lokasi Pihak Berkuasa Pemerakuan Berlesen (CA).

(xvii) **Sistem ICT kerajaan** ialah sistem yang merangkumi perkakasan, perisian, aplikasi, data, pengguna dan rangkaian dalam kerajaan;

(xviii) **Lapisan soket selamat [Secure Socket Layer (SSL)]** ialah protokol rangkaian yang menguruskan pensahihan pelayan dan pengguna, dan komunikasi berenkripsi antara pelayan

dan pengguna. Terdapat beberapa produk sijil SSL seperti yang berikut:

(a) Sijil digital pelayan tunggal sebagaimana yang ditawarkan sekarang;

(b) Sijil digital kad bebas (wild card);

(c) Sijil digital pengesahsahihan yang diperluas (extended validation certificate);

(d) Sijil digital komunikasi dipersatukan (unified communications certificate); dan

(e) Sijil digital pengesahsahihan yang diperluas bagi pelbagai domain (extended validation multi-domain certificate).

(xix) **Antara Muka Pengaturcaraan Aplikasi [Application Programming Interface (API)]** ialah perisian yang dibangunkan untuk tujuan mengintegrasikan Prasarana Kunci Awam Kerajaan (GPKI) dengan sistem ICT kerajaan.

PERNYATAAN DASAR

6. Pernyataan Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) ialah:

“Semua sistem ICT kerajaan yang memerlukan kemudahan Prasarana Kunci Awam (PKI) hendaklah menggunakan Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI).”

TADBIR URUS PERKHIDMATAN GPKI

7. Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) diurustadbirkan dan dipantau pelaksanaannya oleh **Jawatankuasa Pelaksanaan Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI)**.

8. Terma Rujukan **Jawatankuasa Pelaksanaan Perkhidmatan GPKI** adalah seperti yang berikut:

(i) Menentukan hala tuju dan strategi pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI);

(ii) Memantau status pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI) secara menyeluruh;

(iii) Menimbang dan meluluskan cadangan penguatkuasaan dasar; dan

(iv) Menyelesaikan isu-isu dasar yang berkaitan dengan Prasarana Kunci Awam Kerajaan (GPKI).

PERKHIDMATAN GPKI

9. Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) yang disediakan oleh agensi pusat merangkumi:

(i) Pengurusan sijil digital yang merangkumi penyelarasan dengan Pihak Berkuasa Pemerakuan Berlesen (CA) bagi proses permohonan baharu, pembaharuan dan pembatalan sijil digital; dan

(ii) Khidmat nasihat serta konsultasi bagi perancangan dan pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI).

PELAKSANAAN GPKI

10. Pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI) sektor awam melibatkan dua aspek utama, iaitu pengeluaran sijil digital dan penggunaan sijil digital. Sehubungan dengan itu, agensi hendaklah merujuk dan mematuhi dokumen yang berikut:

(i) **Garis Panduan Teknikal Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI)** seperti **LAMPIRAN I**. Garis panduan ini menerangkan kaedah pelaksanaan teknikal bagi aspek penggunaan sijil digital yang merangkumi tatacara pelaksanaan penilaian risiko, panduan penentuan penggunaan sijil digital dan keperluan teknikal; dan

(ii) **Garis Panduan Operasi Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI)** seperti **LAMPIRAN II**. Garis Panduan

ini menerangkan tadbir urus dan tatacara operasi merangkumi aspek pengurusan, pengendalian dan pelaksanaan operasi Prasarana Kunci Awam Kerajaan (GPKI) pada semua peringkat pelaksanaan termasuk pengeluaran sijil digital.

FAEDAH PERLINDUNGAN GPKI

11. Faedah yang diperoleh dalam mengguna pakai perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) ialah perlindungan keselamatan data dan maklumat sistem ICT kerajaan. Secara umumnya Prasarana Kunci Awam Kerajaan (GPKI) ialah satu kawalan keselamatan yang sesuai untuk memenuhi keperluan yang berikut:

(i) **Kerahsiaan (confidentiality)**, iaitu mengekalkan sekatan terhadap akses dan pendedahan maklumat yang diizinkan. Hilang kerahsiaan bererti pendedahan maklumat tanpa izin;

(ii) **Pengesahan identiti (identity authentication),** iaitu mengesahkan pengenalan identiti pengguna, peranti atau pelayan sebelum mendapat akses kepada aplikasi agensi sektor awam;

(iii) **Integriti (integrity)**, iaitu kawalan terhadap pengubahsuaian dan penghapusan maklumat yang tidak teratur, kesilapan dan maklumat tertinggal. Pendedahan dan/atau pengubahsuaian maklumat yang tidak diizinkan bererti tiada integrity; dan

(iv) **Tidak boleh disangkal (non-repudiation),** iaitu keperluan bagi membuktikan integriti dan punca data boleh disahkan daripada penafian penglibatan tindakan sebelumnya.

PRINSIP PEGANGAN PELAKSANAAN GPKI

12. Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) menawarkan sijil digital dalam pelbagai medium yang dikeluarkan oleh beberapa Pihak Berkuasa Pemerakuan Berlesen (CA) di Malaysia. Sistem ICT kerajaan yang menggunakan sijil digital perlu mematuhi prinsip pegangan pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI) yang berikut:

(i) Semua aplikasi yang menggunakan Prasarana Kunci Awam (PKI) yang merentas agensi mestilah membenarkan penggunaan pelbagai medium sijil digital selaras dengan tahap keselamatan aplikasi tersebut;

(ii) Setiap penjawat awam hanya dibenarkan menggunakan satu sijil digital sahaja;

(iii) Pemegang sijil digital yang mempunyai capaian kepada pelbagai aplikasi yang mempunyai tahap kawalan keselamatan yang berbeza hendaklah menggunakan medium sijil digital yang boleh mencapai aplikasi yang mempunyai tahap kawalan keselamatan yang tertinggi;

(iv) Sistem ICT kerajaan yang menggunakan perkhidmatan PKI selain perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI)

mestilah beralih kepada perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) apabila sistem berkenaan hendak dinaik taraf atau tempoh kontrak sistem berkenaan telah tamat;

(v) Agensi pelaksana yang membangunkan sistem ICT kerajaan perlu memastikan sistem berkenaan boleh menyokong mana-mana medium sijil digital perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) yang sedang berkuat kuasa;

(vi) Agensi sektor awam perlu mengambil kira keperluan sijil digital pelayan dalam spesifikasi sistem baharu;

(vii) Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) hanya akan membekalkan sijil digital pelayan untuk tujuan pembaharuan sijil digital pelayan sedia ada yang akan tamat tempoh. Kos sijil digital pelayan dalam sistem baharu adalah di bawah tanggungan agensi berkenaan dengan menggunakan sijil yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) yang dilantik oleh kerajaan menerusi Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM);

(viii) Pemegang sijil digital pengguna perlu memaklumkan atau memulangkan, medium sijil digital yang rosak, tamat tempoh, tamat perkhidmatan, bersara atau disalahgunakan kepada agensi pusat menerusi Pegawai Diberi Kuasa (AP);

(ix) Agensi pusat menanggung semua kos bagi perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) untuk kementerian dan jabatan persekutuan yang bertindak sebagai agensi pelaksana dan semua pengguna aplikasi agensi pelaksana ini;

(x) Kos perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) bagi Badan Berkanun Persekutuan, agensi negeri, Badan Berkanun Negeri dan Pihak Berkuasa Tempatan yang berhasrat untuk bertindak sebagai agensi pelaksana dan semua pengguna aplikasi agensi ini adalah di bawah tanggungan agensi masing-masing; dan

(xi) Agensi pelaksana yang berubah taraf daripada agensi persekutuan kepada agensi swasta atau badan berkanun, kos perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) bagi penggantian medium sijil digital, permohonan sijil digital baharu, naik taraf Antara Muka Pengaturcaraan Aplikasi (API) dan integrasi serta sokongan teknikal adalah di bawah tanggungan agensi berkenaan.

PENGECUALIAN

13. Agensi pelaksana yang masih dalam kontrak perkhidmatan Prasarana Kunci Awam (PKI) selain perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) dikecualikan daripada kos berkenaan. Agensi pelaksana hendaklah menggunakan perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) selepas tamat tempoh kontrak perkhidmatan Prasarana Kunci Awam (PKI).

PINDAAN DAN KEMAS KINI

14. Garis panduan ini adalah tertakluk pada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial.

PENUTUP

15. Agensi hendaklah mematuhi garis panduan ini dalam melaksanakan Prasarana Kunci Awam Kerajaan (GPKI) di agensi masing-masing.

LAMPIRAN I

GARIS PANDUAN TEKNIKAL
PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN
[GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)]

KANDUNGAN

SENARAI RAJAH

SENARAI JADUAL

SENARAI LAMPIRAN

TUJUAN

Garis Panduan Teknikal Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)] ini bertujuan untuk menerangkan kaedah pelaksanaan teknikal bagi aspek penggunaan sijil digital yang merangkumi kaedah penilaian risiko, panduan penentuan penggunaan sijil digital dan keperluan teknikal khususnya bagi:

(i) Membantu agensi membuat penilaian kendiri keperluan Prasarana Kunci Awam [Public Key Infrastructure (PKI)] dalam pelaksanaan sistem ICT kerajaan; dan

(ii) Menjelaskan kaedah pelaksanaan teknikal dalam penggunaan Prasarana Kunci Awam (PKI) yang merangkumi aspek pengesahan identiti, tandatangan digital dan penyulitan maklumat.

SKOP

2. Selaras dengan tujuan dokumen ini, garis panduan teknikal memberikan tumpuan kepada perkara yang perlu dilaksanakan oleh agensi mengikut turutan yang berikut:

(i) Menilai tahap risiko sistem ICT kerajaan untuk mengenal pasti kawalan keselamatan yang sesuai bagi keperluan perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI);

(ii) Menentukan penggunaan sijil digital sama ada bagi tujuan pengesahan identiti, tandatangan digital dan/atau penyulitan maklumat; dan

(iii) Menggariskan keperluan teknikal Prasarana Kunci Awam (PKI) dari segi piawaian, keperluan integrasi dan keperluan khusus bagi Sijil Perisian (softcert).

KUMPULAN SASARAN

3. Kumpulan sasaran garis panduan ini ialah agensi pelaksana khususnya yang terlibat dalam pembangunan sistem ICT kerajaan yang memerlukan kawalan keselamatan maklumat dan data dari segi pengesahan identiti, tidak boleh disangkal melalui tandatangan digital dan penyulitan maklumat.

PENILAIAN RISIKO DALAM KONTEKS PELAKSANAAN GPKI

4. Dalam konteks pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI), penilaian risiko adalah untuk mengenal pasti langkah-langkah kawalan yang boleh menangani risiko berkaitan kerahsiaan, pengesahan identiti, integriti dan tidak boleh disangkal terhadap fungsi teras agensi. Secara umumnya, langkah kawalan yang diguna pakai ialah Prasarana Kunci Awam Kerajaan (GPKI). Mengikut amalan terbaik, agensi hendaklah melaksanakan penilaian risiko pada peringkat awal pembangunan sistem ICT iaitu semasa fasa kajian keperluan sistem. Namun begitu, pelaksanaan penilaian ini boleh dilakukan mengikut keperluan agensi. Tatacara dan laporan penilaian risiko dijelaskan seperti yang berikut:

(i) Proses penilaian risiko terhadap fungsi teras agensi yang disokong oleh sistem ICT akan melibatkan tiga (3) aktiviti utama dan dijelaskan dengan lebih terperinci melalui **Lampiran A1: Tatacara Pelaksanaan Penilaian Risiko.** Tiga (3) aktiviti utama adalah seperti yang berikut:

(a) Mengenal pasti ancaman, kebarangkalian dan impak yang menyumbang risiko kepada asset;

(b) Menilai dan memberikan keutamaan terhadap risiko; dan

(c) Mencadangkan langkah kawalan yang bersesuaian.

(ii) Agensi pelaksana perlu mengemukakan Laporan Penilaian Risiko sebagai dokumen sokongan dalam permohonan perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) kepada agensi pusat. Rujuk **Lampiran B1: Templat Laporan Penilaian Risiko**.

PENENTUAN PENGGUNAAN SIJIL DIGITAL

5. Berdasarkan tahap risiko yang diperoleh daripada penilaian risiko yang dilaksanakan, agensi boleh menentukan penggunaan sijil digital bagi tujuan keperluan pengesahan identiti, tidak boleh disangkal melalui tandatangan digital dan penyulitan maklumat dengan mengambil kira langkah-langkah kawalan keselamatan yang bersesuaian. Panduan untuk menentukan keperluan sijil digital serta medium sijil digital yang bersesuaian dengan keperluan keselamatan yang dipilih adalah seperti yang berikut:

(i) **Rajah 1A**: Gambaran Keseluruhan Panduan Penentuan Penggunaan Sijil Digital;

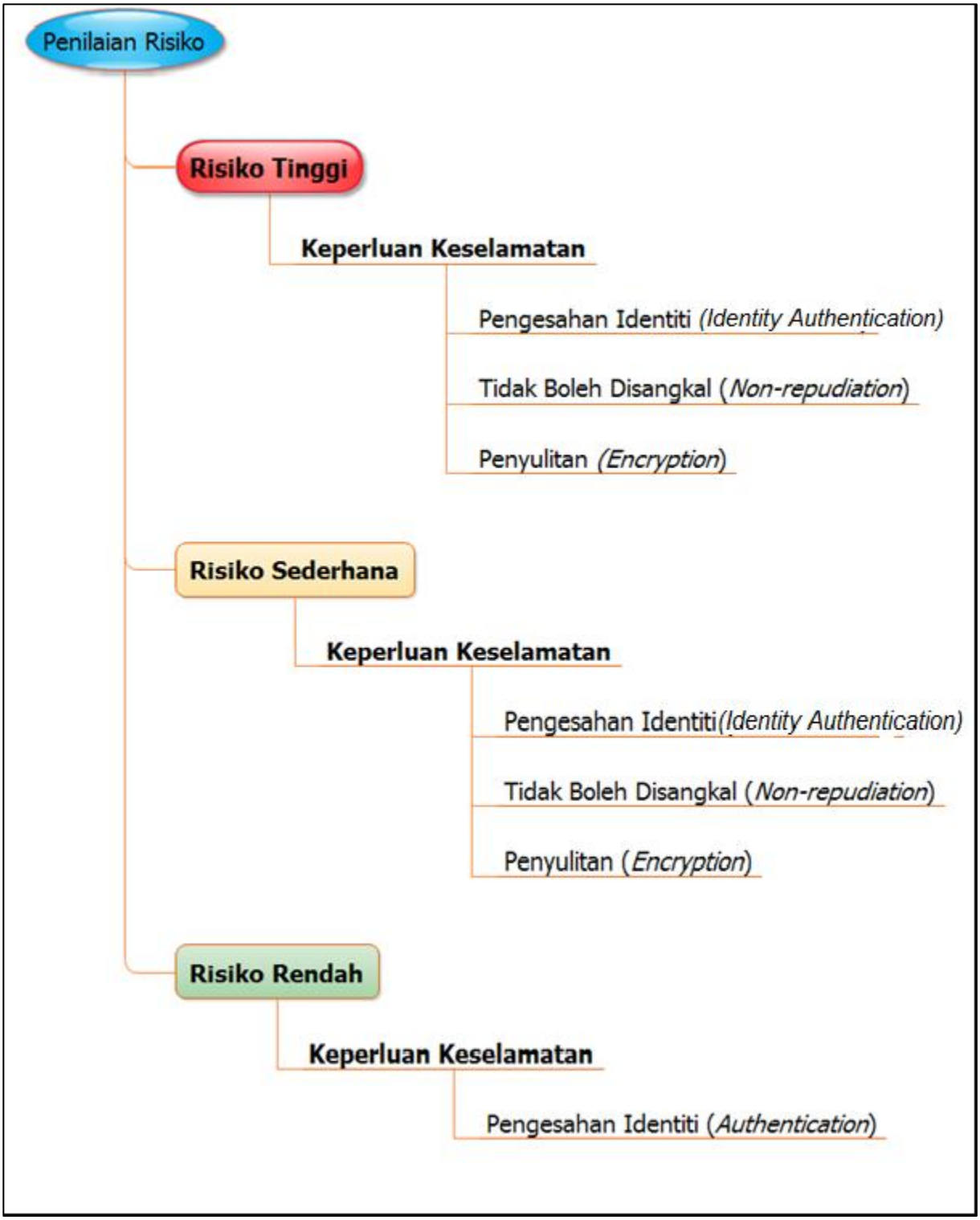
(ii) **Rajah 1B**: Panduan Penentuan Penggunaan Sijil Digital Berisiko Tinggi bagi Keperluan Keselamatan Pengesahan Identiti;

(iii) **Rajah 1C**: Panduan Penentuan Penggunaan Sijil Digital Sistem Berisiko Tinggi bagi Keperluan Keselamatan Tidak Boleh Disangkal dan Penyulitan;

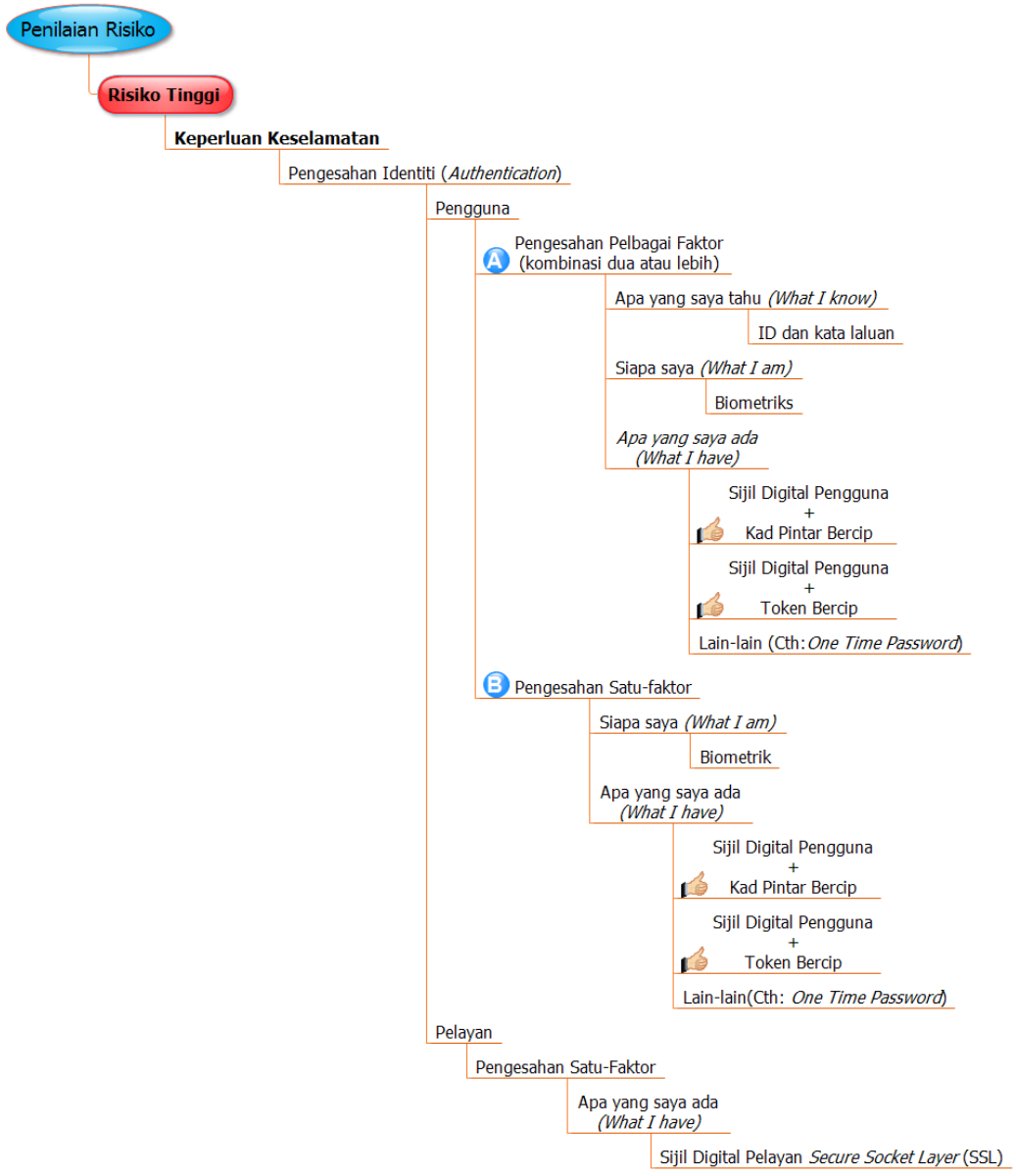
(iv) **Rajah 1D**: Panduan Penentuan Penggunaan Sijil Digital Sistem Berisiko Sederhana bagi Keperluan Keselamatan Pengesahan Identiti;

(v) **Rajah 1E**: Panduan Penentuan Penggunaan Sijil Digital Sistem Berisiko Sederhana bagi Keperluan Keselamatan Tidak Boleh Disangkal dan Penyulitan; dan

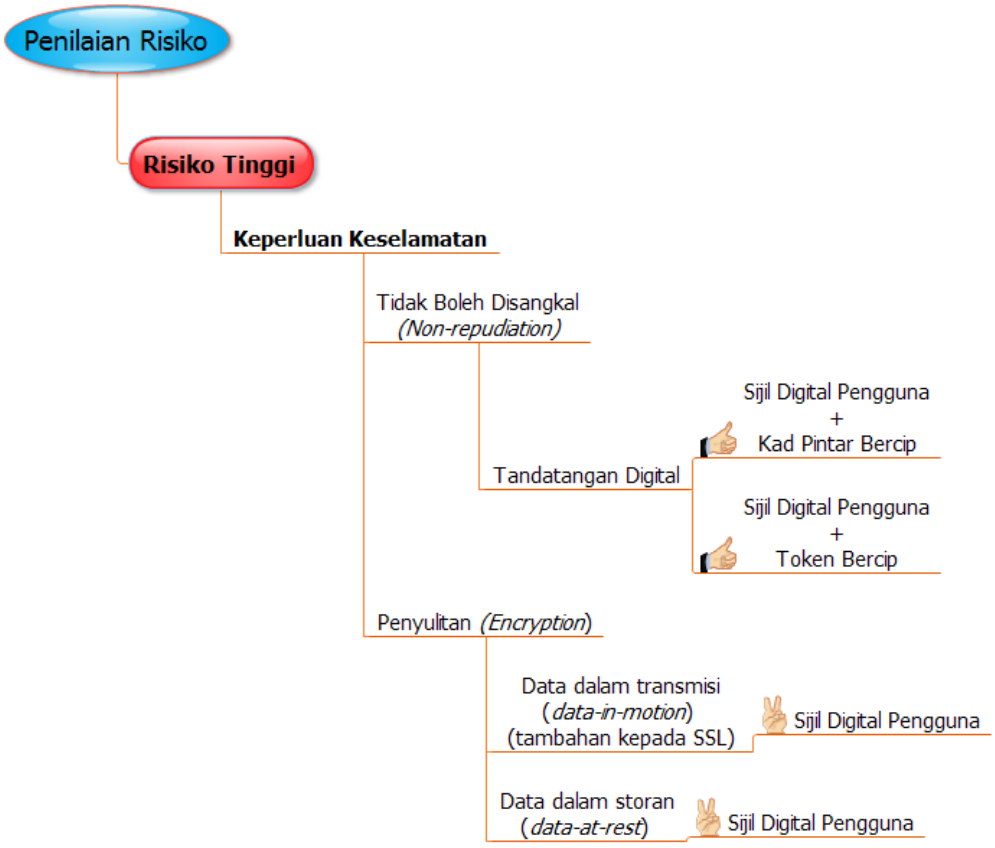
(vi) **Rajah 1F**: Panduan Penentuan Penggunaan Sijil Digital Sistem Berisiko Rendah bagi Keperluan Keselamatan Pengesahan Identiti.



Rajah 1A: Gambaran Keseluruhan Panduan Penentuan Penggunaan Sijil Digital



Rajah 1B: Panduan Penentuan Penggunaan Sijil Digital Berisiko Tinggi bagi Keperluan Keselamatan Pengesahan Identiti



Petunjuk:

A Agensi boleh memilih dua atau lebih kaedah pengesahan identiti yang dicadangkan

B Agensi boleh memilih salah satu daripada kaedah pengesahan identiti yang dicadangkan

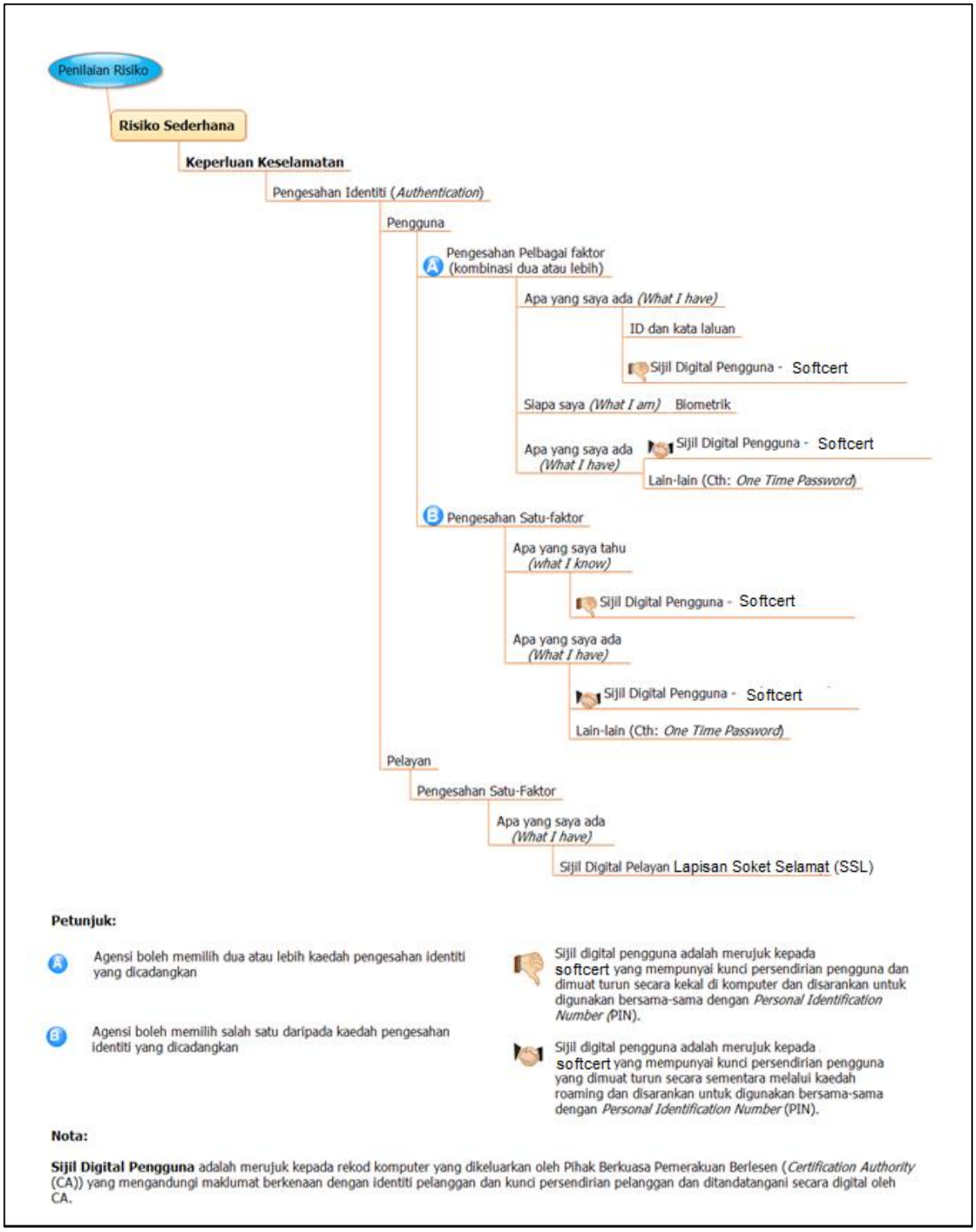
Sijil digital mengandungi kunci persendirian pengguna di dalamnya

Sijil digital yang mengandungi kunci awam yang akan digunakan untuk enkrip dan kunci persendirian pengguna untuk dekrip

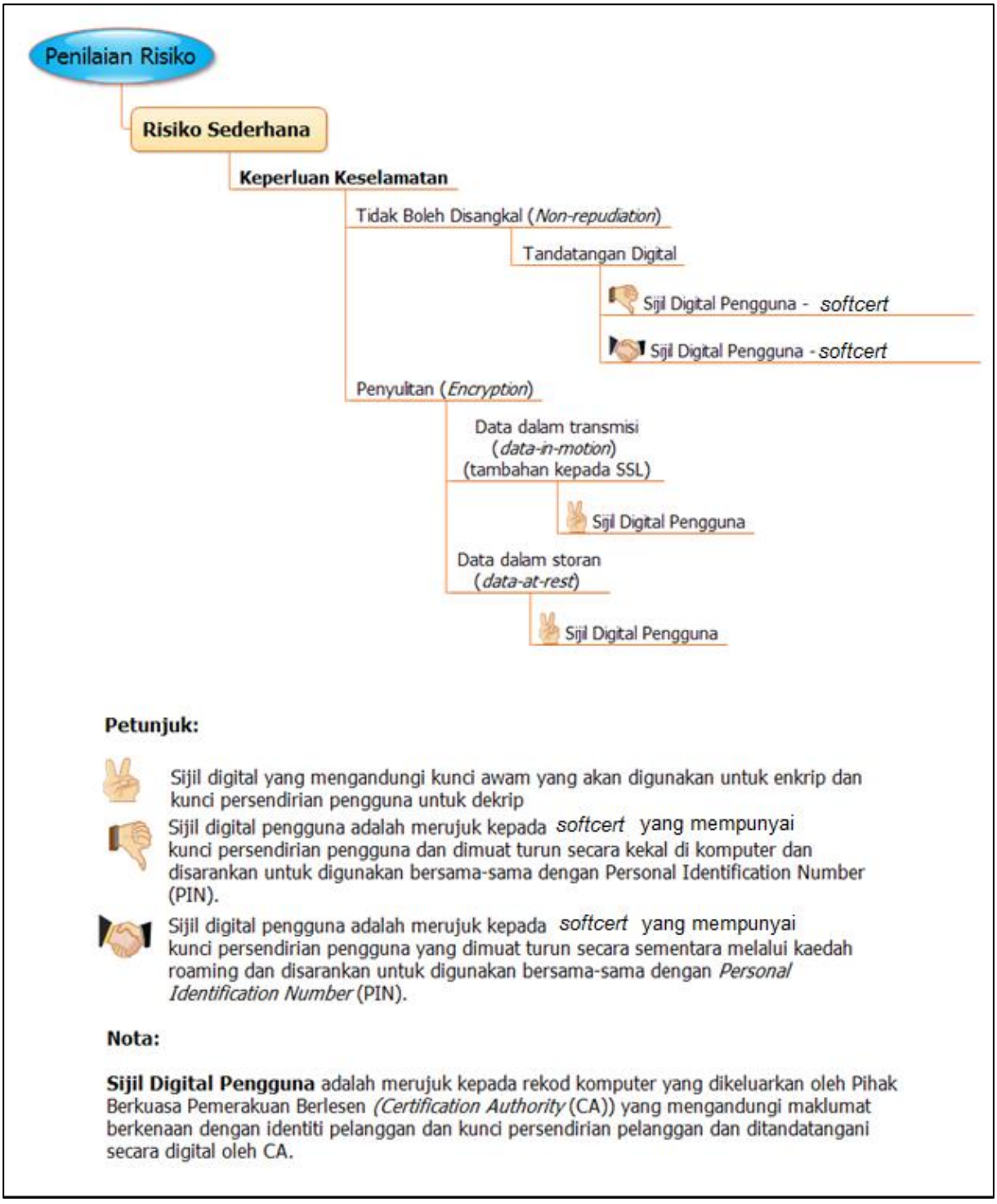
Nota:

Sijil Digital Pengguna adalah merujuk kepada rekod komputer yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (*Certification Authority* (CA)) yang mengandungi maklumat berkenaan dengan identiti pelanggan dan kunci persendirian pelanggan dan ditandatangani secara digital oleh CA.

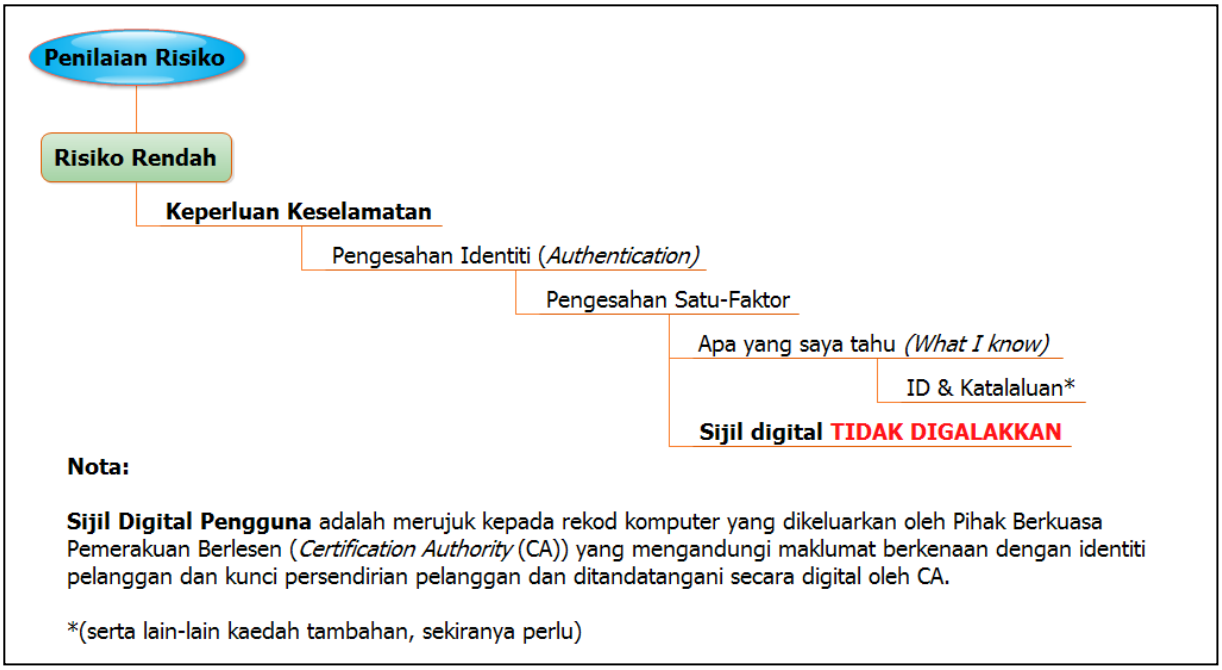
Rajah 1C: Panduan Penentuan Penggunaan Sijil Digital Sistem Berisiko Tinggi bagi Keperluan Keselamatan Tidak Boleh Disangkal dan Penyulitan



Rajah 1D: Panduan Penentuan Penggunaan Sijil Digital Sistem Berisiko Sederhana bagi Keperluan Keselamatan Pengesahan Identiti



Rajah 1E: Panduan Penentuan Penggunaan Sijil Digital Sistem Berisiko Sederhana bagi Keperluan Keselamatan Tidak Boleh Disangkal dan Penyulitan



Rajah 1F: Panduan Penentuan Penggunaan Sijil Digital Bagi Sistem Berisiko Rendah bagi Keperluan Keselamatan Pengesahan Identiti

Pemilihan Kaedah Kawalan Keselamatan

6. Langkah-langkah kawalan keselamatan yang menjadi asas pertimbangan dalam penggunaan Prasarana Kunci Awam (PKI) ialah kerahsiaan, pengesahan identiti, integriti dan tidak boleh disangkal. Agensi boleh merujuk **Jadual 1: Kaedah Kawalan Keselamatan Melalui PKI** sebagai panduan dalam pemilihan kaedah kawalan keselamatan sijil digital.

Konsep Asas Keselamatan PKI	Keterangan	Kaedah Tradisional	Kaedah Kawalan Keselamatan Melalui PKI
Kerahsiaan (Confidentiality)	Maklumat disediakan hanya untuk pegawai yang dibenarkan sahaja.	• Sampul surat yang dimeterai. • Dakwat limunan.	Penyulitan maklumat dibuat menggunakan kunci awam bagi memastikan hanya pemunya kunci persendirian yang sepadan sahaja boleh menyahsulit maklumat. Tujuan penggunaan: **pengesahan identiti** **penyulitan maklumat**
Pengesahan Identiti (Identity Authentication)	Proses mengenal pasti identiti entiti yang menghantar data.	• ID Staf. • Lesen pemandu. • Passport.	Sijil digital yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen mengandungi maklumat yang mengikat individu dengan kunci awam. Tujuan penggunaan: **pengesahan identiti**
Integriti (Integrity)	Maklumat sahih dan tidak diubah.	• Dakwat kekal. • Kertas tera air.	Tandatangan digital yang mengandungi maklumat kunci persendirian penghantar boleh disahkan dengan menyemak kunci awam penghantar. Tujuan penggunaan: **pengesahan identiti** **penyulitan maklumat**

Konsep Asas Keselamatan PKI	Keterangan	Kaedah Tradisional	Kaedah Kawalan Keselamatan Melalui PKI
Tidak Boleh Disangkal (Non-repudiation)	Aktiviti atau transaksi yang telah dilakukan tidak boleh dinafikan kemudiannya.	• Tandatangan yang diperakui. • Pos berdaftar.	Transaksi yang melibatkan tandatangan digital hanya boleh dilakukan oleh pemegang kunci persendirian. Tujuan penggunaan: **tandatangan digital**

Jadual 1: Kaedah Kawalan Keselamatan Melalui PKI

Kelas Sijil Digital

7. Dalam pengeluaran sijil digital, terdapat beberapa kelas sijil digital yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) berdasarkan kepada kelas yang telah ditetapkan oleh Suruhanjaya Komunikasi dan Multimedia (SKMM). Terdapat dua (2) kelas sijil digital yang dikeluarkan mengikut penggunaan jenis-jenis sijil digital. Kelas-kelas yang dimaksudkan adalah seperti **Jadual 2: Kelas-Kelas Sijil Digital.** Semua sijil digital pengguna dan pelayan yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) adalah dari Kelas 2 dan ke atas.

BIL.	KELAS SIJIL DIGITAL	PENGGUNAAN	TAHAP KESELAMATAN
1.	Kelas 1 : Individu	Digunakan untuk penyulitan terhadap data elektronik. Pengesahan identiti pengguna adalah mudah, iaitu memadai dengan pengesahan e-mel.	**Rendah**

BIL.	KELAS SIJIL DIGITAL	PENGGUNAAN	TAHAP KESELAMATAN
		Sijil digital kelas ini tidak boleh digunakan untuk tandatangan digital transaksi perniagaan. Sijil digital Kelas 1 tidak memberikan jaminan identiti pengguna.	
2.	Kelas 2: Organisasi	Digunakan untuk tandatangan digital bagi transaksi perniagaan dalam talian. Pengesahan pengguna adalah wajib. Sijil digital ini juga memberikan jaminan terhadap identiti pengguna dan dibekalkan untuk individu. Sijil digital ini kebanyakannya digunakan untuk pengesahan pengguna dan membekalkan transaksi dalam talian yang selamat dalam perkhidmatan seperti yang berikut: • Perkhidmatan e-Kewangan. • Perkhidmatan e-Kerajaan. • Perkhidmatan e-Pembrokeran Saham. • *e-Commerce*. • Kelulusan elektronik. • Perkhidmatan e-Dokumen. • Perkhidmatan *e-Insurance*.	**Tinggi**

Jadual 2: Kelas-kelas Sijil Digital

Pemilihan Medium Sijil Digital

8. Pemilihan medium sijil digital yang bersesuaian bagi pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI) boleh dilakukan oleh agensi dengan membuat pertimbangan berdasarkan tahap kawalan keselamatan dan juga tahap risiko persekitaran operasi yang menyokong fungsi agensi. Selain daripada itu, pemilihan jenis medium sijil digital bukan sahaja bagi tujuan mitigasi risiko, tetapi berdasarkan hasil analisis faedah kos.

Pemilihan Medium Sijil Digital Pengguna Berdasarkan Tahap Kawalan Keselamatan

9. Sijil digital pengguna yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) disimpan dalam medium yang berbeza. Penerangan berkaitan tahap kawalan keselamatan dan ciri-ciri keselamatan bagi setiap jenis medium sijil digital adalah seperti yang berikut:

(i) **Jadual 3**: Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Berdasarkan Cip - Kad Pintar;

(ii) **Jadual 4**: Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Berdasarkan Cip – Token;

(iii) **Jadual 5**: Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Perayauan; dan

(iv) **Jadual 6**: Tahap Kawalan Dan Ciri Keselamatan Bagi Jenis Medium Sijil Digital Muat Turun.

Bagi sistem aplikasi yang berisiko **rendah**, penggunaan sijil digital **tidak digalakkan**.

Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Berdasarkan Cip – Kad Pintar	
Tahap Kawalan Keselamatan	**TINGGI**
Ciri-ciri Keselamatan	i. Kunci persendirian disimpan dalam kad pintar. ii. Kunci persendirian tidak boleh disalin. iii. Kalis ubah *(*Tamper-proof*)*. iv. Media berlainan daripada komputer. v. Personalisasi. vi. Pasangan kunci (key pair) dijana dalam cip (on board key generation).
Persekitaran Operasi	i. Fungsi agensi yang memberikan implikasi terhadap keselamatan dan kesejahteraan dan kewangan. ii. Fungsi agensi sangat bergantung kepada sistem ICT. iii. Agensi perlu mematuhi Akta/Peraturan/Arahan Kerajaan; dan yang memandatkan kelulusan yang memerlukan tandatangan bagi urusan rasmi yang berkaitan.
Faktor Pertimbangan yang Lain	i. Keperluan peranti pembaca kad pintar di pihak pengguna. ii. Keperluan kos untuk kad pintar dan pembaca kad pintar. iii. Kebarangkalian berlaku kehilangan atau kerosakan kad pintar dan pembaca kad pintar. iv. Kesulitan kepada pengguna dengan kekangan kepada tiga (3) kali cubaan memasukkan katalaluan. v. Kebergantungan kepada ketersediaan rangkaian dari agensi ke pelayan Senarai Pembatalan Perakuan [Certificate Revocation List (CRL)] bagi tujuan pengesahan sijil digital.

Jadual 3: Tahap Kawalan dan Ciri Keselamatan Bagi Jenis Medium Sijil Digital Berdasarkan Cip - Kad Pintar

Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Berdasarkan Cip – Token	
Tahap Kawalan Keselamatan	**TINGGI**
Ciri-ciri Keselamatan	i. Kunci persendirian disimpan dalam token. ii. Kunci persendirian tidak boleh disalin. iii. Kalis Ubah (Tamper-proof). iv. Media berlainan dari komputer. v. Pasangan kunci (key pair) dijana dalam cip (onboard key generation).
Persekitaran Operasi	i. Fungsi agensi yang memberi implikasi terhadap keselamatan dan kesejahteraan dan kewangan. ii. Fungsi agensi sangat bergantung kepada sistem ICT. iii. Agensi perlu mematuhi Akta/Peraturan/Arahan Kerajaan yang memandatkan kelulusan yang memerlukan tandatangan bagi urusan rasmi yang berkaitan.
Faktor Pertimbangan yang Lain	i. Keperluan kos untuk token. ii. Kebarangkalian berlaku kehilangan atau kerosakan token. iii. Penggunaan semula token. iv. Kesulitan kepada pengguna dengan kekangan kepada lima (5) kali cubaan memasukkan kata laluan. v. Kebergantungan kepada ketersediaan rangkaian dari agensi ke pelayan Senarai Pembatalan Perakuan [Certificate Revocation List (CRL)] bagi tujuan pengesahan sijil digital.

Jadual 4: Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Berdasarkan Cip – Token

Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Perayauan	
Tahap Kawalan Keselamatan	**SEDERHANA/TINGGI** (bergantung kepada kombinasi kawalan keselamatan)
Ciri-ciri Keselamatan	i. Kunci persendirian disimpan di Pihak Berkuasa Pemerakuan Berlesen. ii. Kunci hanya disimpan sementara bagi tempoh tertentu dalam komputer pengguna (tidak melebihi empat (4) jam).
Persekitaran Operasi	i. Fungsi agensi yang memberi implikasi terhadap imej atau pentadbiran kerajaan. ii. Fungsi agensi disokong oleh sistem ICT yang digunakan merentas agensi sektor awam. iii. Capaian kepada sistem berkonsepkan di mana-mana (anywhere), pada bila-bila masa (anytime) dan banyak diakses menggunakan peranti mudah alih. iv. Bagi tujuan penggunaan pengesahan identiti dan penyulitan sahaja.
Faktor Pertimbangan yang Lain	i. Keperluan perisian di peranti pengguna. ii. Pemahaman dan persetujuan pengguna untuk membenarkan Pihak Berkuasa Pemerakuan Berlesen menyimpan pasangan kunci (key pairs) dengan selamat dan setiap muat turun mestilah dengan penafian tuntutan liabiliti dari Pihak Berkuasa Pemerakuan Berlesen. iii. Keperluan kawalan keselamatan tambahan khususnya berkaitan dengan pengesahan identiti pelbagai faktor. iv. Kebergantungan kepada ketersediaan rangkaian dari agensi ke pelayan Senarai Pembatalan Perakuan [Certificate Revocation List (CRL)] bagi tujuan pengesahan sijil digital.

Jadual 5: Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Perayauan

Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Muat Turun	
Tahap Kawalan Keselamatan	**SEDERHANA**
Ciri-ciri Keselamatan	i. Kunci persendirian disimpan di komputer pengguna. ii. Kunci disimpan secara tetap dalam komputer pengguna sehingga ianya dihapuskan.
Persekitaran Operasi	i. Fungsi agensi yang memberikan implikasi terhadap imej atau pentadbiran kerajaan. ii. Fungsi agensi disokong oleh sistem ICT yang digunakan merentasi agensi sektor awam. iii. Capaian kepada sistem aplikasi yang berasaskan web ini, kebanyakkannya digunakan pada komputer/komputer riba yang spesifik.
Faktor Pertimbangan yang Lain	i. Tiada keperluan kepada sebarang peranti atau media tambahan. ii. Keperluan penjanaan pasangan kunci (key pairs) menerusi proses muat turun sijil digital di komputer pengguna. iii. Keperluan untuk menghapuskan sijil digital di komputer asal pengguna sekiranya berlaku pertukaran komputer. iv. Penggunaan sijil digital memerlukan katalaluan (PIN) yang ditetapkan oleh pengguna. v. Pemuatan turun sijil digital hanya dibenarkan sekali dan disimpan dalam satu peranti yang ditetapkan sahaja. vi. Kebergantungan kepada ketersediaan rangkaian dari agensi ke pelayan Senarai Pembatalan Perakuan [Certificate Revocation List (CRL)] bagi tujuan pengesahan sijil digital.

Jadual 6: Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Muat Turun

Penafian – Jadual ini hanyalah sebagai panduan kepada agensi untuk menentukan jenis medium sijil digital yang bersesuaian untuk digunakan bagi sistem ICT kerajaan.

Pemilihan Medium Sijil Digital Pelayan Berdasarkan Tahap Kawalan Keselamatan

10. Sijil digital pelayan yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) mempunyai tahap kawalan dan ciri-ciri keselamatan seperti yang diterangkan dalam **Jadual 7: Tahap Kawalan dan Ciri Keselamatan Mengikut Jenis Medium Sijil Digital Pelayan**.

Tahap Kawalan dan Ciri Keselamatan bagi Jenis Medium Sijil Digital Pelayan	
Tahap Kawalan Keselamatan	**TINGGI**
Ciri-ciri Keselamatan	i. Mewujudkan sesi SSL antara pelayan web (web server) dengan pelayar web (web browser) bagi tujuan penyulitan maklumat. ii. Mewujudkan identiti khusus bagi pelayan web.
Faktor Pertimbangan yang Lain	i. Memerlukan janaan Permintaan Tendatangan Sijil [certificate signing request (CSR)] oleh agensi pemilik nama domain. ii. Semua maklumat perlulah dikemas kini dengan pendaftar domain bagi mengelakkan sebarang kesukaran untuk pengeluaran sijil digital pelayan.

Jadual 7: Tahap Kawalan dan Ciri Keselamatan Mengikut Jenis Medium Sijil Digital Pelayan

KEPERLUAN TEKNIKAL PERKHIDMATAN GPKI

11. Keperluan teknikal perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) menerangkan keperluan berkaitan piawaian, integrasi dan keperluan khusus bagi Sijil Perisian (softcert). Seksyen ini adalah untuk membantu agensi dalam persediaan teknikal pelaksanaan perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) khususnya bagi keperluan aplikasi dan infrastruktur ICT.

Piawaian-Piawaian Berkaitan Pelaksanaan PKI

12. Pelaksanaan Prasarana Kunci Awam (PKI) yang melibatkan sijil digital dan lain-lain infrastruktur berpandukan beberapa piawaian antarabangsa yang diterima umum. **Jadual 8: Piawaian Berkaitan Penggunaan PKI** dan **Jadual 9: Piawaian Berkaitan Medium Sijil Digital** di bawah menyenaraikan piawaian antarabangsa tersebut.

Bil.	Penggunaan PKI	Piawaian
1.	Pengesahan Identiti	SSL Mutual Authentication
2.	Penyulitan Maklumat	XML Encryption, S/MIME
3.	Tandatangan Digital	XML Signature, PKCS#7

Jadual 8: Piawaian Berkaitan Penggunaan PKI

Bil.	Medium Sijil Digital	Piawaian
1.	Kriptografi Berasaskan Cip - Kad Pintar	ISO 7816, FIPS 140, FIPS 46, FIPS 196, PKCS#11, CSP
	Pembaca Kad Pintar	ISO 7816, PC/SC

Bil.	Medium Sijil Digital	Piawaian
2.	Kriptografi Berasaskan Cip - Token	FIPS 140, FIPS 46, FIPS 196, PKCS#11, CSP, USB
3.	Sijil Perisian (Softcert)	PKCS#12, PFX
4.	Sijil Digital Perayauan	PKCS#12, PFX

Jadual 9: Piawaian Berkaitan Medium Sijil Digital

Keperluan Integrasi PKI dengan Aplikasi Agensi

13. Agensi pelaksana mempunyai peranan dan tanggungjawab khususnya dalam menentukan keperluan integrasi Prasarana Kunci Awam (PKI) dengan aplikasi berkaitan. Dalam melaksanakan pembangunan sistem aplikasi yang akan diintegrasikan dengan perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI), agensi perlu memastikan kawalan keselamatan terhadap sistem aplikasi yang dilaksanakan. Terdapat dua aspek kawalan keselamatan yang perlu dilaksanakan:

(i) **Pelaksanaan Kawalan Keselamatan Aplikasi**

Agensi perlu mengemas kini perisian pelayar web yang akan digunakan ke versi terkini. Selain itu, agensi hendaklah memastikan sistem yang dibangunkan mempunyai sesi rehat (time-out session) yang bersesuaian dengan sistem aplikasi.

(ii) **Pelaksanaan Integrasi Prasarana Kunci Awam (PKI) dengan Aplikasi Mengikut Tujuan Penggunaan**

Kaedah pelaksanaan integrasi mengikut tujuan penggunaan sijil digital diterangkan melalui **Jadual 10: Pelaksanaan Integrasi Mengikut Tujuan Penggunaan**.

Tujuan Penggunaan	Kaedah Pelaksanaan	Peranan dan Tanggungjawab
Pengesahan Identiti	**Opsyen 1: *SSL Mutual authentication*** i. Fungsi kesahihan saling SSL (SSL mutual authentication) perlu diaktifkan pada pelayan web (web server). (Rujuk pada manual konfigurasi pelayan web bagi melaksanakan konfigurasi punca yang dipercayai CA). ii. Kebenaran capaian berdasarkan sijil digital pengguna. iii. Capaian kepada Senarai Pembatalan Perakuan [Certificate Revocation List (CRL)] perlu diaktifkan bagi tujuan kesahan sijil (certificate validation).	Agensi pelaksana untuk melaksanakan konfigurasi pada pelayan web di agensi masing-masing.
	Opsyen 2: Ejen GPKI i. Skrip API bagi tujuan pengesahan sijil digital (nama pemegang sijil, KP, *status kesahan sijil dan pengeluar sijil).	i. MAMPU bekalkan contoh skrip API atau agensi membangunkan skrip API sendiri.

Tujuan Penggunaan	Kaedah Pelaksanaan	Peranan dan Tanggungjawab
	ii. API bagi tujuan penyimpanan sijil digital dan pengurusan PIN. * status kesahan sijil, pengesahan sijil digital dengan Senarai Pembatalan Perakuan [Certificate Revocation List (CRL)].	ii. MAMPU bekalkan API atau Agensi membangunkan API sendiri.
Tidak Boleh Disangkal Melalui Tandatangan Digital	i. Agen GPKI • Skrip API yang akan digunakan untuk tandatangan digital borang di pelayan. ii. API Pengguna dan Pelayan • Untuk membenarkan komunikasi antara sistem dan sijil digital bagi semua media. • Untuk mengesahkan tandatangan digital dan sijil digital.	i. MAMPU bekalkan contoh skrip API atau agensi membangunkan skrip API sendiri. ii. MAMPU bekalkan API atau Agensi membangunkan API sendiri dan perlu mematuhi piawaian yang ditetapkan.
Penyulitan Maklumat	Kaedah pelaksanaan perlu mengikut piawaian yang ditetapkan, iaitu Penyulitan XML (XML Encryption), S/MIME.	Agensi pelaksana kerana ia bergantung kepada keperluan proses kerja dan sistem aplikasi agensi.

Jadual 10: Pelaksanaan Integrasi Mengikut Tujuan Penggunaan

Keperluan Khusus bagi Pelaksanaan Sijil Digital Pengguna bagi Sijil Digital Perayauan dan Sijil Digital Muat Turun

14. Pada asasnya pelaksanaan sijil digital pengguna yang menggunakan kaedah perayauan atau muat turun ke komputer pengguna memerlukan kemudahan rangkaian. Selain itu, beberapa keperluan khusus lain, adalah seperti yang berikut:

(i) **Penggunaan Sijil Digital Pengguna - Sijil Digital Perayauan**

Pelaksanaan secara kaedah perayauan memerlukan ketersediaan rangkaian pada **setiap kali** sijil digital hendak digunakan. Ia melibatkan komponen-komponen Prasarana Kunci Awam Kerajaan (GPKI) seperti yang disenaraikan dalam **Jadual 11: Komponen GPKI**.

KOMPONEN GPKI	KETERANGAN
Repositori Sijil (Certificate Repository)	Menyediakan repositori bagi kunci awam sijil digital dan senarai sijil digital yang telah dibatalkan [Senarai Pembatalan Perakuan (CRL)].
Broker PKI	Aplikasi perkhidmatan web untuk mengenal pasti sama ada pengguna menggunakan sijil digital secara perayauan.
Perayauan CA (CA Roaming)	Aplikasi perkhidmatan web di pusat data CA yang menyediakan pelbagai fungsi CA seperti mendaftar, mencipta dan membatal serta memuat turun sijil digital.
Ejen GPKI	Modul aplikasi yang perlu dipasang pada setiap komputer pengguna dan perlu diaktifkan setiap kali menggunakan sijil digital secara perayauan.

Jadual 11: Komponen-komponen GPKI

(ii) **Penggunaan Sijil Digital Pengguna – Sijil Digital Muat Turun**

Penggunaan sijil digital pengguna - sijil digital muat turun yang dimuat turun ke komputer pengguna memerlukan capaian rangkaian semasa memuat turun sijil digital pada kali pertama sahaja. Sijil digital pengguna ini perlu dimuat turun melalui Portal GPKI.

(iii) **Penghapusan Sijil Digital Pengguna**

Agensi hendaklah memastikan sijil-sijil digital yang digunakan untuk sistem aplikasi sama ada yang digunakan oleh pengguna atau di pelayan dihapuskan melalui proses sanitasi apabila melakukan pelupusan perkakasan untuk memastikan penggunaan Prasarana Kunci Awam Kerajaan (GPKI) yang terkawal.

PENUTUP

15. Agensi hendaklah mematuhi garis panduan ini bagi mengenal pasti keperluan teknikal perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) dalam penggunaan sijil digital bagi sistem ICT kerajaan. Dokumen ini juga hendaklah dibaca bersama dengan Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) dan Garis Panduan Operasi Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI).

LAMPIRAN A1

Tatacara Pelaksanaan Penilaian Risiko

Aktiviti (I) – Mengenal Pasti Ancaman, Kebarangkalian dan Impak

Proses ini bermula dengan mengenal pasti dan menganalisis semua risiko terhadap sistem aplikasi agensi sektor awam dengan menyenaraikan semua ancaman, sumber ancaman, kebarangkalian dan impaknya.

Secara umumnya, ancaman kepada sistem aplikasi boleh dibahagikan kepada enam (6) kategori seperti **Jadual 1**: **Kategori Ancaman Kepada Sistem Aplikasi.**

BIL.	KATEGORI	PENERANGAN
1.	Penyamaran Identiti (Spoofing)	Satu tindakan ancaman yang bertujuan untuk mengakses sistem aplikasi secara haram dan menggunakan kelayakan pengguna lain seperti ID pengguna dan kata laluan.
2.	Pengubahsuaian Data (Data Tampering)	Satu tindakan ancaman berniat jahat yang bertujuan untuk menukar/mengubahsuai data seperti pengubahsuaian data dalam pangkalan data, dan mengubah data dalam transit antara dua komputer melalui sesuatu rangkaian terbuka, seperti Internet.
3.	Penyangkalan (Repudiation)	Satu tindakan ancaman yang bertujuan untuk melaksanakan operasi haram dalam satu sistem yang tidak mempunyai keupayaan untuk mengesan operasi dilarang.
4.	Pendedahan Maklumat (Information Disclosure)	Tindakan ancaman untuk membaca fail yang salah, tidak diberi akses kepada, atau untuk membaca data dalam transit.
5.	Penafian Perkhidmatan (Denial of Service)	Satu bentuk ancaman yang bertujuan untuk menafikan akses kepada pengguna yang sah, seperti dengan membuat pelayan web tidak berfungsi atau tidak boleh digunakan.

BIL.	KATEGORI	PENERANGAN
6.	Peningkatan Hak Akses (Elevation of Privileges)	Satu bentuk ancaman yang bertujuan untuk mendapatkan hak akses istimewa kepada sumber-sumber maklumat yang tidak dibenarkan atau menjejaskan sistem.

Jadual 1: Kategori Ancaman Kepada Sistem Aplikasi

Penilaian risiko memerlukan pengumpulan maklumat-maklumat ancaman, kebarangkalian berlakunya ancaman dan impaknya terhadap organisasi. Beberapa kaedah pengumpulan maklumat yang digunakan seperti semakan dokumen yang berkaitan, temu duga, soal selidik, perbincangan dan merujuk pandangan pakar dalam sesuatu bidang seperti keselamatan, rangkaian audit dan pihak industri. Antara langkah penting yang boleh digunakan untuk aktiviti ini termasuklah:

(a) Senarai dan terangkan secara ringkas ancaman dan sumber ancaman yang boleh memudaratkan kemudahan ICT organisasi terutamanya yang berkaitan dengan sistem aplikasi kritikal yang telah dikenal pasti dalam proses Analisis Impak Perniagaan (Business Impact Analysis);

(b) Senaraikan langkah-langkah kawalan sedia ada atau langkah-langkah kawalan yang telah dikenal pasti akan dilaksanakan;

(c) Tentukan kebarangkalian ancaman tersebut berlaku. Satu keadah yang boleh digunakan untuk menentukan kebarangkalian ini adalah dengan memberikan penarafan 1 bagi kebarangkalian rendah sehingga 5 bagi kebarangkalian tinggi. **Jadual 2: Contoh Indeks Kebarangkalian dan Indeks Impak** ialah satu contoh indeks kebarangkalian yang boleh diguna pakai. Indeks kebarangkalian ini mungkin berbeza bagi setiap agensi dan perlu disediakan terlebih dahulu berdasarkan kepada keperluan masing-masing. Indeks kebarangkalian bagi setiap ancaman boleh ditentukan berdasarkan pertimbangan yang berasaskan fakta dan pengalaman;

(d) Tentukan tahap impak dari segi ancamannya kepada operasi, kewangan, reputasi, pengguna yang terjejas,dan lain-lain yang berkaitan dengan organisasi masing-masing. Selain itu, ancaman kepada sistem aplikasi seperti pembangunan semula sistem aplikasi (reconstruction of

application system) dan sistem aplikasi yang mudah dieksploitasi. Satu kaedah yang boleh digunakan untuk menentukan tahap impak ini adalah dengan memberi penarafan 1 bagi impak rendah sehingga 5 bagi impak tinggi. Cadangan Indeks Impak yang boleh diguna pakai adalah seperti **Jadual 2: Contoh Indeks Kebarangkalian dan Indeks Impak**. Indeks impak ini perlu disediakan terlebih dahulu dan mungkin berbeza bagi setiap organisasi. Pertimbangan untuk memberikan penarafan impak perlu mengambil kira jenis ancaman dan langkah kawalan sedia ada. Indeks impak bagi setiap ancaman boleh ditentukan berdasarkan pertimbangan ke atas tahap keseriusan (severity) yang perlu ditanggung oleh organisasi sekiranya ancaman berlaku; dan

KEBARANGKALIAN	IMPAK			
	OPERASI	KEWANGAN	REPUTASI	LAIN-LAIN (nyatakan)
(1) > 3 tahun (sangat tidak mungkin)	**(1)** Tidak berkenaan	**(1)** Tidak berkenaan	**(1)** Tidak berkenaan	**(1)** *Mengikut kesesuaian organisasi
(2) 3 tahun (tidak mungkin)	**(2)** < 4 jam	**(2)** < RM10 juta	**(2)** Aduan terpencil	**(2)**
(3) sekali setahun (mungkin)	**(3)** 4 jam ke 3 hari	**(3)** >RM10 juta dan < RM25 juta	**(3)** Aduan terbanyak daripada pemegang kepentingan	**(3)**
(4) > 6 bulan (besar kemungkinan)	**(4)** Antara 3 hingga 7 hari	**(4)** >RM25 juta dan <RM50 juta	**(4)** Publisiti negatif dalam media tempatan	**(4)**
(5) Sekali sebulan (sangat mungkin)	**(5)** > 7 hari	**(5)** >RM50 juta	**(5)** Publisiti negatif dalam media tempatan dan antarabangsa	**(5)**

Jadual 2: Contoh Indeks Kebarangkalian dan Indeks Impak

(e) Dokumenkan maklumat-maklumat hasil dari langkah-langkah (a) hingga (d) menggunakan templat seperti **Jadual 3: Templat Penilaian Risiko**;

	(i) Ancaman		**(ii) Kawalan**	**(iii) Kebarang-kalian**	**(iv) Sekiranya ancaman berlaku apakah impak kepada agensi (Sila Rujuk Jadual 2)**				
No.	(a) Ancaman	(b) Keterangan Ancaman	Kawalan sedia ada	5 Tinggi - 1 Rendah	(a) Manusia	(b) Operasi	(c) Kewangan	(d) Reputasi	(e) Lain-lain (Nyatakan)
					5 Tinggi - 1 Rendah				
1.	Kod jahat	Perisian antivirus tamat tempoh.		5	1	5	5	5	
2.	Sabotaj	Kebocoran maklumat penting oleh pekerja dalaman.		2	1	1	1	5	
3.	Kecurian	Masalah kurang pengawasan.		3	1	2	2	3	

Jadual 3: Templat Penilaian Risiko

(f) Satu ancaman boleh memberikan impak kepada beberapa faktor seperti manusia, kewangan, reputasi dan sebagainya. Nilai kumulatif faktor ini boleh diperolehdengan menggunakan nilai impak setiap faktor seperti **Jadual 4: Nilai Impak Faktor bagi Pengiraan Impak**. **Jadual 5: Kaedah Pengiraan Impak** pula menunjukkan kaedah pengiraan impak apabila berlakunya sesuatu ancaman.

Impak = n1 + n2 + n3 + …n/N iaitu N = nilai impak bagi setiap faktor impak N = bilangan faktor impak

Jadual 4: Nilai Impak Faktor bagi Pengiraan Impak

IMPAK					(iv) IMPAK = (a+b+c+d+e)/5
(a) Manusia	(b) Operasi	(c) Kewangan	(d) Reputasi	(e) Lain-lain (Nyatakan)	
Skala impak 1 hingga 5 dan 1 ialah impak terendah.					
5	5	3	4	4	(5+5+2+4+4)/5 = 4

Jadual 5: Kaedah Pengiraan Impak

Aktiviti (II) - Menilai dan Memberikan Keutamaan Risiko

Hasil daripada aktiviti mengenal pasti ancaman, kebarangkalian dan impak membolehkan penilaian risiko dilaksanakan dan seterusnya menentukan keutamaan risiko yang perlu ditangani. Risiko boleh diungkapkan sebagai fungsi impak dan kebarangkalian. Dalam aktiviti **Menilai dan Memberikan Keutamaan Risiko**, setiap risiko yang telah dikenal pasti dikira menggunakan formula seperti **Jadual 6: Formula Penilaian Risiko**.

Risiko = Kebarangkalian x Impak

Jadual 6: Formula Penilaian Risiko

Pengiraan risiko bagi setiap ancaman yang telah ditentukan dalam Aktiviti (I) diterangkan dalam **Jadual 7 : Risiko dan Nilai Risiko**.

	(i) Ancaman	(ii) Kebarangkalian	(iii) Sekiranya ancaman berlaku apakah impak kepada agensi (Sila Rujuk Jadual 2)					(iv) Impak = (a+b+c+d+e)/n	(v) Risiko (Risiko = Kebarangkalian X Impak
No	Ancaman	5 Tinggi – 1 Rendah	(a) Manusia	(b) Operasi	(c) Kewangan	(d) Reputasi	(e) Lain-lain		
			5 Tinggi - 1 Rendah						
1.	Kod jahat	5	1	5	5	5		4	20
2.	Sabotaj	2	1	1	1	5		2	4
3.	Kecurian	3	1	2	2	3		2	6

Jadual 7: Risiko dan Nilai Risiko

Dalam menentukan keutamaan risiko Matriks Tahap Risiko (seperti **Jadual 8: Contoh Matriks Tahap Risiko**) boleh digunakan sebagai rujukan. Matriks Tahap Risiko ini boleh diubah suai mengikut kesesuaian organisasi khususnya bagi julat kebarangkalian dan julat impak serta julat tahap risiko. Penentuan keutamaan ini bergantung pada nilai kebarangkalian dan nilai impak yang dijana sebelum ini.

TAHAP RISIKO		**IMPAK**				
		(1) Tiada Kesan Signifikan	**(2) Kecil**	**(3) Sederhana**	**(4) Besar**	**(5) Malapetaka**
KEBARANGKALIAN	(5) Kerap/Hampir Pasti	Sederhana	Tinggi	Tinggi	Tinggi	Tinggi
	(4) Besar Berkemungkinan	Sederhana	Sederhana	Tinggi	Tinggi	Tinggi
	(3) Sekali-sekala	Rendah	Sederhana	Sederhana	Tinggi	Tinggi
	(2) Jarang-jarang	Rendah	Sederhana	Sederhana	Sederhana	Tinggi
	(1) Besar Bekemungkinan tidak berlaku	Rendah	Rendah	Rendah	Sederhana	Sederhana

KOD TAHAP RISIKO

Tinggi Sederhana Rendah

Jadual 8: Contoh Matriks Tahap Risiko

Dengan mengambil nilai kebarangkalian dan nilai impak bagi setiap ancaman yang telah dikenal pasti padankannya dalam Matriks Tahap Risiko. Seterusnya keutamaan risiko ditentukan dengan menyenaraikan semua ancaman seperti **Jadual 9: Keutamaan Risiko** mengikut nilai risiko dan kod tahap risiko.

Keutamaan Risiko			
No.	**Ancaman**	**Nilai Risiko**	**Kod Tahap Risiko**
1.	Kod Jahat	20	Tinggi
2.	Kecurian	6	Sederhana
3.	Sabotaj	3	Rendah

Jadual 9: Keutamaan Risiko

Penentuan keutamaan risiko penting bagi membolehkan keputusan dibuat oleh pengurusan atasan organisasi. Sebagai contoh, risiko yang ditentukan sebagai rendah dan boleh diterima, perlu dipantau dan dikaji semula secara berkala untuk memastikan ia masih boleh diterima. Manakala risiko yang dianggap sederhana atau tinggi dan tidak boleh diterima, perlu diberikan cadangan langkah-langkah kawalan.

Aktiviti (III) - Mencadangkan Strategi Memitigasi Risiko

Berdasarkan senarai keutamaan risiko-risiko yang perlu ditangani, organisasi perlu memilih strategi memitigasi risiko yang sesuai. Secara umumnya terdapat empat pilihan strategi memitigasi risiko, iaitu:

(a) Pengelakan Risiko ialah membuat keputusan berdasarkan maklumat untuk tidak melibatkan diri atau menarik diri daripada situasi risiko;

(b) Pengurangan Risiko ialah mengambil langkah kawalan untuk mengurangkan pendedahan kepada risiko;

(c) Pemindahan Risiko ialah memindahkan beban kerugian yang disebabkan oleh risiko kepada pihak lain menerusi perundangan, kontrak, insurans atau lain-lain; dan

(d) Penerimaan Risiko ialah membuat keputusan berdasarkan maklumat untuk menerima kebarangkalian dan impak risiko tertentu.

Oleh itu, strategi yang sesuai perlu ditentukan bagi setiap risiko yang disenaraikan dalam jadual keutamaan risiko. Risiko boleh dikurangkan dengan melaksanakan atau menambah baik kawalan keselamatan. Bagi risiko di bawah strategi pengurangan risiko, tentukan kawalan keselamatan yang sesuai. Kawalan keselamatan ini boleh dirangka berdasarkan faktor yang berikut:

(a) Keberkesanan opsyen yang dicadangkan;

(b) Kesesuaian dan kesannya terhadap sistem-sistem lain, proses dan langkah kawalan;

(c) Undang-undang dan peraturan yang berkaitan;

(d) Polisi dan piawaian dalam organisasi;

(e) Struktur dan budaya kerja organisasi;

(f) Impak terhadap operasi; dan

(g) Kebolehpercayaan, kebolehharapan dan selamat.

Kawalan boleh dibahagikan kepada dua (2), iaitu kawalan bukan ICT dan kawalan ICT. Kawalan bukan ICT merangkumi program kesedaran keselamatan, pemantapan proses kerja yang berkesan dan selamat serta penyelesaian berbentuk perlindungan fizikal. Contoh kawalan bukan ICT adalah seperti yang berikut:

(a) Manual Prosedur Kerja atau Prosedur Operasi Standard yang lengkap dan terkini;

(b) Pas kawalan keselamatan untuk akses ke ruang-ruang tertentu dalam organisasi;

(c) Bekalan kuasa tanpa gangguan [uninterrupted power supply (UPS)] menyediakan bekalan tenaga elektrik yang mencukupi;

(d) Mesin janakuasa (generator) bertujuan membekalkan tenaga yang mencukupi atau membuat perjanjian untuk membekalkan diesel atau bahan api;

(e) Lewahan (redundancy) bagi kemudahan/perkhidmatan kritikal seperti pengangkutan dan komunikasi dalam organisasi;

(f) Sistem pemantauan persekitaran pusat data; dan

(g) Sistem kawalan kebakaran seperti alat pemadam kebakaran.

Manakala langkah-langkah kawalan ICT merangkumi keselamatan rangkaian, pusat data, sistem aplikasi, pangkalan data dan dan lain-lain infrastruktur ICT dalam organisasi. Contoh kawalan ICT adalah seperti yang berikut:

(a) Kawalan akses sistem dengan kaedah pengesahan identiti pengguna pelbagai faktor (multi-factors authentication);

(b) Seni bina sistem rangkaian yang selamat termasuk pelaksanaan prinsip pertahanan mendalam (defence-in-depth), segmentasi rangkaian serta perlindungan tembok api (firewall) dan sistem pengesan pencerobohan [Intrusion Prevention System (IPS)];

(c) Penggunaan penyulitan untuk maklumat terperingkat;

(d) Pelaksanaan mekanisme penyimpanan dan pemulihan aset ICT seperti data, fail-fail konfigurasi dan kod sumber aplikasi; dan

(e) Mewujudkan pendua bagi perkhidmatan ICT kritikal.

Pemilihan kawalan keselamatan mestilah mengambil kira justifikasi kos dan faedah serta prosedur dan keutamaan implementasi. Semasa membuat justifikasi kos dan faedah, pertimbangan jumlah keseluruhan kos pemilikan (total cost of ownership) penting dan melibatkan:

(a) Kos perolehan;

(b) Kos penempatan dan pelaksanaan;

(c) Kos penyelenggaran;

(d) Kos pengujian dan penilaian;

(e) Pematuhan, pemantauan dan penguatkuasaan; dan

(f) Kesannya kepada pengguna.

Pada peringkat pelaksanaan, organisasi perlu mengambilkira prosedur untuk mengukur keberkesanan langkah-langkah kawalan yang diambil dan mekanisme semakan secara berkala untuk memastikan keberkesanannya.

Penggunaan templat seperti **Jadual 10: Templat untuk Mengenal Pasti Kawalan Keselamatan** digunakan bagi strategi pengurangan risiko. Templat tersebut boleh membantu dalam proses mengenal pasti dan menentukan aspek kawalan keselamatan.

Jadual 10: Templat untuk Mengenal Pasti Kawalan Keselamatan

ID	(i)		(ii)	(iii)	(iv)	(v)	(vi)					(vii)		(viii)							(ix)
	Ancaman	Keterangan Sumber Ancaman	Risiko (Risiko = Kejadian X Kebarangkalian X Impak)	Kod Risiko	Kesan Keselamatan: Kerahsiaan/ Integriti/ kebolehsediaan	Pilihan Rawatan: Hindar/ Kurang/ Pindah/ Terima	Komponen Sistem yang Berkaitan: Aplikasi	Pangkalan Data	*Host*	Rangkaian	E-mel / Internet	Kawalan Pencegahan Semasa: Kawalan Pencegahan Sedia Ada	Perlindungan Insurans	Cadangan Penambahbaikan Aspek Pencegahan: Orang	Proses	Teknologi: Rangkaian	Keselamatan	Data	*Server*	Peranti	Teknologi yang Dicadangkan
1	*Kecurian Identiti*	Pengesahan pengguna lemah	20		Kerahsiaan dan integriti	Kurangkan risiko	Sistem A	Pangkalan Data Sistem A	*Server Mercury*	1Gov*Net	E-mel Agensi	Kawalan akses pengguna sistem – ID dan Kata Laluan	Waranti Perkakasan	-	wujudkan polisi/ prosedur kerja	Y	Y	Y	Y	Y	Meningkatkan kaedah pengesahan identiti pengguna kepada *pengesahan multifaktor*
2																					

LAMPIRAN B1

Templat Laporan Penilaian Risiko

1. Keterangan Projek

1.1 Pengenalan.

1.2 Latar Belakang.

(Nota: Nyatakan maklumat berkaitan misi dan objektif organisasi dan menetapkan konteks bagi pelaksanaan penilaian risiko)

2. Hasil Penemuan

2.1 Analisis penemuan.

2.2 Ringkasan keputusan.

2.2.1 Risiko dan langkah kawalan keselamatan sedia ada.

2.2.2 Hasil penilaian risiko.

3. Cadangan

3.1 Cadangan langkah kawalan yang spesifik bagi setiap ancaman yang dikenal pasti.

3.2. Strategi dan pelan tindakan.

LAMPIRAN II

GARIS PANDUAN OPERASI
PERKHIDMATAN PRASARANA KUNCI AWAM
[GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)]

KANDUNGAN

SENARAI RAJAH

SENARAI JADUAL

SENARAI LAMPIRAN

TUJUAN

Garis Panduan Operasi Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)] ini bertujuan menerangkan tadbir urus dan tatacara operasi perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI).

SKOP

2. Garis Panduan Operasi Prasarana Kunci Awam Kerajaan (GPKI) ini memberikan fokus kepada keterangan mengenai:

(i) Model pengurusan dan operasi perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI), peranan dan tanggungjawab semua pihak yang berkaitan dengan pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI); dan

(ii) Jenis perkhidmatan dan prosedur permohonan.

KUMPULAN SASARAN

3. Garis Panduan ini disasarkan khusus kepada kumpulan pengguna di agensi pusat, agensi pelaksana dan agensi sektor awam.

MODEL PENGURUSAN DAN OPERASI PERKHIDMATAN GPKI

4. Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) melaksanakan satu model pengurusan dan operasi seperti di **Rajah 1: Model Pengurusan dan Operasi Perkhidmatan GPKI** yang melibatkan pihak-pihak yang berikut:

(i) Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM);

(ii) Pihak Berkuasa Pemerakuan Berlesen [Licensed Certification Authority (CA)];

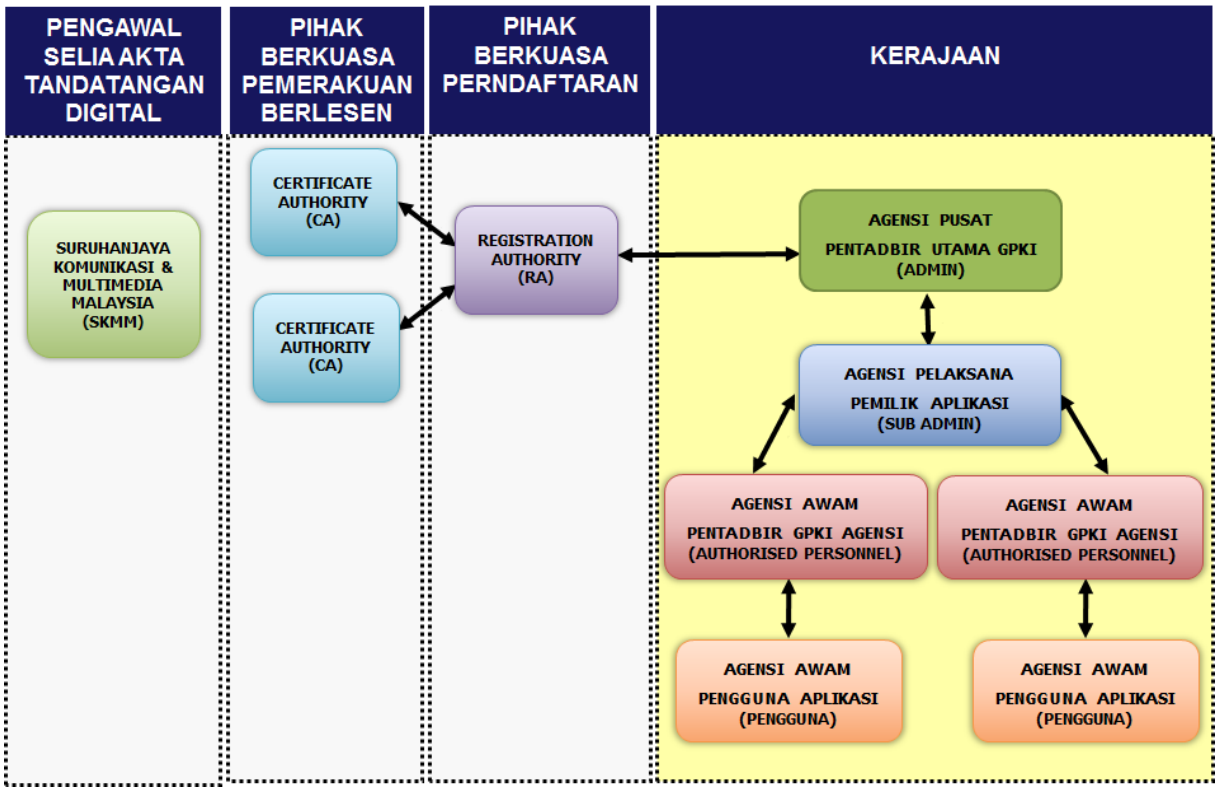
(iii) Pihak Berkuasa Pendaftaran [Registration Authority (RA)];

(iv) Agensi pusat yang terdiri daripada Pentadbir (Admin);

(v) Agensi pelaksana yang terdiri daripada SubPentadbir (SA) dan Pentadbir Pelayan (PS);

(vi) Agensi sektor awam yang terdiri daripada Pegawai Diberi Kuasa (AP); dan

(vii) Penjawat awam yang terdiri daripada pengguna aplikasi agensi pelaksana.



Rajah 1: Model Pengurusan dan Operasi Perkhidmatan GPKI

5. Peranan dan tanggungjawab bagi setiap pihak yang terlibat dalam Model Pengurusan dan Operasi Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) diterangkan dalam **Jadual 1**.

Bil.	Entiti	Peranan	Tanggungjawab
i.	Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM)	Pengawal Selia Akta Tandatangan Digital 1997	Badan Kerajaan yang mengawal selia CA seperti termaktub dalam Akta Tandatangan Digital 1997 dan *Digital Signature Regulations* 1998.
ii.	Pihak Berkuasa Pemerakuan Berlesen (CA)	Pihak pengeluar sijil digital	Pihak berlesen mengeluarkan sijil digital yang sah berdasarkan Akta Tandatangan Digital 1997 dan *Digital Signature Regulations* 1998.
iii.	Pihak Berkuasa Pendaftaran (RA)	Pihak pengesah permohonan sijil digital	RA pihak yang dilantik oleh CA bagi menjalankan kerja semakan permohonan dan mengesahkan pengeluaran sijil digital sebelum dikeluarkan oleh CA.
iv.	Agensi pusat	Pentadbir (Admin)	Pentadbir Portal GPKI bagi perkhidmatan GPKI dan melantik SA dan PS.
v.	Agensi pelaksana	SubPentadbir (SA)	Pentadbir Portal GPKI di agensi pelaksana bertanggungjawab untuk mengemukakan pelantikan dan penamatan AP serta mengurus permohonan pengguna di agensi-agensi.
vi.	Agensi pelaksana	Pentadbir Pelayan (PS)	Pentadbir dan pengurus permohonan sijil digital pelayan.
vii.	Agensi sektor awam	Pegawai Diberi Kuasa (AP)	AP menguruskan pendaftaran dan permohonan sijil digital pengguna agensi sektor awam.
viii.	Penjawat awam	Pengguna aplikasi agensi pelaksana	Pegawai yang diberi kebenaran untuk menggunakan sijil digital pengguna bagi membuat pengesahan, penyulitan dan tandatangan digital terhadap data dan maklumat aplikasi agensi pelaksana.

Jadual 1: Peranan dan Tanggungjawab

PERKHIDMATAN GPKI

6. Berdasarkan Model Pengurusan dan Operasi Prasarana Kunci Awam Kerajaan (GPKI), MAMPU berperanan sebagai agensi peneraju bagi perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI). Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) yang disediakan oleh MAMPU meliputi perkara-perkara yang berikut:

(i) Pengurusan Sijil Digital yang merangkumi penyelarasan dengan Pihak Berkuasa Pemerakuan Berlesen (CA) bagi proses-proses pengeluaran, pembaharuan dan pembatalan sijil digital, pengurusan pentadbir Prasarana Kunci Awam Kerajaan (GPKI) dan pengguna serta sokongan teknikal; dan

(ii) Khidmat nasihat dan konsultasi bagi perancangan dan pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI).

7. Keterangan mengenai jenis dan sasaran penerima perkhidmatan adalah seperti **Jadual 2**.

BIL.	JENIS PERKHIDMATAN	SASARAN PENERIMA	
		AGENSI PELAKSANA	AGENSI SEKTOR AWAM
i.	Permohonan Perkhidmatan GPKI	□	-
ii.	Pengurusan Pengeluaran Sijil Digital	□	□
iii.	Capaian Perkhidmatan GPKI Melalui Portal GPKI	□	□
iv.	Sokongan Teknikal Perkhidmatan GPKI	□	□
v.	Konsultasi Bagi Perancangan dan Pelaksanaan GPKI	□	-

Jadual 2: Jenis Dan Sasaran Penerima Perkhidmatan GPKI

Permohonan Perkhidmatan GPKI

8. Agensi pelaksana yang memerlukan permohonan baharu perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) hendaklah melaksanakan penilaian risiko berpandukan Garis Panduan Teknikal Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) dan mengemukakan Laporan Penilaian Risiko berserta surat permohonan rasmi seperti di **Lampiran A2: Contoh Surat Permohonan Perkhidmatan GPKI** kepada MAMPU. Proses permohonan baharu perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) ditunjukkan dalam carta alir seperti **Lampiran B2: Carta Alir Proses Permohonan Baharu Perkhidmatan GPKI**.

Pengurusan Pengeluaran Sijil Digital

9. Pengurusan pengeluaran sijil digital meliputi permohonan baharu, pembaharuan dan pembatalan sijil digital. Pihak yang terlibat dalam proses pengeluaran sijil digital ialah agensi pusat, agensi pelaksana, agensi sektor awam, pihak berkuasa pendaftaran dan Pihak Berkuasa Pemerakuan Berlesen (CA).

Proses Pengeluaran Sijil Digital

10. Proses pengeluaran sijil digital diterangkan dalam carta alir seperti **Lampiran C: Carta Alir Proses Pengeluaran Sijil Digital**. Maklumat lanjut mengenai proses yang terlibat boleh diperoleh oleh Pentadbir Portal GPKI daripada dokumen **Manual Pengguna Sijil Perisian (Softcert), Manual Pengguna Kad Pintar, Manual Pengguna Token dan Manual Pengguna Pentadbir Pelayan (PS)**. Dalam melaksanakan proses pengeluaran sijil digital, semua pihak yang terlibat perlu memberi perhatian kepada perkara-perkara penting yang berikut:

(i) Sebelum membuat permohonan sijil digital, semua pengguna sistem aplikasi perlu melalui proses pendaftaran profil pengguna yang diuruskan oleh agensi pelaksana;

(ii) Terdapat dua (2) jenis sijil digital yang dikeluarkan, iaitu sijil digital pengguna dan sijil digital pelayan. **Tempoh sah laku** bagi sijil digital pengguna **ialah 25 bulan** manakala tempoh sah laku sijil digital pelayan **ialah antara 12 bulan** hingga **24 bulan** tertakluk pada polisi Pihak Berkuasa Pemerakuan Berlesen (CA) yang berkenaan;

(iii) Agensi pusat menyediakan sijil digital dalam medium kad pintar, token dan Sijil Perisian (softcert);

(iv) Bagi permohonan pembaharuan sijil digital yang menggunakan token, pengguna perlu memuat turun sijil digital baharu dan memasukkan (inject) sijil tersebut ke dalam token manakala sijil digital yang menggunakan kad pintar, kad baharu akan dikeluarkan bagi permohonan pembaharuan sijil digital;

(v) Sijil digital dalam bentuk Sijil Perisian (softcert) hanya dibenarkan dimuat turun sekali sahaja;

(vi) Agensi pusat hanya menyediakan sijil digital pelayan berbentuk Sijil Perisian (softcert) secara **khusus mengikut domain yang didaftarkan**. Agensi pelaksana perlu mengemukakan permohonan kepada agensi pusat melalui surat rasmi bagi menggunakan perkhidmatan pembekalan sijil digital pelayan yang disediakan;

(vii) Dalam operasi sijil digital pelayan, Pentadbir Pelayan (PS) yang bertanggungjawab perlu memastikan fail Permintaan Tandatangan Sijil [Certificate Signing Request (CSR)] dijana di pelayan terlibat sahaja. Selain daripada itu, Pentadbir Pelayan (PS) juga perlu memastikan kunci persendirian (private key) sijil digital pelayan dengan kaedah menyimpan kunci tersebut bagi perlindungan maklumat Rahsia Rasmi mengikut Arahan Keselamatan. Kawalan keselamatan ini perlu bagi mengelakkan berlakunya penyalinan sijil digital secara tidak sah yang akan membawa implikasi ketidakbolehpercayaan terhadap pelayan tersebut;

(viii) Dalam operasi sijil digital pelayan, Pentadbir Pelayan (PS) yang bertanggungjawab perlu memastikan:

(a) Fail Permintaan Tandatangan Sijil (CSR) dijana di pelayan yang terlibat sahaja; dan

(b) Kaedah menyimpan kunci persendirian (private key) sijil digital pelayan mengikut Arahan Keselamatan. Kawalan keselamatan ini perlu bagi melindungi maklumat rahsia rasmi dan mengelakkan berlakunya penyalinan sijil digital secara tidak sah yang akan membawa implikasi ketidakbolehpercayaan terhadap pelayan tersebut.

(ix) Pengguna **bertanggungjawab** untuk memastikan:

(a) Sijil digital disimpan dengan selamat dan tidak dipindah milik. Akta Tandatangan Digital 1997 **tidak membenarkan** sijil pengguna atau sijil digital pelayan untuk dipindah milik kerana sijil digital tersebut merupakan identiti pengguna atau pelayan dalam ruang siber;

(b) Sijil digital kad pintar atau/dan token dibawa bersama apabila pengguna bertukar agensi; dan

(c) Salinan sijil bagi Sijil Perisian (softcert) dalam komputer riba atau komputer peribadi dihapuskan apabila tidak lagi bertanggungjawab atas komputer tersebut.

Penggantian dan Pembatalan Sijil Digital Pengguna

11. Pemegang sijil digital perlu memaklumkan atau memulangkan kepada agensi pusat menerusi Pihak Berkuasa Pendaftaran (RA), medium sijil digital yang rosak, tamat tempoh, tamat perkhidmatan, bersara atau disalahgunakan. Pemegang sijil digital perlu mengambil tindakan seperti yang berikut:

(i) **Kad Pintar/Token yang Rosak**

Kad pintar atau token yang rosak perlu dipulangkan oleh pemegang sijil digital kepada agensi pusat menerusi AP. AP perlu mengemukakan kad pintar atau token yang rosak berserta surat rasmi seperti **Lampiran D: Contoh Surat Permohonan Penggantian Kad Pintar/Token** kepada agensi pusat**.** Sekiranya kad pintar atau token disahkan rosak, pemegang sijil digital perlu membuat permohonan penggantian melalui Portal GPKI selepas Pihak Berkuasa Pendaftar (RA) membuat pembatalan kad pintar atau token yang rosak dan disahkan oleh Subpentadbir (SA).

(ii) **Kad Pintar/Token yang Hilang atau Disalahgunakan oleh Pihak Ketiga**

Kad pintar atau token yang hilang **perlu** dilaporkan oleh pemegang sijil digital kepada Pihak Berkuasa Pendaftaran (RA). Pihak Berkuasa Pemerakuan Berlesen (CA) perlu mengemukakan surat tunjuk sebab seperti **Lampiran E: Contoh Surat Tunjuk Sebab Kehilangan Kad Pintar/Token** kepada agensi pusat. Pemegang sijil digital membuat permohonan penggantian sijil digital melalui Portal GPKI selepas Pihak Berkuasa Pendaftaran (RA) membuat pembatalan kad pintar atau token yang hilang dan disahkan oleh Subpentadbir (SA).

(iii) **Penyalahgunaan oleh Pemegang Sijil Digital Pengguna**

Sekiranya penyalahgunaan sijil digital dikesan oleh pihak agensi sektor awam, Pihak Berkuasa Pemerakuan Berlesen (CA) perlu mengambil tindakan seperti yang berikut:

(a) Melapor dan mengemukakan surat rasmi seperti **Lampiran F: Contoh Surat Makluman Penyalahgunaan oleh Pemegang Sijil Digital** kepada agensi pusat; dan

(b) Membuat permohonan pembatalan sijil digital berkenaan dan disahkan oleh Subpentadbir (SA).

(iv) **Pengguna yang Tamat Perkhidmatan/Bersara**

Pengguna yang tamat perkhidmatan atau bersara, Pegawai Diberi Kuasa (AP) perlu mengambil tindakan seperti yang berikut:

(a) Melapor dan mengemukakan surat rasmi seperti **Lampiran G: Contoh Surat Makluman Tamat Perkhidmatan/Bersara** kepada agensi pusat bagi tujuan pembatalan sijil digital pengguna; dan

(b) Membuat permohonan pembatalan sijil digital berkenaan dan disahkan oleh Subpentadbir (SA).

Capaian Perkhidmatan GPKI melalui Portal GPKI

12. Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) oleh agensi pusat dimudahcarakan melalui Portal GPKI. Perkhidmatan yang Disediakan melalui Portal GPKI adalah:

(i) Permohonan sijil digital pengguna;

(ii) Pembatalan sijil digital pengguna;

(iii) Permohonan sijil digital pelayan;

(iv) Permohonan pembaca kad pintar;

(v) Semakan status permohonan;

(vi) Penjanaan laporan untuk Pentadbir (Admin); dan

(vii) Pendaftaran pentadbir dan lain-lain.

Panduan Penggunaan Portal GPKI

13. Pengguna Portal GPKI boleh menggunakan perkhidmatan tersebut setelah didaftarkan oleh Pentadbir Portal GPKI. Pengguna boleh merujuk panduan-panduan seperti yang berikut:

(i) Panduan Pengguna Pengguna Akhir;

(ii) Panduan Pengguna Pegawai Diberi Kuasa (AP);

(iii) Panduan Pengguna Pentadbir Pelayan (PS);

(iv) Panduan Pengguna Subpentadbir (SA);

(v) Panduan Pengguna Pentadbir (Admin); dan

(vi) Prosedur Operasi Standard Perkhidmatan GPKI (Pengurusan Sijil Digital).

Kawalan Akses Portal GPKI

14. Kawalan akses Portal GPKI dilaksanakan pada tiga (3) peringkat kawalan:

(i) Agensi pusat oleh Pentadbir (Admin);

(ii) Agensi pelaksana oleh Subpentadbir (SA); dan

(iii) Agensi sektor awam oleh Pegawai Diberi Kuasa (AP).

Sokongan Teknikal Perkhidmatan GPKI

15. Sokongan teknikal perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) diberikan oleh agensi pusat kepada agensi pelaksana dan agensi sektor awam melalui khidmat meja bantuan dan bantuan di lokasi pengguna. Sokongan Teknikal ini meliputi khidmat nasihat teknikal Portal GPKI dan penggunaan sijil digital serta penyelesaian masalah operasi

Prasarana Kunci Awam Kerajaan (GPKI). Maklumat mengenai perkara ini boleh dirujuk dalam dokumen **Panduan Pengguna Kad Pintar, Panduan Pengguna Token** dan **Panduan Pengguna Pegawai Diberi Kuasa (AP)** yang boleh diperoleh secara dalam talian dalam Portal GPKI.

16. Pengguna yang memerlukan khidmat nasihat teknikal atau mempunyai sebarang pertanyaan berkaitan dengan perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) perlu merujuk kepada Pegawai Diberi Kuasa (AP) terlebih dahulu. Sekiranya Pegawai Diberi Kuasa (AP) memerlukan bantuan tambahan, rujukan boleh dibuat kepada Subpentadbir (SA) dan seterusnya kepada Meja Bantuan GPKI. Maklumat perhubungan kepada Meja Bantuan GPKI boleh diperoleh melalui Portal GPKI.

Konsultasi Bagi Perancangan dan Pelaksanaan GPKI

17. Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) dilaksanakan oleh Bahagian Pembangunan Perkhidmatan Gunasama, Infrastruktur dan Keselamatan ICT di MAMPU dan dipantau oleh Jawatankuasa Pelaksanaan Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI). MAMPU memberikan konsultasi bagi perkara seperti yang berikut:

(i) Penggunaan Prasarana Kunci Awam (PKI) di dalam sistem ICT kerajaan;

(ii) Konsultasi integrasi aplikasi kerajaan dan Prasarana Kunci Awam Kerajaan (GPKI);

(iii) Perancangan dan pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI); dan

(iv) Latihan kepada Pentadbir Prasarana Kunci Awam Kerajaan (GPKI).

18. Carta alir yang menggambarkan tadbir urus dan proses kerja permohonan konsultasi adalah seperti **Lampiran H: Carta Alir Proses Permohonan Khidmat Nasihat dan Konsultasi**.

PEMILIKAN SIJIL DIGITAL INDIVIDU

19. Secara dasarnya, seorang pengguna hanya boleh memiliki satu sijil digital sahaja. Dalam keadaan pengguna tersebut perlu membuat capaian lebih daripada satu sistem aplikasi yang mempunyai keperluan medium sijil digital yang berbeza, pengguna tersebut perlu dibekalkan dengan medium sijil digital yang mempunyai tahap keselamatan yang lebih tinggi.

20. **Jadual 3: Penentuan Medium Sijil Digital Mengikut Keperluan Sistem Aplikasi** memberikan panduan kepada pengguna baharu atau sedia ada mengenai penentuan medium sijil digital yang sesuai digunakan. Rujukan tambahan bagi pemilihan medium sijil digital boleh diperoleh dalam Garis Panduan Teknikal Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI).

Keperluan Tahap Kawalan Keselamatan Sistem Aplikasi	Jenis Medium Sijil Digital yang Dimiliki oleh Pengguna	Perlu Pertukaran Medium	Jenis Medium Sijil Digital yang Diperlukan (Berdasarkan Keperluan Khusus Sistem Aplikasi)
Tinggi	Kad Pintar atau Token	Tidak	Tidak berkenaan
	Sijil Digital Perayauan	Ya	Kad Pintar atau Token
	softcert	Ya	Kad Pintar atau Token
Sederhana	Kad Pintar atau Token	Tidak	Tidak berkenaan
	Sijil Digital Perayauan	Tidak	
	softcert	Tidak	

Jadual 3: Penentuan Medium Sijil Digital Mengikut Keperluan Sistem Aplikasi

PENUTUP

21. Agensi **hendaklah** mematuhi garis panduan ini bagi memahami proses operasi perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) dengan lebih jelas. Dokumen ini **hendaklah** dibaca bersama dengan Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) dan Garis Panduan Teknikal Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI).

LAMPIRAN A2

Contoh Surat Permohonan Perkhidmatan GPKI

< No. Rujukan Surat Agensi >
<Tarikh>

Pengarah,
Bahagian Pembangunan Perkhidmatan Guna Sama
Infrastruktur dan Keselamatan ICT (BPG),
Unit Pemodenan Tadbiran dan Perancangan
Pengurusan Malaysia (MAMPU),
Jabatan Perdana Menteri,
Aras 1, Blok B, Bangunan MKN-EMBASSY Techzone,
Jalan Teknokrat 2, 63000 Cyberjaya, Sepang,
SELANGOR.

Tuan,

PERMOHONAN MENGGUNAKAN PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN [GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)] BAGI SISTEM < nama sistem >

Dengan hormatnya saya merujuk kepada perkara di atas.

2. Sukacita dimaklumkan bahawa <nama agensi, kementerian> ingin memohon menggunakan perkhidmatan GPKI bagi sistem < nama sistem >.

3. Maklumat mengenai sistem dan skop perkhidmatan yang diperlukan adalah seperti yang berikut:

(a) **Keterangan Sistem** : Nyatakan ringkasan mengenai sistem dan tujuan penggunaan sistem.

Contoh:
Ringkasan sistem
Sistem Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)] merupakan

			sistem permohonan perkhidmatan PKI yang disediakan oleh MAMPU. **Tujuan** Tujuan penggunaan API PKI adalah bagi membuat tandatangan digital pada borang permohonan kad pintar selaras dengan keperluan Akta Tandatangan Digital 1997. Sila lampirkan aliran proses yang memerlukan penggunaan PKI.
(b)	**API yang diperlukan**	:	tandatangan digital/pengesahan penyulitan/penyahsulitan
(c)	**Medium sijil digital pengguna yang akan digunakan**	:	sijil digital perayauan/sijil perisian (softcert)/kad pintar/token
(d)	**Jumlah sijil digital pengguna yang diperlukan**	:	XX unit
(e)	**Jumlah sijil ujian yang diperlukan**	:	XX unit
(f)	**Jumlah sijil digital pelayan yang diperlukan**	:	XX unit
(g)	**Nama domain**	:	<Nama domain sistem: >
(h)	**Capaian ke sistem**	:	Melalui Internet/Intranet

4. Bersama-sama ini juga disertakan Laporan Penilaian Risiko untuk makluman tuan. Sehubungan dengan itu, kerjasama tuan dalam mempertimbangkan dan meluluskan permohonan ini didahului dengan ucapan terima kasih.

Sekian.

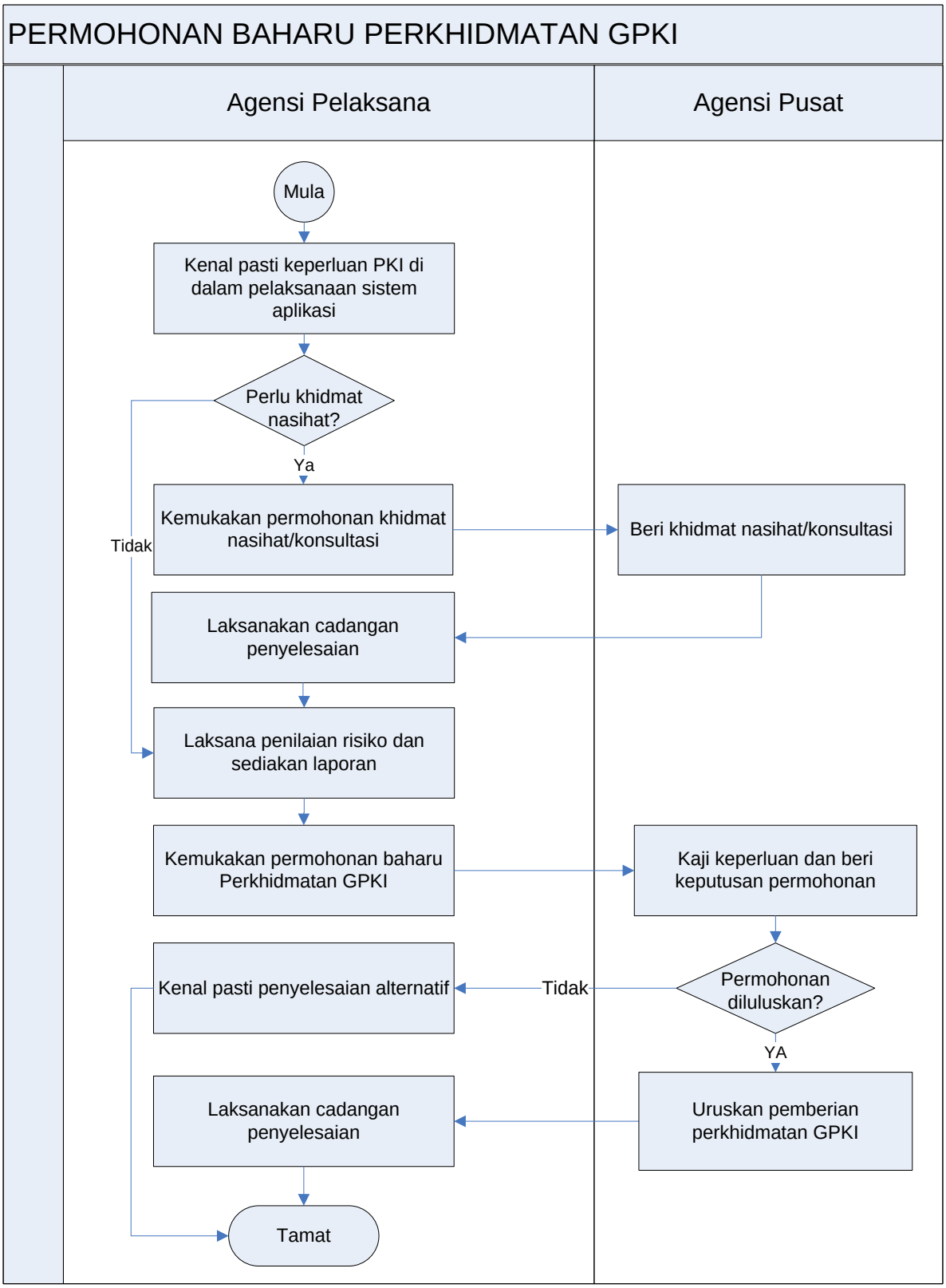
“BERKHIDMAT UNTUK NEGARA”

Saya yang menurut perintah,

< Nama >
< Jawatan >
< Nama agensi >
Telefon :
Faks :
E-mel :

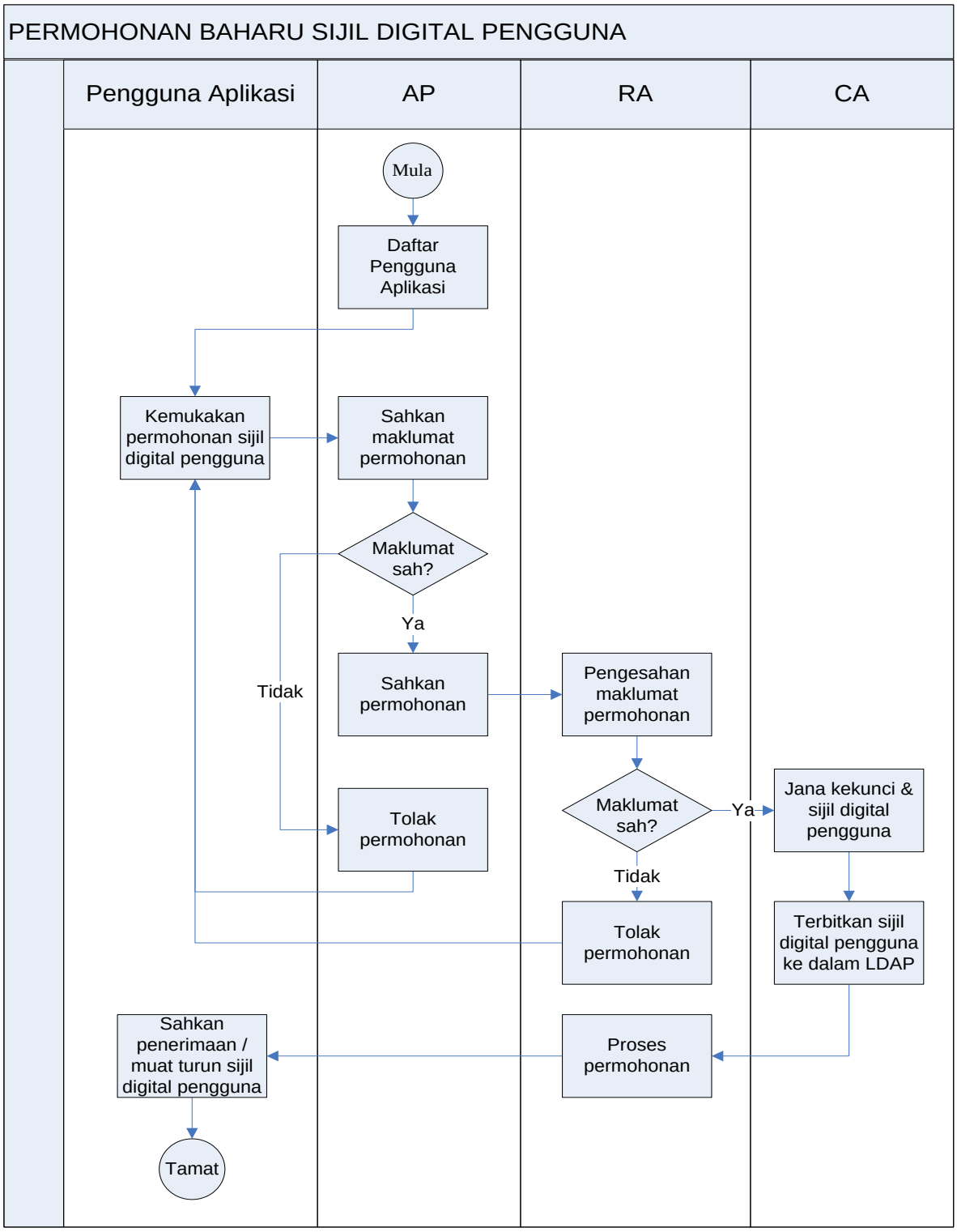
LAMPIRAN B2

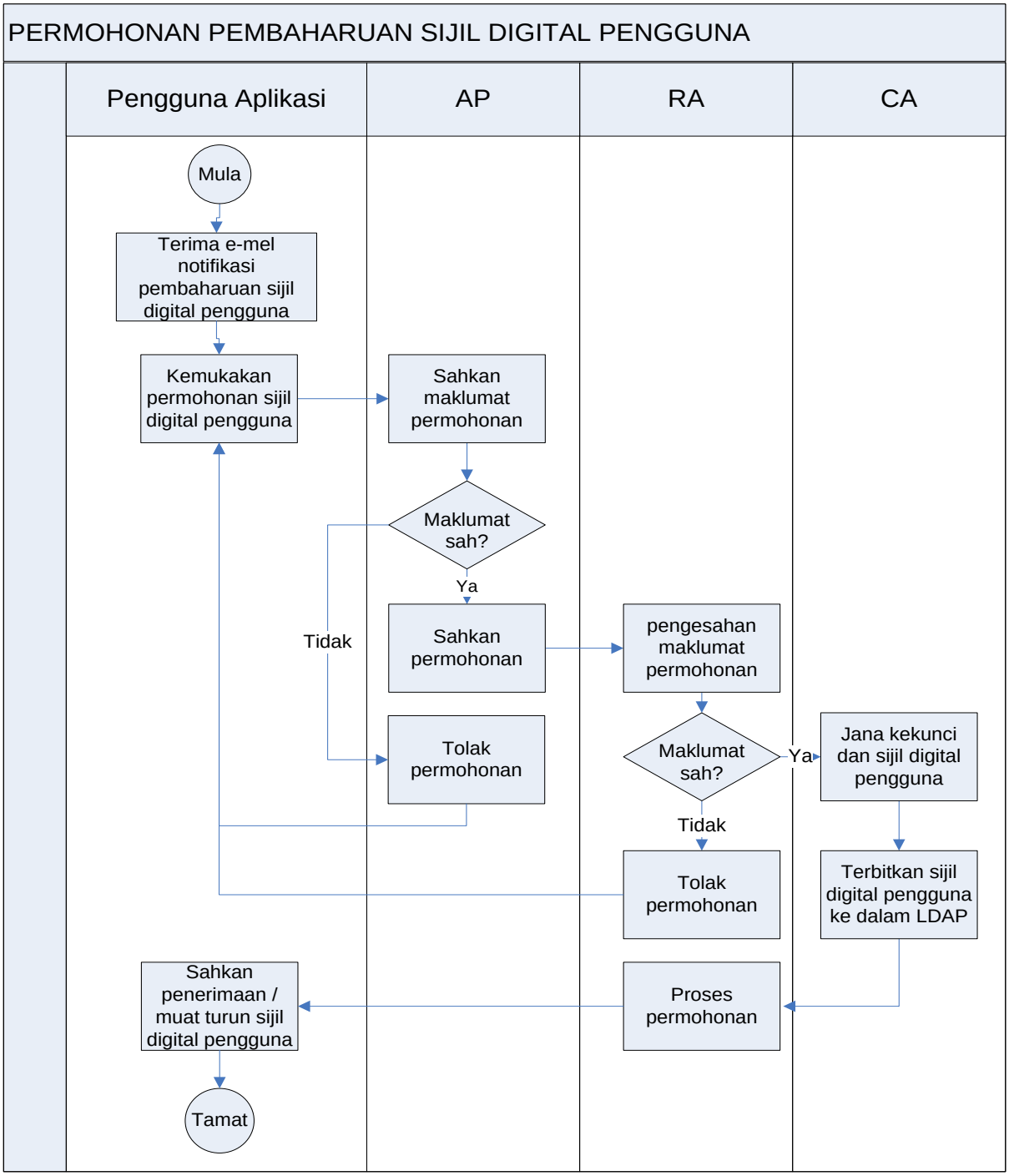
Carta Alir Proses Permohonan Baharu Perkhidmatan GPKI

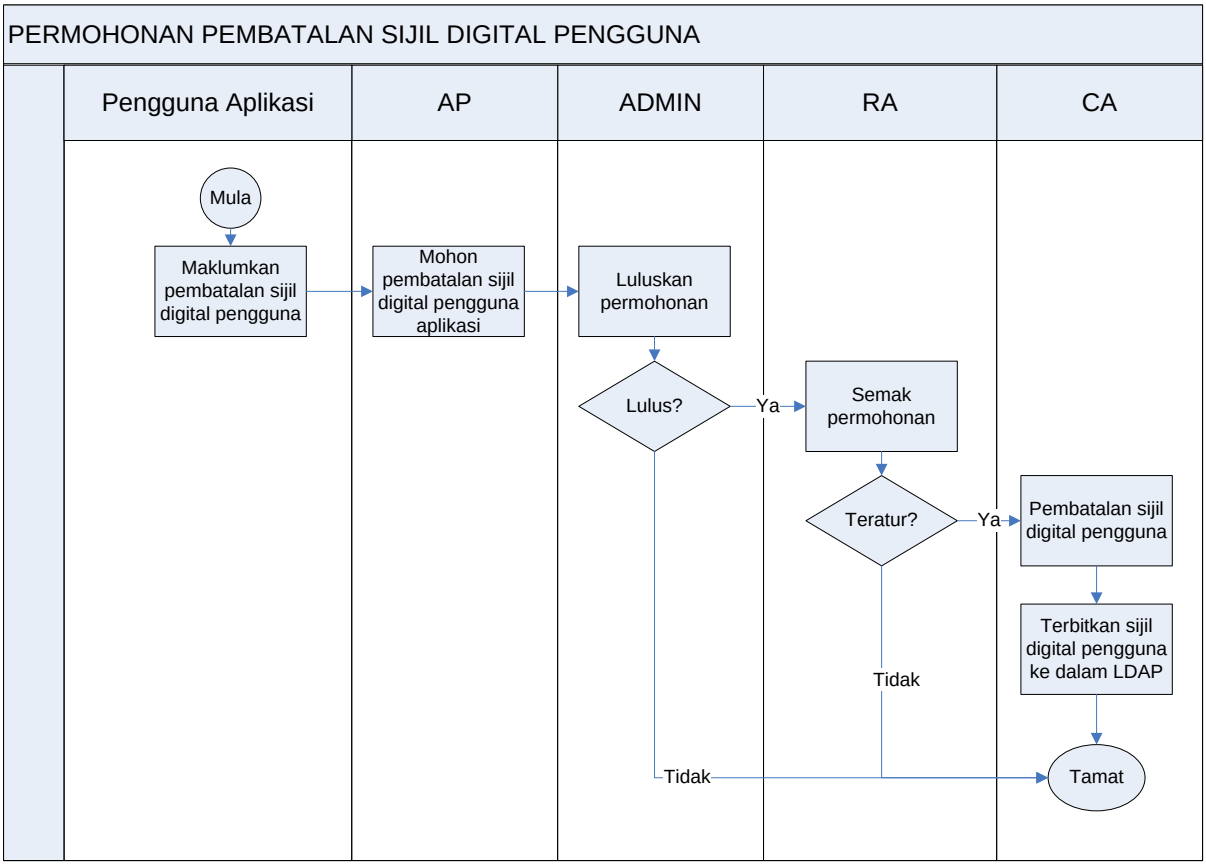


LAMPIRAN C

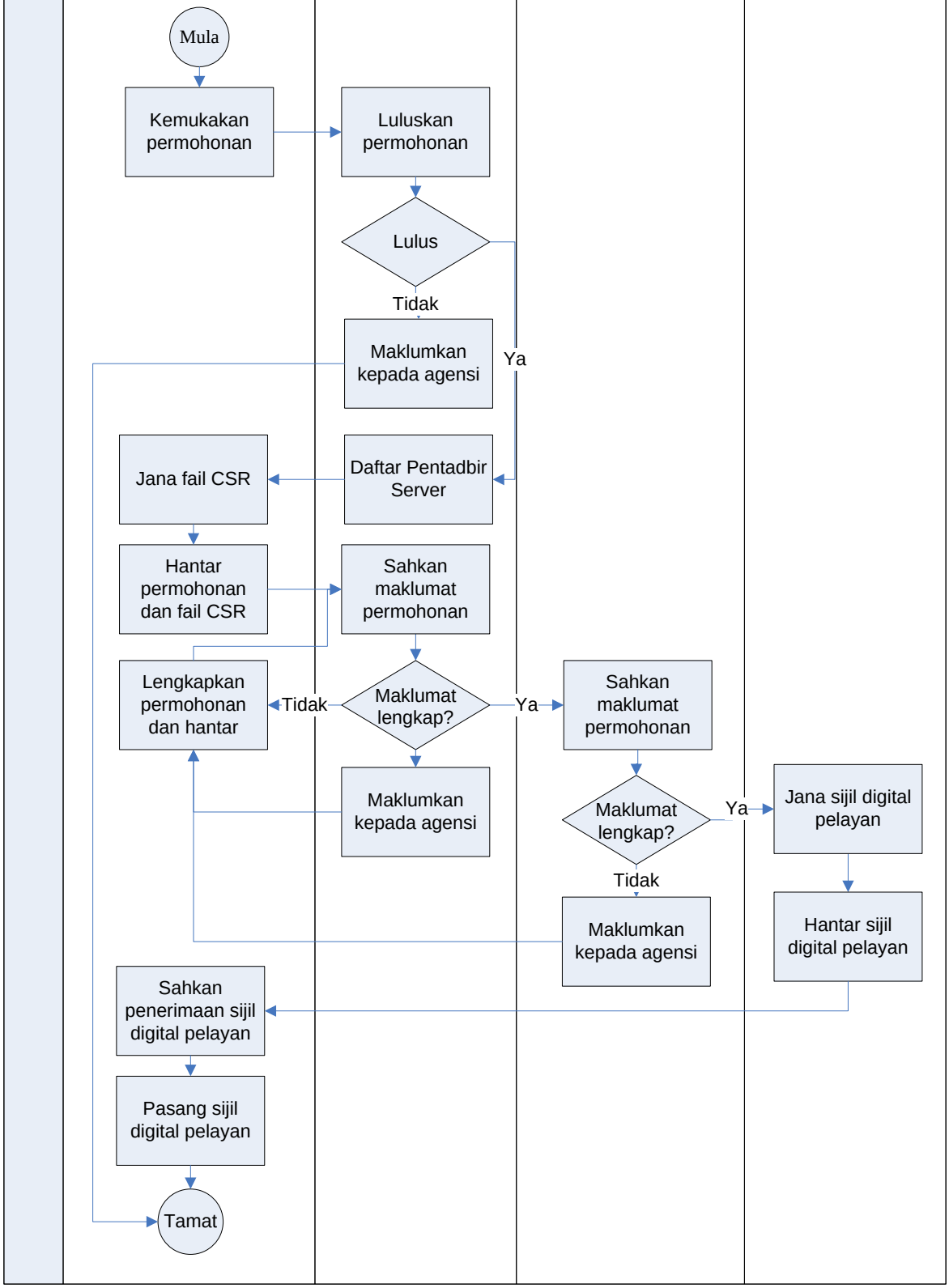
Carta Alir Proses Pengeluaran Sijil Digital

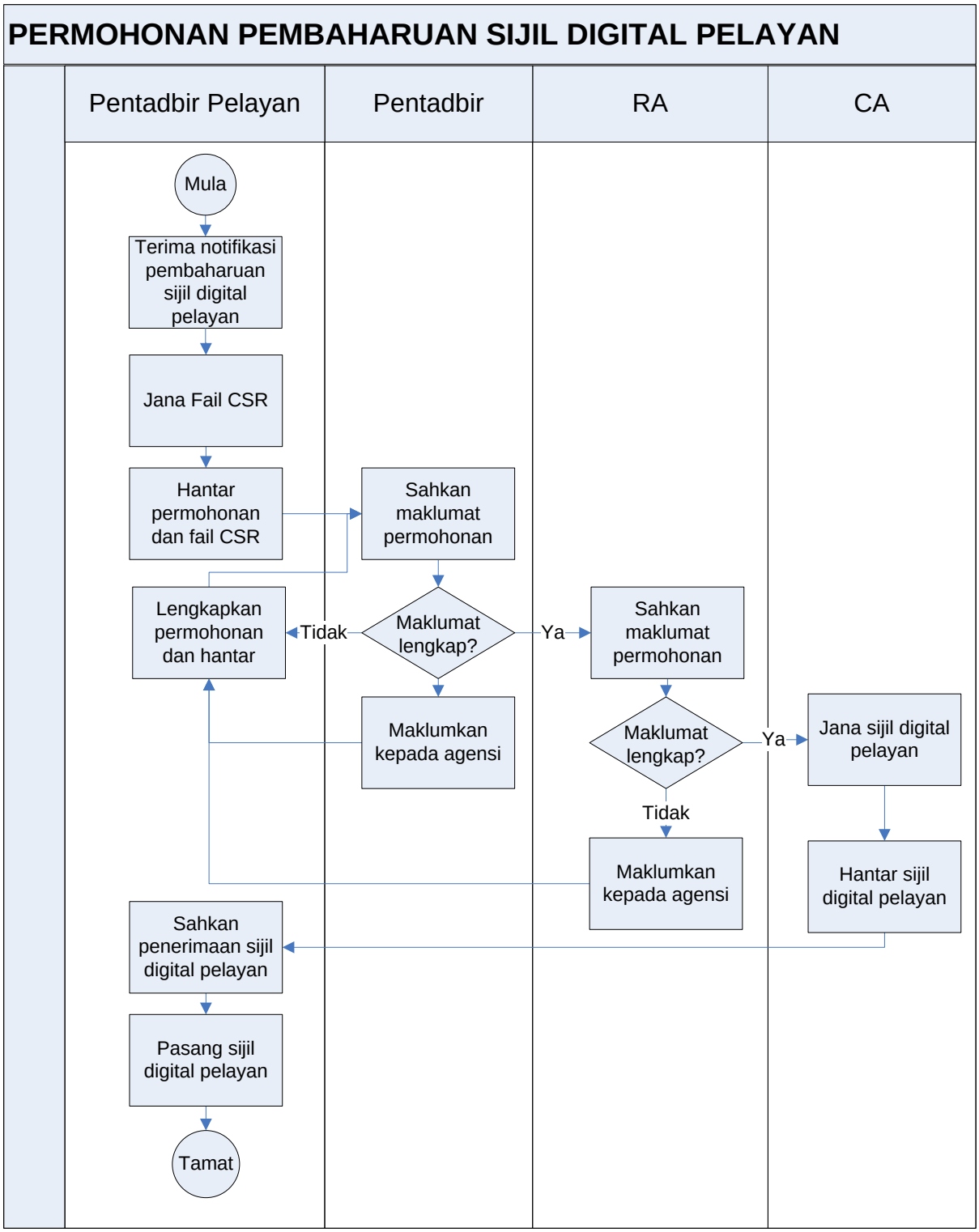



PERMOHONAN PEMBAHARUAN SIJIL DIGITAL PENGGUNA
Pengguna Aplikasi
AP
RA
CA
Mula
Terima e-mel notifikasi pembaharuan sijil digital pengguna
Kemukakan permohonan sijil digital pengguna
Sahkan maklumat permohonan
Maklumat sah?
Ya
Tidak
Sahkan permohonan
Tolak permohonan
pengesahan maklumat permohonan
Maklumat sah?
Ya
Tidak
Jana kekunci dan sijil digital pengguna
Tolak permohonan
Terbitkan sijil digital pengguna ke dalam LDAP
Proses permohonan
Sahkan penerimaan / muat turun sijil digital pengguna
Tamat


PERMOHONAN PEMBATALAN SIJIL DIGITAL PENGGUNA
Pengguna Aplikasi
AP
ADMIN
RA
CA
Mula
Maklumkan pembatalan sijil digital pengguna
Mohon pembatalan sijil digital pengguna aplikasi
Luluskan permohonan
Lulus?
Ya
Semak permohonan
Teratur?
Ya
Pembatalan sijil digital pengguna
Terbitkan sijil digital pengguna ke dalam LDAP
Tidak
Tidak
Tamat

PERMOHONAN BAHARU SIJIL DIGITAL PELAYAN




PERMOHONAN PEMBAHARUAN SIJIL DIGITAL PELAYAN
Pentadbir Pelayan
Pentadbir
RA
CA
Mula
Terima notifikasi pembaharuan sijil digital pelayan
Jana Fail CSR
Hantar permohonan dan fail CSR
Sahkan maklumat permohonan
Lengkapkan permohonan dan hantar
Tidak
Maklumat lengkap?
Ya
Sahkan maklumat permohonan
Maklumkan kepada agensi
Maklumat lengkap?
Ya
Jana sijil digital pelayan
Tidak
Maklumkan kepada agensi
Hantar sijil digital pelayan
Sahkan penerimaan sijil digital pelayan
Pasang sijil digital pelayan
Tamat

LAMPIRAN D

Contoh Surat Permohonan Penggantian Kad Pintar/Token

Rujukan Surat :
Tarikh :

Pengarah
Bahagian Pembangunan Perkhidmatan Guna Sama
Infrastruktur dan Keselamatan ICT (BPG),
Unit Pemodenan Tadbiran dan Perancangan
Pengurusan Malaysia(MAMPU),
Jabatan Perdana Menteri,
Aras 1, Blok B, Bangunan MKN-EMBASSY Techzone,
Jalan Teknokrat 2, 63000 Cyberjaya, Sepang,
SELANGOR.

Tuan,

PERMOHONAN PENGGANTIAN KAD PINTAR/TOKEN ROSAK

Dengan hormatnya saya merujuk perkara di atas.

2. Untuk makluman tuan, kad pintar/token pengguna yang dilampirkan didapati telah rosak. Butiran maklumat pengguna adalah seperti yang berikut:

Nama Pemegang Kad Pintar/Token	:
No. Kad Pengenalan	:
No. Kad Pintar/ No. Siri Token	:
Keterangan Kerosakan	:

3. Bersama-sama ini dikembalikan kad pintar/token pengguna tersebut untuk semakan dan penggantian oleh pihak tuan. Untuk makluman tuan, permohonan melalui Portal GPKI telah disahkan pada (tarikh). Kerjasama tuan dalam perkara ini didahului dengan ucapan terima kasih.

Sekian.

Saya yang menurut perintah,

(Nama Pegawai Diberi Kuasa (AP))
(Jawatan)
Telefon :
E-mel :

LAMPIRAN E

Contoh Surat Tunjuk Sebab Kehilangan Kad Pintar/Token

Rujukan Surat :
Tarikh :

Pengarah
Bahagian Pembangunan Perkhidmatan Guna Sama
Infrastruktur dan KeselamatanICT (BPG),
Unit Pemodenan Tadbiran dan Perancangan
Pengurusan Malaysia (MAMPU),
Jabatan Perdana Menteri,
Aras 1, Blok B, Bangunan MKN-EMBASSY Techzone,
Jalan Teknokrat 2, 63000 Cyberjaya, Sepang,
SELANGOR.

Tuan,

PENGESAHAN KEHILANGAN KAD PINTAR/TOKEN

Dengan hormatnya saya merujuk perkara di atas.

2. Untuk makluman tuan, kad pintar pengguna yang dilampirkan didapati telah hilang. Kehilangan kad ini merupakan kehilangan kali.....(contoh: pertama). Butiran maklumat pengguna adalah seperti yang berikut:

Nama Pemegang Kad Pintar/Token	:
No. Kad pengenalan	:
Tarikh Hilang	:
Lokasi Kehilangan Kad Pintar/Token	:
Sebab Hilang	:

3. Sehubungan dengan itu, saya amat berbesar hari sekiranya penggantian bagi kad pintar/token tersebut dapat dipertimbangkan. Kerjasama awal dan perhatian tuan dalam perkara ini didahului dengan ucapan terima kasih.

Sekian.

Saya yang menurut perintah,

(Nama Pegawai Diberi Kuasa (AP))
(Jawatan)
Telefon :
E-mel :

LAMPIRAN F

Contoh Surat Makluman Penyalahgunaan Sijil Digital oleh Pemegang Sijil Digital

Rujukan Surat :
Tarikh :

Pengarah
Bahagian Pembangunan Perkhidmatan Guna Sama
Infrastruktur dan Keselamatan ICT (BPG),
Unit Pemodenan Tadbiran dan Perancangan
Pengurusan Malaysia (MAMPU),
Jabatan Perdana Menteri,
Aras 1, Blok B, Bangunan MKN-EMBASSY Techzone,
Jalan Teknokrat 2, 63000 Cyberjaya, Sepang,
SELANGOR.

Tuan,

MAKLUMAN PENYALAHGUNAAN SIJIL DIGITAL PENGGUNA

Dengan hormatnya saya merujuk perkara di atas.

2. Untuk makluman tuan, kad pintar pengguna yang dilampirkan didapati telah disalahgunakan oleh individu lain bagi tujuan ..... Butiran maklumat pengguna adalah seperti yang berikut:

Nama Pemegang Kad :
No. Kad pengenalan :

3. Sehubungan dengan itu, sukacita sekiranya pihak tuan dapat membatalkan sijil digital pengguna tersebut. Perhatian tuan dalam perkara ini didahului dengan ucapan terima kasih.

Sekian.

Saya yang menurut perintah,

(Nama Pegawai Diberi Kuasa (AP))
(Jawatan)
Telefon :
E-mel :

LAMPIRAN G

CONTOH SURAT MAKLUMAN TAMAT PERKHIDMATAN/BERSARA

Rujukan Surat :
Tarikh :

Pengarah
Bahagian Pembangunan Perkhidmatan Guna Sama
Infrastruktur dan Keselamatan ICT (BPG),
Unit Pemodenan Tadbiran dan
PerancanganPengurusan Malaysia (MAMPU),
Jabatan Perdana Menteri,
Aras 1, Blok B, Bangunan MKN-EMBASSY Techzone,
Jalan Teknokrat 2, 63000 Cyberjaya, Sepang,
SELANGOR.

Tuan,

MAKLUMAN TAMAT PERKHIDMATAN/BERSARA

Dengan hormatnya saya merujuk perkara di atas.

2. Untuk makluman tuan, pengguna dibawah telah tamat perkhidmatan/ bersara. Butiran maklumat pengguna adalah seperti yang berikut:

Nama Pengguna :
No. Kad pengenalan :

3. Perhatian tuan dalam perkara ini didahului dengan ucapan terima kasih.

Sekian.

Saya yang menurut perintah,

(Nama Pegawai Diberi Kuasa (AP))
(Jawatan)
Telefon :
E-mel :

LAMPIRAN H

CARTA ALIR PROSES
PERMOHONAN KHIDMAT NASIHAT DAN KONSULTASI