KERAJAAN MALAYSIA

PEKELILING PENDIGITALAN PERKHIDMATAN AWAM BILANGAN 4 TAHUN 2025

DASAR PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN (*GOVERNMENT PUBLIC KEY INFRASTRUCTURE* – MyGPKI)

JABATAN DIGITAL NEGARA
KEMENTERIAN DIGITAL

KANDUNGAN

KETUA SETIAUSAHA NEGARA
MALAYSIA
Jabatan Perdana Menteri
Aras 4 Blok Timur, Bangunan Perdana Putra
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya

Tel : 03-8872 7211
Faks : 03-8889 4479

Rujukan : JDN.100-1/3/1 (15)
Tarikh : 12 Ogos 2025

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

PEKELILING PENDIGITALAN PERKHIDMATAN AWAM
BILANGAN 4 TAHUN 2025

DASAR PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN (*GOVERNMENT PUBLIC KEY INFRASTRUCTURE* – MyGPKI)

TUJUAN

1. Pekeliling ini bertujuan untuk menjelaskan Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* – MyGPKI) kepada Agensi Sektor Awam bagi memantapkan tahap keselamatan data dan maklumat sistem teknologi maklumat dan komunikasi (*Information and Communications Technology* – ICT) serta meningkatkan kecekapan dan keberkesanan sistem penyampaian kerajaan.

LATAR BELAKANG

2. Prasarana Kunci Awam (*Public Key Infrastructure* – PKI) ialah gabungan perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan komunikasi dan transaksi urus niaga secara dalam talian. PKI digunakan bagi tujuan pengesahan identiti pengguna, penyulitan maklumat dan

tandatangan digital dalam Sistem ICT Kerajaan dengan memenuhi ciri-ciri keselamatan maklumat sepertimana yang dinyatakan dalam Arahan Teknologi Maklumat 2007 seperti berikut:

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

b. **kesahihan (*authenticity*)** iaitu jaminan bahawa sesuatu subjek iaitu pengguna, program atau proses telah dikenal pasti dan disahkan dengan suatu set pengenalan, berbanding dengan maklumat yang telah disimpan bagi memastikan bahawa subjek berkenaan ialah entiti seperti yang didakwa.

c. **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 integriti.

d. **tanpa sangkalan (*non-repudiation*)** iaitu keperluan bagi membuktikan integriti dan punca data boleh disahkan daripada penafian penglibatan tindakan sebelumnya. Tidak boleh disangkal dapat dilaksanakan secara kriptografi dengan penggunaan tandatangan digital.

3. Jabatan Digital Negara (JDN) yang merupakan agensi Peneraju telah menyediakan perkhidmatan PKI sejak tahun 2002 kepada Agensi Sektor Awam bagi menyokong pelaksanaan projek-projek Kerajaan Elektronik (*Electronic Government* – EG). Pelaksanaan perkhidmatan PKI melibatkan 2 aspek utama iaitu pengeluaran dan penggunaan Sijil Digital. Perkhidmatan ini disediakan selaras dengan Arahan Teknologi Maklumat 2007, Akta Aktiviti Kerajaan Elektronik 2007, Akta Tandatangan Digital 1997, Akta Rahsia Rasmi 1972, Peraturan-Peraturan Tandatangan Digital 1998 dan Arahan Keselamatan (Semakan dan Pindaan 2017).

4. Pada tahun 2011, perkhidmatan PKI telah ditambah baik dengan penggunaan sistem secara dalam talian yang berpusat di JDN. Perkhidmatan ini dikenali sebagai Perkhidmatan Prasarana Kunci Awam Kerajaan. Seterusnya, perkhidmatan ini telah dijenamakan semula kepada Perkhidmatan MyGPKI pada tahun 2019 dan kini telah diperluaskan selaras dengan hasrat serta aspirasi kerajaan dalam pelaksanaan inisiatif pendigitalan perkhidmatan kerajaan kepada rakyat.

5. Dasar dan aspirasi kerajaan telah digubal ke arah menjadikan Malaysia sebagai sebuah negara yang mampan, sejahtera, berdaya cipta, saling menghormati serta bersikap ihsan. Perkhidmatan MyGPKI merupakan salah satu inisiatif yang dijajarkan selaras dengan pemboleh daya strategik di bawah digitalisasi penyampaian perkhidmatan yang mendukung aspirasi tersebut. Oleh itu, pendigitalan sistem penyampaian perkhidmatan awam melalui Perkhidmatan MyGPKI ini dijangka berupaya merealisasi hasrat negara dalam memacu pertumbuhan ekonomi negara, memperkasa reformasi institusi dan tatakelola serta menegakkan keadilan sosial.

6. Skop Perkhidmatan MyGPKI merangkumi perkara berikut:

a. Pembekalan dan pengurusan Sijil Digital Pengguna dan Sijil Digital Pelayan yang melibatkan penyelarasan dengan Pihak Berkuasa Pemerakuan Berlesen (*Certification Authority* – CA).

b. Khidmat nasihat dan konsultasi bagi penggunaan PKI serta integrasi Sistem ICT Kerajaan dengan Sistem MyGPKI.

c. Perkhidmatan meja bantuan dan khidmat sokongan teknikal.

d. Program pengurusan perubahan termasuk latihan kepada Pentadbir dan Pengguna MyGPKI.

KEPERLUAN/RASIONAL

7. Perkhidmatan MyGPKI yang menyokong agenda pendigitalan dalam meningkatkan digitalisasi merentas negeri, syarikat dan masyarakat ini dapat membantu Agensi Sektor Awam mengurangkan risiko ancaman keselamatan ke atas data dan maklumat Sistem ICT Kerajaan masing-masing dengan lebih berkesan melalui penggunaan teknologi PKI.

PELAKSANAAN

8. Agensi Sektor Awam yang memerlukan kemudahan PKI bagi Sistem ICT Kerajaan hendaklah menggunakan Perkhidmatan MyGPKI.

9. Pelaksanaan Perkhidmatan MyGPKI adalah berdasarkan prinsip pegangan yang berikut:

a. Semua Sistem ICT Kerajaan yang menggunakan PKI merentas agensi mestilah membenarkan penggunaan pelbagai medium Sijil Digital selaras dengan tahap keselamatan Sistem ICT Kerajaan tersebut.

b. Agensi Pelaksana yang membangunkan Sistem ICT Kerajaan perlu memastikan sistem berkenaan boleh menyokong mana-mana Medium Sijil Digital Pengguna Perkhidmatan MyGPKI yang sedang berkuat kuasa.

c. Setiap penjawat awam hanya dibenarkan mempunyai satu Sijil Digital Pengguna sahaja pada satu-satu masa.

d. Pengguna MyGPKI yang memerlukan capaian kepada pelbagai Sistem ICT Kerajaan yang mempunyai tahap keselamatan berbeza hendaklah menggunakan Medium Sijil Digital Pengguna yang mempunyai tahap keselamatan tertinggi.

e. Pengguna MyGPKI yang tamat peranan atau tamat perkhidmatan hendaklah membuat pembatalan Sijil Digital Pengguna dan bagi pengguna

Sijil Digital Token hendaklah mengembalikan Token kepada Agensi Peneraju.

f. Pengguna MyGPKI yang kehilangan Sijil Digital Token disebabkan oleh kecuaian akan dikenakan tindakan secara pentadbiran.

g. Agensi Pelaksana hendaklah melaporkan kepada Agensi Peneraju sekiranya terdapat penyalahgunaan Sijil Digital Pengguna.

h. Agensi Peneraju menanggung kos pelaksanaan Perkhidmatan MyGPKI bagi Sijil Digital Pengguna untuk Perkhidmatan Awam Persekutuan iaitu Kementerian, Jabatan Persekutuan, Agensi Persekutuan serta Badan Berkanun Persekutuan Yang Tidak Diasingkan Pengurusan Saraannya yang bertindak sebagai Agensi Pelaksana dan semua pengguna Sistem ICT Kerajaan Agensi Pelaksana.

i. Agensi Peneraju menanggung kos pelaksanaan Perkhidmatan MyGPKI bagi Sijil Digital Pelayan untuk Sistem ICT Kerajaan Perkhidmatan Awam Persekutuan iaitu di Kementerian, Jabatan Persekutuan, Agensi Persekutuan dan Badan Berkanun Persekutuan Yang Tidak Diasingkan Pengurusan Saraannya.

j. Kos perkhidmatan PKI bagi Perkhidmatan Awam Negeri, Badan Berkanun Persekutuan Yang Diasingkan Pengurusan Saraannya, Badan Berkanun Negeri dan Pihak Berkuasa Tempatan yang berhasrat untuk bertindak sebagai Agensi Pelaksana dan semua pengguna Sistem ICT Kerajaan agensi ini adalah di bawah tanggungan agensi masing-masing. Agensi boleh berurusan secara terus bagi pelaksanaan PKI dengan CA yang diiktiraf oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM).

10. Semua Agensi Sektor Awam yang menggunakan Perkhidmatan MyGPKI bagi pengurusan Sijil Digital hendaklah menggunakan Sistem MyGPKI yang disediakan oleh Agensi Peneraju.

11. Pelaksanaan Perkhidmatan MyGPKI hendaklah berdasarkan garis panduan seperti **Lampiran A** iaitu:

a. **Bahagian A**: Garis Panduan Teknikal Perkhidmatan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* – MyGPKI)

   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 integrasi antara Sistem ICT Kerajaan dan Sistem MyGPKI. Garis panduan ini ialah seperti **Bab 1 hingga Bab 4**.

b. **Bahagian B**: Garis Panduan Operasi Perkhidmatan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* – MyGPKI)

   Garis panduan ini menerangkan jenis model dan tatacara operasi yang merangkumi aspek pengurusan, pengendalian dan pelaksanaan Perkhidmatan MyGPKI termasuk pengeluaran Sijil Digital. Garis panduan ini ialah seperti **Bab 5 hingga Bab 10**.

STRUKTUR TADBIR URUS

12. Perkhidmatan MyGPKI dipantau pelaksanaannya oleh Jawatankuasa Pelaksanaan Perkhidmatan MyGPKI dan peranannya boleh dilaksanakan oleh Jawatankuasa Pemandu Projek Perkhidmatan MyGPKI sedia ada.

13. Terma Rujukan Jawatankuasa Pelaksanaan Perkhidmatan MyGPKI ialah seperti yang berikut:

a. Menentukan hala tuju dan strategi pelaksanaan projek.
b. Memantau status pelaksanaan projek secara menyeluruh.
c. Memantau dan menyelaras aliran kewangan projek bersamaan kemajuan projek.
d. Meluluskan setiap pembayaran projek yang hendak dilakukan.

e. Menimbang dan meluluskan cadangan penguatkuasaan terma-terma kontrak seperti penalti, pelanjutan masa (*extension of time*) dan penamatan kontrak.
f. Menyelesaikan isu-isu dasar yang timbul berkaitan dengan projek.
g. Meluluskan dan mengesahkan pelaksanaan setiap peringkat projek.
h. Meluluskan serahan projek.

PEMAKAIAN

14. Pekeliling ini terpakai kepada semua Agensi Perkhidmatan Awam Persekutuan termasuk Badan Berkanun Persekutuan Yang Tidak Diasingkan Pengurusan Saraannya. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, peruntukan pekeliling ini dipanjangkan kepada semua Perkhidmatan Awam Negeri, Badan Berkanun Persekutuan Yang Diasingkan Pengurusan Saraannya, Badan Berkanun Negeri dan Pihak Berkuasa Tempatan.

TARIKH KUAT KUASA

15. Pekeliling ini berkuat kuasa mulai tarikh dikeluarkan dan terpakai sehingga dibatalkan.

PEMBATALAN

16. Dengan berkuat kuasa Pekeliling ini, maka Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 3 Tahun 2015: Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [*Government Public Key Infrastructure* (GPKI)] bertarikh 23 Oktober 2015 **DIBATALKAN**.

PERTANYAAN

17. Sebarang pertanyaan mengenai Pekeliling ini boleh dikemukakan kepada:

Pengarah
Bahagian Pembangunan Perkhidmatan Gunasama Infrastruktur
dan Keselamatan Digital (BPG)
Jabatan Digital Negara
Kementerian Digital
Bangunan MKN Embassy Techzone
Blok B, No. 3200, Jalan Teknokrat 2
63000 Cyberjaya
SELANGOR DARUL EHSAN
No. Telefon : 03-8000 8000
E-mel : pmo.gpki@jdn.gov.my
Laman Web : https://mygpki.gov.my/gpki_portal

"MALAYSIA MADANI"
"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

(TAN SRI SHAMSUL AZRI BIN ABU BAKAR)

SENARAI LAMPIRAN

LAMPIRAN	TAJUK
A	Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* – MyGPKI)
	Bahagian A: Garis Panduan Teknikal Perkhidmatan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* – MyGPKI)
	Bahagian B: Garis Panduan Operasi Perkhidmatan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* – MyGPKI)
A2	Tatacara Pelaksanaan Penilaian Risiko Dalam Konteks Perkhidmatan MyGPKI
A3	Format Laporan Penilaian Risiko Sistem ICT Kerajaan
A4	Format Laporan Penilaian Risiko Laman Web Dan Portal

LAMPIRAN A
Pekeliling Pendigitalan Perkhidmatan Awam
Bilangan 4 Tahun 2025

DASAR PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN (*GOVERNMENT PUBLIC KEY INFRASTRUCTURE* – MyGPKI)

JABATAN DIGITAL NEGARA
KEMENTERIAN DIGITAL

KANDUNGAN

PERKARA **MUKA SURAT**

SENARAI RAJAH

SENARAI JADUAL

AKRONIM

AKRONIM	PENERANGAN
Admin	*Administrator*
AP	*Authorised Personnel*
API	*Application Programming Interface*
CA	*Certification Authority*
CRL	*Certificate Revocation List*
ICT	*Information and Communication Technology*
JDN	Jabatan Digital Negara
MyGPKI	*Government Public Key Infrastructure*
OTP	*One-Time Password*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
SA	Sub Admin
SAP	Sub Admin Pelaksana
SOP	*Standard Operating Procedure*
SSL	*Secure Sockets Layer*

TAKRIFAN

Bagi maksud pemakaian Pekeliling Pendigitalan Perkhidmatan Awam (PPPA) Bilangan 4 Tahun 2025 Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (Government Public Key Infrastructure – MyGPKI), takrifan yang berikut diguna pakai:

1.	*Administrator (*Admin*)*	Pegawai di Agensi Peneraju yang bertanggungjawab mengurus Sistem GPKI serta melantik dan mengurus Sub Admin Pelaksana.
2.	Agen MyGPKI	Perisian yang dipasang pada komputer Pengguna MyGPKI bagi melaksanakan fungsi PKI iaitu pengesahan identiti (*authentication*), penyulitan maklumat (*information encryption*) dan tandatangan digital (*digital signature*) serta pengurusan Sijil Digital Pengguna, Sijil Digital Latihan dan Sijil Digital Ujian.
3.	Agensi Pelaksana	Agensi Sektor Awam yang terdiri daripada Perkhidmatan Awam Persekutuan yang merangkumi Kementerian, Jabatan Persekutuan dan Agensi Persekutuan yang merupakan pemilik Sistem ICT Kerajaan serta bertanggungjawab mengurus, menyelaras dan mentadbir Sistem ICT Kerajaan yang menggunakan Perkhidmatan MyGPKI.
4.	Agensi Peneraju	Agensi Sektor Awam yang bertanggungjawab menyelaras, memantau dan memperluaskan pelaksanaan Perkhidmatan MyGPKI kepada Perkhidmatan Awam Persekutuan serta memberi khidmat nasihat kepada penggunaan teknologi PKI bagi Sistem ICT Kerajaan dan seterusnya mentadbir Sistem MyGPKI.
5.	Agensi Sektor Awam	Semua peringkat pentadbiran Kerajaan iaitu agensi Perkhidmatan Awam Persekutuan, Perkhidmatan Awam Negeri, Badan Berkanun Persekutuan, Badan Berkanun Negeri serta Pihak Berkuasa Tempatan (PBT).
6.	*Application Programming Interface (API) MyGPKI*	Antara muka kod sumber yang digunakan sebagai perantara bagi melaksanakan integrasi antara Sistem MyGPKI dan Sistem ICT Kerajaan.

7.	*Authorised Personnel (AP)*	Pegawai yang bertanggungjawab mentadbir Pengguna MyGPKI di agensi masing-masing.
8.	*Certificate Revocation List (CRL)*	Senarai yang mengandungi nombor siri Sijil Digital Pengguna yang dibatalkan.
9.	*Elliptic Curve Cryptography (ECC)*	Algoritma kriptografi kunci awam yang menyediakan tahap keselamatan yang tinggi seperti algoritma kriptografi tradisional tetapi dengan saiz kunci yang lebih kecil.
10.	*MyGPKI Mobile*	Sistem aplikasi mudah alih bagi Perkhidmatan MyGPKI.
11.	Kunci Awam (*Public Key*)	Satu nilai integer nombor perdana yang besar yang dijana menggunakan algoritma kriptografi dan boleh dikongsi dengan umum bagi membolehkan penyulitan data atau maklumat dilaksanakan.
12.	Kunci Peribadi (*Private Key*)	Satu nilai integer nombor perdana yang besar yang dijana menggunakan algoritma kriptografi dan hendaklah sentiasa disimpan dengan selamat. Kunci peribadi digunakan untuk penyahsulitan data atau maklumat.
13.	Medium Sijil Digital Pengguna	Perkakasan atau perisian yang digunakan sebagai perantara untuk menyimpan Sijil Digital Pengguna.
14.	*One Time Password* (OTP)	Susunan aksara angka (kod) yang dijana secara automatik oleh sistem dan hanya boleh digunakan sekali sahaja untuk setiap transaksi.
15.	Pengguna MyGPKI	Pegawai di Agensi Sektor Awam yang diberi kebenaran untuk menggunakan Sijil Digital Pengguna bagi membuat pengesahan identiti dan tandatangan digital terhadap data dan maklumat Sistem ICT Kerajaan melalui Perkhidmatan MyGPKI.
16.	Pentadbir MyGPKI	Pentadbir bagi Sistem MyGPKI yang terdiri daripada *Administrator* (Admin), Sub Admin Pelaksana (SAP), Sub Admin (SA) dan *Authorised Personnel* (AP).

17.	Pentadbir Pelayan	Pegawai yang mentadbir pelayan bagi Sistem ICT Kerajaan yang terdiri daripada Pegawai Pemohon, Pegawai Teknikal dan Pegawai Pengesah.
18.	Perkhidmatan MyGPKI	Perkhidmatan keselamatan ICT yang disediakan oleh Agensi Peneraju melibatkan pembekalan dan pengurusan Sijil Digital Pengguna dan pembekalan Sijil Digital Pelayan yang menyediakan fungsi pengesahan identiti, penyulitan dan penyahsulitan maklumat serta tandatangan digital dengan menggunakan teknologi PKI.
19.	*Personal Identification Number* (PIN)	Susunan angka yang pendek iaitu 8 digit yang digunakan sebagai kata laluan bagi mengesahkan identiti Pengguna MyGPKI.
20.	Pihak Berkuasa Pemerakuan Berlesen (*Certification Authority* – CA)	Organisasi yang diberi lesen dan diiktiraf oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) bagi pengeluaran Sijil Digital berdasarkan Akta Tandatangan Digital 1997, Peraturan-Peraturan Tandatangan Digital 1998 dan undang-undang berkaitan yang sedang berkuat kuasa.
21.	Prasarana Kunci Awam (Public Key Infrastructure – PKI)	Prasarana keselamatan teknologi maklumat dan komunikasi yang merangkumi elemen perkakasan, perisian, individu, teknologi, polisi dan tatacara yang perlu bagi menjana, mengurus, mengedar, mengguna, menyimpan dan membatalkan Sijil Digital.
22.	*Roaming* OTP	Kaedah bagi pelaksanaan tandatangan digital menggunakan Sijil Digital Perayauan (*RoamingCert*) dengan *One Time Password* (OTP) bagi tujuan meningkatkan tahap kawalan keselamatan.
23.	*RoamingCert* + OTP	Kombinasi Sijil Digital Perayauan (*RoamingCert*) dengan *One Time Password* (OTP).
24.	*Rivest-Shamir-Adleman* (RSA) *Cryptography*	Algoritma kriptografi yang digunakan secara meluas bagi penyulitan kunci awam untuk melindungi proses penghantaran data melalui internet.

25.	*Secure Sockets Layer (SSL)*	Protokol rangkaian yang mengesahkan kesahihan pelayan dan pengguna serta penyulitan komunikasi antara pelayan dan aplikasi pengguna.
26.	Sijil Digital	Sijil Digital Pengguna dan Sijil Digital Pelayan yang dikeluarkan oleh CA untuk mengesahkan identiti pengguna atau pelayan.
27.	Sijil Digital Pelayan	Sijil yang dikeluarkan oleh CA untuk mengesahkan identiti pelayan Sistem ICT Kerajaan.
28.	Sijil Digital Pelayan *Multi* Domain	Sijil yang mengandungi sekurang-kurangnya 2 domain atau subdomain.
29.	Sijil Digital Pelayan *Single* Domain	Sijil yang mengandungi satu domain sahaja.
30.	Sijil Digital Pelayan *Wildcard*	Sijil yang mengandungi pelbagai subdomain di bawah satu domain yang sama dan menggunakan simbol '*'(*Wildcard*) dalam satu Sijil Digital Pelayan.
31.	Sijil Digital Pengguna	Sijil yang dikeluarkan kepada individu oleh CA yang mengandungi maklumat berkenaan dengan identiti dan kunci persendirian (*private key*) pengguna tersebut.
32.	Sijil Digital Perayauan (*RoamingCert*)	Fail yang mengandungi Sijil Digital Pengguna, *private key* bagi pengesahan identiti, penyulitan dan penyahsulitan maklumat serta tandatangan digital. Sijil Digital Pengguna ini disimpan dalam pelayan di Agensi Peneraju.
33.	Sijil Digital Perisian (*SoftCert*)	Fail yang mengandungi Sijil Digital Pengguna, *private key* bagi pengesahan identiti, penyulitan dan penyahsulitan maklumat dan tandatangan digital. Sijil Digital Pengguna ini disimpan pada medium storan data.
34.	Sijil Digital Token	Fail yang mengandungi Sijil Digital Pengguna, *private key* bagi pengesahan identiti, penyulitan dan penyahsulitan maklumat serta tandatangan digital. Sijil Digital Token ini dijana secara *onboard* pada Token.

35.	Sistem MyGPKI	Sistem yang digunakan bagi tujuan pengurusan Perkhidmatan MyGPKI.
36.	Sistem ICT Kerajaan	Sistem, portal, laman web atau aplikasi ICT yang digunakan oleh Agensi Sektor Awam bagi menyokong perkhidmatan kerajaan.
37.	Sub Admin (SA)	Pegawai di Agensi Sektor Awam yang berperanan melantik AP serta mentadbir Pengguna MyGPKI di agensi masing-masing.
38.	Sub Admin Pelaksana (SAP)	Pegawai di Agensi Pelaksana yang berperanan mengurus Pentadbir GPKI (SA dan AP) dan Pengguna MyGPKI di agensi masing-masing.
39.	Token	Peranti atau perkakasan yang mengandungi cip kriptografi untuk menyimpan *private key* dan Sijil Digital Pengguna bagi melaksanakan pengesahan identiti, penyulitan dan penyahsulitan maklumat serta tandatangan digital.

BAHAGIAN A

GARIS PANDUAN TEKNIKAL
PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN
(GOVERNMENT PUBLIC KEY INFRASTRUCTURE – MyGPKI)

BAB 1: LATAR BELAKANG GARIS PANDUAN TEKNIKAL

1.1 Tujuan

1.1.1 Garis Panduan Teknikal Perkhidmatan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* – MyGPKI) ini bertujuan untuk menerangkan langkah-langkah pelaksanaan aktiviti di bawah skop teknikal yang merangkumi pelaksanaan penilaian risiko sistem, panduan penentuan penggunaan jenis medium Sijil Digital dan keperluan teknikal khusus bagi:

a. Membantu agensi membuat penilaian kendiri keperluan penggunaan Prasarana Kunci Awam (*Public Key Infrastructure* – PKI) dalam pelaksanaan Sistem ICT Kerajaan.

b. Menjelaskan kaedah pelaksanaan teknikal dalam penggunaan PKI yang merangkumi aspek pengesahan identiti, tandatangan digital serta penyulitan data dan maklumat.

1.2 Skop

1.2.1 Garis panduan teknikal ini memberikan tumpuan kepada perkara yang perlu dilaksanakan oleh agensi mengikut turutan yang berikut:

a. Menilai tahap risiko Sistem ICT Kerajaan untuk mengenal pasti kawalan keselamatan yang sesuai bagi keperluan Perkhidmatan MyGPKI.

b. Menentukan penggunaan jenis medium Sijil Digital sama ada bagi tujuan pengesahan identiti, tandatangan digital dan/atau penyulitan maklumat.

c. Menggariskan keperluan teknikal dalam pelaksanaan PKI daripada segi piawaian, keperluan integrasi dan keperluan khusus bagi setiap jenis medium Sijil Digital.

1.3 Kumpulan Sasar

1.3.1 Kumpulan sasaran garis panduan ini ialah Agensi Pelaksana Sistem ICT Kerajaan yang memerlukan kawalan keselamatan daripada segi pengesahan identiti, tanpa sangkalan serta integriti data dan maklumat.

BAB 2: KEPERLUAN TEKNIKAL PERKHIDMATAN MyGPKI

2.1 Pengenalan

2.1.1 Keperluan teknikal Perkhidmatan MyGPKI merangkumi keperluan berkaitan piawaian PKI, Sijil Digital Pengguna dan Sijil Digital Pelayan. Bab ini dapat membantu agensi untuk menyediakan keperluan teknikal dalam pelaksanaan Perkhidmatan MyGPKI khususnya bagi keperluan Sistem ICT Kerajaan dan infrastruktur ICT.

2.2 Piawaian Antarabangsa Berkaitan Pelaksanaan PKI

2.2.1 Agensi Pelaksana hendaklah memastikan semua pembangunan dan pelaksanaan fungsi PKI mematuhi piawaian antarabangsa seperti **Jadual 1** di bawah:

Jadual 1: Piawaian Antarabangsa PKI

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

2.2.2 Piawaian antarabangsa bagi Sijil Digital Pengguna dan Pelayan ialah seperti **Jadual 2** di bawah:

Jadual 2: Senarai Piawaian Antarabangsa bagi Sijil Digital

Bil.	Jenis Sijil Digital	Piawaian Antarabangsa
1.	Kriptografi Berasaskan Cip (Sijil Digital Token)	FIPS 140, FIPS 46, FIPS 196, PKCS#11, PKCS#15, CSP, USB
2.	Sijil Digital Perayauan (*RoamingCert*)	PKCS#12, RFC X.509
3.	Sijil Digital Perisian (*SoftCert*)	PKCS#12, RFC X.509
4.	Sijil Digital Pelayan	PKCS#7, PKCS#12, RFC 5280 X.509

2.2.3 Terdapat beberapa kelas Sijil Digital yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (*Certification Authority*, CA) mengikut penggunaan jenis-jenis Sijil Digital seperti **Jadual 3** di bawah:

Jadual 3: Kelas Sijil Digital

Bil.	Kelas Sijil Digital	Tujuan Penggunaan	Pengesahan Identiti Pemohon	Tahap Jaminan Keselamatan
1.	Kelas 1 (Individu/ Organisasi)	Digunakan bagi transaksi bukan komersial atau komunikasi e-mel	Pengesahan identiti pemohon adalah mudah, iaitu dengan pengesahan nama pengguna dan alamat e-mel	Rendah
2.	Kelas 2 (Individu/ Organisasi)	Digunakan bagi transaksi komersial secara dalam talian atau capaian kepada laman web	Pengesahan identiti pemohon adalah wajib	Sederhana
3.	Kelas 3 (Individu/ Organisasi)	Digunakan dalam perbankan elektronik, transaksi kewangan dan dokumentasi perundangan	Pengesahan dan semakan identiti dibuat oleh CA	Tinggi

2.2.4 Struktur Sijil Digital Pengguna yang digunakan dalam Perkhidmatan MyGPKI adalah berdasarkan piawaian RFC 5280 X.509 dan senarai atribut yang berkaitan ialah seperti **Jadual 4** di bawah:

Jadual 4: Struktur Sijil Digital Pengguna Perkhidmatan MyGPKI

Bil.	Atribut	Keterangan	Jenis Atribut	Contoh
1.	*Version numb*er	Versi Sijil Digital Pengguna	Atribut wajib	V3
2.	*Serial number*	Nombor siri Sijil Digital Pengguna	Atribut wajib	22 ab 2c 48 a1 da 7c 22 58 69 fe 36 85 53 3d 40

Bil.	Atribut	Keterangan	Jenis Atribut	Contoh
3.	*Signature Algorithm*	Algoritma yang digunakan untuk menandatangani Sijil Digital Pengguna	Atribut wajib	*Signature Algorithm*: RSA – sha256RSA ECC – sha256ECDSA
4.	*Signature Hash Algorithm*	Nilai cincangan (*hash value*) Sijil Digital Pengguna	Atribut wajib	*Signature hash algorithm*: sha256
5.	*Issuer*	Maklumat pengeluar Sijil Digital Pengguna CN: *Root Certificate Holder Name* OU: *Organization* Unit (Nama CA) O: *Organization Name* C: *Country Name*	Atribut wajib	CN = JDN *Class* 2 CA OU = *Authenticated by* CA O = Jabatan Digital Negara C = MY
6.	*Validity Period*	Tempoh sah laku Sijil Digital Pengguna Tempoh sah laku Sijil Digital Pengguna ialah 24 bulan *Valid From*: Tarikh Pengeluaran Sijil Digital Pengguna Valid To: Tarikh Tamat Sijil Digital Pengguna	Atribut wajib	*Valid From*: Isnin, 2 Oktober 2017 8:00:00 pagi *Valid* To: Selasa, 1 Oktober 2017 8:00:00 pagi

Bil.	Atribut	Keterangan	Jenis Atribut	Contoh
7.	*Subject*	Maklumat pemegang Sijil Digital Pengguna C: *Country N*ame (MY) SN: *Serial Number* (No. MyKad) SERIALNUMBER: *Serial Number* (No. MyKad) CN: *Certificate Holder N*ame	Atribut wajib	Contoh Sijil Digital Pengguna C = MY SN= 82010804**** SERIALNUMBER= 82010804**** CN= NORAMIRA BINTI MOHD NOR Contoh Sijil Digital Pelayan CN = abc.jdn.gov.my SERIALNUMBER = 1096-02-01 2.5.4.15 = *Government Entity* O = JDN (Jabatan Digital Negara) 1.3.6.1.4.1.311.60.2.1.3 = MY L = Putrajaya S = Putrajaya C = MY
8.	*Public Key*	Maklumat kunci awam Sijil Digital Pengguna	Atribut wajib	30 82 01 0a 02 82 01 01 00 90 03 d1 94 4b 0a aa cd cf fd d0 aa e7 84 93 74 d1 62 8b c8 55 20 b7 80 0d 1e 36 71F c4 c7 ae d9
9.	*Public Key Parameters*	Maklumat algoritma kriptografi yang digunakan oleh CA untuk menandatangani Sijil Digital Pengguna	Atribut wajib	05 00

Bil.	Atribut	Keterangan	Jenis Atribut	Contoh
10.	*Certificate Revocation List* (CRL) *Distribution Points*	Maklumat status Sijil Digital Pengguna sama ada telah dibatalkan atau masih sah	Extensions	CRL *Distribution Point* *Distribution Point Name*: *Full Name*: URL=http://crl.msctrustgate.com/JDNGPKI/LatestCRL.crl
11.	*Key Usage*	Tujuan penggunaan kunci awam yang terdapat di dalam Sijil Digital	Atribut janaan komputer. Bukan sebahagian Sijil Digital	Digital *Signature*, *Non-Repudiation, Key Encipherment, Data Encipherment* (f0)

2.3 Pemilihan Kaedah Kawalan Keselamatan

2.3.1 Kawalan keselamatan diperlukan bagi memberi perlindungan terhadap data atau maklumat daripada ancaman keselamatan. Kaedah kawalan PKI digunakan bagi tujuan melindungi maklumat Sistem ICT Kerajaan berdasarkan ciri-ciri keselamatan maklumat seperti **Jadual 5** di bawah:

Jadual 5: Kaedah Kawalan PKI berdasarkan Ciri-Ciri Keselamatan Maklumat

Bil.	Ciri-ciri Keselamatan Maklumat	Kaedah Kawalan PKI
1.	Kerahsiaan (*Confidentiality* - C)	Penyulitan dan Penyahsulitan Penyulitan maklumat dilaksanakan dengan menggunakan kunci awam bagi memastikan hanya pemilik kunci awam yang sepadan sahaja boleh menyahsulitkan maklumat menggunakan kunci peribadi. Fungsi PKI ini memastikan hanya pihak yang mempunyai capaian yang dibenarkan sahaja boleh mengakses data atau maklumat tersebut.

Bil.	Ciri-ciri Keselamatan Maklumat	Kaedah Kawalan PKI
2.	Kesahihan (*Authenticity* – A)	Pengesahan Identiti Pengesahan identiti menerusi Sijil Digital Pengguna yang mengandungi maklumat pengguna dan kunci awam (*public key*). Maklumat pengguna akan disahkan oleh CA bagi memastikan identiti pengguna adalah betul. Manakala, maklumat domain akan disahkan oleh CA bagi memastikan identiti pelayan adalah betul.
3.	Integriti (*Integrity* – I)	Penyulitan dan Penyahsulitan Integriti maklumat yang ditandatangani oleh Pengguna MyGPKI secara digital boleh disahkan dengan menyemak kunci awam penghantar. Hanya pemilik kunci awam yang sepadan sahaja boleh menyahsulitkan maklumat menggunakan kunci peribadi (*private key*). Sekiranya terdapat sebarang perubahan data atau maklumat, perubahan tersebut dapat dikesan berdasarkan perbandingan maklumat asal dengan maklumat yang telah diubah.
4.	Tanpa sangkalan (*Non-repudiation* – N)	Tandatangan Digital Dokumen yang ditandatangani oleh Pengguna MyGPKI secara elektronik tidak boleh disangkal bagi menjamin integriti data atau maklumat terlibat.

2.3.2 Penggunaan kaedah kawalan PKI oleh Agensi Pelaksana ialah berdasarkan kategori Sistem ICT Kerajaan, peringkat keselamatan data atau maklumat dan nilai data atau maklumat, tahap risiko Sistem ICT Kerajaan serta faedah pelaksanaan kawalan PKI yang telah dikenal pasti. Penerangan faktor pertimbangan bagi pemilihan kaedah kawalan PKI yang bersesuaian ialah seperti **Jadual 6** di bawah:

Jadual 6: Faktor Pertimbangan Pemilihan Kaedah Kawalan Menggunakan PKI

<table>
<tr><th rowspan="2">Kategori Sistem ICT Kerajaan</th><th rowspan="2">Peringkat Keselamatan Data/Maklumat</th><th rowspan="2">Nilai Data/ Maklumat</th><th colspan="4">Tahap Risiko</th></tr>
<tr><th>Rendah</th><th>Sederhana</th><th>Tinggi</th><th>Ekstrem</th></tr>
<tr><td rowspan="4">Teras/ Strategik/ Sokongan Umum/ Sokongan Dalaman</td><td>Rahsia Besar*/ Rahsia*/Sulit</td><td>Tinggi</td><td colspan="4" rowspan="2">Pengesahan Identiti, Penyulitan dan Tandatangan Digital</td></tr>
<tr><td>Terhad</td><td>Sederhana</td></tr>
<tr><td>Terkawal/ Sensitif</td><td>Sederhana</td><td colspan="2">Pengesahan Identiti dan Penyulitan</td><td colspan="2">Pengesahan Identiti, Penyulitan dan Tandatangan Digital</td></tr>
<tr><td>Terbuka</td><td>Rendah</td><td colspan="4">Pengesahan Identiti dan Penyulitan</td></tr>
</table>

*Nota: Pelaksanaan terhadap data atau maklumat yang mempunyai peringkat keselamatan rahsia besar dan rahsia secara dalam talian bagi data perlu merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia.

2.4 Pemilihan Medium Sijil Digital

2.4.1 Sijil Digital digunakan sebagai bukti secara digital yang mengesahkan bahawa identiti pemegang Sijil Digital atau organisasi adalah sahih sepertimana yang dinyatakan pada Sijil Digital. CA akan mengesahkan kesahihan identiti pengguna atau organisasi melalui proses pengesahan identiti pemegang Sijil Digital atau organisasi semasa permohonan Sijil Digital serta semakan pada *Certificate Revocation List* (CRL).

2.4.2 Penggunaan Sijil Digital bagi tujuan pengesahan identiti, tandatangan digital dan penyulitan maklumat dapat ditentukan berdasarkan perkara berikut:

a. Tahap kepentingan Sistem ICT Kerajaan terhadap fungsi organisasi menentukan tahap keselamatan Sistem ICT Kerajaan.

b. Peringkat keselamatan data atau maklumat menentukan tahap perlindungan data atau maklumat yang bersesuaian.

c. Nilai data, maklumat nilai data atau maklumat terhadap fungsi organisasi.

d. Tahap risiko dan faedah pelaksanaan kawalan keselamatan.

2.4.3 Pemilihan medium Sijil Digital yang bersesuaian bagi pelaksanaan Perkhidmatan MyGPKI ialah berdasarkan keperluan tahap kawalan keselamatan data atau maklumat dan juga tahap risiko persekitaran operasi yang menyokong fungsi agensi. Selain itu, pemilihan jenis medium Sijil Digital bukan sahaja bagi tujuan mitigasi risiko, tetapi berdasarkan hasil analisis faedah kos atau lain-lain pertimbangan yang bersesuaian.

2.5 Pemilihan Medium Sijil Digital Pengguna

2.5.1 Sijil Digital Pengguna yang dikeluarkan oleh CA disimpan dalam Medium Sijil Digital Pengguna yang berbeza. Medium Sijil Digital Pengguna Perkhidmatan MyGPKI terdiri daripada perisian iaitu *RoamingCert* dan *SoftCert* serta perkakasan iaitu Sijil Digital Token. Keterangan bagi setiap jenis Medium Sijil Digital Pengguna ialah seperti **Jadual 7** berikut:

Jadual 7: Jenis Medium Sijil Digital Pengguna Perkhidmatan MyGPKI

Bil.	Jenis Medium	Keterangan	Ciri-Ciri	Jaminan Tahap Keselamatan
1.	Sijil Digital Token	Kunci kriptografi yang dilindungi dan disimpan dalam perkakasan untuk mengakses	a. Memerlukan PIN bagi mengaktifkan padanan kunci (*key pair*) kriptografi b. Kunci kriptografi tidak boleh dieksport	Tinggi

Bil.	Jenis Medium	Keterangan	Ciri-Ciri	Jaminan Tahap Keselamatan
		data atau maklumat	keluar daripada perkakasan c. Sijil digital dijana dalam persekitaran komputer pengguna (*onboard key generation*)	
2.	*RoamingCert* + OTP	Kombinasi Sijil Digital Perayauan (*RoamingCert*) dengan *One Time Password* (OTP)	a. Memerlukan PIN bagi mengaktifkan padanan kunci kriptografi b. Sijil digital akan hanya dimuat turun ke komputer pengguna sekiranya transaksi dilaksanakan c. Sijil Digital yang disimpan dalam komputer pengguna akan dihapuskan selepas tempoh tertentu d. Memerlukan faktor pengesahan tambahan iaitu OTP	Tinggi
3.	*RoamingCert*	Kunci kriptografi yang dilindungi dan disimpan di dalam	a. Memerlukan PIN bagi mengaktifkan padanan kunci kriptografi	Sederhana

Bil.	Jenis Medium	Keterangan	Ciri-Ciri	Jaminan Tahap Keselamatan
		pelayan *roaming*	b. Sijil digital akan hanya dimuat turun ke komputer pengguna sekiranya transaksi dilaksanakan c. Sijil digital yang disimpan dalam komputer pengguna akan dihapuskan selepas tempoh tertentu	
4.	*SoftCert*	Kunci kriptografi yang dilindungi dan disimpan dalam pelbagai medium simpanan Sijil Digital. Contohnya disimpan dalam memori komputer atau pena pemacu	Memerlukan PIN bagi mengaktifkan padanan kunci kriptografi Sijil Digital boleh disalin dan dipindahkan ke pelbagai medium simpanan	Sederhana

2.5.2 Penentuan jenis Medium Sijil Digital Pengguna yang perlu digunakan ialah berdasarkan kategori Sistem ICT Kerajaan, peringkat keselamatan data atau maklumat dan nilai data atau maklumat serta tahap risiko Sistem ICT Kerajaan yang telah dikenal pasti seperti **Jadual 8** berikut:

Jadual 8: Penentuan Jenis Medium Sijil Digital Pengguna

<table>
<tr><th rowspan="2">Kategori Sistem ICT Kerajaan</th><th rowspan="2">Peringkat Keselamatan Data/ Maklumat</th><th rowspan="2">Nilai Data/ Maklumat</th><th colspan="4">Tahap Risiko</th></tr>
<tr><th>Rendah</th><th>Sederhana</th><th>Tinggi</th><th>Ekstrem</th></tr>
<tr><td rowspan="4">Teras/ Strategik/ Sokongan Umum/ Sokongan Dalaman</td><td>Rahsia Besar*/ Rahsia*/Sulit</td><td>Tinggi</td><td colspan="4">Sijil Digital Token/ RoamingCert + OTP</td></tr>
<tr><td>Terhad</td><td>Sederhana</td><td>SoftCert</td><td>Roaming Cert</td><td colspan="2">Sijil Digital Token/ RoamingCert + OTP</td></tr>
<tr><td>Terkawal/ Sensitif</td><td>Sederhana</td><td>Tiada</td><td>SoftCert</td><td colspan="2">RoamingCert</td></tr>
<tr><td>Terbuka</td><td>Rendah</td><td colspan="4">Tiada</td></tr>
</table>

Nota (*): Pelaksanaan terhadap data atau maklumat yang mempunyai peringkat keselamatan rahsia besar dan rahsia secara dalam talian bagi data perlu merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia.

2.6 Pemilihan Medium Sijil Digital Pelayan

2.6.1 Sijil Digital Pelayan digunakan bagi tujuan pengesahan identiti organisasi serta melindungi maklumat semasa transaksi secara dalam talian dilaksanakan. Keterangan fungsi Sijil Digital Pelayan ialah seperti yang berikut:

a. Pengesahan identiti organisasi

CA akan mengesahkan bahawa identiti organisasi yang berperanan sebagai pemilik pelayan Sistem ICT Kerajaan tersebut adalah sahih. Kaedah pengesahan identiti organisasi ialah seperti **Jadual 9** berikut:

Jadual 9: Kaedah Pengesahan Identiti Organisasi

Bil.	Kaedah Pengesahan Identiti Organisasi	Keterangan	Jaminan Tahap Keselamatan
1.	*Extended Validation* (EV)	a. Sijil Digital Pelayan yang dikeluarkan oleh CA b. CA akan mengesahkan maklumat pendaftaran domain, organisasi dan maklumat pemohon, iaitu semakan sebagai pemilik domain yang sah c. CA akan menghubungi pemilik domain untuk mengesahkan maklumat organisasi berdasarkan rekod di repositori rasmi kerajaan d. Proses pengesahan maklumat lebih teliti dan menyeluruh berbanding kaedah pengesahan *Organisation Validation* (OV) e. Sesuai digunakan bagi kegunaan laman web atau Sistem ICT Kerajaan yang memerlukan kawalan keselamatan tertinggi f. Bar alamat pelayar akan memaparkan maklumat CA dan pemilik domain yang sah g. Memenuhi piawaian RFC 5280 X.509	Tinggi
2.	*Organisation Validation* (OV)	a. Sijil Digital Pelayan yang dikeluarkan oleh CA b. CA akan mengesahkan maklumat pendaftaran domain dan maklumat organisasi c. CA akan menghubungi pemilik domain untuk mengesahkan maklumat organisasi berdasarkan rekod di repositori rasmi kerajaan d. Sesuai digunakan bagi kegunaan laman web Sistem ICT Kerajaan	Sederhana

Bil.	Kaedah Pengesahan Identiti Organisasi	Keterangan	Jaminan Tahap Keselamatan
		yang memerlukan kawalan keselamatan sederhana e. Memenuhi piawaian RFC 5280 X.509	
3.	Domain *Validated* (DV)	a. Sijil Digital Pelayan dikeluarkan oleh CA b. Pengesahan maklumat domain hanya dilaksanakan berdasarkan maklumat pendaftaran domain c. Maklumat yang disahkan hanya maklumat pemohon, iaitu sebagai pemilik domain yang sah d. Tiada pengesahan tambahan bagi maklumat organisasi dalam memastikan kewujudan organisasi pemohon e. Sesuai digunakan bagi laman web peribadi atau organisasi yang memerlukan kawalan keselamatan yang rendah f. Memenuhi piawaian RFC 5280 X.509	Rendah
4.	*Private Trust*	a. Sijil Digital Pelayan dikeluarkan oleh CA b. Nama domain utama tidak perlu didaftarkan c. Tidak memerlukan pengesahan maklumat domain, pemohon dan organisasi oleh CA d. Sesuai digunakan bagi kegunaan laman web atau Sistem ICT Kerajaan yang mempunyai capaian menerusi rangkaian dalaman sahaja seperti persekitaran Intranet, VPN, API	Persendirian / dalaman sahaja

Bil.	Kaedah Pengesahan Identiti Organisasi	Keterangan	Jaminan Tahap Keselamatan
		dalaman, *Staging*, Pengujian dan Pembangunan Sistem e. Memenuhi piawaian RFC 5280 X.509	

b. Penyulitan data dan maklumat

Perlindungan keselamatan Sistem ICT Kerajaan merangkumi perlindungan kepada maklumat rahsia rasmi yang sedang bertransaksi secara dalam talian antara pelayan Sistem ICT Kerajaan dan pelayar Internet melalui penggunaan fungsi penyulitan. Sambungan selamat (*secured connection*) akan diwujudkan antara pelayan Sistem ICT Kerajaan dan pelayar Internet. Fungsi penyulitan maklumat ini dapat mengurangkan risiko ancaman pemintasan komunikasi antara pelayan Sistem ICT Kerajaan dan pelayar Internet.

Sekiranya Sijil Digital Pelayan dipasang pada pelayar, *Secured Hypertext Transfer Protocols* (https) akan dipaparkan pada bar alamat pelayar (*browser address bar*) yang digunakan untuk membuat capaian ke domain tersebut bagi memaklumkan tahap jaminan keselamatan domain. Antara Jenis Sijil Digital Pelayan yang dibekalkan oleh Perkhidmatan MyGPKI ialah seperti **Jadual 10** berikut:

Jadual 10: Jenis Sijil Digital Pelayan Perkhidmatan MyGPKI

Bil.	Jenis Sijil Digital Pelayan	Keterangan	Ciri-ciri
1.	Sijil Digital Pelayan *Single* Domain	a. Merupakan Sijil Digital Pelayan yang didaftarkan bagi satu domain atau subdomain sahaja Contoh 1: Domain mygpki.gov.my Contoh 2: Subdomain helpdesk.mygpki.gov.my b. Kunci peribadi (*private key*) pelayan dijana khusus bagi domain atau subdomain yang didaftarkan sahaja c. Sekiranya kunci peribadi pelayan terdedah atau terjejas (*compromised*), implikasi keselamatan hanya melibatkan domain atau subdomain tersebut sahaja	a. Nama domain utama telah didaftarkan dengan pendaftar domain b. Keperluan Sijil Digital Pelayan bagi satu domain atau subdomain sahaja c. Capaian menerusi Internet
2.	Sijil Digital Pelayan Multi Domain	a. Merupakan Sijil Digital Pelayan yang mengandungi satu domain utama dan sekurang-kurangnya satu *subdomain* (*Subject Alternative Names* – SANs) atau mempunyai pelbagai domain di bawah organisasi yang sama Contoh 1: Domain dan subdomain domain utama: mygpki.gov.my subdomain: sub1.mygpki.gov.my	a. Nama domain utama telah didaftarkan dengan pendaftar domain b. Keperluan Sijil Digital Pelayan melebihi satu domain atau pelbagai subdomain yang berada di aras hierarki yang berlainan c. Nama domain atau subdomain telah ditetapkan

Bil.	Jenis Sijil Digital Pelayan	Keterangan	Ciri-ciri
		Contoh 2: Pelbagai domain di organisasi yang sama domain utama: mygpki.gov.my subdomain: mygpki.jdn.gov.my b. Kunci peribadi pelayan yang sama dikongsi oleh dua atau lebih domain atau subdomain yang didaftarkan c. Sekiranya kunci peribadi pelayan terdedah atau terjejas (*compromised*), implikasi keselamatan ialah ke atas semua domain atau subdomain yang menggunakan kunci yang sama	d. Capaian menerusi Internet
3.	Sijil Digital Pelayan *Wildcard*	a. Sijil Digital Pelayan yang mengandungi pelbagai subdomain yang berada di aras hierarki yang sama dan menggunakan simbol *wildcard* (“*”) dalam satu Sijil Digital Pelayan Contoh: domain utama: *.mygpki.gov.my subdomain 1: sub1.mygpki.gov.my subdomain 2: sub2.mygpki.gov.my b. Kunci peribadi pelayan bagi domain atau subdomain akan dikongsi bagi semua subdomain yang didaftarkan di bawah	a. Nama domain utama telah didaftarkan pada pendaftar domain b. Keperluan Sijil Digital Pelayan bagi lebih daripada satu subdomain dalam suatu domain yang sama c. Nama subdomain belum ditetapkan dan berkemungkinan terdapat pertambahan subdomain pada masa akan datang d. Capaian menerusi Internet

Bil.	Jenis Sijil Digital Pelayan	Keterangan	Ciri-ciri
		domain atau subdomain yang sama c. Sekiranya kunci peribadi pelayan terdedah atau terjejas (*compromised*), implikasi keselamatan ialah kepada semua subdomain yang menggunakan kunci yang sama	

2.6.2 Penentuan penggunaan jenis medium Sijil Digital Pelayan ialah berdasarkan tahap risiko yang telah dikenal pasti. Penerangan faktor pertimbangan bagi pemilihan medium Sijil Digital Pelayan berdasarkan tahap risiko seperti Jadual **11** berikut:

Jadual 11: Penentuan Jenis Medium Sijil Digital Pelayan

<table>
<tr><th rowspan="2">Kategori Sistem ICT Kerajaan</th><th rowspan="2">Peringkat Keselamatan Data/ Maklumat</th><th rowspan="2">Nilai Data/ Maklumat</th><th colspan="4">Tahap Risiko</th></tr>
<tr><th>Rendah</th><th>Sederhana</th><th>Tinggi</th><th>Ekstrem</th></tr>
<tr><td rowspan="4">Teras/ Strategik/ Sokongan Umum/ Sokongan Dalaman</td><td>Rahsia Besar*/ Rahsia*/Sulit</td><td>Tinggi</td><td colspan="4">Sijil Digital Pelayan EV</td></tr>
<tr><td>Terhad</td><td>Sederhana</td><td colspan="2">Sijil Digital Pelayan OV</td><td colspan="2">Sijil Digital Pelayan EV</td></tr>
<tr><td>Terkawal/ Sensitif</td><td>Sederhana</td><td colspan="4" rowspan="2">Sijil Digital Pelayan OV</td></tr>
<tr><td>Terbuka</td><td>Rendah</td></tr>
</table>

Nota (*): Pelaksanaan bagi sistem secara dalam talian yang mempunyai data/maklumat rahsia besar atau rahsia hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia.

BAB 3: PELAKSANAAN PERKHIDMATAN MyGPKI

3.1 Pengenalan

3.1.1 Pelaksanaan Perkhidmatan MyGPKI merangkumi skop integrasi antara Sistem ICT Kerajaan dengan Sistem MyGPKI dan pembekalan Sijil Digital.

3.1.2 Terdapat dua kaedah pelaksanaan Perkhidmatan MyGPKI di agensi iaitu melibatkan:

a. Pelaksanaan integrasi Sistem ICT Kerajaan dengan *Application Programming Interface* (API) MyGPKI oleh Agensi Pelaksana serta pembekalan Sijil Digital oleh Agensi Peneraju.

b. Pembangunan API PKI di bawah inisiatif Agensi Pelaksana dan pembekalan Sijil Digital daripada Agensi Peneraju.

3.1.3 Proses pelaksanaan Perkhidmatan MyGPKI yang perlu dipatuhi oleh Agensi Pelaksana ialah seperti yang berikut:

a. Langkah 1: Kajian Keperluan Pelaksanaan Perkhidmatan MyGPKI

Agensi Peneraju akan memberi penerangan berkaitan Perkhidmatan MyGPKI kepada Agensi Pelaksana dan menilai kesesuaian Sistem ICT Kerajaan untuk menggunakan Perkhidmatan MyGPKI. Semasa peringkat ini, Agensi Pelaksana akan mengenal pasti perkara yang diperlukan seperti tujuan penggunaan Perkhidmatan MyGPKI, skop pelaksanaan, strategi pelaksanaan, keperluan sistem, perisian, perkakasan dan lain-lain keperluan teknikal, aktiviti yang terlibat serta pihak yang berkaitan dengan pelaksanaan Perkhidmatan MyGPKI.

b. Langkah 2: Pelaksanaan Penilaian Risiko

Agensi Pelaksana hendaklah mengenal pasti tahap risiko ancaman keselamatan data atau maklumat terhadap fungsi Sistem ICT Kerajaan, laman web atau portal yang akan menggunakan Perkhidmatan MyGPKI. Berdasarkan hasil penilaian risiko, Agensi Pelaksana hendaklah mengenal pasti kawalan keselamatan iaitu fungsi PKI dan Sijil Digital yang diperlukan bagi perlindungan data dan maklumat.

c. Langkah 3: Permohonan Penggunaan Perkhidmatan MyGPKI

Agensi Pelaksana hendaklah mengemukakan permohonan rasmi berserta laporan penilaian risiko kepada Agensi Peneraju. Permohonan ini akan diangkat untuk perakuan dan kelulusan oleh Jawatankuasa Pelaksanaan Perkhidmatan MyGPKI.

d. Langkah 4: Pelaksanaan Perkhidmatan MyGPKI

Pelaksanaan Perkhidmatan MyGPKI di Agensi Pelaksana akan dimulakan setelah mendapat kelulusan daripada Jawatankuasa Pelaksanaan Perkhidmatan MyGPKI. Agensi Pelaksana akan melaksanakan pembangunan sistem mengikut keperluan yang telah dikenal pasti semasa Langkah 1.

e. Langkah 5: Pengujian Fungsi PKI atau Semakan Konfigurasi Pemasangan Sijil Digital Pelayan:

i. Pengujian Fungsi PKI bagi pelaksanaan integrasi Sistem ICT Kerajaan

Agensi Pelaksana hendaklah membuat pengujian fungsi PKI bersama Agensi Peneraju bagi memastikan pelaksanaan fungsi PKI mengikut piawaian yang ditetapkan serta berfungsi mengikut keperluan. Semua

ralat yang ditemui semasa fasa pengujian hendaklah diperbaiki sebelum Sistem ICT Kerajaan digunakan secara rasmi.

ii. Semakan Konfigurasi Pemasangan Sijil Digital Pelayan

Pentadbir Pelayan hendaklah menyemak dan memastikan konfigurasi pemasangan Sijil Digital Pelayan dilaksanakan dengan betul dan mendapat Taraf A bagi setiap domain dan subdomain.

f. Langkah 6: Latihan Pentadbir MyGPKI dan Pengguna MyGPKI bagi pelaksanaan integrasi Sistem ICT Kerajaan

Pentadbir MyGPKI hendaklah menghadiri latihan penggunaan Sistem MyGPKI merangkumi pengurusan Sijil Digital Pengguna, pengurusan Pengguna MyGPKI dan pengurusan Pentadbir MyGPKI yang dianjurkan oleh Agensi Peneraju.

Agensi Pelaksana hendaklah menyediakan latihan penggunaan Sistem MyGPKI kepada Pengguna MyGPKI di bawah Agensi Pelaksana.

3.2 Pelaksanaan Integrasi Sistem ICT Kerajaan Dengan API MyGPKI

3.2.1 Perkhidmatan MyGPKI menyediakan platform yang membolehkan fungsi PKI iaitu proses pengesahan identiti pengguna, penyulitan dan penyahsulitan serta tandatangan digital dilaksanakan menggunakan API MyGPKI yang mengandungi komponen seperti yang berikut:

a. MyGPKI *Client* iaitu perisian yang digunakan untuk melaksanakan fungsi MyGPKI.

b. MyGPKI *Script* iaitu skrip yang digunakan untuk membolehkan MyGPKI *Client* berkomunikasi dengan API Sistem ICT Kerajaan bagi melaksanakan fungsi PKI pada MyGPKI *Client*. Agensi Pelaksana perlu membuat instalasi

Agen MyGPKI bagi tujuan komunikasi antara Sijil Digital Pengguna dan API MyGPKI.

c. MyGPKI Server API iaitu API MyGPKI yang diletakkan pada pelayan Sistem ICT Kerajaan bagi melaksanakan fungsi PKI pada pelayan atau perisian PKI Sistem ICT Kerajaan.

d. MyGPKI *Web Service* iaitu *web service* yang diletakkan pada pelayan Sistem ICT Kerajaan bagi melaksanakan fungsi PKI pada pelayan atau perisian PKI Sistem ICT Kerajaan menggunakan MyGPKI *Web Service*.

3.2.2 Terdapat 3 kaedah integrasi API MyGPKI namun tidak terhad kepada kaedah yang berikut:

a. *Client integration* iaitu integrasi antara Sistem ICT Kerajaan dan MyGPKI Client bagi melaksanakan fungsi PKI.

b. *Server integration* iaitu integrasi antara pelayan Sistem ICT Kerajaan dan API MyGPKI bagi melaksanakan fungsi PKI.

c. *Web service integration* iaitu integrasi antara pelayan Sistem ICT Kerajaan dan MyGPKI Web Service bagi melaksanakan fungsi PKI.

3.2.3 Integrasi Sistem ICT Kerajaan dengan API MyGPKI membolehkan sebarang perubahan konfigurasi pada pelayan sistem dilaksanakan secara berpusat di Agensi Peneraju sekiranya terdapat perubahan *root certificate*, *Certificate Revocation List* (CRL) atau versi pelayar. Selain itu, proses pencarisilapan mudah dilaksanakan sekiranya berlaku ralat berkaitan fungsi PKI.

3.2.4 Agensi Peneraju bertanggungjawab bagi membekalkan API MyGPKI yang diperlukan manakala Agensi Pelaksana bertanggungjawab untuk membangunkan fungsi PKI pada Sistem ICT Kerajaan, melaksanakan pengujian fungsi PKI serta menanggung kos yang terlibat bagi kerja-kerja pengintegrasian dengan API MyGPKI.

3.2.5 Agensi Peneraju juga bertanggungjawab membekalkan Sijil Digital Pengguna dan Sijil Digital Pelayan. Kos bagi pembekalan Sijil Digital Pengguna dan Sijil Digital Pelayan juga ialah di bawah tanggungan Agensi Peneraju. Selain itu, Agensi Peneraju akan menyediakan Sijil Digital Ujian yang mempunyai tempoh sah laku selama 12 bulan bagi tujuan pengujian fungsi PKI Sistem ICT Kerajaan Agensi Pelaksana. Permohonan Sijil Digital Ujian hendaklah dikemukakan oleh Sub Admin Pelaksana (SAP) menerusi Sistem MyGPKI.

3.2.6 Kaedah pelaksanaan integrasi API MyGPKI mengikut keperluan keselamatan ialah seperti **Jadual 12** berikut:

Jadual 12: Kaedah Pelaksanaan Integrasi Mengikut Keperluan Keselamatan

Bil.	Keperluan Keselamatan	Kaedah Pelaksanaan
1.	Pengesahan Identiti	Integrasi melalui API MyGPKI
2.	Penyulitan Maklumat	
3.	Tandatangan Digital	

3.2.7 Selain daripada keperluan keselamatan yang dinyatakan dalam **Jadual 12**, berikut ialah keperluan teknikal khusus yang perlu diberi perhatian oleh Agensi Pelaksana sekiranya berhasrat menggunakan Perkhidmatan MyGPKI, iaitu:

a. Memastikan ketersediaan dan kestabilan rangkaian di Agensi Pelaksana.

b. Memastikan keperluan pelayar dan persekitaran komputer atau peranti pengguna mengikut spesifikasi yang ditetapkan.

c. Memastikan Agen MyGPKI atau MyGPKI *Mobile* dipasang oleh pengguna mengikut keperluan.

3.3 Pembangunan API PKI Di Bawah Inisiatif Agensi Pelaksana

3.3.1 Agensi Pelaksana yang membangunkan dan menggunakan API PKI di bawah inisiatif sendiri hendaklah memastikan agar semua pembangunan dan pelaksanaan fungsi PKI mematuhi piawaian antarabangsa seperti **Jadual 1**, mematuhi struktur Sijil Digital Pengguna seperti **Jadual 4** serta menggunakan Sijil Digital Pengguna sekurang-kurangnya Kelas 2.

3.3.2 Kaedah pelaksanaan fungsi PKI mengikut keperluan keselamatan ialah seperti **Jadual 13** di bawah:

Jadual 13: Pelaksanaan Fungsi PKI Mengikut Keperluan Keselamatan

Bil.	Keperluan Keselamatan	Kaedah Pelaksanaan
1.	Pengesahan Identiti	**Pilihan 1: Mutual *Authentication*** **Tindakan:** a. Mengaktifkan fungsi Mutual *Authentication* pada pelayan b. Membuat capaian Sijil Digital Pengguna c. Membuat capaian dan semakan CRL
		Pilihan 2: PKI *Authentication* API **Tindakan:** a. Menggunakan PKI *Authentication* API bagi tujuan pengesahan identiti pengguna b. Membuat capaian Sijil Digital Pengguna c. Membuat capaian dan semakan CRL
2.	Penyulitan Maklumat	**PKI *Encryption* API** **Tindakan:** a. Menggunakan PKI *Encryption* API bagi tujuan penyulitan maklumat dan pengesahan penyulitan maklumat b. Membuat capaian Sijil Digital Pengguna c. Membuat capaian dan semakan CRL

Bil.	Keperluan Keselamatan	Kaedah Pelaksanaan
3.	Tandatangan Digital	**PKI *Signing* API** **Tindakan:** a. Menggunakan PKI *Signing* API bagi tujuan penyulitan maklumat dan pengesahan penyulitan maklumat b. Membuat capaian Sijil Digital Pengguna c. Membuat capaian dan semakan CRL

3.3.3 Agensi Pelaksana bertanggungjawab untuk membangunkan fungsi PKI, melaksanakan pengujian fungsi PKI serta menanggung kos yang terlibat bagi kerja-kerja pembangunan dan pengujian fungsi PKI tersebut. Agensi Peneraju bertanggungjawab untuk membekalkan Sijil Digital Pengguna dan/atau Sijil Digital Pelayan. Agensi Peneraju akan menyediakan Sijil Digital Ujian yang mempunyai tempoh sah laku selama 12 bulan bagi tujuan pengujian fungsi PKI Sistem ICT Kerajaan Agensi Pelaksana. Permohonan Sijil Digital Ujian hendaklah dikemukakan oleh SAP melalui Sistem MyGPKI.

BAB 4: PENILAIAN RISIKO DALAM KONTEKS PERKHIDMATAN MyGPKI

4.1 Pengenalan

4.1.1 Agensi Sektor Awam hendaklah melaksanakan penilaian risiko untuk mengenal pasti tahap kawalan keselamatan menggunakan PKI yang bersesuaian dan memastikan pemilihan kawalan risiko yang melibatkan data atau maklumat rahsia rasmi kerajaan selaras dengan akta, arahan, peraturan atau pekeliling kawalan keselamatan data atau maklumat rahsia rasmi yang sedang berkuat kuasa.

4.1.2 Dalam konteks pelaksanaan Perkhidmatan MyGPKI, penilaian risiko dilaksanakan untuk mengenal pasti langkah-langkah kawalan yang boleh menangani risiko berkaitan kerahsiaan, pengesahan identiti, integriti dan tanpa sangkalan terhadap data dan maklumat Sistem ICT Kerajaan. Penilaian risiko ini hendaklah dilaksanakan sekiranya Sistem ICT Kerajaan, laman web atau portal:

a. Mengandungi maklumat rasmi.
b. Dikategorikan sebagai sistem teras atau strategik.
c. Berkaitan keselamatan negara.
d. Melibatkan transaksi kewangan.

4.2 Tatacara Penilaian Risiko

4.2.1 Mengikut amalan terbaik, agensi hendaklah melaksanakan penilaian risiko pada peringkat awal pembangunan Sistem ICT Kerajaan iaitu semasa fasa kajian keperluan sistem. Namun begitu, agensi digalakkan untuk melaksanakan penilaian risiko ke atas maklumat Sistem ICT Kerajaan secara berkala bagi memastikan sebarang risiko terhadap maklumat sentiasa dipantau dan kawalan keselamatan yang dilaksanakan masih relevan.

4.2.2 Proses penilaian risiko terhadap fungsi teras agensi yang disokong oleh Sistem ICT Kerajaan melibatkan 6 langkah utama dan dijelaskan dengan lebih terperinci pada Lampiran 2: Tatacara Pelaksanaan Penilaian Risiko Dalam Konteks Perkhidmatan MyGPKI. Secara ringkasnya, 6 langkah utama digambarkan seperti **Rajah 1** berikut:

Rajah 1: Proses Penilaian Risiko

4.2.3 Agensi Pelaksana perlu mengemukakan permohonan Perkhidmatan MyGPKI secara rasmi bersama Laporan Penilaian Risiko sebagai dokumen sokongan kepada Agensi Peneraju. Rujuk Lampiran A3: Format Laporan Penilaian Risiko Sistem ICT Kerajaan serta Lampiran A4: Format Laporan Penilaian Risiko Laman Web dan Portal.

BAHAGIAN B

GARIS PANDUAN OPERASI
PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN
(*GOVERNMENT PUBLIC KEY INFRASTRUCTURE* – MyGPKI)

BAB 5: LATAR BELAKANG GARIS PANDUAN OPERASI

5.1 Tujuan

5.1.1 Garis Panduan Operasi Perkhidmatan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* – MyGPKI) ini bertujuan untuk menerangkan mengenai pengurusan permohonan dan pengoperasian Perkhidmatan MyGPKI.

5.2 Skop

5.2.1 Skop bagi garis panduan ini ialah seperti yang berikut:

a. Model operasi MyGPKI.
b. Pengoperasian Perkhidmatan MyGPKI.
c. Prosedur permohonan Perkhidmatan MyGPKI.

5.3 Kumpulan Sasaran

5.3.1 Skop bagi garis panduan ini disasarkan kepada Agensi Sektor Awam yang berhasrat atau sedang menggunakan Perkhidmatan MyGPKI serta Pentadbir dan Pengguna MyGPKI.

BAB 6: PENGURUSAN AGENSI, PENTADBIR DAN PENGGUNA MyGPKI

6.1 Pengenalan

6.1.1 Pengurusan Pentadbir dan Pengguna MyGPKI dilaksanakan berdasarkan Model Operasi MyGPKI bagi memastikan pengurusan perkhidmatan yang lebih teratur dan berkesan. Pihak yang terlibat dalam pengurusan Agensi, Pentadbir dan Pengguna MyGPKI ialah seperti yang berikut:

a. Agensi Peneraju.
b. Agensi Pelaksana.
c. Agensi Sektor Awam.

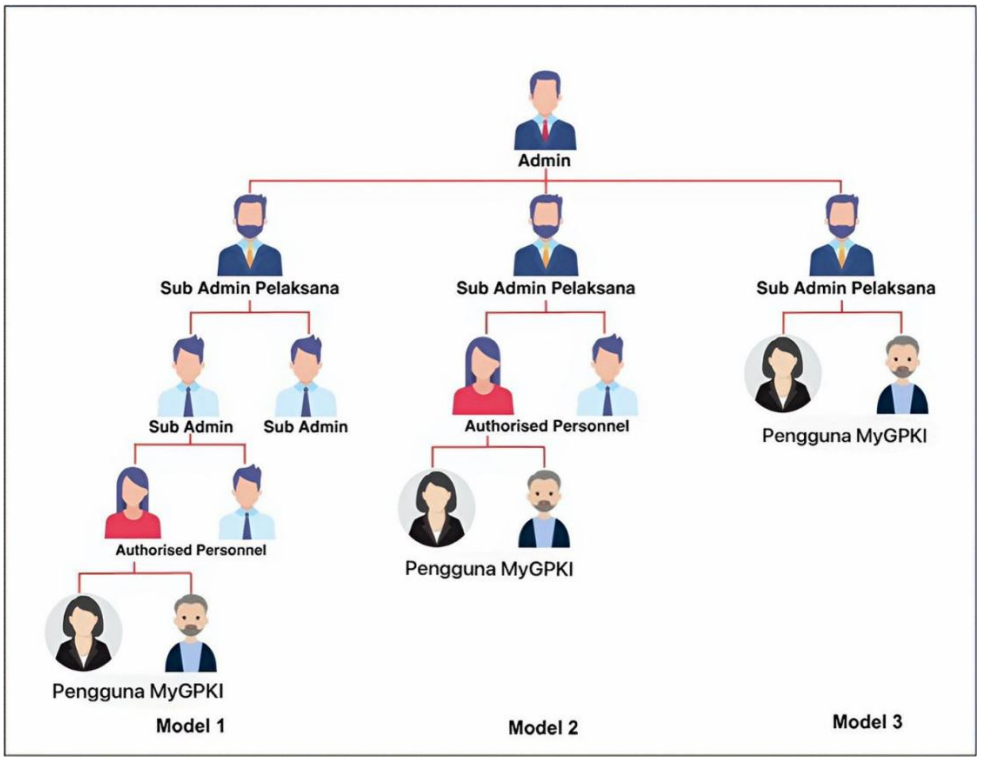
6.2 Model Operasi MyGPKI

6.2.1 Terdapat 3 jenis Model Operasi MyGPKI yang digunakan dalam pengurusan Perkhidmatan MyGPKI. Model ini mengandungi Pentadbir MyGPKI iaitu Administrator (Admin), Sub Admin Pelaksana (SAP), Sub Admin (SA) dan *Authorised Personnel* (AP). Pemilihan Model Operasi MyGPKI bergantung kepada kesesuaian pelaksanaan Perkhidmatan MyGPKI di agensi. Keterangan serta kriteria pemilihan bagi setiap jenis model ialah seperti **Jadual 14** dan gambaran bagi setiap model ialah seperti **Rajah 2** berikut:

Jadual 14: Model Operasi MyGPKI

Bil.	Model Operasi	Keterangan	Kriteria Pemilihan
1.	Model 1	Model ini mengandungi Pentadbir MyGPKI iaitu: a. SAP b. SA c. AP Pentadbir MyGPKI dilantik di setiap peringkat agensi berkaitan	a. Pengguna Sistem ICT Kerajaan merentas Agensi Sektor Awam b. Pengguna Sistem ICT Kerajaan berada di lokasi yang berbeza seperti di ibu pejabat/negeri/daerah c. Jumlah Pengguna Sistem ICT Kerajaan melebihi 1,000 orang

Bil.	Model Operasi	Keterangan	Kriteria Pemilihan
2.	Model 2	Model ini mengandungi Pentadbir MyGPKI iaitu: a. SAP b. AP	a. Pengguna Sistem ICT Kerajaan merentas agensi sektor awam atau hanya melibatkan kementerian/ agensi sahaja b. Pengguna Sistem ICT Kerajaan berada di lokasi yang berbeza c. Jumlah pengguna Sistem ICT Kerajaan melebihi 400 orang
3.	Model 3	Model ini mengandungi Pentadbir SAP sahaja	a. Pengguna Sistem ICT Kerajaan merentas agensi sektor awam atau hanya melibatkan kementerian/ agensi sahaja b. Pengguna Sistem ICT Kerajaan berada di lokasi yang sama atau berbeza c. Jumlah Pengguna Sistem ICT Kerajaan kurang daripada atau sama dengan 400 orang

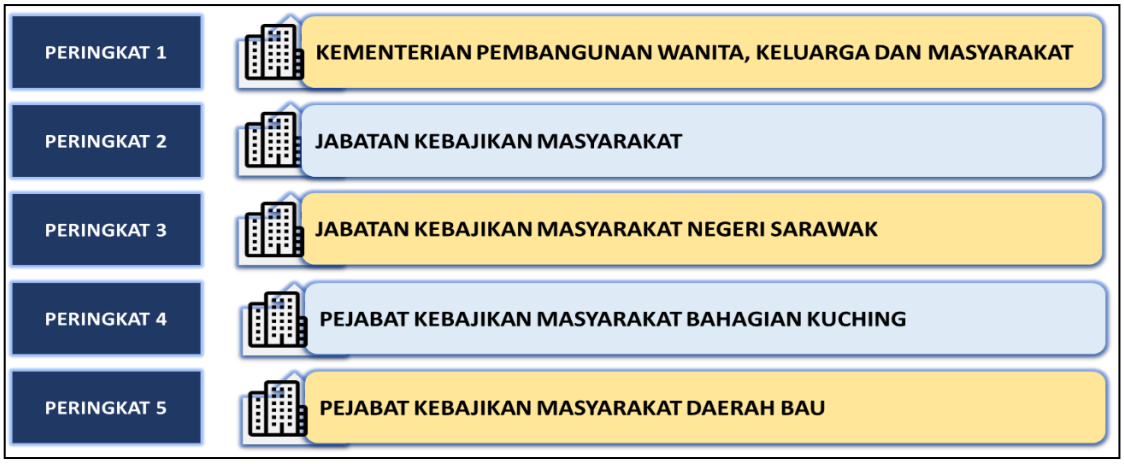


Rajah 2: Model Operasi MyGPKI

6.3 Pengurusan Agensi MyGPKI

6.3.1 Agensi MyGPKI ialah Agensi Sektor Awam yang menggunakan Perkhidmatan MyGPKI iaitu organisasi yang bertaraf kementerian, jabatan atau agensi sahaja. Struktur Agensi MyGPKI terdiri daripada 5 peringkat seperti berikut dan contoh bagi struktur Agensi MyGPKI ialah seperti **Rajah 3** berikut:

a. Peringkat 1 : Kementerian.
b. Peringkat 2 : Ibu pejabat atau pejabat negeri.
c. Peringkat 3 : Pejabat negeri, pejabat bahagian atau pejabat daerah.
d. Peringkat 4 : Pejabat bahagian atau daerah.
e. Peringkat 5 : Agensi di bawah pejabat bahagian, pejabat daerah atau agensi di bawah pejabat daerah.



Rajah 3: Contoh Struktur Agensi MyGPKI

6.3.2 Pengurusan Agensi MyGPKI melibatkan proses pewujudan dan pengemaskinian profil Agensi MyGPKI. Permohonan pendaftaran dan pengemaskinian profil Agensi MyGPKI perlu dikemukakan secara rasmi kepada Agensi Peneraju. Semua permohonan perlu mendapat pengesahan daripada SAP dan Ketua Jabatan sebelum dikemukakan kepada Agensi Peneraju.

6.3.3 Kaedah pengurusan profil Agensi MyGPKI akan melibatkan proses-proses berikut:

a. Pentadbir MyGPKI hendaklah mengemukakan permohonan bagi mewujudkan atau mengemas kini profil Agensi GPKI kepada Meja Bantuan MyGPKI.

b. Pentadbir MyGPKI (Admin) akan membuat pewujudan, penambahan dan pengemaskinian profil Agensi MyGPKI menerusi Sistem MyGPKI.

6.4 Pengurusan Pentadbir MyGPKI

6.4.1 Pentadbir MyGPKI ialah pegawai di Agensi Peneraju atau Agensi Pelaksana yang bertanggungjawab untuk mengurus permohonan Sijil Digital Pengguna, mentadbir dan memantau pengguna Sistem ICT Kerajaan di bawah seliaannya. Pentadbir MyGPKI terdiri daripada Admin, SAP, SA dan AP. Peranan dan tanggungjawab setiap Pentadbir MyGPKI diterangkan seperti **Jadual 15** berikut:

Jadual 15: Peranan dan Tanggungjawab Pentadbir MyGPKI

Bil.	Entiti	Peranan	Tanggungjawab
1.	Agensi Peneraju	Admin	**Peranan Utama:** a. Sebagai pentadbir Sistem MyGPKI b. Memohon pelantikan dan penamatan peranan Admin c. Memantau dan mengemas kini senarai Agensi MyGPKI d. Mendaftarkan SAP sebagai Pengguna MyGPKI e. Melantik dan menamatkan peranan SAP f. Memantau SAP, SA dan AP g. Mengesahkan dan meluluskan permohonan Sijil Digital Pengguna yang dikemukakan oleh SAP h. Mengesahkan dan meluluskan permohonan Sijil Digital Pelayan yang dikemukakan oleh Agensi Pelaksana i. Memantau Pengguna MyGPKI di bawah seliaannya j. Memberi penerangan kepada pengguna berkaitan pengurusan Sijil Digital Pengguna dan profil pengguna k. Merancang dan mengadakan latihan Sistem MyGPKI kepada Pentadbir MyGPKI **Peranan Tambahan:** Peranan tambahan akan dilaksanakan sekiranya Pentadbir MyGPKI di bawah seliaannya tidak dapat melaksanakan peranan berikut: a. Mendaftarkan pengguna Sistem ICT Kerajaan menerusi Sistem MyGPKI b. Mengesahkan permohonan peranan SA dan AP c. Memastikan ID pengguna telah diwujudkan dalam Sistem ICT Kerajaan sebelum pengguna membuat permohonan Sijil Digital Pengguna d. Mengesahkan permohonan Sijil Digital Pengguna SA, AP dan Pengguna MyGPKI e. Menyediakan perkhidmatan meja bantuan dan khidmat sokongan teknikal kepada Pengguna MyGPKI

Bil.	Entiti	Peranan	Tanggungjawab
2.	Agensi Pelaksana	SAP	**Peranan Utama:** a. Sebagai Pentadbir MyGPKI bagi Sistem ICT Kerajaan b. Memohon pelantikan dan penamatan peranan SAP c. Mengenal pasti Model Operasi MyGPKI yang bersesuaian d. Memantau dan menyemak senarai Agensi MyGPKI di bawah seliaannya e. Mendaftarkan SA sebagai Pengguna MyGPKI f. Melantik dan menamatkan peranan SA g. Memantau SA dan AP h. Mengesah dan meluluskan permohonan Sijil Digital Pengguna yang dikemukakan oleh SA i. Memantau Pengguna MyGPKI di bawah seliaannya j. Melaporkan penyalahgunaan Sijil Digital Pengguna di bawah seliaannya kepada Admin k. Memberi penerangan kepada pengguna berkaitan pengurusan Sijil Digital Pengguna dan profil pengguna l. Merancang dan mengadakan latihan Sistem GPKI kepada Pentadbir MyGPKI dan Pengguna MyGPKI **Peranan Tambahan:** Peranan tambahan akan dilaksanakan sekiranya Pentadbir MyGPKI di bawah seliaannya tidak dapat melaksanakan peranan berikut: a. Mendaftarkan pengguna Sistem ICT Kerajaan di bawah seliaannya menerusi Sistem MyGPKI b. Mengesahkan permohonan peranan AP c. Memastikan ID pengguna telah diwujudkan dalam Sistem ICT Kerajaan sebelum pengguna membuat permohonan Sijil Digital Pengguna d. Mengesahkan permohonan Sijil Digital Pengguna AP dan Pengguna MyGPKI e. Menyediakan khidmat sokongan teknikal kepada Pengguna MyGPKI

Bil.	Entiti	Peranan	Tanggungjawab
			f. Melaporkan kehilangan Token atau kerosakan Sijil Digital Pengguna kepada Admin atau Meja Bantuan MyGPKI
3.	Kementerian	SA	**Peranan Utama:** a. Sebagai Pentadbir MyGPKI di peringkat Kementerian b. Memohon pelantikan dan penamatan peranan SA c. Memantau dan menyemak senarai Agensi MyGPKI di bawah seliaannya d. Mendaftarkan AP sebagai Pengguna MyGPKI e. Melantik dan menamatkan peranan AP f. Memantau AP g. Mengesahkan dan meluluskan permohonan Sijil Digital Pengguna yang dikemukakan oleh AP h. Memantau Pengguna MyGPKI di bawah seliaannya i. Melaporkan penyalahgunaan Sijil Digital Pengguna di bawah seliaannya kepada Admin dan SAP j. Memberi penerangan kepada Pengguna MyGPKI berkaitan pengurusan Sijil Digital Pengguna dan profil pengguna **Peranan Tambahan:** Peranan tambahan akan dilaksanakan sekiranya Pentadbir MyGPKI di bawah seliaannya tidak dapat melaksanakan peranan berikut: a. Mendaftarkan pengguna Sistem ICT Kerajaan di bawah seliaannya menerusi Sistem MyGPKI b. Memastikan ID pengguna telah diwujudkan dalam Sistem ICT Kerajaan sebelum pengguna membuat permohonan Sijil Digital Pengguna c. Mengesahkan permohonan Sijil Digital Pengguna yang dikemukakan oleh Pengguna MyGPKI d. Menyediakan khidmat sokongan teknikal kepada Pengguna MyGPKI

Bil.	Entiti	Peranan	Tanggungjawab
			g. Melaporkan kehilangan Token atau kerosakan Sijil Digital Pengguna kepada Admin atau Meja Bantuan MyGPKI
4.	Agensi Sektor Awam	AP	**Peranan Utama:** a. Sebagai Pentadbir MyGPKI di peringkat agensi b. Memohon pelantikan dan penamatan peranan AP c. Memantau dan menyemak senarai Agensi MyGPKI di bawah seliaannya d. Mendaftarkan pengguna Sistem ICT Kerajaan sebagai Pengguna MyGPKI e. Memantau Pengguna MyGPKI f. Memastikan ID pengguna telah diwujudkan dalam Sistem ICT Kerajaan sebelum pengguna membuat permohonan Sijil Digital Pengguna g. Mengesahkan dan meluluskan permohonan Sijil Digital Pengguna yang dikemukakan oleh Pengguna MyGPKI h. Memantau Pengguna MyGPKI di bawah seliaannya i. Melaporkan penyalahgunaan Sijil Digital Pengguna di bawah seliaannya kepada Admin dan SAP h. Melaporkan kehilangan Token atau kerosakan Sijil Digital Pengguna kepada Admin atau Meja Bantuan MyGPKI j. Memberi penerangan kepada pengguna berkaitan pengurusan Sijil Digital Pengguna dan profil pengguna k. Membantu menyediakan khidmat sokongan teknikal kepada Pengguna MyGPKI

6.4.2 Agensi Pelaksana perlu mengenal pasti dan melantik Pentadbir MyGPKI berdasarkan Model Operasi MyGPKI yang bersesuaian dengan pelaksanaan Sistem ICT Kerajaan.

6.4.3 Bagi kelancaran operasi dan pengurusan Sijil Digital Pengguna, Agensi Pelaksana perlu memastikan perkara-perkara berikut:

a. Melantik dua orang pegawai bagi setiap peranan mengikut Model Operasi MyGPKI.

b. Pegawai yang akan dilantik sebagai Pentadbir MyGPKI perlu memiliki Sijil Digital Pengguna.

c. Mengemukakan permohonan pelantikan Pentadbir MyGPKI melalui Sistem MyGPKI.

6.4.4 Pentadbir MyGPKI yang telah berpindah jabatan atau tidak lagi mempunyai peranan hendaklah membuat penamatan peranan melalui Sistem MyGPKI.

6.4.5 Pentadbir MyGPKI yang tidak aktif melebihi tempoh enam bulan akan ditamatkan peranannya sebagai Pentadbir MyGPKI oleh Pentadbir MyGPKI (Admin). Sekiranya Pentadbir MyGPKI masih memerlukan peranan sebagai Pentadbir MyGPKI, permohonan baharu sebagai Pentadbir MyGPKI perlu dikemukakan semula melalui Sistem MyGPKI.

6.5 Pengurusan Pengguna MyGPKI

6.5.1 Pentadbir MyGPKI di agensi perlu memastikan perkara-perkara berikut telah dilaksanakan sebelum membuat pendaftaran Pengguna MyGPKI:

a. ID pengguna telah diwujudkan di dalam Sistem ICT Kerajaan.

b. Pengguna Sistem ICT Kerajaan telah dibekalkan dengan Sijil Digital Pengguna atau perlu membuat permohonan baharu.

c. Maklumat pengguna iaitu nama, nombor MyKad, e-mel, maklumat agensi, nombor telefon pejabat dan telefon bimbit adalah sah bagi permohonan baharu.

6.5.2 Pendaftaran Pengguna MyGPKI melibatkan proses-proses yang berikut:

a. Pentadbir MyGPKI (Admin/SAP/SA/AP) mendaftarkan pengguna dalam Sistem MyGPKI berdasarkan Sistem ICT Kerajaan yang dibenarkan, Medium Sijil Digital Pengguna yang berkaitan serta Model Operasi MyGPKI yang bersesuaian.

b. Pentadbir MyGPKI (SAP/SA/AP) hendaklah memaklumkan kepada Meja Bantuan MyGPKI sekiranya Pengguna MyGPKI memerlukan penggunaan lebih daripada satu jenis Medium Sijil Digital Pengguna. Pentadbir MyGPKI (Admin) mendaftarkan pengguna dalam Sistem MyGPKI bagi Sistem ICT Kerajaan yang baharu dengan membuat penambahan medium setelah disahkan oleh Pentadbir MyGPKI (SAP/SA/AP).

6.6 Pengemaskinian Profil Pengguna MyGPKI

6.6.1 Pengguna MyGPKI hendaklah memastikan semua maklumat dalam profil Pengguna MyGPKI adalah sah dan terkini. Pengemaskinian profil pengguna perlu dilaksanakan oleh Pengguna MyGPKI sekiranya terdapat perubahan maklumat pengguna atau berpindah ke agensi baharu bagi memastikan semua butiran profil pengguna adalah sah.

6.6.2 Pengguna MyGPKI tidak dibenarkan untuk mendedahkan maklumat soalan rahsia (soalan keselamatan) dan jawapan rahsia (jawapan keselamatan).

6.7 Penamatan Peranan Pengguna MyGPKI

6.7.1 Penamatan peranan Pengguna MyGPKI perlu dilakukan sekiranya pengguna tidak lagi mempunyai peranan dalam Sistem ICT Kerajaan atau pengguna telah tamat perkhidmatan, bersara atau meninggal dunia.

6.7.2 Tindakan berikut perlu dilaksanakan oleh pihak yang terlibat:

a. Pengguna MyGPKI perlu membuat permohonan pembatalan Sijil Digital Pengguna menerusi Sistem MyGPKI sekiranya telah tamat peranan dalam Sistem ICT Kerajaan.

b. Pengguna MyGPKI atau Pentadbir MyGPKI (SAP/SA/AP) perlu membuat permohonan pembatalan Sijil Digital Pengguna menerusi Sistem MyGPKI sekiranya pengguna telah tamat perkhidmatan, bersara atau meninggal dunia.

BAB 7: PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PENGGUNA

7.1 Pengenalan

7.1.1 Sijil Digital Pengguna digunakan oleh Agensi Sektor Awam bagi tujuan pengesahan identiti pengguna Sistem ICT Kerajaan semasa melaksanakan transaksi secara dalam talian.

7.1.2 Terdapat 3 jenis Sijil Digital Pengguna iaitu Sijil Digital Token, *RoamingCert* dan *SoftCert* yang disediakan di bawah Perkhidmatan MyGPKI. Tempoh sah laku Sijil Digital Pengguna adalah selama 24 bulan. Agensi Pelaksana perlu mengenal pasti keperluan sebenar jenis Sijil Digital Pengguna yang bersesuaian dengan Sistem ICT Kerajaan dengan merujuk Lampiran A3: Format Laporan Penilaian Risiko Sistem ICT Kerajaan.

7.1.3 Semua permohonan Sijil Digital Pengguna hendaklah dikemukakan oleh Pengguna MyGPKI melalui Sistem MyGPKI.

7.2 Pengurusan Sijil Digital Pengguna

7.2.1 Pengurusan Sijil Digital Pengguna meliputi proses permohonan baharu, pembaharuan, penggantungan, pembatalan dan penggantian Sijil Digital Pengguna. Pihak yang terlibat dalam pengurusan Sijil Digital Pengguna ialah Agensi Peneraju, Agensi Pelaksana, Agensi Sektor Awam dan CA.

7.2.2 Pengguna MyGPKI bertanggungjawab untuk memastikan:

a. Sijil Digital Pengguna disimpan dengan selamat dan tidak boleh dipindah milik selaras dengan Akta Tandatangan Digital 1997, Peraturan-Peraturan Tandatangan Digital 1998 dan Arahan Teknologi Maklumat 2007.

b. *Personal Identification Number* (PIN) Sijil Digital Pengguna dan soalan serta jawapan rahsia (keselamatan) disimpan dengan selamat dan tidak didedahkan.

c. Salinan *SoftCert* dalam medium storan komputer dihapuskan apabila sijil digital tidak lagi digunakan.

d. Sijil Digital Token yang telah dibatalkan perlu dipulangkan kepada Agensi Peneraju.

7.3 Permohonan Baharu Sijil Digital Pengguna

7.3.1 Dalam melaksanakan proses permohonan baharu Sijil Digital Pengguna, pengguna perlu memastikan maklumat pengguna telah didaftar dalam Sistem MyGPKI.

7.3.2 Permohonan baharu Sijil Digital Pengguna melibatkan proses-proses berikut:

a. Pengguna membuat pengesahan alamat e-mel yang telah didaftarkan oleh Pentadbir MyGPKI setelah menerima e-mel notifikasi.

b. Pengguna membuat permohonan baharu Sijil Digital Pengguna melalui Sistem MyGPKI.

c. Pentadbir MyGPKI (SAP/SA/AP) mengesahkan permohonan baharu Sijil Digital Pengguna setelah permohonan diterima.

d. Permohonan baharu Sijil Digital Pengguna yang tidak disahkan oleh Pentadbir MyGPKI (SAP/SA/AP) akan ditolak secara automatik oleh Sistem MyGPKI dan pengguna perlu memohon semula.

e. Pihak Berkuasa Pemerakuan Berlesen (*Certification Authority* – CA) memproses permohonan baharu Sijil Digital Pengguna setelah mendapat pengesahan daripada Pentadbir MyGPKI.

f. Pengguna akan menerima e-mel notifikasi berkaitan maklumat penjanaan Sijil Digital Pengguna atau penghantaran Sijil Digital Token melalui pos berdaftar.

g. Pengguna hendaklah membuat pengaktifan Sijil Digital Pengguna setelah menerima sijil.

7.4 Permohonan Pembaharuan Sijil Digital Pengguna

7.4.1 Pengguna MyGPKI perlu membuat permohonan pembaharuan sekiranya masih memerlukan Sijil Digital Pengguna sebelum tamat tempoh sah laku sijil tersebut.

7.4.2 Permohonan Pembaharuan Sijil Digital Pengguna melibatkan proses-proses berikut:

a. Pengguna membuat permohonan pembaharuan Sijil Digital Pengguna menerusi Sistem MyGPKI dalam tempoh 30 hari sebelum tamat tempoh sah laku sijil sedia ada.

b. Pengguna MyGPKI mengemas kini profil pengguna sekiranya terdapat perubahan maklumat sebelum mengemukakan permohonan pembaharuan.

c. Pentadbir MyGPKI (SAP/SA/AP) mengesahkan permohonan pembaharuan Sijil Digital Pengguna setelah permohonan diterima.

d. Permohonan pembaharuan Sijil Digital Pengguna yang tidak disahkan oleh Pentadbir MyGPKI (SAP/SA/AP) akan ditolak secara automatik oleh Sistem MyGPKI dan pengguna perlu memohon semula.

e. CA memproses permohonan pembaharuan Sijil Digital Pengguna setelah mendapat pengesahan daripada Pentadbir MyGPKI (SAP/SA/AP).

f. Setelah proses permohonan selesai, pengguna menerima notifikasi e-mel berkaitan maklumat penjanaan Sijil Digital Pengguna.

g. Pengguna MyGPKI hendaklah membuat pengaktifan Sijil Digital Pengguna setelah menerima sijil.

7.5 Permohonan Pembatalan Dan Penggantian Sijil Digital Pengguna

7.5.1 Terdapat dua jenis kategori permohonan pembatalan Sijil Digital Pengguna iaitu:

a. Permohonan pembatalan yang memerlukan penggantian Sijil Digital Pengguna.

b. Permohonan pembatalan yang tidak memerlukan penggantian Sijil Digital Pengguna.

7.5.2 Terdapat 5 situasi bagi permohonan pembatalan yang memerlukan penggantian Sijil Digital Pengguna seperti yang berikut:

a. Fizikal Token rosak.
b. Token hilang/dicuri/tidak diterima.
c. Sijil Digital Pengguna rosak.
d. Pertukaran Medium Sijil Digital Pengguna.
e. Lain-lain sebab pembatalan.

7.5.3 Kerosakan fizikal Token boleh disebabkan oleh ralat berkaitan Sistem MyGPKI atau Sistem CA, masalah teknikal pada Token (*manufacturing defect*) atau kecuaian pengguna semasa pengendalian Token. Berikut ialah tindakan lanjut yang perlu diambil sekiranya fizikal Token didapati rosak:

a. Pengguna MyGPKI membuat pengujian pengesahan terhadap Token yang rosak melalui Agen MyGPKI.

b. Pengguna MyGPKI melaporkan kerosakan fizikal Token kepada Pentadbir MyGPKI (SAP/SA/AP) dan membuat aduan kepada Meja Bantuan MyGPKI bagi tujuan mendapatkan maklum balas pengesahan kerosakan fizikal Token tersebut.

c. Pengguna MyGPKI membuat permohonan pembatalan Token melalui Sistem MyGPKI setelah menerima notifikasi e-mel maklum balas pengesahan fizikal Token rosak daripada Meja Bantuan MyGPKI.

d. Pentadbir MyGPKI (SAP/SA/AP) mengesahkan permohonan pembatalan Token setelah menerima permohonan pembatalan tersebut.

e. Permohonan pembatalan Sijil Digital Pengguna yang tidak disahkan oleh Pentadbir MyGPKI (SAP/SA/AP) akan ditolak secara automatik oleh Sistem MyGPKI dan pengguna perlu memohon semula.

f. Pentadbir MyGPKI (Admin) meluluskan permohonan pembatalan setelah permohonan pembatalan disahkan oleh Pentadbir MyGPKI (SAP/SA/AP).

g. CA akan memproses permohonan pembatalan Sijil Digital Pengguna setelah menerima kelulusan pembatalan daripada Pentadbir MyGPKI (Admin).

h. Pengguna MyGPKI memulangkan Token yang disahkan rosak kepada Agensi Peneraju setelah permohonan pembatalan dikemukakan.

i. Pengguna MyGPKI mengemukakan permohonan penggantian setelah proses permohonan pembatalan Sijil Digital Pengguna selesai.

7.5.4 Sijil Digital Token yang hilang/dicuri/tidak diterima boleh digantikan dengan Sijil Digital Token yang baharu selepas tindakan berikut telah diambil oleh pihak yang terlibat:

a. Pengguna MyGPKI melaporkan kehilangan/kecurian/tidak menerima Token kepada Pentadbir MyGPKI (SAP/SA/AP) dan Meja Bantuan MyGPKI bagi tujuan pembatalan Sijil Digital Token.

b. Pengguna MyGPKI membuat permohonan pembatalan Token melalui Sistem MyGPKI setelah menerima notifikasi e-mel pengesahan Token hilang/dicuri/tidak diterima daripada Meja Bantuan MyGPKI.

c. Pentadbir MyGPKI (SAP/SA/AP) mengesahkan permohonan pembatalan Token setelah menerima permohonan pembatalan tersebut.

d. Permohonan pembatalan Sijil Digital Pengguna yang tidak disahkan oleh Pentadbir MyGPKI (SAP/SA/AP) akan ditolak secara automatik oleh Sistem MyGPKI dan pengguna perlu memohon semula.

e. Pentadbir MyGPKI (Admin) meluluskan permohonan pembatalan setelah permohonan pembatalan disahkan oleh Pentadbir MyGPKI (SAP/SA/AP).

f. CA memproses permohonan pembatalan Sijil Digital Pengguna setelah menerima kelulusan pembatalan daripada Pentadbir MyGPKI (Admin).

g. Pengguna MyGPKI mengemukakan permohonan penggantian setelah proses permohonan pembatalan sijil selesai.

h. Pengguna MyGPKI memulangkan Token dengan segera sekiranya Token yang hilang telah dijumpai semula kepada Agensi Peneraju.

7.5.5 Sijil Digital Pengguna yang rosak ialah Sijil Digital Pengguna yang mempunyai kesilapan pada maklumat (nama atau nombor MyKad) Pengguna MyGPKI atau Sijil Digital Pengguna yang tidak boleh digunakan (*corrupted*). Tindakan berikut perlu diambil oleh pihak yang terlibat sekiranya Sijil Digital Pengguna didapati rosak:

a. Pengguna MyGPKI membuat pengujian terhadap Sijil Digital Pengguna yang rosak melalui Agen MyGPKI.

b. Pengguna MyGPKI melaporkan kerosakan Sijil Digital Pengguna kepada Pentadbir MyGPKI (SAP/SA/AP) dan Meja Bantuan MyGPKI bagi tujuan pembatalan Sijil Digital Pengguna.

c. Pengguna MyGPKI membuat permohonan pembatalan Sijil Digital Pengguna melalui Sistem MyGPKI setelah menerima notifikasi e-mel pengesahan Sijil Digital Pengguna rosak.

d. Pentadbir MyGPKI (SAP/SA/AP) mengesahkan permohonan pembatalan Sijil Digital Pengguna setelah menerima permohonan pembatalan tersebut.

e. Permohonan pembatalan Sijil Digital Pengguna yang tidak disahkan oleh Pentadbir MyGPKI (SAP/SA/AP) akan ditolak secara automatik oleh Sistem MyGPKI dan pengguna perlu memohon semula.

f. Pentadbir MyGPKI (Admin) meluluskan permohonan pembatalan setelah permohonan pembatalan disahkan oleh Pentadbir MyGPKI (SAP/SA/AP).

g. CA memproses permohonan pembatalan Sijil Digital Pengguna setelah menerima kelulusan pembatalan daripada Pentadbir MyGPKI (Admin).

h. Bagi pengguna Sijil Digital Token, Pengguna MyGPKI hendaklah memulangkan Token yang disahkan rosak kepada Agensi Peneraju setelah permohonan pembatalan dikemukakan.

i. Pengguna MyGPKI mengemukakan permohonan penggantian setelah proses permohonan pembatalan sijil selesai.

7.5.6 Pengguna MyGPKI boleh mengemukakan permohonan pertukaran Medium Sijil Digital Pengguna sekiranya terdapat keperluan bagi mengakses Sistem ICT Kerajaan yang tidak menyokong Medium Sijil Digital Pengguna sedia ada. Tindakan berikut perlu diambil oleh pihak yang terlibat dalam proses pertukaran Medium Sijil Digital Pengguna:

a. Pengguna MyGPKI melaporkan kepada Pentadbir MyGPKI (SAP/SA/AP) dan membuat aduan kepada Meja Bantuan MyGPKI bagi tujuan pembatalan Sijil Digital Pengguna.

b. Pengguna MyGPKI membuat permohonan pembatalan setelah menerima notifikasi e-mel maklum balas pengesahan daripada Meja Bantuan MyGPKI.

c. Pentadbir MyGPKI (SAP/SA/AP) mengesahkan permohonan pembatalan Sijil Digital Pengguna setelah menerima permohonan pembatalan tersebut.

d. Permohonan pembatalan Sijil Digital Pengguna yang tidak disahkan oleh Pentadbir MyGPKI (SAP/SA/AP) akan ditolak secara automatik oleh Sistem MyGPKI dan pengguna perlu memohon semula.

e. Pentadbir MyGPKI (Admin) meluluskan permohonan pembatalan setelah permohonan pembatalan tersebut disahkan oleh Pentadbir MyGPKI (SAP/SA/AP).

f. CA memproses permohonan pembatalan Sijil Digital Pengguna setelah menerima kelulusan pembatalan daripada Pentadbir MyGPKI (Admin).

g. Pengguna MyGPKI hendaklah memulangkan Token sedia ada (jika berkaitan) kepada Agensi Peneraju.

h. Pentadbir MyGPKI (Admin) akan mendaftarkan pengguna dalam Sistem MyGPKI bagi Sistem ICT Kerajaan yang baharu dengan membuat pertukaran Medium Sijil Digital Pengguna setelah disahkan oleh Pentadbir MyGPKI (SAP/SA/AP).

i. Pengguna MyGPKI hendaklah mengemukakan permohonan Sijil Digital Pengguna bagi Medium Sijil Digital Pengguna yang terkini melalui Sistem MyGPKI.

7.5.7 Antara lain-lain sebab pembatalan dan penggantian ialah Token sedia ada yang tidak menyokong perkakasan dan teknologi baharu seperti penggunaan algoritma *Elliptic Curve Cryptography* (ECC). Berikut ialah tindakan lanjut yang perlu diambil:

a. Pengguna MyGPKI membuat pengujian pengesahan terhadap kegagalan penggunaan Token pada perkakasan dan teknologi baharu melalui Agen MyGPKI.

b. Pengguna MyGPKI melaporkan kegagalan penggunaan Token sedia ada kepada Pentadbir MyGPKI (SAP/SA/AP) dan membuat aduan kepada Meja Bantuan MyGPKI bagi tujuan pembatalan Sijil Digital Token.

c. Pengguna MyGPKI membuat permohonan pembatalan melalui Sistem MyGPKI setelah menerima notifikasi e-mel maklum balas pengesahan daripada Meja Bantuan MyGPKI.

d. Pentadbir MyGPKI (SAP/SA/AP) mengesahkan permohonan pembatalan Token setelah menerima permohonan pembatalan tersebut.

e. Permohonan pembatalan Sijil Digital Pengguna yang tidak disahkan oleh Pentadbir MyGPKI (SAP/SA/AP) akan ditolak secara automatik oleh Sistem MyGPKI dan pengguna perlu memohon semula.

f. Pentadbir MyGPKI (Admin) meluluskan permohonan pembatalan setelah permohonan pembatalan disahkan oleh Pentadbir MyGPKI (SAP/SA/AP).

g. CA akan memproses permohonan pembatalan Sijil Digital Pengguna setelah menerima kelulusan pembatalan daripada Pentadbir MyGPKI (Admin).

h. Pengguna MyGPKI memulangkan Token sedia ada kepada Agensi Peneraju setelah permohonan pembatalan dikemukakan.

i. Pengguna MyGPKI mengemukakan permohonan Sijil Digital Pengguna bagi jenis medium Sijil Digital yang terkini setelah proses permohonan pembatalan sijil selesai.

7.5.8 Terdapat 2 situasi bagi permohonan pembatalan yang tidak memerlukan penggantian Sijil Digital Pengguna iaitu Pengguna MyGPKI tidak lagi mempunyai sebarang peranan di dalam Sistem ICT Kerajaan dan penyalahgunaan Sijil Digital Pengguna.

7.5.9 Sijil Digital Pengguna hendaklah dibatalkan bagi tujuan keselamatan sekiranya Pengguna MyGPKI tidak lagi mempunyai peranan dalam Sistem ICT Kerajaan atau pengguna telah tamat perkhidmatan, bersara atau meninggal dunia. Tindakan yang perlu diambil dalam proses pembatalan Sijil Digital Pengguna ialah seperti yang berikut:

a. Pengguna MyGPKI/Pentadbir MyGPKI (SAP/SA/AP) membuat permohonan pembatalan Sijil Digital Pengguna melalui Sistem MyGPKI.

b. Pentadbir MyGPKI (SAP/SA/AP) mengesahkan permohonan pembatalan Sijil Digital Pengguna setelah menerima permohonan pembatalan tersebut.

c. Pentadbir MyGPKI (Admin) meluluskan permohonan pembatalan setelah permohonan pembatalan disahkan oleh Pentadbir MyGPKI (SAP/SA/AP).

d. CA akan memproses permohonan pembatalan Sijil Digital Pengguna setelah menerima kelulusan pembatalan daripada Pentadbir MyGPKI (Admin).

e. Pengguna MyGPKI/ Pentadbir MyGPKI (SAP/SA/AP) hendaklah memulangkan Token sedia ada kepada Agensi Peneraju setelah permohonan pembatalan dikemukakan.

7.5.10 Penyalahgunaan Sijil Digital Pengguna boleh berlaku disebabkan oleh penggunaan Sijil Digital Pengguna secara tidak sah sama ada oleh pemilik sendiri atau individu lain. Sekiranya telah disahkan terdapat penyalahgunaan Sijil Digital Pengguna oleh pihak berkuasa atau Agensi Pelaksana, tindakan berikut perlu dilaksanakan oleh semua pihak yang terlibat:

a. Pentadbir Sistem ICT Kerajaan membuat sekatan capaian kepada sistem bagi pengguna Sistem ICT Kerajaan yang terlibat.

b. Pentadbir MyGPKI (SAP) melaporkan penyalahgunaan Sijil Digital Pengguna kepada Pentadbir MyGPKI (Admin) menerusi Meja Bantuan MyGPKI.

c. Pentadbir MyGPKI (SAP) membuat permohonan pembatalan Sijil Digital Pengguna melalui Sistem MyGPKI.

d. Pentadbir MyGPKI (Admin) akan meluluskan permohonan pembatalan setelah permohonan pembatalan disahkan oleh Pentadbir MyGPKI (SAP).

e. CA akan memproses pembatalan Sijil Digital Pengguna setelah menerima pengesahan pembatalan daripada Pentadbir MyGPKI (Admin).

f. Pentadbir MyGPKI (SAP) hendaklah memulangkan Token kepada Agensi Peneraju setelah pembatalan selesai dilaksanakan.

7.6 Permohonan Penggantungan Sementara Sijil Digital Pengguna

7.6.1 Terdapat 2 situasi bagi permohonan penggantungan sementara Sijil Digital Pengguna iaitu bagi pengguna yang terlibat dalam siasatan penyalahgunaan Sijil Digital Pengguna dan bagi pengguna yang mengambil cuti dengan tempoh minimum selama 3 bulan.

7.6.2 Sijil Digital Pengguna boleh digantung sementara bagi kes penyalahgunaan sijil yang masih dalam tempoh siasatan oleh pihak berkuasa. Proses penggantungan sementara Sijil Digital Pengguna melibatkan perkara berikut:

a. Pentadbir Sistem ICT Kerajaan membuat sekatan akses kepada Sistem ICT Kerajaan bagi Pengguna MyGPKI yang terlibat.

b. Pentadbir MyGPKI (SAP) melaporkan dan mengemukakan permohonan penggantungan sementara Sijil Digital Pengguna melalui Sistem MyGPKI.

c. Pentadbir MyGPKI (Admin) meluluskan permohonan penggantungan sementara setelah permohonan diterima dan Sijil Digital Pengguna tersebut tidak boleh digunakan sepanjang tempoh penggantungan.

d. Pihak berkuasa menyimpan Sijil Digital Token untuk tujuan siasatan sekiranya terdapat keperluan.

e. Pentadbir MyGPKI (SAP) mengemukakan permohonan penamatan penggantungan sementara kepada Agensi Peneraju sekiranya proses siasatan telah selesai.

f. Pentadbir MyGPKI (Admin) akan meluluskan permohonan penamatan penggantungan sementara.

g. Pentadbir MyGPKI (SAP) akan mengemukakan permohonan pembatalan Sijil Digital Pengguna sekiranya Pengguna MyGPKI didapati bersalah.

7.6.3 Sijil Digital Pengguna juga boleh digantung sementara bagi situasi melibatkan Pengguna MyGPKI yang mengambil cuti dengan tempoh minimum selama 3 bulan. Proses penggantungan sementara Sijil Digital Pengguna melibatkan perkara yang berikut:

a. Pentadbir Sistem ICT Kerajaan membuat sekatan akses kepada Sistem ICT Kerajaan bagi Pengguna MyGPKI yang terlibat.

b. Pentadbir MyGPKI (SAP/SA/AP) melapor dan mengemukakan permohonan penggantungan sementara Sijil Digital Pengguna melalui Sistem MyGPKI.

c. Pentadbir MyGPKI (Admin) meluluskan permohonan penggantungan sementara setelah permohonan diterima dan Sijil Digital Pengguna tersebut tidak boleh digunakan.

d. Pengguna MyGPKI menyimpan Sijil Digital Token dengan selamat dan tidak perlu dipulangkan kepada Agensi Peneraju.

e. Sekiranya Pengguna MyGPKI tamat bercuti, Pentadbir MyGPKI (SAP/SA/AP) mengemukakan permohonan penamatan penggantungan sementara melalui Sistem MyGPKI kepada Agensi Peneraju.

f. Pentadbir MyGPKI (Admin) akan meluluskan permohonan penamatan penggantungan sementara setelah mendapat pengesahan daripada Pentadbir MyGPKI (SAP/SA/AP).

7.7 Semakan Status Permohonan Sijil Digital Pengguna

7.7.1 Semakan status permohonan Sijil Digital Pengguna bagi permohonan baharu, pembaharuan, penggantungan, pembatalan atau penggantian boleh dibuat melalui Sistem MyGPKI seperti yang berikut:

a. Pentadbir MyGPKI (Admin/SAP/SA/AP) menyemak status permohonan Sijil Digital Pengguna melalui Sistem MyGPKI.

b. Pengguna MyGPKI juga boleh menyemak status permohonan Sijil Digital Pengguna melalui MyGPKI Mobile.

BAB 8: PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PELAYAN

8.1 Pengenalan

8.1.1 Sijil Digital Pelayan digunakan oleh Agensi Sektor Awam bagi tujuan pengesahan identiti dan maklumat organisasi bagi Sistem ICT Kerajaan, laman web atau portal yang diakses oleh pengguna. Sijil Digital Pelayan juga digunakan bagi tujuan penyulitan data dan maklumat yang sedang dipindahkan menerusi Internet bagi mengelakkan data dan maklumat dipintas oleh penggodam.

8.1.2 Terdapat 3 jenis Sijil Digital Pelayan iaitu Sijil Digital Pelayan *Single* Domain, Sijil Digital Pelayan Multi Domain dan Sijil Digital Pelayan *Wildcard* yang disediakan di bawah Perkhidmatan MyGPKI. Tempoh sah laku Sijil Digital Pelayan adalah selama 12 bulan, tertakluk kepada polisi semasa CA. Agensi Sektor Awam perlu mengenal pasti keperluan sebenar jenis Sijil Digital Pelayan yang bersesuaian dengan Sistem ICT Kerajaan, laman web atau portal agensi.

8.1.3 Permohonan Sijil Digital Pelayan hendaklah dikemukakan oleh agensi melalui Sistem MyGPKI. Antara kemudahan yang terdapat pada Sistem MyGPKI ialah seperti yang berikut:

a. Permohonan baharu dan pembaharuan Sijil Digital Pelayan.
b. Permohonan pembatalan Sijil Digital Pelayan.
c. Semakan status permohonan Sijil Digital Pelayan.

8.2 Pengurusan Pembekalan Sijil Digital Pelayan

8.2.1 Pengurusan Pembekalan Sijil Digital Pelayan meliputi permohonan baharu, pembaharuan, pembatalan dan penggantian Sijil Digital Pelayan. Pihak-pihak yang terlibat dalam proses pengeluaran Sijil Digital Pelayan ialah Agensi Sektor Awam, Agensi Peneraju, CA dan Prinsipal CA (pengeluar sijil) manakala pihak yang terlibat dalam pengurusan Sijil Digital Pelayan terdiri daripada Pemohon, Pegawai Teknikal dan Pegawai Pengesah.

8.2.2 Agensi hendaklah memenuhi syarat-syarat seperti di bawah dalam mengemukakan permohonan pembekalan Sijil Digital Pelayan:

a. Hanya Agensi Sektor Awam yang terdiri daripada Perkhidmatan Awam Persekutuan dan Badan Berkanun Persekutuan Yang Tidak Diasingkan Pengurusan Saraannya sahaja boleh mengemukakan permohonan Sijil Digital Pelayan kepada Agensi Peneraju. Tanggungan kos bagi agensi selain daripada yang dinyatakan ialah di bawah tanggungan masing-masing.

b. Pelayan Sistem ICT Kerajaan, laman web atau portal mempunyai tahap keselamatan yang sederhana atau tinggi bagi melindungi maklumat rahsia rasmi.

c. Sistem ICT Kerajaan, laman web atau portal digunakan bagi menyokong fungsi teras agensi.

d. Capaian bagi Sistem ICT Kerajaan, laman web atau portal hendaklah menerusi Internet.

e. Domain/subdomain Sistem ICT Kerajaan, laman web atau portal hendaklah telah diluluskan oleh pengurusan agensi dan telah didaftarkan dengan pendaftar domain rasmi .MY iaitu MyNIC Berhad.

f. Nama domain/subdomain dan jenis Sijil Digital Pelayan hendaklah kekal setelah permohonan diluluskan dan sepanjang tempoh sah laku Sijil Digital Pelayan.

8.2.3 Agensi Sektor Awam hendaklah merujuk Lampiran 4: Format Laporan Penilaian Risiko Laman Web Dan Portal bagi menentukan penggunaan jenis Sijil Digital Pelayan yang bersesuaian.

8.3 Permohonan Baharu Sijil Digital Pelayan

8.3.1 Permohonan baharu Sijil Digital Pelayan boleh dikemukakan oleh agensi melalui Sistem MyGPKI sekiranya telah memenuhi syarat-syarat yang telah ditetapkan. Permohonan baharu Sijil Digital Pelayan melibatkan proses-proses yang berikut:

a. Agensi hendaklah melaksanakan Penilaian Risiko Laman Web dan Portal Agensi Sektor Awam dan menyediakan laporan penilaian risiko tersebut. Format laporan penilaian risiko boleh dirujuk pada Lampiran A4: Format Laporan Penilaian Risiko Laman Web Dan Portal.

b. Pentadbir Pelayan (Pegawai Teknikal) hendaklah menjana fail *Certificate Signing Request* (CSR) pada pelayan yang terlibat mengikut saiz kunci (*key length*) dan algoritma kriptografi yang ditetapkan.

c. Pendaftaran Pentadbir Sijil Digital Pelayan perlu dilaksanakan terlebih dahulu sekiranya belum pernah membuat permohonan Sijil Digital Pelayan melalui Sistem MyGPKI.

d. Pentadbir Pelayan (Pegawai Pemohon) hendaklah mengemukakan permohonan Sijil Digital Pelayan melalui Sistem MyGPKI. Semua maklumat perlu dikemukakan dengan lengkap dan tepat.

e. Pentadbir Pelayan (Pegawai Pemohon) hendaklah mengemukakan permohonan rasmi berserta laporan penilaian risiko kepada Agensi Peneraju melalui Sistem MyGPKI.

f. Pentadbir MyGPKI (*Admin*) menyemak dan meluluskan permohonan Sijil Digital Pelayan setelah permohonan lengkap diterima.

g. Prinsipal CA membuat audit pengesahan organisasi dan domain bagi setiap domain/subdomain berdasarkan permohonan Sijil Digital Pelayan. CA menjana dan menghantar Sijil Digital Pelayan selepas mendapat kelulusan Prinsipal CA.

h. Pentadbir Pelayan (Pegawai Teknikal) di agensi hendaklah memasang Sijil Digital Pelayan pada pelayan Sistem ICT Kerajaan, laman web atau portal setelah menerima sijil daripada CA.

i. Pentadbir Pelayan (Pegawai Pemohon) di agensi hendaklah membuat pengesahan penerimaan dan pemasangan Sijil Digital Pelayan.

8.4 Permohonan Pembaharuan Sijil Digital Pelayan

8.4.1 Permohonan pembaharuan Sijil Digital Pelayan boleh dikemukakan oleh agensi melalui Sistem MyGPKI sekiranya telah memenuhi syarat-syarat yang telah ditetapkan. Berikut ialah tindakan yang perlu diambil oleh semua pihak yang terlibat dalam melaksanakan proses permohonan pembaharuan Sijil Digital Pelayan:

a. Pentadbir Pelayan (Pegawai Pemohon) hendaklah membuat permohonan pembaharuan Sijil Digital Pelayan melalui Sistem MyGPKI seawal 30 hari sebelum tamat tempoh sijil sedia ada.

b. Pentadbir Pelayan (Pegawai Pemohon) hendaklah membuat pengemaskinian Laporan Penilaian Risiko Laman Web dan Portal sedia ada sekiranya terdapat perubahan maklumat.

c. Pentadbir Pelayan (Pegawai Teknikal) hendaklah menjana fail *Certificate Signing Request* (CSR) yang baharu pada pelayan yang terlibat mengikut saiz kunci (*key length*) dan algoritma kriptografi yang ditetapkan.

d. Pentadbir Pelayan (Pegawai Pemohon) hendaklah mengemukakan permohonan Sijil Digital Pelayan melalui Sistem MyGPKI.

e. Pentadbir Pelayan (Pegawai Pemohon) hendaklah mengemukakan permohonan rasmi berserta laporan penilaian risiko kepada Agensi Peneraju melalui Sistem MyGPKI.

f. Pentadbir MyGPKI (Admin) menyemak dan meluluskan permohonan Sijil Digital Pelayan setelah permohonan lengkap diterima.

g. Prinsipal CA (pengeluar sijil) membuat audit pengesahan organisasi dan domain bagi setiap domain/subdomain berdasarkan permohonan Sijil Digital Pelayan. CA menjana dan menghantar Sijil Digital Pelayan selepas mendapat kelulusan Prinsipal CA.

h. Pentadbir Pelayan (Pegawai Teknikal) di agensi hendaklah memasang Sijil Digital Pelayan pada pelayan Sistem ICT Kerajaan, laman web atau portal setelah menerima sijil daripada CA.

i. Pentadbir Pelayan (Pegawai Pemohon) di agensi hendaklah membuat pengesahan penerimaan dan pemasangan Sijil Digital Pelayan.

8.5 Permohonan Pembatalan Sijil Digital Pelayan

8.5.1 Terdapat 3 situasi yang memerlukan proses pembatalan Sijil Digital Pelayan iaitu sijil yang rosak, berlaku penyalahgunaan sijil (*compromised*) atau domain/subdomain tidak aktif. Sijil Digital Pelayan yang rosak merujuk kepada sijil yang mempunyai kesilapan maklumat atau tidak dapat dibaca (*unreadable*).

8.5.2 Berikut ialah tindakan yang perlu diambil oleh semua pihak yang terlibat dalam melaksanakan proses permohonan pembatalan Sijil Digital Pelayan:

a. Sekiranya Sijil Digital Pelayan disahkan rosak atau berlaku penyalahgunaan sijil (*compromised*), Pentadbir Pelayan (Pegawai Pemohon/Pegawai Teknikal/Pegawai Pengesah) hendaklah melaporkan kepada Meja Bantuan MyGPKI bagi tujuan bantuan teknikal dan pengesahan kerosakan sijil atau penyalahgunaan sijil (*compromised*).

b. Sekiranya domain/subdomain tidak aktif, Pentadbir Pelayan (Pegawai Pemohon/Pegawai Teknikal/Pegawai Pengesah) hendaklah melaporkan kepada Agensi Peneraju untuk tujuan rekod dan pemantauan.

c. Pentadbir Pelayan (Pegawai Pemohon) membuat permohonan pembatalan melalui Sistem MyGPKI setelah menerima maklum balas daripada Meja Bantuan MyGPKI atau Agensi Peneraju.

d. Pentadbir MyGPKI (Admin) meluluskan permohonan pembatalan Sijil Digital Pelayan setelah permohonan pembatalan diterima.

e. CA memproses pembatalan Sijil Digital Pelayan setelah menerima kelulusan daripada Pentadbir MyGPKI (Admin).

f. Pentadbir Pelayan (Pegawai Pemohon) memohon penggantian Sijil Digital Pelayan sekiranya perlu melalui Sistem MyGPKI.

8.6 Semakan Status Permohonan Sijil Digital Pelayan

8.6.1 Semakan status permohonan Sijil Digital Pelayan bagi permohonan baharu, pembaharuan, pembatalan atau penggantian boleh dibuat melalui Sistem MyGPKI seperti yang berikut:

a. Pentadbir Pelayan (Pegawai Pemohon/Pegawai Teknikal/Pegawai Pengesah) menyemak status permohonan Sijil Digital Pelayan melalui Sistem MyGPKI.

b. Pentadbir Pelayan (Pegawai Pemohon/Pegawai Teknikal/Pegawai Pengesah) menyemak status permohonan Sijil Digital Pelayan melalui MyGPKI *Mobile*.

8.7 Penilaian Risiko Dalam Konteks Laman Web/ Portal

8.7.1 Dalam konteks laman web/portal, penilaian risiko dilaksanakan untuk mengenal pasti langkah-langkah kawalan yang boleh menangani risiko berkaitan kerahsiaan serta pengesahan identiti terhadap data dan maklumat Sistem ICT Kerajaan. Penilaian risiko ini hendaklah dilaksanakan sekiranya Sistem ICT Kerajaan, laman web atau portal:

a. Mengandungi maklumat rasmi.
b. Dikategorikan sebagai sistem teras atau strategik.
c. Berkaitan keselamatan negara.
d. Melibatkan transaksi kewangan.

8.7.2 Proses penilaian risiko terhadap fungsi teras agensi yang disokong oleh Sistem ICT Kerajaan melibatkan enam langkah utama dan dijelaskan dengan lebih terperinci pada **Lampiran A2**: Tatacara Pelaksanaan Penilaian Risiko Dalam Konteks Perkhidmatan MyGPKI.

8.7.3 Agensi perlu menyediakan laporan penilaian risiko bagi laman web atau portal seperti **Lampiran A4**: Format Laporan Penilaian Risiko Laman Web Dan Portal.

BAB 9: PERKHIDMATAN MEJA BANTUAN DAN KHIDMAT SOKONGAN TEKNIKAL

9.1 Pengenalan

9.1.1 Perkhidmatan meja bantuan dan khidmat sokongan teknikal disediakan kepada Pengguna MyGPKI untuk membuat aduan atau mengemukakan pertanyaan berkaitan Perkhidmatan MyGPKI.

9.1.2 Pengurusan bagi perkhidmatan meja bantuan dan sokongan teknikal dilaksanakan melalui Sistem *Helpdesk* MyGPKI. Oleh itu, semua aduan atau pertanyaan berkaitan Perkhidmatan MyGPKI hendaklah dikemukakan melalui sistem ini.

9.2 Perkhidmatan Meja Bantuan MyGPKI

9.2.1 Meja Bantuan MyGPKI merujuk kepada perkhidmatan yang disediakan bagi mengurus dan mengendalikan tiket aduan berkaitan permasalahan dan pertanyaan yang diterima berkaitan Perkhidmatan MyGPKI.

9.2.2 Semua aduan atau pertanyaan hendaklah dibuat secara rasmi menerusi Sistem Meja Bantuan MyGPKI. Pengguna MyGPKI hendaklah terlebih dahulu merujuk kepada panduan pengguna dan soalan-soalan lazim dalam Sistem MyGPKI sebelum membuat aduan atau mengemukakan pertanyaan.

9.2.3 Berikut merupakan proses-proses yang terlibat dalam mengemukakan aduan permasalahan atau pertanyaan kepada Meja Bantuan MyGPKI:

a. Pengguna MyGPKI hendaklah mengemukakan butiran maklumat yang terdiri daripada nama penuh, nombor MyKad, nombor telefon pejabat dan telefon bimbit, e-mel, butiran dan lampiran permasalahan sekiranya ada.

b. Pegawai Meja Bantuan MyGPKI akan menjana tiket mengikut aduan permasalahan atau pertanyaan yang dikemukakan oleh Pengguna. Maklum balas dan tindakan penyelesaian bagi aduan permasalahan dan

pertanyaan akan dilaksanakan mengikut keutamaan tiket dan tempoh tindak balas ialah seperti **Jadual 16** berikut:

Jadual 16: Tempoh Tindak Balas Meja Bantuan MyGPKI

Bil.	Keutamaan	Keterangan	Tempoh Masa Tindak Balas Maksimum	Tempoh Masa Penyelesaian Maksimum
1.	Tindak Balas Awal (T^0)	Tindak balas daripada Meja Bantuan selepas aduan dilaporkan	1 jam	-
2.	Masa tindak balas dalam talian (T^1)	Tindakan penyelesaian menerusi e-mel, telefon atau capaian jauh (*remote access*) ke komputer pengguna selepas aduan diterima		
	Keutamaan 1	Keseluruhan fungsi PKI tidak dapat digunakan oleh kesemua pengguna untuk melaksanakan transaksi Sistem ICT Kerajaan	2 jam	4 jam
	Keutamaan 2	Keseluruhan fungsi PKI tidak dapat digunakan oleh sebahagian pengguna untuk melaksanakan transaksi Sistem ICT Kerajaan	2 jam	8 jam
	Keutamaan 3	Sebahagian fungsi utama PKI tidak dapat digunakan oleh semua atau sebahagian pengguna untuk melaksanakan transaksi Sistem ICT Kerajaan	2 jam	24 jam
	Keutamaan 4	Sebahagian fungsi bukan utama PKI tidak dapat digunakan oleh sebahagian pengguna untuk melaksanakan transaksi Sistem ICT Kerajaan atau lain-lain pertanyaan berkaitan atau tidak berkaitan Perkhidmatan MyGPKI	2 jam	48 jam

c. Pengguna MyGPKI hendaklah memberi maklum balas bagi tiket aduan permasalahan atau pertanyaan yang diterima mengikut tempoh masa yang ditetapkan seperti **Jadual 17**. Tiket aduan permasalahan atau pertanyaan baharu akan dibuka sekiranya Pengguna MyGPKI gagal memberi maklum balas mengikut tempoh masa maklum balas yang ditetapkan:

Jadual 17: Tempoh Maklum Balas Pengguna MyGPKI

Bil.	Keutamaan	Tempoh Masa Penyelesaian Maksimum	Tempoh Masa Maklum Balas Pengguna MyGPKI
1.	Keutamaan 1	4 jam	2 jam
2.	Keutamaan 2	8 jam	4 jam
3.	Keutamaan 3	24 jam	6 jam
4.	Keutamaan 4	48 jam	8 jam

d. Sekiranya permasalahan tidak dapat diselesaikan secara dalam talian menerusi Perkhidmatan Meja Bantuan MyGPKI, tiket akan dimajukan kepada pegawai sokongan teknikal untuk bantuan lanjut atau sokongan teknikal secara *on-site* akan diberikan kepada Pengguna MyGPKI.

e. Notifikasi peringatan seperti berikut akan dihantar menerusi Sistem MyGPKI sekiranya tiada maklum balas diterima daripada Pengguna MyGPKI:

i. Notifikasi pertama akan dihantar kepada Pengguna MyGPKI sekiranya tiada sebarang maklum balas diterima oleh Pasukan Meja Bantuan MyGPKI selepas 8 jam (waktu bekerja) e-mel langkah-langkah penyelesaian dihantar kepada Pengguna MyGPKI.

ii. Notifikasi kedua akan dihantar kepada Pengguna MyGPKI sekiranya Pengguna MyGPKI tidak memberi sebarang maklum balas selepas 8 jam (waktu bekerja) e-mel notifikasi peringatan pertama dihantar kepada Pengguna MyGPKI.

f. Tiket akan ditutup sekiranya aduan permasalahan atau pertanyaan telah selesai diambil tindakan oleh semua pihak yang terlibat. Notifikasi penutupan tiket juga akan dihantar sekiranya tiada maklum balas diterima selepas 8 jam (waktu bekerja) notifikasi peringatan kedua dihantar kepada Pengguna MyGPKI.

9.3 Khidmat Sokongan Teknikal

9.3.1 Sokongan teknikal secara *on-site* akan diberikan kepada Pengguna MyGPKI sekiranya permasalahan tidak dapat diselesaikan secara dalam talian selepas mendapat kelulusan daripada Agensi Peneraju.

9.3.2 Perkhidmatan Sokongan Teknikal di lokasi Pengguna akan dilaksanakan sekiranya Pengguna telah bersetuju dengan tarikh dan masa perkhidmatan Sokongan Teknikal yang akan dilaksanakan serta wakil daripada pihak Agensi Peneraju dan pihak agensi hendaklah hadir bersama. Pegawai teknikal akan melaksanakan proses pencarisilapan (*troubleshooting*) permasalahan dalam tempoh masa yang telah ditetapkan di lokasi Pengguna MyGPKI.

BAB 10: KHIDMAT NASIHAT DAN KONSULTASI

10.1 Pengenalan

10.1.1 Khidmat nasihat dan konsultasi disediakan oleh Agensi Peneraju kepada Agensi Sektor Awam bagi menangani isu atau masalah yang telah dikenal pasti atau membantu agensi untuk melaksanakan projek berkaitan Penggunaan PKI dalam Sistem ICT Kerajaan. Khidmat nasihat dan konsultasi yang disediakan merangkumi perkara-perkara berikut:

a. Penggunaan PKI dalam Sistem ICT Kerajaan.
b. Pelaksanaan integrasi Sistem ICT Kerajaan dan Sistem MyGPKI.
c. Perancangan dan pelaksanaan Perkhidmatan MyGPKI di Agensi Sektor Awam.

10.2 Khidmat Nasihat

10.2.1 Khidmat nasihat berkaitan Perkhidmatan MyGPKI diberikan oleh Agensi Peneraju kepada Agensi Sektor Awam bagi menangani isu atau masalah yang telah dikenal pasti dan boleh diselesaikan dengan kadar segera. Panduan dan bimbingan kepada Agensi Sektor Awam akan diberikan semasa sesi khidmat nasihat.

10.3 Khidmat Konsultasi

10.3.1 Khidmat konsultasi berkaitan Perkhidmatan MyGPKI diberikan oleh Agensi Peneraju kepada Agensi Sektor Awam bagi pelaksanaan projek dalam penggunaan PKI. Skop perkhidmatan konsultasi yang diberikan merangkumi perkara-perkara berikut:

a. Teknikal

Agensi Peneraju menyediakan khidmat konsultasi berkaitan penggunaan PKI dalam Sistem ICT Kerajaan yang meliputi:

i. Pelaksanaan penilaian risiko.
ii. Integrasi dengan Sistem MyGPKI.
iii. Pengujian fungsi PKI.
iv. Pelaksanaan fungsi PKI.

b. Operasi

Menyedia khidmat konsultasi bagi perancangan dan pelaksanaan Perkhidmatan MyGPKI di Agensi Sektor Awam, tadbir urus Pentadbir MyGPKI dan Pengguna MyGPKI, pembekalan serta pengurusan Sijil Digital Pengguna dan pembekalan Sijil Digital Pelayan.

10.3.2 Agensi Sektor Awam yang ingin mendapatkan khidmat nasihat dan konsultasi hendaklah mengemukakan permohonan rasmi melalui surat atau e-mel kepada Agensi Peneraju.

BAB 11: PENUTUP

Agensi Sektor Awam hendaklah memahami serta merujuk kepada garis panduan teknikal dan operasi ini bagi mengenal pasti keperluan Perkhidmatan MyGPKI dalam penggunaan Sijil Digital untuk Sistem ICT Kerajaan. Garis panduan ini juga hendaklah dibaca bersekali dengan Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* – MyGPKI) serta Arahan Keselamatan (Semakan dan Pindaan 2017) bagi memastikan kelancaran dalam penggunaan Perkhidmatan MyGPKI secara keseluruhannya. Prosedur serta SOP terperinci mengenai manual pengurusan pengguna dan sijil digital kerajaan bagi Perkhidmatan MyGPKI pula boleh dirujuk melalui Sistem MyGPKI.

BIBLIOGRAFI

1. Akta Tandatangan Digital 1997 (Akta 562). Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) (1998). Cyberjaya, Selangor. Kementerian Komunikasi dan Multimedia Malaysia (KKMM): Wilayah Persekutuan Putrajaya.

2. Undang-Undang Malaysia Akta 88 – Akta Rahsia Rasmi 1972. Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) (2006). Wilayah Persekutuan Putrajaya. Pesuruhjaya Penyemak Undang-Undang, Malaysia Secara Usaha Sama dengan Percetakan Nasional Malaysia Bhd.

3. Undang-Undang Malaysia Akta 680 Akta Aktiviti Kerajaan Elektronik 2007. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) (2017). Wilayah Persekutuan Putrajaya. Pesuruhjaya Penyemak Undang-Undang Malaysia.

4. Peraturan-Peraturan Tandatangan Digital 1998. Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM). Cyberjaya, Selangor. Kementerian Komunikasi dan Multimedia Malaysia (KKMM).

5. Licensing Guidebook Digital Signature. Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) (2024) (2nd ed.). Cyberjaya, Selangor.

6. Arahan Teknologi Maklumat 2007. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) (2007). Wilayah Persekutuan Putrajaya.

7. Laws of Malaysia: Act 854 – Cyber Security Act 2024. (2024). Wilayah Persekutuan Putrajaya: Agensi Keselamatan Siber Negara (NACSA), Jabatan Perdana Menteri. (2024). Kuala Lumpur: Percetakan Nasional Malaysia Bhd.

8. Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) (2007). Surat Pekeliling Am Bilangan 3 Tahun 2009: Wilayah Persekutuan Putrajaya.

9. Kerry, Cameron F. & Gallagher, Patrick D. (2013). United States of America (USA). FIPS PUB 186-4 Digital Signature Standard (DSS). Federal Information Processing Standards Publication.

10. MS ISO/IEC 27001:2013 Information Security Management System (ISMS) Standard (2013). SIRIM Berhad: Shah Alam, Selangor.

11. RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2018). Institut Piawaian dan Teknologi Kebangsaan (NIST): Maryland, USA.

12. Pelan Risiko MAMPU 2021 - 2025. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) (2021). Wilayah Persekutuan Putrajaya.

13. Arahan Keselamatan (Semakan dan Pindaan 2017). Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (2020). Wilayah Persekutuan Putrajaya.

LAMPIRAN A2

TATACARA PELAKSANAAN PENILAIAN RISIKO DALAM KONTEKS PERKHIDMATAN *GOVERNMENT PUBLIC KEY INFRASTRUCTURE* – MyGPKI

1.1. PENGENALAN

1.1.1 Penilaian Risiko Dalam Konteks Perkhidmatan MyGPKI melibatkan enam proses utama yang berikut dan perlu dilaksanakan oleh Agensi Sektor Awam sebelum mengemukakan permohonan menggunakan Perkhidmatan MyGPKI kepada Agensi Peneraju:

a. Menetapkan Konteks Penilaian Risiko;

i. Langkah 1: Mengenal pasti kategori Sistem ICT Kerajaan, laman web atau portal.
ii. Langkah 2: Mengenal pasti klasifikasi dan peringkat keselamatan data dan maklumat.
iii. Langkah 3: Mengenal pasti nilai data atau maklumat yang terlibat.
iv. Langkah 4: Menentukan kriteria penerimaan risiko.

b. Mengenal Pasti Ancaman;

c. Melaksanakan Analisis dan Menentukan Tahap Risiko.

i. Langkah 1: Mengenal pasti kebarangkalian.
ii. Langkah 2: Mengenal pasti impak.
iii. Langkah 3: Menilai tahap risiko.
iv. Langkah 4: Menentukan tahap risiko.

d. Menentukan Strategi Kawalan Risiko.

e. Pemilihan Kawalan Keselamatan.

f. Pelaporan Penilaian Risiko.

1.2. PENETAPAN KONTEKS PENILAIAN RISIKO

1.2.1 Agensi Sektor Awam hendaklah menetapkan konteks penilaian risiko ke atas Sistem ICT Kerajaan dengan mengenal pasti kategori Sistem ICT Kerajaan,

klasifikasi dan peringkat keselamatan data atau maklumat serta nilai data atau maklumat yang terlibat.

1.2.2 Langkah-langkah yang terlibat dalam menetapkan konteks penilaian risiko terdiri daripada:

a. Langkah 1: Mengenal Pasti Kategori Sistem ICT Kerajaan

Kategori Sistem ICT Kerajaan dalam konteks Perkhidmatan MyGPKI terdiri daripada teras, strategik, sokongan dalaman dan sokongan luaran. Keterangan lanjut bagi setiap kategori ialah seperti **Jadual 18**.

Jadual 18: Kategori Sistem ICT Kerajaan

Bil.	Kategori	Keterangan
1.	Teras	Sistem yang mempunyai keutamaan tertinggi dan memerlukan ketersediaan yang tinggi. Sekiranya berlaku ancaman atau gangguan terhadap sistem dalam tempoh yang singkat akan memberi impak yang tinggi terhadap kewangan, pelanggaran perundangan, ketidakpuasan hati pelanggan, operasi, reputasi organisasi serta pendedahan maklumat rahsia rasmi. Sistem ICT Kerajaan ini mengandungi maklumat rahsia rasmi dan juga berkemungkinan terdapat kebergantungan organisasi luar kepada sistem ini
2.	Strategik	Sistem yang menyokong inisiatif perkhidmatan yang disediakan oleh organisasi. Sekiranya berlaku ancaman atau gangguan kepada Sistem ICT Kerajaan akan menyebabkan impak kepada reputasi organisasi, liabiliti organisasi dan memerlukan kos yang tinggi untuk pemulihan. Sistem ICT Kerajaan ini mengandungi maklumat rahsia rasmi
3.	Sokongan Dalaman	Sistem ICT Kerajaan ini menyokong keperluan operasi organisasi dan hanya mengakses maklumat dalaman organisasi. Sekiranya berlaku ancaman atau gangguan akan memberikan impak yang sederhana terhadap kewangan, fungsi organisasi, reputasi dan memerlukan kos pemulihan yang sederhana
4	Sokongan Umum	Sistem ICT Kerajaan ini merupakan sokongan umum kepada orang awam. Sekiranya berlaku ancaman atau gangguan akan memberikan impak yang rendah terhadap kewangan, fungsi organisasi, reputasi dan memerlukan kos pemulihan yang rendah

b. Langkah 2: Mengenal Pasti Klasifikasi dan Peringkat Keselamatan Data atau Maklumat

Agensi Sektor Awam hendaklah mengenal pasti klasifikasi dan peringkat keselamatan data atau maklumat yang terlibat dalam pelaksanaan penilaian risiko. Klasifikasi data atau maklumat sepertimana yang ditakrifkan dalam Arahan Keselamatan (Semakan dan Pindaan 2017) dan Akta Rahsia Rasmi 1972 (Akta 88) terdiri daripada:

i. Rahsia Rasmi iaitu apa-apa suratan yang dinyatakan dalam jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang menteri, menteri besar atau ketua menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik bawah seksyen 2B Akta 88; dan

ii. Maklumat Rasmi iaitu pengetahuan mengenai perkara rasmi, walau cara mana sekalipun diperoleh, termasuk:

a) Jenis atau kandungan apa-apa dokumen rasmi atau sebahagiannya;
b) Jenis, kegunaan dan komposisi bahan-bahan.
c) Kaedah dan cara menghasilkan serta teknik dan proses yang digunakan untuk pengeluaran.
d) Proses saintifik terutama berkenaan dengan pembuatan senjata dan kelengkapan.
e) Butir-butir kegiatan rasmi yang diperoleh secara lisan.

Peringkat keselamatan data atau maklumat terdiri daripada Rahsia Besar, Rahsia, Sulit, Terhad, Data Terkawal/ Sensitif dan Terbuka. Keterangan bagi setiap peringkat keselamatan ialah seperti **Jadual 19**.

Jadual 19: Peringkat Keselamatan Data atau Maklumat

Bil.	Peringkat Keselamatan Data/Maklumat	Keterangan
1.	Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia, hendaklah diperingkatkan sebagai “Rahsia Besar”
2.	Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan Negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberikan keuntungan besar kepada sesebuah kuasa asing hendaklah diperingkatkan sebagai “Rahsia”
3.	Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan Negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing hendaklah diperingkatkan sebagai “Sulit”
4.	Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan sebagai “Rahsia Besar”, “Rahsia” atau “Sulit” tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan hendaklah diperingkatkan sebagai “Terhad”
5.	Data Terkawal/ Sensitif	Maklumat rasmi yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh mana-mana agensi Kerajaan semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara. Berikut ialah beberapa contoh bagi maklumat rasmi kerajaan: a. Kewangan b. Perubatan c. Kesihatan d. Akademik e. Percukaian f. Perjanjian/kontrak g. Data Kajian

Bil.	Peringkat Keselamatan Data/Maklumat	Keterangan
		h. Pengenalan Peribadi (*Personally Identifiable Information* – PII) *Maklumat Rasmi seperti di atas juga boleh menjadi rahsia rasmi sekiranya pemula (pemilik data) membuat tafsiran risiko yang sepadan dengan salah satu peringkat keselamatan rahsia rasmi yang dimaksudkan
6.	Terbuka	Maklumat rasmi yang telah dibuat saringan dan pengesahan di peringkat pemula data untuk bebas digunakan, dikongsi serta digunakan semula oleh orang awam, agensi kerajaan dan organisasi swasta untuk pelbagai tujuan

c. Langkah 3: Mengenal Pasti Nilai Data atau Maklumat

Agensi Sektor Awam hendaklah mengenal pasti nilai data atau maklumat kepada perkhidmatan utama Agensi Sektor Awam iaitu sama ada tinggi (T), sederhana (S) atau rendah (R). Nilai ini ialah berdasarkan kepentingan data atau maklumat sekiranya data atau maklumat tersebut terjejas bagi setiap ciri keselamatan PKI iaitu kerahsiaan (*confidentiality* – C), kesahihan (*authenticity* – A), integriti (*integrity* – I) dan tanpa sangkalan (*non-repudiation* – N). Semakin penting data atau maklumat tersebut kepada agensi, semakin tinggi nilai data atau maklumat tersebut. Keterangan mengenai nilai tahap keselamatan data atau maklumat mengikut kategori Sistem ICT Kerajaan ialah seperti **Jadual 20** di bawah:

Jadual 20: Nilai Data atau Maklumat

Bil.	Klasifikasi	Peringkat Keselamatan Data/Maklumat	Kategori Sistem ICT Kerajaan			
			Teras	Strategik	Sokongan Dalaman	Sokongan Umum
1.	Rahsia Rasmi	Rahsia Besar	Tinggi			
2.		Rahsia				
3.		Sulit				
4.		Terhad	Sederhana			

Bil.	Klasifikasi	Peringkat Keselamatan Data/Maklumat	Kategori Sistem ICT Kerajaan			
			Teras	Strategik	Sokongan Dalaman	Sokongan Umum
5.	Maklumat Rasmi	Terkawal/ Sensitif	Sederhana			
6.		Terbuka	Rendah			

d. Langkah 4: Menentukan Kriteria Penerimaan Risiko

Kriteria penerimaan risiko membolehkan Agensi Sektor Awam menentukan strategi kawalan risiko yang bersesuaian sama ada risiko tersebut akan diterima atau perlu menentukan strategi kawalan risiko yang lain. Kriteria risiko ini hendaklah ditetapkan sebelum penilaian risiko dilaksanakan. Secara umumnya terdapat 4 pilihan strategi kawalan risiko, iaitu:

i. Pengelakan risiko (*risk avoidance*) ialah membuat keputusan berdasarkan maklumat untuk tidak melibatkan diri atau menarik diri daripada situasi risiko.

ii. Pengurangan risiko (*risk reduction*) ialah mengambil langkah kawalan untuk mengurangkan pendedahan kepada risiko.

iii. Pemindahan risiko (*risk transfer*) ialah memindahkan beban kerugian yang disebabkan oleh risiko kepada pihak lain menerusi perundangan, kontrak, insurans atau lain-lain atau tanggungan risiko bersama-sama dengan pihak lain.

iv. Penerimaan risiko (*risk acceptance*) ialah membuat keputusan berdasarkan maklumat untuk menerima kebarangkalian dan impak risiko tertentu. Strategi ini dipilih sekiranya:

a) Kos untuk mencegah risiko melebihi manfaat yang akan diperoleh dan menerima risiko merupakan opsyen yang lebih sesuai.
b) Tahap risiko rendah dan tidak memerlukan sebarang tindakan pencegahan.

c) Tiada kawalan atau tindakan yang lebih sesuai.

Contoh penentuan kriteria penerimaan risiko ialah seperti **Jadual 21**.

Jadual 21: Kriteria Penerimaan Risiko

Bil.	Tahap Risiko	Strategi Kawalan Risiko
1.	Ekstrem	Kurang/Pindah
2.	Tinggi	Kurang/Pindah
3.	Sederhana	Kurang
4.	Rendah	Kurang/Terima

1.3. MENGENAL PASTI ANCAMAN

1.3.1 Agensi Sektor Awam perlu mengenal pasti kebarangkalian ancaman yang akan berlaku ke atas Sistem ICT Kerajaan tersebut. Jenis ancaman boleh dibahagikan kepada 8 kategori seperti **Jadual 22** berdasarkan ciri-ciri keselamatan maklumat iaitu C, A, I, N bagi Sistem ICT Kerajaan manakala laman web atau portal melibatkan C dan A.

Jadual 22: Kategori Ancaman Kepada Sistem ICT Kerajaan

Bil.	Kategori Ancaman	Keterangan	Ciri-ciri Keselamatan Maklumat			
			C	A	I	N
Sistem ICT Kerajaan						
1.	Penyamaran Identiti (*Spoofing*)	Satu tindakan ancaman yang bertujuan untuk mengakses sistem aplikasi secara tidak sah 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 atau mengubahsuai data seperti pengubahsuaian data dalam pangkalan data dan mengubah data dalam transit antara 2 komputer melalui sesuatu rangkaian terbuka, seperti Internet			√	

Bil.	Kategori Ancaman	Keterangan	Ciri-ciri Keselamatan Maklumat			
			C	A	I	N
3.	Sangkalan (*Repudiation*)	Satu tindakan ancaman keselamatan yang menyebabkan pengguna komputer menafikan tindakan yang telah diambil atau telah mengaku melakukan sesuatu tindakan yang tidak dilakukan				√
4.	Pendedahan Maklumat (*Information Disclosure*)	Tindakan ancaman untuk membaca fail yang tidak diberi akses kepada/atau untuk membaca data dalam transit	√			
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	√	√	√	
Laman Web atau Portal						
7.	*SSL hijacking*	Satu tindakan ancaman di mana penggodam menukar haluan komunikasi trafik Internet pengguna	√	√		
8.	*HTTPS spoofing*	Satu tindakan ancaman di mana penggodam mewujudkan laman web palsu yang menyerupai laman web asal bagi tujuan memindahkan komunikasi kepada pelayan penggodam untuk tujuan pemintasan data atau maklumat yang sedang berinteraksi		√		

1.4. MELAKSANAKAN ANALISIS DAN MENENTUKAN TAHAP RISIKO

1.4.1 Langkah ini membolehkan Agensi Sektor Awam mengenal pasti risiko yang memberi impak kepada Sistem ICT Kerajaan serta perkhidmatan utama Agensi Sektor Awam tersebut. Proses yang terlibat dalam langkah ini ialah mengenal pasti kebarangkalian dan impak kepada setiap ancaman yang dikenal pasti serta menentukan tahap risiko seperti yang berikut:

a. Langkah 1: Mengenal Pasti Kebarangkalian

Agensi Sektor Awam perlu menentukan kebarangkalian ancaman berdasarkan skala seperti **Jadual 23**. Kaedah yang boleh digunakan untuk menentukan kebarangkalian ini adalah dengan memberikan skala satu bagi kebarangkalian rendah hingga skala 5 bagi kebarangkalian tinggi.

Jadual 23: Skala Kebarangkalian

Skala	Definisi	Keterangan
5	Hampir Pasti	Kebarangkalian ancaman berlaku sekurang-kurangnya sekali dalam tempoh 1 - 6 bulan
4	Kemungkinan Tinggi	Kebarangkalian ancaman berlaku sekurang-kurangnya sekali dalam tempoh 7 - 12 bulan
3	Ada Kemungkinan	Kebarangkalian ancaman berlaku sekurang-kurangnya sekali dalam tempoh 2 - 3 tahun
2	Kemungkinan Rendah	Kebarangkalian ancaman berlaku sekurang-kurangnya sekali dalam tempoh 3 - 5 tahun
1	Jarang	Kebarangkalian ancaman tidak akan berlaku dalam tempoh 5 tahun

b. Langkah 2: Mengenal Pasti Impak

Kaedah yang boleh digunakan untuk menentukan impak ini ialah dengan memberikan skala satu bagi impak rendah hingga 5 bagi impak tinggi. Pertimbangan untuk memberikan skala impak perlu mengambil kira jenis ancaman dan langkah kawalan sedia ada. Impak diperoleh berdasarkan formula pengiraan seperti yang berikut:

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

Agensi Sektor Awam perlu menentukan tahap impak kepada strategik dan operasi (SO), kewangan (W), reputasi (R), perundangan, peraturan atau Prosedur Operasi Standard (*Standard Operating Procedure* – SOP) (P) dan Sistem (S) seperti **Jadual 24**.

Jadual 24: Skala Impak

Skala	Keterangan	Impak				
		Strategik dan Operasi (SO)	**Kewangan (W)**	**Reputasi (R)**	**Prosedur Operasi Standard (P)**	**Sistem (S)**
5	Sangat Besar	Menjejaskan keseluruhan perkhidmatan atau objektif agensi	Kerugian >50% daripada nilai projek/pendapatan tahunan agensi	Menjejaskan reputasi sehingga hilang keyakinan rakyat kepada kerajaan	Pelanggaran perundangan/ peraturan kerajaan atau pelbagai agensi yang berkaitan	Kegagalan laman web/Sistem ICT Kerajaan yang teruk atau perkhidmatan pelbagai agensi yang berkaitan terjejas
4	Besar	Menjejaskan sebahagian perkhidmatan atau objektif organisasi	Kerugian <50% daripada nilai projek/pendapatan tahunan agensi	Menjejaskan reputasi sehingga mendapat liputan antarabangsa	Pelanggaran perundangan/ peraturan kerajaan atau sebahagian agensi yang berkaitan	Kegagalan laman web/Sistem ICT Kerajaan yang meluas dan banyak rungutan daripada pengguna atau sebahagian perkhidmatan agensi yang berkaitan terjejas
3	Sederhana	Menjejaskan sebahagian perkhidmatan atau objektif organisasi	Kerugian <30% daripada nilai projek/pendapatan tahunan agensi	Menjejaskan reputasi sehingga mendapat liputan media massa tempatan	Pelanggaran perundangan atau peraturan sebahagian agensi yang berkaitan	Kegagalan laman web/Sistem ICT Kerajaan yang sederhana dan terdapat rungutan daripada sebahagian pengguna atau

Skala	Keterangan	Impak				
		Strategik dan Operasi (SO)	**Kewangan (W)**	**Reputasi (R)**	**Prosedur Operasi Standard (P)**	**Sistem (S)**
						sebahagian perkhidmatan agensi yang berkaitan terjejas
2	Kecil	Menjejaskan sebahagian perkhidmatan atau objektif organisasi	Kerugian <20% daripada nilai projek/pendapatan tahunan agensi	Menjejaskan reputasi dan menimbulkan rasa ketidakpuasan hati kumpulan/organisasi	Pelanggaran perundangan/peraturan agensi	Kegagalan laman web/Sistem ICT Kerajaan yang rendah dan terdapat rungutan daripada sebilangan kecil pengguna atau hanya menjejaskan perkhidmatan organisasi
1	Sangat Kecil	Menjejaskan sebahagian perkhidmatan atau objektif organisasi	Kerugian <10% daripada nilai projek/pendapatan tahunan agensi	Menjejaskan reputasi dan menimbulkan rasa ketidakpuasan hati individu	Tidak melibatkan pelanggaran perundangan/peraturan	Ralat yang kecil dan hanya memerlukan tindakan pembetulan. Tidak menjejaskan perkhidmatan agensi yang berkaitan

a. Langkah 3: Menilai Tahap Risiko

Proses ini membolehkan Agensi Sektor Awam mengenal pasti dan menentukan tahap risiko yang memberi impak kepada Sistem ICT Kerajaan, laman web atau portal serta perkhidmatan utama Agensi Sektor Awam tersebut. Penentuan tahap risiko ialah berdasarkan formula seperti yang berikut:

Risiko = Kebarangkalian x Impak

b. Langkah 4: Menentukan Tahap Risiko

Dalam menentukan Tahap Risiko, **Jadual 25** boleh digunakan sebagai rujukan. Matriks Tahap Risiko ini boleh diubah suai mengikut kesesuaian Agensi Sektor Awam khususnya bagi julat kebarangkalian, impak serta tahap risiko.

Jadual 25: Matriks Tahap Risiko

Kebarangkalian	**Impak**				
	1	**2**	**3**	**4**	**5**
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Kod Risiko	**Nilai Risiko**	**Tahap Risiko**
	15-25	Ekstrem
	8-12	Tinggi
	4-6	Sederhana
	1-3	Rendah

Contoh:

Kebarangkalian = 5, Impak = 5

Risiko = 5 x 5 = 25

Nilai risiko yang diperoleh ialah 25 di mana tahap risiko ialah ekstrem.

1.5. MENENTUKAN STRATEGI KAWALAN RISIKO

1.5.1 Agensi Sektor Awam perlu menentukan strategi kawalan risiko yang bersesuaian berdasarkan kriteria penerimaan risiko yang telah ditetapkan pada Para 1.2.2 d: Langkah 4. Contoh penentuan strategi kawalan risiko ialah seperti **Jadual 26**.

Jadual 26: Strategi Kawalan Risiko

Bil.	Ancaman	Tahap Risiko	Strategi Kawalan Risiko
1.	Akses tidak sah	Ekstrem	Kurang
2.	Perubahan data atau maklumat secara tidak sah	Tinggi	Kurang

1.6. PEMILIHAN KAWALAN KESELAMATAN

1.6.1 Kawalan keselamatan boleh dibahagikan kepada 3 kategori iaitu operasi, teknologi dan perundangan. Contoh kawalan operasi meliputi penyediaan prosedur kerja atau kawalan keselamatan terhadap persekitaran fizikal. Kawalan keselamatan berdasarkan aspek teknologi meliputi penggunaan teknologi PKI dalam pengesahan identiti pengguna manakala perundangan melibatkan penguatkuasaan undang-undang semasa.

1.6.2 Agensi Sektor Awam perlu melaksanakan kawalan keselamatan berdasarkan strategi risiko yang telah ditetapkan serta keutamaan pelaksanaan kawalan risiko. Risiko boleh dikurangkan dengan melaksanakan kawalan keselamatan yang baharu atau menambah baik kawalan keselamatan semasa. Kawalan keselamatan ini boleh dirangka berdasarkan faktor-faktor yang berikut:

a. Keberkesanan kawalan risiko 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.
e. Struktur dan budaya kerja.
f. Impak terhadap operasi serta organisasi.

1.6.3 Pemilihan kawalan keselamatan mestilah mengambil kira justifikasi kos dan faedah serta prosedur dan keutamaan implementasi. Pertimbangan lain yang perlu diberi perhatian oleh Agensi Sektor Awam ialah seperti yang berikut:

a. Kos perolehan.
b. Kos penempatan dan pelaksanaan.
c. Kos penyenggaraan.
d. Kos pengujian dan penilaian.
e. Pematuhan, pemantauan dan penguatkuasaan.
f. Kesan pelaksanaan kawalan keselamatan kepada pengguna.

1.6.4 Penentuan keutamaan pelaksanaan kawalan risiko ialah berdasarkan kepada tahap risiko serta faedah yang tertinggi seperti **Jadual 27**. Pelaksanaan kawalan keselamatan yang mempunyai faedah yang tertinggi akan disyor untuk dilaksanakan. 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 risiko tersebut masih boleh diterima. Manakala risiko yang ditentukan sebagai sederhana, tinggi atau ekstrem dan tidak boleh diterima, perlu diberikan cadangan langkah-langkah kawalan.

Jadual 27: Keutamaan Pelaksanaan Kawalan Keselamatan

Tahap Risiko	**Faedah**		
	Rendah	**Sederhana**	**Tinggi**
Ekstrem	1	1	1
Tinggi	2	2	1
Sederhana	3	2	2
Rendah	4	3	3
Kod Keutamaan	**Tahap Keutamaan**	**Keterangan**	
	1	Perlu Laksana Segera	
	2	Perlu Laksana	
Kod Keutamaan	**Tahap Keutamaan**	**Keterangan**	
	3	Laksana Kemudian	
	4	Tidak Perlu Laksana	

1.6.5 Dalam konteks pelaksanaan Perkhidmatan MyGPKI, cadangan kawalan keselamatan yang boleh dilaksanakan ialah seperti **Jadual 28**. Agensi Sektor Awam juga hendaklah memastikan pemilihan kawalan risiko yang melibatkan maklumat rahsia rasmi kerajaan selaras dengan akta/arahan/peraturan/ pekeliling kawalan keselamatan maklumat rahsia rasmi yang sedang berkuat kuasa.

1.6.6 Agensi Sektor Awam perlu mengambil kira keberkesanan langkah kawalan yang diambil dan semakan secara berkala perlu dilaksanakan untuk menjamin keselamatan data dan maklumat Sistem ICT Kerajaan.

Jadual 28: Kawalan Keselamatan dalam Konteks Perkhidmatan MyGPKI

<table>
<tr><th rowspan="2">Bil.</th><th rowspan="2">Kategori Sistem ICT Kerajaan</th><th rowspan="2">Peringkat Keselamatan Data/ Maklumat</th><th rowspan="2">Nilai Data/ Maklumat</th><th colspan="4">Tahap Risiko</th></tr>
<tr><th>Rendah</th><th>Sederhana</th><th>Tinggi</th><th>Ekstrem</th></tr>
<tr><td rowspan="2">1.</td><td rowspan="2">Teras/ Strategik/ Sokongan Umum/ Sokongan Dalaman</td><td>Rahsia Besar/ Rahsia/ Sulit</td><td>Tinggi</td><td colspan="4">Sijil Digital Pengguna
a. Sijil Digital Token
b. RoamingCert + OTP

Sijil Digital Pelayan
Sijil Digital Pelayan EV

Fungsi PKI
a. Pengesahan Identiti
b. Penyulitan
c. Tandatangan Digital</td></tr>
<tr><td>Terhad</td><td>Sederhana</td><td>Sijil Digital Pengguna
SoftCert

Sijil Digital Pelayan
Sijil Digital Pelayan OV

Fungsi PKI
a. Pengesahan Identiti
b. Penyulitan
c. Tandatangan Digital</td><td colspan="2">Sijil Digital Pengguna
RoamingCert

Sijil Digital Pelayan
Sijil Digital Pelayan OV

Fungsi PKI
a. Pengesahan Identiti
b. Penyulitan
c. Tandatangan Digital</td><td>Sijil Digital Pengguna
a. Sijil Digital Token
b. RoamingCert + OTP

Sijil Digital Pelayan
Sijil Digital Pelayan EV

Fungsi PKI
a. Pengesahan Identiti
b. Penyulitan
c. Tandatangan Digital</td></tr>
</table>

		Terkawal/ Sensitif	Sederhana	**Sijil Digital Pengguna** Tidak berkaitan **Sijil Digital Pelayan** Sijil Digital Pelayan OV **Fungsi PKI** a. Pengesahan Identiti b. Penyulitan	**Sijil Digital Pengguna** *SoftCert* **Sijil Digital Pelayan** Sijil Digital Pelayan OV **Fungsi PKI** a. Pengesahan Identiti b. Penyulitan c. Tandatangan Digital	**Sijil Digital Pengguna** *RoamingCert* **Sijil Digital Pelayan** Sijil Digital Pelayan OV **Fungsi PKI** a. Pengesahan Identiti b. Penyulitan c. Tandatangan Digital
2.	Strategik/ Sokongan Umum/ Sokongan Dalaman	Terbuka	Rendah	**Sijil Digital Pengguna** Tiada **Sijil Digital Pelayan** Sijil Digital Pelayan OV **Fungsi PKI** a. Pengesahan Identiti b. Penyulitan		

Contoh pelaksanaan kawalan risiko berdasarkan keutamaan ialah seperti **Jadual 29** berikut:

Jadual 29: Contoh Penetapan Keutamaan Pelaksanaan Kawalan Keselamatan

Bil.	Ancaman	Tahap Risiko	Strategi Kawalan Risiko	Kaedah Kawalan Keselamatan	Faedah Pelaksanaan	Keutamaan
1.	Akses tidak sah	Ekstrem	Kurang	Pelaksanaan **pengesahan identiti pengguna** semasa log masuk ke Sistem ICT Kerajaan	Tinggi	**1** Perlu Laksana Segera
2.	Perubahan data atau maklumat secara tidak sah	Tinggi	Kurang	Pelaksanaan **tandatangan digital** bagi mengesahkan identiti pengguna yang melaksanakan perubahan ke atas data atau maklumat	Tinggi	**1** Perlu Laksana Segera
				Pelaksanaan **penyulitan data atau maklumat** yang disimpan	Sederhana	**2** Perlu Laksana

1.7. PELAPORAN HASIL PENILAIAN RISIKO

Agensi Sektor Awam hendaklah menghasilkan dan mengemukakan Laporan Penilaian Risiko seperti Lampiran A3: Laporan Penilaian Risiko Sistem ICT Kerajaan dan Lampiran A4: Format Laporan Penilaian Risiko Laman Web Dan Portal bagi laman web atau portal sebagai dokumen sokongan dalam permohonan Perkhidmatan MyGPKI kepada Agensi Peneraju.

LAMPIRAN A3

FORMAT/CONTOH LAPORAN PENILAIAN RISIKO SISTEM ICT KERAJAAN

LAPORAN PENILAIAN RISIKO BAGI SISTEM ABC
BAHAGIAN PEMBANGUNAN PERKHIDMATAN GUNASAMA INFRASTRUKTUR DAN KESELAMATAN DIGITAL, JABATAN DIGITAL NEGARA

1.1. PENGENALAN

(Nota: Nyatakan tujuan penilaian risiko dilaksanakan serta skop pelaksanaan penilaian risiko)

Penilaian risiko dilaksanakan bagi mengenal pasti ancaman atau kelemahan yang berkaitan dengan Sistem ICT Kerajaan di bawah seliaan Bahagian Pembangunan Perkhidmatan Gunasama Infrastruktur dan Keselamatan Digital (BPG), Jabatan Digital Negara (JDN). Hasil daripada penilaian risiko ini akan digunakan bagi mengenal pasti kaedah dan pelaksanaan kawalan PKI yang bersesuaian. Antara kaedah kawalan yang boleh dilaksanakan ialah pelaksanaan integrasi antara Sistem ICT Kerajaan dan Sistem MyGPKI serta pemasangan Sijil Digital Pelayan ke atas pelayan-pelayan Sistem ICT Kerajaan (Contoh: **Sistem ABC**).

Skop pelaksanaan penilaian risiko ini ialah bagi data dan maklumat modul-modul yang terdapat di dalam **Sistem ABC**.

1.2. LATAR BELAKANG

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

BPG merupakan bahagian yang bertanggungjawab untuk merancang, mengurus, menganalisis, melaksana dan memantau Perkhidmatan *Advanced Business Central* (ABC) bagi Agensi Sektor Awam selaras dengan visi JDN sebagai penggerak dan peneraju transformasi penawaran perkhidmatan awam menjelang 2025.

Oleh itu, Sistem ABC yang telah dibangunkan bertujuan menyedia dan mengurus proses aliran integrasi perkhidmatan dalam Sektor Awam. Sistem ini dilaksanakan pada dokumen elektronik dan pengurusan maklumat pentadbir Sistem ABC di agensi digunakan bagi menyokong fungsi JDN iaitu menyediakan perkhidmatan gunasama

kepada agensi sektor awam. Sistem ABC terdiri daripada beberapa komponen iaitu Portal ABC dan Perisian ABC. Fungsi dan keterangan bagi setiap komponen ialah seperti yang berikut:

(a) Portal ABC mengandungi modul penyediaan dan pengurusan proses aliran integrasi serta pengurusan pentadbir ABC di agensi; dan

(b) Perisian ABC digunakan semasa proses pengesahan dan kelulusan proses aliran integrasi.

Sistem ini dikategorikan sebagai sistem teras kerana digunakan merentasi Agensi Sektor Awam dan sekiranya terdapat gangguan kepada sistem dalam tempoh yang singkat akan memberi impak yang tinggi kepada operasi Agensi Sektor Awam dalam melaksanakan transaksi menggunakan Sistem ICT Kerajaan serta menjejaskan reputasi JDN sebagai penyedia Perkhidmatan ABC.

Pengguna sistem ini terdiri daripada Perkhidmatan Awam Persekutuan, Perkhidmatan Awam Negeri dan Badan Berkanun Persekutuan. Jumlah Pengguna semasa ialah seramai 5,000 orang. Latar belakang Sistem ABC ialah seperti **Jadual 30** dan **Jadual 31**.

Jadual 30: Latar Belakang Sistem ABC

Bil.	Perkara		Keterangan
1.	Kementerian	:	<Nyatakan nama Kementerian>
2.	Nama Agensi	:	<Nyatakan nama agensi> Jabatan Digital Negara (JDN)
3.	Alamat	:	<Nyatakan alamat agensi> Blok B, No. 3200, Bangunan MKN Embassy Techzone, Jalan Teknokrat 2, 63000 Cyberjaya, Selangor Darul Ehsan
4.	Pemilik Sistem ICT Kerajaan		<Nyatakan maklumat pemilik Sistem ICT Kerajaan >
	(i) Nama	:	Shuhadah binti Abdullah
	(ii) Jawatan	:	Timbalan Pengarah/Pengurus Projek
	(iii) No. Tel Pejabat	:	03-8000 8000
	(iv) No. Tel Bimbit	:	017-772 1098
	(v) E-mel	:	shuhadah@jdn.gov.my

Bil.	Perkara	Keterangan
5.	Pegawai Teknikal Sistem ICT Kerajaan :	<Nyatakan maklumat pegawai teknikal Sistem ICT Kerajaan>
	(i) Nama :	Ariffin bin Ismail
	(ii) Jawatan :	Ketua Penolong Pengarah Kanan
	(iii) No. Tel Pejabat :	03-8000 8000
	(iv) No. Tel Bimbit :	017-572 3302
	(v) E-mel :	ariffin@jdn.gov.my
6.	Pegawai Pengesah :	<Nyatakan maklumat pegawai pengesah Sistem ICT Kerajaan sekiranya melibatkan Permohonan Sijil Digital Pelayan>
	(i) Nama :	Burhanuddin bin Rahman
	(ii) Jawatan :	Ketua Penolong Pengarah Kanan
	(iii) No. Tel Pejabat :	03-8000 8000
	(iv) No. Tel Bimbit :	017-572 3302
	(v) E-mel :	burhan@jdn.gov.my
7.	Pembekal Sistem ICT Kerajaan :	<Nyatakan maklumat pembekal Sistem ICT Kerajaan>
	(i) Nama :	Iskandar bin Abdullah
	(ii) Jawatan :	Pengurus Projek
	(iii) No. Tel Pejabat :	03-8734 9002
	(iv) No. Tel Bimbit :	017-471 5308
	(v) E-mel :	iskandar@it.com.my
8.	Latar Belakang Sistem ICT Kerajaan :	<Nyatakan latar belakang Sistem ICT Kerajaan agensi secara ringkas>
	(i) Objektif :	<Nyatakan objektif Sistem ICT Kerajaan agensi/domain> Pengesahan masa transaksi yang dilaksanakan pada dokumen elektronik, pengurusan transaksi tandaan masa serta pengurusan maklumat pentadbir ABC di agensi
	(ii) Perkhidmatan Teras yang Disokong :	<Nyatakan perkhidmatan teras agensi yang disokong> Perkhidmatan gunasama kepada agensi sektor awam
	(iii) Perundangan/Pekeliling/SOP Berkaitan Kawalan Akses Data dan Tandatangan :	<Nyatakan Perundangan/Pekeliling/SOP Berkaitan Kawalan Akses Data dan Tandatangan yang dirujuk atau digunakan> 1. Akta Kerajaan Elektronik 2007 2. Arahan Teknologi Maklumat 2007 3. Akta Tandatangan Digital 1998 4. Peraturan Tandatangan Digital 1998
	(iv) Kategori Sistem :	<Nyatakan kategori sistem> Sistem Teras

Bil.	Perkara	Keterangan
	(v) Kaedah Capaian Sistem :	<Nyatakan kaedah capaian ke sistem (Intranet/Internet)> Internet
	(vi) Platform :	<Nyatakan platform yang digunakan oleh sistem> Spring Framework
	(vii) Bahasa Pengaturcaraan :	<Nyatakan bahasa pengaturcaraan yang digunakan oleh sistem> JAVA
	(viii) Arkitektur Sistem ICT Kerajaan :	<Maklumat arkitektur yang mengandungi rajah atau aliran proses dan antara muka modul Sistem ICT Kerajaan yang terlibat> Seperti di **Lampiran A**
9.	Maklumat Pengguna	<Nyatakan kategori agensi Pengguna yang menggunakan sistem>
	(i) Jumlah Pengguna Keseluruhan :	Agensi Sektor Awam : 5,000 orang Agensi Sektor Swasta: tiada
	(ii) Kategori Agensi Pengguna :	☑ Perkhidmatan Awam Persekutuan ☑ Perkhidmatan Awam Negeri ☑ Badan Berkanun Persekutuan ☐ Badan Berkanun Negeri ☐ Pihak Berkuasa Tempatan ☐ Syarikat Swasta
10.	Latar Belakang Domain :	<Nyatakan domain dan subdomain yang terlibat>
	(i) Nama Domain :	https://abc.gov.my (**Domain utama** bagi Sistem ABC)
	(ii) Jenis Domain :	Single Domain

Jadual 31: Latar Belakang Domain Sistem ABC

Bil.	Nama Domain	Keterangan	Kategori Domain	Kategori Sistem ICT Kerajaan	Jenis Sijil Digital Pelayan Semasa	Tarikh Luput Sijil Digital Pelayan Semasa	CA Prinsipal	Kaedah Capaian	Platform	Jenis Pelayan	Tanggungan Kos	Maklumat Pemohon	Maklumat Pegawai Teknikal	Maklumat Pegawai Pengesah
	<Nyatakan nama domain atau subdomain Sistem ICT Kerajaan>	<Nyatakan keterangan Sistem ICT Kerajaan>	<Nyatakan sama ada domain utama atau subdomain>	<Nyatakan kategori Sistem ICT Kerajaan>	<Nyatakan jenis Sijil Digital Pelayan Semasa>	<Nyatakan tarikh luput Sijil Digital Pelayan semasa bagi domain atau subdomain>	<Nyatakan nama pengeluar Sijil Digital Pelayan terdahulu>	<Nyatakan kaedah capaian ke Sistem ICT Kerajaan>	<Nyatakan platform Sistem ICT Kerajaan>	<Nyatakan platform Sistem ICT Kerajaan>	<Nyatakan pihak yang menanggung kos bagi perolehan Sijil Digital Pelayan terdahulu>	<Nyatakan maklumat berikut: i. Nama ii. Jawatan iii. No. Telefon Pejabat iv. No. Telefon Bimbit v. E-mel	<Nyatakan maklumat berikut: i. Nama ii. Jawatan iii. No. Telefon Pejabat iv. No. Telefon Bimbit v. E-mel	<Nyatakan maklumat berikut: i. Nama ii. Jawatan iii. No. Telefon Pejabat iv. No. Telefon Bimbit v. E-mel
1.	abc.gov.my	Domain ini digunakan bagi Sistem ABC yang dibangunkan bertujuan untuk menyedia dan mengurus proses aliran integrasi perkhidmatan dalam Sektor Awam	Domain utama	Kritikal	*Single* Domain EV	12-Jan-23	Entrust	Internet	Linux	Apache	JDN	**Nama :** Mas Ayu binti Abdullah **Jawatan:** Penolong Pengarah **No. Telefon Pejabat:** 03-8788922 **No. Telefon Bimbit:** 019-8827771 **E-mel:** mas.ayu@jdn.gov.my	**Nama :** Tahir bin Jaafar **Jawatan**: Ketua Penolong Pengarah **No. Telefon Pejabat:** 03-8788924 **No. Telefon Bimbit:** 017-9828871 **E-mel:** tahir@jdn.gov.my	**Nama :** Faridah binti Abu Bakar **Jawatan:** Timbalan Pengarah **No. Telefon Pejabat:**03-8788920 **No. Telefon Bimbit:** 013-9990237 **E-mel:** faridah@jdn.gov.my
2	latihan.abc.gov.my	Domain ini digunakan bagi Sistem Latihan Portal ABC	Subdomain	Strategik	*Single* Domain OV	12-Jan-23	Entrust	Internet	Linux	Apache	Agensi			
3.	dev.abc.gov.my	Domain ini digunakan bagi Sistem ABC semasa fasa pembangunan dan pengujian	Subdomain	Sokongan Dalaman	Tiada	Tidak berkaitan	Tidak berkaitan	Intranet	Linux	Apache	Tidak berkaitan			

1.3. PENILAIAN RISIKO

Penilaian risiko dilaksanakan untuk mengenal pasti langkah-langkah kawalan dalam menangani risiko berkaitan kerahsiaan, pengesahan identiti, integriti dan tanpa sangkalan terhadap data dan maklumat Sistem ICT Kerajaan. Maklumat ancaman yang telah dikenal pasti bagi Sistem ABC ialah seperti **Jadual 32**. Hasil penilaian risiko mendapati Sistem ABC mempunyai **satu risiko tinggi** dan **2 risiko sederhana**. Keterangan bagi modul dan transaksi yang mempunyai risiko tinggi dan sederhana ialah seperti yang berikut:

a. Risiko Tinggi

Modul *Advanced Business Central* mempunyai risiko yang tinggi bagi transaksi kelulusan permohonan dan pengesahan di mana terdapat kebarangkalian ancaman penyangkalan transaksi berlaku. Data atau maklumat yang terlibat diperingkatkan sebagai terhad dan mempunyai nilai sederhana. Tiada kawalan semasa yang dilaksanakan bagi mengurangkan risiko ancaman yang melibatkan ciri keselamatan tanpa sangkalan (N). Ancaman ini memberi impak kepada reputasi organisasi, kebolehpercayaan terhadap Sistem ABC serta pelanggaran kepada Polisi Keselamatan Siber JDN. Kebarangkalian ancaman berlaku ialah sekurang-kurangnya sekali dalam tempoh 3 hingga 5 tahun.

b. Risiko Sederhana

Modul *Advanced Business Central* mempunyai risiko yang sederhana bagi transaksi kelulusan permohonan dan pengesahan di mana terdapat kebarangkalian ancaman penyamaran identiti berlaku. Data atau maklumat yang terlibat diperingkatkan sebagai terhad dan mempunyai nilai sederhana. Kawalan semasa yang dilaksanakan ialah menggunakan login ID dan kata laluan untuk mengakses Sistem ABC di mana didapati langkah kawalan ini tidak mencukupi bagi mengurangkan risiko ancaman yang melibatkan ciri-ciri keselamatan pengesahan identiti (A), integriti (I) dan kerahsiaan (C). Ancaman ini memberi impak kepada reputasi organisasi, kebolehpercayaan terhadap Sistem ABC serta pelanggaran kepada Polisi Keselamatan Siber JDN. Kebarangkalian ancaman berlaku ialah sekurang-kurangnya sekali dalam tempoh 3 hingga 5 tahun.

Jadual 32: Hasil Penilaian Risiko Sistem ABC

Bil.	Kategori Sistem ICT Kerajaan	Nama Modul	Fungsi Modul	Transaksi	Data /Maklumat Terlibat	Peringkat Keselamatan Data /Maklumat	Nilai Data	Ancaman Keselamatan	Kesan Ancaman Keselamatan				Kebarangkalian	Impak					Tahap Risiko	Strategi Kawalan Risiko	Cadangan Kawalan PKI		
									Kesahihan Identiti	Integriti	Kerahsiaan	Tanpa Sangkalan	<Nyatakan kebarangkalian ancaman berlaku berdasarkan>	Strategik /Operasi /SO	Kewangan (W)	Reputasi (R)	Perundangan /Peraturan /SOP (P)	<Nyatakan jumlah impak Impak =SO+W+R+P/4			Fungsi PKI	Jenis Sijil Digital Pengguna	Jenis Sijil Digital Pelayan
	<Nyatakan kategori Sistem ICT Kerajaan>	<Nyatakan Nama Modul yang terlibat>	<Nyatakan fungsi modul>	<Nyatakan transaksi yang dilaksanakan dalam modul>	<Nyatakan data /maklumat terlibat>	<Nyatakan peringkat keselamatan data atau maklumat>	<Nyatakan nilai data atau maklumat>	<Nyatakan ancaman keselamatan yang berkaitan dan keterangan ancaman>											<Nyatakan Tahap Risiko>		<Nyatakan kaedah kawalan PKI>		
1	Kritikal	*Advanced Business Central*	Mengesah permohonan aliran proses integrasi	Permohonan aliran proses integrasi	Nama Pemohon	Terhad	Sederhana	Penyamaran identiti • Penceroboh menyamar sebagai pengguna sebenar untuk melaksanakan transaksi	√		√	√	2	3	4	3	5	3	6	Kurang	Penyulitan Saluran Komunikasi Pelayan	Roaming-*Cert*	OV
				Kelulusan permohonan	Nama Pelulus	Terhad	Sederhana	Pengubahsuaian data • Penceroboh mengubah suai data yang akan dihantar tanpa kebenaran		√			2	3	4	3	5	3	6	Kurang	Pengesahan Identiti Pelayan	Tiada	OV
				Kelulusan permohonan	Tandatangan dan tandaan masa kelulusan	Sulit	Tinggi	Penyamaran identiti • Penceroboh menyamar sebagai pengguna sebenar untuk melaksanakan transaksi	√		√	√	4	3	4	3	5	3	12	Kurang	Tandatangan Digital	Token	EV
				Paparan Maklumat Agensi	Maklumat Agensi	Terbuka	Sederhana	Pengubahsuaian data • Penceroboh mengubah suai maklumat yang dipaparkan		√			1	1	1	1	1	1	1	Kurang	Pengesahan Identiti Pelayan	Tiada	OV

1.4. STRATEGI DAN KAEDAH KAWALAN RISIKO

Kriteria risiko yang ditetapkan dalam penilaian risiko ini ialah seperti yang berikut:

(a) Tinggi/Sederhana: Kurang.
(b) Rendah: Terima (Pengguna) dan Kurang (Pelayan).

Oleh itu, kawalan keselamatan yang akan dilaksanakan hanya terhadap modul Sistem ABC yang mempunyai tahap risiko tinggi dan mempunyai capaian menerusi Internet seperti **Jadual 32**. Secara keseluruhannya, cadangan kaedah kawalan PKI yang bersesuaian untuk dilaksanakan mengikut keutamaan ialah seperti yang berikut:

(a) Sijil Digital Pengguna: Sijil Digital Token.
(b) Sijil Digital Pelayan: Sijil Digital Pelayan EV.
(c) Ciri keselamatan PKI: A, I, C dan N.
(d) Fungsi PKI: Pengesahan identiti pengguna dan pelayan, penyulitan serta tandatangan digital.

1.5. PENUTUP

Berdasarkan analis penilaian risiko, didapati Sistem ABC mempunyai tahap risiko tinggi. Langkah kawalan PKI yang sesuai dilaksanakan ialah dengan menggunakan Sijil Digital Token bagi pengesahan identiti pengguna dan tandatangan digital serta pemasangan Sijil Digital Pelayan EV ke atas pelayan-pelayan yang terlibat bagi fungsi pengesahan identiti pelayan. Cadangan pelaksanaan ialah berdasarkan kawalan keselamatan tertinggi yang diperlukan oleh Sistem ABC.

LAMPIRAN A4

FORMAT/ CONTOH LAPORAN PENILAIAN RISIKO LAMAN WEB DAN PORTAL

1.1. LATAR BELAKANG AGENSI

BIL.	PERKARA	KETERANGAN
1	**Kementerian**	**<Nyatakan nama Kementerian>**
2	**Nama Agensi**	**<Nyatakan nama Jabatan/Agensi>** Jabatan Digital Negara (JDN)
3	**Alamat**	**<Nyatakan alamat Kementerian/Jabatan/Agensi>** Blok B, No. 3200, Bangunan MKN Embassy Techzone, Jalan Teknokrat 2, 63000 Cyberjaya, Selangor Darul Ehsan
4	**Kategori Kementerian/ Jabatan/Agensi**	**<Nyatakan Kategori Jabatan/Agensi>** ☐ Perkhidmatan Awam Persekutuan ☐ Perkhidmatan Awam Negeri ☐ Badan Berkanun Persekutuan ☐ Badan Berkanun Negeri ☐ Pihak Berkuasa Tempatan
5	**Kategori Saraan Kementerian/ Jabatan/Agensi**	**<Nyatakan Kategori Saraan Kementerian/Jabatan/Agensi>** ☐ Ditanggung ☐ Tidak Ditanggung

1.2. LATAR BELAKANG LAMAN WEB ATAU PORTAL

Bil.	Nama Domain	Keterangan	Kategori Domain	Jumlah Pengguna Keseluruhan	Kategori Agensi Pengguna	Kategori Laman Web	Jenis Sijil Digital Pelayan Semasa	Tarikh Luput Sijil Digital Pelayan Semasa	Tarikh Penerimaan Sijil Digital Pelayan Semasa	Tarikh Pemasangan Sijil Digital Pelayan Semasa	Prinsipal CA dan CA	Kaedah Capaian	Platform	Jenis Pelayan	Tanggungan Kos
	<Nyatakan nama domain atau subdomain laman web/portal>	<Nyatakan keterangan dan fungsi laman web/portal/ Sistem ICT Kerajaan yang terlibat secara jelas dan terperinci yang terdapat pada domain atau subdomain>	<Nyatakan sama ada domain utama atau subdomain>	<Nyatakan jumlah pengguna keseluruhan yang menggunakan laman web/portal/ Sistem ICT Kerajaan >	<Nyatakan kategori agensi pengguna yang menggunakan laman web/portal/ Sistem ICT Kerajaan >	<Nyatakan kategori laman web/portal/ Sistem ICT Kerajaan >	<Nyatakan jenis Sijil Digital Pelayan semasa>	<Nyatakan tarikh luput Sijil Digital Pelayan semasa bagi domain atau subdomain>	<Nyatakan tarikh penerimaan Sijil Digital Pelayan daripada CA bagi domain atau subdomain>	<Nyatakan tarikh pemasangan Sijil Digital Pelayan bagi domain atau subdomain>	<Nyatakan nama pengeluar Sijil Digital Pelayan terdahulu>	<Nyatakan kaedah capaian ke laman web/portal/ Sistem ICT Kerajaan>	<Nyatakan platform laman web/portal/ Sistem ICT Kerajaan>	<Nyatakan pelayan/ *web service* laman web/portal/ Sistem ICT Kerajaan >	<Nyatakan pihak yang menanggung kos bagi perolehan sijil digital pelayan terdahulu>
1	www.jdn.gov.my	Domain ini digunakan sebagai portal utama agensi	Domain utama	1,000,000 orang	Semua	Sokongan Umum	*Wildcard* OV	29-Apr-21	29-Apr-19	29-Apr-19	GlobalSign dan Pos Digicert	Internet	Linux Redhat	Apache (Tomcat)	Agensi Peneraju (JDN)
2	dts.jdn.gov.my	Subdomain ini digunakan bagi Sistem ABC yang dibangunkan bagi tujuan pengurusan tandaan masa dan pengurusan pentadbir agensi di agensi persekutuan dan negeri	Subdomain	150,000 orang	Kementerian Agensi Pentadbiran Persekutuan Perkhidmatan Awam Negeri Badan Berkanun Persekutuan Badan Berkanun Yang Tidak Diasingkan Saraan	Teras	*Single* Domain EV	12-Jan-20	12-Jan-18	15-Jan-18	Entrust dan Pos Digicert	Internet	Linux	Nginx	Agensi Peneraju (JDN)

1.3. PENILAIAN RISIKO LAMAN WEB ATAU PORTAL

Bil.	Nama Domain	Data/ Maklumat Terlibat	Peringkat Keselamatan Data/ Maklumat	Nilai Data	Kawalan Sedia Ada	Ancaman Keselamatan	Keterangan Ancaman	Kesan Ancaman Keselamatan		Kebarangkalian	Impak						Tahap Risiko	Cadangan Kawalan PKI	
								Kesahihan	Kerahsiaan		Strategik/Operasi	Kewangan (W)	Reputasi (R)	Perundangan/ Peraturan/SOP/ Manusia (P)	Laman Web (S)	Jumlah		Fungsi PKI	Jenis Sijil Digital Pelayan
	<Nama domain atau subdomain>	<Nyata-kan data/mak-lumat terlibat>	<Nyatakan peringkat keselamatan data atau maklumat>	<Nya-takan nilai data atau maklu-mat>	<Nyatakan kawalan semasa yang telah dilaksana-kan bagi mengu-rangkan risiko ancaman keselama-tan>	<Nyatakan ancaman keselamatan yang berkemungki-nan atau telah berlaku terhadap data atau maklumat>	<Nyata-kan keteran-gan anca-man kesela-matan yang berke-mungki-nan atau telah berlaku terhadap data atau maklu-mat>	<Nyatakan ciri keselamatan PKI yang berkaitan dengan ancaman keselamatan >		<Nyatakan kebarangkalian ancaman berlaku>	<Nyatakan impak sekiranya ancaman berlaku>				<Nyatakan jumlah impak berdasarkan formula: Impak =SO+W+R+P+S/ 5>		<Nya-takan Tahap Risiko >	<Tentukan strategi kawalan risiko>	<Nyatakan kaedah kawalan PKI>
1	www.jdn.gov.my	Portal JDN yang mengan-dungi maklumat umum aktiviti organisasi dan garis panduan yang perlu	Terbuka	Seder-hana	Pemasa-ngan sijil digital pelayan *Wildcard* OV	*HTTPS spoofing*	Penggo-dam mewu-judkan laman web palsu yang menye-rupai laman		✔	3	1	1	5	1	2	2	6	Pengesa-han Identiti Pelayan	*Wildcard OV*

Bil.	Nama Domain	Data/ Maklumat Terlibat	Peringkat Keselamatan Data/ Maklumat	Nilai Data	Kawalan Sedia Ada	Ancaman Keselamatan	Keterangan Ancaman	Kesan Ancaman Keselamatan		Kebarangkalian	Impak						Tahap Risiko	Cadangan Kawalan PKI	
								Kesahihan	Kerahsiaan		Strategik/Operasi	Kewangan (W)	Reputasi (R)	Perundangan/ Peraturan/SOP/ Manusia (P)	Laman Web (S)	Jumlah		Fungsi PKI	Jenis Sijil Digital Pelayan
	<Nama domain atau subdomain>	<Nyata-kan data/mak-lumat terlibat>	<Nyatakan peringkat keselamatan data atau maklumat>	<Nya-takan nilai data atau maklu-mat>	<Nyatakan kawalan semasa yang telah dilaksana-kan bagi mengu-rangkan risiko ancaman keselama-tan>	<Nyatakan ancaman keselamatan yang berkemungki-nan atau telah berlaku terhadap data atau maklumat>	<Nyata-kan keteran-gan anca-man kesela-matan yang berke-mungki-nan atau telah berlaku terhadap data atau maklu-mat>	<Nyatakan ciri keselamatan PKI yang berkaitan dengan ancaman keselamatan >		<Nyatakan kebarangkalian ancaman berlaku>	<Nyatakan impak sekiranya ancaman berlaku>				<Nyatakan jumlah impak berdasarkan formula: Impak =SO+W+R+P+S/ 5>		<Nya-takan Tahap Risiko >	<Tentukan strategi kawalan risiko>	<Nyatakan kaedah kawalan PKI>
		dicapai oleh semua agensi kerajaan					web asal bagi tujuan memin-dahkan komuni-kasi kepada pelayan penggo-dam bagi tujuan peminta-san data												

Bil.	Nama Domain	Data/ Maklumat Terlibat	Peringkat Keselamatan Data/ Maklumat	Nilai Data	Kawalan Sedia Ada	Ancaman Keselamatan	Keterangan Ancaman	Kesan Ancaman Keselamatan		Kebarangkalian	Impak						Tahap Risiko	Cadangan Kawalan PKI	
								Kesahihan	Kerahsiaan		Strategik/Operasi	Kewangan (W)	Reputasi (R)	Perundangan/ Peraturan/SOP/ Manusia (P)	Laman Web (S)	Jumlah		Fungsi PKI	Jenis Sijil Digital Pelayan
	<Nama domain atau subdomain>	<Nyata-kan data/mak-lumat terlibat>	<Nyatakan peringkat keselamatan data atau maklumat>	<Nya-takan nilai data atau maklu-mat>	<Nyatakan kawalan semasa yang telah dilaksana-kan bagi mengu-rangkan risiko ancaman keselama-tan>	<Nyatakan ancaman keselamatan yang berkemungki-nan atau telah berlaku terhadap data atau maklumat>	<Nyata-kan keteran-gan anca-man kesela-matan yang berke-mungki-nan atau telah berlaku terhadap data atau maklu-mat>	<Nyatakan ciri keselamatan PKI yang berkaitan dengan ancaman keselamatan >		<Nyatakan kebarangkalian ancaman berlaku>	<Nyatakan impak sekiranya ancaman berlaku>			<Nyatakan jumlah impak berdasarkan formula: Impak =SO+W+R+P+S/ 5>			<Nya-takan Tahap Risiko >	<Tentukan strategi kawalan risiko>	<Nyatakan kaedah kawalan PKI>
							atau maklu-mat yang sedang berinte-raksi												
2	dts.jdn. gov.my	Mengan-dungi rekod tandaan masa dan maklumat pengguna.	Sulit	Tinggi	Pemasa-ngan Sijil Digital Pelayan *Single* Domain EV dan	*SSL hijacking*	Anca-man di mana penggo-dam menukar komuni-	✔	✔	4	5	1	5	5	3	4	15	Pengesa-han Identiti Pelayan, Penyulitan Saluran	*Single Domain EV*

Bil.	Nama Domain	Data/ Maklumat Terlibat	Peringkat Keselamatan Data/ Maklumat	Nilai Data	Kawalan Sedia Ada	Ancaman Keselamatan	Keterangan Ancaman	Kesan Ancaman Keselamatan		Kebarangkalian	Impak						Tahap Risiko	Cadangan Kawalan PKI	
								Kesahihan	Kerahsiaan		Strategik/Operasi	Kewangan (W)	Reputasi (R)	Perundangan/ Peraturan/SOP/ Manusia (P)	Laman Web (S)	Jumlah		Fungsi PKI	Jenis Sijil Digital Pelayan
	<Nama domain atau subdomain>	<Nyata-kan data/mak-lumat terlibat>	<Nyatakan peringkat keselamatan data atau maklumat>	<Nya-takan nilai data atau maklu-mat>	<Nyatakan kawalan semasa yang telah dilaksana-kan bagi mengu-rangkan risiko ancaman keselama-tan>	<Nyatakan ancaman keselamatan yang berkemungki-nan atau telah berlaku terhadap data atau maklumat>	<Nyata-kan keteran-gan anca-man kesela-matan yang berke-mungki-nan atau telah berlaku terhadap data atau maklu-mat>	<Nyatakan ciri keselamatan PKI yang berkaitan dengan ancaman keselamatan >		<Nyatakan kebarangkalian ancaman berlaku>	<Nyatakan impak sekiranya ancaman berlaku>			<Nyatakan jumlah impak berdasarkan formula: Impak =SO+W+R+P+S/ 5>			<Nya-takan Tahap Risiko >	<Tentukan strategi kawalan risiko>	<Nyatakan kaedah kawalan PKI>
		Sistem DTS memain-kan peranan dalam memasti-kan sesuatu transaksi atau maklumat adalah SAHIH wujud			pengguna login ID dan kata laluan		kasi antara 2 pihak yang sedang berko-munikasi dengan pelayan penggo-dam											Komunika-si Pelayan	

Bil.	Nama Domain	Data/ Maklumat Terlibat	Peringkat Keselamatan Data/ Maklumat	Nilai Data	Kawalan Sedia Ada	Ancaman Keselamatan	Keterangan Ancaman	Kesan Ancaman Keselamatan		Kebarangkalian	Impak						Tahap Risiko	Cadangan Kawalan PKI	
								Kesahihan	Kerahsiaan		Strategik/Operasi	Kewangan (W)	Reputasi (R)	Perundangan/ Peraturan/SOP/ Manusia (P)	Laman Web (S)	Jumlah		Fungsi PKI	Jenis Sijil Digital Pelayan
	<Nama domain atau subdomain>	<Nyata-kan data/mak-lumat terlibat>	<Nyatakan peringkat keselamatan data atau maklumat>	<Nya-takan nilai data atau maklu-mat>	<Nyatakan kawalan semasa yang telah dilaksana-kan bagi mengu-rangkan risiko ancaman keselama-tan>	<Nyatakan ancaman keselamatan yang berkemungki-nan atau telah berlaku terhadap data atau maklumat>	<Nyata-kan keteran-gan anca-man kesela-matan yang berke-mungki-nan atau telah berlaku terhadap data atau maklu-mat>	<Nyatakan ciri keselamatan PKI yang berkaitan dengan ancaman keselamatan >		<Nyatakan kebarangkalian ancaman berlaku>	<Nyatakan impak sekiranya ancaman berlaku>				<Nyatakan jumlah impak berdasarkan formula: Impak =SO+W+R+P+S/ 5>		<Nya-takan Tahap Risiko >	<Tentukan strategi kawalan risiko>	<Nyatakan kaedah kawalan PKI>
		pada masa yang dinyata-kan																	