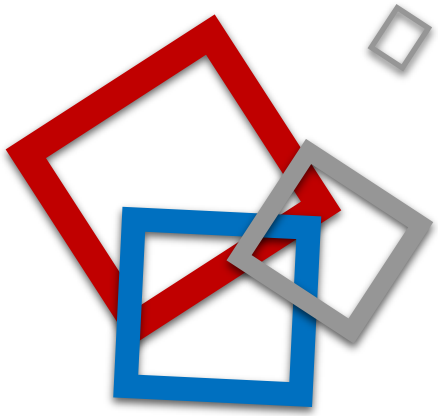
TAKLIMAT PERKHIDMATAN GOVERNMENT *PUBLIC KEY INFRASTRUCTURE* (GPKI)

Versi 1.0

AGENDA



1 | PENGENALAN PERKHIDMATAN GPKI

2 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PENGGUNA

3 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PELAYAN

4 | MEJA BANTUAN DAN KHIDMAT SOKONGAN TEKNIKAL GPKI

5 | KHIDMAT NASIHAT DAN KONSULTASI BAGI PENGGUNAAN PKI

1 | PENGENALAN PERKHIDMATAN GPKI

Prasarana Kunci Awam (Public Key Infrastructure, PKI)

Gabungan perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan komunikasi dan transaksi urus niaga dalam Internet.

Perkhidmatan Prasarana Kunci Awam Kerajaan (Government Public Key Infrastructure, GPKI)

Perkhidmatan keselamatan ICT berasaskan teknologi PKI yang disediakan kepada agensi sektor awam selaras dengan Akta Tandatangan Digital 1997, Peraturan-Peraturan Tandatangan Digital 1998, Akta Kerajaan Elektronik 2007 dan Arahan Teknologi Maklumat 2007.

1 | PENGENALAN PERKHIDMATAN GPKI

TUJUAN

Melindungi maklumat terperingkat Kerajaan di dalam talian daripada ancaman keselamatan maklumat

C A I N

CIRI KESELAMATAN

Kesahihan

Pengesahan Identiti

- Pengesahan identiti individu atau pelayan yang sedang bertransaksi.

A

Kerahsiaan

Penyulitan

- Melindungi maklumat daripada pemintasan semasa transaksi.

C

Integriti

- Memastikan mesej atau dokumen tidak diubah atau rosak.

I

Tanpa Sangkalan

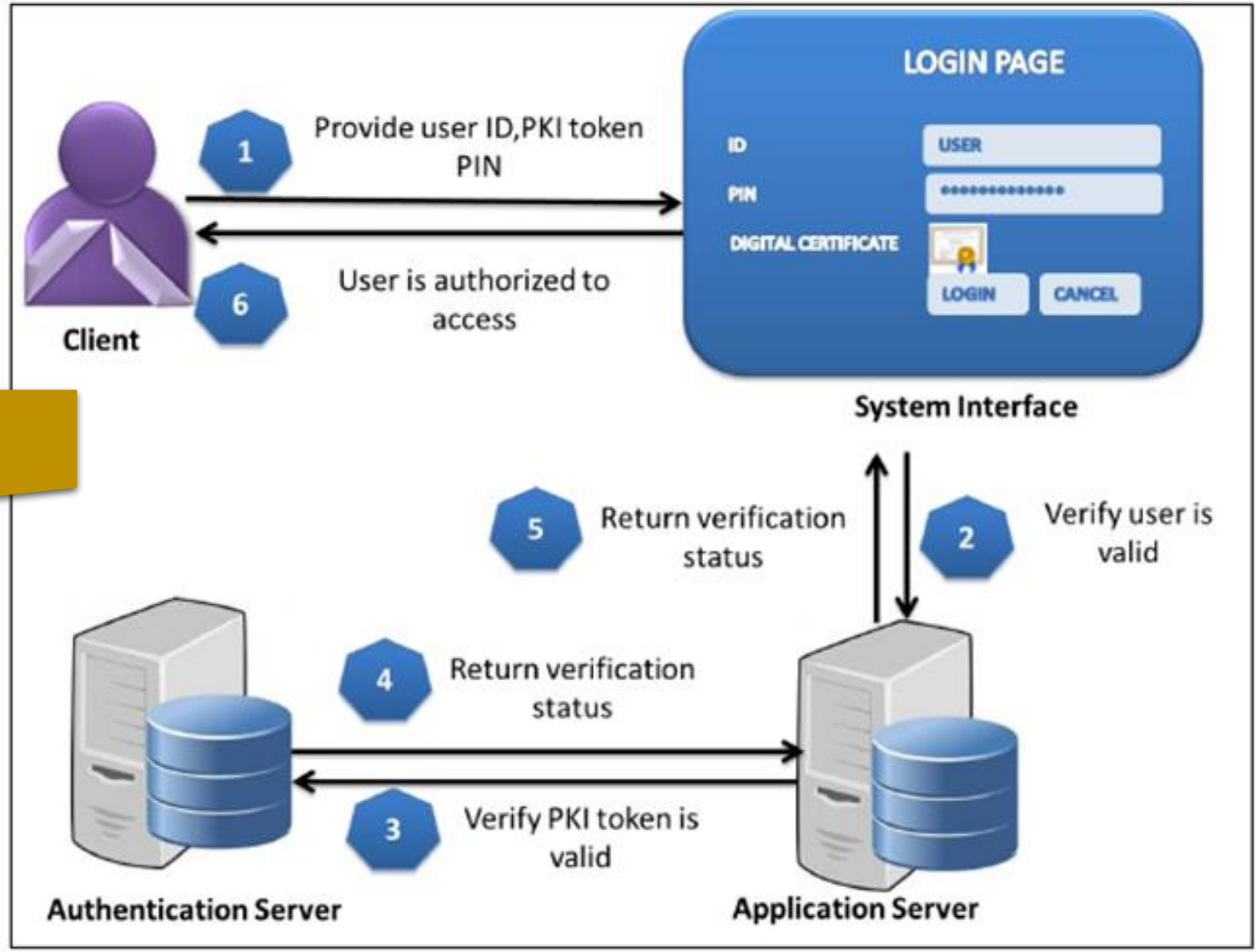
Tandatangan Digital

- Mengesahkan identiti pengguna, mengelakkan pengguna menyangkal tandatangan digital yang telah dilakukan.

N

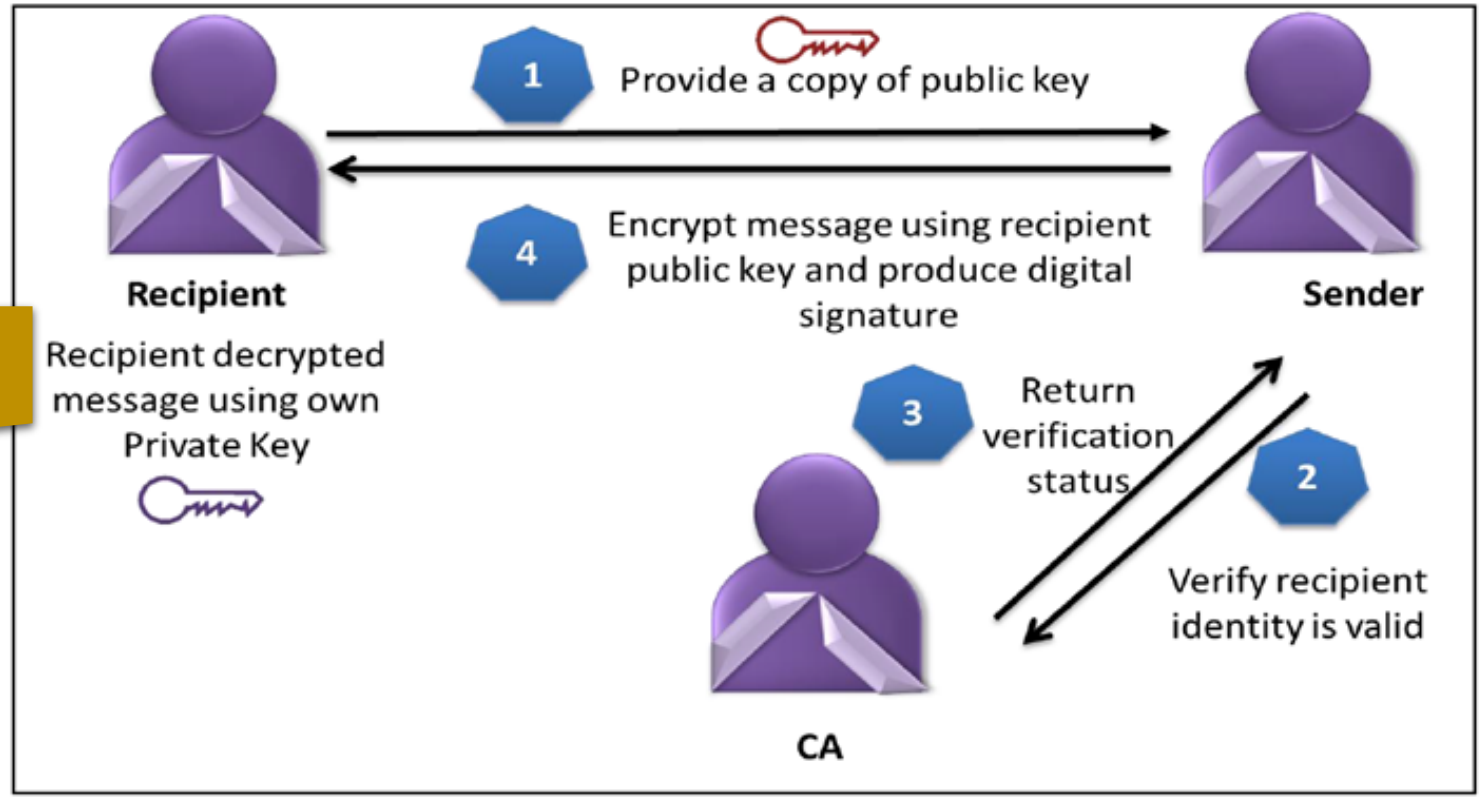
1 | PENGENALAN PERKHIDMATAN GPKI

PENGESAHAN IDENTITI

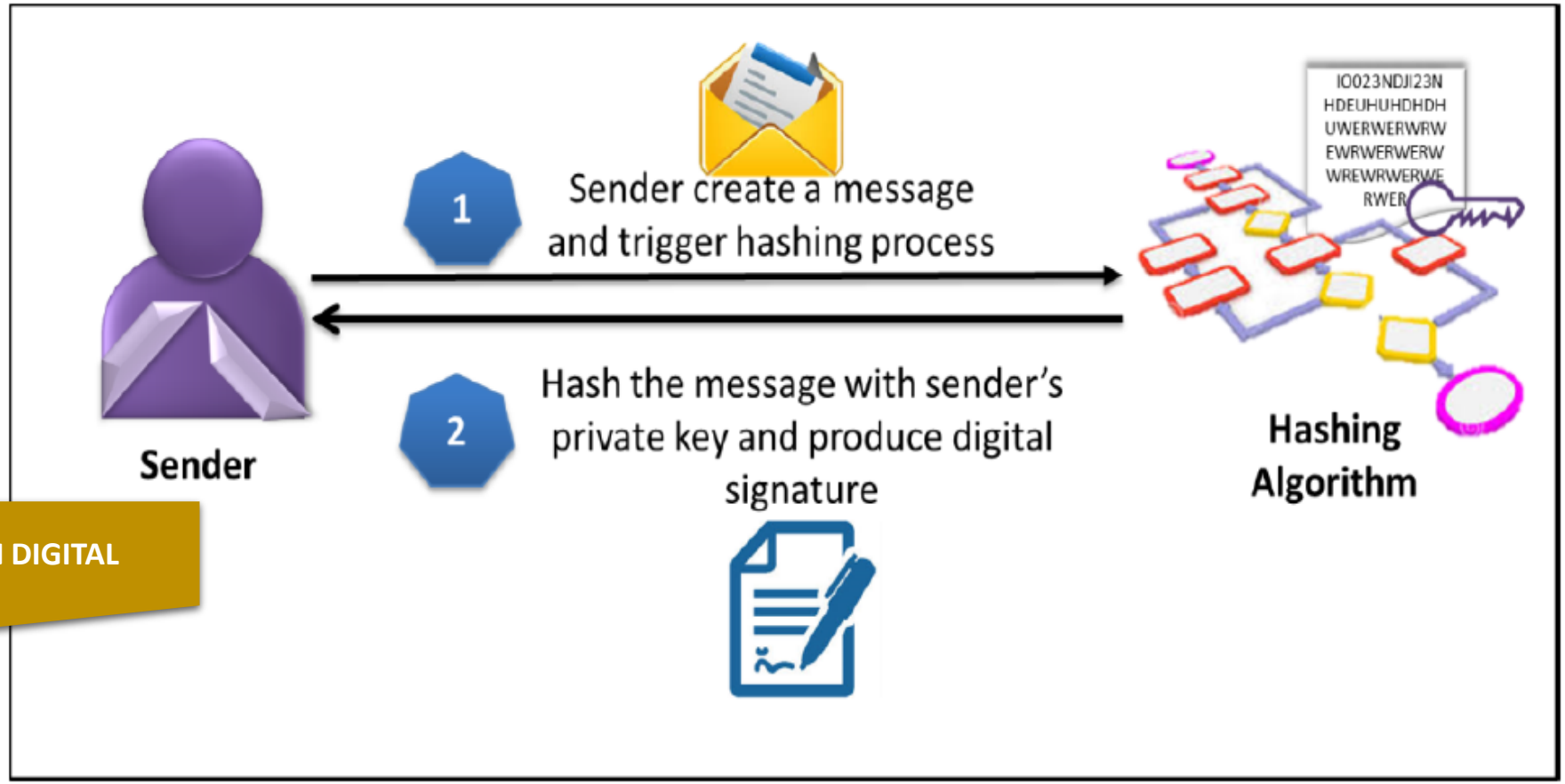


1 | PENGENALAN PERKHIDMATAN GPKI

PENYULITAN DAN PENYAHSULITAN



1 | PENGENALAN PERKHIDMATAN GPKI



TANDATANGAN DIGITAL

PELAKSANAAN TRANSAKSI SECARA ELEKTRONIK

PELAKSANAAN TANDATANGAN DIGITAL

AKTA AKTIVITI KERAJAAN ELEKTRONIK 2007

BAHAGIAN III PENGIKTIRAFAN UNDANG-UNDANG MESEJ ELEKTRONIK

10. (1) Apa-apa maklumat tidak boleh dinafikan kesan undang-undang, kesahan atau kebolehlaksanaan atas alasan bahawa ia adalah secara keseluruhan atau sebahagian dalam suatu bentuk elektronik

BAHAGIAN IV MEMENUHI KEHENDAK UNDANG-UNDANG MELALUI CARA ELEKTRONIK

13. (1) Jika mana-mana undang-undang menghendaki tandatangan seseorang di atas suatu dokumen, kehendak undang-undang itu dipenuhi, jika dokumen itu adalah dalam bentuk suatu mesej elektronik, oleh suatu tandatangan elektronik yang—

(a) dilampirkan kepada atau dikaitkan secara logik dengan mesej elektronik itu;
(b) mengenal pasti secukupnya orang itu dan menunjukkan secukupnya kelulusan orang itu terhadap maklumat yang berhubungan dengan tandatangan itu; dan
(c) adalah boleh dipercayai sewajarnya memberikan maksud bagi, dan hal keadaan yang tandatangan itu dikehendaki.

PELAKSANAAN TANDATANGAN DIGITAL

AKTA AKTIVITI KERAJAAN ELEKTRONIK 2007

BAHAGIAN IV MEMENUHI KEHENDAK UNDANG-UNDANG MELALUI CARA ELEKTRONIK

13. (2) Bagi maksud perenggan (1)(c), suatu tandatangan elektronik adalah sewajarnya boleh dipercayai jika—

(a) cara menghasilkan tandatangan elektronik itu dikaitkan dengan dan di bawah kawalan orang itu sahaja;

(b) apa-apa perubahan yang dibuat kepada tandatangan elektronik itu selepas masa penandatanganan itu boleh dikesan; dan

(c) apa-apa perubahan yang dibuat kepada dokumen itu selepas masa penandatanganan itu boleh dikesan.

(3) Akta Tandatangan Digital 1997 [Akta 562] hendaklah terus terpakai bagi apa-apa tandatangan digital yang digunakan sebagai suatu tandatangan elektronik dalam apa-apa aktiviti Kerajaan.

ARAHAN TEKNOLOGI MAKLUMAT 2007

18. CIRI-CIRI KESELAMATAN MAKLUMAT

18.1.2.5 Tidak Boleh Disangkal

(b) Tandatangan digital hendaklah digunakan bagi tujuan tidak boleh disangkal. Penggunaan tandatangan digital hendaklah mematuhi keperluankeperluan “Akta Tandatangan Digital 1997 (Akta 562)”.

PELAKSANAAN PENYULITAN DATA TERPERINGKAT KERAJAAN

ARAHAN TEKNOLOGI MAKLUMAT 2007

18. CIRI-CIRI KESELAMATAN MAKLUMAT

18.1.2.1 Kerahsiaan

(b) Semua maklumat terperingkat hendaklah dienkrip semasa dalam storan dan penghantaran dengan menggunakan algoritma standard industri yang mematuhi “Akta Tandatangan Digital 1997” (Akta 562).

(e) Agensi hendaklah memastikan penghantaran yang selamat di setiap peringkat dan melindungi trafik dari dicuri dengar, connection hijacking dan serangan rangkaian lain dengan menggunakan protokol Secure Socket Layer (SSL), Secure Shell (SSH) dan HSM versi semasa.

18.2.2. Integriti

(b) Agensi hendaklah melaksanakan semakan integriti seperti hash total untuk mencegah kesilapan dan maklumat tertinggal bagi mengekalkan integriti

PELAKSANAAN PENGESAHAN IDENTITI PENGGUNA YANG MELAKSANAKAN TRANSAKSI ELEKTRONIK

ARAHAN TEKNOLOGI MAKLUMAT 2007

18. CIRI-CIRI KESELAMATAN MAKLUMAT

18.1.2.4 Kesahihan

(d) Agensi hendaklah menilai teknik yang digunakan bagi pengenalan identiti dan kesahihan untuk menentukan mekanisme yang sesuai dengan persekitaran.

(e) Agensi hendaklah melaksanakan *two factor authentication*

PENYIMPANAN KUNCI PERIBADI DENGAN SELAMAT

AKTA TANDATANGAN DIGITAL 1997

KEWAJIPAN PELANGGAN UNTUK MENYIMPAN KUNCI PERSENDIRIAN DENGAN SELAMAT

43. Dengan menerima sesuatu perakuan yang dikeluarkan oleh pihak berkuasa pemerakuan berlesen, pelanggan yang dinamakan dalam perakuan itu menerima kewajipan untuk menjalankan jagaan yang munasabah untuk mengekalkan kawalan ke atas kunci persendirian dan mencegah pendedahannya kepada mana-mana orang yang tidak diberi kuasa untuk menghasilkan tandatangan digital pelanggan itu.

PENYIMPANAN KUNCI PERIBADI DENGAN SELAMAT

PERATURAN-PERATURAN TANDATANGAN DIGITAL 1998

REGULATION 30. STORAGE OF PRIVATE KEYS

(1) The data storage medium for the private key may be hardware based or software based.
(2) If the data storage medium of the private key is hardware based, the holder of the private key shall ensure that the token, smart card or other external device in which the private key is stored is kept in a secure place and in a secure manner.
(3) If the data storage medium of the private key is software based, the holder of the private key shall ensure that the computer system in which the private key is stored
is reasonably secure.
(4) The personal identification numbers or other data used for the identification of the rightful holder of the private key in conjunction with the data storage medium for the private key shall be kept secret.

ARAHAN TEKNOLOGI MAKLUMAT 2007

18.2.1. Kerahsiaan

(c) Semua *private keys* perlu dilindungi dan dirahsiakan. Laporan hendaklah dibuat dengan segera apabila *private keys* hilang atau musnah.

PELANGGARAN PERUNDANGAN

AKTA TANDATANGAN DIGITAL 1997

MAKLUMAT PALSU

73. Seseorang yang membuat, secara lisan atau bertulis, menandatangani atau memberikan apa-apa perisytiharan, penyata, perakuan atau dokumen atau maklumat lain yang dikehendaki dibawah Akta ini yang tidak benar, tidak tepat atau mengelirukan dalam apa-apa butir-butir melakukan suatu kesalahan dan boleh, apabila disabitkan, **didenda tidak melebihi lima ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi sepuluh tahun atau kedua-duanya**.

1 | PENGENALAN PERKHIDMATAN GPKI

PEKELILING KEMAJUAN PENTADBIRAN AWAM BIL. 3/2015: DASAR PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN [GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)]

PERNYATAAN DASAR

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

PRINSIP PEGANGAN

1. **Agensi Pusat menanggung semua kos bagi perkhidmatan GPKI untuk kementerian dan jabatan persekutuan yang bertindak sebagai agensi pelaksana dan semua aplikasi agensi pelaksana.**
2. **Semua penjawat awam hanya dibenarkan menggunakan satu sijil digital sahaja.**
3. **Agensi Pelaksana yang membangunkan sistem ICT kerajaan perlu memastikan sistem berkenaan boleh menyokong mana-mana medium sijil digital perkhidmatan GPKI yang sedang berkuat kuasa.**
4. **Pemegang sijil digital yang mempunyai capaian kepada pelbagai aplikasi yang mempunyai tahap kawalan keselamatan yang berbeza hendaklah menggunakan medium sijil digital yang boleh mencapai aplikasi yang mempunyai tahap kawalan keselamatan yang tertinggi.**

TANGGUNGAN KOS AGENSI

Bil.	Kategori Agensi	Sektor Perkhidmatan	Tanggungan Kos	
			Integrasi / Sijil Digital Pelayan	Sijil Digital Pengguna
1.	Kementerian	Agensi Sektor Awam	✔	✔
2.	Jabatan			
	i. Agensi Pentadbiran Persekutuan		✔	✔
	ii. Agensi Pentadbiran Negeri		✘	✔
3.	Badan Berkanun			
	i. Badan Berkanun Persekutuan Tidak Diasingkan Saraan		✔	✔
	ii. Badan Berkanun Persekutuan Diasingkan Saraan		✘	✔
	iii. Badan Berkanun Negeri		✘	✔
4.	Pihak Berkuasa Tempatan / Penguasa Tempatan			
	i. Pihak Berkuasa Tempatan / Penguasa Tempatan Persekutuan		✘	✔
	ii. Pihak Berkuasa Tempatan / Penguasa Tempatan Negeri		✘	✔

SISTEM GPKI

2011

SISTEM GPKI 1.0
DAN SCAN GPKI
AGENT 1.0

2015

GPKI MOBILE
CLIENT 1.0

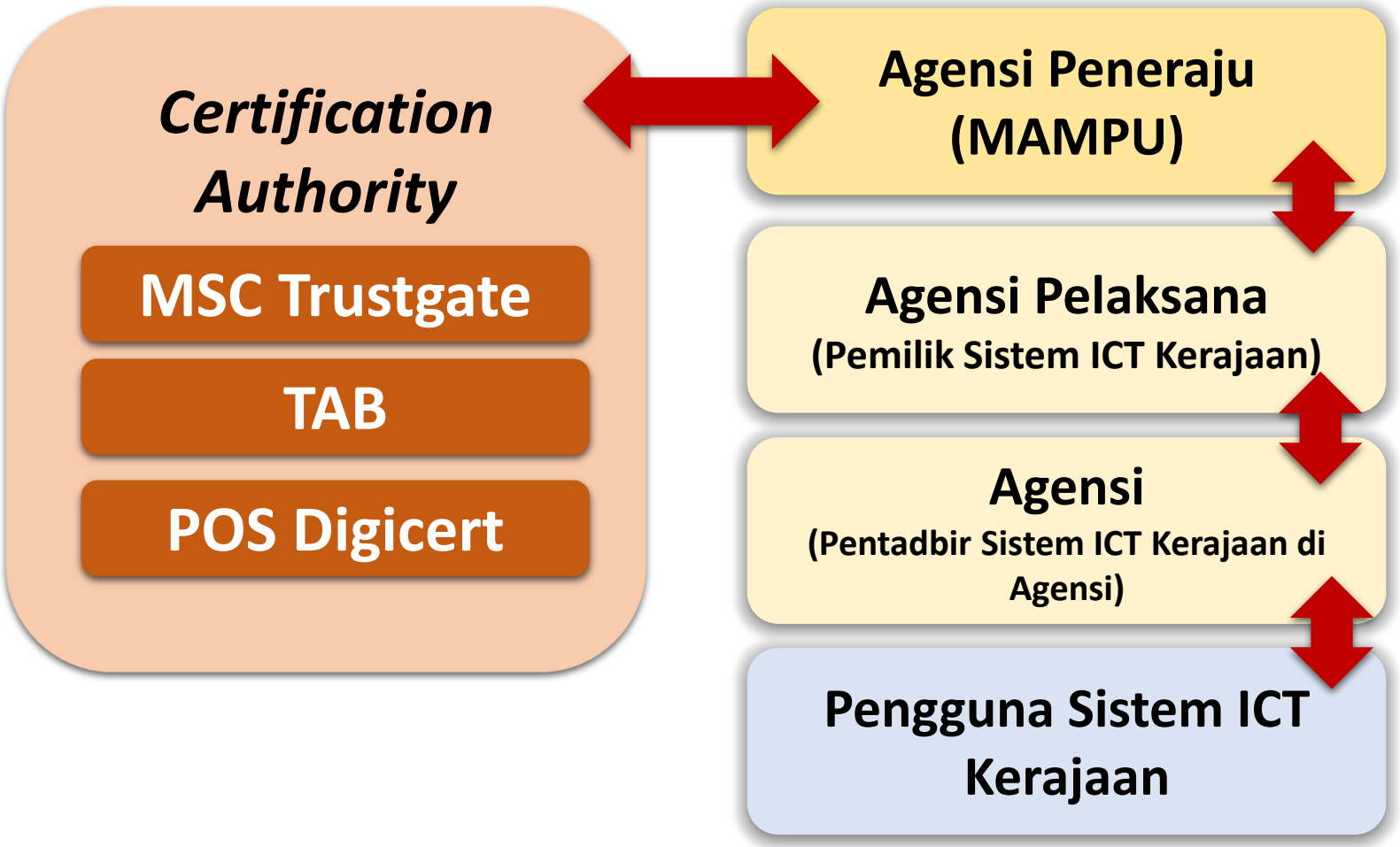
2016

SISTEM GPKI 1.0
DAN SCAN GPKI
AGENT 1.1

2017

SISTEM GPKI 2.0
GPKI AGENT 2.0
GPKI MOBILE
CLIENT 1.0

MODEL OPERASI

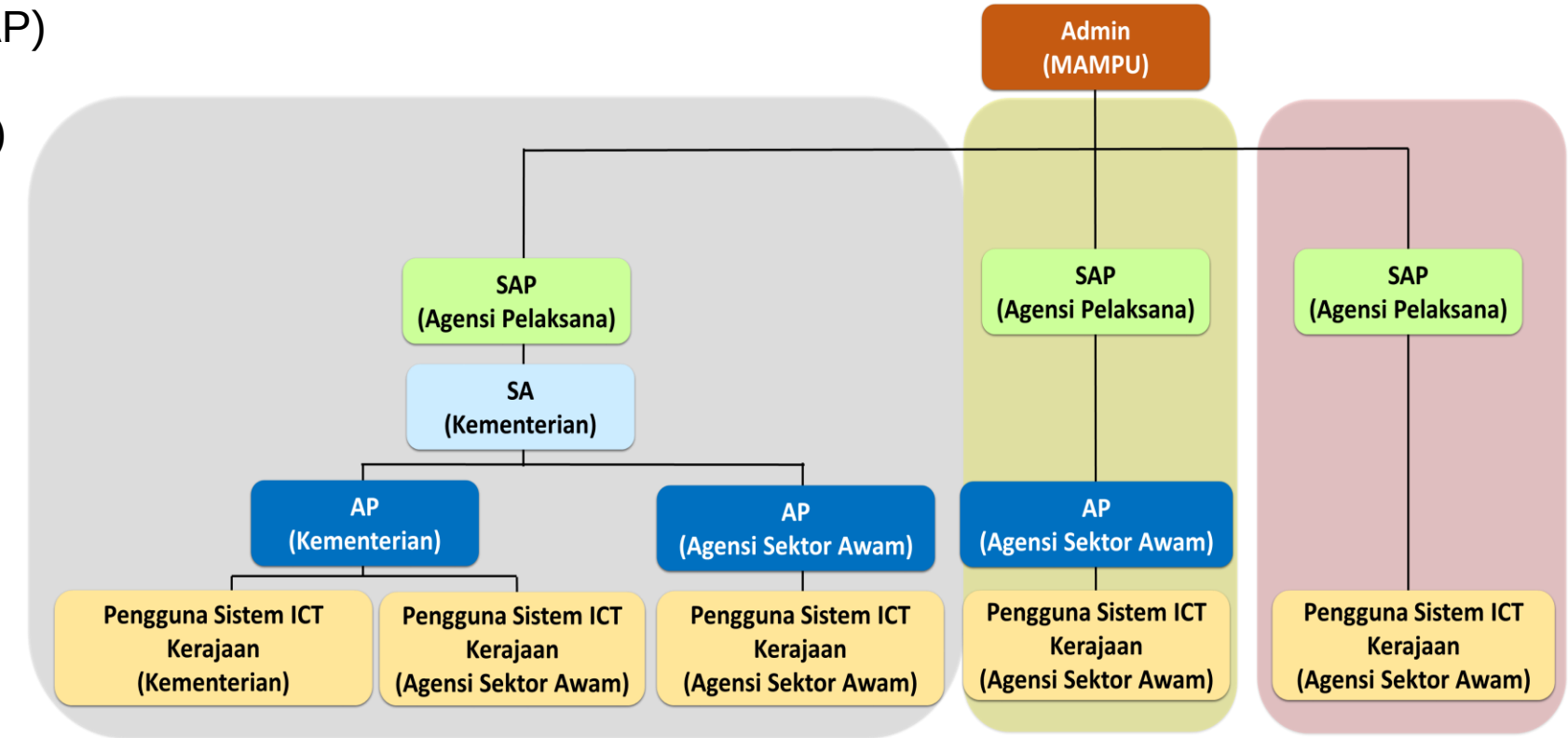


1 | PENGENALAN PERKHIDMATAN GPKI

Pentadbir GPKI adalah pegawai di agensi sektor awam yang bertanggungjawab untuk mentadbir dan memantau pengguna dan pengurusan sijil digital pengguna di bawah seliaannya.

Pentadbir GPKI terdiri daripada:

i. Admin
ii. Sub Admin Pelaksana (SAP)
iii. Sub Admin (SA)
iv. Authorized Personnel (AP)



1 | PENGENALAN PERKHIDMATAN GPKI

ADMIN

Pemilik Perkhidmatan GPKI

- Mendaftar SAP di Agensi Pelaksana
- Mengesahkan permohonan sijil digital SAP aplikasi ICT Kerajaan di bawah agensi / negeri
- Memantau SAP, SA, AP dan pengguna Sistem GPKI
- Memantau dan menyelaras pelaksanaan Sistem GPKI

SUB ADMIN PELAKSANA (SAP)

Pemilik Sistem Aplikasi ICT Kerajaan di Agensi Pelaksana

- Mendaftar SA kementerian / JANM Negeri
- Mengesahkan permohonan sijil digital SA aplikasi ICT Kerajaan di bawah agensi / negeri
- Memantau SA, AP dan pengguna bagi Sistem Aplikasi ICT Kerajaan

***SUB ADMIN* (SA)**

Pentadbir Sistem GPKI di Kementerian / JANM Negeri

- Mendaftar AP di agensi
- Mengesahkan permohonan sijil digital AP aplikasi ICT Kerajaan di bawah agensi / negeri
- Memantau AP dan pengguna di kementerian / negeri

AUTHORIZED PERSONNEL (AP)

Pentadbir Sistem GPKI di Agensi

- Mendaftar pengguna di agensi.
- Mengesahkan permohonan sijil digital pengguna aplikasi ICT Kerajaan di bawah agensi.
- Memantau pengguna di agensi

1 | PENGENALAN PERKHIDMATAN GPKI

1. **Permohonan Peranan Pengguna GPKI**

Pengguna

PERMOHONAN

AP

2. **Permohonan Peranan AP**

AP

PERMOHONAN

SA

3. **Permohonan Peranan SA**

SA

PERMOHONAN

SA PELAKSANA

4. **Permohonan Peranan SA Pelaksana**

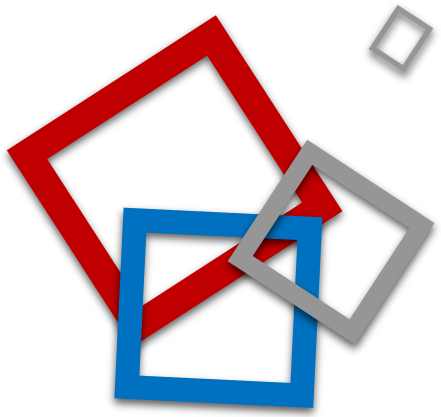
SA PELAKSANA

PERMOHONAN

ADMIN

PERKHIDMATAN YANG DITAWARKAN

1. Pengurusan dan Pembekalan Sijil Digital Pengguna
2. Pengurusan dan Pembekalan Sijil Digital Pelayan



3. Perkhidmatan Meja Bantuan dan Khidmat Sokongan Teknikal
4. Khidmat Nasihat dan Konsultasi bagi Penggunaan PKI

2 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PENGGUNA

1. Pengurusan Sijil Digital Pengguna meliputi proses pengesahan permohonan dan identiti pemohon, penjanaan pasangan kunci awam dan peribadi, pengeluaran dan pembatalan Sijil Digital Pengguna

2 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PENGGUNA

2. MAMPU menyediakan perkhidmatan pembekalan Sijil Digital Pengguna yang dikeluarkan oleh CA seperti berikut:

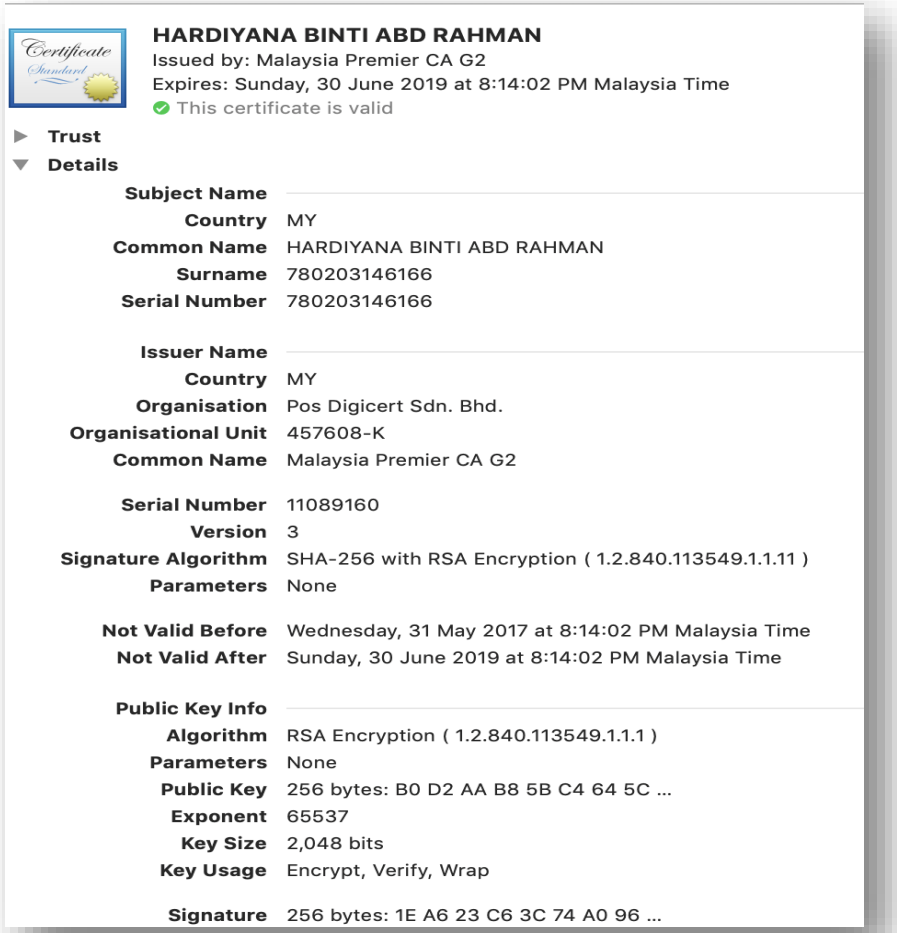
BIL.	PERKARA	SIJIL DIGITAL TOKEN	SIJIL DIGITAL ROAMING	SOFTCERT
1.	Keterangan	Sijil digital yang disimpan di dalam peranti di mana kunci peribadi dijana secara onboard dan disimpan di dalam token yang mengandungi cip kriptografi	Fail yang mengandungi sijil digital pengguna dan kunci peribadi (private key) yang disimpan dalam pelayan di agensi peneraju	Fail yang mengandungi sijil digital pengguna dan kunci peribadi (private key) yang dimuat turun dan disimpan ke dalam komputer pengguna.
2.	Jaminan Keselamatan	**TINGGI**	**SEDERHANA**	**SEDERHANA**
3.	Ciri-ciri keselamatan	i. Kunci peribadi (private key) disimpan dalam token ii. Kunci peribadi (private key) tidak boleh disalin iii. Kalis ubah (tamper-proof) iv. Pasangan kunci (key pair) dijana dalam cip (onboard key generation)	i. Kunci peribadi (private key) disimpan di agensi peneraju ii. Kunci hanya disimpan bagi tempoh tidak melebihi dua jam dalam komputer pengguna	i. Kunci peribadi (private key) disimpan di komputer pengguna ii. Kunci disimpan secara tetap dalam komputer pengguna sehingga ianya dihapuskan
4.	Storan			

2 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PENGGUNA

3. **Sijil Digital Pengguna** ialah sijil yang dikeluarkan kepada individu oleh CA yang mengandungi maklumat berkenaan dengan identiti pengguna dan kunci awam (*public key*) pengguna tersebut.

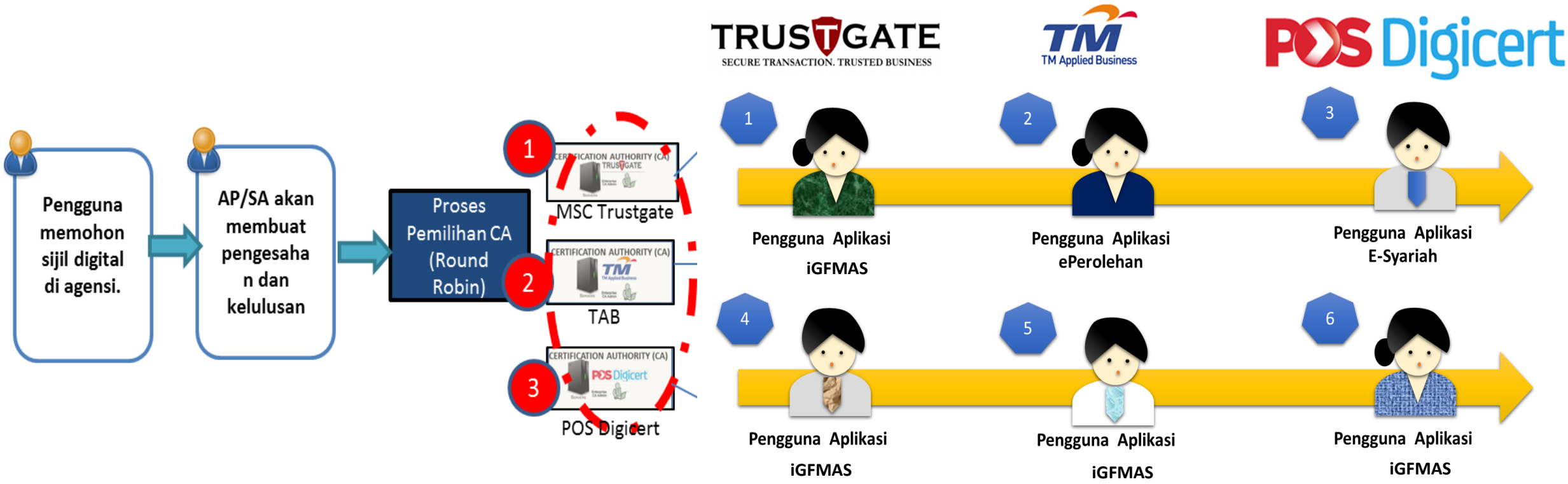
4. Tempoh sah laku Sijil Digital Pengguna yang dibekalkan adalah **24 bulan.**

5. **Seorang pengguna** hanya boleh memiliki **satu Sijil Digital Pengguna** sahaja yang mempunyai **tahap kawalan tertinggi** bagi mengakses kesemua sistem ICT kerajaan yang dibenarkan.



2 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PENGGUNA

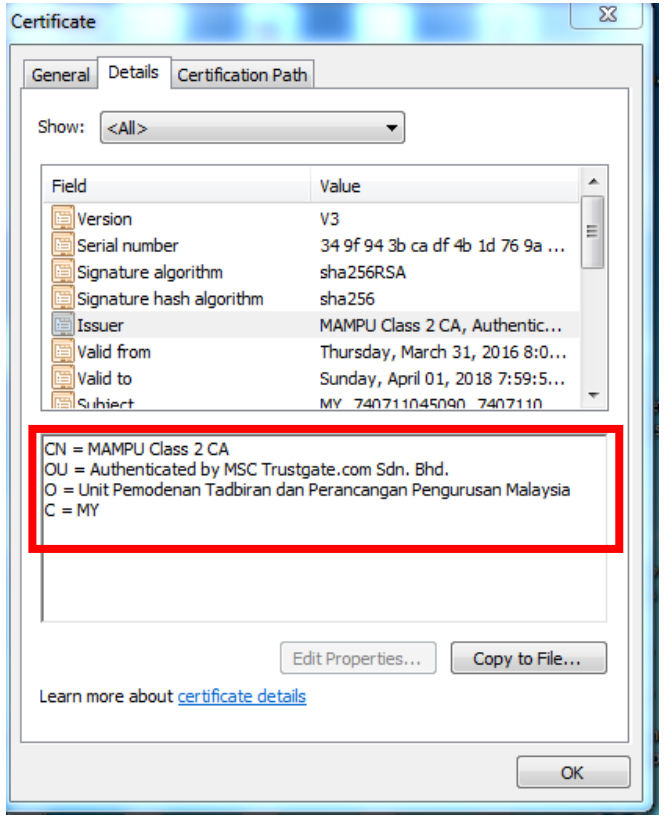
5. Pembekalan Sijil Digital Pengguna adalah secara round robin.



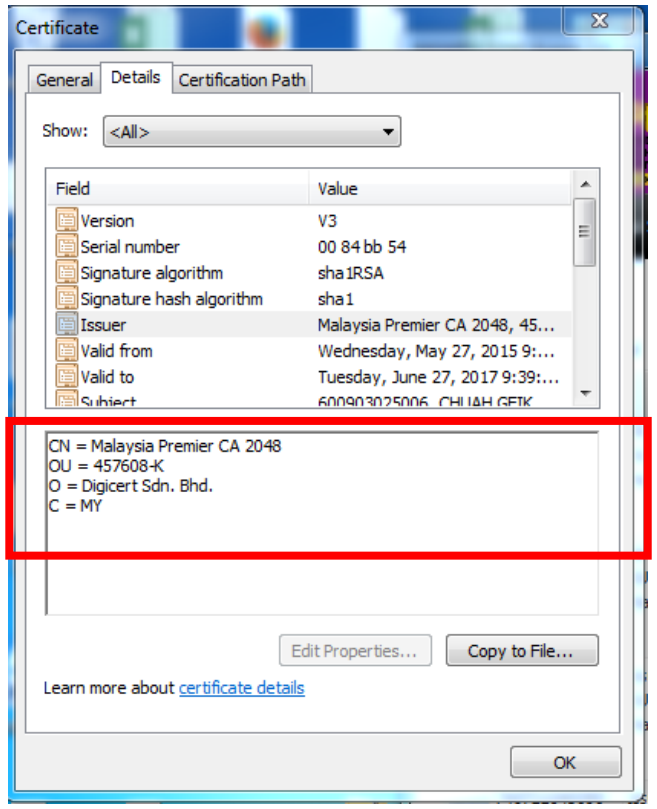
2 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PENGGUNA

5. Profil Sijil Digital Pengguna

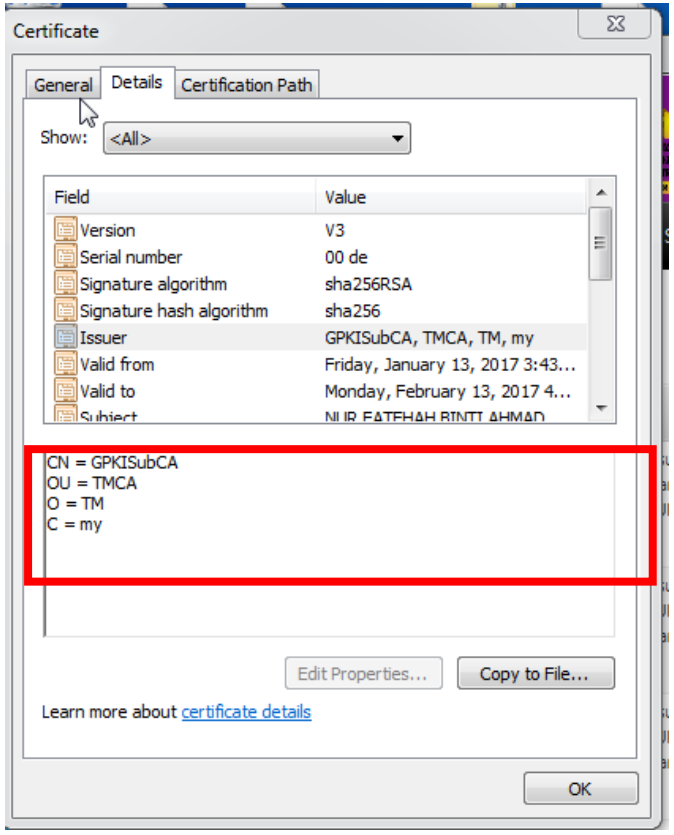
SIJIL DIGITAL MSC TRUSTGATE



SIJIL DIGITAL POS DIGICERT



SIJIL DIGITAL TAB



2 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PENGGUNA

Bil.	Keperluan Tahap Kawalan Keselamatan Sistem ICT	Keperluan Medium Sijil Digital Pengguna	Medium Sijil Digital Pengguna Yang Perlu Disokong Oleh Sistem ICT Kerajaan	Sijil Digital Pengguna	
				Medium Sijil Digital Pengguna Semasa	Keperluan Pertukaran Medium Sijil Digital Pengguna
1.	Tinggi	Token	Token	Token	Tidak Perlu
				RoamingCert	Token
				SoftCert	Token
2.	Sederhana	RoamingCert	Token RoamingCert	Token	Tidak Perlu
				RoamingCert	Tidak Perlu
				SoftCert	RoamingCert
3.	Sederhana	SoftCert	Token RoamingCert SoftCert	Token	Tidak Perlu
				RoamingCert	Tidak Perlu
				SoftCert	Tidak Perlu

2 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PENGGUNA

KRITERIA PERMOHONAN

1. Agensi pengguna adalah termasuk di dalam kategori agensi yang kos pembekalan Sijil Digital Pengguna di bawah tanggungan MAMPU.

2. Pengguna mestilah mempunyai peranan di dalam sistem ICT kerajaan dan memerlukan Sijil Digital Pengguna untuk melaksanakan transaksi di dalam sistem ICT kerajaan.

3. Pengguna tidak disenaraihitamkan untuk memohon Sijil Digital Pengguna.

4. Semua permohonan dikemukakan melalui Portal GPKI.

PROSES PERMOHONAN SIJIL DIGITAL PENGGUNA

1. Pentadbir GPKI di agensi mendaftarkan pengguna.

2. Pengguna membuat Permohonan Sijil Digital Pengguna. Dokumen yang diperlukan:
   i. Salinan MyKad

3. Pentadbir GPKI di agensi mengesahkan permohonan Sijil Digital Pengguna.

4. CA meluluskan dan memproses permohonan Sijil Digital Pengguna.

5. Pengguna mengaktifkan Sijil Digital Pengguna menggunakan GPKI Agent.

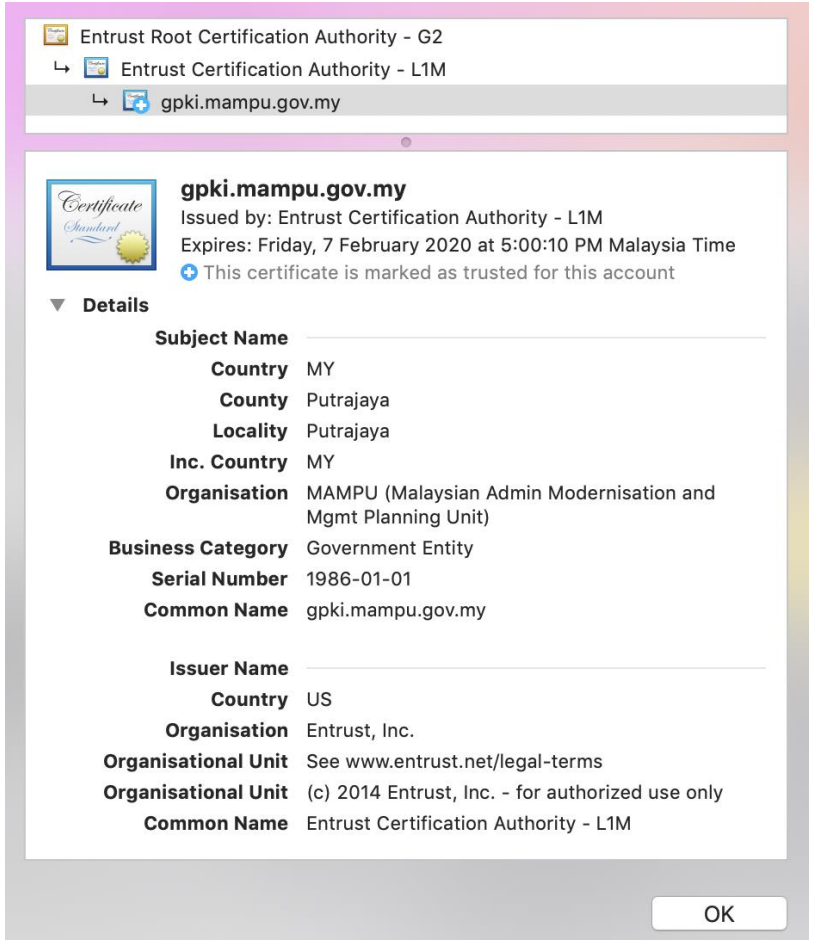
Nota: Semua proses permohonan Sijil Digital Pengguna melalui Portal GPKI kecuali pengaktifan Sijil Digital Pengguna melalui GPKI Agent.

3 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PELAYAN

1. Pengurusan Sijil Digital Pelayan meliputi proses pengesahan permohonan dan identiti pemohon, organisasi dan domain; penjanaan pasangan kunci awam dan peribadi, pengeluaran dan pembatalan Sijil Digital Pelayan.

2. Sijil Digital Pelayan ialah sijil yang dikeluarkan oleh CA untuk mengesahkan identiti pelayan sistem ICT kerajaan supaya maklumat transaksi dihantar dengan selamat.

3. Tempoh **sah laku** Sijil Digital Pengguna yang dibekalkan adalah **24 bulan**



3 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PELAYAN

1. MAMPU menyediakan perkhidmatan pembekalan Sijil Digital Pengguna yang dikeluarkan oleh CA seperti berikut:

i. Sijil Digital Pelayan Single Domain EV

- Merupakan Sijil Digital Pelayan yang didaftarkan bagi satu domain sahaja.
- Kunci peribadi (private key) pelayan dijana khusus bagi domain yang didaftarkan sahaja.
- Sekiranya kunci peribadi (private key) pelayan terdedah atau terjejas (compromised), implikasi keselamatan hanya melibatkan domain tersebut

Contoh domain: gpki.mampu.gov.my.

ii. Sijil Digital Pelayan Multi Domain EV

- Sijil Digital Pelayan Multi Domain merupakan Sijil Digital Pelayan yang mengandungi satu domain utama dan sekurang-kurangnya satu subdomain (Subject Alternative Names, SANs).
- Kunci peribadi (private key) pelayan adalah sama dan dikongsi oleh dua atau lebih domain yang didaftarkan.
- Sekiranya kunci peribadi (private key) pelayan terdedah atau terjejas (compromised), implikasi keselamatan adalah ke atas semua domain.

Contoh: domain utama - gpki.mampu.gov.my
subdomain - gpki.bpg.gov.my

iii. Sijil Digital Pelayan Wildcard OV

- Sijil Digital Pelayan Wildcard ialah Sijil Digital Pelayan yang mengandungi pelbagai subdomain di bawah satu domain yang sama dan menggunakan simbol wildcard (“*”) dalam satu sijil.
- Kunci peribadi (private key) pelayan bagi domain akan dikongsi bagi semua subdomain yang didaftarkan di bawah domain yang sama.
- Sekiranya kunci peribadi (private key) pelayan terdedah atau terjejas (compromised), implikasi keselamatan adalah kepada semua subdomain yang menggunakan kunci yang sama.

Contoh domain: domain utama - *.gpki.gov.my,
subdomain 1 – gpki1.gpki.gov.my,
subdomain 2 – gpki2.gpki.gov.my

3 | PENGURUSAN DAN PEMBEKALAN SIJIL DIGITAL PELAYAN

KRITERIA PERMOHONAN

1. Agensi pengguna adalah termasuk di dalam kategori agensi yang kos pembekalan Sijil Digital Pengguna di bawah tanggungan MAMPU.

2. Tahap risiko sistem ICT kerajaan /laman web / portal.

3. Domain sistem ICT kerajaan /laman web / portal gensi hendaklah menggunakan domain ".gov.my." dan telah mendapat kelulusan pengurusan agensi.

4. Organisasi tidak disenaraihitamkan untuk memohon Sijil Digital Pelayan.

5. Semua permohonan dikemukakan melalui Portal GPKI.

PROSES PERMOHONAN SIJIL DIGITAL PELAYAN

1. Pentadbir Pelayan di agensi Permohonan Sijil Digital Pelayan. Dokumen yang diperlukan:

   i. Surat Permohonan
   ii. Laporan Penilaian Risiko
   iii. Fail *Certificate Signing Request* (CSR)

2. Admin mengesahkan permohonan Sijil Digital Pelayan.

3. CA meluluskan dan memproses permohonan Sijil Digital Pelayan.

4. Pentadbir Pelayan di agensi memasang Sijil Digital Pelayan di pelayan sistem ICT kerajaan /laman web / portal.

4| MEJA BANTUAN DAN KHIDMAT SOKONGAN TEKNIKAL GPKI

1. Meja Bantuan GPKI merujuk kepada perkhidmatan yang disediakan bagi mengurus dan mengendalikan tiket aduan yang diterima daripada Pengguna berkaitan Perkhidmatan GPKI.

2. Medium saluran aduan Meja Bantuan GPKI terdiri daripada:

    i. Portal GPKI
    ii. E-mel
    iii. Telefon
    iv. Kaunter Meja Bantuan

3. Khidmat Sokongan Teknikal merujuk kepada bantuan teknikal yang diberikan di lokasi agensi bagi masalah berkaitan Perkhidmatan GPKI.

4. Skop Perkhidmatan Meja Bantuan dan Khidmat Sokongan Teknikal GPKI adalah seperti berikut:

    i. Bantuan secara dalam talian.
    ii. Bantuan teknikal di lokasi agensi.

4| MEJA BANTUAN DAN KHIDMAT SOKONGAN TEKNIKAL GPKI

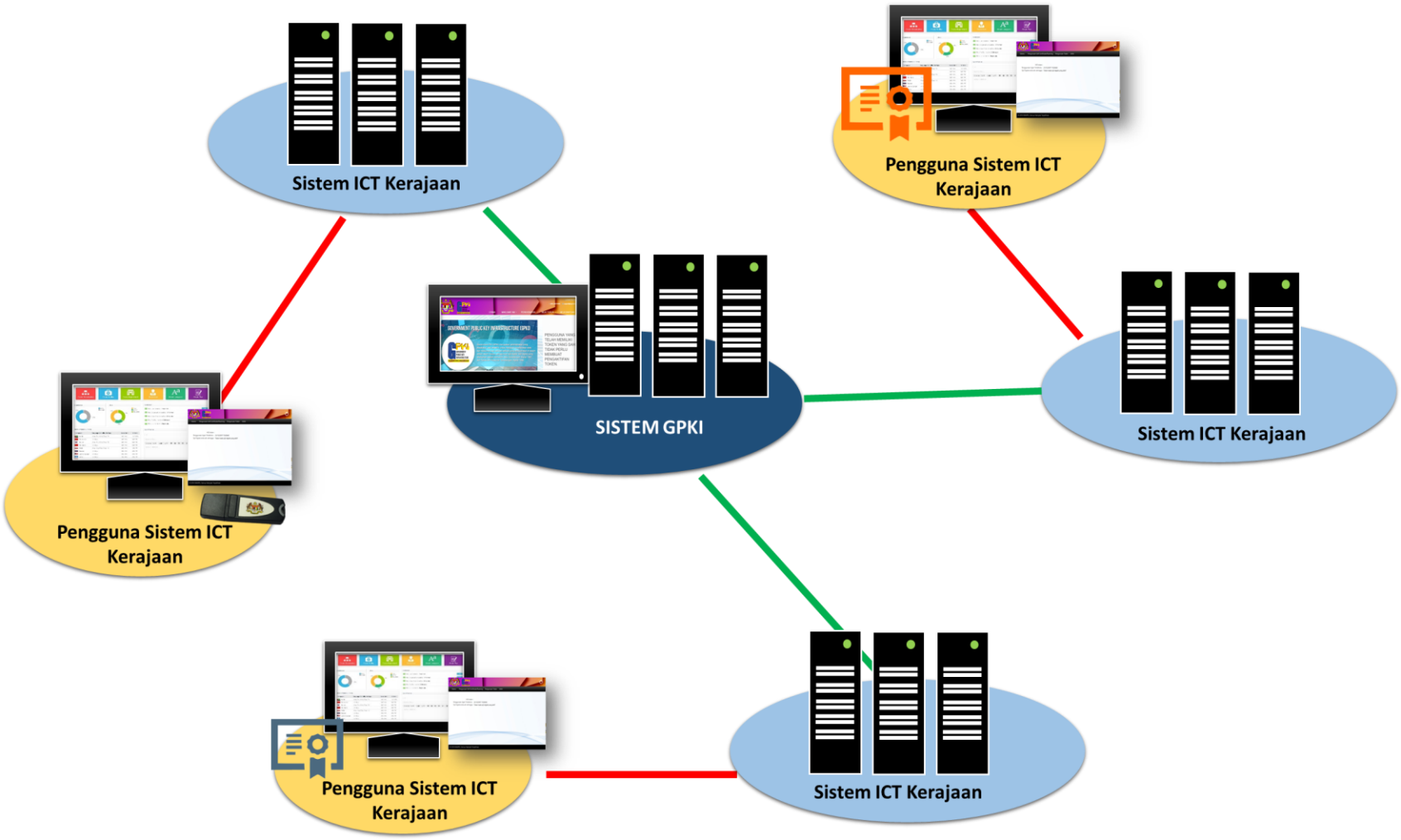
5 | KHIDMAT NASIHAT DAN KONSULTASI BAGI PENGGUNAAN PKI

1. Perkhidmatan GPKI dilaksanakan oleh MAMPU dan dipantau oleh Jawatankuasa Pelaksana Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) atau Jawatankuasa Pemandu Projek GPKI.

2. Skop khidmat nasihat dan konsultasi bagi ialah seperti yang berikut:

   i. Penggunaan PKI dalam sistem ICT kerajaan.
   ii. Konsultasi integrasi sistem ICT kerajaan dan perkhidmatan GPKI.
   iii. Perancangan dan pelaksanaan Perkhidmatan GPKI.
   iv. Latihan kepada Pentadbir GPKI.

INTEGRASI SISTEM ICT KERAJAAN DENGAN SISTEM GPKI



5 | KHIDMAT NASIHAT DAN KONSULTASI BAGI PENGGUNAAN PKI

KEPERLUAN PENGGUNAAN PKI

Kriteria				Kawalan Keselamatan					
Kategori Sistem ICT Kerajaan	Klasifikasi Data /Maklumat	Nilai Data / Maklumat	Tahap Risiko	Ciri Keselamatan Maklumat	Keperluan Sijil Digital Pengguna	Keperluan Sijil Digital Pelayan			
						Capaian Melalui Internet			Capaian Melalui Intranet
						Jumlah Domain = 1	Jumlah Domain / Subdomain > 1	Jumlah Domain / Subdomain antara 1 hingga 3	
Kritikal	Rahsia Besar	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Rahsia	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Sulit	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Terhad	Sederhana	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	SoftCert	Single Domain OV	Multi Domain OV	Wildcard OV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Terbuka	Sederhana	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	SoftCert	Multi Domain OV	Multi Domain OV	Wildcard OV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
Strategik	Rahsia Besar	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Rahsia	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Sulit	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Terhad	Sederhana	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	SoftCert	Single Domain OV	Multi Domain OV	Wildcard OV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Terbuka	Rendah	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	SoftCert	Multi Domain OV	Multi Domain OV	Wildcard OV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada

5 | KHIDMAT NASIHAT DAN KONSULTASI BAGI PENGGUNAAN PKI

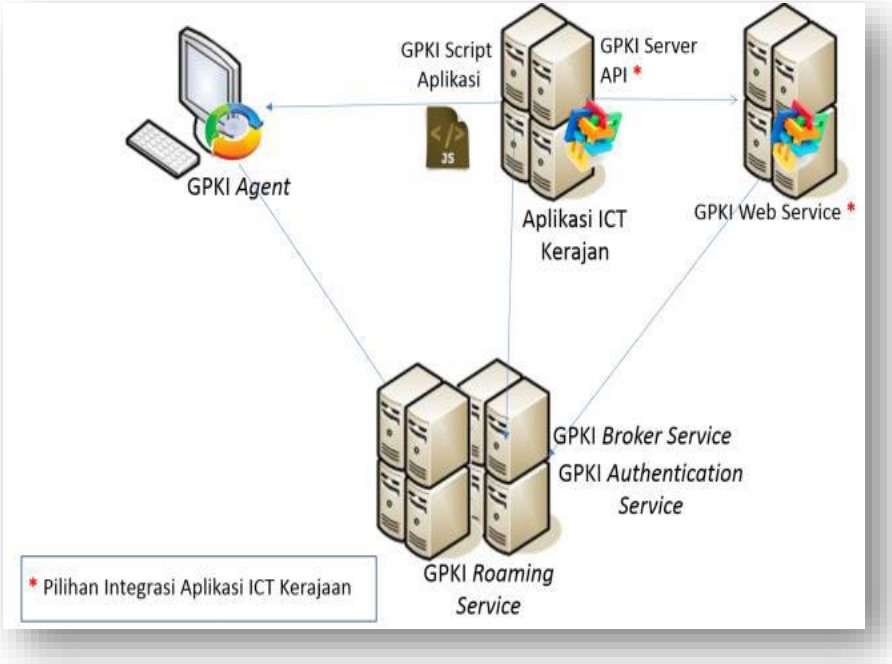
KEPERLUAN PENGGUNAAN PKI

Kriteria				Kawalan Keselamatan					
						Keperluan Sijil Digital Pelayan			
						Capaian Melalui Internet			
Kategori Sistem ICT Kerajaan	Klasifikasi Data /Maklumat	Nilai Data / Maklumat	Tahap Risiko	Ciri Keselamatan Maklumat	Keperluan Sijil Digital Pengguna	Jumlah Domain = 1	Jumlah Domain / Subdomain > 1	Jumlah Domain / Subdomain antara 1 hingga 3	Capaian Melalui Intranet
Sokongan Dalaman	Rahsia Besar	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Rahsia	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Sulit	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Terhad	Sederhana	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	SoftCert	Single Domain OV	Multi Domain OV	Wildcard OV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Terbuka	Rendah	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	SoftCert	Multi Domain OV	Multi Domain OV	Wildcard OV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
Sokongan Umum	Rahsia Besar	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Rahsia	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Sulit	Tinggi	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	RoamingCert	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Terhad	Sederhana	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	SoftCert	Single Domain OV	Multi Domain OV	Wildcard OV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada
	Terbuka	Rendah	Tinggi	C, A, I, N	Token	Single Domain EV	Multi Domain EV	Multi Domain EV	Self Signed Certificate
			Sederhana	C, A, I, N	SoftCert	Multi Domain OV	Multi Domain OV	Wildcard OV	Self Signed Certificate
			Rendah	Tiada	Tiada	Tiada	Tiada	Tiada	Tiada

5 | KHIDMAT NASIHAT DAN KONSULTASI BAGI PENGGUNAAN PKI

KEPERLUAN PELAKSANAAN

1. Menggunakan profil Sijil Digital Pengguna yang disediakan oleh agensi peneraju.
2. Memastikan medium sijil digital yang dibekalkan bersesuaian (compatible) dengan sistem ICT kerajaan.
3. Memastikan ketersediaan rangkaian.
4. Memasang GPKI Agent pada setiap komputer pengguna yang terlibat.
5. Memasang pemacu perisian token (token software driver) pada setiap komputer pengguna yang terlibat.
6. Melaksanakan pengujian integrasi sistem ICT kerajaan dengan Sistem GPKI.
7. Keperluan pelayar dan sistem pengoperasian
    i. Pelayar : IE6 dan ke atas, Chrome, Mozilla Firefox
    ii. Sistem Pengoperasian : Windows XP dan ke atas
8. Menyemak dan memastikan CRL adalah yang terkini berdasarkan tarikh pengeluaran oleh CA **(Optional)**
9. Memasang root cert CA di dalam pelayan Sistem ICT Kerajaan **(Optional)**



5 | KHIDMAT NASIHAT DAN KONSULTASI BAGI PENGGUNAAN PKI

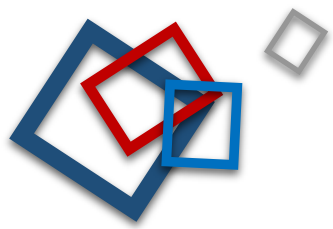
KRITERIA PERMOHONAN INTEGRASI SISTEM ICT DENGAN SISTEM GPKI

1. Agensi pengguna adalah termasuk di dalam kategori agensi yang kos Perkhidmatan GPKI di bawah tanggungan MAMPU.

2. Sistem ICT Kerajaan / Laman Web / Portal mempunyai nilai risiko sekurang-kurangnya sederhana dan mempunyai capaian melalui Internet.

3. Semua permohonan telah dikemukakan secara rasmi kepada :

   Pengarah
   Bahagian Pembangunan Perkhidmatan Gunasama
   Infrastruktur dan Keselamatan ICT (BPG)
   Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)
   Jabatan Perdana Menteri
   Aras 1, Blok B, Bangunan MKN-Embassy Techzone
   Jalan Teknokrat 2, 63000 Cyberjaya,
   Sepang, Selangor
   E-mel : pmo@mampu.gov.my



5 | KHIDMAT NASIHAT DAN KONSULTASI BAGI PENGGUNAAN PKI

PROSES PERMOHONAN PERKHIDMATAN GPKI

1. Agensi Pelaksana melaksanakan penilaian risiko ke atas sistem ICT kerajaan dalam konteks PKI serta mengenal pasti keperluaan penggunaan PKI sebagai langkah kawalan keselamatan Sistem ICT.

2. Pengguna membuat Permohonan Integrasi / Sijil Digital Pengguna / Sijil Digital Pelayan dengan mengemukakan perkara berikut:

   i. Surat Permohonan
   ii. Laporan Penilaian Risiko
   iii. Dokumen Keperluan Penggunaan PKI bagi Sistem ICT Kerajaan
   iv. Jadual Pelaksanaan

3. Pasukan Projek GPKI akan memproses permohonan dan diangkat ke Mesyuarat Jawatankuasa Teknikal Projek GPKI untuk pertimbangan serta Mesyuarat Jawatankuasa Pemandu Projek GPKI untuk kelulusan.

4. MAMPU akan mengeluarkan surat kelulusan pelaksanaan selepas kelulusan Mesyuarat Jawatankuasa Pemandu Projek GPKI diperoleh.

5 | KHIDMAT NASIHAT DAN KONSULTASI BAGI PENGGUNAAN PKI

JADUAL PELAKSANAAN

BIL.	AKTIVITI	TINDAKAN	TEMPOH (MINGGU)	CARTA PERBATUAN (MINGGU)																				TARIKH MULA	TARIKH SIAP
				BULAN 1				BULAN 2				BULAN 3				BULAN 4				BULAN 5				BULAN 6					
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24		
1	**Pengumpulan Maklumat Integrasi** i. Taklimat GPKI dan keperluan integrasi ii.Taklimat Sistem ICT dan keperluan sistem	MAMPU / AGENSI	1																										
2	**Penilaian Risiko**	AGENSI	2																										
3	**Permohonan dan kelulusan pelaksanaan integrasi**	MAMPU / AGENSI	4																										
4	**Pelaksanaan Integrasi** i.Perbincangan Teknkal ii.Serahan API GPKI iii.Serahan medium pengujian iv.Integrasi API GPKI dengan Sistem ICT	MAMPU / AGENSI	12																										
5	**Pengujian SIT**	MAMPU / AGENSI	1																										
6	**Pengujian UAT**	MAMPU / AGENSI	2																										
7	**Pengujian FAT**	MAMPU / AGENSI	1																										
8	**Latihan Pentadbir Portal GPKI**	MAMPU / AGENSI	1																										
9	**Sign Off**	MAMPU / AGENSI	1																										

TERIMA KASIH