



TAKLIMAT PENGURUSAN PERMOHONAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN (SSL) BAGI PENTADBIR-PENTABDIR DI AGENSI

BAHAGIAN PEMBANGUNAN PERKHIDMATAN GUNASAMA
INFRASTRUKTUR DAN KESELAMATAN ICT (BPG)
MAMPU, JPM



KANDUNGAN

BIL	ISI KANDUNGAN
1.	TAKRIFAN DAN EVOLUSI SIJIL DIGITAL PELAYAN
2.	DASAR DAN PRINSIP PEGANGAN SIJIL DIGITAL
3.	KEPUTUSAN TAMBAHAN BERKAITAN DASAR
4.	KEPERLUAN PERUNDANGAN
5.	ALIRAN PROSES KERJA PENGELUARAN SIJIL DIGITAL PELAYAN
6.	PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN
7.	SENARAI SEMAK PERMOHONAN SIJIL DIGITAL PELAYAN
8.	LAPORAN PENILAIAN RISIKO LAMAN WEB AGENSI
9.	PENENTUAN KATEGORI DAN JENIS SIJIL DIGITAL PELAYAN
10.	KATEGORI SIJIL DIGITAL PELAYAN
11.	JENIS SIJIL DIGITAL PELAYAN

KANDUNGAN

BIL	ISI KANDUNGAN
11.	CA DAN PRINSIPAL
12.	PENJANAAN CSR MENGIKUT PLATFORM & WEBSERVICE
13.	PENDAFTARAN PEGAWAI PENTADBIR PELAYAN DI PORTAL GPKI
14.	KRITERIA DAN PRA SYARAT PERMOHONAN SIJIL DIGITAL PELAYAN
15.	SYARAT KELULUSAN SIJIL DIGITAL PELAYAN
16.	PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN
17.	CONTOH PAPARAN DI PELAYAR BAGI SIJIL DIGITAL PELAYAN
18.	SEMAKAN KONFIGURASI PEMASANGAN SIJIL

TAKRIFAN SIJIL DIGITAL PELAYAN



Sumber: PKPA Bil. 3/2016 – Dasar GPKI :

PERKARA 5(i):

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

PERKARA 5(vi):

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

PERKARA 5(vii):

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

TAKRIFAN SIJIL DIGITAL PELAYAN



Sumber: PKPA Bil. 3/2016 – Dasar GPKI :

PERKARA 5(xv):

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

TAKRIFAN SIJIL DIGITAL PELAYAN



Sumber: PKPA Bil. 3/2016 – Dasar GPKI :

PERKARA 5(xviii):

- ❑ **Protokol Lapisan Soket Selamat (SSL)** digunakan untuk **menyulitkan maklumat** yang dihantar melalui internet. Sijil digital pelayan SSL membolehkan pelayan web mewujudkan sesi SSL dengan pelayar web. Terdapat beberapa produk sijil SSL seperti yang berikut:
 - (a) Sijil digital pelayan tunggal sebagaimana yang ditawarkan sekarang;
 - (b) Sijil digital kad bebas (*wild card*);
 - (c) Sijil digital pengesahsahihan yang diperluas (*extended validation certificate*);
 - (d) Sijil digital komunikasi dipersatukan (*unified communications certificate*); dan
 - (e) Sijil digital pengesahsahihan yang diperluas bagi pelbagai domain (*extended validation multi-domain certificate*).

TAKRIFAN SIJIL DIGITAL PELAYAN

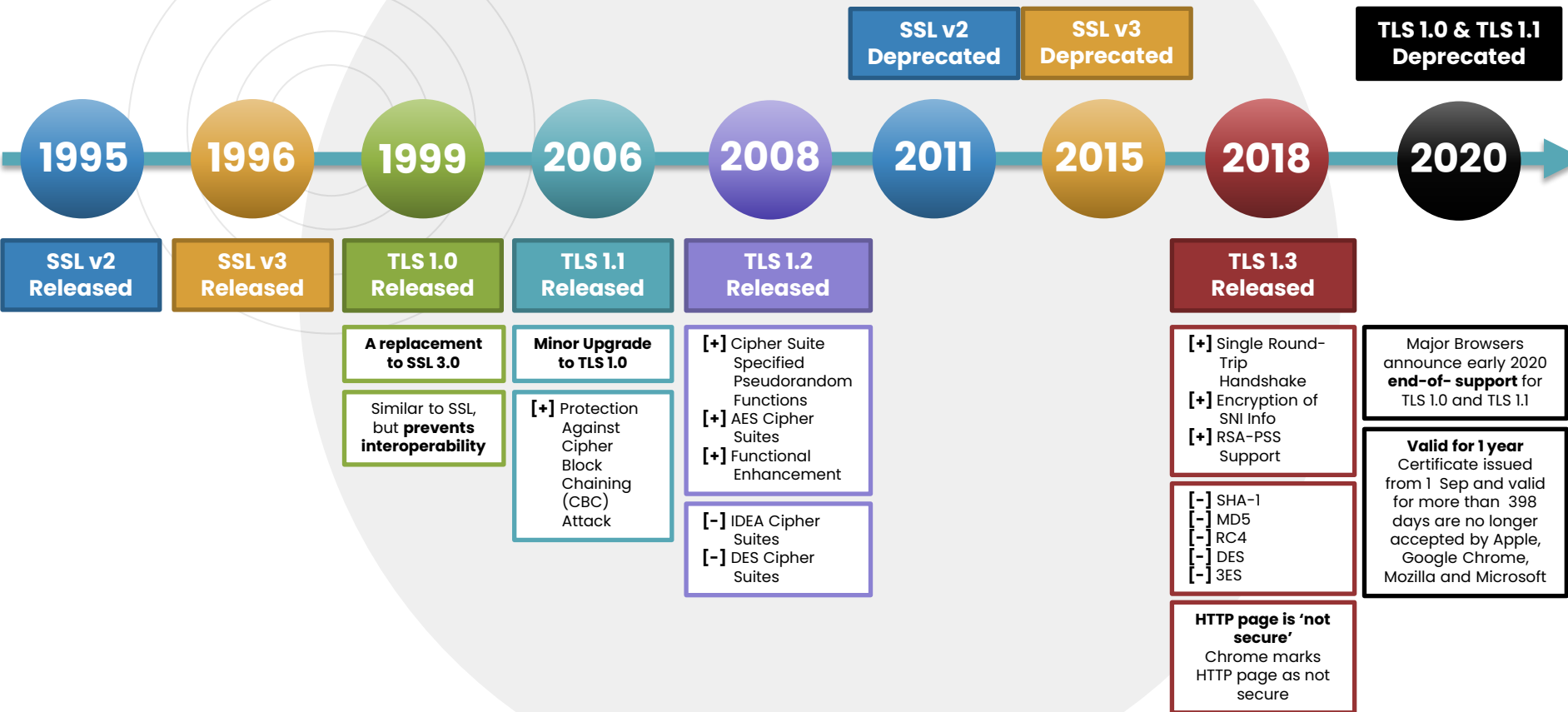


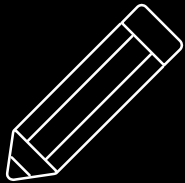
Sumber Dewan Bahasa dan Pustaka (PRPM):

Sijil Digital Pelayan dikenali dengan nama **Protokol Lapisan Soket Selamat (SSL)** yang juga sinonim dengan **Keselamatan Lapisan Pengangkutan [Transport Layer Security - TLS]**. **TLS adalah merupakan versi SSL yang telah dinaik taraf. Versi terkini TLS adalah versi 1.3.**

Definisi: Protokol keselamatan yang **membenarkan komunikasi antara pelayan** dengan **aplikasi pelanggan** seperti pelayar web. SSL/TLS bertindak sebagai **antara muka antara aplikasi dengan protokol TCP/IP** bagi menyediakan penyahihan pelayan dan pelanggan serta saluran komunikasi yang disulitkan antara pelayan dan pelanggan. Pelanggan dan pelayan bersetuju untuk menggunakan sekumpulan **penyulitan untuk sesi penyulitan dan pencincangan**. Contohnya, algoritma penyulitan yang digunakan ialah DES, SHA-J atau RC4 dengan kekunci 128 bit dan MD5.

EVOLUSI SIJIL DIGITAL PELAYAN





DASAR DAN PRINSIP PEGANGAN SIJIL DIGITAL



PERNYATAAN DASAR

(Pekeliling Kemajuan Pentadbiran Awam Bil.
3/2015)

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



PRINSIP PEGANGAN PELAKSANAAN GPKI

(Pekeliling Kemajuan Pentadbiran Awam Bil. 3/2015)

SIJIL DIGITAL PELAYAN

Semua pengguna GPKI hendaklah mematuhi Prinsip Pegangan berikut:



- 1 Sistem ICT kerajaan yang menggunakan perkhidmatan PKI selain Prasarana Kunci Awam (GPKI) **mestilah beralih** kepada Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) apabila **sistem berkenaan hendak dinaik taraf** atau **tempoh kontrak sistem berkenaan telah tamat**
- 2 Agensi sektor awam perlu **mengambil kira keperluan** sijil digital pelayan dalam **spesifikasi sistem baharu**
- 3 Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) **hanya akan membekalkan** sijil digital pelayan untuk **tujuan pembaharuan sijil digital pelayan sedia ada yang akan tamat tempoh**. Kos sijil digital pelayan dalam sistem baharu adalah di bawah **tanggungjawab agensi** berkenaan dengan menggunakan sijil yang dikeluarkan oleh **Pihak Berkuasa Pemerakuan Berlesen (CA)** yang **dilantik** oleh kerajaan menerusi **Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM)**

Nota Keterangan:

Baharu bermaksud Sistem ICT kerajaan **baharu** yang dibangunkan secara **outsource** perlu mengambil kira kos pemasangan SSL dalam kontrak baharu masing-masing. Walau bagaimanapun sekiranya agensi **tidak mempunyai sumber kewangan yang mencukupi** maka kos pemasangan SSL akan ditanggung oleh Agensi Pusat. Bagi Sistem ICT Kerajaan yang dibangunkan secara **inhouse** akan ditanggung oleh Agensi Pusat.

Semua pengguna GPKI hendaklah mematuhi Prinsip Pegangan berikut:



- 4 Agensi Pusat **akan menanggung semua kos** bagi perkhidmatan GPKI untuk **kementerian dan jabatan persekutuan sahaja** yang bertindak sebagai agensi pelaksana
- 5 **Badan Berkanun Persekutuan, agensi negeri, Badan Berkanun Negeri dan Pihak Berkuasa Tempatan** yang berhasrat jadi agensi pelaksana, semua kos perkhidmatan GPKI adalah di bawah tanggungannya agensi berkenaan
- 6 Agensi pelaksana yang **berubah taraf** daripada agensi persekutuan **kepada agensi swasta** atau **badan berkanun**, semua kos perkhidmatan GPKI adalah di bawah tanggungannya agensi berkenaan

KEPUTUSAN TAMBAHAN BERKAITAN DASAR

Bil.	Isu Sijil Digital Pelayan SSL	Keterangan	Keputusan JKP
1.	<p>Prinsip Pegangan 3</p> <p>Tiada kriteria kelulusan permohonan sijil digital pelayan SSL</p> <p>1. Terdapat permohonan sijil digital pelayan SSL yang dikemukakan oleh agensi bagi pelbagai jenis pelayan termasuk <u>pelayan latihan</u> dan <u>pelayan pembangunan</u></p> <p>2. Prinsip pegangan Dasar GPKI menyatakan pembekalan sijil digital SSL hanya bagi tujuan <u>pembaharuan</u>. Kos sijil digital pelayan dalam sistem baharu adalah di bawah tanggungan agensi. Namun, terdapat permohonan pembekalan sijil digital pelayan bagi sistem baharu</p>	<p>1. Pembekalan sijil digital pelayan SSL kepada Sistem ICT Kerajaan merupakan satu daripada skop perkhidmatan GPKI dan penggunaan sijil digital pelayan SSL ini adalah bertujuan:</p> <ul style="list-style-type: none"> • sebagai pengesahan identiti organisasi kepada pengguna • penyulitan maklumat yang dihantar melalui Internet <p>2. Tiada kriteria kelulusan sijil digital pelayan SSL yang dinyatakan di dalam Dasar Perkhidmatan GPKI terutama bagi kelulusan permohonan sijil digital SSL untuk kegunaan pelayan selain pelayan produksi dan pelayan bagi sistem baharu</p> <p>3. Oleh itu, Pasukan Projek menghadapi kesukaran bagi meluluskan permohonan sijil digital SSL yang dikemukakan oleh agensi</p>	<p>1. Agensi hendaklah menggunakan sijil digital pelayan SSL sumber terbuka (open source) bagi kegunaan pelayan, selain pelayan produksi</p> <p>2. Cadangan kriteria kelulusan permohonan sijil digital pelayan SSL seperti berikut:</p> <ol style="list-style-type: none"> Pelayan Sistem ICT memerlukan tahap kawalan keselamatan yang tinggi Capaian sistem hendaklah melalui Internet Semua maklumat pelayan perlulah didaftarkan dengan pendaftar domain Memerlukan Janaan Permintaan Tandatangan Sijil - CSR (certificate signing request) oleh agensi pemilik nama domain Pelayan bagi sistem baharu yang dibangunkan secara dalaman (<i>inhouse</i>) Telah mendapat kelulusan JPICT/ JTISA bagi pelayan bagi sistem baharu <p>Kriteria (i-iv) adalah mandatori manakala kriteria (v-vi) adalah terpakai bagi pelayan sistem baharu sahaja</p>

KEPERLUAN PERUNDANGAN

Pekeliling Kemajuan Pentadbiran Awam Bil. 3/2015: Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan
[Government Public Key Infrastructure (GPKI)]



BIL.	KATEGORI AGENSI	TANGGUNGAN KOS SIJIL DIGITAL PELAYAN	
1.	Kementerian	✔ Ditanggung	
2.	Jabatan	a. Agensi Pentadbiran Persekutuan	✔ Ditanggung
		b. Agensi Pentadbiran Negeri	✘ Tidak Ditanggung
3.	Badan Berkanun	a. Badan Berkanun Persekutuan Tidak Diasingkan Saraan	✔ Ditanggung sekiranya menggunakan Sistem ICT kerajaan Jabatan Persekutuan
		b. Badan Berkanun Persekutuan Diasingkan Saraan	✘ Tidak Ditanggung
		c. Badan Berkanun Negeri	✘ Tidak Ditanggung
4.	Pihak Berkuasa Tempatan / Penguasa Tempatan	a. Pihak Berkuasa Tempatan / Penguasa Tempatan Persekutuan	✘ Tidak Ditanggung
		b. Pihak Berkuasa Tempatan / Penguasa Tempatan Negeri	✘ Tidak Ditanggung
5.	Swasta	✘ Tidak Ditanggung	

ALIRAN PROSES KERJA PERMOHONAN SIJIL DIGITAL PELAYAN

01 Pegawai di Agensi menyediakan/kemas kini **Laporan Penilaian Risiko** setiap subdomain

- Pilih: Pendaftaran Pengguna / **Permohonan Baharu**
- Pilih: **Kategori** (*Single Domain/ Multi Domain/ Wildcard*)
- Isi maklumat pelayan
- Muat naik **CSR** (panjang kunci perlu **2048 bit** dan jenis kunci **RSA SHA2 serta** telah didaftar di portal MYNIC)
- Muat naik "**Surat Permohonan Sijil Digital Pelayan**"

02 Pegawai di Agensi membuat Permohonan Sijil Digital Pelayan di Portal GPKI

03 Kelulusan oleh Pentadbir (Admin)

04 Proses **pengesahan (eVetting)** sijil digital oleh Prinsipal dan CA kepada Agensi

Diproses penjanaan dalam **7 hari bekerja** dari tarikh dokumen lengkap

- Sijil MESTI dipasang dalam **tempoh 14 hari** selepas tarikh terimaan sijil daripada CA
- Agensi perlu mengemaskini **tarikh penerimaan dan tarikh pemasangan**
**** Sekiranya didapati pemasangan tidak dibuat dalam tempoh 14 hari, kos permohonan semula dan kos pembaharuan bagi domain berkenaan akan ditanggung sepenuhnya oleh agensi**

e-Vetting = pengesahan domain (e-mel kepada admin berdaftar di MYNIC) dan pengesahan organisasi (e-mel dan panggilan ke telefon pejabat).
eVetting lengkap = dokumen lengkap

05 Penjanaan sijil digital oleh Prinsipal

06 E-mel sijil digital kepada pemohon oleh Prinsipal

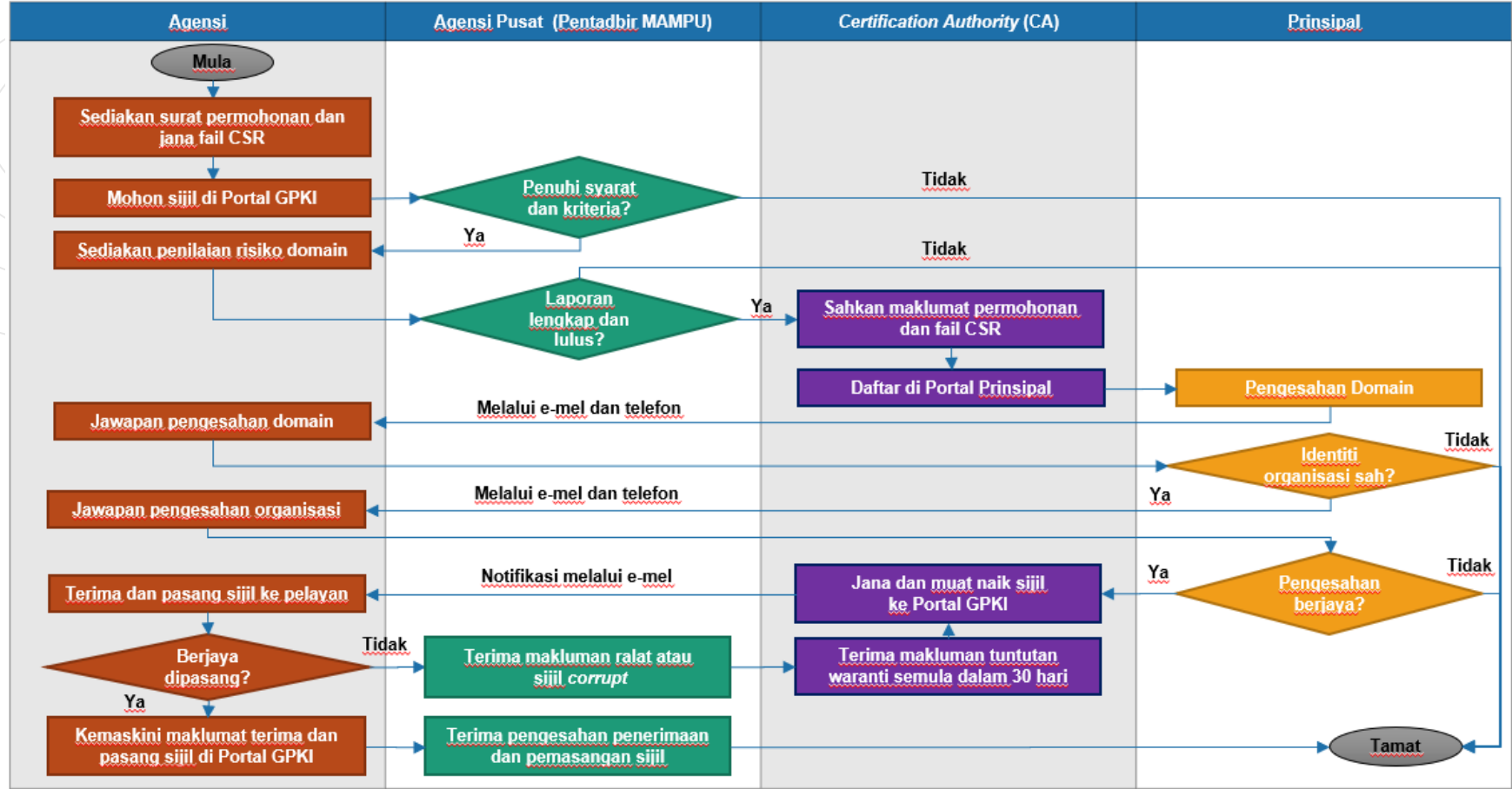
07 CA kemas kini maklumat penghantaran sijil digital

E-mel makluman kepada pemohon dan CA, bahawa sijil digital telah dihantar kepada pemohon

08 Pemohon kemas kini maklumat penerimaan di Portal GPKI

09 Pemohon membuat pemasangan sijil digital dan kemaskini tarikh dan taraf pemasangan di Portal GPKI

ALIRAN PROSES KERJA LENGKAP PERMOHONAN SIJIL DIGITAL PELAYAN



PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



- ❑ **Tempoh sah laku sijil digital pelayan** yang dibekalkan oleh MAMPU kepada agensi ialah **12 bulan** tertakluk pada polisi Pihak Berkuasa Pemerakuan Berlesen (CA) yang berkenaan.
- ❑ Pegawai-pegawai yang telah didaftarkan sebagai pentadbir SSL akan menerima notifikasi pembaharuan sijil digital pelayan pada **30 hari sebelum tamat tempoh sijil** dan **pada hari tamat tempoh sijil tersebut**.
- ❑ Agensi boleh membuat pembaharuan sijil digital pelayan **seawal 30 hari** sebelum **tamat tempoh sijil** tersebut melalui Portal GPKI.

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



SENARAI SEMAK PERMOHONAN SIJIL DIGITAL PELAYAN :

- ✓ **Penyediaan laporan penilaian risiko** laman web agensi;
- Penjanaan fail *Certificate Signing Request* (CSR)** di pelayan;
- Pendaftaran pegawai pentadbir pelayan** di Portal GPKI;
- Permohonan baharu atau pembaharuan sijil digital pelayan** di Portal GPKI
- Kelulusan pengesahan organisasi dan domain oleh prinsipal** (eVetting)
- Penjanaan sijil digital pelayan** oleh CA
- Penerimaan dan pemasangan** sijil digital pelayan oleh agensi
- Semakan konfigurasi** dan kemaskini **tarikh dan taraf pemasangan** sijil digital pelayan di Portal GPKI
- Pembatalan sijil digital pelayan** (jika berkaitan sahaja)

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

LAPORAN PENILAIAN RISIKO LAMAN WEB AGENSI

Contoh templat laporan penilaian risiko laman web agensi adalah seperti pautan menu di bawah:

- Portal GPKI <https://gпки.mampu.gov.my> >
- Muat Turun >
- Dokumen GPKI >
- Permohonan Perkhidmatan GPKI >
- Perkara 10: Sijil Digital Pelayan – Templat Penilaian Risiko Laman Web Sektor Awam Dalam Konteks Perkhidmatan GPKI)

Bil.	Nama Domain	Data / Maklumat Terlibat	Klasifikasi Data / Maklumat	Nilai Data	Kawalan Sedia Ada	Ancaman Keselamatan	Keterangan Ancaman
<p>3. PENILAIAN RISIKO</p> <p>Penilaian Risiko ini bertujuan untuk:</p> <ol style="list-style-type: none"> Mengenal pasti kawalan keselamatan yang sesuai bagi keperluan perkhidmatan GPKI Menentukan penggunaan sijil digital pelayan sama ada bagi tujuan pengesahan identiti dan penyulitan maklumat Mengenal pasti keperluan kategori dan jenis sijil digital pelayan yang diperlukan oleh agensi berdasarkan tahap risiko 							
1	www.mampu.gov.my	Portal MAMPU yang mengandungi maklumat umum aktiviti organisasi dan garis panduan yang perlu dicapai oleh semua agensi kerajaan.	Terbuka	Sederhana	Pemasangan sijil digital pelayan Wildcard OV	HTTPS Spoofing	a) Penggodam mewujudkan laman web palsu yang menyerupai laman web asal bagi tujuan memindahkan komunikasi kepada pelayan penggodam bagi tujuan pemintasan data atau maklumat yang sedang berinteraksi.
2	dts.mampu.gov.my	Mengandungi rekod tandatangan masa dan maklumat pengguna. Sistem DTS memainkan peranan dalam memastikan sesuatu transaksi atau maklumat adalah SAHH wujud pada masa yang dinyatakan.	Sulit	Tinggi	Pemasangan sijil digital pelayan single domain EV dan penggusa login ID dan kata laluan	HTTPS Spoofing SSL hijacking Penyamaran Identiti (Identity Spoofing) Pembaharuan Data (Data Tampering)	a) Penggodam mewujudkan laman web palsu yang menyerupai laman web asal bagi tujuan memindahkan komunikasi kepada pelayan penggodam bagi tujuan pemintasan data atau maklumat yang sedang berinteraksi. b) Ancaman di mana penggodam menukar komunikasi antara dua pihak yang sedang berkomunikasi dengan pelayan penggodam. c) Satu tindakan ancaman yang bertujuan untuk mengakses sistem secara tidak sah dan menggunakan kelayakan pengguna lain seperti ID pengguna dan kata laluan. d) Satu tindakan ancaman berniat jahat yang bertujuan untuk menukar/mengubahsuai data seperti pembaharuan data dalam pangkalan data dan mengubah data dalam transit antara dua komputer.
3	latihan.dts.gov.my	Mengandungi maklumat pengguna dan rekod tandatangan masa bukan yang sebenar (dummy data) yang digunakan untuk membolehkan latihan kepada pengguna berkaitan aliran proses kerja sistem DTS.	Terbuka	Rendah	Tiada	HTTPS Spoofing	Penggodam mewujudkan laman web palsu yang menyerupai laman web asal bagi tujuan memindahkan komunikasi kepada pelayan penggodam bagi tujuan pemintasan data atau maklumat yang sedang berinteraksi.
4	dev.dts.gov.my	Mengandungi maklumat pengguna dan rekod tandatangan masa pengujian (dummy data) yang digunakan untuk memastikan proses transaksi berjaya dilaksanakan.	Terhad	Sederhana	Self Signed Certificate	HTTPS Spoofing Pembaharuan Data (Data Tampering)	a) Penggodam mewujudkan laman web palsu yang menyerupai laman web asal bagi tujuan memindahkan komunikasi kepada pelayan penggodam bagi tujuan pemintasan data atau maklumat yang sedang berinteraksi. b) Satu tindakan ancaman berniat jahat yang bertujuan untuk

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN















KRITERIA DAN PRA SYARAT PERMOHONAN SIJIL DIGITAL PELAYAN

- 1 Pelayan Sistem ICT memerlukan **tahap kawalan keselamatan yang tinggi** kerana sistem mengandungi **maklumat rahsia rasmi**. Hanya pelayan produksi sahaja akan ditanggung oleh Agensi Pusat tidak termasuk pelayan pembangunan (*staging* atau *development*), latihan (*training with dummy data*) dan pengujian (*testing*)
- 2 Capaian sistem hendaklah melalui **Internet (Public) sahaja** tidak termasuk Intranet
- 3 Semua **maklumat domain pelayan** (contoh: gpkimampu.gov.my) **telah wujud** dan **telah didaftarkan** dengan pendaftar domain (MYNIC)
- 4 Perlu sediakan janaan **Permintaan Tandatangan Sijil - CSR** (*Certificate Signing Request*) oleh agensi
- 5 Sebarang **perubahan ke atas nama domain** dan **jenis sijil digital pelayan** adalah **tidak dibenarkan** setelah permohonan diluluskan
- 6 Permohonan pembaharuan **hanya akan mula diproses seawal 30 hari** sebelum tamat tempoh sijil digital sedia ada.

Rujukan:

Portal GPKI > Muat Turun > Dokumen GPKI > Permohonan Perkhidmatan GPKI > Perkara 8: Prasyarat dan Kriteria Sijil Digital Pelayan

PENENTUAN JENIS SIJIL DIGITAL PELAYAN

KEPERLUAN TAHAP KAWALAN KESELAMATAN SISTEM ICT KERAJAAN	JENIS SIJIL DIGITAL PELAYAN YANG DIPERLUKAN		
	SINGLE DOMAIN EV	MULTI DOMAIN OV	WILDCARD
TINGGI (Klasifikasi Data : Rahsia Rasmi Risiko: Tinggi, Sederhana dan Rendah)			
SEDERHANA (Klasifikasi Data : Data Terkawal/ Sensitif Risiko: Tinggi dan Sederhana)			
SEDERHANA (Klasifikasi Data : Data Terkawal/ Sensitif Risiko: Rendah)			
RENDAH (Klasifikasi Data : Data Terbuka Risiko: Tinggi, Sederhana dan Rendah)			

 **DIPERLUKAN**

 **TIDAK DIPERLUKAN**

KATEGORI SIJIL DIGITAL PELAYAN

Nota:

- ✓ Ditanggung oleh MAMPU berdasarkan kriteria dan syarat ditetapkan
- ✗ Tidak ditanggung oleh MAMPU. Agensi perlu melaksanakan perolehan sendiri daripada CA

✓ **EV**

Extended Validation

LINGKAP

1. Menyediakan keselamatan *session* dan privasi
2. Maklumat organisasi dipapar secara automatik di alamat pelayar dengan perbezaan warna yang kontra

INTERNET

✓ **OV**

Organization Validation

PERTENGAHAN

1. Menyediakan keselamatan *session* dan privasi
2. Maklumat organisasi hanya dipaparkan apabila diperiksa oleh pelawat

✗ **DV**

Domain Validated

ASAS

1. Menyediakan keselamatan *session* dan privasi
2. Tidak memaparkan jenama/ organisasi
3. Open source / free ssl/tls

✗ **Private Trust**

PERSENDIRIAN

1. URL dan Top Level Domain (TLD) tidak didaftarkan
2. IP local 127.0.0.1

INTRANET

JENIS SIJIL DIGITAL PELAYAN

**Sijil Digital Pelayan
Single Domain EV dan OV**

01

RM2,850.00 seunit

Sijil Digital Pelayan yang didaftarkan hanya ke atas **satu domain**

**Sijil Digital Pelayan
Multi Domain OV**

02

RM2,850.00 seunit

Sijil Digital Pelayan yang mengandungi sekurang-kurangnya **dua domain**

**Sijil Digital Pelayan
Wildcard OV**

03

RM5,600.00 seunit

Sijil Digital Pelayan yang mengandungi **pelbagai sub-domain di bawah satu domain yang sama** dan menggunakan **simbol *** (*Wildcard*) dalam satu sijil

01 SIJIL DIGITAL PELAYAN SINGLE DOMAIN

KETERANGAN

01

Didaftarkan hanya ke atas 1 domain atau 1 subdomain sahaja

Mempunyai ciri keselamatan tambahan melalui pengesahan terperinci (*Extended Validation, EV*)

02

03

Kunci peribadi (*private key*) pelayan dijana khusus bagi domain yang didaftarkan sahaja

Sekiranya kunci peribadi (*private key*) pelayan terdedah/terjejas (*compromised*), implikasi keselamatan hanya melibatkan domain tersebut sahaja

04

KRITERIA PEMILIHAN

- ◆ Aplikasi kritikal yang berisiko tinggi dan mempunyai maklumat rahsia rasmi.
- ◆ Contoh aplikasi: transaksi pembayaran dalam talian

Contoh 1:

- gpi.mampu.gov.my

Contoh 2:

- www.mampu.gov.my

KETERANGAN

01

merupakan Sijil Digital Pelayan yang mengandungi kombinasi 2-4 domain atau subdomain yang sama atau berlainan

Kunci peribadi (*private key*) pelayan adalah sama dan dikongsi oleh dua atau lebih domain yang didaftarkan

02**03**

Sekiranya kunci peribadi (*private key*) pelayan terdedah atau terjejas (*compromised*), implikasi keselamatan adalah kepada semua domain

KRITERIA PEMILIHAN

- ◆ Aplikasi yang **berisiko tinggi atau sederhana**; atau
- ◆ Aplikasi yang **beroperasi menggunakan platform Microsoft**

Contoh 1:

- gpci.mampu.gov.my
- gpci.bpg.gov.my
- dts.mampu.gov.my

Contoh 2:

- www.mampu.gov.my
- www.mampu.org.my
- itims.mampu.gov.my

KETERANGAN

01

mengandungi pelbagai sub-domain di bawah satu domain yang sama dan menggunakan simbol * (Wildcard) dalam satu sijil

Kunci peribadi (private key) pelayan bagi domain akan dikongsi bagi semua aplikasi yang didaftarkan di bawah domain yang sama

02

Sekiranya kunci peribadi (private key) pelayan terdedah atau terjejas (compromised), implikasi keselamatan adalah kepada semua sub-domain (kunci yang sama)

03*** Nota:**

Walaupun wildcard mempunyai kelebihan tiada had bilangan subdomain dan boleh menjangkau sehingga melebihi 150 subdomain namun ia hanya meliputi subdomain pada 1 aras hirarki yang sama sahaja dan tidak boleh digunakan bersama dengan jenis multi domain dan single domain atas faktor keselamatan.

KRITERIA PEMILIHAN



Aplikasi yang berisiko sederhana dan mempunyai maklumat rahsia rasmi.

Contoh 1:

- *.mampu.gov.my
- gпки.mampu.gov.my
- dts.mampu.gov.my
- itims.mampu.gov.my

Contoh 2:

- *.anm.gov.my
- gпки.anm.gov.my
- dts.anm.gov.my
- itims.anm.gov.my

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



SENARAI SEMAK PERMOHONAN SIJIL DIGITAL PELAYAN :

- ✓ Penyediaan laporan penilaian risiko laman web agensi;
- ✓ Penjanaan fail *Certificate Signing Request (CSR)* di pelayan;
- Pendaftaran pegawai pentadbir pelayan di Portal GPKI;
- Permohonan baharu atau pembaharuan sijil digital pelayan di Portal GPKI
- Kelulusan pengesahan organisasi dan domain oleh prinsipal (eVetting)
- Penjanaan sijil digital pelayan oleh CA
- Penerimaan dan pemasangan sijil digital pelayan oleh agensi
- Semakan konfigurasi dan kemaskini tarikh dan taraf pemasangan sijil digital pelayan di Portal GPKI
- Pembatalan sijil digital pelayan (jika berkaitan sahaja)

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

PENJANAAN FAIL CERTIFICATE SIGNING REQUEST (CSR)

Nota:

Fail CSR yang akan dijana **MESTI** sama dengan maklumat domain yang **TELAH** didaftarkan dengan pendaftar domain (portal MYNIC). **Saiz fail** hendaklah kurang daripada **2MB**. Fail CSR mestilah mempunyai jenis kunci **RSA SHA2** dan panjang kunci **2048 bit ke atas**. Diingatkan supaya agensi **HENDAKLAH** menjana semula CSR yang baharu dan **dilarang menggunakan CSR dan private key yang sama dengan permohonan terdahulu**.

Peringatan:

- ❖ Sebelum penjana fail CSR dilaksanakan, Pentadbir Pelayan perlu mengenal pasti terlebih dahulu **lokasi pemasangan** sijil digital pelayan yang akan dibuat sama ada di **WAF, IDP, IPS, Proxy, Firewall, Load Balancer atau Web Service bergantung kepada infrastruktur rangkaian di agensi masing-masing**.
- ❖ Pentadbir Pelayan juga perlu mengenal pasti terlebih dahulu **configuration setting untuk ssl/tls** di pelayan (terutamanya pelayan sedia ada) yang perlu dipasang dengan sijil digital pelayan kerana setiap pelayan adalah **berbeza cara dan format fail** yang diperlukan bergantung kepada jenis platform dan web service masing-masing.

Kaedah semakan kandungan CSR

The screenshot shows the Entrust CSR Viewer interface. At the top, there's a browser address bar with 'confirm.entrust.net/public/en'. Below it, the page title is 'ENTRUST CSR Viewer'. A text box contains a long base64-encoded CSR string. Below the text box, there's a 'Success! Look below for details.' message. The main content area is titled 'CSR Contents' and includes a 'CSR Checks' section with the following items:

- Signature: ✓ Signature is valid.
- Debian Weak Key: ✓ No Debian weak key detected.
- ROCA Vulnerable Key: ✓ No ROCA vulnerable key detected.
- RSA Public Key Quality: ✓ RSA public key checks passed.

The 'Subject' section shows the following details:

- Email: webmaster@mampu.gov.my
- Common Name: www.mampu.gov.my
- Organizational Unit: Bahagian Pembangunan Aplikasi
- Organization: Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
- Locality: Putrajaya
- State: Wilayah Persekutuan
- Country: MY
- Subject Alternative Names: aplikasi.mampu.gov.my (dNSName), dasar.mampu.gov.my (dNSName), myevent.mampu.gov.my (dNSName)

The 'Properties' section shows the following details:

- Key Type: RSA
- Key Size: 2048
- Signature Type: sha256WithRSAEncryption
- Fingerprint (MD5): [REDACTED]
- Fingerprint (SHA-1): [REDACTED]

Annotations in red text and arrows point to specific parts of the interface:

- An arrow points to the browser address bar with the text: 'URL untuk semakan kandungan fail CSR yang telah dijana'.
- An arrow points to the CSR string text box with the text: 'Buka fail *.csr menggunakan notepad atau text editor. Copy dan paste code base 64 ke ruangan ini'.
- An arrow points to the 'Common Name' field with the text: 'Common Nama (CN) adalah nama domain/subdomain yang perlu dipasang dengan sijil digital pelayan. Limit 64 character termasuk notkth'.
- An arrow points to the 'Country' field with the text: 'Subject Alternative Names atau dikenali sebagai SANs hanya akan dipaparkan bagi sijil jenis multidomain sahaja. Paparan ini adalah berkaitan dengan fail *.cnf semasa penjanaan csr'.
- An arrow points to the 'International code untuk Malaysia (2 character sahaja)' text next to the 'Country' field.
- An arrow points to the 'Key Type' field with the text: 'Nama organization (O) dan organization unit (OU) perlu menggunakan nama penuh agensi (bukan akronim) kerana akan dipaparkan di browser client dan mewakili imej Kerajaan Malaysia. Limit 64 character sahaja. Tidak digalakkan sebarang special character seperti &() bagi mengelakkan ralat di portal prinsipal'.
- An arrow points to the 'Key Size' field with the text: 'perlu RSA sahaja'.
- An arrow points to the 'Signature Type' field with the text: 'perlu 2048 sahaja'.
- An arrow points to the 'Signature Type' field with the text: 'perlu sha2 sahaja'.

At the bottom of the screenshot, there's a red star icon and the text: 'Nota: Kesemua ruangan adalah mandatori (wajib) dilengkapkan dengan betul kecuali e-mel sahaja'.

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

PENJANAAN CSR MENGIKUT CRYPTO LIBRARY TOOL & WEB SERVICE

Bil.	<i>Crypto Library Tool</i>	<i>Web Service</i>	Jenis Sijil Digital Pelayan	Fail yang perlu dijana
1.	OpenSSL	<ul style="list-style-type: none">• Apache HTTP Server• NGINX	<ul style="list-style-type: none">• <i>Single Domain</i>• <i>Multi Domain</i>• <i>Wildcard</i>	<ul style="list-style-type: none">• Fail Private Key: *.key / *.pem• Fail CSR
2.	JSSE (Keytool)	<ul style="list-style-type: none">• Apache Tomcat• JBoss (Wildfly)• Weblogic	<ul style="list-style-type: none">• <i>Single Domain</i>• <i>Multi Domain</i>• <i>Wildcard</i>	<ul style="list-style-type: none">• Fail Private Key: *.ks / *.jks (keystore)• Fail CSR
3.	IBM Java SDK (iKeyMan)	<ul style="list-style-type: none">• IBM HTTP Server• Websphere	<ul style="list-style-type: none">• <i>Single Domain</i>• <i>Wildcard</i>	<ul style="list-style-type: none">• Fail Private Key: *.kdb• Fail CSR
4.	Mozilla NSS (certutil)	<ul style="list-style-type: none">• Sun Java Web Server	<ul style="list-style-type: none">• <i>Single Domain</i>• <i>Wildcard</i>	<ul style="list-style-type: none">• Fail CSR
5.	SChannel	<ul style="list-style-type: none">• Microsoft IIS• Microsoft Exchange	<ul style="list-style-type: none">• <i>Single Domain</i>• <i>Multi Domain</i>• <i>Wildcard</i>	<ul style="list-style-type: none">• Fail CSR

Rujukan: Keterangan lanjut kaedah penjanaaan CSR di slaid bertajuk PENJANAAN CSR DAN KONFIGURASI PELAYAN

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



PENJANAAN FAIL CERTIFICATE SIGNING REQUEST (CSR)

Tatacara penjaan CSR bagi pelayan adalah seperti pautan menu di bawah:

Portal GPKI (<https://gпки.mampu.gov.my>) >
Muat Turun > Dokumen GPKI > Permohonan Perkhidmatan GPKI > Perkara 11: Sijil Digital Pelayan – Tatacara Penjaan CSR bagi Pelayan

Peringatan:

Fail private key *.key / *.ks / *.pem / *.jks / keystore / *.kdb perlu disimpan dengan selamat untuk pemasangan. Sekiranya fail tersebut hilang maka sijil yang diterima tidak dapat dipasang dan perlu penjaan semula sijil dari pihak CA.



TATACARA PENJANAAN FAIL CSR BAGI PELAYAN

Panduan menjana fail csr di pautan:

- <https://www.digicert.com.my/support> (tools penjaan csr serta perlu pilih mengikut *platform* dan *webservice*)
- <https://www.entrustdatacard.com/knowledgebase/ssl/ssl-tls-tools> (tools penjaan csr serta perlu *platform* mengikut *webservice*)
- <https://www.entrust.net/ssl-technical/csr-viewer.cfm> (semakan kandungan csr)

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



DO AND DON'T

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

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



SENARAI SEMAK PERMOHONAN SIJIL DIGITAL PELAYAN :

- ✓ Penyediaan laporan penilaian risiko laman web agensi;
- ✓ Penjanaan fail *Certificate Signing Request (CSR)* di pelayan;
- ✓ Pendaftaran pegawai pentadbir pelayan di Portal GPKI;
- Permohonan baharu atau pembaharuan sijil digital pelayan di Portal GPKI
- Kelulusan pengesahan organisasi dan domain oleh prinsipal (eVetting)
- Penjanaan sijil digital pelayan oleh CA
- Penerimaan dan pemasangan sijil digital pelayan oleh agensi
- Semakan konfigurasi dan kemaskini tarikh dan taraf pemasangan sijil digital pelayan di Portal GPKI
- Pembatalan sijil digital pelayan (jika berkaitan sahaja)

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

PORTAL GPKI



The screenshot shows the MyGPKI portal interface. The top navigation bar includes 'UTAMA', 'MAKLUMAT AM', 'PERKHIDMATAN', 'MUAT TURUN', 'SOALAN LAZIM', 'MEJA BANTUAN', and 'eLEARNING'. The 'PERKHIDMATAN' menu is expanded, showing a list of services. A red box highlights the 'PENGURUSAN SIJIL DIGITAL PELAYAN' section, which includes options like 'Pendaftaran Pengguna Sijil Digital Pelayan', 'Permohonan Sijil Digital Pelayan', 'Permohonan Pembatalan Sijil Digital Pelayan', 'Semak Status Sijil Digital Pelayan', 'Kemas Kini Janji Temu', 'Kemas kini penerimaan Sijil Digital Pelayan', 'Kemas Kini Tarikh dan Masa Pemasangan Sijil Digital Pelayan', 'Kemas Kini Profil Pegawai', 'Tukar Kata Laluan', 'Reset Kata Laluan', 'Panduan Penajaan CSR', 'Panduan Pemasangan Sijil Digital Pelayan', and 'Semakan Domain'. A red arrow points from a text box on the right to this highlighted section.

Kesemua 13 menu yang terdapat di bawah Menu **“Pengurusan Sijil Digital Pelayan”** di Portal GPKI 3.0 perlu digunakan oleh pegawai pentadbir pelayan di agensi bagi menguruskan permohonan masing-masing.

Manual Pengguna Permohonan Sijil Digital Pelayan bagi Sistem GPKI 3.0 boleh dimuat turun daripada pautan berikut:

Portal GPKI (<https://gпки.mampu.gov.my>) > Muat Turun > Dokumen GPKI > Panduan Pengguna > Perkara 6: Manual Pengguna Permohonan Sijil Digital Pelayan (SSL)

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

PENDAFTARAN PEGAWAI PENTADBIR PELAYAN DI PORTAL GPKI

Nota:

Pentadbir Pelayan adalah terdiri daripada 3 iaitu Pegawai Pemohon (PIC), Pegawai Teknikal dan Pegawai Pengesah serta hendaklah terdiri daripada **individu yang berbeza**. Ketiga-tiga pegawai ini akan menerima kata laluan masing-masing dan mempunyai capaian ke Portal GPKI.

➤ Pendaftaran Pentadbir Pelayan

Pendaftaran pentadbir pelayan hanya dibenarkan bagi permohonan sijil digital pelayan baharu untuk domain yang tidak pernah didaftarkan dalam Sistem GPKI.

➤ Pentadbir Pelayan Sedia Ada (Terlupa Kata Laluan)

Bagi pentadbir pelayan sedia ada atau pegawai yang pernah memohon sijil digital pelayan akan menerima e-mel notifikasi maklumat pendaftaran sebagai pengguna sijil digital pelayan berserta kata laluan sementara dari Sistem GPKI. Sekiranya, kata laluan tidak diterima atau terlupa kata laluan maka Pentadbir Pelayan boleh reset kata laluan masing-masing bagi mendapatkan kata laluan yang baharu di **Portal GPKI > Menu Perkhidmatan > Pengurusan Sijil Digital Pelayan > Reset Kata Laluan**. Kata laluan akan diterima melalui e-mel notifikasi Sistem GPKI dan Portal GPKI boleh dicapai dengan menggunakan kata laluan yang telah diberikan pada **Portal GPKI > Menu Perkhidmatan > Pengurusan Sijil Digital Pelayan > Permohonan Sijil Digital Pelayan**. Pentadbir pelayan perlu memastikan e-mel masing-masing masih sah dan sama seperti mana yang telah didaftarkan di dalam Sistem GPKI. Sekiranya e-mel tidak diterima atau e-mel bertukar, sila maklumkan kepada admingpki@mampu.gov.my sebelum reset kata laluan dilaksanakan.

➤ Pentadbir Pelayan Bertukar atau Berpindah Agensi

Sebarang perubahan dan pengemaskinian maklumat pentadbir pelayan yang bertukar atau berpindah agensi boleh dilaksanakan sendiri oleh salah seorang pentadbir pelayan yang lain di Menu Kemaskini Profil Pegawai (**Portal GPKI > Menu Perkhidmatan > Pengurusan Sijil Digital Pelayan > Kemaskini Profil Pegawai**). Sekiranya masih gagal, maka pentadbir perlu melengkapkan butiran berikut bagi tujuan pengemaskinian maklumat dan e-melkan kepada admingpki@mampu.gov.my. Pegawai pengganti akan menerima maklumat kata laluan yang baharu melalui e-mel notifikasi Sistem GPKI.

a. Nama Penuh
b. No. MyKad

c. Jawatan
d. E-mel

e. No. Telefon Pejabat
f. No. Telefon Bimbit

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



SENARAI SEMAK PERMOHONAN SIJIL DIGITAL PELAYAN :

- ✓ **Penyediaan laporan penilaian risiko** laman web agensi;
- ✓ **Penjanaan fail *Certificate Signing Request (CSR)*** di pelayan;
- ✓ **Pendaftaran pegawai pentadbir pelayan** di Portal GPKI;
- ✓ **Permohonan baharu atau pembaharuan sijil digital pelayan** di Portal GPKI
- Kelulusan pengesahan organisasi dan domain oleh prinsipal (eVetting)**
- Penjanaan sijil digital pelayan** oleh CA
- Penerimaan dan pemasangan** sijil digital pelayan oleh agensi
- Semakan konfigurasi** dan kemaskini **tarikh dan taraf pemasangan** sijil digital pelayan di Portal GPKI
- Pembatalan sijil digital pelayan** (jika berkaitan sahaja)

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



PERMOHONAN BAHARU ATAU PEMBAHARUAN SIJIL DIGITAL PELAYAN

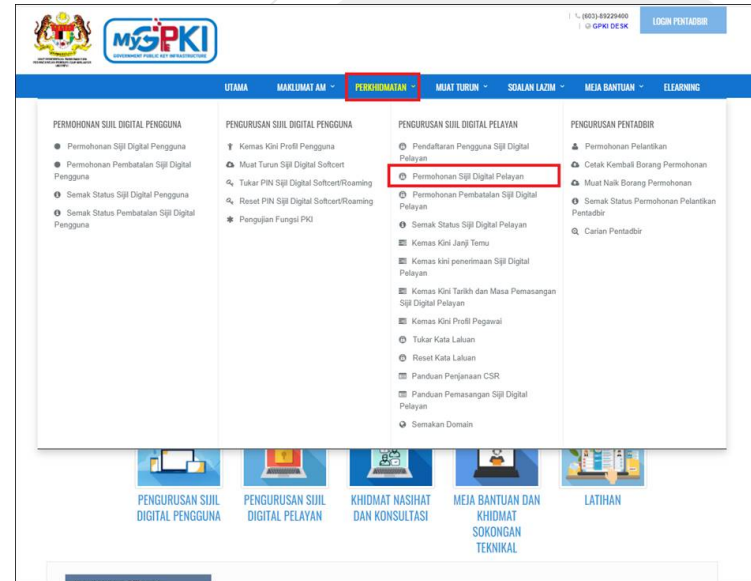
- Portal GPKI > Menu Perkhidmatan > Pengurusan Sijil Digital Pelayan > Permohonan Sijil Digital Pelayan

➤ Bagi **Permohonan Baharu** untuk pentadbir pelayan yang tidak pernah berdaftar akan menggunakan borang /paparan yang sama daripada Menu Pendaftaran Pengguna Sijil Digital Pelayan

➤ Bagi **Permohonan Baharu atau Tambahan untuk** pentadbir pelayan sedia ada akan menggunakan butang “**Permohonan Baharu**” di Menu Permohonan Sijil Digital Pelayan

Permohonan Baharu

➤ Bagi **Permohonan Pembaharuan** akan menggunakan butang icon “+” berwarna hijau yang berfungsi sebagai butang “**Permohonan Pembaharuan**” di Menu Permohonan Sijil Digital Pelayan



Ralat: Tiada Icon

- Butang pembaharuan **hanya akan dipaparkan seawal 30 hari** sebelum tarikh tamat tempoh sijil sedia ada.
- Ralat Butang pembaharuan masih tidak dipaparkan walaupun tempoh telah kurang dari 30 hari disebabkan **kitaran permohonan terdahulu tidak lengkap atau tidak selesai sepenuhnya**.
- Oleh itu, Pentadbir Pelayan (Pegawai Pemohon) perlu melaksanakan **Penerimaan dan pemasangan sijil digital pelayan oleh agensi** seperti di slaid 47 – 49 (Item 1 – 4)

Nota:

Agensi pelaksana perlu mengemukakan permohonan kepada agensi pusat melalui **surat rasmi permohonan sijil digital pelayan (menggunakan kepala surat (letterhead) agensi)** bagi menggunakan perkhidmatan pembekalan sijil digital pelayan yang disediakan. Surat tidak perlu dihantar secara fizikal tetapi akan dimuat naik semasa permohonan dibuat.

Contoh templat surat permohonan sijil digital pelayan seperti pautan menu di bawah:

Portal GPKI

(<https://gpki.mampu.gov.my>) >

Muat Turun >

Dokumen GPKI

> Permohonan Perkhidmatan GPKI

> Perkara 6: Sijil Digital Pelayan –

Contoh Surat Permohonan Sijil Digital Pelayan

CONTOH TEMPLAT SURAT PERMOHONAN SIJIL DIGITAL PELAYAN

Kepala Surat Jabatan (*Department Letterhead*)

Rujukan Surat :

Tarikh :

Pengarah
Bahagian Pembangunan Perkhidmatan Gunasama
Infrastruktur dan Keselamatan ICT (BPG)
Unit Pemodenan Tadbiran dan Perancangan
Pengurusan Malaysia (MAMPU)
Aras 1, Blok B, Bangunan MKN-Embassy Techzone
Jalan Teknokrat 2, 63000 Cyberjaya, Sepang
SELANGOR

Tuan,

PERMOHONAN SIJIL DIGITAL PELAYAN {*SINGLE DOMAIN EXTENDED VALIDATION/ MULTI DOMAIN/WILDCARD*} BAGI {*NAMA AGENSI*}

Dengan hormatnya saya merujuk kepada perkara di atas.

2. Sukacita dimaklumkan bahawa {*nama agensi, kementerian*} ingin memohon menggunakan Sijil Digital Pelayan {*Single Domain Extended Validation/ Multi Domain/ Wildcard*} yang disediakan melalui Perkhidmatan GPKI bagi domain {*nama/URL domain*}. Oleh yang demikian, bersama-sama ini disertakan Laporan Penilaian Risiko Laman Web Sektor Awam Dalam Konteks Perkhidmatan GPKI bagi pelayan domain tersebut seperti di **Lampiran A** untuk rujukan dan penilaian lanjut jua.

3. Sehubungan dengan itu, pihak {*nama agensi*} amat berbesar hari sekiranya tuan dapat mempertimbangkan dan meluluskan permohonan ini. Kerjasama tuan dalam perkara ini didahului dengan ucapan terima kasih.

Sekian.

“BERKHIDMAT UNTUK NEGARA”

Saya yang menjalankan amanah,

{*Tandatangan Ketua Jabatan*}

{*Nama Ketua Jabatan*}

{*Jawatan*}

Telefon :

E-mel :

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



SENARAI SEMAK PERMOHONAN SIJIL DIGITAL PELAYAN :

- ✓ Penyediaan laporan penilaian risiko laman web agensi;
- ✓ Penjanaan fail *Certificate Signing Request (CSR)* di pelayan;
- ✓ Pendaftaran pegawai pentadbir pelayan di Portal GPKI;
- ✓ Permohonan baharu atau pembaharuan sijil digital pelayan di Portal GPKI
- ✓ Kelulusan pengesahan organisasi dan domain oleh prinsipal (eVetting)
- Penjanaan sijil digital pelayan oleh CA
- Penerimaan dan pemasangan sijil digital pelayan oleh agensi
- Semakan konfigurasi dan kemaskini tarikh dan taraf pemasangan sijil digital pelayan di Portal GPKI
- Pembatalan sijil digital pelayan (jika berkaitan sahaja)

CA DAN PRINSIPAL



Certification Authority (CA)

Pihak Pemerakuan Berlesen di Malaysia yang menyediakan perkhidmatan pembekalan sijil digital pelayan dan pelanggan (*subscribe*) daripada prinsipal yang diiktiraf



Semua jenis



Multi domain dan Wildcard

Single Domain EV



Semua jenis



semua jenis

Prinsipal

Pihak yang diiktiraf dalam menyediakan pembekalan sijil digital di seluruh dunia (luar negara)



Prinsipal Lain

* Tidak termasuk



SYARAT KELULUSAN e-VETTING SIJIL DIGITAL PELAYAN

Agensi perlu **melengkapkan dokumen** permohonan selepas kelulusan diperolehi daripada Agensi Pusat iaitu:

- 1 **Menjana fail CSR yang betul** mengikut jenis sijil berdasarkan kelulusan yang diterima.
- 2 Mengemaskini maklumat **Pentadbir domain** yang didaftarkan di **MyNIC** dan memastikannya adalah terkini (<https://mynic.my/whois/#>).
- 3 Melaksanakan **pengesahan domain / subdomain** oleh **Pentadbir domain** yang diterima daripada prinsipal dan CA melalui kedua-dua cara iaitu **e-mel** dan **telefon pejabat**
- 4 **Menjawab e-mel yang diterima daripada prinsipal** dengan tindakan berikut: **Muat turun, mencetak, menyemak maklumat** dan **menandatangani dokumen** berserta **cop pegawai dan cop jabatan**. Setelah dokumen lengkap, ianya perlu diimbas dan dimuat naik serta dikembalikan semula kepada pihak prinsipal melalui e-mel

KELULUSAN PENGESAHAN SIJIL DIGITAL PELAYAN

KAEDAH PENGESAHAN SIJIL DIGITAL PELAYAN OLEH PRINSIPAL MENGIKUT JENIS SIJIL

Bil.	Jenis Sijil	Semakan Domain	Pengesahan Kebenaran oleh kakitangan	Subject Domain Name (DN)
1.	Extended Validation (EV)	Pemilikan atau kawalan domain	<ul style="list-style-type: none"> Prinsipal akan menghubungi Pengurusan Atasan melalui e-mel, borang permohonan dan telefon pejabat untuk mengesahkan identiti organisasi. Prinsipal akan menghubungi organisasi melalui e-mel untuk pengesahan pengeluaran sijil (pentadbir domain). 	<ul style="list-style-type: none"> Nama Domain Nama Organisasi dan lokasi termasuk negara Nombor Pendaftaran (Registration Number) Lokasi Pendaftaran (Registration Location)
2.	Organization Validation (OV)	Pemilikan atau kawalan domain	<ul style="list-style-type: none"> Prinsipal akan menghubungi organisasi melalui e-mel untuk pengesahan pengeluaran sijil (pentadbir domain). 	<ul style="list-style-type: none"> Nama Domain Nama Organisasi dan lokasi termasuk negara

KELULUSAN PENGESAHAN SIJIL DIGITAL PELAYAN

KAEDAH PENGESAHAN SIJIL DIGITAL PELAYAN OLEH PRINSIPAL

1. KAEDAH PENGESAHAN ORGANISASI (*ORGANIZATION VALIDATION*)

Terdapat beberapa cara pengesahan organisasi yang akan dilaksanakan bergantung kepada kaedah operasi prinsipal.

➤ URL DOMAIN/SUBDOMAIN

- Agensi perlu memastikan domain/subdomain **telah wujud** dan **telah didaftarkan di MyNIC**.
- Agensi perlu memastikan domain/subdomain **boleh dicapai oleh prinsipal yang berada di luar negara** untuk mengesahkan kewujudan domain/subdomain yang dimohon sijil digital pelayan ke atasnya.
- Agensi juga perlu mengemaskini maklumat domain/subdomain di portal **malaysia.gov.my** yang menjadi direktori sumber rujukan prinsipal untuk portal-portal di Malaysia.

➤ TELEFON PEJABAT

- Proses pengesahan oleh prinsipal hanya bermula **24 -48 jam** selepas permohonan oleh CA di portal prinsipal bergantung kepada giliran permohonan di prinsipal.
- Agensi perlu menetapkan **3 sesi cadangan tarikh dan masa janji temu** untuk membolehkan pihak prinsipal menghubungi pentadbir melalui **telefon pejabat agensi sahaja**. Tarikh dan masa mestilah selepas tempoh 24-48 jam tersebut di **Portal GPKI > Menu Perkhidmatan > Pengurusan Sijil Digital Pelayan > Kemaskini Janji Temu**.

➤ BORANG PERMOHONAN

- Agensi perlu menjawab e-mel yang diterima daripada prinsipal dengan tindakan berikut: **Muat turun, mencetak, menyemak maklumat** dan **menandatangani dokumen** berserta **cop pegawai dan cop jabatan**. Setelah dokumen lengkap, ianya perlu **diimbas dan dimuat naik** serta **dikembalikan semula** kepada pihak prinsipal **melalui e-mel** (*bagi jenis *single domain extended validation*).
- Agensi perlu menjawab e-mel yang diterima daripada prinsipal dengan **menyalin semula petikan yang mengandungi ayat dan random key** untuk pengesahan. E-mel hanya boleh dijawab semula oleh pegawai yang menerima sahaja. Sekiranya e-mel diterima dari pegawai yang berlainan dari penerima maka ianya adalah tidak sah.

KELULUSAN PENGESAHAN SIJIL DIGITAL PELAYAN

KAEDAH PENGESAHAN SIJIL DIGITAL PELAYAN OLEH PRINSIPAL

2. KAEDAH PENGESAHAN DOMAIN (*DOMAIN VALIDATION*)

Terdapat beberapa cara pengesahan domain yang boleh dipilih oleh agensi (pilih salah satu sahaja).

➤ E-MEL (paling mudah dan cepat)

- Pemilihan pengesahan menggunakan e-mel bermaksud e-mel akan hantar oleh prinsipal kepada **e-mel pentadbir yang telah didaftarkan sebagai *Administrative Contact* di MYNIC**. Cara semakan di MyNIC melalui <https://mynic.my/whois/#> dan masukkan nama domain.
- Sekiranya terdapat **pertukaran pegawai**, maka agensi hendaklah menghubungi terus kepada pihak MYNIC untuk pengemaskinian maklumat. Pihak MyNIC akan mengambil masa dalam tempoh 3-5 hari untuk proses pengemaskinian sebagaimana prosedur yang telah ditetapkan oleh pihak MyNIC.

➤ DNS

- Pemilihan pengesahan menggunakan DNS bermaksud membuat **penambahan random text** yang diberikan oleh pihak prinsipal melalui e-mel **ke dalam DNS bagi domain** tersebut. Pengesahan domain adalah berjaya sekiranya prinsipal dapat menyemak semula kewujudan random text di DNS domain/subdomain. Kebiasaannya sebarang perubahan DNS bagi sektor awam adalah di bawah kelolaan pihak GITN bergantung kepada struktur rangkaian agensi masing-masing. Oleh itu, pihak agensi perlu menghubungi terus kepada pihak GITN untuk memohon penambahan random text di DNS melalui portal GITN iaitu <https://mygovosf.gitn.net.my> - add txt record dalam DNS (nama domain).

➤ HTTPD

- Pemilihan pengesahan menggunakan HTTPD bermaksud membuat **penambahan random text** yang diberikan oleh pihak prinsipal melalui e-mel **ke dalam folder pki** yang ditetapkan oleh prinsipal (/well-known/pki folder) bagi pelayan untuk domain/subdomain tersebut. Pengesahan domain adalah berjaya sekiranya prinsipal dapat menyemak semula kewujudan random text di folder pki bagi domain/subdomain tersebut.

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



SENARAI SEMAK PERMOHONAN SIJIL DIGITAL PELAYAN :

- ✓ **Penyediaan laporan penilaian risiko** laman web agensi;
- ✓ **Penjanaan fail *Certificate Signing Request* (CSR)** di pelayan;
- ✓ **Pendaftaran pegawai pentadbir pelayan** di Portal GPKI;
- ✓ **Permohonan baharu atau pembaharuan sijil digital pelayan** di Portal GPKI
- ✓ **Kelulusan pengesahan organisasi dan domain oleh prinsipal** (eVetting)
- ✓ **Penjanaan sijil digital pelayan** oleh CA
- Penerimaan dan pemasangan** sijil digital pelayan oleh agensi
- Semakan konfigurasi** dan kemaskini **tarikh dan taraf pemasangan** sijil digital pelayan di Portal GPKI
- Pembatalan sijil digital pelayan** (jika berkaitan sahaja)

PENJANAAN SIJIL DIGITAL PELAYAN

Nota:

Pihak CA akan memuatnaik salinan sijil digital pelayan ke dalam Portal GPKI serta menghantar salinan sijil digital pelayan melalui e-mel kepada pentadbir pelayan.

➤ **Salinan Sijil Digital Melalui E-mel Notifikasi Sistem GPKI**

Sistem GPKI akan menghantar e-mel notifikasi berserta lampiran sijil digital pelayan dalam format *.cer.

➤ **Salinan Sijil Digital Melalui Portal GPKI**

Pentadbir pelayan boleh memuat turun sijil digital pelayan mengikut domain/subdomain masing-masing di Portal GPKI > Semakan Status Sijil Digital Pelayan > Pilih butang "Tindakan" pada senarai domain/subdomain > Maklumat Pelayan > Sijil Digital Pelayan > Klik pada pautan Papar untuk memuat turun sijil digital pelayan dalam format *.cer.

➤ **Salinan Sijil Digital Melalui E-mel CA**

Pihak CA akan menghantar e-mel yang mengandungi salinan sijil kepada Pegawai Pemohon, Pegawai Teknikal dan Pegawai Pengesah. Sijil digital pelayan dihantar dalam format *.crt, text atau lampiran e-mel prinsipal.

➤ **Salinan Sijil Digital Melalui E-mel dan Muat Turun dari Portal Prinsipal**

Prinsipal akan menghantar e-mel yang mengandungi salinan sijil kepada kepada Pegawai Pemohon, Pegawai Teknikal dan Pegawai Pengesah. Sijil digital pelayan dihantar dalam lampiran text atau pautan muat turun.

Nota:

Kaedah pemasangan sijil digital pelayan adalah berbeza mengikut *platform* dan *webservice* bagi setiap domain/subdomain

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



SENARAI SEMAK PERMOHONAN SIJIL DIGITAL PELAYAN :

- ✓ Penyediaan laporan penilaian risiko laman web agensi;
- ✓ Penjanaan fail *Certificate Signing Request (CSR)* di pelayan;
- ✓ Pendaftaran pegawai pentadbir pelayan di Portal GPKI;
- ✓ Permohonan baharu atau pembaharuan sijil digital pelayan di Portal GPKI
- ✓ Kelulusan pengesahan organisasi dan domain oleh prinsipal (eVetting)
- ✓ Penjanaan sijil digital pelayan oleh CA
- ✓ Penerimaan dan pemasangan sijil digital pelayan oleh agensi
- Semakan konfigurasi dan kemaskini tarikh dan taraf pemasangan sijil digital pelayan di Portal GPKI
- Pembatalan sijil digital pelayan (jika berkaitan sahaja)

TINDAKAN AGENSI SELEPAS PENERIMAAN SIJIL

- 1** **MESTI mengemas kini tarikh penerimaan** sijil digital pelayan di Portal GPKI bagi tujuan pengesahan penerimaan sejurus sijil digital diterima daripada CA atau prinsipal di Portal GPKI (<https://gpkimampu.gov.my>) > **Menu Perkhidmatan** > **Menu Pengurusan Sijil Digital Pelayan** > **Kemaskini Penerimaan Sijil Digital Pelayan** > **NoMyKad dan nama domain/subdomain** > **kemaskini tarikh terima sijil**. Sekiranya tarikh penerimaan tidak dikemaskini, pihak agensi akan mengalami ralat dan tidak dapat memohon pembaharuan sijil tersebut di Portal GPKI kelak.
- 2** **MESTI memasang** sijil digital pelayan di pelayan agensi masing-masing dalam **tempoh 14 hari** selepas penerimaan sijil digital pelayan tersebut. Bagi **tujuan pemasangan sijil digital pelayan dengan konfigurasi yang betul dan sijil rantaian (chain) yang lengkap**, pihak agensi memerlukan **sijil rantaian tambahan iaitu intermediate dan root** bagi CA dan juga **fail private key (*.key/*.pem)** (sekiranya pelayan bukan Windows) yang sepadan dengan fail csr yang telah dikemukakan semasa permohonan di Portal GPKI terutama kepada agensi yang pertama kali pertama menggunakan prinsipal ini. Sila pastikan arahan pemasangan diikuti dengan teliti kerana **setiap prinsipal mempunyai sijil rantaian yang berbeza** yang perlu dipasang. Malahan, **kaedah pemasangan juga adalah berbeza mengikut platform dan webservice** bagi pelayan masing-masing.

TINDAKAN AGENSI SELEPAS PENERIMAAN SIJIL

Item yang diperlukan semasa pemasangan sijil digital pelayan

- Sijil digital pelayan untuk subdomain yang dimohon**
- Sijil rantaian tambahan -> intermediate cert CA**
- Sijil rantaian tambahan -> root cert CA**
- Fail private key (*.key/*.pem/*.jks/*.keystore)**

Bagi sesetengah prinsipal item **b** dan **c** digabungkan dalam satu fail dan dikenali sebagai “**Chain Bundle**”.

CHAIN COMPLETE

```
-----BEGIN CERTIFICATE-----  
(Your Primary SSL certificate: your_domain_name.crt)  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
(Your Intermediate certificate: Ca_Cert_Intermediate.crt)  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
(Your Root certificate: Ca_Cert_Root.crt)  
-----END CERTIFICATE-----
```

Sijil intermediate dan root CA boleh diperoleh dari pelbagai cara berlainan bergantung kepada kaedah operasi setiap prinsipal sama ada akan diterima dari prinsipal melalui e-mel semasa penghantaran sijil bagi domain/subdomain atau boleh dimuat turun daripada Portal Prinsipal berkenaan.

Manual dan garis panduan pemasangan sijil digital pelayan mengikut **platform dan webservice** yang berkaitan.

- <https://www.entrust.com/knowledgebase/ssl/ssl-tls-certificate-installation-help?keyword=&productType=&serverType=>
- <https://support.globalsign.com/ssl/ssl-certificates-installation/install-ssl-certificate-overview>
- <https://www.digicert.com/kb/ssl-certificate-installation.htm>

TINDAKAN AGENSI SELEPAS PENERIMAAN SIJIL

3 Agensi **MESTI menyemak dan memastikan konfigurasi** pemasangan sijil digital pelayan dilaksanakan dengan betul dan mendapat **“Taraf A” bagi setiap subdomain** dengan menggunakan *tools* berikut:

- <https://www.ssllabs.com/ssltest/> (semakan konfigurasi pelayan)
- <https://www.sslshopper.com/ssl-checker.html> (semakan pemasangan chain sijil)

4 Mengemas kini tarikh dan masa pemasangan sijil dalam Portal GPKI (<https://gпки.mampu.gov.my>) > Menu Perkhidmatan > Menu Pengurusan Sijil Digital Pelayan > Kemaskini Tarikh dan Masa Pemasangan Sijil Digital Pelayan > No. MyKad dan Katalaluan > Pilih domain/subdomain > Tindakan > Tarikh pemasangan dan catatan taraf pemasangan). Ruangan catatan perlulah dimasukkan **maklumat penarafan pemasangan dan konfigurasi A** yang diperolehi. Sekiranya agensi masih mendapat **Taraf B-Z**, nyatakan **ralat atau masalah konfigurasi berserta justifikasi berkaitan diruang catatan tersebut**

5 Memaklumkan **segera** kepada **Agensi Pusat dan CA** sekiranya terdapat ralat atau berlakunya **sijil corrupt** bagi membolehkan waranti ke atas sijil digital pelayan tersebut **dituntut dalam tempoh 14 hari** tersebut.

6 Sekiranya pemasangan tidak dilaksanakan dalam tempoh yang ditetapkan, permohonan seterusnya **tidak akan dipertimbangkan** dan kos sijil digital pelayan akan **ditanggung sepenuhnya oleh agensi sendiri**.

TINDAKAN AGENSI SELEPAS PENERIMAAN SIJIL

7

Agensi **MESTI menyemak dan memastikan konfigurasi** pemasangan sijil digital pelayan dilaksanakan dengan betul dan mendapat **“Taraf A” bagi setiap subdomain** dengan menggunakan *tools* berikut:

- <https://www.ssllabs.com/ssltest/> (semakan konfigurasi pelayan)
- <https://www.sslshopper.com/ssl-checker.html> (semakan pemasangan chain sijil)

8

Bagi sijil digital pelayan **multi domain** atau **wildcard**, pihak agensi perlulah menjana fail csr baharu bagi setiap subdomain di pelayan masing-masing secara berasingan dengan kandungan CSR yang sama seperti CSR sebelumnya selepas sijil digital pelayan asal telah dijana dan berjaya dipasang oleh agensi.

9

Diingatkan juga bahawa agensi hendaklah memastikan **kunci persendirian (private key)** sijil digital pelayan yang dijana bersekali semasa penjanaaan csr **tidak hilang atau corrupt serta disimpan dengan selamat** kerana ianya **sangat diperlukan semasa pemasangan** sijil di pelayan kelak. Fail csr yang telah dijana untuk salinan sijil bagi **multi domain** dan **wildcard** perlu dikemukakan kepada Pentadbir GPKI melalui e-mel admingpki@mampu.gov.my untuk diserahkan kepada pihak CA bagi tujuan **penjanaaan semula (reissue)**. Sebagai makluman, bagi kes penjanaaan semula (reissue) sijil digital pelayan ini tidak memerlukan sebarang permohonan baharu di Portal GPKI ataupun di pihak CA.

DO AND DON'T

Sebagai langkah keselamatan, diingatkan supaya agensi menyimpan **salinan sijil yang diterima** (*.crt/*.cer) dan **kunci persendirian (private key)** format *.pem/*.key/*.ks/*.jks/*.keystore/*.kdb disimpan dengan **selamat dengan kaedah penyimpanan kunci di bawah perlindungan maklumat Rahsia Rasmi mengikut Arahan Keselamatan.**

Pentadbir pelayan bertanggungjawab untuk memastikan sijil digital **disimpan dengan selamat dan tidak dipindah milik. Akta Tandatangan Digital 1997 tidak membenarkan sijil digital pelayan untuk dipindah milik kerana sijil digital tersebut merupakan identiti pelayan dalam ruang siber.** Pentadbir pelayan **juga dilarang pindah milik atau mengedarkannya kepada pihak tidak berkenaan** termasuk **kerja-kerja pemasangan sijil digital pelayan perlu dilaksanakan sendiri oleh pegawai di agensi** ataupun pembekal yang telah dilantik secara sah sahaja. Sekiranya **keterdedahan** berlaku maka **risiko untuk menerima ancaman keselamatan** ke atas pelayan yang telah dipasang dengan sijil tersebut adalah **tinggi.**

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



PENJANAAN CSR DAN KONFIGURASI PEMASANGAN DI PELAYAN

Bil.	Crypto Library Tool	Fail yang diperlukan	Kaedah Konfigurasi	Rujukan
1.	<p>OpenSSL</p> <p>Web Service</p> <ul style="list-style-type: none"> Apache HTTP Server Nginx 	<p>Fail yang perlu dijana</p> <ul style="list-style-type: none"> Fail Private key = domain.key Fail CSR= domain.csr <p>Fail yang diperlukan semasa instalasi</p> <ul style="list-style-type: none"> Fail Private key = domain.key/ domain.pem (Nginx-perlu convert ke format *.pem) Fail domain/ subdomain certificate = domain.crt/ domain.cer Fail combine intermediate dan root certificate CA = cacert.crt/ cacert.cer 	<p>Jana Private Key dan CSR untuk Single Domain /Wildcard (tanpa SANs)</p> <pre>openssl req -new -newkey rsa:2048 -sha256 -nodes -keyout privateKey.key -out domain.csr -subj "/C=MY/ST=Selangor/L=Cyberjaya/O=Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia/OU=Bahagian Pembangunan Aplikasi/CN=www.mampu.gov.my"</pre> <p>Jana Private Key dan CSR untuk Multi Domain (dengan SANs)</p> <pre>openssl req -new -newkey rsa:2048 -sha256 -nodes -keyout privateKey.key -out domain.csr -subj "/C=MY/ST=Selangor/L=Cyberjaya/O=Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia/OU=Bahagian Pembangunan Aplikasi/CN=www.mampu.gov.my" -config san.conf</pre> <p>*Nota: 1. Maklumat SANs disimpan pada fail di pelayan adalah berbeza mengikut webservice masing-masing seperti san.conf /ssl.conf / san.cnf. Pindaan maklumat SANs seperti slide seterusnya 2. Kesemua subjek bagi CSR mandatori untuk diisi. Country Code (C), State (ST), Locality (L), Organization (O), Organization Unit (OU), dan Common Name (CN) 3. Nama fail privateKey.key, domain.csr boleh diubah mengikut kesesuaian subdomain. Contoh: www.mampu.gov.my2022.key</p> <p>Instalasi</p> <ul style="list-style-type: none"> Cari dan konfigurasi fail httpd.conf / conf.d / ssl.conf di pelayan <ul style="list-style-type: none"> ➢ SSLCertificateFile /path/to/domain.cer ➢ SSLCertificateKeyFile /path/to/domain.key ➢ SSLCertificateChainFile /path/to/cacert.cer Restart Apache (systemctl restart httpd or apachectl -k restart) 	<ul style="list-style-type: none"> Read DER file openssl x509 -text -noout -in domain.cer Read PEM file openssl x509 -text -noout -in domain.pem Convert DER (.cer, .der) to PEM openssl x509 -inform der -in domain.cer -out domain.pem Convert PEM to P7B openssl crl2pkcs7 -nocrl -certfile domain.cer -out domain.p7b -certfile cacert.cer Convert P7B to PEM openssl pkcs7 -print_certs -in domain.p7b -out domain.pem Convert PEM to PKCS#12 (PFX) file openssl pkcs12 -export -out domain.pfx -inkey privateKey.key -in domain.cer -certfile cacert.cer Convert PFX to PEM openssl pkcs12 -in domain.pfx -out domain.pem -nodes Convert PEM to DER openssl x509 -outform der -in domain.pem -out domain.der <p>https://www.sslshopper.com/article-most-common-openssl-commands.html</p>

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



PENJANAAN CSR DAN KONFIGURASI PEMASANGAN DI PELAYAN

Pindaan fail san.conf atau ssl.conf atau san.cnf untuk mewujudkan Subject Alternative Names (SANS) bagi Multi Domain

*Nota 1:

Pentadbir perlu mencari fail kewujudan fail san.conf / ssl.conf / san.cnf di pelayan masing-masing terlebih dahulu

Linux cmd: **locate *.conf**

*Nota 2:

Secara default command telah disabled.

Perlu uncomment atau keluar # pada command supaya kod berfungsi bagi multi domain sahaja.

```
[ req ]
default_bits                = 2048
distinguished_name          = req_distinguished_name
req_extensions              = req_ext

[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
countryName_default        = MY
stateOrProvinceName        = State or Province Name (full name)
stateOrProvinceName_default = Selangor
localityName                = Locality Name (eg, city)
localityName_default       = Cyberjaya
organizationName            = Organization Name (eg, company)
organizationName_default   = Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
commonName                  = Common Name (e.g. server FQDN or YOUR name - subdomain1.mampu.gov.my)
commonName_max              = 64

[ req_ext ]
subjectAltName = @alt_names

[alt_names]
DNS.1           = www.subdomain2.mampu.gov.my
DNS.2           = www.subdomain3.mampu.gov.my
DNS.3           = www.subdomain4.mampu.gov.my
```

*Nota 3:

DNS.1, 2 atau 3 adalah senarai SANS yang perlu ditambah dalam CSR. Ia **MESTILAH tidak berulang atau tidak sama** dengan nama domain/subdomain di Common Name (CN)

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



PENJANAAN CSR DAN KONFIGURASI PEMASANGAN DI PELAYAN

Bil.	Crypto Library Tool	Fail yang diperlukan	Kaedah Konfigurasi	Rujukan
2.	<p>JSSE (Keytool)</p> <p>Web Service</p> <ul style="list-style-type: none"> Apache Tomcat JBoss (Wildfly) Weblogic 	<p>Fail yang perlu dijana</p> <ul style="list-style-type: none"> Fail Private key = domain.ks/ domain.jks (keystore) Fail CSR= domain.csr <p>Fail yang diperlukan semasa instalasi</p> <ul style="list-style-type: none"> Fail Private key = domain.ks/ domain.jks (keystore) Fail domain/ subdomain certificate = domain.crt/ domain.cer Fail intermediate CA = cacert.crt/ cacert.cer Fail root certificate CA = root.crt/root.cer 	<p>Jana Private Key untuk Single Domain /Wildcard (tanpa SANs)</p> <pre>keytool -genkey -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -alias domain -keystore privateKey.jks -dname "CN=www.domain.gov.my, O=Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, OU=Bahagian Pembangunan Aplikasi, L=Cyberjaya, S=Selangor, C=MY"</pre> <p>Jana CSR untuk Single Domain /Wildcard (tanpa SANs)</p> <pre>keytool -certreq -keyalg RSA -sigalg SHA256withRSA -alias domain -keystore privateKey.jks -file domain.csr</pre> <p>Jana Private Key untuk Multi Domain (dengan SANs)</p> <pre>keytool -genkey -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -alias domain -keystore privateKey.jks -dname "CN=www.domain.gov.my, O=Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, OU=Bahagian Pembangunan Aplikasi, L=Cyberjaya, S=Selangor, C=MY" -ext "SAN=DNS:subdomain2.domain.gov.my,DNS:subdomain3.domain.gov.my,DNS:subdomain4.domain.gov.my"</pre> <p>Jana CSR untuk Single Domain /Wildcard (dengan SANs)</p> <pre>keytool -certreq -keyalg RSA -sigalg SHA256withRSA -alias domain -keystore privateKey.jks -ext "SAN=DNS:subdomain2.domain.gov.my,DNS:subdomain3.domain.gov.my,DNS:subdomain4.domain.gov.my" -file domain.csr</pre> <p><i>*Nota:</i> 1. Kesemua subjek bagi CSR mandatori untuk diisi. Country Code (C), State (ST), Locality (L), Organization (O), Organization Unit (OU), dan Common Name (CN) 2. Nama fail privateKey.jks, domain.csr, domain boleh diubah mengikut kesesuaian subdomain. Contoh: www.mampu.gov.my2022.jks</p>	<ul style="list-style-type: none"> Read Read a certificate file keytool -printcert -v -file domain.cer Check certificates in java keystore keytool -list -v -keystore domain.jks Check particular keystore using alias keytool -list -v -keystore tomcat.jks -alias domain Convert PFX to JKS keytool -v -importkeystore -srckeystore server.pfx -srcstoretype PKCS12 -destkeystore domain.jks -deststoretype JKS Convert JKS to PFX keytool -importkeystore -srckeystore domain.jks -srcstoretype JKS -destkeystore domain.pfx -deststoretype PKCS12

Bersambung seterusnya...

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



PENJANAAN CSR DAN KONFIGURASI PEMASANGAN DI PELAYAN

Bil.	Crypto Library Tool	Fail yang diperlukan	Kaedah Konfigurasi	Rujukan
2.	<p>JSSE (Keytool)</p> <p>Web Service</p> <ul style="list-style-type: none"> • Apache Tomcat • JBoss (Wildfly) • Weblogic 		<p>(sambungan...)</p> <p>Instalasi</p> <ul style="list-style-type: none"> • Save domain/subdomain certificate as domain.cer or domain.crt • Save intermediate (CA) cert as cacert.cer or ca-cert.crt • Save Root cert as root.cer or root.crt <p>• RUN: <code>keytool -import -alias root -keystore privateKey.jks -trustcacerts -file root.cer</code></p> <p>• RUN: <code>keytool -import -alias inter -keystore privateKey.jks -trustcacerts -file ca-cert.cer</code></p> <p>• RUN: <code>keytool -import -alias domain -keystore privateKey.jks -file domain.cer</code></p> <p>• Update server.xml (Prior Tomcat 8.5)</p> <pre><Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" scheme="https" secure="true" SSLEnabled="true" keystoreFile="/path/to/privateKey.jks" keystorePass="ehangeit" clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="TLSv1.3,TLSv1.2" .../></pre> <p>• Update server.xml (Tomcat 8.5 and later)</p> <pre><Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" scheme="https" secure="true" SSLEnabled="true" defaultSSLHostConfigName="*.host.com"> <SSLHostConfig hostName="*.host.com" protocols="TLSv1.3,TLSv1.2"> <Certificate certificateKeystoreFile="conf/privateKey.jks" certificateKeystorePassword="ehangeit" certificateKeyAlias="domain" type="RSA"/> </SSLHostConfig> </Connector></pre> <ul style="list-style-type: none"> • Restart Tomcat (systemctl restart tomcat) 	

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



PENJANAAN CSR DAN KONFIGURASI PEMASANGAN DI PELAYAN

Bil.	Crypto Library Tool	Fail yang diperlukan	Kaedah Konfigurasi	Rujukan
3.	<p>IBM Java SDK (iKeyMan)</p> <p>Web Service</p> <ul style="list-style-type: none"> IBM HTTP Server Websphere 	<p>Fail yang perlu dijana</p> <ul style="list-style-type: none"> Fail Private key = domain.kdb Fail CSR= domain.csr <p>Fail yang diperlukan semasa instalasi</p> <ul style="list-style-type: none"> Fail Private key = domain.kdb Fail domain/subdomain certificate = domain.crt/domain.cer Fail intermediate CA = cacert.crt/cacert.cer Fail root certificate CA = root.crt/root.cer 	<p>Jana New Certificate Database untuk Single Domain /Wildcard (tanpa SANs)</p> <pre>gskcapiamd -keydb -create -db privateKey.kdb -pw password -type cms -stashpw</pre> <p>Jana CSR – Single Domain /Wildcard (tanpa SANs)</p> <pre>gskcapiamd -certreq -create -db privateKey.kdb -pw password -labelservername -dn "CN=www.domain.gov.my, O=Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, OU=Bahagian Pembangunan Aplikasi, L=Cyberjaya, S=Selangor, C=MY" -size 2048 -file domain.csr</pre> <p><i>*Nota:</i> 1. Kesemua subjek bagi CSR mandatori untuk diisi. Country Code (C), State (ST), Locality (L), Organization (O), Organization Unit (OU), dan Common Name (CN) 2. Nama fail privateKey.kdb, domain.csr, boleh diubah mengikut kesesuaian subdomain. Contoh: www.mampu.gov.my2022.kdb</p> <p>Instalasi (Tambah Certificate to Database)</p> <ul style="list-style-type: none"> gskcapiamd -cert -receive -db privateKey.kdb -pw password -format ascii -file domain.cer -default_cert yes gskcapiamd -cert -add -db privateKey.kdb -pw password -format ascii -file cacert.cer Configure httpd.conf <ul style="list-style-type: none"> ➢ Enable LoadModule ibm_ssl_module modules/mod_ibm_ssl.so ➢ Set KeyFile "/path/to/privateKey.kdb" ➢ Set SSLStashFile "/path/to/stash_file" Restart Web Server Double click at root.cer to install root certificate 	<ul style="list-style-type: none"> Convert KDB to PFX gskcapiamd -cert -export -db domain.kdb -pw password -label servername - type cms -target server.pfx -target_pw password -target_type pkcs12 Convert PFX to KDB gskcapiamd -cert -import -db domain.kdb -pw password -label servername - type cms -target server.pfx -target_pw password -target_type pkcs12 - new_label servername Details for certificate database gskcapiamd -cert -details -db domain.kdb -pw password -label servername Extract a certificate from a key database gskcapiamd -cert -extract -db domain.kdb -pw password -label servername - target server.cer - format ascii List all certificates in a key database gskcapiamd -cert -list all personal CA

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



PENJANAAN CSR DAN KONFIGURASI PEMASANGAN DI PELAYAN

Bil.	Crypto Library Tool	Fail yang diperlukan	Kaedah Konfigurasi	Rujukan
4.	<p>Mozilla NSS (certutil)</p> <p>Web Service</p> <ul style="list-style-type: none"> Sun Java Web Server Oracle iPlanet Web Server 	<p>Fail yang perlu dijana</p> <ul style="list-style-type: none"> Fail CSR= domain.csr <p>Fail yang diperlukan semasa instalasi</p> <ul style="list-style-type: none"> Fail Private key = dijana secara build-in dalam webserver Fail domain/subdomain certificate = domain.crt/ domain.cer Fail intermediate CA = cacert.crt/ cacert.cer Fail root certificate CA = root.crt/root.cer 	<p>Jana New Certificate Database untuk Single Domain /Wildcard (tanpa SANs)</p> <pre>certutil -N -d /path/to/certdir</pre> <p>Jana CSR untuk Single Domain /Wildcard (tanpa SANs)</p> <pre>certutil -R -k rsa -g 2048 -s "CN=www.domain.gov.my, O=Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, OU=Bahagian Pembangunan Aplikasi, L=Cyberjaya, S=Selangor, C=MY" -d /path/to/certdir -o domain.csr</pre> <p>Instalasi (Tambah Certificate to Database)</p> <ul style="list-style-type: none"> certutil -A -n Server-Cert -t u,u,u -d /path/to/certdir -i domain.cer certutil -A -n CANAME -t C,, -d /path/to/certdir -i cacert.cer Restart Web Server <p><i>*Nota:</i> 1. Kesemua subjek bagi CSR mandatori untuk diisi. Country Code (C), State (ST), Locality (L), Organization (O), Organization Unit (OU), dan Common Name (CN) 2. Nama fail domain.csr boleh diubah mengikut kesesuaian subdomain. Contoh: www.mampu.gov.my2022.csr</p>	<ul style="list-style-type: none"> Check all certificates in database certutil -L -d /path/to/certdir Check certain certificate in database certutil -L -d /path/to/certdir -n Server-Cert -a Convert from PFX pk12util -i domain.pfx -w password -d /path/to/certdir Convert to PFX pk12util -o domain.pfx -n Server-Cert -d /path/to/certdir Check certificates in a PFX file pk12util -l domain.pfx <p>https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/tools/NSS_Tools_certutil</p>

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



PENJANAAN CSR DAN KONFIGURASI PEMASANGAN DI PELAYAN

Bil.	Crypto Library Tool	Fail yang diperlukan	Kaedah Konfigurasi	Rujukan
5.	<p>SChannel (MMC2 Command)</p> <p>Web Service</p> <ul style="list-style-type: none"> Microsoft IIS Microsoft Exchange 	<p>Fail yang perlu dijana</p> <ul style="list-style-type: none"> Fail CSR= domain.csr Fail Private key = dijana secara build-in dalam webserver (perlu pilih enable export sekiranya perlu pasang pada subdomain lain – wildcard) <p>Fail yang diperlukan semasa instalasi</p> <ul style="list-style-type: none"> Fail domain/ subdomain certificate = domain.crt/ domain.cer Fail intermediate CA = cacert.crt/ cacert.cer Fail root certificate CA = root.crt/root.cer <p>ATAU</p> <ul style="list-style-type: none"> Fail certificate dalam format PFX (import certificate dari pelayan lain dan covert menggunakan openssl) = domain.pfx 	<p>Jana CSR untuk Single Domain /Wildcard</p> <ul style="list-style-type: none"> Menggunakan MMC2 Command <p>Instalasi</p> <ul style="list-style-type: none"> Menggunakan MMC2 Command <p>Jana CSR untuk Multi Domain (hanya Ms Exchange Sahaja)</p> <ul style="list-style-type: none"> Menggunakan Exchange <p>Instalasi</p> <ul style="list-style-type: none"> Menggunakan Exchange <p>Sekiranya pemasangan multidomain, private key perlu ditukar format ke PKCS#12 terlebih dahulu sebelum diimport masuk ke server Windows menggunakan format *.pfx</p> <ul style="list-style-type: none"> ❖ Convert dan gabungkan key, subdomain/domain certificate dan CA certificate ke format PFX (import masuk ke IIS untuk multi domain atau wildcard) <pre>openssl pkcs12 -export -out domain.pfx -inkey domain.key -in domain.crt -certfile ca_bundle.crt</pre>	<ul style="list-style-type: none"> MMC2 Command Sekiranya penjanaan menggunakan MMC2 command maka instalasi juga perlu menggunakan kaedah MMC2 command juga. <p>https://medium.com/@yldirimabdrh m/how-to-create-sha256-csr-on-windows-739cba893fae</p> <p>https://www.tbs-certificates.co.uk/FAQ/en/windows-install-mmc.html#volet</p>

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

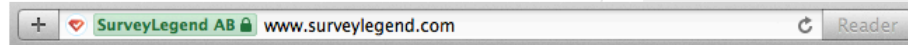


CONTOH PAPARAN SIJIL DIGITAL PELAYAN *EXTENDED VALIDATION (EV)* DI PELAYAR

- Kawalan Keselamatan Tertinggi
- Meningkatkan kepercayaan pengguna dan imej organisasi



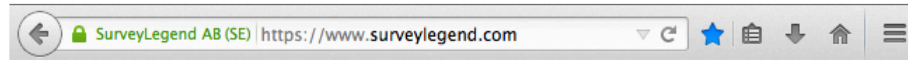
Safari



Chrome



Firefox



Internet Explorer



PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



CONTOH PAPARAN SIJIL DIGITAL PELAYAN EXTENDED VALIDATION (EV) DI PELAYAR

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 1.3.6.1.4.1.4146.1.1
- 2.23.140.1.1

* Refer to the certification authority's statement for details.

Issued to: gпки.mampu.gov.my

Issued by: GlobalSign Extended Validation CA - SHA256 - G3

Valid from: 21/01/2022 **to:** 22/02/2023

Issuer Statement

OK

Certificate

General Details Certification Path

Show: <All>

Field	Value
Valid to	22 February 2023 10:31:08 AM
Subject	gпки.mampu.gov.my, Unit Pem...
Public key	RSA (2048 Bits)
Public key parameters	33 86
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Basic Constraints	Subject Type=End Entity, Pat...
Subject Alternative Name	DNS Name=gпки.mampu.gov.my

CN = gпки.mampu.gov.my
O = Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
OU = SKICT BPG
STREET = Aras 6, Setia Perdana 2, Kompleks Setia Perdana, Pusat Pentadbiran Kerajaan Persekutuan
L = PUTRAJAYA
S = PUTRAJAYA
C = MY
1.3.6.1.4.1.311.60.2.1.3 = MY

Edit Properties... Copy to File...

OK

Certificate

General Details Certification Path

Certification path

- GlobalSign Root CA - R3
 - GlobalSign Extended Validation CA - SHA256 - G3
 - gпки.mampu.gov.my

View Certificate

Certificate status:

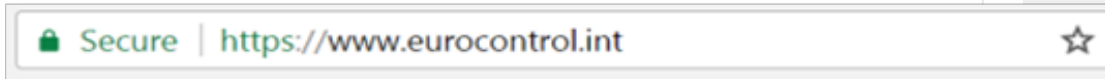
This certificate is OK.

OK

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

CONTOH PAPARAN SIJIL DIGITAL PELAYAN ORGANIZATION VALIDATION (OV) DI PELAYAN

- ❑ Mengandungi identiti organisasi
- ❑ Meningkatkan kepercayaan pengguna dan imej organisasi



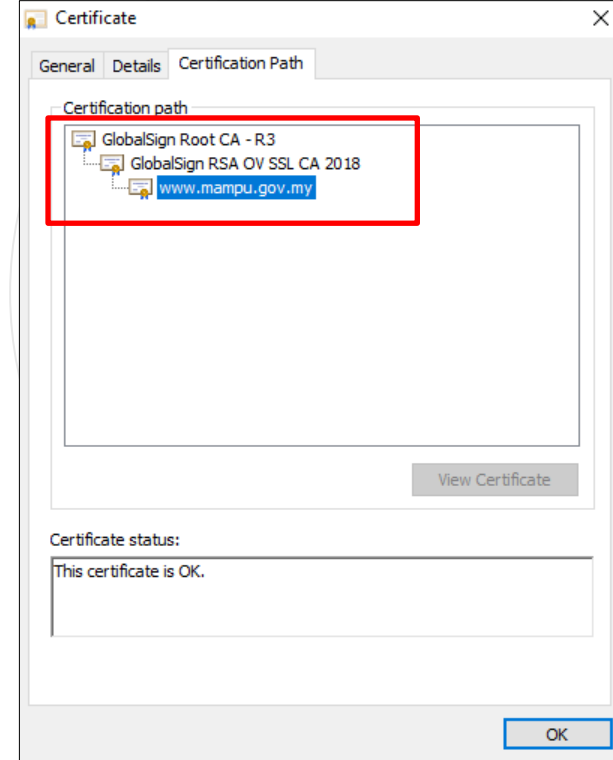
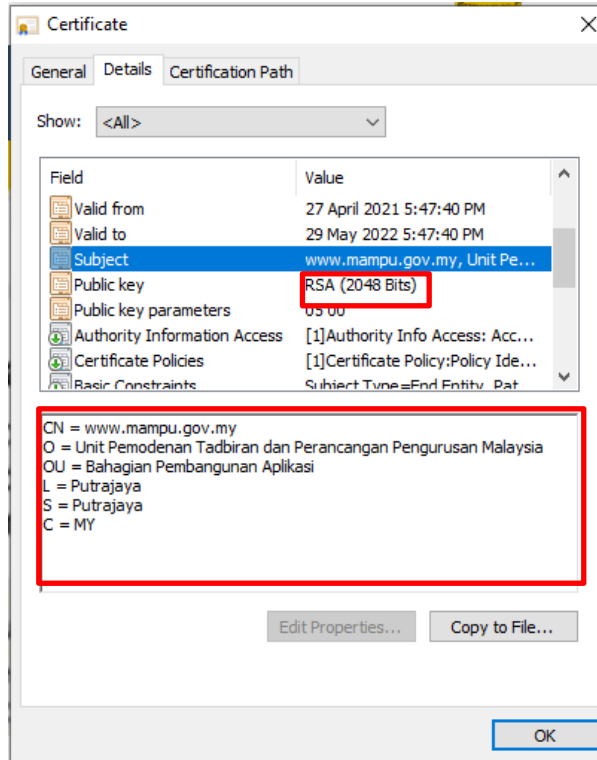
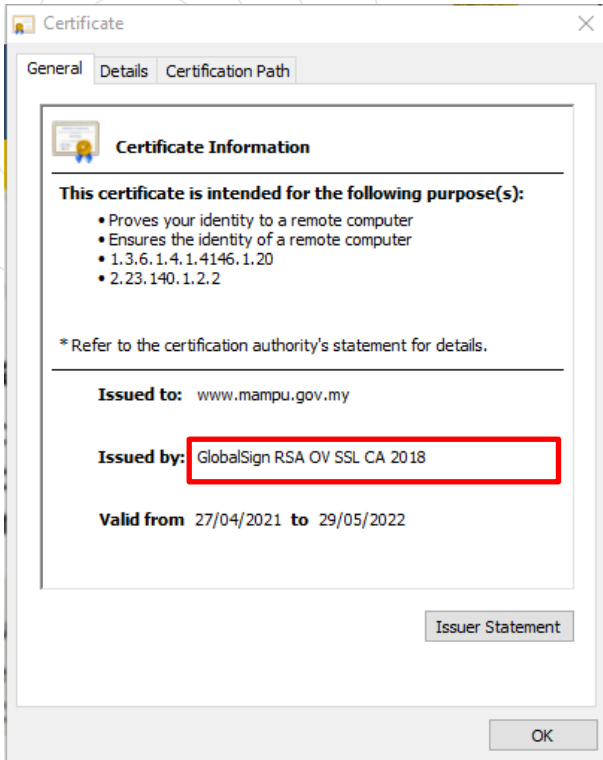
OV SSL in Chrome



OV SSL in IE

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

CONTOH PAPARAN SIJIL DIGITAL PELAYAN ORGANIZATION VALIDATION (OV) DI PELAYAR



PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

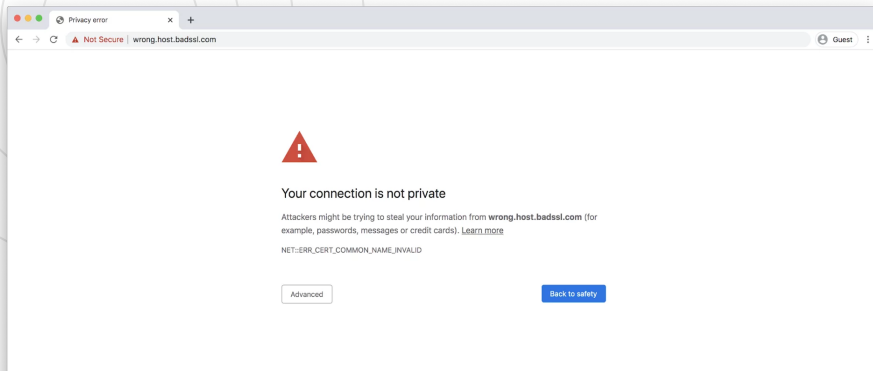


SENARAI SEMAK PERMOHONAN SIJIL DIGITAL PELAYAN :

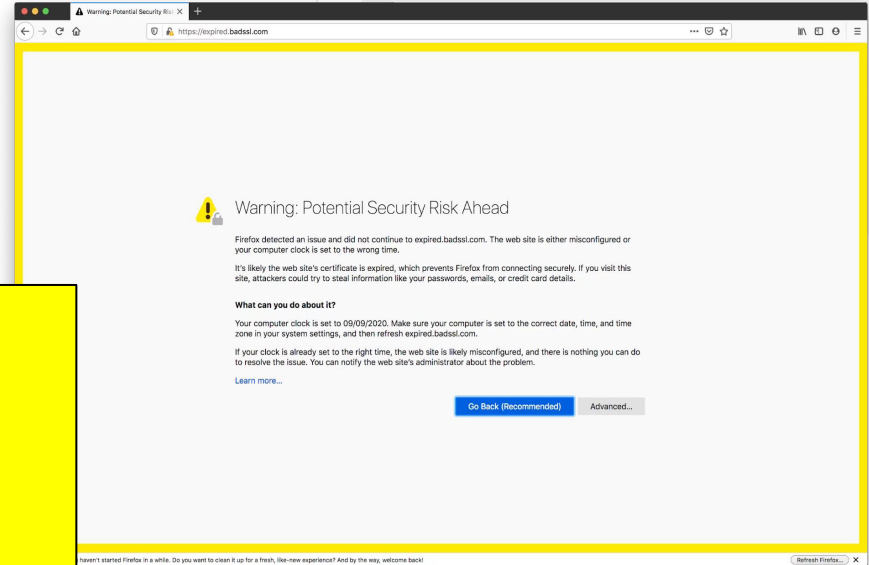
- ✓ **Penyediaan laporan penilaian risiko** laman web agensi;
- ✓ **Penjanaan fail *Certificate Signing Request* (CSR)** di pelayan;
- ✓ **Pendaftaran pegawai pentadbir pelayan** di Portal GPKI;
- ✓ **Permohonan baharu atau pembaharuan sijil digital pelayan** di Portal GPKI
- ✓ **Kelulusan pengesahan organisasi dan domain oleh prinsipal** (eVetting)
- ✓ **Penjanaan sijil digital pelayan** oleh CA
- ✓ **Penerimaan dan pemasangan** sijil digital pelayan oleh agensi
- ✓ **Semakan konfigurasi** dan kemaskini **tarikh dan taraf pemasangan** sijil digital pelayan di Portal GPKI
- Pembatalan sijil digital pelayan** (jika berkaitan sahaja)

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN

PAPARAN RALAT BAGI GOOGLE CHROME



PAPARAN RALAT BAGI FIREFOX



Antara Punca-Punca Ralat Pada Pelayar (Browser)

- Sijil digital pelayan tamat tempoh
- Sijil digital pelayan tidak aktif
- Tempoh hayat sijil digital pelayan melebihi 398 hari
- Nama hos hilang (Common Name tidak sah)
- Rantian sijil tidak sah atau tidak lengkap
- Sijil digital pelayan telah dibatalkan
- *Certification Authority (CA)* yang tidak diiktiraf
- Algoritma yang tidak selamat – SHA1
- Maklumat sijil digital pelayan yang hilang atau tidak sah

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



MANDATORY DISCARDS

- ❑ **aNULL** contains non-authenticated Diffie-Hellman key exchanges, that are subject to Man-In-The-Middle (MITM) attacks
- ❑ **eNULL** contains null-encryption ciphers (cleartext)
- ❑ **EXPORT** are legacy weak ciphers that were marked as exportable by US law
- ❑ **RC4** contains ciphers that use the deprecated ARCFOUR algorithm
- ❑ **DES** contains ciphers that use the deprecated Data Encryption Standard
- ❑ **SSLv2** contains all ciphers that were defined in the old version of the SSL standard, now deprecated
- ❑ **MD5** contains all the ciphers that use the deprecated message digest 5 as the hashing algorithm

BEST PRACTICES

- ❑ Enable **only TLSv1.2** and above
- ❑ Use an explicit, **strong cipher string** (disable weak cipher) and server preferences
- ❑ **Prefer Perfect Forward Secrecy (FPS)** – Done via prioritize Ephemeral (DHE, ECDHE) ciphers
- ❑ Set the option for **Secure Renegotiation to "Require"**
- ❑ Enable **TLS_FALLBACK_SCVS extension**
- ❑ Enable **HTTP Strict Transport Security (HSTS)**
- ❑ **Dedicated Private Key** for each web server instance
- ❑ Test before going live

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



SEMAKAN KONFIGURASI PEMASANGAN SIJIL

1

Tools: Nmap

```
nmap -sT -PN --script ssl-enum-ciphers.nse <IP Address> [ -p <Port> ]
```

Contoh: nmap -sT -PN -p 8443 --script ssl-enum-ciphers.nse 192.168.0.138

2

Tools: OpenSSL (SSL connection)

```
openssl s_client -connect <Hostname/IP Address>:<Port Number>
```

Contoh: openssl s_client -connect www.domain.gov.my:443

3

Tools: OpenSSL (Show Certificate)

```
openssl s_client -showcerts <Hostname/IP Address>:<Port Number>
```

Contoh: openssl s_client -showcerts www.domain.gov.my:443

4

Tools: OpenSSL (TLS Certificate Lifecycle Management)

```
echo | openssl s_client -connect <Hostname/IP Address>:<Port Number> | openssl x509 -noout -enddate
```

Contoh: openssl s_client -connect www.domain.gov.my:443 | openssl x509 -noout -enddate

```
$ nmap -sT -PN -p 8443 --script ssl-enum-ciphers.nse 192.168.0.138
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-14 09:11 a/k
Nmap scan report for 192.168.0.138
Host is up (0.00s latency).
```

```
PORT      STATE SERVICE
8443/tcp  open  https-alt
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|     cipher preference: server
|_  least strength: A
Nmap done: 1 IP address (1 host up) scanned in 1.98 seconds
```

PERKHIDMATAN MyGPKI BAGI PEMBEKALAN SIJIL DIGITAL PELAYAN



SEMAKAN KONFIGURASI PEMASANGAN SIJIL

5 Tools: OpenSSL (To verify the consistency of the RSA private key and to view its modulus)

```
openssl rsa -modulus -noout -in myserver.key | openssl md5 Nmap  
openssl rsa -check -noout -in myserver.key  
openssl x509 -modulus -noout -in myserver.crt | openssl md5
```

6 Tools: OpenSSL (Check a certificate)

Check a certificate and return information about it (signing authority, expiration date, etc.):

```
openssl x509 -in server.crt -text -noout
```

7 Tools: OpenSSL (Check a private key)

Check the SSL key and verify the consistency:

```
openssl rsa -in server.key -check
```

8 Tools: OpenSSL (Verify a certificate and key matches)

These two commands print out md5 checksums of the certificate and key; the checksums can be compared to verify that the certificate and key match.

```
openssl x509 -noout -modulus -in server.crt | openssl md5  
openssl rsa -noout -modulus -in server.key | openssl md5
```

9 Tools: SSL Labs

Rujukan Tindakan Pembetulan

#Ralat 1: supports TLS 1.0 and TLS 1.1. & vulnerable to the POODLE attack

Tindakan pembetulan: SSL3, TLS 1.0 and TLS 1.1 perlu disablekan... hanya allow TLS 1.2 ke atas sahaja

Tomcat:

https://support.solarwinds.com/SuccessCenter/s/article/Disable-TLS-1-0-for-the-default-HTTPS-connector-in-DPA?language=en_US

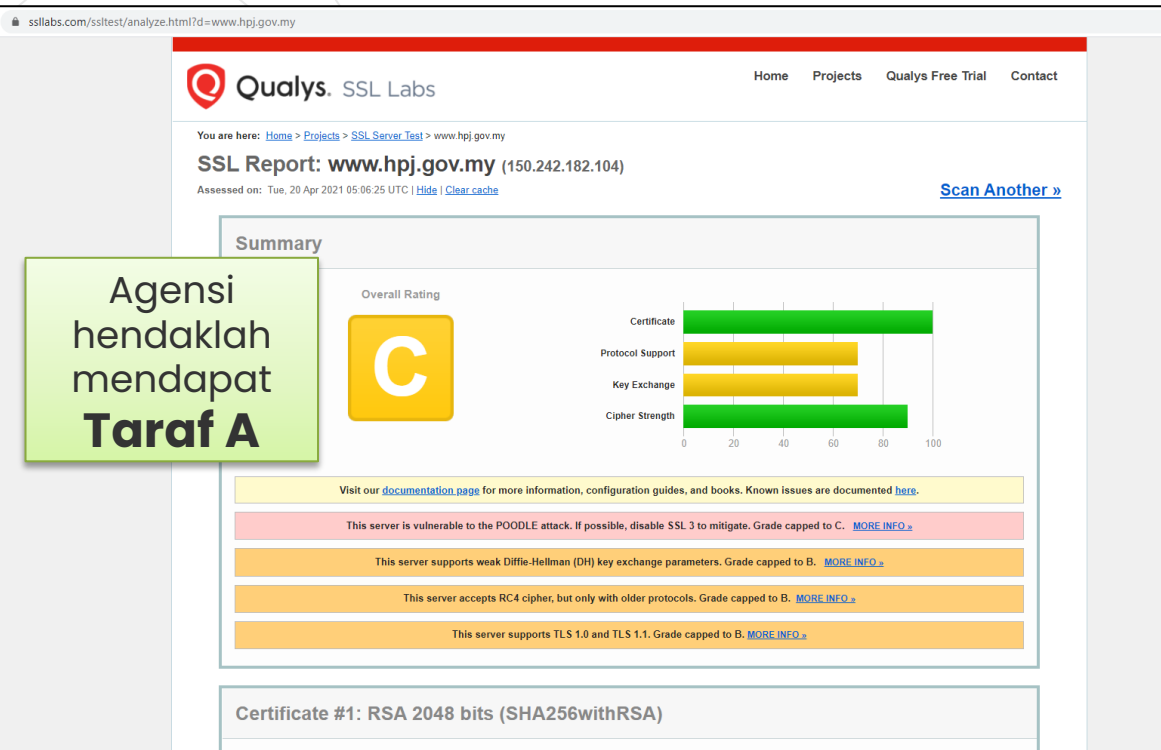
Apache:

<https://www.leaderssl.com/news/471-how-to-disable-outdated-versions-of-ssl-tls-in-apache>

Apache:

<https://www.ssl.com/guide/disable-tls-1-0-and-1-1-apache-nginx>

Agensi hendaklah mendapat **Taraf A**



sslabs.com/ssltest/analyze.html?d=www.hpj.gov.my

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact


You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.hpj.gov.my

SSL Report: **www.hpj.gov.my** (150.242.182.104)

Assessed on: Tue, 20 Apr 2021 05:06:25 UTC | [Hide](#) | [Clear cache](#) | [Scan Another »](#)

Summary

Overall Rating



Category	Score
Certificate	100
Protocol Support	70
Key Exchange	70
Cipher Strength	90

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. [MORE INFO »](#)

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)

Nota : Agensi perlu membuat konfigurasi tambahan - **auto force redirect** dari HTTP ke HTTPS untuk memudahkan pengguna mengakses https di URL masing-masing secara automatik

Rujukan Tindakan Pembedulan (samb.)

#Ralat 2: not support Forward Secrecy

Tindakan pembedulan: Perlu set chipers enable secrecy

<https://www.digicert.com/kb/ssl-support/ssl-enabling-perfect-forward-secrecy.htm>

** perlu update version openssl, apache perlu version 2.4.+ sahaja

#Ralat 3: accepts RC4 cipher, but only with older protocols

windows - <https://foxontherock.com/solve-rc4-warning-qualys-ssllabs-test>

apache - <https://superuser.com/questions/866738/disabling-rc4-in-the-ssl-cipher-suite-of-an-apache-server>

** (utk apache) ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH:ECDHE-RSA-AE\$';

tomcat - <https://grok.lsu.edu/Article.aspx?articleid=17596>

tomcat - <https://support.comodo.com/index.php?/Knowledgebase/Article/View/659/17/how-to----disable-weak-ciphers-in-tomcat-7--8>

#Ralat 4: weak Diffie-Hellman (DH) key exchange parameters

Guide to Deploying Diffie-Hellman for TLS (<https://weakdh.org/sysadmin.html>)

#Ralat 5: ROBOT vulnerability

** most probably kerana menggunakan WAF F5/citrix/cisco

<https://robotattack.org>

#Ralat 6: 64-bit block cipher (3DES / DES / RC2 / IDEA)

Disable 64-bit block cipher

<https://warlord0blog.wordpress.com/2017/02/03/ssl-64-bit-block-size-cipher-suites-supported-sweet32-tomcat>

SEMAKAN KONFIGURASI PEMASANGAN SIJIL

Contoh pemasangan sijil dengan konfigurasi yang betul



Qualys. SSL Labs Free Trial Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.mampu.gov.my](#) > 103.233.161.234

SSL Report: [www.mampu.gov.my](#) (103.233.161.234)

Assessed on: Mon, 03 May 2021 08:43:14 UTC | [Clear cache](#) [Scan Another »](#)

Summary

Overall Rating

A+

Metric	Score
Certificate	100
Protocol Support	100
Key Exchange	90
Cipher Strength	100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

SEMAKAN KONFIGURASI PEMASANGAN SIJIL

10

Tools: SSL Shopper (Chain Certificate)

Rujukan Tindakan Pembetulan

Finding 1: failed to connect due to firewall restrictions

=> firewall yang tidak allow untuk scanning atau port di firewall ditutup

#Finding 2: HTTPS on port 443

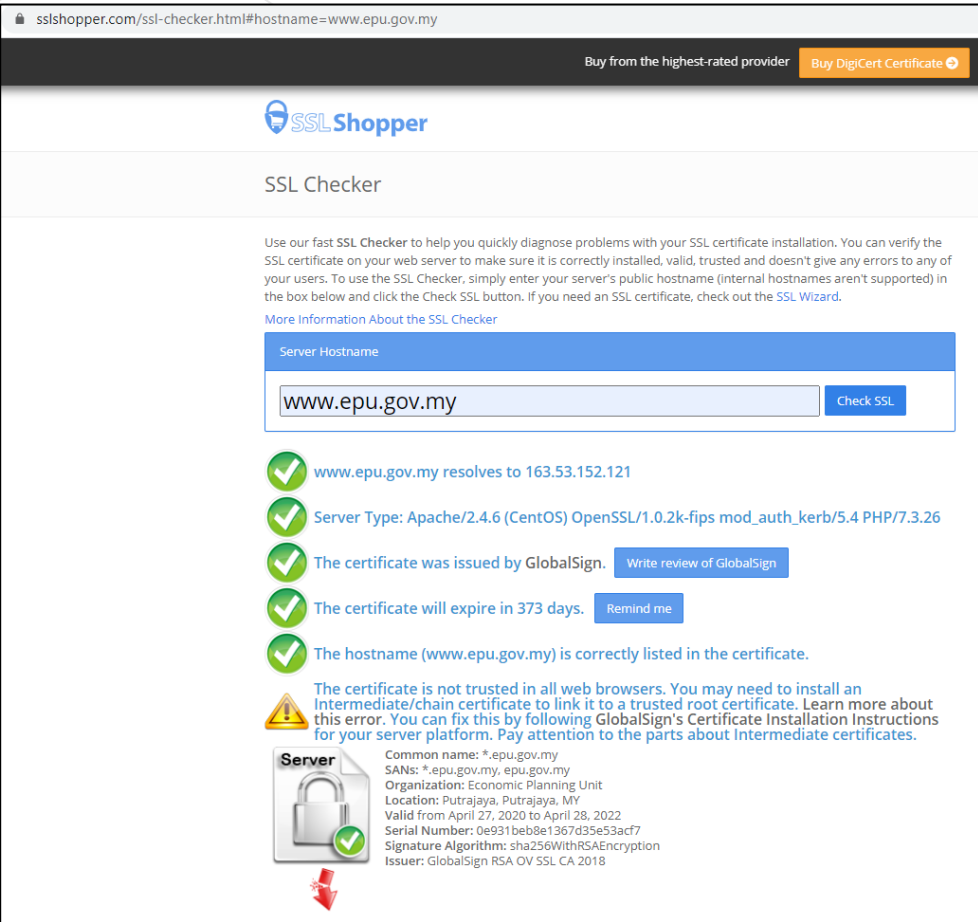
=> restricted on firewall/load balancer atau check firewall allow tidak HTTPS connection inbound

#Finding 3: not allow port 443

=> tidak pointing port 80/8080 untuk thru melalui port 443'

#Finding 4: The certificates is not trusted in all web browsers

=> Perlu pasang intermediate dan root cert bagi chain cert yang lengkap



sslshopper.com/ssl-checker.html#hostname=www.epu.gov.my

Buy from the highest-rated provider Buy DigiCert Certificate

SSL Shopper

SSL Checker

Use our fast SSL Checker to help you quickly diagnose problems with your SSL certificate installation. You can verify the SSL certificate on your web server to make sure it is correctly installed, valid, trusted and doesn't give any errors to any of your users. To use the SSL Checker, simply enter your server's public hostname (internal hostnames aren't supported) in the box below and click the Check SSL button. If you need an SSL certificate, check out the [SSL Wizard](#).

[More Information About the SSL Checker](#)

Server Hostname

www.epu.gov.my Check SSL

- ✓ www.epu.gov.my resolves to 163.53.152.121
- ✓ Server Type: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_auth_kerb/5.4 PHP/7.3.26
- ✓ The certificate was issued by GlobalSign. [Write review of GlobalSign](#)
- ✓ The certificate will expire in 373 days. [Remind me](#)
- ✓ The hostname (www.epu.gov.my) is correctly listed in the certificate.

Warning: The certificate is not trusted in all web browsers. You may need to install an intermediate/chain certificate to link it to a trusted root certificate. Learn more about this error. You can fix this by following GlobalSign's Certificate Installation Instructions for your server platform. Pay attention to the parts about intermediate certificates.

Server

Common name: *.epu.gov.my
SANs: *.epu.gov.my, epu.gov.my
Organization: Economic Planning Unit
Location: Putrajaya, Putrajaya, MY
Valid from April 27, 2020 to April 28, 2022
Serial Number: 0e931beb8e1367d35e53ac7
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign RSA OV SSL CA 2018

SEMAKAN KONFIGURASI PEMASANGAN SIJIL

Server Hostname

gпки.mampu.gov.my [Check SSL](#)

- ✓ gпки.mampu.gov.my resolves to 103.233.161.239
- ✓ Server Type: nginx
- ✓ The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).
- ✓ The certificate was issued by GlobalSign. [Write review of GlobalSign](#)
- ✓ The certificate will expire in 264 days. [Remind me](#)
- ✓ The hostname (gпки.mampu.gov.my) is correctly listed in the certificate.

Server

Common name: gпки.mampu.gov.my
SANs: gпки.mampu.gov.my
Organization: Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia Org. BPG
Location: Putrajaya, Putrajaya, MY
Valid from January 23, 2020 to January 23, 2022
Serial Number: 793f0097385b26efbec08fc6
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign Extended Validation CA - SHA256 - G3

↓

Chain

Common name: GlobalSign Extended Validation CA - SHA256 - G3
Organization: GlobalSign nv-sa
Location: BE
Valid from September 20, 2016 to September 20, 2026
Serial Number: 48a402dd27920da208349dd1997b
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign

↓

Root

Common name: GlobalSign
Organization: GlobalSign Org. Unit: GlobalSign Root CA - R3
Valid from March 18, 2009 to March 18, 2029
Serial Number: 0400000000121585308a2
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign

**Contoh
pemasangan sijil
dengan susunan
rantai (chain)
sijil yang lengkap**



TERIMA KASIH

Maklumat yang dipaparkan dalam slaid ini adalah hak milik
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)
Jabatan Perdana Menteri
Sebarang salinan hendaklah mendapat persetujuan dan kelulusan MAMPU



ISO/IEC 27006:2011
ISMS 02062013 CB 02



ISO / IEC 27001

Pengiktirafan MS ISO/IEC 27001:2013
NO. SIJIL: 027-ISO49