UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Taklimat Pengurusan Sijil Digital Pelayan (SSL/TLS) Perkhidmatan MyGPKI

The Everly Hotel Putrajaya
26 September 2022

Kandungan Taklimat Sijil Digital Pelayan

01 Teori dan Pengenalan Sijil Digital Pelayan

02 Sijil Digital Pelayan Dalam Konteks Perkhidmatan MyGPKI

03 Permohonan Sijil Digital Pelayan

04 POV: e-Vetting SSL

05 Pemasangan Sijil Digital Pelayan

06 Pengurusan Pentadbir Sijil Digital Pelayan, Sistem GPKI & GPKI Mobile

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Teori & Pengenalan Sijil Digital Pelayan

What is SSL/TLS?

Secure Socket Layer (SSL) / Transport Layer Security (TLS) is a security protocol that aims to secure the communication between web browser and web server through authentication and encryption. It was set up by Netscape in 1994 to address Internet's safety concerns.

The TLS is an upgraded version of the SSL protocol. The functionality of both protocols is the same, while the differences are over the security features.

The Evolution of SSL/TLS Protocol

1994
SSL 2.0
Developed by Netscape. Unfortunately with many security flaws

1995
SSL 3.0
First commercial SSL at 64

1999
TLS 1.0
IEFT takes over. Microsoft forced the protocol name change to Transport Layer Security (TLS)

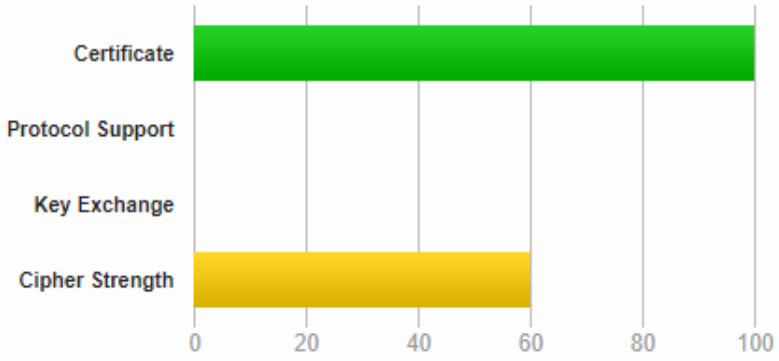
2006
TLS 1.1
Protections against Cipher Block Chaining (CBC) attacks

2008
TLS 1.2
Adding PRFs, AES cipher suites, removing IDEA and DES cipher suites, and several other enhancements

2018
TLS 1.3
Remove insecure features + add new Cipher Suites

The **Internet Engineering Task Force (IETF) is** to produce relevant technical and engineering documents that influence the way people design, use, and manage the Internet to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds.

Overall Rating



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports insecure Diffie-Hellman (DH) key exchange parameters (Logjam). Grade set to F. MORE INFO »

This server is vulnerable to the Return Of Bleichenbacher's Oracle Threat (ROBOT) vulnerability. Grade set to F. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2 or TLS 1.3. Grade capped to C. MORE INFO »

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. MORE INFO »

This server's certificate chain is incomplete. Grade capped to B.

HTTP request to this server failed, see below for details.

This server supports TLS 1.0. Grade capped to B. MORE INFO »

SSL Report: www.posdigicert.com.my (110.74.186.40)

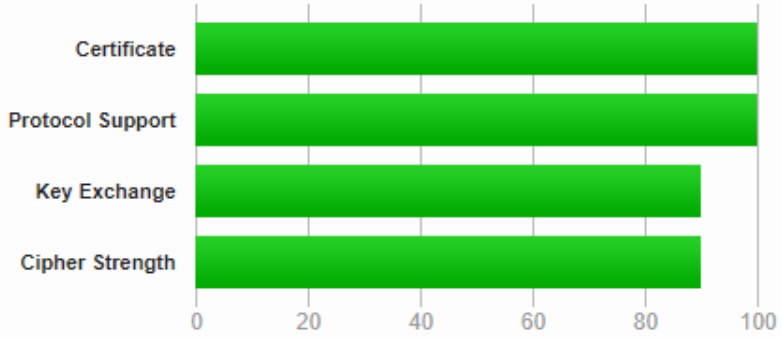
Assessed on: Thu, 22 Sep 2022 06:38:27 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



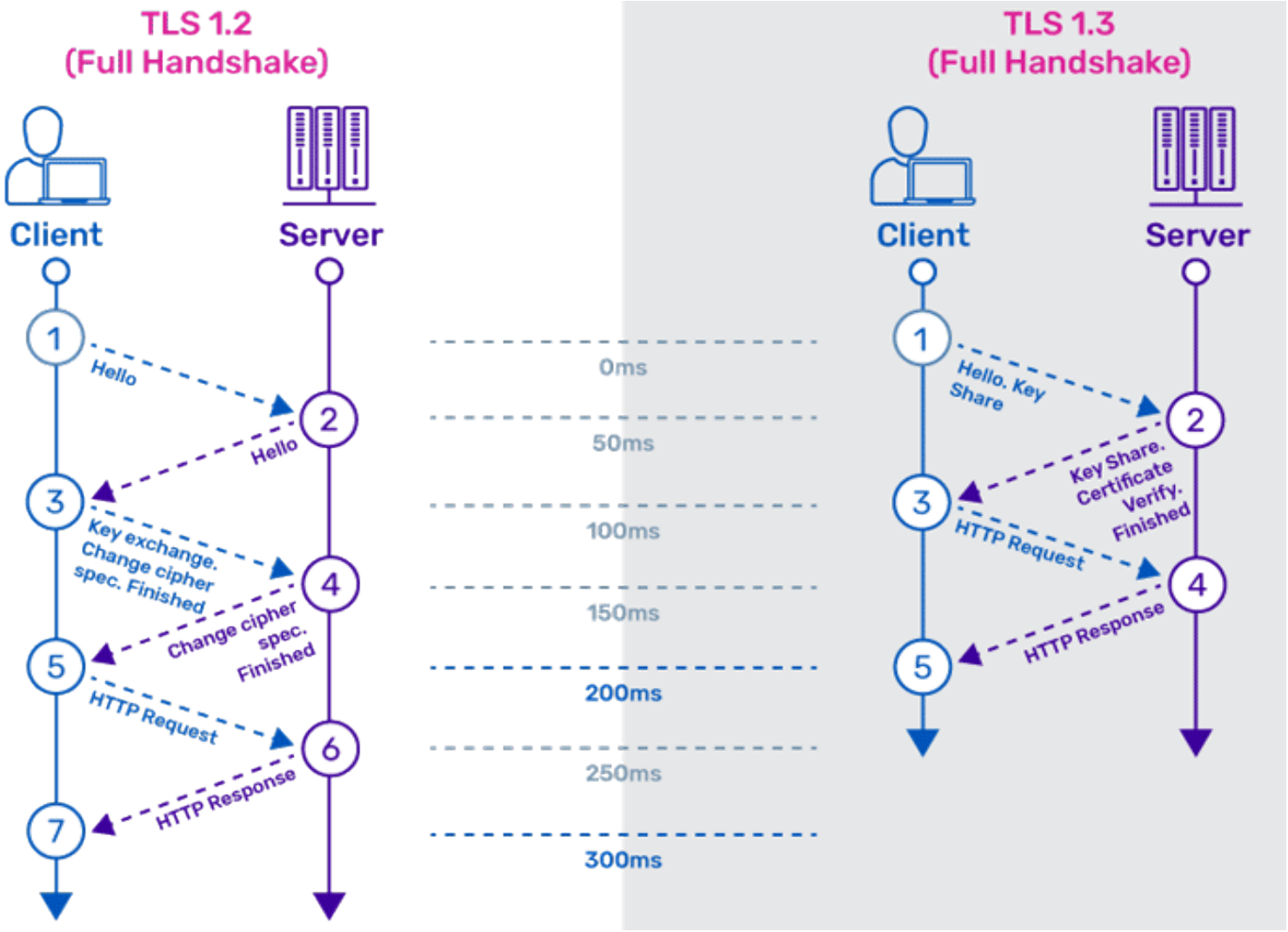
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

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

www.ssllabs.com/ssltest/

Zero Round-Trip Time (0-RTT)



SSL Algorithms

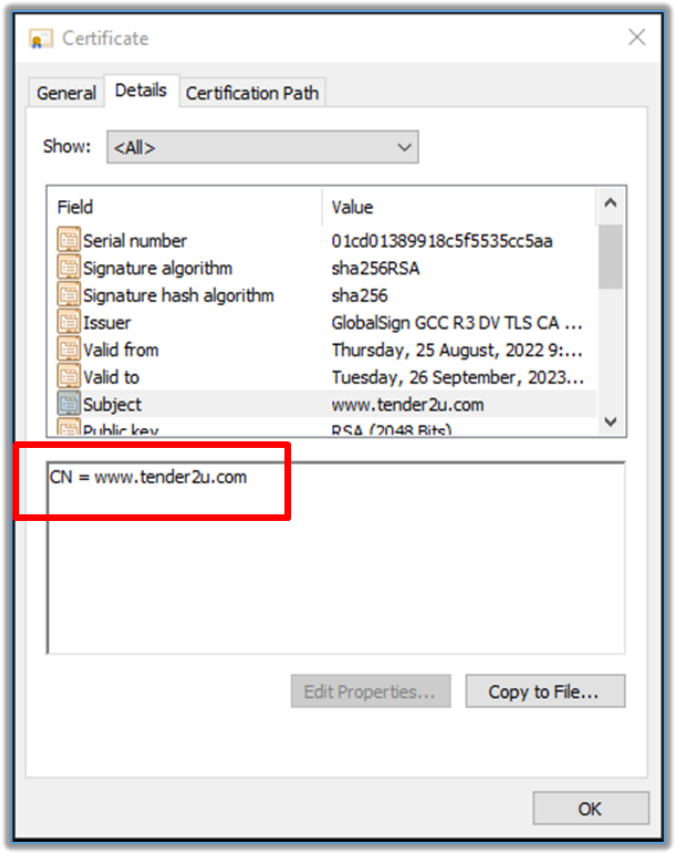
There are primarily two types of encryption methods which are primarily used: "symmetric encryption" and "asymmetric encryption." Both methods use different mathematical algorithms to scramble the data. The encryption list used in SSL certificates as below:

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	Status
SHA1	X	/	/	/	/	X	Discontinue in 2016
SHA2	X	X	X	X	/	/	Still in use
ECC	X	X	X	X	X	/	Still in use

	ENTRUST	GlobalSign	GeoTrust
Validation Type	Organisation Extended	Domain Organisation Extended	Domain Organisation Extended
Certificate Type	Single Multi-domain Wildcard	Single Multi-domain Wildcard	Single Multi-domain Wildcard
Encryption	RSA ECC	RSA ECC	RSA ECC
Certificate Validity	1 Year	1 Year	1 Year

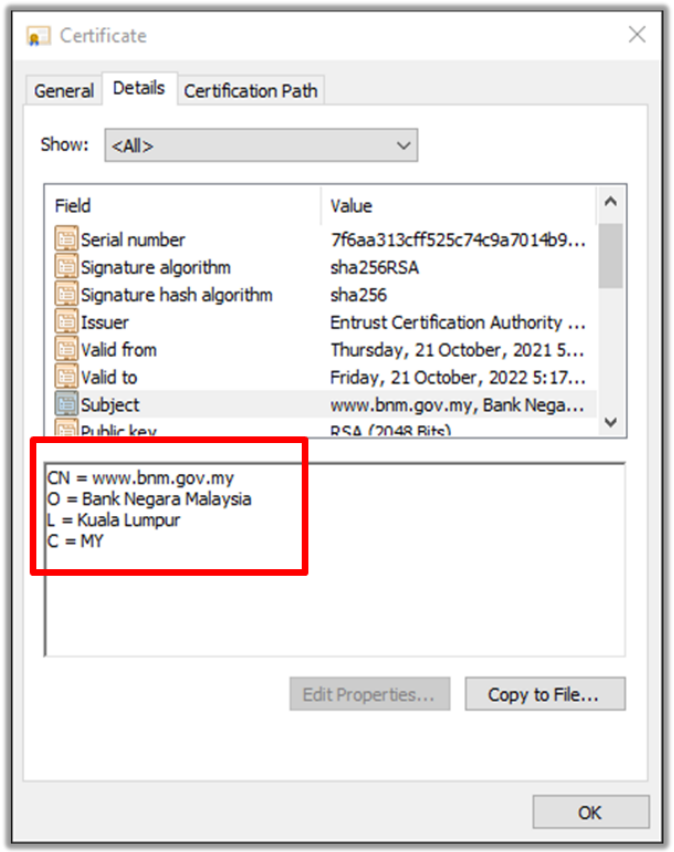
DOMAIN VALIDATED (DV)

- Domain Name



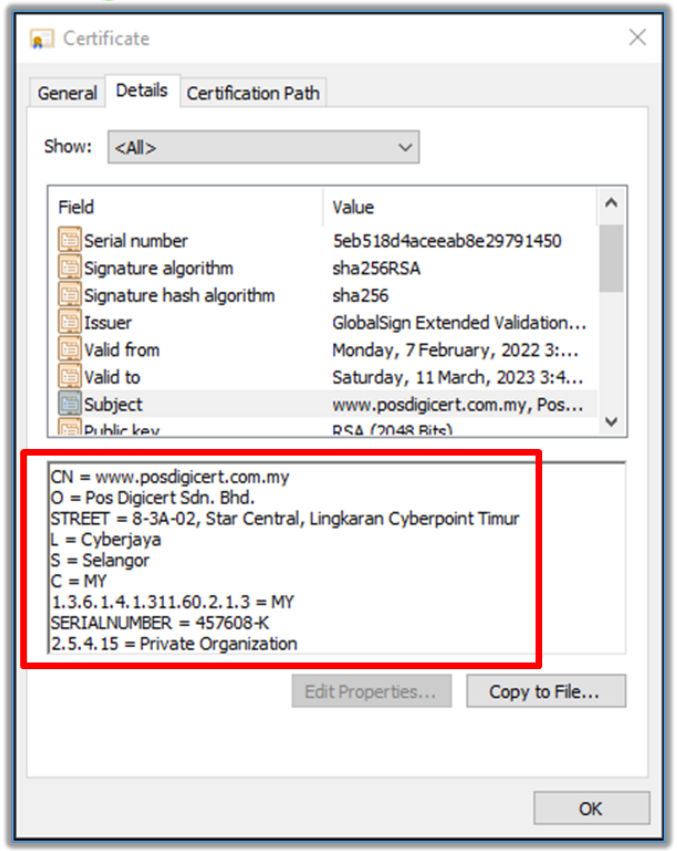
ORGANISATION VALIDATED (OV)

- Domain Name
- Organisation Name

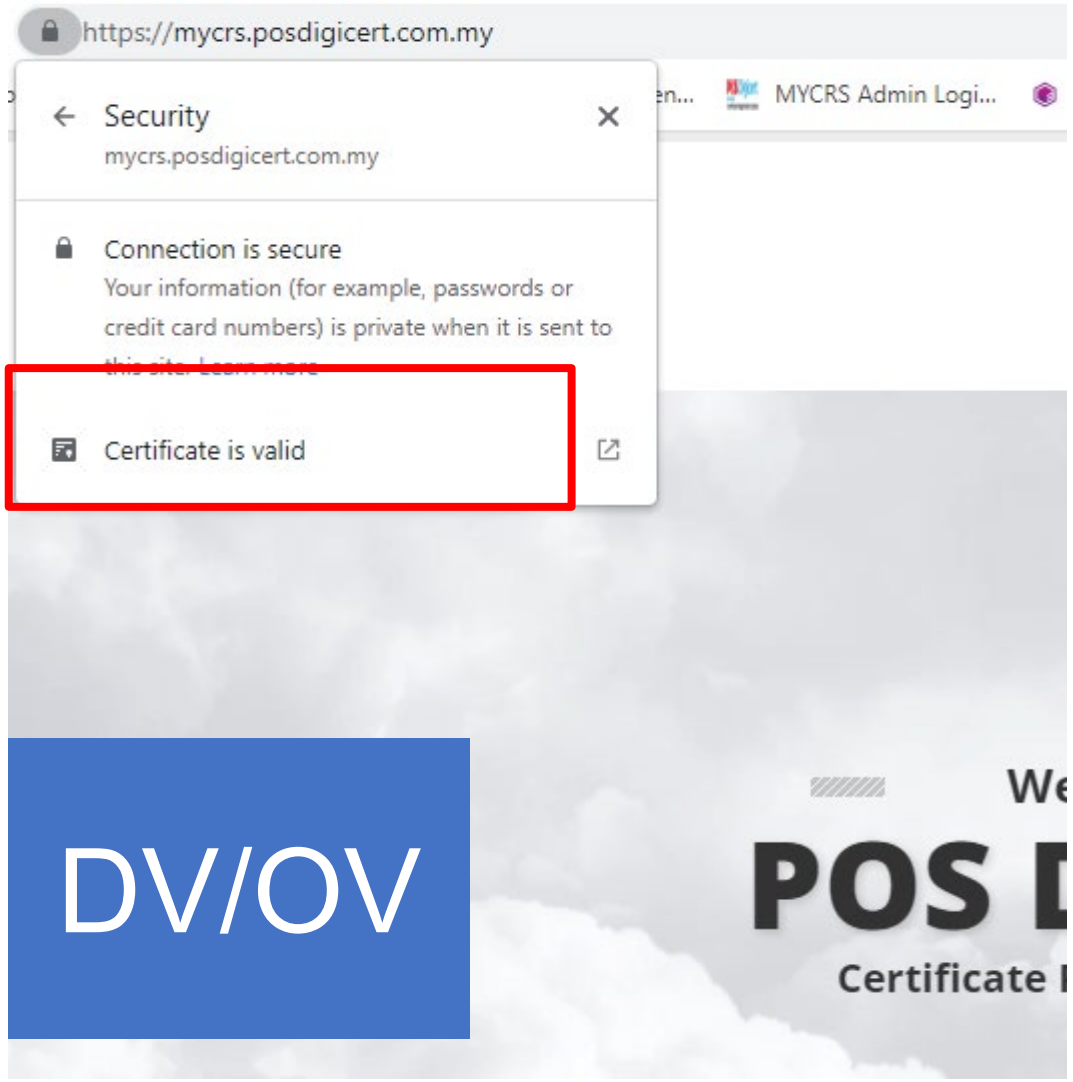


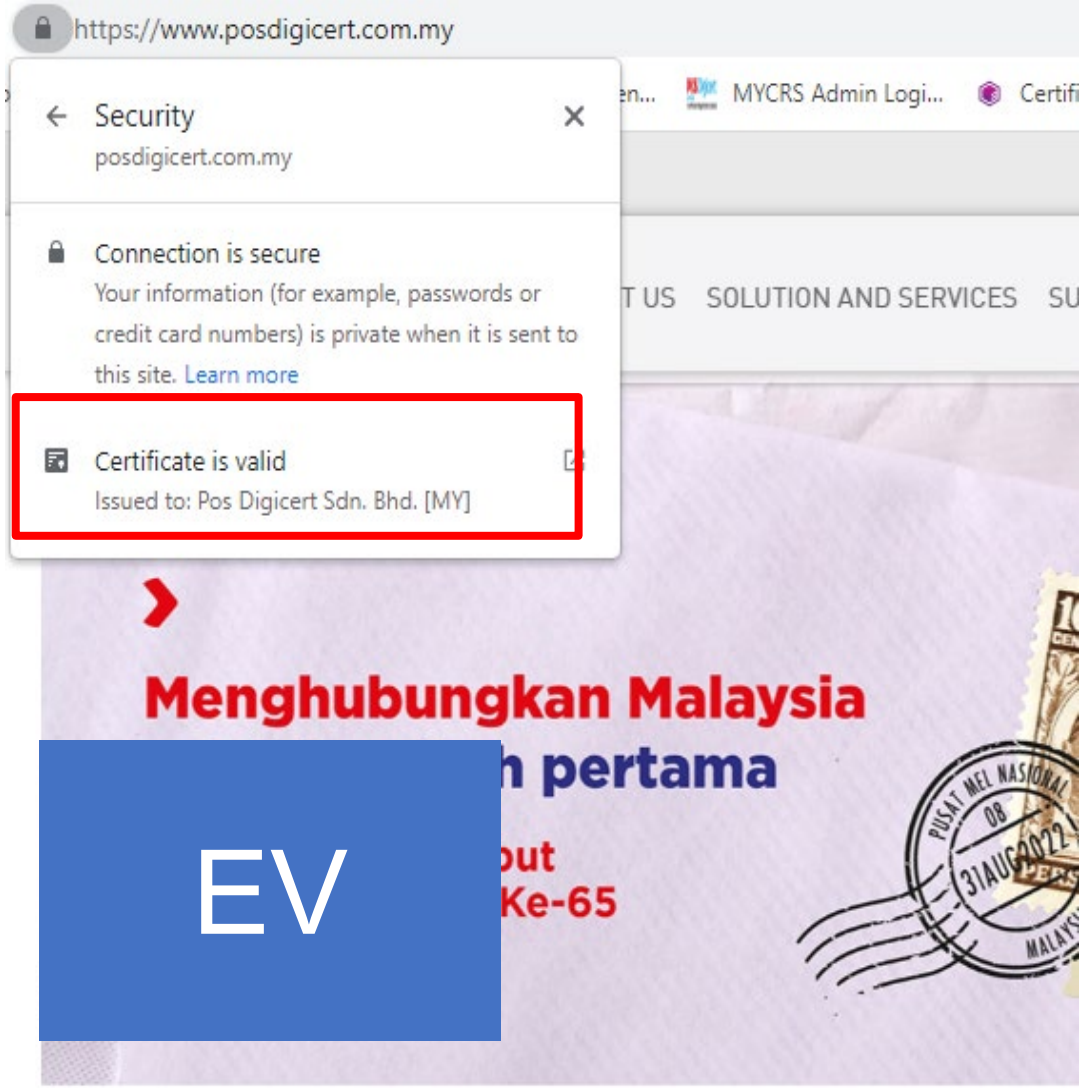
EXTENDED VALIDATION (EV)

- Domain Name
- Organisation Name
- Organisation Address

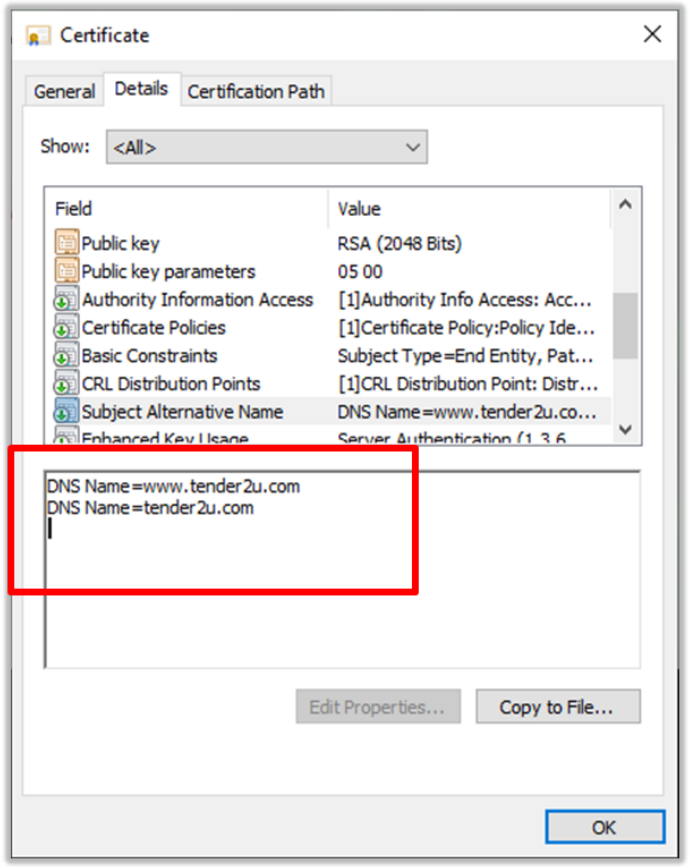


The difference of DV,OV & EV once the SSL certificate is installed in your web browser



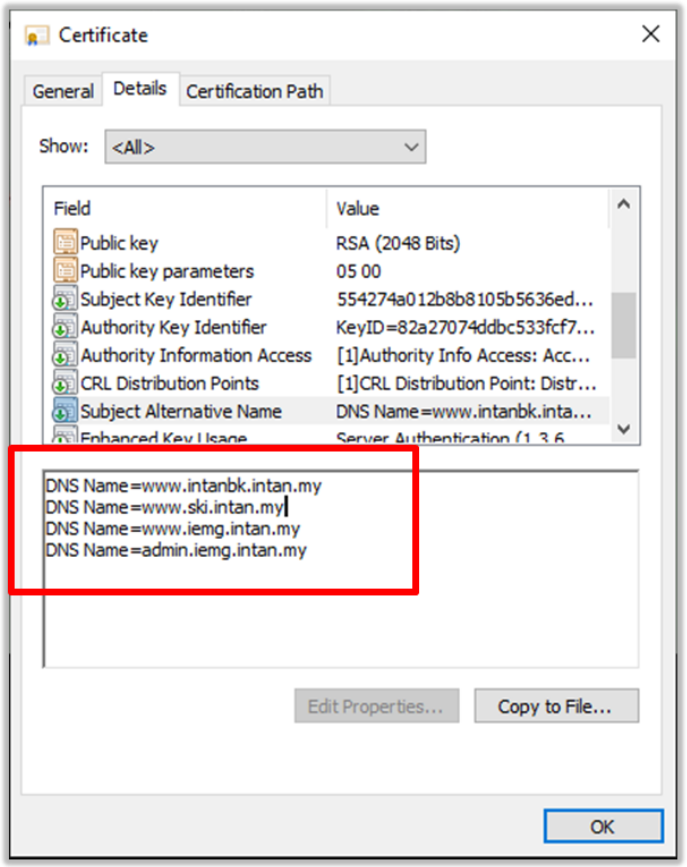


SINGLE DOMAIN



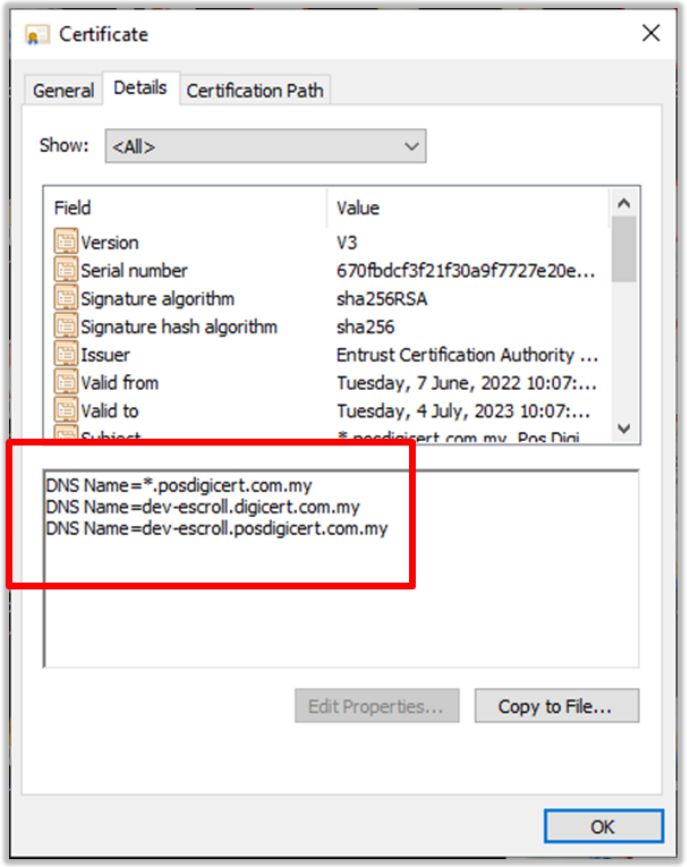
1 domain name
www. is free

MULTI-DOMAIN



More than 2 domain names

WILDCARD



1 root domain
Multiple sub-domains

What is TLS/SSL?

https://www.youtube.com/watch?v=YmdZNWXVvsw

All SSL certificates can be reissued, regardless of how many times. The reissue request can be made anytime before 2 months of the expiry date. A new CSR is required for each certificate re-issue. The current certificate will be revoked one month after the issuance of the new certificate.

Why reissue the certificate?:

1. Missing private key
2. Corrupt server

Reliance Limit / Warranty

The accumulated maximum amount that the CA will pay in the event of the wrongful issuance / validation:

	ENTRUST	GlobalSign	GeoTrust
Domain Validated	-	USD 10 K	USD 500 K
Organisation Validated	USD 100 K	USD 1.25 M	USD 1.25 M
Extended Validation	USD 100 K	USD 1.5 M	USD 1.5 M

Previous SSL Incidents

2015 - The Italian partners (registration authorities; namely GlobalTrust.it and InstantSSL.it) of the certificate authority company **Comodo** were hacked and nine Secure Sockets Layer (SSL) encryption certificates fraudulently issued for Google, Microsoft, Skype, and Yahoo, among others.

2017 - Symantec had issued over 100 certificates without proper validation, including certificates for example.com that were not authorized by example.com's owner. The ensuing investigation uncovers further malfeasance by Symantec, leading to the distrust of Symantec by all major platforms.

What is Secure Site Seal?

- To let your visitors know that you have taken measures to ensure the safety of their information is with the Secure Site Seal.
- To show that you are committed to online security
- Visitors can check the authenticity of your website and the status of the certificate
- Studies have shown that shopping cart abandonment is reduced and that the number of completed orders increases when using a website seal

Site Seal Icon / Logo			
How do I get a Site Seal?	The technical contact will receive an Entrust Site Seal upon the fulfillment of your certificate order.	https://www.globalsign.com/en/ssl/secure-site-seal	https://www.digicert.com/support/access-site-seal-installation

GlobalSign by GMO

Web Site Profile

This web site is secured by an ExtendedSSL Certificate.

SSL Certificate Information and Contact Information.

Common Name (URL)	www.globalsign.com
Validity Period (DD/MM/YYYY)	16/09/2021-18/10/2022
Validity Status	Valid
Organization Name	GMO GlobalSign, Inc.
Place of Business	
Street	2 International Drive, Suite 150
City	Portsmouth
State/Province	New Hampshire
Country Code	US
ZIP Code	03801
Tel Number	+1 603 570 7060
Jurisdiction Information	
Jurisdiction Country	US
Jurisdiction State/Province	New Hampshire
Incorporating agency registration number	578611

Please verify the following.

1. There are no warning messages in the details above
2. That the SSL 'Validity status' is 'Valid'
3. That the address of this profile page starts with https://profile.globalsign.com/

ENTRUST

Sunday 2022-09-18 15:30+0000

buy.entrust.net has been verified by Entrust.

ENTRUST VERIFIED

Site Name:

buy.entrust.net

Site Seal Status:

Valid

Verification:

Entrust or an independent local registration authority has verified that **Entrust Limited** is an existing business and owns or operates the domain name **buy.entrust.net**

Data Security:

This site is capable of using SSL to encrypt data going between your Web browser and the website. The communication of your private information from any address beginning with "https" is encrypted and secured using SSL. For more information about SSL encryption, see the certificate FAQ.

Always check that the information provided here matches that of the site you are visiting.

> Report Seal Misuse

01 SIJIL DIGITAL PELAYAN SINGLE DOMAIN

KETERANGAN

01 Didaftarkan hanya ke atas 1 domain atau 1 subdomain sahaja

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

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

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

KRITERIA PEMILIHAN

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

Contoh 1:

- **gpki.mampu.gov.my**

Contoh 2:

- **www.mampu.gov.my**

02 SIJIL DIGITAL PELAYAN MULTI DOMAIN

KETERANGAN

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

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

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:

- gpki.mampu.gov.my
- gpki.bpg.gov.my
- dts.mampu.gov.my

Contoh 2:

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

03 SIJIL DIGITAL PELAYAN WILDCARD

KETERANGAN

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

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

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

*** Nota:**
Walaupun wildcard mempunyai kelebihan tiada had bilangan subdomain dan boleh menjangkau sehingga melebihi 150 subdomain namun ia hanya meliputi subdomain pada 1 aras hirearki 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
  - gpki.mampu.gov.my
  - dts.mampu.gov.my
  - itims.mampu.gov.my

Contoh 2:
- *.anm.gov.my
  - gpki.anm.gov.my
  - dts.anm.gov.my
  - itims.anm.gov.my

Sijil Digital Pelayan Dalam Konteks Perkhidmatan MyGPKI

2.1: PENGENALAN PERKHIDMATAN MyGPKI

2.2: DASAR DAN PENERANGAN UMUM MENGENAI SIJIL DIGITAL PELAYAN

2.3: JENIS-JENIS SIJIL YANG DIBEKALKAN OLEH PERKHIDMATAN MyGPKI

2.4: HAD WARANTI MAKSIMUM MENGIKUT JENIS SIJIL DAN PRINSIPAL

2.1: PENGENALAN PERKHIDMATAN MyGPKI

- Perkhidmatan MyGPKI merupakan perkhidmatan keselamatan ICT yang berasaskan teknologi *Public Key Infrastructure* (PKI) yang dilaksanakan selaras dengan **Akta Kerajaan Elektronik 2007**, **Akta Tandatangan Digital 1997 dan Peraturan-peraturan Tandatangan Digital 1998**, serta **Arahan Teknologi Maklumat 2007**.

- Perkhidmatan MyGPKI mula dilaksanakan pada tahun 2002 dengan melibatkan pembekalan sijil digital oleh Pihak Berkuasa Pemerakuan Berlesen - *Certification Authority* (CA) yang dilantik oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM)

- MAMPU merupakan agensi peneraju yang diberi tanggungjawab untuk melaksanakan pembekalan Perkhidmatan MyGPKI kepada agensi sektor awam.

2.1: PENGENALAN PERKHIDMATAN MyGPKI

FUNGSI

Menyediakan perkhidmatan *Public Key Infrastructure* (PKI) dengan **membekalkan Sijil Digital Pengguna** bagi tujuan pengesahan identiti, tandatangan digital, penyulitan dan penyahsulitan maklumat serta **Sijil Digital Pelayan** (SSL) kepada agensi-agensi Kerajaan bagi mengukuhkan keselamatan sistem ICT Kerajaan.

OBJEKTIF

Memantapkan tahap keselamatan data dan maklumat bagi sistem ICT Kerajaan.

Melindungi keselamatan data/ maklumat Kerajaan dalam talian daripada ancaman keselamatan melalui pengesahan identiti, penyulitan dan tandatangan digital.

Meningkatkan tahap kepercayaan pengguna untuk melaksanakan transaksi secara dalam talian bagi sebarang urusan Kerajaan.

Skop Perkhidmatan MyGPKI

1 Pengurusan dan Pembekalan Sijil Digital Pengguna

- Token
- *Soft Certificate*
- *Roaming Certificate*

2 Pengurusan dan Pembekalan Sijil Digital Pelayan

- *Single Domain EV*
- *Multi Domain OV*
- *Wildcard OV*

3 Perkhidmatan Meja Bantuan dan Khidmat Sokongan Teknikal

4 Khidmat Nasihat dan Konsultasi bagi Penggunaan PKI

2.1: Pengenalan Perkhidmatan MyGPKI

Transformasi Perkhidmatan MyGPKI

2002

Kad Pintar
Sijil digital disimpan di dalam kad pintar. Key Lenght:1024 bit

ivest client
ivest client diperkenalkan bagi membolehkan kad pintar yang dibekalkan dibaca oleh Sistem ICT

2009

Soft Certificate
Sijil digital disimpan di dalam medium storan pengguna

RA Portal
RA Portal diperkenalkan bagi pengurusan sijil digital *soft certificate*

2011

Sistem GPKI 1.0
Sistem GPKI 1.0 dan MAMPU GPKI Agent 1.0 diperkenalkan bagi pengurusan perkhidmatan GPKI

2012

Roaming Certificate
Sijil digital disimpan di dalam pelayan perayauan dan akan dimuat turun ke komputer pengguna jika digunakan.

2014

Kad Pintar
Sijil digital disimpan di dalam kad pintar. Key Length:2048 bit

Token
Sijil digital disimpan di dalam kripto token

2015

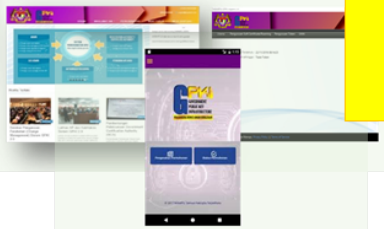
GPKI Mobile Client 1.0
GPKI Mobile Client 1.0 diperkenalkan

2016

Sistem GPKI 1.1
MAMPU GPKI Agent 1.1 diperkenalkan bagi menggantikan SCAN GPKI Agent 1.0

2017

Sistem GPKI 2.0
Sistem GPKI 2.0, MAMPU GPKI Agent 2.0 dan GPKI Mobile Client 2.0 diperkenalkan bagi menggantikan Sistem GPKI 1.0



Menu Permohonan Sijil Digital Pelayan diperkenalkan (hanya sijil *Single Domain* sahaja)

2020

Sistem GPKI 3.0
1. GPKI Agent 3.0 Release 1.0.0.0
2. Sistem GPKI Desk
3. Sistem GPKI eLearning
4. GPKI Mobile
5. Multi token:
   - Token ST3
   - Secure Token ST3 ACE
   - SafeNet eToken 5110
6. Multi Algo (RSA, ECC)

2021 - kini

Sistem GPKI 3.0
GPKI Agent 3.0 Release 1.0.0.1 dan Secure Token ST3 ACE mula digunakan
Pengenalan OTP + Roaming Certificate

- **Permohonan Sijil Digital Pelayan untuk semua jenis sijil *Single Domain EV, Multi Domain OV* dan *Wildcard OV***
- **12 Menu tambahan - permohonan pembatalan sijil, semak status , kemaskini penerimaan dan pemasangan, kemaskini profil pegawai, tukar dan reset kata laluan**

2.1: Pengenalan Perkhidmatan MyGPKI

Penggunaan Perkhidmatan MyGPKI – Sijil Digital Pelayan

JPM 595 subdomain	KKM 318 subdomain	MoF 173 subdomain	MoHR 69 subdomain	MoE 55 subdomain
MoT 53 subdomain	MoHA 385 subdomain	KPWKM 36 subdomain	KPKT 66 subdomain	KeTSA 54 subdomain
KBS 20 subdomain	KASA 54 subdomain	KPDNHEP 40 subdomain	MoSTI 75 subdomain	MED 4 subdomain
MoHE 10 subdomain	MOTAC 1 subdomain	KKMM 77 subdomain	MPIC 10 subdomain	KPLB 62 subdomain	MAFI 12 subdomain
MoD 1 subdomain	MEDAC 21 subdomain	PERPADUAN 1 subdomain	KKR 1 subdomain	MITI 0 subdomain	KLN 0 subdomain

25 kementerian

350 Pentadbir SSL

2,193 subdomain

4 Certification Authority (CA)

3 prinsipal

2.1: PENGENALAN PERKHIDMATAN MyGPKI

Certification Authority (CA)

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

Prinsipal

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

TRUSTGATE → Semua jenis → GeoTrust powered by digicert

POS Digicert → Multi domain dan Wildcard → Entrust Datacard

POS Digicert → Single Domain EV → GlobalSign GMO INTERNET GROUP

TM Applied Business → Semua jenis → GlobalSign GMO INTERNET GROUP

RAFFTECH → Semua jenis → GlobalSign GMO INTERNET GROUP

Prinsipal Lain

*** Tidak termasuk**

Symantec Website Security, digicert, Norton SECURED, GeoTrust, RapidSSL, thawte, VeriSign, SECTIGO FORMERLY COMODO CA, GoDaddy

2.2: DASAR DAN PENERANGAN UMUM MENGENAI SIJIL DIGITAL PELAYAN

PERNYATAAN DASAR

KERAJAAN MALAYSIA

PEKELILING KEMAJUAN PENTADBIRAN AWAM
BILANGAN 3 TAHUN 2015

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

JABATAN PERDANA MENTERI
MALAYSIA

23 OKTOBER 2015

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

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

Pekeliling Kemajuan Pentadbiran Awam
Bil. 3/2015

PRINSIP PEGANGAN PELAKSANAAN GPKI

(Pekeliling Kemajuan Pentadbiran Awam Bil. 3/2015)

SIJIL DIGITAL PELAYAN

PRINSIP PEGANGAN PELAKSANAAN GPKI

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 **tanggungan agensi** berkenaan dengan menggunakan sijil yang dikeluarkan oleh **Pihak Berkuasa Pemerakuan Berlesen (CA)** yang **dilantik** oleh kerajaan menerusi **Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM)**

Nota:

- **Baharu - Sistem ICT baharu yang dibangunkan secara outsource, perlu mengambil kira kos pemasangan SSL dalam kontrak masing-masing**
- **Sistem ICT yang dibangunkan secara inhouse, kos pemasangan SSL akan ditanggung oleh Agensi Pusat**
- **Agensi boleh menggunakan SSL sumber terbuka (Open Source) bagi pelayan selain pelayan produksi**

PRINSIP PEGANGAN PELAKSANAAN GPKI

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 tanggungan agensi berkenaan

6. Agensi pelaksana yang **berubah taraf** daripada agensi persekutuan **kepada agensi swasta** atau **badan berkanun**, semua kos perkhidmatan GPKI adalah di bawah tanggungan agensi berkenaan

2.2: DASAR DAN PENERANGAN UMUM MENGENAI SIJIL DIGITAL PELAYAN

PEMATUHAN KEPADA DASAR

Pekeliling Kemajuan Pentadbiran Awam Bil. 3/2015: Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (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 (contoh: Suruhanjaya Integriti Agensi Penguatkuasaan - EAIC)
		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

2.3 JENIS-JENIS SIJIL YANG DIBEKALKAN OLEH PERKHIDMATAN MyGPKI

Nota:

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

EV

Extended Validation

LENGKAP

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

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

INTERNET | **INTRANET**

TINGGI — **TAHAP KESELAMATAN DAN KEPERCAYAAN** — RENDAH

DALAMAN

2.3 JENIS-JENIS SIJIL YANG DIBEKALKAN OLEH PERKHIDMATAN MyGPKI

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

✔ **DIPERLUKAN** ✘ **TIDAK DIPERLUKAN**

2.3 JENIS-JENIS SIJIL YANG DIBEKALKAN OLEH PERKHIDMATAN MyGPKI

JENIS SIJIL DIGITAL PELAYAN	NILAI WARANTI MAKSIMUM MENGIKUT PRINSIPAL		
	ENTRUST	GlobalSign by GMO	GeoTrust
SINGLE DOMAIN (EV)	100 Ribu (USD)	1.5 Juta (USD)	1.5 Juta (USD)
MULTI DOMAIN (OV)	100 Ribu (USD)	1.25 Juta (USD)	1.25 Juta (USD)
WILDCARD (OV)	100 Ribu (USD)	1.25 Juta (USD)	1.25 Juta (USD)

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

MyGPKI GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Permohonan Sijil Digital Pelayan

3.1: PROSES PERMOHONAN SIJIL DIGITAL PELAYAN

3.2: KRITERIA DAN PRA SYARAT

3.3: PENILAIAN RISIKO

3.4: PENJANAAN FAIL CERTIFICATE SIGNING REQUEST (CSR)

3.1: PROSES PERMOHONAN SIJIL DIGITAL PELAYAN

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

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

- 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 MyNIC)
- Muat naik "**Surat Permohonan Sijil Digital Pelayan"**

03 Pentadbir (Admin MAMPU) semak dan membuat **kelulusan**

04 CA **memproses permohonan** sijil digital dengan Prinsipal

05 Prinsipal melaksanakan proses **pengesahan (eVetting)** dengan Pegawai 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**

06 Prinsipal/CA membuat **penjanaan** sijil digital

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

07 CA akan **menghantar** sijil digital melalui e-mel kepada Pegawai Agensi

08 Pegawai Agensi **kemas kini maklumat penerimaan** di Portal GPKI

- 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

09 Pegawai Agensi membuat pemasangan sijil digital dan **kemas kini tarikh dan taraf pemasangan** di Portal GPKI

3.2: KRITERIA DAN PRA SYARAT

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

MyGPKI GOVERNMENT PUBLIC KEY INFRASTRUCTURE

1 KESELAMATAN

Pelayan Sistem ICT perlu tahap kawalan keselamatan yang tinggi kerana mengandungi maklumat rahsia rasmi.

2 CAPAIAN SISTEM

Melalui internet (Public) sahaja dan tidak termasuk Intranet.

3 MAKLUMAT DOMAIN PELAYAN

Maklumat telah wujud dan telah didaftarkan dengan pendaftar domain (MyNIC)

4 JANA CERTIFICATE SIGNING REQUEST (CSR)

Sediakan janaan Permintaan Tandatangan Sijil - CSR

5 SELEPAS KELULUSAN

Nama domain dan jenis sijil digital pelayan tidak boleh diubah.

6 PERMOHONAN PEMBAHARUAN

Hanya 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

3.3: PENILAIAN RISIKO

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

Portal GPKI https://gpki.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)

Kelulusan penilaian risiko perlu diperolehi terlebih dahulu untuk **menentukan jenis sijil digital pelayan** yang sesuai sebelum permohonan di Portal GPKI dilaksanakan

PENILAIAN RISIKO LAMAN WEB SEKTOR AWAM DALAM KONTEKS PERKHIDMATAN GPKI (SIJIL DIGITAL PELAYAN)

Penilaian Risiko ini bertujuan untuk:
1. Mengenal pasti kawalan keselamatan yang sesuai bagi keperluan perkhidmatan GPKI
2. Menentukan penggunaan sijil digital pelayan sama ada bagi tujuan pengesahan identiti dan penyulitan maklumat
3. Mengenal pasti keperluan kategori dan jenis sijil digital pelayan yang diperlukan oleh agensi berdasarkan tahap risiko

Bil.	Nama Domain	Data / Maklumat Terlibat	Klasifikasi Data / Maklumat	Nilai Data	Kawalan Sedia Ada	Ancaman Keselamatan	Keterangan Ancaman
	<Nama domain atau subdomain>	< Data / maklumat terlibat perlulah dinyatakan dengan jelas dan terperinci bagi menggambarkan klasifikasi maklumat yang telah ditetapkan. Maklumat ini akan menjadi pemberat / penentu kepada tahap risiko dan jenis sijil digital pelayan yang diperlukan oleh agensi.	<Nyatakan klasifikasi data atau maklumat. Rujuk Jadual 2: Klasifikasi Data/Maklumat>	<Nyatakan nilai data atau maklumat. Rujuk Jadual 3: Nilai Data/Maklumat>	<Nyatakan kawalan semasa yang telah dilaksanakan bagi mengurangkan risiko ancaman keselamatan>	<Nyatakan ancaman keselamatan yang berkemungkinan atau telah berlaku terhadap data atau maklumat. Rujuk Jadual 4: Keterangan Ancaman Keselamatan Maklumat>	<Nyatakan keterangan ancaman keselamatan yang berkemungkinan atau telah berlaku terhadap data atau maklumat>
1	www.mampu.gov.my	Portal MAMPU yang mengandungi maklumat umum aktiviti organiasasi 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 tandaan masa dan maklumat pengguna. Sistem DTS memainkan peranan dalam memastikan sesuatu transaksi atau maklumat adalah SAHIH wujud pada masa yang dinyatakan.	Sulit	Tinggi	Pemasangan sijil digital pelayan single domain EV dan pengguna login ID dan katalaluan	*HTTPS Spoofing* *SSL hijacking* *Penyamaran Identiti (Identity Spoofing)* *Pengubahsuaian 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 pengubahsuaian data dalam pangkalan data dan mengubah data dalam transit antara dua komputer.
3	latihan.dts.gov.my	Mengandungi maklumat pengguna dan rekod tandaan masa bukan yang sebenar (dummy data) yang digunakan untuk memberikan 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 tandaan masa pengujian (dummy data) yang digunakan untuk memastikan proses transaski berjaya dilaksanakan.	Terhad	Sederhana	Self Signed Certificate	*HTTPS Spoofing* *Pengubahsuaian 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

1. LATAR BELAKANG AGENSI | 2. LATAR BELAKANG LAMAN WEB | 3. PENILAIAN RISIKO | JADUAL 1 | JADUAL 2 | JADUAL 3 | JADUAL 4 | JADUAL ...

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

APA ITU PERMINTAAN TANDATANGAN SIJIL *CERTIFICATE SIGNING REQUEST* (CSR) ?

- **Satu langkah/kaedah** untuk mendapatkan **sijil digital pelayan** (SSL/TLS) bagi domain/ subdomain
- **Dijana pada pelayan** bagi domain/ subdomain yang perlu dipasang sijil digital pelayan
- Mengandungi **maklumat yang akan digunakan** oleh CA dan prinsipal untuk **menjana sijil** dan **maklumat akan dipaparkan di browser pengguna**
- Mengandungi **kunci awam** yang akan disertakan dalam sijil digital pelayan dan **ditandatangani dengan kunci persendirian (private key)** yang sepadan

SYARAT PENJANAAN CSR

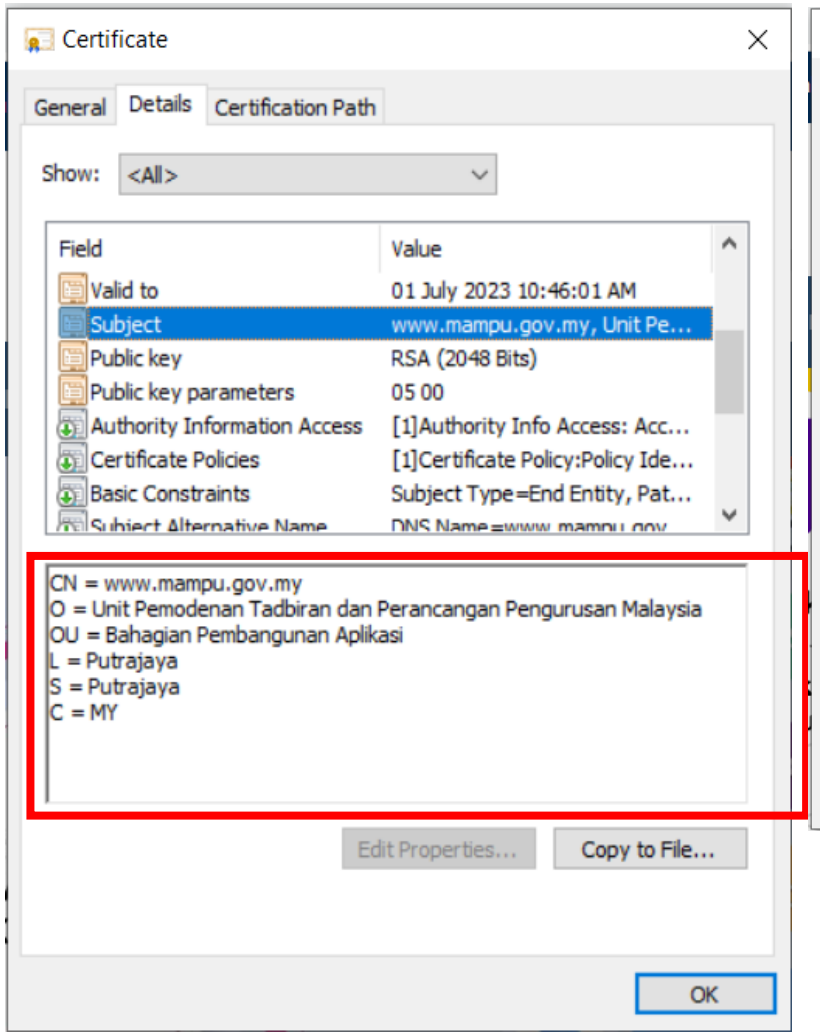
1. Fail CSR yang akan dijana **MESTI** sama dengan maklumat domain yang **TELAH** didaftarkan dengan **Pendaftar Domain (MyNIC)**.
2. Saiz fail hendaklah **kurang daripada 2MB.**
3. Fail CSR mestilah mempunyai jenis kunci **RSA SHA2** dan panjang kunci **2048 bit ke atas**.

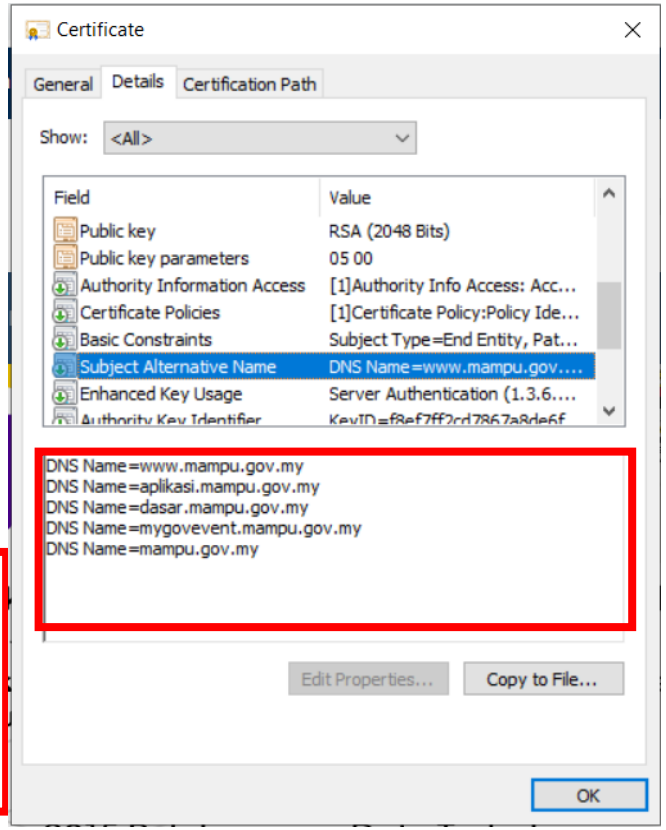
Contoh Format Kandungan CSR (Base-64 code)

-----BEGIN CERTIFICATE REQUEST-----
MIIDYjCCAkoCAQAwgb0xCzAJBgNVBAYTAk1ZMREwDwYDVQQIDAhTZWxhbmdvcjES
MBAGA1UEBwwJQ3liZXJqYXlhMUQwQgYDVQQKDDtVbml0IFBlbW9kZW5hbiBUYWRi
aXJhbiBkYW4gUGVyYW5jYW5nYW4gUGVuZ3VydXNhbiBNYWxheXNpYTEmMCQGA1UE
CwwdQmFoYWdpYW4gUGVtYmFuZ3VuYW4gQXBsaWthc2kxGTAXBgNVBAMMEHd3dy5t
YW1wdS5nb3YubXkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDFLyfN
x1zUgGtOjEccJgWpI7+l3Qu23xYryJU9tzzeSgCKEIxkSZ8gghsIa/wHFMG2OyYI
kT99SjwLERDVfLLoPGK56G/7jjhU7YWCdqnTkdtSVxXlst7xXHM64uWLcyUJZ50R
VnOzBR/OBnwUyPd4Q5PzccBsdw0HqLLirQu7V4xhDvQ5fXzUsZU5zpaMtWsRkmZX
WAo8inYSi3ZJOS9in6DLrablYhkyDWUieOyWdLkixx8JbPes/NuzVbew2ufmYXVJ
qbJBYfpmQmMF91uEQl2RZk8V/HhwGtlnuExNVBd+QaL+3TC09qAwddlzJMJH14+d
AO9xHgmgqnyC0qKVAgMBAAGgXzBdBgkqhkiG9w0BCQ4xUDBOMDQGA1UdEQQtMCuC
FWFwbGlrYXNpLm1hbXB1Lmdvdi5teYISZGFzYXIubWFtcHUuZ292Lm15MAkGA1Ud
EwQCMAAwCwYDVR0PBAQDAgXgMA0GCSqGSIb3DQEBCwUAA4IBAQB+vPzy3EQtfWMZ
wF+De2n7N6Kb4/3cQdSeImK3qwOKoTSYA77r58LjumQbareZ869j8/5AxCDBwONU
rUnsB4xie+hnBVGgEnVU5zHkALKhxnSu9X+q4ExwcK93wEejxzM9JD104l/+DWbO
+4wAceW7p3jdX0JG4M7g6dbnmi9rs/LUrOc4gLjjFWZYPYI0DODhY84/2gziQVrr
X3QpJnmkmeCEDkt28SEqb3+m/dYpqZU9ieEUz1oTXgJjBBjxPJM8qoCg9kQXl3Wk
CQ2tclryQ1B0BWm1OzlPHCUzN0zS+dZIJqFYByTPAFVNq2N5ds+70U/yKCxSk9+k
tlERN1YN
-----END CERTIFICATE REQUEST-----

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

KOD CSR	KETERANGAN
Common Name (CN)*	Nama domain/subdomain (FQDN) pada pelayan (hanya **64 aksara sahaja** termasuk simbol noktah). Tidak boleh simbol **underscore – Standard RFC1035**
Organisation (O)*	Nama organisasi (**Nama penuh agensi**). Tidak digalakkan untuk menggunakan simbol khas bagi mengelakkan ralat semasa permohonan di portal prinsipal
Organisation Unit (OU)	Nama unit bagi organisasi (**Nama penuh unit/bahagian**) Tidak digalakkan untuk menggunakan simbol khas bagi mengelakkan ralat semasa permohonan di portal prinsipal
City/ Locality (L)*	Bandar bagi organisasi
State (S)*	Negeri bagi organisasi
Country (C):	Kod antarabangsa bagi negara
Email Address	Alamat e-mel bagi organisasi
Subject Alternative Names (SANs)	Paparan bagi sijil digital pelayan jenis multi domain





3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

PENJANAAN CSR MENGIKUT *CRYPTO LIBRARY TOOL* & *WEB SERVICE*

BIL.	*CRYPTO LIBRARY TOOL*	*WEB SERVICE*	JENIS SIJIL DIGITAL PELAYAN	FAIL YANG PERLU DIJANA
1.	OpenSSL	• Apache HTTP Server • NGINX	• *Single Domain* • *Multi Domain* • *Wildcard*	• Fail Private Key: *.key / *.pem • Fail CSR
2.	JSSE (Keytool)	• Apache Tomcat • JBoss (Wildfly) • Weblogic	• *Single Domain* • *Multi Domain* • *Wildcard*	• Fail Private Key: *.ks /*.jks (keystore) • Fail CSR
3.	IBM Java SDK (iKeyMan)	• IBM HTTP Server • Websphere	• *Single Domain* • *Wildcard*	• Fail Private Key: *.kdb • Fail CSR
4.	Mozilla NSS (certutil)	• Sun Java Web Server	• *Single Domain* • *Wildcard*	• Fail CSR
5.	SChannel	• Microsoft IIS • Microsoft Exchange	• *Single Domain* • *Multi Domain* • *Wildcard*	• Fail CSR

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

BIL.	*CRYPTO LIBRARY TOOL*	FAIL YANG DIPERLUKAN	KAEDAH KONFIGURASI	RUJUKAN
1.	OpenSSL ***Web Service*** • Apache HTTP Server • Nginx	**Fail yang perlu dijana** • Fail Private key = domain.key • Fail CSR= domain.csr **Fail yang diperlukan semasa instalasi** • 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	**Jana Private Key dan CSR untuk Single Domain /Wildcard (tanpa SANs)** 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" **Jana Private Key dan CSR untuk Multi Domain (dengan SANs)** 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** *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 **Instalasi** • Cari dan konfigurasi fail httpd.conf / conf.d / ssl.conf di pelayan ➢ SSLCertificateFile /path/to/**domain.cer** ➢ SSLCertificateKeyFile /path/to/**domain.key** ➢ SSLCertificateChainFile /path/to/**cacert.cer** • Restart Apache (systemctl restart httpd or apachectl –k restart)	• **Read DER file** openssl x509 -text -noout -in domain.cer • **Read PEM file** openssl x509 -text -noout -in domain.pem • **Convert DER (.crt .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 https://www.sslshopper.com/article-most-common-openssl-commands.html

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

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)

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

Cypto Library Tool: OpenSSL

Jenis Algoritma: RSA
Panjang kunci: 2048
Jenis kunci: SHA2

Request

Fail private key yang akan dijana

Fail CSR yang akan dijana

Maklumat kandungan dalam CSR

baca kandungan fail *.conf untuk tambah SANs

```
openssl req -new -newkey rsa:2048 -sha256 -nodes
-keyout www.mampu.gov.my2022.key
-out www.mampu.gov.my2022.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
```

How to Create a CSR in Apache OpenSSL

(https://www.youtube.com/watch?v=ZAE9p1_N6_Q)

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

BIL.	*CRYPTO LIBRARY TOOL*	FAIL YANG DIPERLUKAN	KAEDAH KONFIGURASI	RUJUKAN
2.	JSSE (Keytool) ***Web Service*** • Apache Tomcat • JBoss (Wildfly) • Weblogic **Bersambung seterusnya...**	**Fail yang perlu dijana** • Fail Private key = domain.ks/ domain.jks (keystore) • Fail CSR= domain.csr **Fail yang diperlukan semasa instalasi** • 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	**Jana Private Key untuk Single Domain /Wildcard (tanpa SANs)** 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" **Jana CSR untuk Single Domain /Wildcard (tanpa SANs)** keytool -certreq -keyalg RSA -sigalg SHA256withRSA -alias **domain** -keystore **privateKey.jks** -file **domain.csr** **Jana Private Key untuk Multi Domain (dengan SANs)** keytool -genkey -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -alias **domain** -keystore **privateKey.jks** -dname "CN=www.mampu.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" **Jana CSR untuk Single Domain /Wildcard (dengan SANs)** 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** *Nota: 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	• **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

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

BIL.	*CRYPTO LIBRARY TOOL*	FAIL YANG DIPERLUKAN	KAEDAH KONFIGURASI	RUJUKAN
2.	JSSE (Keytool) ***Web Service*** • Apache Tomcat • JBoss (Wildfly) • Weblogic		**(sambungan...)** **Instalasi** • Save domain/subdomain certificate as **domain.cer** or **domain.crt** • Save Intermediate (CA) cert as cacert.cer or **cacert.crt** • Save Root cert as root.cer or root.crt • RUN: keytool -import -alias root -keystore **privateKey.jks** -trustcacerts -file **root.cer** • RUN: keytool -import -alias inter -keystore **privateKey.jks** –trustcacerts -file **cacert.cer** • RUN: keytool -import -alias **domain** -keystore **privateKey.jks** –file **domain.cer** • Update server.xml (Prior Tomcat 8.5) <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" scheme="https" secure="true" SSLEnabled="true" keystoreFile="/path/to/**privateKey.jks**" keystorePass="~~changeit~~“ clientAuth="false" sslProtocol="TLS“ sslEnabledProtocols="TLSv1.3,TLSv1.2" .../> • Update server.xml (Tomcat 8.5 and later) <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="~~changeit~~" certificateKeyAlias=“domain" type="RSA"/> </SSLHostConfig> </Connector> • Restart Tomcat (systemctl restart tomcat)	

Cypto Library Tool: Keytool

Generate private key

Jenis Algoritma: RSA
Panjang kunci: 2048
Jenis kunci: SHA2

Fail private key yang akan dijana

Maklumat kandungan dalam CSR

```
keytool -genkey -keyalg RSA -sigalg
SHA256withRSA -keysize 2048 -alias domain –
www.mampu.gov.my2022.jks -dname
"CN=www.mampu.gov.my, O=Unit Pemodenan
Tadbiran dan Perancangan Pengurusan Malaysia,
OU=Bahagian Pembangunan Aplikasi, L=Cyberjaya,
S=Selangor, C=MY"
```

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

Certificate request

Jenis Algoritma: RSA
Panjang kunci: 2048
Jenis kunci: SHA2

Fail private key yang akan dipadankan

Extension tambah SANs

Fail CSR yang akan dijana

```
keytool -certreq -keyalg RSA -sigalg
SHA256withRSA -alias domain
-keystore www.mampu.gov.my2022.jks
–ext “SAN=DNS:subdomain2.domain.gov.my,
DNS:subdomain3.domain.gov.my,DNS:subdomain4.
domain.gov.my”
-file www.mampu.gov.my2022.csr
```

How to Create a Java Key Store and Generate a CSR

https://www.youtube.com/watch?v=KPkPWx07zA8

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

BIL.	*CRYPTO LIBRARY TOOL*	FAIL YANG DIPERLUKAN	KAEDAH KONFIGURASI	RUJUKAN
3.	IBM Java SDK (iKeyMan) ***Web Service*** • IBM HTTP Server • Websphere	**Fail yang perlu dijana** • Fail Private key = domain.kdb • Fail CSR= domain.csr **Fail yang diperlukan semasa instalasi** • 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	**Jana New Certificate Database untuk Single Domain /Wildcard (tanpa SANs)** gskcapicmd -keydb -create -db **privateKey.kdb** -pw password –type cms -stashpw **Jana CSR – Single Domain /Wildcard (tanpa SANs)** gskcapicmd -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** *Nota: 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 **Instalasi (Tambah Certificate to Database)** • gskcapicmd -cert -receive -db **privateKey.kdb** -pw password -format ascii -file **domain.cer** -default_cert yes • gskcapicmd -cert -add -db **privateKey.kdb** -pw password -format ascii -file **cacert.cer** • Configure httpd.conf ➢ 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	• **Convert KDB to PFX** gskcapicmd -cert -export -db domain.kdb -pw password -label servername - type cms -target server.pfx -target_pw password -target_type pkcs12 • **Convert PFX to KDB** gskcapicmd -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** gskcapicmd -cert -details -db domain.kdb -pw password -label servername • **Extract a certificate from a key database** gskcapicmd -cert -extract -db domain.kdb -pw password -label servername - target server.cer -format ascii • **List all certificates in a key database** gskcapicmd -cert -list all | personal | CA

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

BIL.	*CRYPTO LIBRARY TOOL*	FAIL YANG DIPERLUKAN	KAEDAH KONFIGURASI	RUJUKAN
4.	Mozilla NSS (certutil) ***Web Service*** • Sun Java Web Server • Oracle iPlanet Web Server	**Fail yang perlu dijana** • Fail CSR= domain.csr **Fail yang diperlukan semasa instalasi** • 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	**Jana New Certificate Database untuk Single Domain /Wildcard (tanpa SANs)** certutil -N -d /path/to/certdir **Jana CSR untuk Single Domain /Wildcard (tanpa SANs)** 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** **Instalasi (Tambah Certificate to Database)** • 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 *Nota: 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	• **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 https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/tools/NSS_Tools_certutil

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

BIL.	*CRYPTO LIBRARY TOOL*	FAIL YANG DIPERLUKAN	KAEDAH KONFIGURASI	RUJUKAN
5.	SChannel (MMC2 Command) ***Web Service*** • Microsoft IIS • Microsoft Exchange	**Fail yang perlu dijana** • Fail CSR= domain.csr • Fail Private key = dijana secara build–in dalam webserver (perlu pilih enable export sekiranya perlu pasang pada subdomain lain – wildcard) **Fail yang diperlukan semasa instalasi** • Fail domain/ subdomain certificate = domain.crt/ domain.cer • Fail intermediate CA = cacert.crt/ cacert.cer • Fail root certificate CA = root.crt/root.cer **ATAU** • Fail certificate dalam format PFX (import certificate dari pelayan lain dan covert menggunakan openSSL) = domain.pfx	**Jana CSR untuk Single Domain /Wildcard** • Menggunakan **MMC2 Command** **Instalasi** • Menggunakan **MMC2 Command** **Jana CSR untuk Multi Domain (hanya Ms Exchange Sahaja)** • Menggunakan **Exchange** **Instalasi** • Menggunakan **Exchange** Sekiranya pemasangan multidomain, private key perlu ditukar format ke PKCS#12 terlebih dahulu sebelum diimport masuk ke server Windows menggunakan **format *.pfx** ❖ Convert dan gabungkan key, subdomain/domain certificate dan CA certificate ke format PFX (import masuk ke IIS untuk multi domain atau wildcard) openssl pkcs12 -export -out domain.pfx -inkey domain.key -in domain.crt -certfile ca_bundle.crt	• **MMC2 Command** Sekiranya penjanaan menggunakan MMC2 command maka instalasi juga perlu menggunakan kaedah MMC2 command juga. https://medium.com/@yildirimabdrhm/how-to-create-sha256-csr-on-windows-739cba893fae https://www.tbs-certificates.co.uk/FAQ/en/windows-install-mmc.html#volet

How to Create a Certificate Signing Request (CSR) in Microsoft Management Console (MMC) Windows 2012

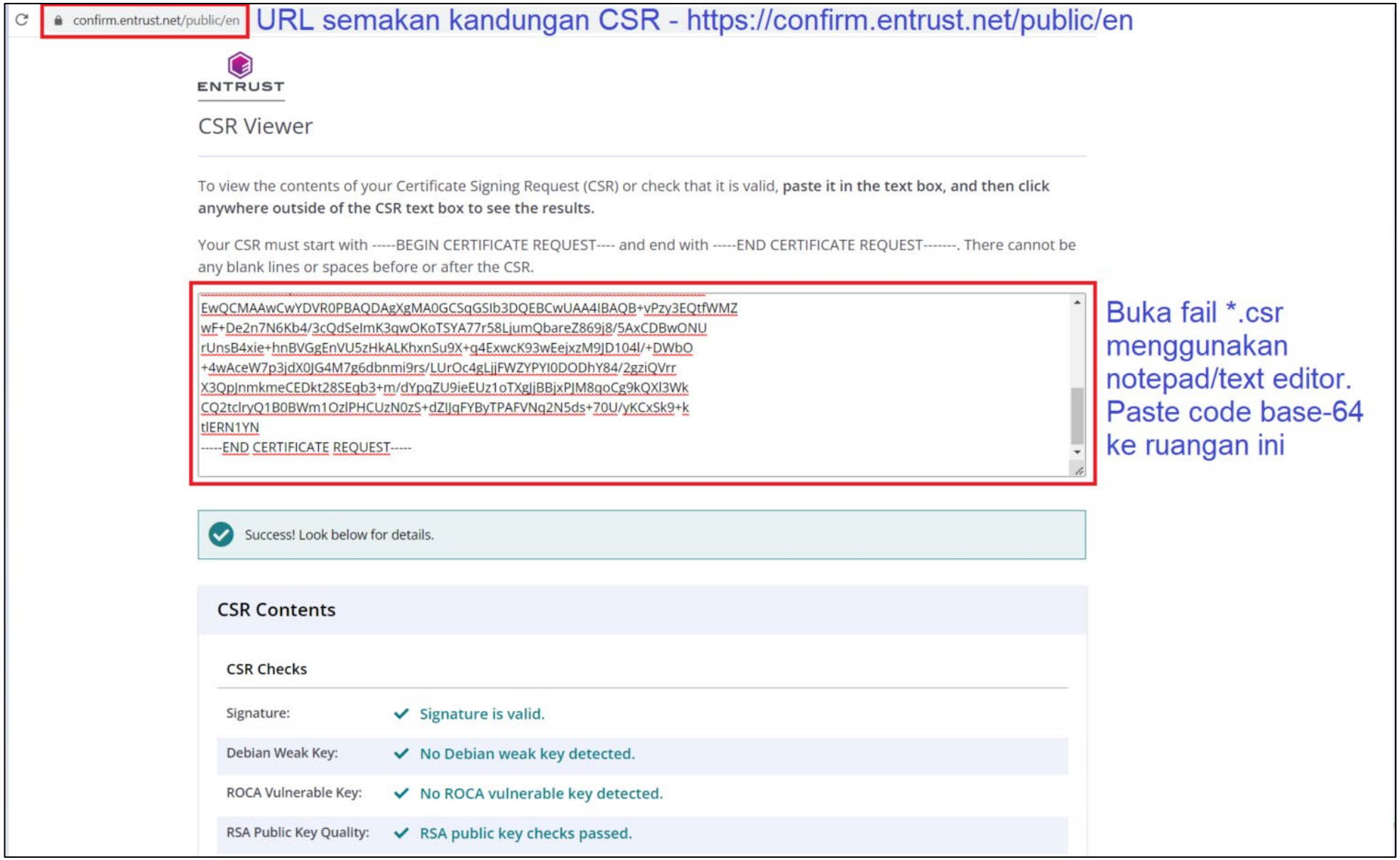
(https://www.youtube.com/watch?v=W2-IphtGcZU)

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

Semakan Kandungan CSR

TOOLS

- https://confirm.entrust.net/public/en
- https://www.digicert.com/ssltools/view-csr/
- https://www.sslshopper.com/csr-decoder.html
- https://comodosslstore.com/ssltools/csr-decoder.php
- https://certlogik.com/decoder/



Nama domain/subdomain (FQDN) pada pelayan dan hanya terhad **64 aksara sahaja** termasuk simbol noktah). Tidak boleh **underscore (Standard RFC1035)**

Subject	
Common Name:	www.mampu.gov.my
Organizational Unit:	Bahagian Pembangunan Aplikasi
Organization:	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
Locality:	Cyberjaya
State:	Selangor
Country:	MY
Subject Alternative Names:	aplikasi.mampu.gov.my (dNSName)
	dasar.mampu.gov.my (dNSName)

Nama penuh agensi kerana mewakili imej agensi/jabatan kerajaan

dua aksara kod negara

Dikenali sebagai SANs dan hanya akan dipaparkan bagi sijil digital pelayan jenis multi domain. Paparan SANs dapat ditetapkan dalan fail *.cnf/ san.conf/ ssl.conf semasa jana CSR

Properties	
Key Type:	RSA
Key Size:	2048
Signature Type:	sha256WithRSAEncryption
Fingerprint (MD5):	B1:DE:DB:3D:C0:C1:52:69:48:15:81:50:2B:08:99:C0
Fingerprint (SHA-1):	74:D1:76:B2:52:85:24:2B:8E:30:56:96:82:24:2D:36:56:1A:FB:92

perlu memenuhi syarat minimum yang ditetapkan

kunci awam sijil digital pelayan

digicert.com/kb/csr-creation.htm

digicert®

Support

Award-Winning Customer Service

Create a CSR (Certificate Signing Request)

General CSR Creation Guidelines

Before you can order an SSL certificate, it is recommended that you generat server or device. Learn more about SSL certificates »

A CSR is an encoded file that provides you with a standardized way to send D information that identifies your company and domain name. When you gene following information: common name (e.g., www.example.com), organizatic city/town), key type (typically RSA), and key size (2048-bit minimum).

If you aren't sure of the exact company name or location when you generate that information during our review process before we issue the certificate.

Once your CSR is created, you'll need to copy and paste it into the online orc certificate. Online Certificate Order Form »

Search the knowledgebase...

Not sure which SSL certificate you need? »

Common Platforms & Operating Systems

Microsoft IIS

entrust.com/resources/certificate-solutions...

ENTRUST

OPEN SSL CSR COMMAND BUILDER

The first step in requesting an SSL certificate for your Apache based Web server, is to generate a Certificate Signing Request (CSR) using an OpenSSL command that contains information about your identity. Entrust has created this page to simplify the process of creating this command. Please fill out the following form and click **Generate** to obtain the OpenSSL command.

Common Name	
Organization	
Organizational Unit	
Country	United States
State	Select State
City	
Key Size	RSA 2048 (recommended)
Key Store File Name	
CSR File Name	

GENERATE

Copy the text displayed below and paste into a command line on your serve. to

support.globalsign.com/ssl/ssl-certificates-i...

GlobalSign by GMO

GlobalSign Support

Tell us what you're looking for...

GlobalSign Support
> SSL Certificates
> SSL Certificates Insta... > Generate CSR - Open...

Generate CSR - OpenSSL

Introduction

This article provides step-by-step instructions for generating a Certificate Signing Request (CSR) in OpenSSL. This is most commonly required for web servers such as Apache HTTP Server and NGINX. If this is not the solution you are looking for, please search for your solution in the search bar above.

Switch to a working directory

To generate a CSR in Apache OpenSSL, you can check the video below for a tutorial.

3.4: PENJANAAN FAIL *CERTIFICATE SIGNING REQUEST* (CSR)

DO'S

- **Kenal pasti lokasi pemasangan** terlebih dahulu sama ada di WAF, IDP, IPS, Proxy, Firewall, Load Balancer atau Web Service.
- **Kenal pasti *configuration setting* pelayan sedia ada** terlebih dahulu sebelum jana fail CSR
- Pastikan fail CSR **dijana di pelayan** (*server*) yang terlibat sahaja.

DON'TS

- **Jangan hilangkan *private key*** yang telah dijana.
- **Jangan kongsi atau dedahkan *private key*** dengan pihak lain.
- **Dilarang** menggunakan **CSR dan *private key* yang sama** dengan permohonan terdahulu.

3.8: PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN OLEH AGENSI

DO'S

DON'TS

- Pastikan **kunci persendirian (*private key*)** (key/ks/pem/jks/keystore/kdb) sijil digital pelayan **tidak hilang atau *corrupt*** dan **disimpan di tempat yang selamat**.
- Kerja-kerja pemasangan perlu **dilaksanakan sendiri oleh pegawai** di agensi atau pembekal yang **dilantik secara sah sahaja**

- **Jangan pindah milik** sijil digital pelayan dan *private key*.
- Jangan **mengedarkan atau membuat salinan sijil digital pelayan dan *private key*** kepada pihak yang tidak berkenaan

Permohonan Sijil Digital Pelayan

3.5: PERMOHONAN SIJIL DIGITAL PELAYAN DI PORTAL GPKI

3.6: PROSES PENGESAHAN (e-Vetting) OLEH PRINSIPAL

3.7: PENJANAAN DAN PENGHANTARAN SIJIL DIGITAL PELAYAN OLEH PRINSIPAL/CA

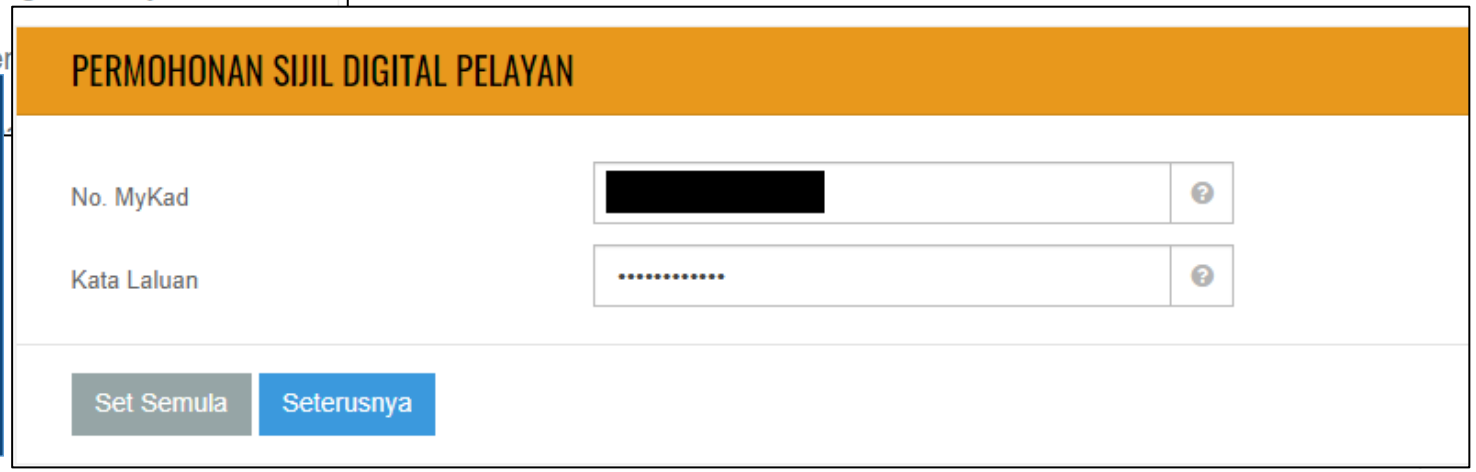
3.8: PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN OLEH AGENSI

3.5: PERMOHONAN SIJIL DIGITAL PELAYAN DI PORTAL GPKI

PORTAL GPKI

Menu **"Pendaftaran Pengguna Sijil Digital Pelayan"** hanya dibenarkan bagi permohonan sijil digital pelayan baharu untuk Pentadbir Pelayan (SSL) yang tidak pernah didaftarkan dalam Sistem GPKI.

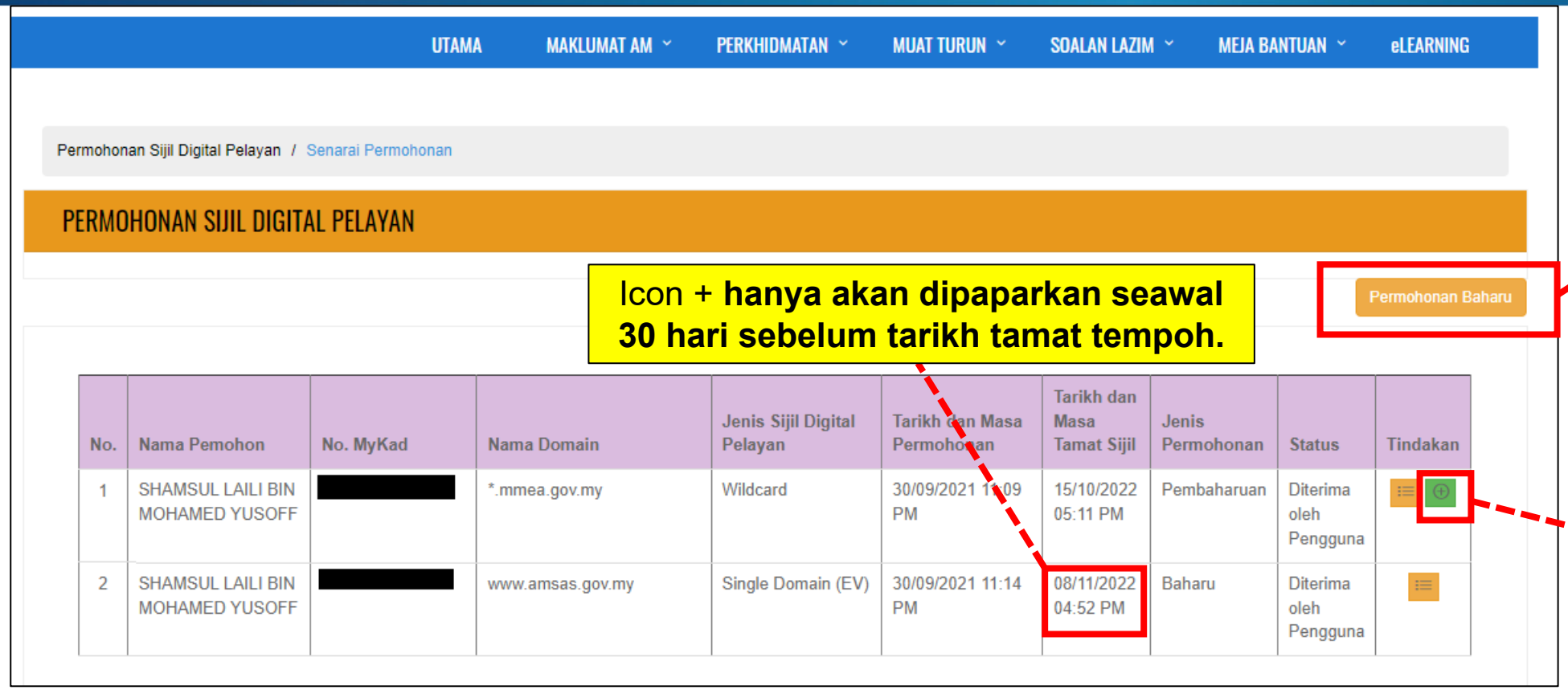
Menu **"Permohonan Sijil Digital Pelayan"** hanya boleh dicapai oleh Pentadbir Pelayan (SSL) sedia ada yang mempunyai ID (No. MyKad) dan kata laluan. Digunakan untuk membuat permohonan pembaharuan atau tambahan bagi domain/subdomain baharu.



Empat item yang perlu disediakan sebelum permohonan sijil digital pelayan dilaksanakan di Portal GPKI:

a. **Laporan penilaian risiko** yang telah diluluskan
b. **Fail CSR** yang betul
c. Maklumat **3 Pentadbir Pelayan** (SSL)
d. **Surat permohonan rasmi** dari agensi

3.5: PERMOHONAN SIJIL DIGITAL PELAYAN DI PORTAL GPKI



No.	Nama Pemohon	No. MyKad	Nama Domain	Jenis Sijil Digital Pelayan	Tarikh dan Masa Permohonan	Tarikh dan Masa Tamat Sijil	Jenis Permohonan	Status	Tindakan
1	SHAMSUL LAILI BIN MOHAMED YUSOFF	[redacted]	*.mmea.gov.my	Wildcard	30/09/2021 11:09 PM	15/10/2022 05:11 PM	Pembaharuan	Diterima oleh Pengguna	
2	SHAMSUL LAILI BIN MOHAMED YUSOFF	[redacted]	www.amsas.gov.my	Single Domain (EV)	30/09/2021 11:14 PM	08/11/2022 04:52 PM	Baharu	Diterima oleh Pengguna	

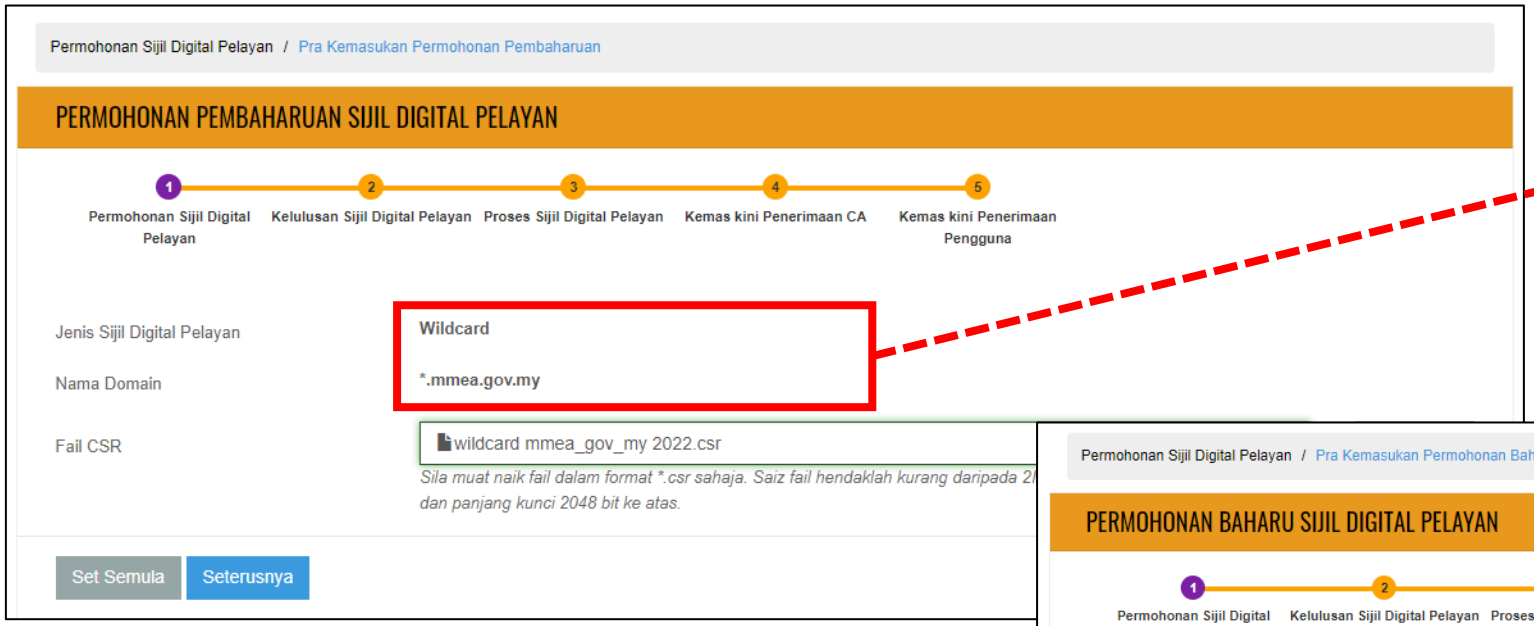
Butang **"Permohonan Baharu" digunakan untuk permohonan** domain/ subdomain tambahan yang baharu.

Icon + **digunakan untuk permohonan pembaharuan** domain/ subdomain sedia ada.

Ralat: Tiada Icon +

- Ralat icon + 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 sahaja) perlu melaksanakan **mengemas kini tarikh penerimaan dan pemasangan sijil digital pelayan sedia ada** terlebih dahulu oleh agensi.

3.5: PERMOHONAN SIJIL DIGITAL PELAYAN DI PORTAL GPKI

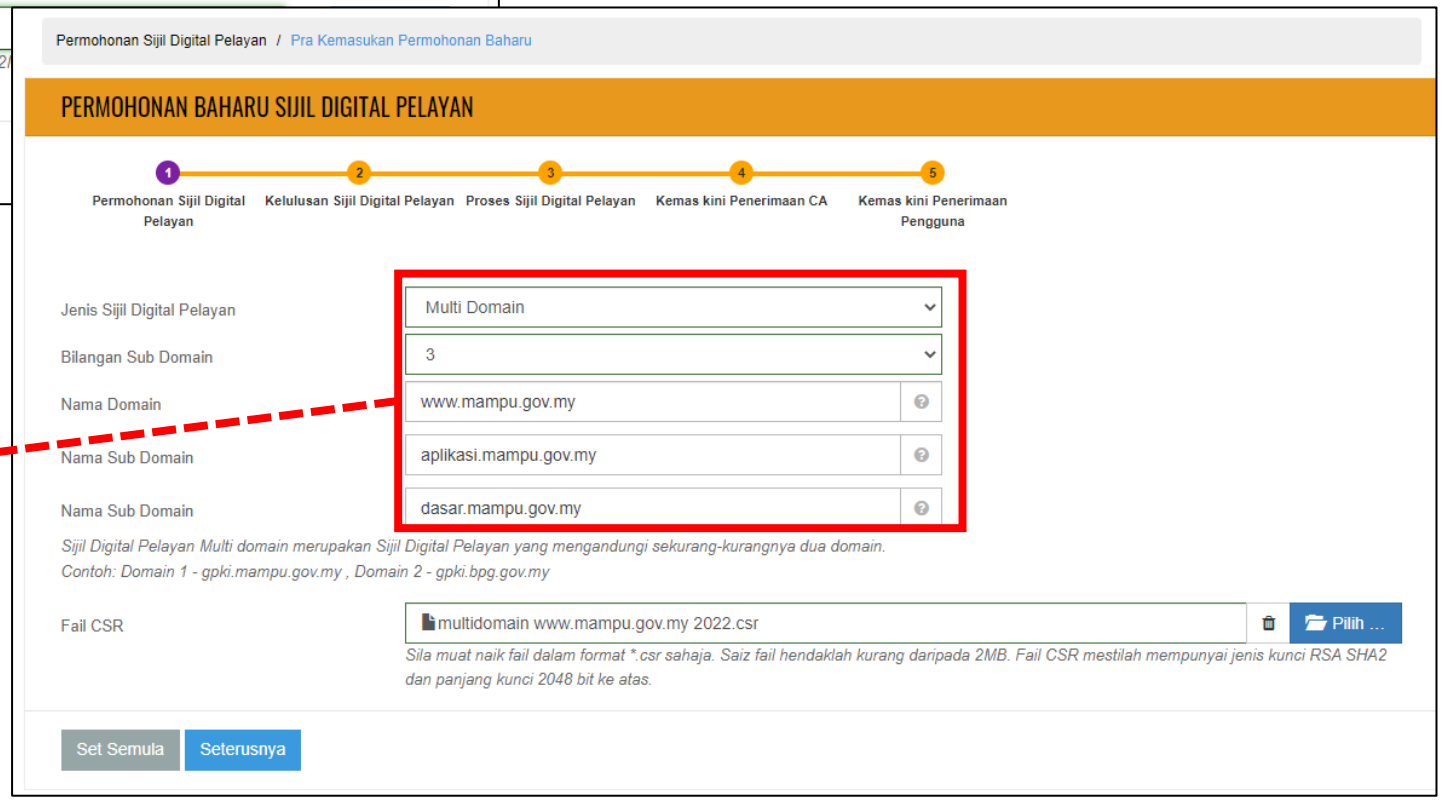


Jenis Single Domain / Wildcard

Kemasukan nama domain/subdomain **MESTILAH** sama dengan kandungan fail CSR yang telah dijana. Bagi wildcard nama domain/subdomain perlulah dimulakan dengan simbol * (contoh: *.mampu.gov.my)

Jenis Multi Domain

Kemasukan nama dan bilangan domain/subdomain **MESTILAH** mengikut susunan dalam kandungan fail CSR yang telah dijana



3.5: PERMOHONAN SIJIL DIGITAL PELAYAN DI PORTAL GPKI

PERMOHONAN PEMBAHARUAN SIJIL DIGITAL PELAYAN

1. Permohonan Sijil Digital Pelayan
2. Kelulusan Sijil Digital Pelayan
3. Proses Sijil Digital Pelayan
4. Kemas kini Penerimaan CA
5. Kemas kini Penerimaan Pengguna

Maklumat Permohonan

Jenis Permohonan	Pembaharuan
Jenis Sijil Digital Pelayan	Wildcard
Justifikasi Permohonan	Domain ini digunakan oleh APMM yang dibangunkan bagi tujuan pelbagai urusan berkaitan agensi dan mengandungi maklumat aktiviti organisasi bagi subdomain a. www.mmea.gov.my b. spm.mmea.gov.my

Maklumat Pemohon

Nama	SHAMSUL LAILI BIN MOHAMED YUSOFF
No. MyKad	[redacted]
E-mel	[redacted]
No. Telefon Pejabat	[redacted]
No. Telefon Bimbit	[redacted]
Jawatan	[redacted]
Kementerian / Agensi	AGENSI PENGUATKUASAAN MARITIM MALAYSIA
Alamat Agensi / Bahagian	KEMENTERIAN DALAM NEGERI TING 4-11,ONE IOI SQUARE, IOI RESORT 62502 WILAYAH PERSEKUTUAN PUTRAJAYA
Laporan Penilaian Risiko	MMEA _ Penilaian Risiko Laman Web Sektor Awam _Sijil Digital Pelayan_ v1.6@09092022.xlsx [Pilih ...]

Sila rujuk dan muat naik templat Laporan Penilaian Risiko berkaitan Sijil Digital Pelayan di Portal GPKI dan muat naik semula dalam format xls atau xlsx dan saiz tidak melebihi 10MB

Maklumat Pegawai Teknikal

Nama	NOOR ASMAH BINTI HALIMI (☐ Pegawai Teknikal Baharu)
No. MyKad	[redacted]
E-mel	[redacted]
No. Telefon Pejabat	[redacted]
No. Telefon Bimbit	[redacted]
Jawatan	PEGAWAI TEKNOLOGI MAKLUMAT

Maklumat Pegawai Pengesah

Nama	AIDA BINTI ZULKIFLI (☐ Pegawai Pengesah Baharu)
No. MyKad	[redacted]
E-mel	[redacted]
No. Telefon Pejabat	[redacted]
No. Telefon Bimbit	[redacted]
Jawatan	KETUA PENOLONG PENGARAH

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

Laporan penilaian risiko perlu mendapat kelulusan dan telah dimuktamadkan oleh Pentadbir GPKI terlebih dahulu.

3.5: PERMOHONAN SIJIL DIGITAL PELAYAN DI PORTAL GPKI

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

MyGPKI GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Maklumat Pelayan

Nama Domain: *.mmea.gov.my

Kriteria Pelayan : (Pilih kriteria yang tertinggi)

a. Klasifikasi Data	b. Capaian	c. Penilaian
○ Terbuka	● Internet	○ Tinggi
● Terhad	○ Intranet	● Sederhana
○ Sulit		○ Rendah
○ Rahsia		
○ Rahsia Besar		

Platform: ○ Unix ○ Linux ○ Solaris ● Window Server ○ Lain-lain

Web Service: IIS dan Apache

Surat Rasmi dari Agensi: Surat Rasmi SSL 2022 mmea.pdf [Pilih ...]

Sila rujuk dan muat turun templat Surat Rasmi yang berkaitan Sijil Digital Pelayan di Portal GPKI. Surat yang dimuat naik hendaklah dalam format pdf dan saiz kurang atau 5MB.

Atribut CSR: RSA 2048

C=MY,ST=Wilayah Persekutuan,L=Putrajaya,O=Agensi Penguatkuasaan Maritim Malaysia,OU=Bahagian Teknologi

CSR:

-----BEGIN CERTIFICATE REQUEST-----
MIIDRDCCAiwCAQAwgdIxCzAJBgNVBAYTAk1ZMRwwGgYDVQQIDBNXaWxheWFoIFBI
cnNla3V0dWFuMRIwEAYDVQQHDAlQdXRyYWpheWExLzAtBgNVBAoMJkFnZW5zaSBQ
ZW5ndWF0a3Vhc2FhbiBNYXJpdGltIE1hbGF5c2lhMSQwIgYDVQQLDBtCYWhhZ2lh
biBUZWtub2xvZ2kgTWFrbHVtYXQxFjAUBgNVBAMMDSoubW1IYS5nb3YubXkxIjAg
BgkqhkiG9w0BCQEWE3NoYW1zdWxAbW1IYS5nb3YubXkwggEiMA0GCSqGSIb3DQE
B
AQUAA4IBDwAwggEKAoIBAQC/JZLdQIS1M2oT8QttT8jpTMkqPlhKrO1ZgARU0z9c

Pengesahan Keselamatan: p76eb

Penyataan

a. Surat rasmi tidak perlu dihantar kepada Admin.
b. Surat yang dimuat naik hendaklah dalam format pdf dan saiz kurang atau 5MB.
c. Laporan Penilaian Risiko yang dimuat naik hendaklah dalam format excel dan saiz kurang daripada 10MB.
d. Laporan Penilaian Risiko bagi permohonan Sijil Digital Pelayan Multi Domain dan Wildcard hendaklah disertakan dengan senarai semua subdomain dan perincian keterangan.

Draf | Hantar

Pemilihan kriteria pelayan MESTILAH sama sepadan dengan hasil laporan penilaian risiko yang telah diluluskan

Surat rasmi agensi MESTILAH disediakan mengikut format yang telah ditetapkan.

Fail CSR yang telah dimuat naik.

3.5: PERMOHONAN SIJIL DIGITAL PELAYAN DI PORTAL GPKI

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

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

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.

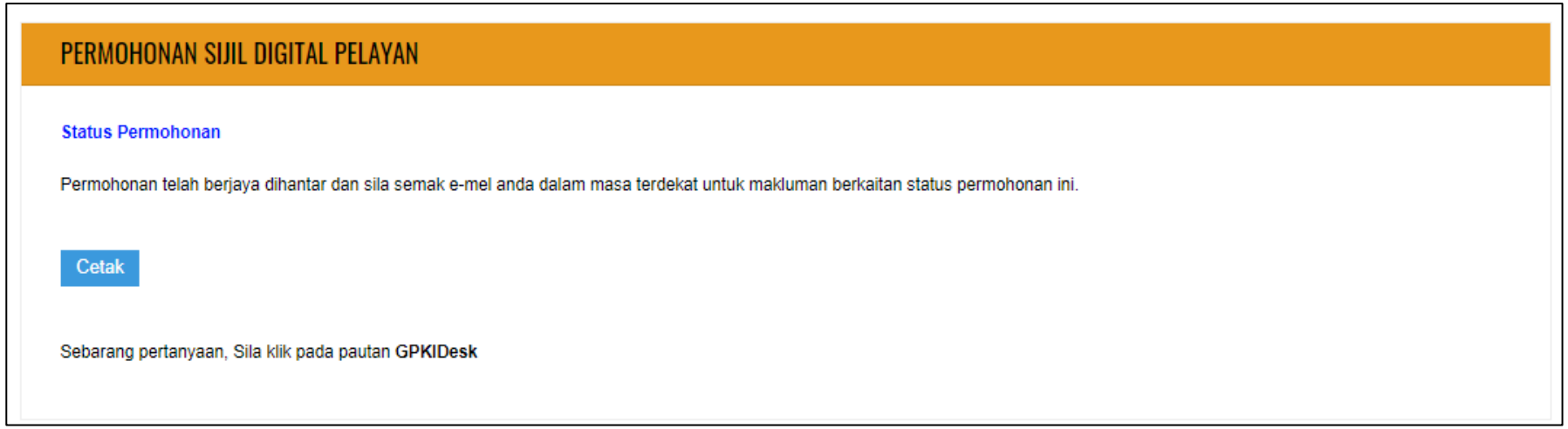
Sekian.

"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

{Tandatangan Ketua Jabatan}
{Nama Ketua Jabatan}
{Jawatan}
Telefon :
E-mel :

3.5: PERMOHONAN SIJIL DIGITAL PELAYAN DI PORTAL GPKI



- **Tempoh sah laku sijil digital pelayan** yang dibekalkan oleh Agensi Pusat (MAMPU) kepada agensi ialah **12 bulan** tertakluk pada polisi CA dan prinsipal 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 hanya dibenarkan membuat pembaharuan sijil digital pelayan **seawal 30 hari** sebelum **tamat tempoh sijil** tersebut melalui Portal GPKI.

3.6: PROSES PENGESAHAN (e-Vetting) OLEH PRINSIPAL

SYARAT KELULUSAN e-Vetting SIJIL DIGITAL PELAYAN

KAEDAH PENGESAHAN ORGANISASI (*ORGANIZATION VALIDATION*)

a. URL DOMAIN/SUBDOMAIN

- domain/subdomain **telah wujud** dan **telah didaftarkan di MyNIC**.
- domain/subdomain **boleh dicapai secara dalam talian melalui Internet oleh prinsipal yang berada di luar negara**
- mengemaskini maklumat domain/subdomain di portal agensi masing-masing dan portal **malaysia.gov.my** yang menjadi direktori sumber rujukan prinsipal untuk portal-portal di Malaysia

b. TELEFON PEJABAT

- pengesahan oleh prinsipal hanya bermula **24-48 jam** selepas pergiliran 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 yang dihubungkan setelah menghubungi **operator kementerian/jabatan/MyGCC**

c. BORANG PERMOHONAN

- Memberi **maklum balas e-mel yang diterima daripada prinsipal** – muat turun, cetak, semak maklumat dan tandatangan dokumen (berserta cop pegawai dan cop jabatan). Setelah dokumen lengkap, ianya perlu diimbas dan dimuat naik atau dikembalikan semula kepada pihak prinsipal melalui e-mel (**WAJIB** bagi jenis *single domain extended validation*)
- **menyalin semula petikan yang mengandungi ayat dan *random key*** untuk pengesahan melalui e-mel. E-mel hanya boleh dijawab semula oleh pegawai yang menerima sahaja

3.6: PROSES PENGESAHAN (e-Vetting) OLEH PRINSIPAL

SYARAT KELULUSAN e-Vetting SIJIL DIGITAL PELAYAN

KAEDAH PENGESAHAN DOMAIN (*DOMAIN VALIDATION*)

a. E-MEL (*paling mudah dan cepat)

- E-mel akan **hantar oleh prinsipal kepada e-mel pentadbir** yang telah didaftarkan sebagai ***Administative 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. Proses pengemaskinian mengambil masa dalam tempoh 3-5 hari untuk.

b. DNS

- 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. 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).

c. HTTPD

- 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.

3.6: PROSES PENGESAHAN (e-Vetting) OLEH PRINSIPAL

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	• 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).	• Nama **Domain** • Nama **Organisasi** dan **lokasi** termasuk negara • **Nombor Pendaftaran** (Registration Number) • **Lokasi Pendaftaran** (Registration Location)
2.	Organization Validation (OV)	Pemilikan atau kawalan domain	• Prinsipal akan menghubungi organisasi melalui **e-mel** untuk **pengesahan pengeluaran sijil** (pentadbir domain).	• Nama **Domain** • Nama **Organisasi** dan **lokasi** termasuk negara

3.7: PENJANAAN DAN PENGHANTARAN SIJIL DIGITAL PELAYAN OLEH PRINSIPAL/CA

BIL.	PLATFORM	KETERANGAN	FORMAT SIJIL DIGITAL PELAYAN
1.	E-mel notifikasi Sistem GPKI	E-mel notifikasi berserta lampiran sijil digital pelayan	*.cer
2.	Portal GPKI	Muat turun sijil digital pelayan mengikut domain/subdomain masing-masing di Portal GPKI 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	*.cer
3.	E-mel CA	E-mel kepada Pegawai Pemohon, Pegawai Teknikal dan Pegawai Pengesah	*.crt, text atau lampiran e-mel prinsipal
4.	E-mel dan Portal Prinsipal	E-mel kepada Pegawai Pemohon, Pegawai Teknikal dan Pegawai Pengesah	Lampiran text atau pautan muat turun (dari portal prinsipal)

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

3.8: PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN OLEH AGENSI

TINDAKAN AGENSI SELEPAS PENERIMAAN SIJIL

01 Kemas kini tarikh penerimaan sijil digital pelayan di Portal GPKI.

02 Pasang sijil digital pelayan di pelayan agensi dalam tempoh 14 hari selepas penerimaan. Pastikan arahan pemasangan diikuti dengan teliti.

03 Semak dan pastikan konfigurasi pemasangan sijil digital pelayan dilaksanakan dengan betul & mendapat “Taraf A”.

04 Kemas kini tarikh dan masa pemasangan sijil dalam Portal GPKI.

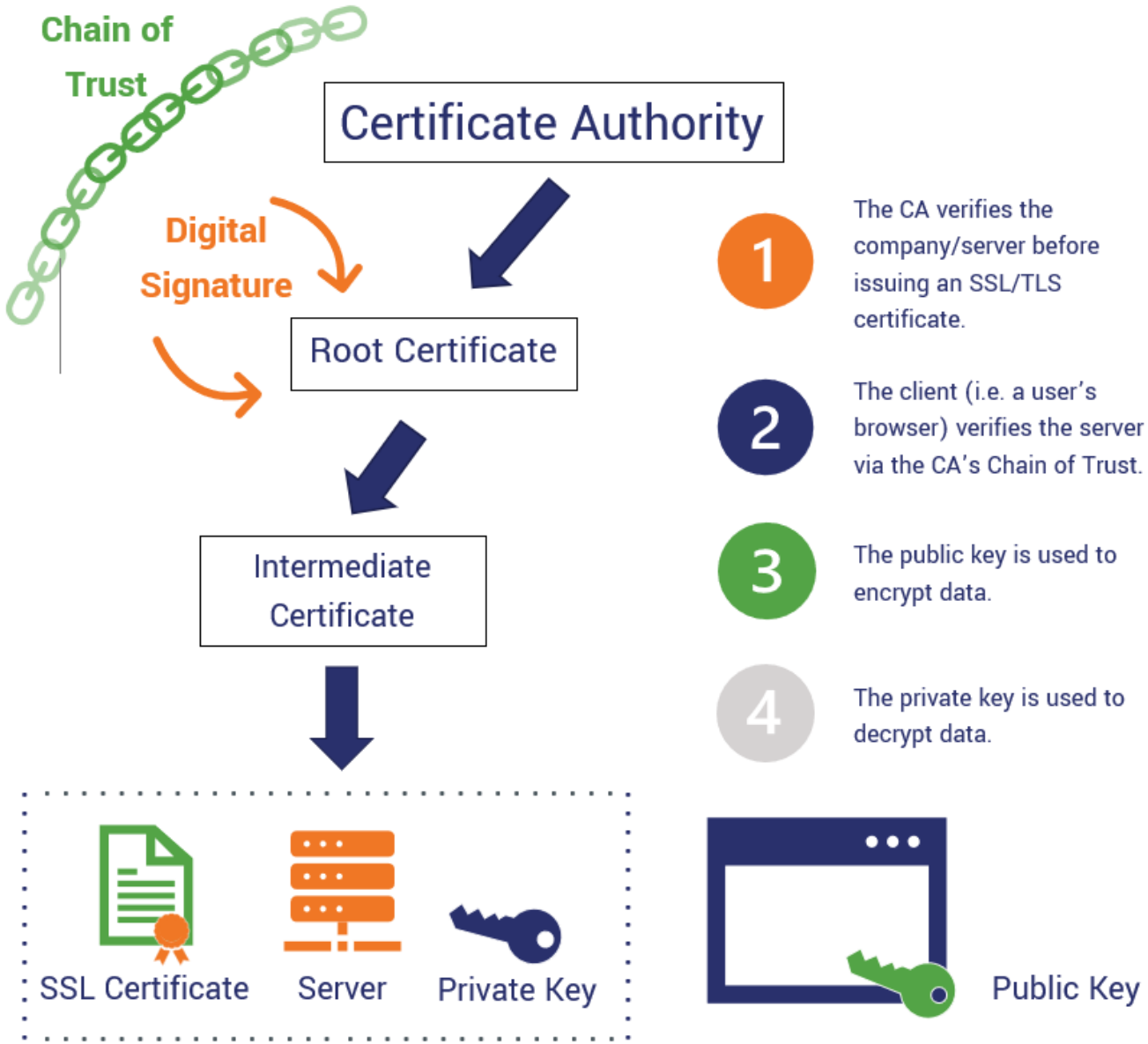
05 Maklum segera kepada Agensi Pusat (MAMPU) sekiranya terdapat ralat atau sijil *corrupt* dalam tempoh 14 hari tersebut.

06 Berdasarkan amalan terbaik, sijil digital pelayan multi domain atau wildcard perlu mempunyai salinan sijil dan private key yang berasingan setiap subdomain.

07 Fail CSR yang telah dijana untuk salinan sijil bagi multi domain dan wildcard perlu dikemukakan kepada Pentadbir GPKI untuk diserahkan kepada pihak CA bagi tujuan penjanaan semula salinan sijil

Kos akan **ditanggung sepenuhnya** oleh **agensi sendiri** sekiranya pemasangan tidak dilaksanakan dalam tempoh 14 hari tersebut

3.8: PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN OLEH AGENSI



1. The CA verifies the company/server before issuing an SSL/TLS certificate.
2. The client (i.e. a user's browser) verifies the server via the CA's Chain of Trust.
3. The public key is used to encrypt data.
4. The private key is used to decrypt data.

3.8: PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN OLEH AGENSI

Empat item yang diperlukan semasa pemasangan sijil digital pelayan

a. Sijil digital pelayan > subdomain yang dimohon

b. Sijil rantaian tambahan > intermediate cert CA

c. Sijil rantaian tambahan > root cert CA

d. Fail private key(*.key/*.pem/*.jks/*.keystore)

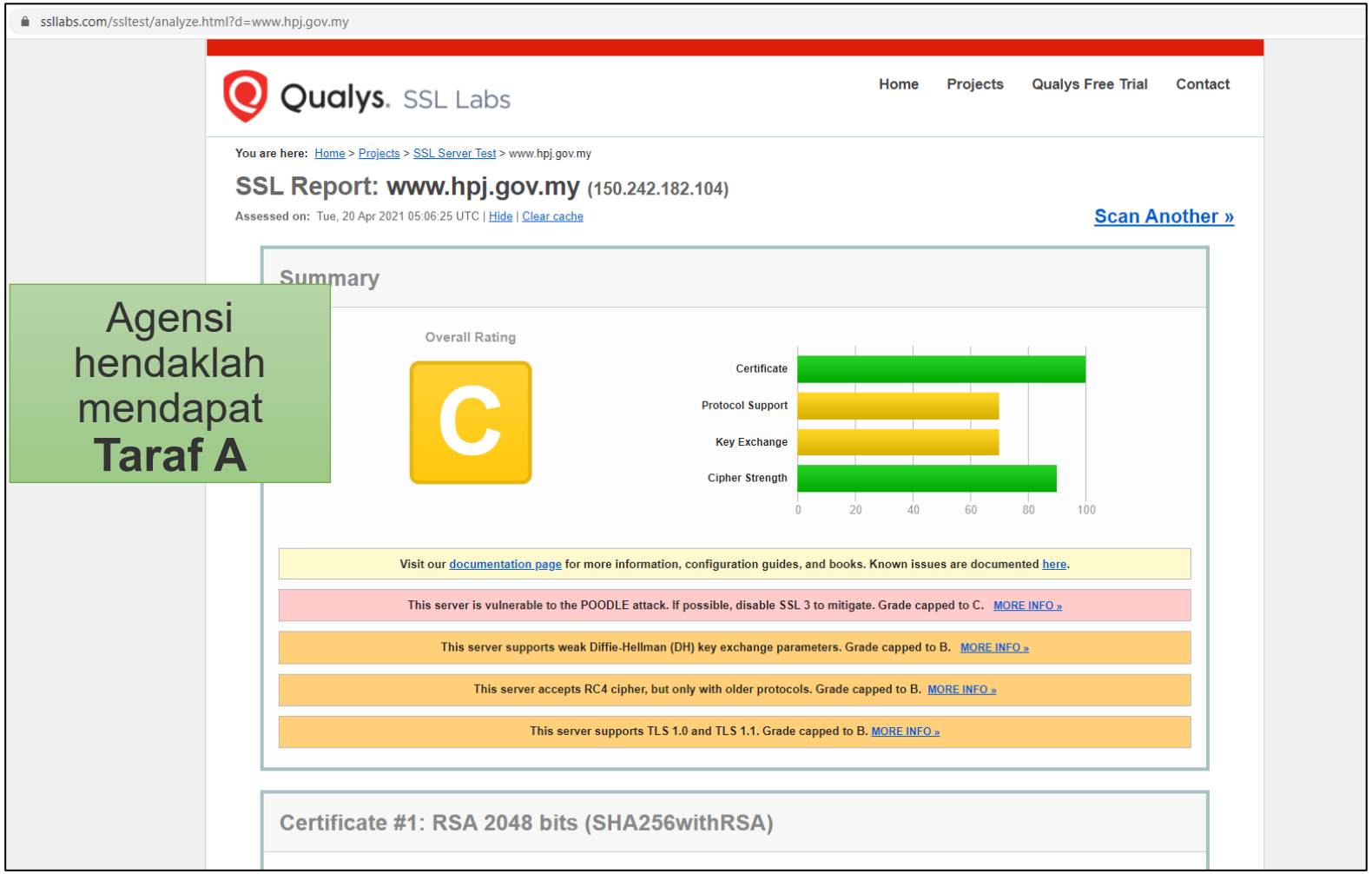
Bagi sesetengah prinsipal item **b** dan **c** digabungkan dalam satu fail dan dikenali sebagai "**Chain Bundle".**

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.

3.8: PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN OLEH AGENSI



Agensi hendaklah mendapat **Taraf A**

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

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 Pembetulan (samb.)

#Ralat 2: not support Forward Secrecy
Tindakan pembetulan: 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

3.8: PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN OLEH AGENSI

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)

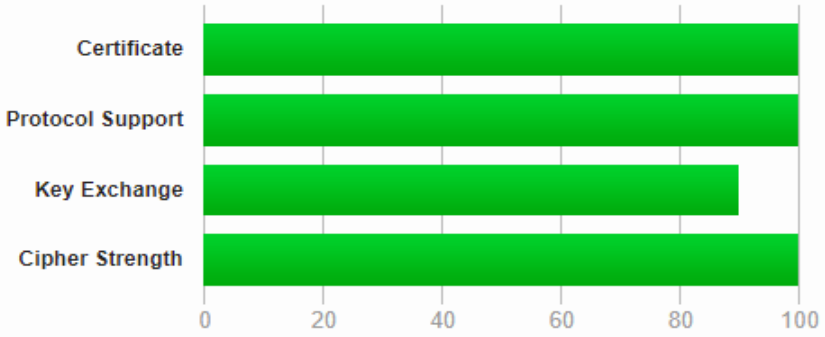
Assessed on: Mon, 03 May 2021 08:43:14 UTC | Clear cache

Scan Another »

Summary

Overall Rating

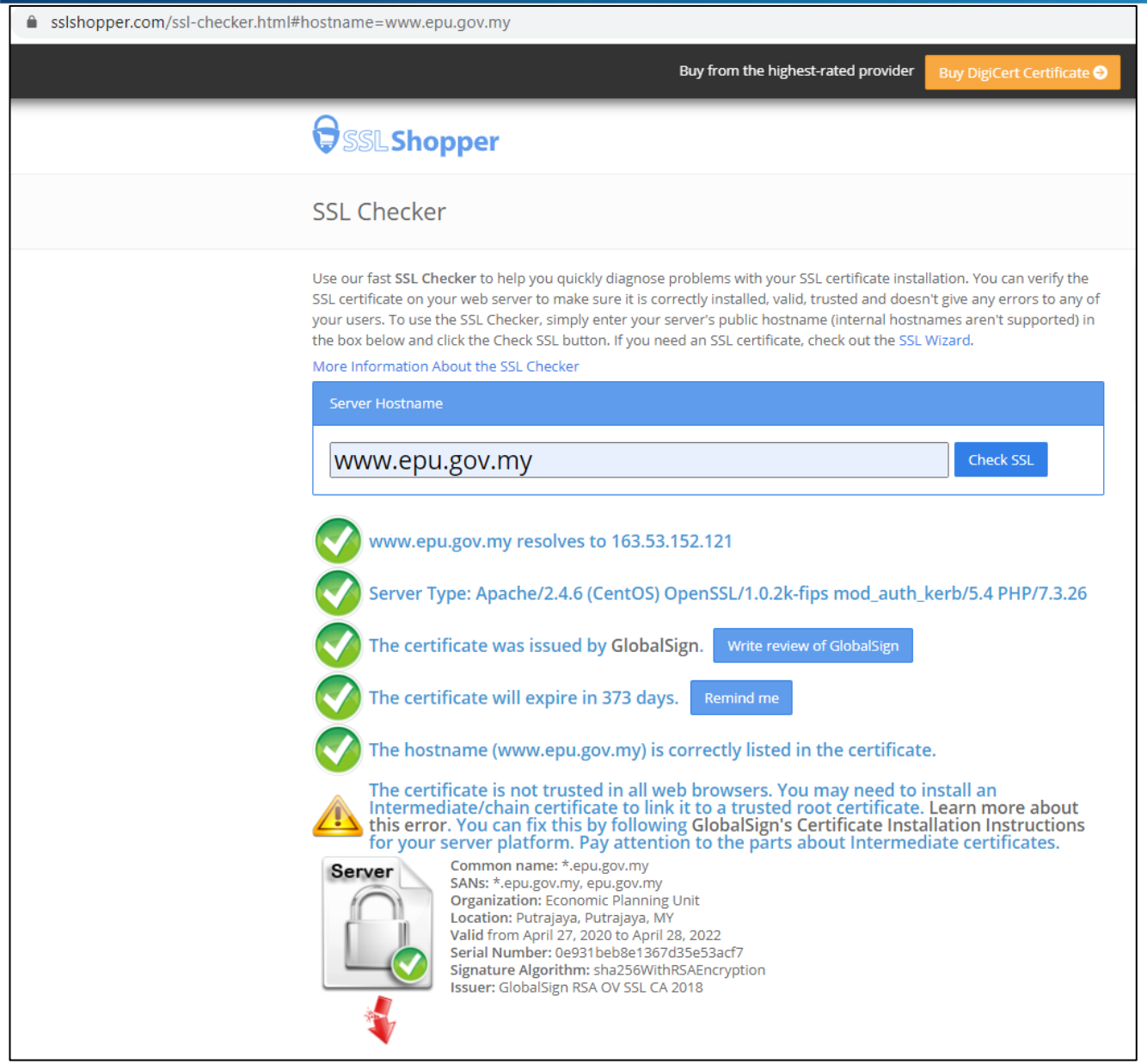
A+



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 »

3.8: PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN OLEH AGENSI



10 Tools: SSL Shopper (Chain Certificate)

Rujukan Tindakan Pembetulan

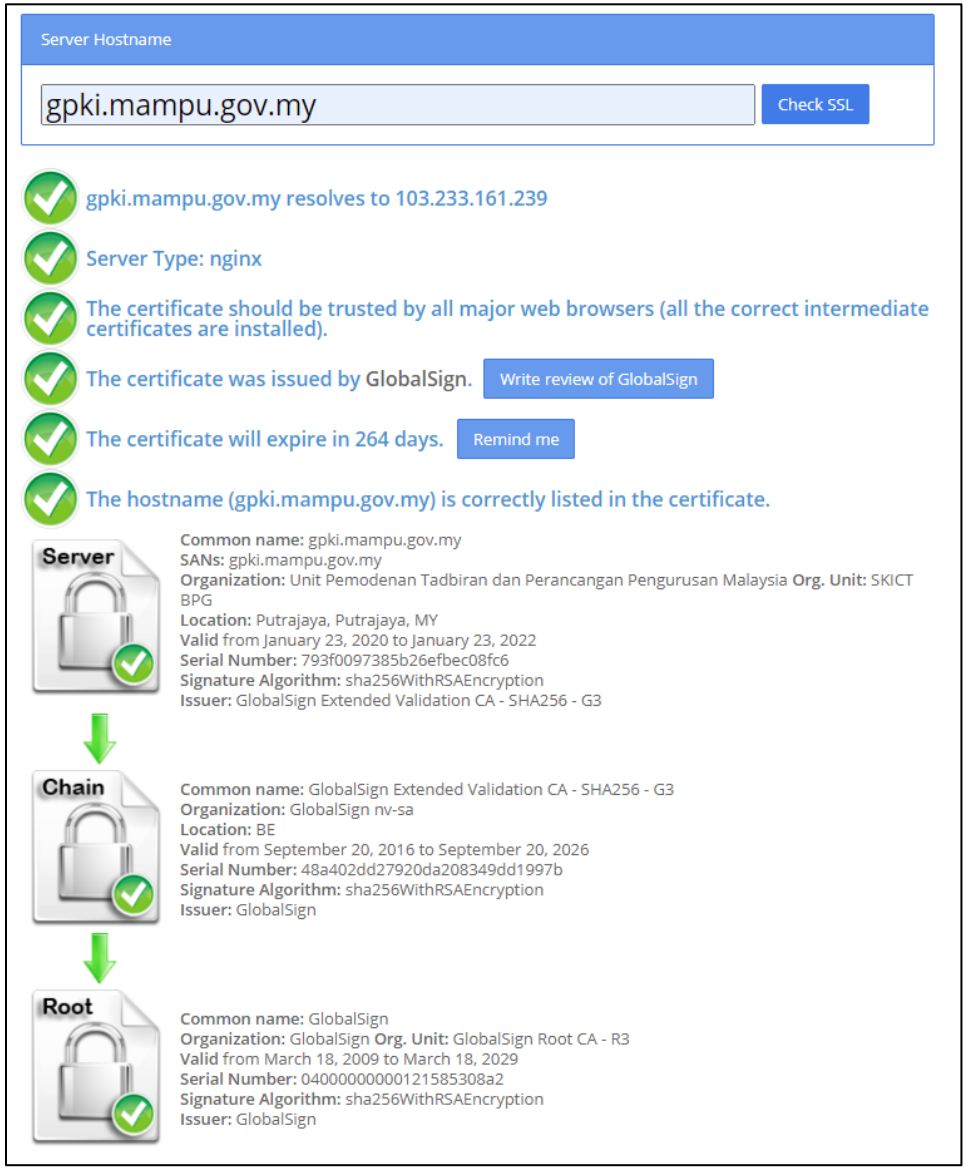
 # Finding 1: failed to connect due to firewall restrictions
=> firewall yang tidak allow untuk scanning atau port di firewall ditutup

#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

3.8: PENERIMAAN DAN PEMASANGAN SIJIL DIGITAL PELAYAN OLEH AGENSI



Contoh pemasangan sijil dengan susunan rantaian (chain) sijil yang lengkap

POS Digicert | TRUSTGATE

Topik 4: POV: e-Vetting SSL

"Isu-isu semasa proses pengesahan sijil digital pelayan"

ENTRUST GlobalSign by GMO GeoTrust powered by digicert

Topik 4: POV: e-Vetting SSL

ENTRUST

GlobalSign by GMO

GeoTrust powered by digicert

"Isu-isu semasa proses pengesahan sijil"

1

PROSES VERIFIKASI

- Kurang faham proses verifikasi SSL dan bagaimana melakukannya.

2

PENGESAHAN DOMAIN

- Butiran pentadbir domain tidak dikemaskini dalam rekod WHOIS MYNIC.

Klik

3

MAKLUMAT AGENSI

- Tidak dikemaskini di dalam portal MyGov - GeoTrust

www.malaysia.gov.my

Klik

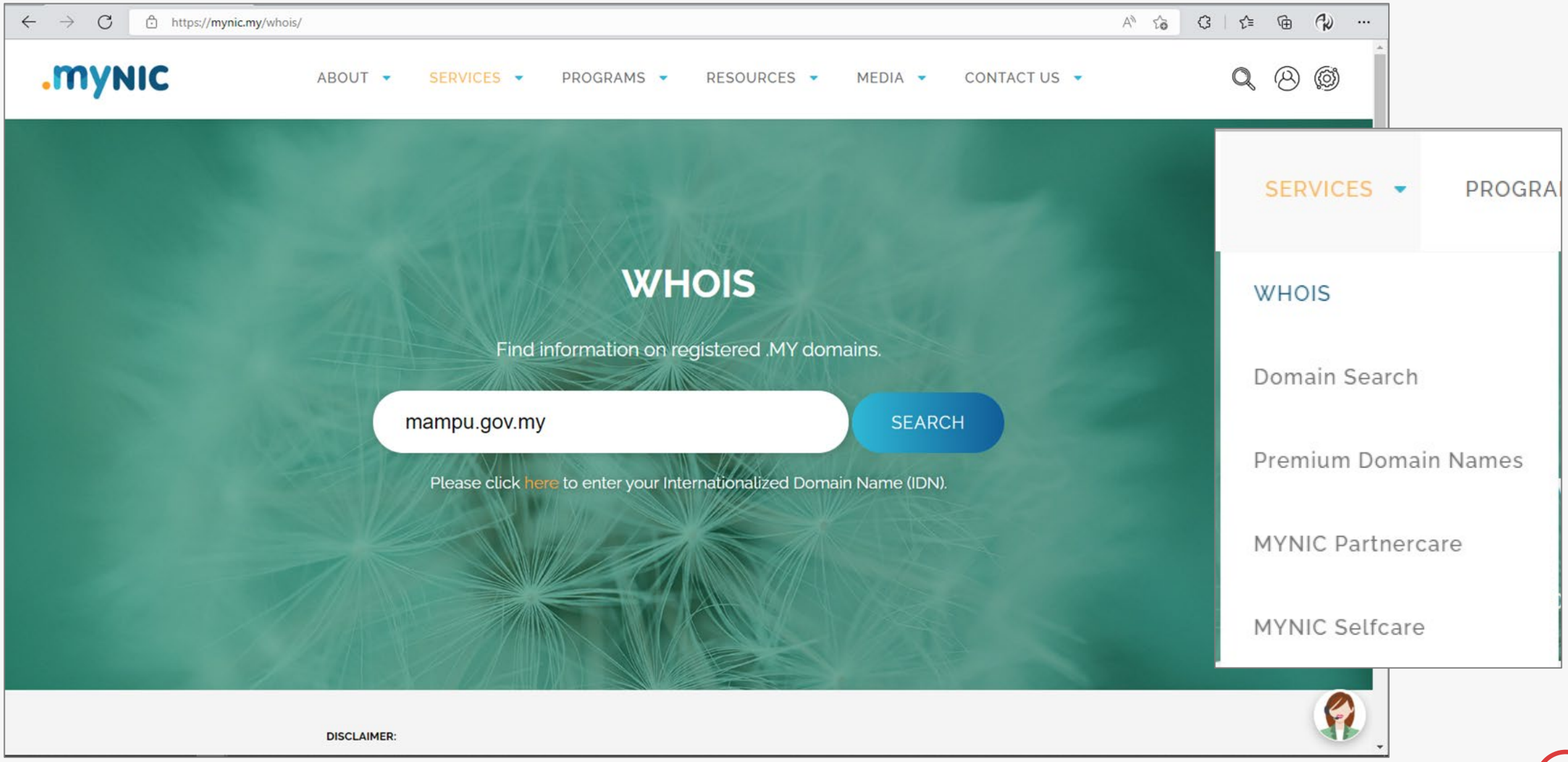
4

MAKLUMAT PEMOHON

- Tiada dalam rekod MyGCC (Malaysia Government Call Centre) - GeoTrust

Klik

https://mynic.my → SERVICES → WHOIS



Kembali

mynic.my/whois#suggestedresult

WHOIS Result

Domain Name	mampu.gov.my
DNSSEC	Signed Delegation
Registration No.	D30024
Record Created	29 May 1996
Record Expired	29 May 2023
Record Last Modified	27 April 2022

Invoicing Party

MYNIC Berhad
Level 3, Tower 2, Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor
Malaysia

Email : **billing@mynic.my**

Registrant

MAMPU (Unit Pemodenan Tadbiran Malaysia) (-)

MAMPU (Unit Pemodenan Tadbiran Malaysia)
Jabatan Perdana Menteri
Aras 1, Blok B2, Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
Wilayah Persekutuan
Malaysia

Administrative Contact

Pengarah BPG Seksyen Pembangunan Infrastruktur Rangkaian ICT

MAMPU (Unit Pemodenan Tadbiran Malaysia)
Jabatan Perdana Menteri
Aras 1, Blok B2, Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
Wilayah Persekutuan
Malaysia

Email : **bpg.spiri@mampu.gov.my**

Billing Contact

GSB CFO

GITN Sdn Berhad
Level 2, TM IT Complex
3300 Lingkaran Usahawan 1 Timur
63000 Cyberjaya
Selangor
Malaysia

Email : **planning@gitn.com.my**

https://mynic.my → Contact Us → Where We Are

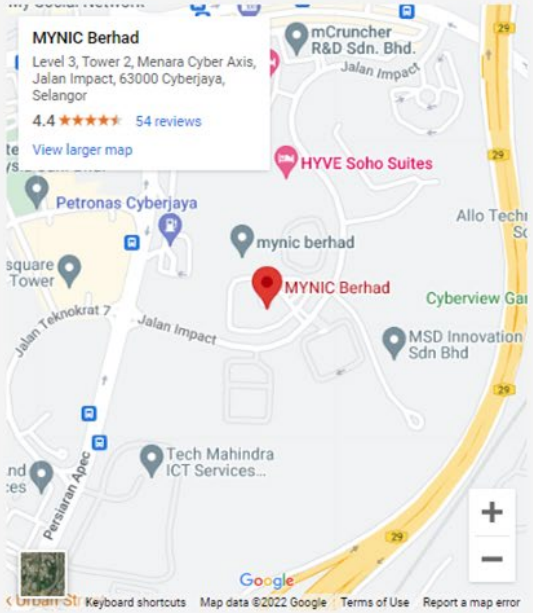
We are here

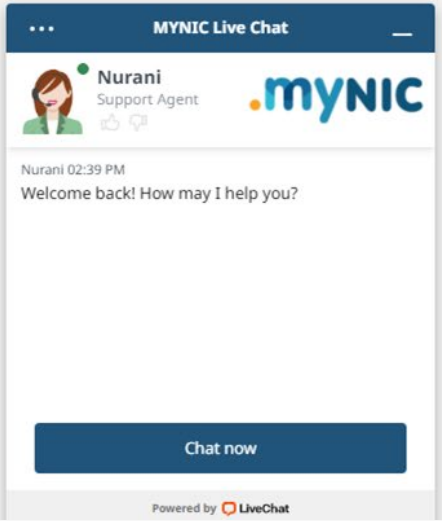
MYNIC Berhad (Co.No. 735031-H)
Level 3, Tower 2, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia

Local Hotline:
1300-88-7277

International Hotline:
+603-2107 6562

General Line (9am – 6pm):
Telephone:+603 8008 2000
Facsimile:+603 8008 2020





E-Mail: customercare@mynic.my
Chatbot: MYNIC Live Chat

Kembali

MyGOV - Portal Rasmi Kerajaan

https://www.malaysia.gov.my/portal/index

Manual | Mengenai Kami

English | Daftar | Log Masuk

Warna Tema: Saiz Tulisan: Jenis Tulisan: Arial

Soalan Lazim | Hubungi Kami | Aduan & Maklum Balas | Peta Laman

MyGovernment

Laman Utama | Topik | MyInfo | MyInisiatif | Perkhidmatan Digital

APA ITU ANALITIS DATA RAYA SEKTOR AWAM (DRSA)?

Analitis Data Raya Sektor Awam (DRSA) merupakan salah satu program berpacukan data yang bertujuan untuk memanfaatkan nilai data dari pelbagai sumber dan jenis (berstruktur dan tidak berstruktur) bagi menghasilkan pengetahuan yang berguna (insightful) dalam bentuk deskriptif, diagnostik, prediktif mahupun preskriptif bagi membantu dalam perancangan dan pembuatan keputusan yang tepat dan berkesan berasaskan fakta

Bagaimana Kami Boleh Membantu Anda?

Taipkan kata kunci carian di sini | CARI

INFORMASI MENGIKUT PERISTIWA KEHIDUPAN

Capaian Maklumat dan Perkhidmatan Kerajaan Berdasarkan Kategori Peristiwa Kehidupan

Warganegara | Bukan Warganegara

MENGURUS PENGENALAN DIRI

MENGURUS INSTITUSI KELUARGA

MENDAPAT PENDIDIKAN FORMAL

Play

Seterusnya

MyGOV - Hubungi Kami

https://www.malaysia.gov.my/portal/contact

Manual | Mengenai Kami

English | Daftar | Log Masuk

Warna Tema: Saiz Tulisan: Jenis Tulisan: Arial

Soalan Lazim | Hubungi Kami | Aduan & Maklum Balas | Peta Laman

MyGovernment

Laman Utama | Topik | MyInfo | MyInisiatif | Perkhidmatan Digital

Hubungi Kami

Laman Utama

Hubungi Kami

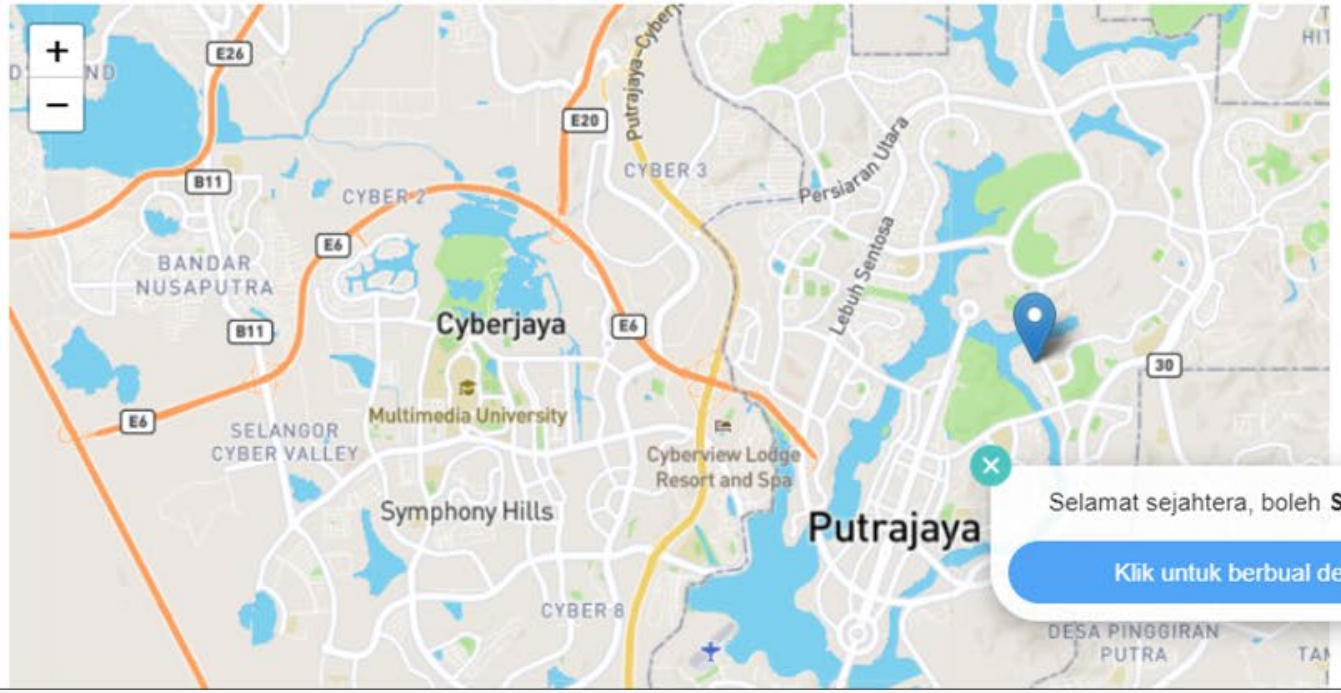
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA

Aras 6, Setia Perdana 2,
Kompleks Setia Perdana,
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
Malaysia

2.9370395,101.6955217

603 8000 8000

603 8888 3721



Selamat sejahtera, boleh **SITI** bantu anda?

Klik untuk berbual dengan SITI

Kembali

MULTICHANNEL MyGCC

Terdapat tujuh (7) saluran bagi perkhidmatan MyGCC iaitu Panggilan Suara, SMS, E-mel, Facebook, Twitter, Instagram dan Aplikasi Chatbot yang boleh diringkaskan seperti berikut:

- **Telefon/SMS/IVR : 03-8000 8000**
- **E-mel : 80008000@mygcc.gov.my**
- **Chatbot : SITI@MyGCC**
- **Facebook : facebook.com/MyGCCMalaysia**
- **Instagram : @MyGCCMalaysia**
- **Twitter : twitter.com/MyGCCMalaysia**
- **Portal : www.malaysia.gov.my**

Aplikasi Chatbot SITI@MyGCC (Sharing Information Through Innovation) merupakan sistem pengkomputeran soal jawab (Q&A) pintar yang dibangunkan secara Artificial Intelligence (AI) memberikan informasi dihujung jari.

Waktu Operasi Perkhidmatan MyGCC

i. Saluran Panggilan : 7.30 pagi - 9.00 malam, 7 hari/minggu

ii. Saluran Bukan Panggilan : 24 jam, 7 hari/minggu

Kembali

SITI@MyGCC

Not secure | mygcc.gov.my/SITI_DaftarMasuk?theme_no=1ebebc

SITI @MyGCC

SHARING INFORMATION THROUGH INNOVATION
BERKONGSI MAKLUMAT MELALUI INOVASI

Gerbang Rasmi Kerajaan Malaysia
MyGovernment

Terima kasih kerana menggunakan perkhidmatan SITI@MyGCC
(Buat masa ini perkhidmatan ini hanya disediakan dalam Bahasa Melayu / Currently this service is only available in Malay)

Siapakah nama anda?
(Cth: 'Hairul')

Sila masukkan info anda di sini...

Sila masukkan nombor telefon anda
(Cth: '0121234567')

Sila masukkan info anda di sini...

Saya juga memerlukan e-mail anda supaya pegawai kami boleh berhubung terus dengan anda pada masa hadapan
(Cth: 'name@gmail.com')

Sila masukkan info anda di sini...

HANTAR

Kembali

Topik 4: POV: e-Vetting SSL

ENTRUST

GlobalSign by GMO

GeoTrust powered by digicert

"Isu-isu semasa proses pengesahan sijil"

5 PEMBAHARUAN SSL

- Pemohon lewat membuat permohonan pembaharuan SSL.
- Proses pengesahan oleh Prinsipal mengambil masa 3-5 hari bekerja (waktu MY), tertakluk kepada dokumen tambahan yang diperlukan oleh Prinsipal serta proses pengesahan domain dan pesanan dari pemohon.

6 PANGGILAN PENGESAHAN

Klik

- Prinsipal gagal menghubungi pemohon untuk proses pengesahan (tiada di pejabat, mesyuarat, no. telefon sambungan telefon , tiada respon dari operator agensi).

gpki.mampu.gov.my/gpki_portal/

GPKI DESK | LOGIN PENTADBIR

MyGPKI GOVERNMENT PUBLIC KEY INFRASTRUCTURE

UTAMA | MAKLUMAT AM | PERKHIDMATAN | MUAT TURUN | SOALAN LAZIM | MEJA BANTUAN | eLEARNING

PERMOHONAN SIJIL DIGITAL PENGGUNA

- Permohonan Sijil Digital Pengguna
- Permohonan Pembatalan Sijil Digital Pengguna
- Semak Status Sijil Digital Pengguna
- Semak Status Pembatalan Sijil Digital Pengguna

PENGURUSAN SIJIL DIGITAL PENGGUNA

- Kemas Kini Profil Pengguna
- Muat Turun Sijil Digital Softcert
- Tukar PIN Sijil Digital Softcert/Roaming
- Reset PIN Sijil Digital Softcert/Roaming
- Pengujian Fungsi PKI

PENGURUSAN SIJIL DIGITAL PELAYAN

- 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

PENGURUSAN PENTADBIR

- Permohonan Pelantikan
- Cetak Kembali Borang Permohonan
- Muat Naik Borang Permohonan
- Semak Status Permohonan Pelantikan Pentadbir
- Carian Pentadbir

Cadangan Tarikh dan Masa Janji Temu dengan CA

Cadangan Janji Temu 1	12/01/2022 03:00 PM
Cadangan Janji Temu 2	12/01/2022 04:30 PM
Cadangan Janji Temu 3	13/01/2022 03:00 PM

Kembali

Topik 4: POV: e-Vetting SSL

ENTRUST

GlobalSign by GMO

GeoTrust powered by digicert

"Isu-isu semasa proses pengesahan sijil"

7 KELEWATAN RESPON

- Pemohon lewat memberi respon (tiada di pejabat, mesyuarat, bercuti).
- Tiada/tidak dapat memberikan respon (tidak membaca e-mel, whatsapp, telefon, no. telefon sambungan tidak dapat dihubungi, server down, masalah elektrik).
- Ragu-ragu untuk memberi respon kepada emel/ panggilan telefon dari Prinsipal.

Klik

8 MASALAH PEMASANGAN SIJIL

- Private key hilang/tiada/mismatch.
- Bagaimana untuk install?
- Tidak cuba untuk buat pemasangan sendiri.
- Pemasangan via Remote.

Klik

RESPON YANG TIDAK DITERIMA OLEH PIHAK PRINSIPAL

ENTRUST

Hello Noor Afiqa,

I have called the accountant already and got his confirmation that he wrote the legal letter.

The only pending item now is the confirmation of J[redacted]e himself since he is the Authorizing Contact in the account. I've tried calling +603[redacted]this number again since this is what is listed in the legal letter for their company but the number is not working. I've sent an email to the email address in the legal letter and he can just reply with his confirmation.

The subject line of the email is "Entrust: Employment Check Email: Account # 1-1OB3EY | Cross Light Capital Sdn Bhd" and it was sent to '[redacted]com'.

This is the only pending item. Once we get his confirmation (by phone or email), we can send this off to our auditors for completion.

Please note that I will be logging out in 30 mins. I will endorse this to our team in EMEA and Canada so that they can keep an eye on it later today. If you have any urgent questions, please call us and give your case number 0189[redacted]

GlobalSign by GMO

Good day,

This request has been done and the DVP status is approved now.

Currently we're pending with the confirmation of the order, we've sent separate email to r[redacted].my for the confirmation of the order.

Kindly advise client to check and reply.

GeoTrust powered by digicert

Hello MIMI NURAKMAL,

I am trying to finish the validation of your company (**KEMENTERIAN KESIHATAN MALAYSIA - Company ID #902276**) so you can order certificates for it, and I need your help:

First, Please provide us with a **currently active** government issued photo ID of [redacted] such as a driver's license or a passport. To ensure that the ID is clear, we recommend scanning or taking a digital photo of the ID and emailing it. If the document you send does not also show the correct address, send a document such as a utility bill (telephone, gas, electric, water, or internet), bank statement, rental agreement, or any government issued document. You may block out any sensitive information as long as it shows the **name** ([redacted] **photo**, **address** and **expiration date**.

Please attach the document with a reply to this email or fax it to 1-866-842-0223.

Kembali

entrust.com/knowledgebase/ssl/ss...

ENTRUST

Home › ••• › Knowledge Base Detail

Certificate Services Support

Refine search by:

Search Knowledge Base

All Product Types | All Server Types

SSL/TLS CERTIFICATE INSTALLATION HELP

Entrust Certificate Services Certificates are provided as x.509 PEM format, you may use 3rd party tools (e.g. OpenSSL) to change the format if needed. It is recommended to check with your server/software vendor for compatibility concerns, and as always Entrust Support is standing by to assist with any questions.

Platform	Server Type	CSR Guide	Install Guide
Microsoft	Microsoft IIS 10	VIEW	View
Microsoft	Microsoft IIS 8/8.5	VIEW	VIEW
Microsoft	Microsoft Skype for Business Server 2019	VIEW	VIEW
Microsoft	Microsoft Exchange 2016	VIEW	VIEW
Microsoft	Microsoft Forefront TMG	N/A	VIEW
Microsoft	Apache for Windo		

Hello, if you have any questions, I'm ready to chat.

Kembali

support.globalsign.com/ssl/ssl-certificates-i...

GlobalSign by GMO

GlobalSign Support

Tell us what you're looking for...

GlobalSign Support
> SSL Certificates
> SSL Certificates Insta... > Install an SSL Certific...

Install an SSL Certificate - Overview

Introduction

This article will provide you an overview on how to install an SSL Certificate and its prerequisites.

Prerequisites

- You have successfully received a new SSL Certificate using a new Certificate Signing Request (CSR) which you are ready to install.
  - If you are installing an SSL due to the ICA revocations, please ensure you have reissued your certificate before installing it. More info can be found here: https://support.globalsign.com/ssl/general-ssl/ica-revocations-and-remediation-steps.
- You have a copy of the correct Intermediate Certificate ready to install (refer to Intermediate Certificates). The Intermediate Certificates are necessary for browsers to the SSL Certificate you are going to install. It is importa note that for some servers (such as Microsoft) the Intermediate Certificates are already included with the SSL

digicert.com/kb/ssl-certificate-...

digicert®

Support
Award-Winning Customer Service

SSL Certificate Installation Instructions & Tutorials

How to Install an SSL Certificate

An SSL Certificate is a text file with encrypted data that you install on your server communications between your site and your customers. Learn more about SSL cer

After you create a CSR (certificate signing request) and purchase a certificate, our certificate request. (Learn more about the certificate validation process.) Once val send it to you via email. You can also download your SSL Certificate in your DigiCer

Verified Mark Certificates
Looking for instructions on how to install your Verified Mark Certificate (VMC)? article, VMC, PEM file and SVG: Where Does Everything Go?

Intermediate Certificate

When you install an SSL certificate on a server or SSL-enabled application, you'll als This intermediate certificate establishes the trust of your SSL certificate by tying it certificate (your DigiCert issued SSL certificate → the intermediate certificate → D certificate trust chain, a Browser requires the intermediate certificate to be prese intermediate and root certificates.

Note: For some servers (such as Microsoft), the intermediate certificates are bun

Search the knowledgebase...

Need to create your CSR? »
Need to purchase your SSL certificate? »

Common Platforms & Operating Systems

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Pemasangan Sijil Digital Pelayan

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

MyGPKI GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Pemasangan Sijil Digital Pelayan

Operating System: Windows Server

Web Server: IIS 6/7/8

Pemasangan Sijil Digital Pelayan

Proses Pemasangan Terbahagi Kepada 4 Bahagian

Bahagian 1: Muat Turun Sijil Digital Pelayan
Bahagian 2: Pasang Sijil Digital Pelayan
Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web
Bahagian 4: Semak Konfigurasi Sijil Digital Pelayan

Bahagian 1: Muat Turun Sijil Digital

auto-notice@entrust.com 11:29 AM

Entrust Certificate Request Ready www.customsgc.gov.my

If there are problems with how this message is displayed, click here to view it in a web browser.

Entrust CERTIFICATE SERVICES

Dear Certificate Requester,

Your account administrator has accepted your request for a SSL Certificate for:
cn=www.customsgc.gov.my, o=Jabatan Kastam Diraja Malaysia, l=Putrajaya, c=MY

This certificate was issued from Entrust - L1K. If this is the first time you are using this CA, make sure you follow the installation instructions carefully as each CA may have different chain certificates that you need to install.

Use the following URL to collect your certificate:

https://www.entrust.net/ssl/certpickup.cfm?id=1253416-CC6A8F45-BB39-82B8-FF40CC15E481B704

Muat Turun Sijil Digital Pelayan

Entrust Certificate Services

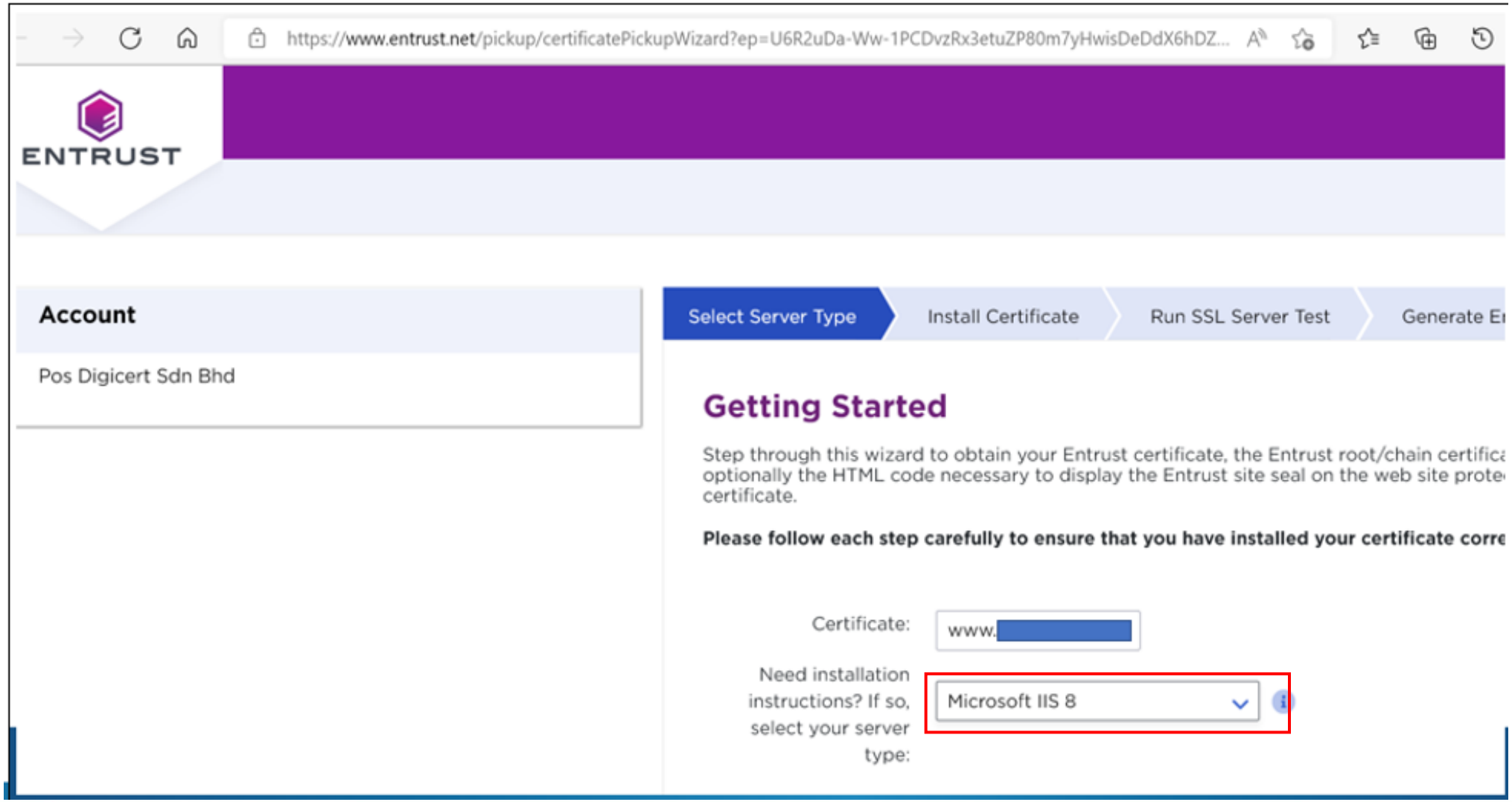
Phone Support:
North America: 1-866-267-9297
Local/International: 1-613-270-2680

Email Support:
Verification Support: ecs.verification@entrustdatacard.com
Technical Support: ecs.support@entrustdatacard.com
Sales: sales@entrustdatacard.com

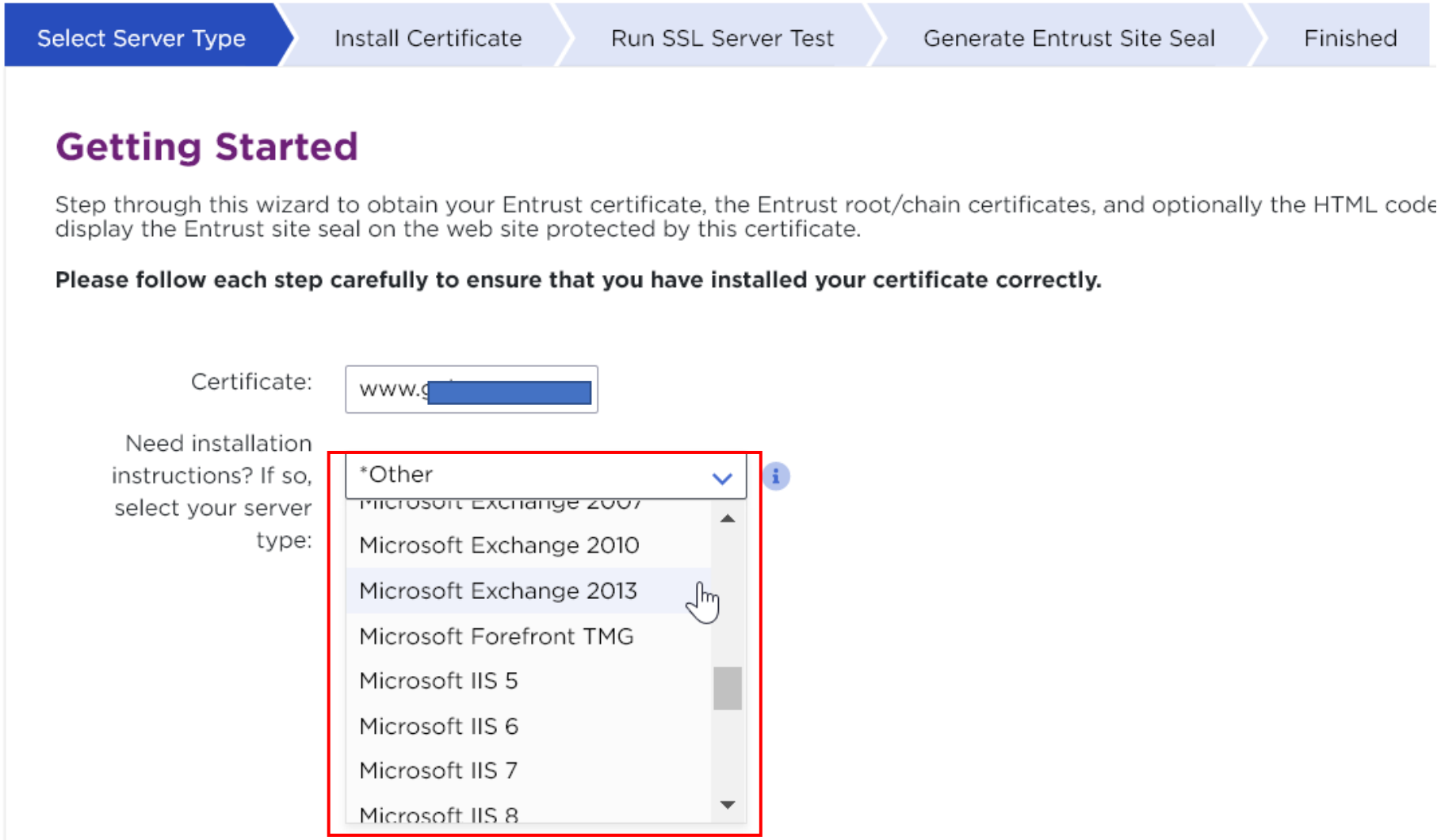
Contoh Pautan Muat Turun Sijil Digital Pelayan

https://www.entrust.net/pickup/certificatePickup?ep=U6R2uDa-Ww-1PCDvzRx3etuZP80m7yHwisDeDdX6hDZISI23KQYIQ3pvpf3qDoyuUdtZXSHPzQvBBL6cyP50rniDcFnVWilGujyMA9ugPaEAO4dmQi3HI3IAmk7FrYmQDh5Nu4s4076vkqHYw2ysoPEW7COGXRov4sqElchKeu0hafOd-Fh9WafKc7rx54K2oSM6575L6wL_hbyYfMit9yP_8trVT-HohS7CXdz6TMo

Bahagian 1: Muat Turun Sijil Digital



Bahagian 1: Muat Turun Sijil Digital



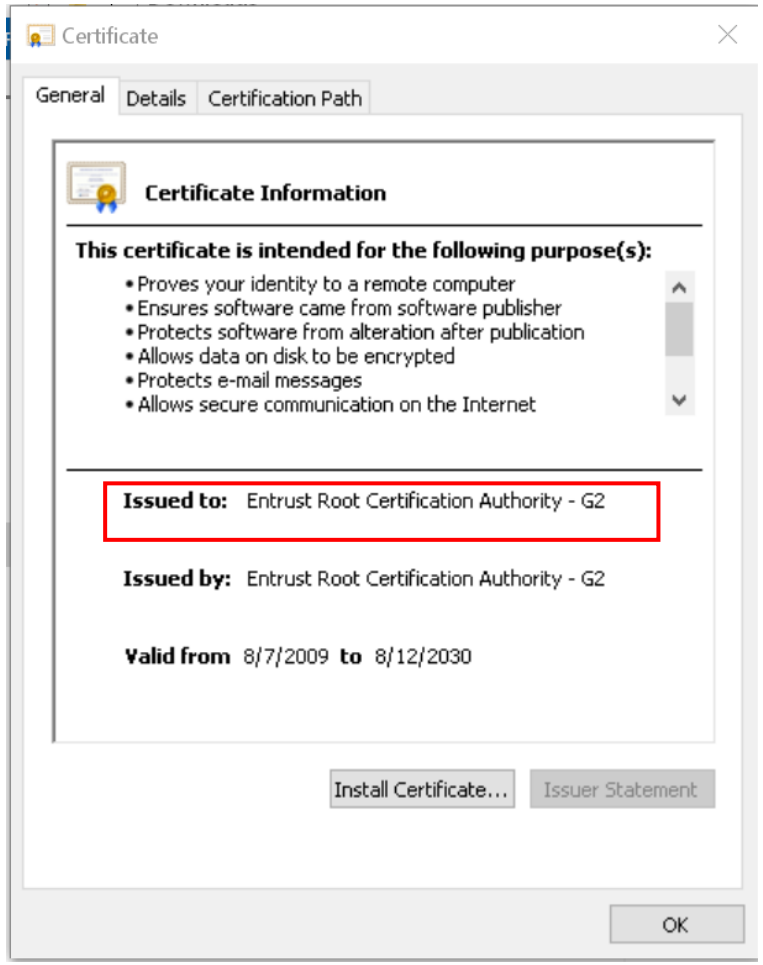
Bahagian 1: Muat Turun Sijil Digital

3 Jenis Fail Bagi Windows Server IIS 6/7/8

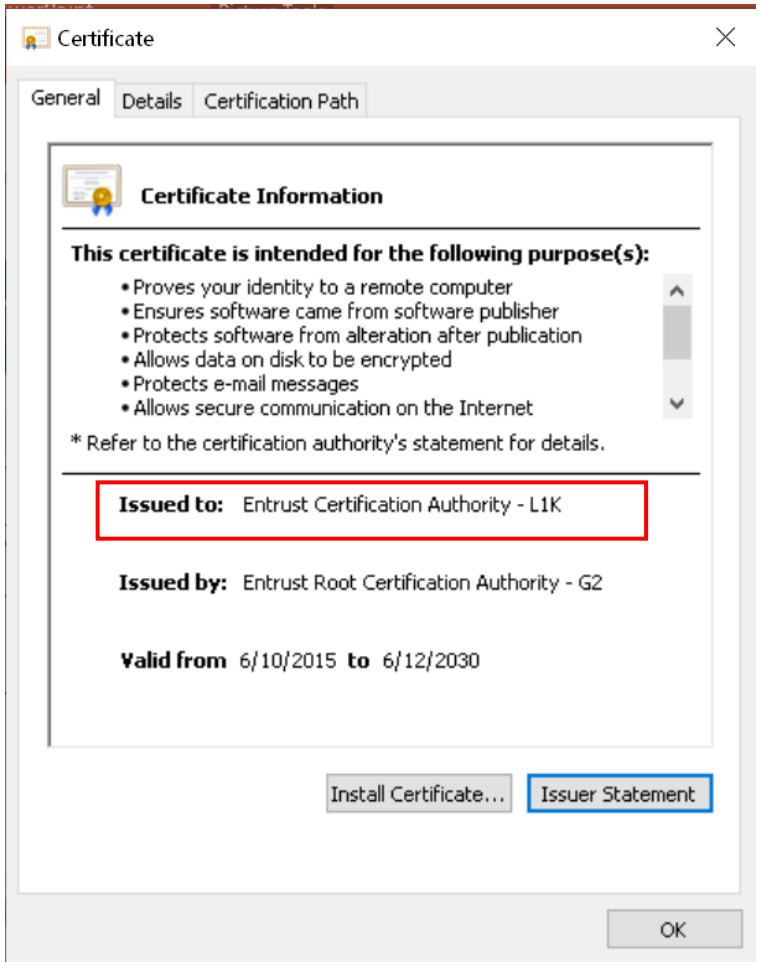
2 Jenis Fail Bagi Apache

Bahagian 1: Muat Turun Sijil Digital

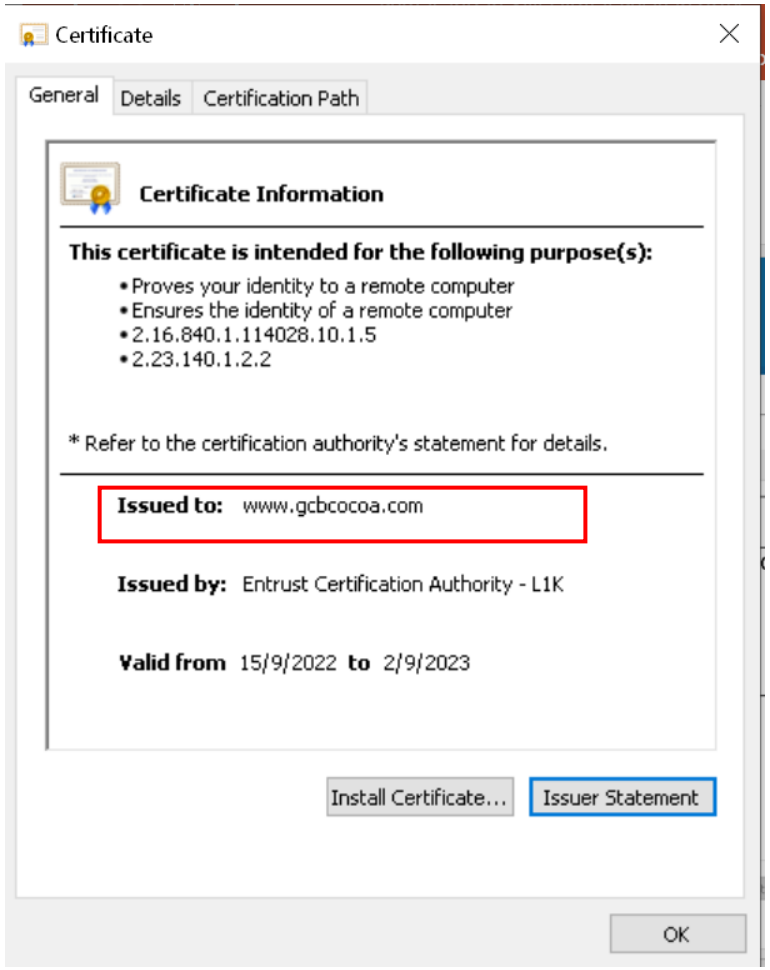
Root



Intermediate



Server Certificate



Bahagian 1: Muat Turun Sijil Digital

-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIMDulMwwAAAABR03eFMA0GCSqGSIb3DQEBCwUAMIG+MQsw
CQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2Vl
IHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMDkg
RW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTIwMAYDVQQD
EylFbnRydXN0IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBHMjAeFw0x
NTEwMDUxOTEzNTZaFw0zMDEyMDUxOTQzNTZaMIG6MQswCQYDVQQGEwJVUzEWMBQG
A1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2VlIHd3dy5lbnRydXN0Lm5l
dC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMTIgRW50cnVzdCwgSW5jLiAt
IGZvciBhdXRob3JpemVkIHVzZSBvbmx5MS4wLAYDVQQDEyVFbnRydXN0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IC0gTDFLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2j+W0E25L0Tn2zlem1DuXKVh2kFnUwmqAJqOV38pa9vH4SEkqjrQ
jUcj0u1yFvCRIdJdt7hLqIOPt5EyaM/OJZMssn2XyP7BtBe6CZ4DkJNfEmDImiK
m95HwzGYei59QAvS7z7Tsoyqj0ip/wDoKVgG97aTWpRzJiatWA7lQrjV6nN5ZGhT
JbiEz5R6rgZFDKNrTdDGvuoYpDbwkrK6HIiPOlJ/915tgxyd8B/lw9bdpXiSPbBt
LOrJz5RBGXFEaLpHPATpXbo+8DX3Fbae8i4VHj9HyMg4p3NFXU2wO7GOFyk36t0F
ASK7lDYqjVs1/lMZLwhGwSqzGmIdTivZGwIDAQABo4IBDDCCAQgwDgYDVR0PAQH/
BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwMwYIKwYBBQUHAQEEJzAlMCMGCCsG
AQUFBzABhhdodHRwOi8vb2NzcC5lbnRydXN0Lm5ldDAwBgNVHR8EKTAnMCWgI6Ah
hh9odHRwOi8vY3JsLmVudHJ1c3QubmV0L2cyY2EuY3JsMDsGA1UdIAQ0MDIwMAYE
VR0gADAoMCYGCCsGAQUFBwIBFhpodHRwOi8vd3d3LmVudHJ1c3QubmV0L3JwYTAd
BgNVHQ4EFgQUgqJwdN28Uz/Pe9T3zX+nYMYKTL8wHwYDVR0jBBgwFoAUanImetAe
733nO2lR1GyNn5ASZqswDQYJKoZIhvcNAQELBQADggEBADnVjpiDYcgsY9NwHRkw
y/YJrMxp1cncN0HyMg/vdMNY9ngnCTQIlZIv19+4o/0OgemknNM/TWgrFTEKFcxS
BJPok1DD2bHi4Wi3Ogl08TRYCj93mEC45mj/XeTIRsXsgdfJghhcg85x2Ly/rJkC
k9uUmITSnKa1/ly78EqvIazCP0kkZ9Yujs+szGQVGHLlbHfTUqi53Y2sAEo1GdRv
c6N172tkw+CNgxKhiucOhk3YtCAbvmqljEtoZuMrx1gL+1YQ1JH7HdMxWBCMRON1
exCdtTix9qrKgWRs6PLigVWXUX/hwidQosk8WwBD9lu51aX8/wdQQGcHsFXwt35u
Lcw=
-----END CERTIFICATE-----

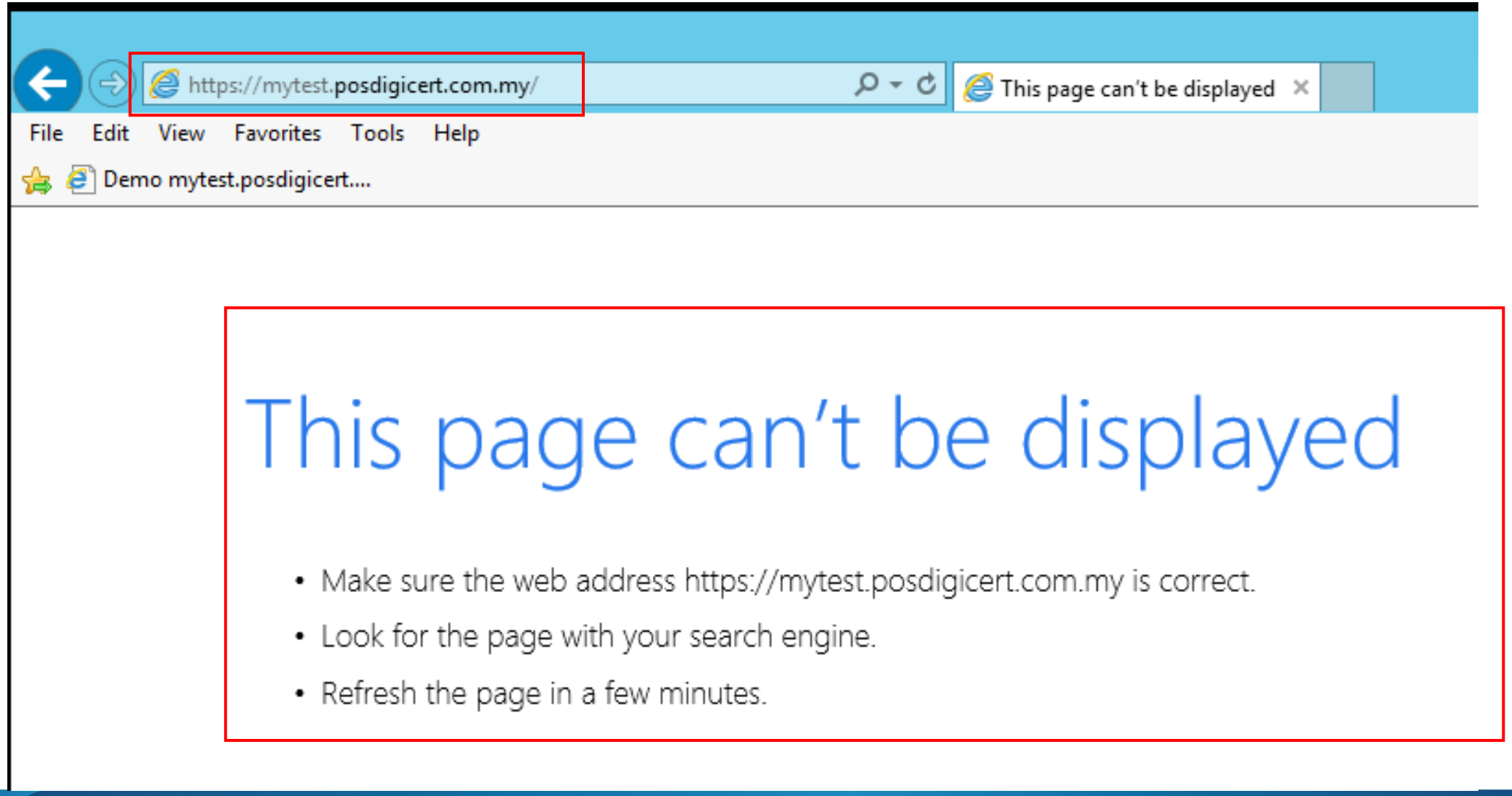
-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIMDulMwwAAAABR03eFMA0GCSqGSIb3DQEBCwUAMIG+MQsw
CQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2Vl
IHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMDkg
RW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTIwMAYDVQQD
EylFbnRydXN0IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBHMjAeFw0x
NTEwMDUxOTEzNTZaFw0zMDEyMDUxOTQzNTZaMIG6MQswCQYDVQQGEwJVUzEWMBQG
A1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2VlIHd3dy5lbnRydXN0Lm5l
dC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMTIgRW50cnVzdCwgSW5jLiAt
IGZvciBhdXRob3JpemVkIHVzZSBvbmx5MS4wLAYDVQQDEyVFbnRydXN0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IC0gTDFLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2j+W0E25L0Tn2zlem1DuXKVh2kFnUwmqAJqOV38pa9vH4SEkqjrQ
jUcj0u1yFvCRIdJdt7hLqIOPt5EyaM/OJZMssn2XyP7BtBe6CZ4DkJNfEmDImiK
m95HwzGYei59QAvS7z7Tsoyqj0ip/wDoKVgG97aTWpRzJiatWA7lQrjV6nN5ZGhT
JbiEz5R6rgZFDKNrTdDGvuoYpDbwkrK6HIiPOlJ/915tgxyd8B/lw9bdpXiSPbBt
LOrJz5RBGXFEaLpHPATpXbo+8DX3Fbae8i4VHj9HyMg4p3NFXU2wO7GOFyk36t0F
ASK7lDYqjVs1/lMZLwhGwSqzGmIdTivZGwIDAQABo4IBDDCCAQgwDgYDVR0PAQH/
BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwMwYIKwYBBQUHAQEEJzAlMCMGCCsG
AQUFBzABhhdodHRwOi8vb2NzcC5lbnRydXN0Lm5ldDAwBgNVHR8EKTAnMCWgI6Ah
hh9odHRwOi8vY3JsLmVudHJ1c3QubmV0L2cyY2EuY3JsMDsGA1UdIAQ0MDIwMAYE
VR0gADAoMCYGCCsGAQUFBwIBFhpodHRwOi8vd3d3LmVudHJ1c3QubmV0L3JwYTAd
BgNVHQ4EFgQUgqJwdN28Uz/Pe9T3zX+nYMYKTL8wHwYDVR0jBBgwFoAUanImetAe
733nO2lR1GyNn5ASZqswDQYJKoZIhvcNAQELBQADggEBADnVjpiDYcgsY9NwHRkw
y/YJrMxp1cncN0HyMg/vdMNY9ngnCTQIlZIv19+4o/0OgemknNM/TWgrFTEKFcxS
BJPok1DD2bHi4Wi3Ogl08TRYCj93mEC45mj/XeTIRsXsgdfJghhcg85x2Ly/rJkC
k9uUmITSnKa1/ly78EqvIazCP0kkZ9Yujs+szGQVGHLlbHfTUqi53Y2sAEo1GdRv
c6N172tkw+CNgxKhiucOhk3YtCAbvmqljEtoZuMrx1gL+1YQ1JH7HdMxWBCMRON1
exCdtTix9qrKgWRs6PLigVWXUX/hwidQosk8WwBD9lu51aX8/wdQQGcHsFXwt35u
Lcw=
-----END CERTIFICATE-----

Global Sign

Pautan Panduan Pemasangan Bagi Jenis IIS 6/7/8

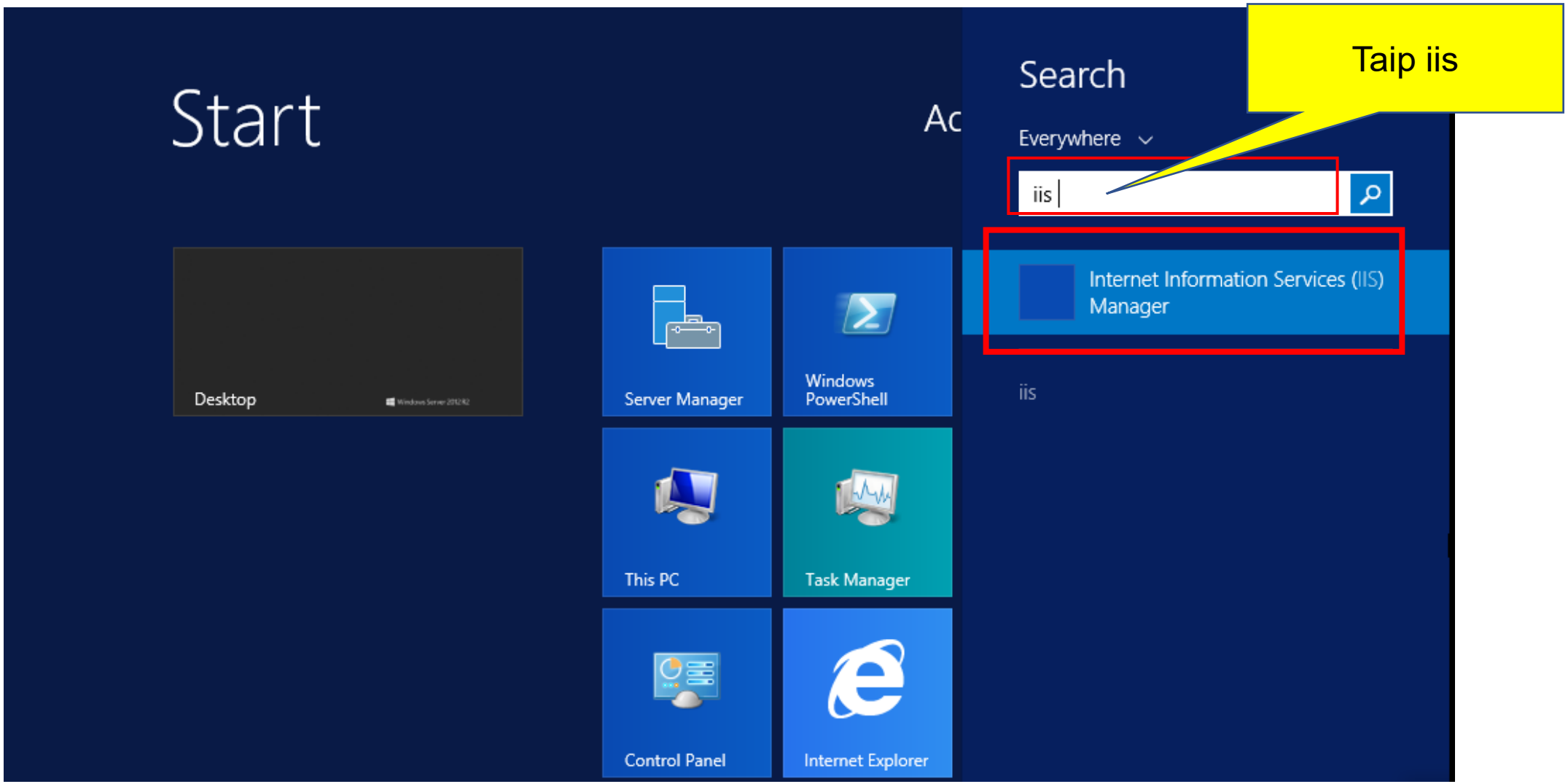
https://www.entrust.com/knowledgebase/ssl/how-to-install-a-certificate-through-microsoft-iis8

Bahagian 2: Pasang Sijil Digital Pelayan



Bagaimanakah Cara Untuk *Bind* Sijil Digital Pelayan Dengan Laman Web?

Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web



Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web

WIN-00BEJ064VC4 ▸ Sites ▸ Default Web Site ▸

File View Help

Connections

- Start Page
- WIN-00BEJ064VC4 (WIN-00BEJ064VC4
  - Application Pools
  - Sites
    - Default Web Site

Default Web Site Home

Filter: Go Show All Group by: Area

IIS

Authentic... Compression Default Document Directory Browsing Error Pages Handler Mappings

HTTP Respon... Logging MIME Types Modules Output Caching Request Filtering

SSL Settings

Management

Configurat...

Actions

Explore
Edit Permissions...

Edit Site

Bindings...
Basic Settings...

View Applications
View Virtual Directories

Manage Website

Restart
Start
Stop

Browse Website

Browse *:80 (http)

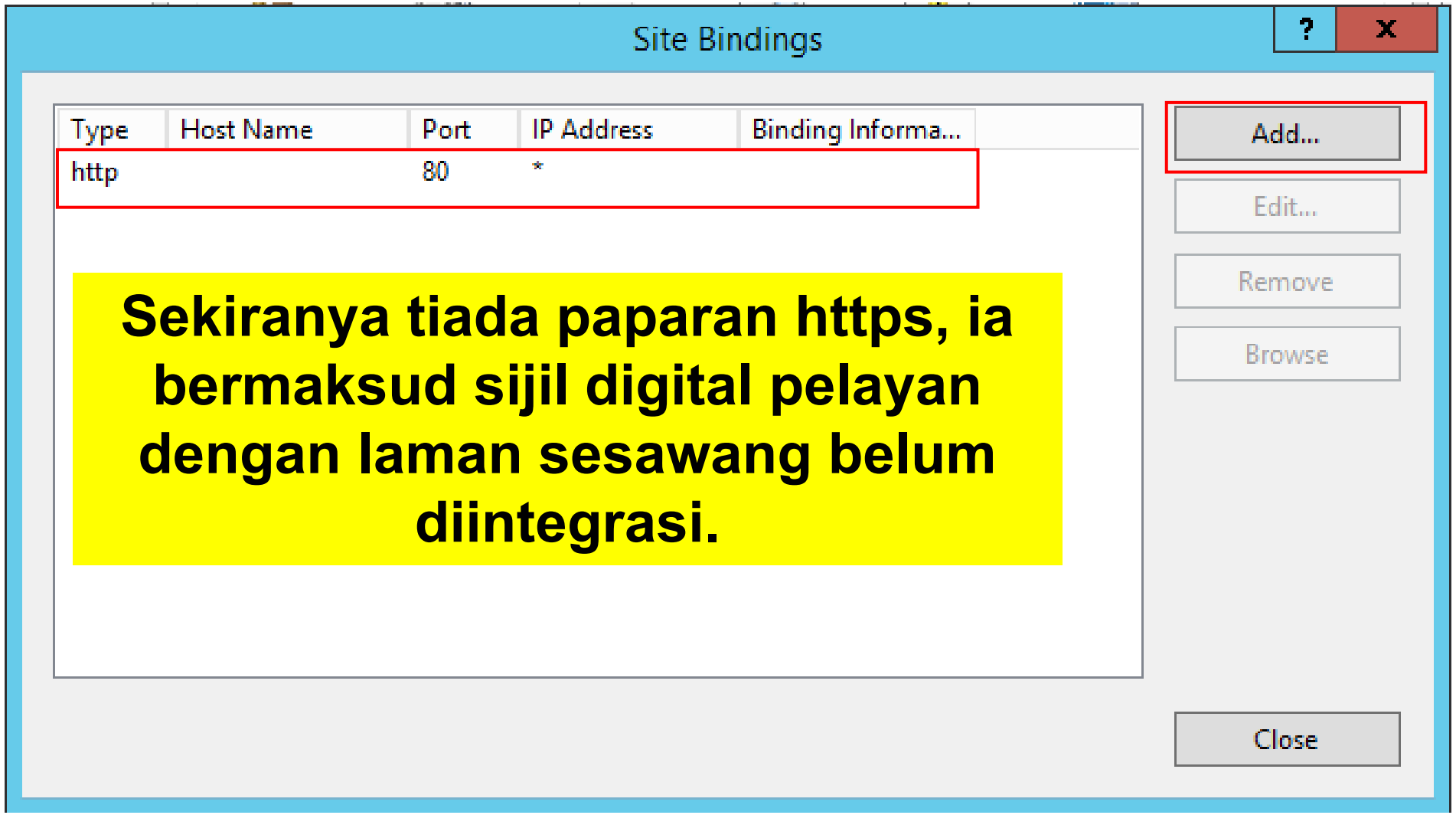
Advanced Settings...

Configure

Limits...

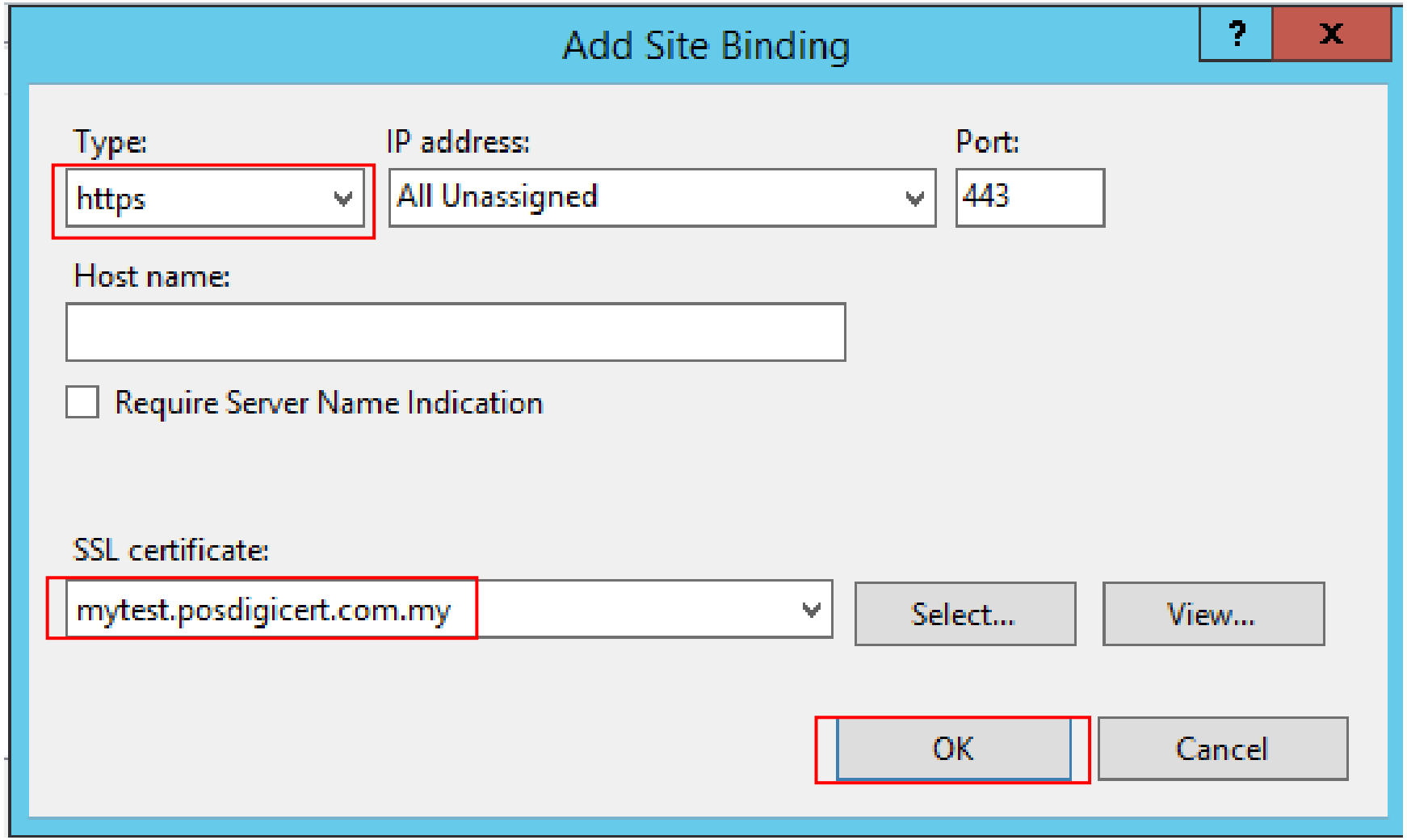
Help

Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web

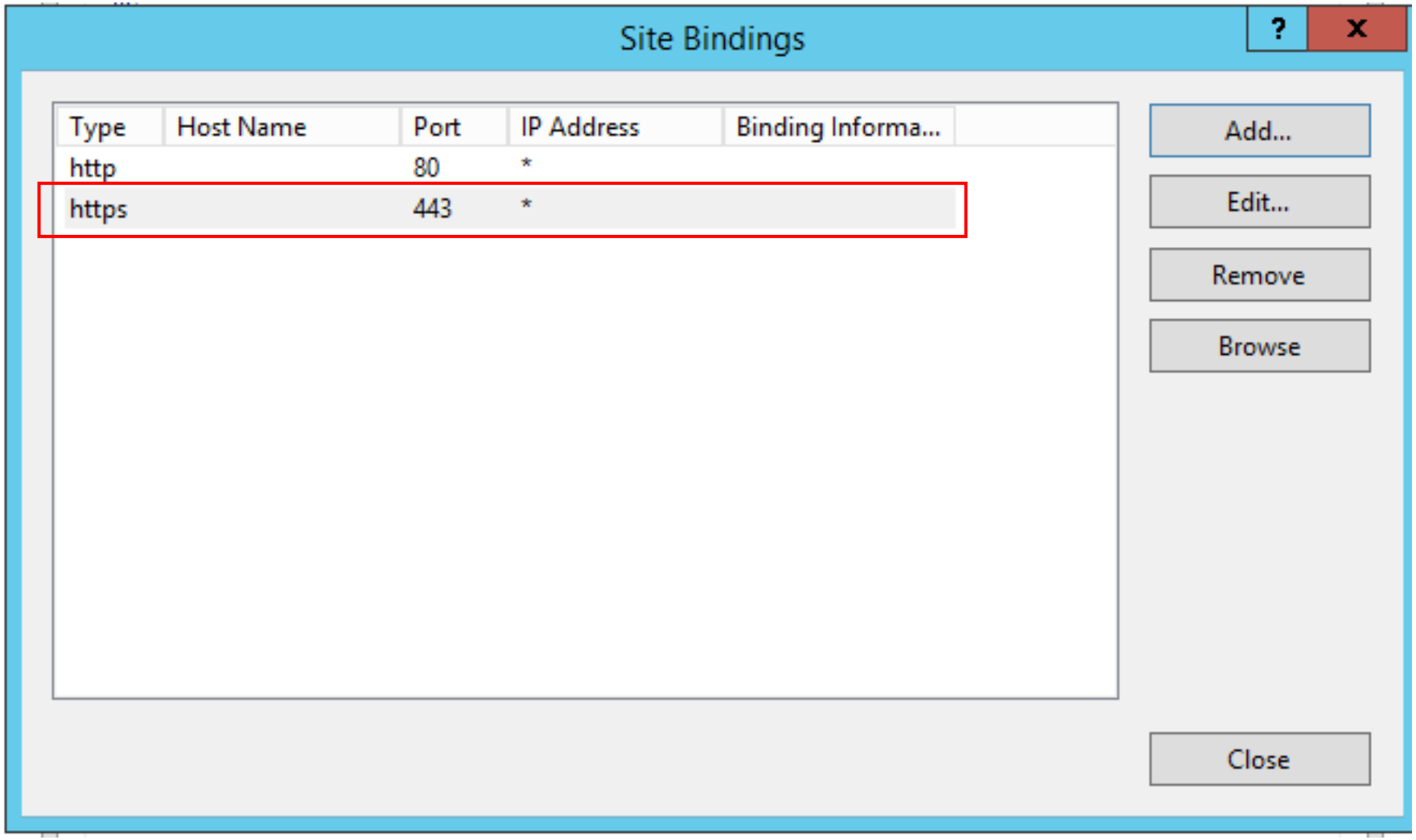


Sekiranya tiada paparan https, ia bermaksud sijil digital pelayan dengan laman sesawang belum diintegrasi.

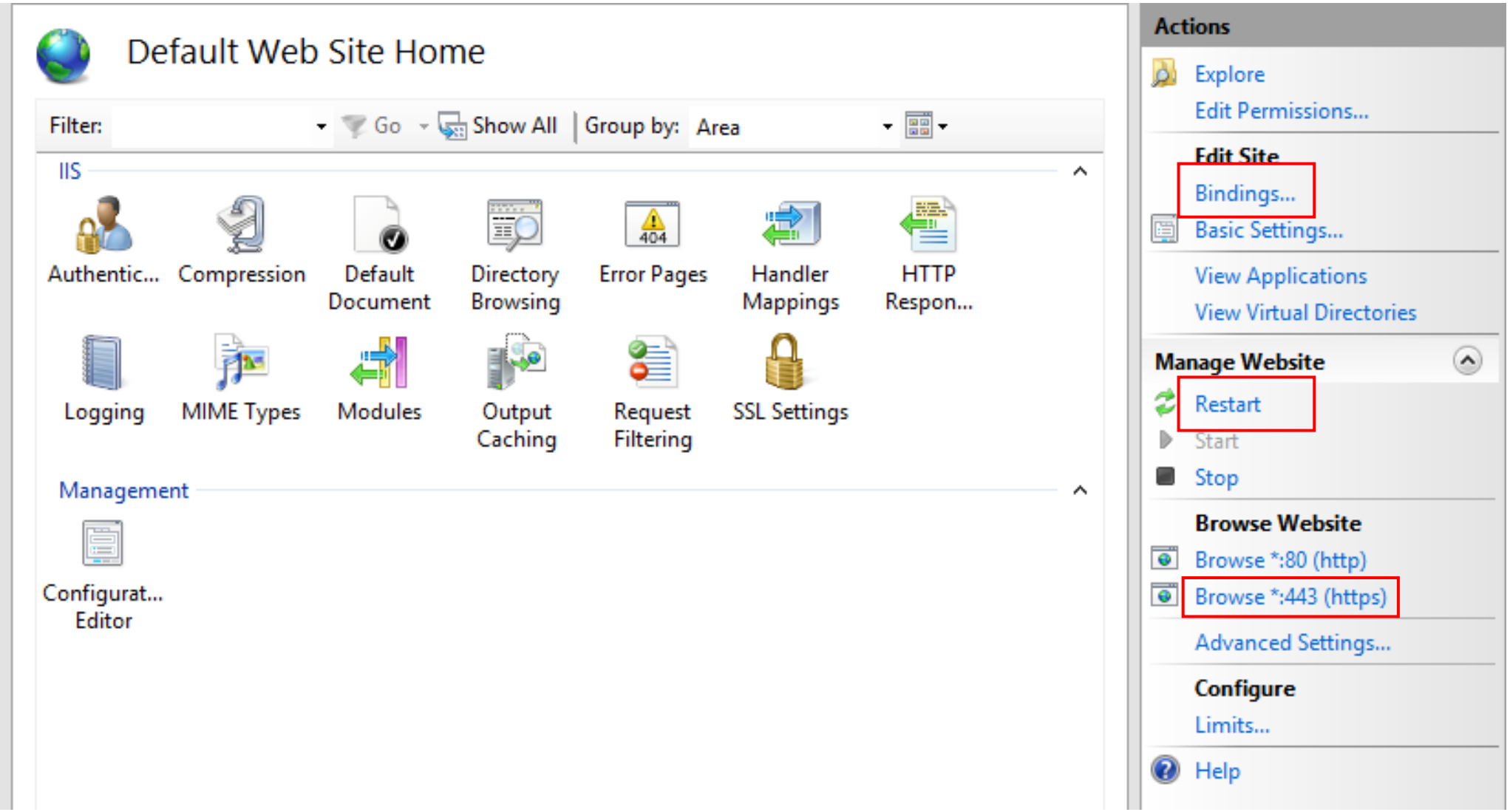
Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web



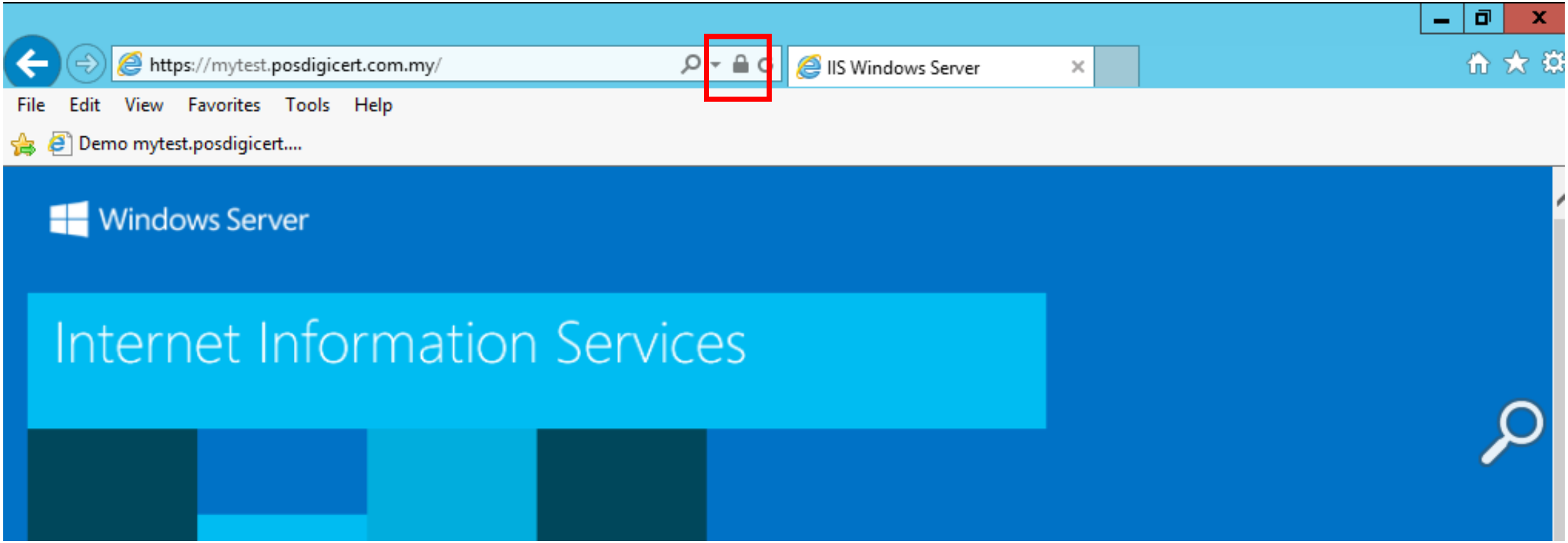
Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web



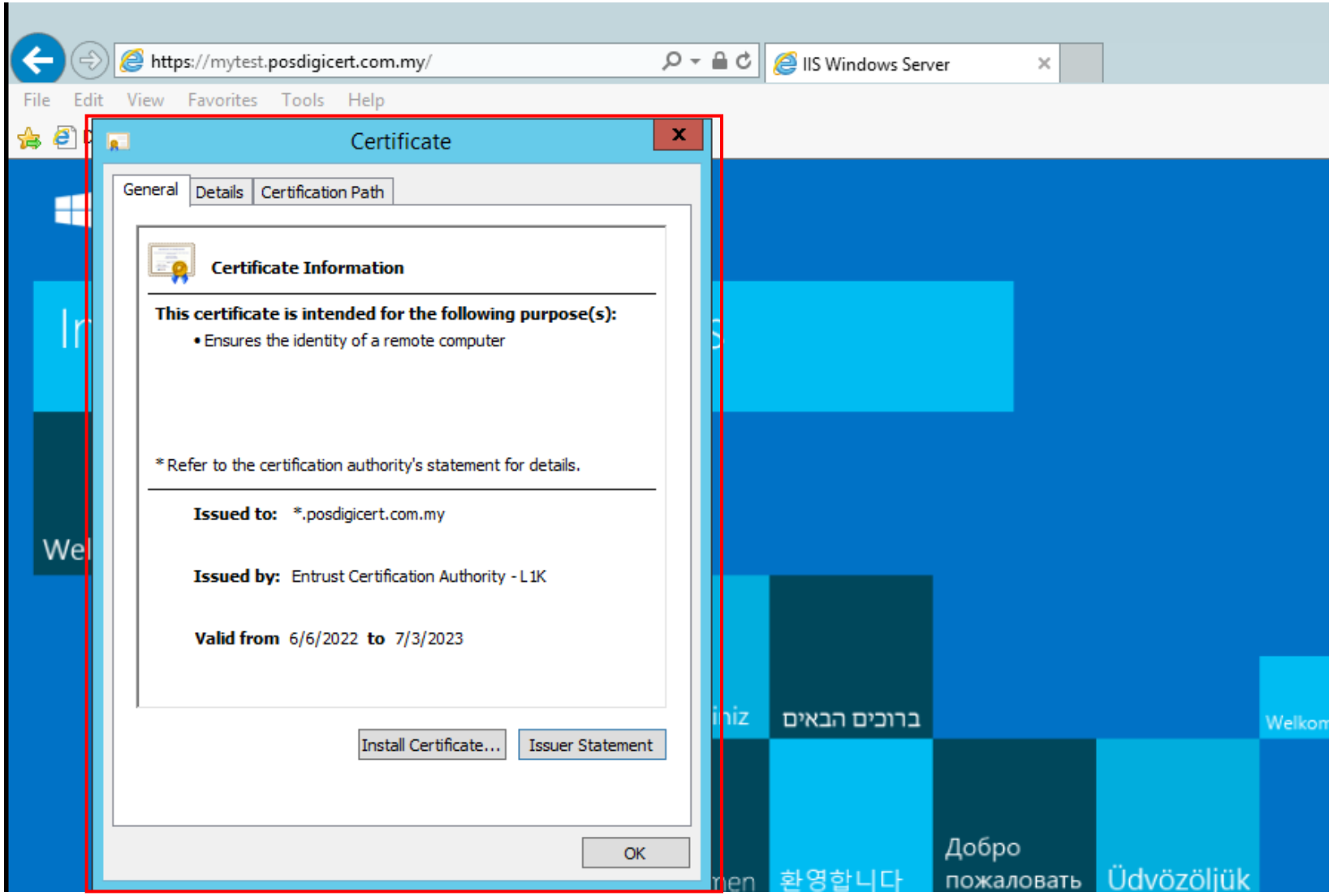
Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web



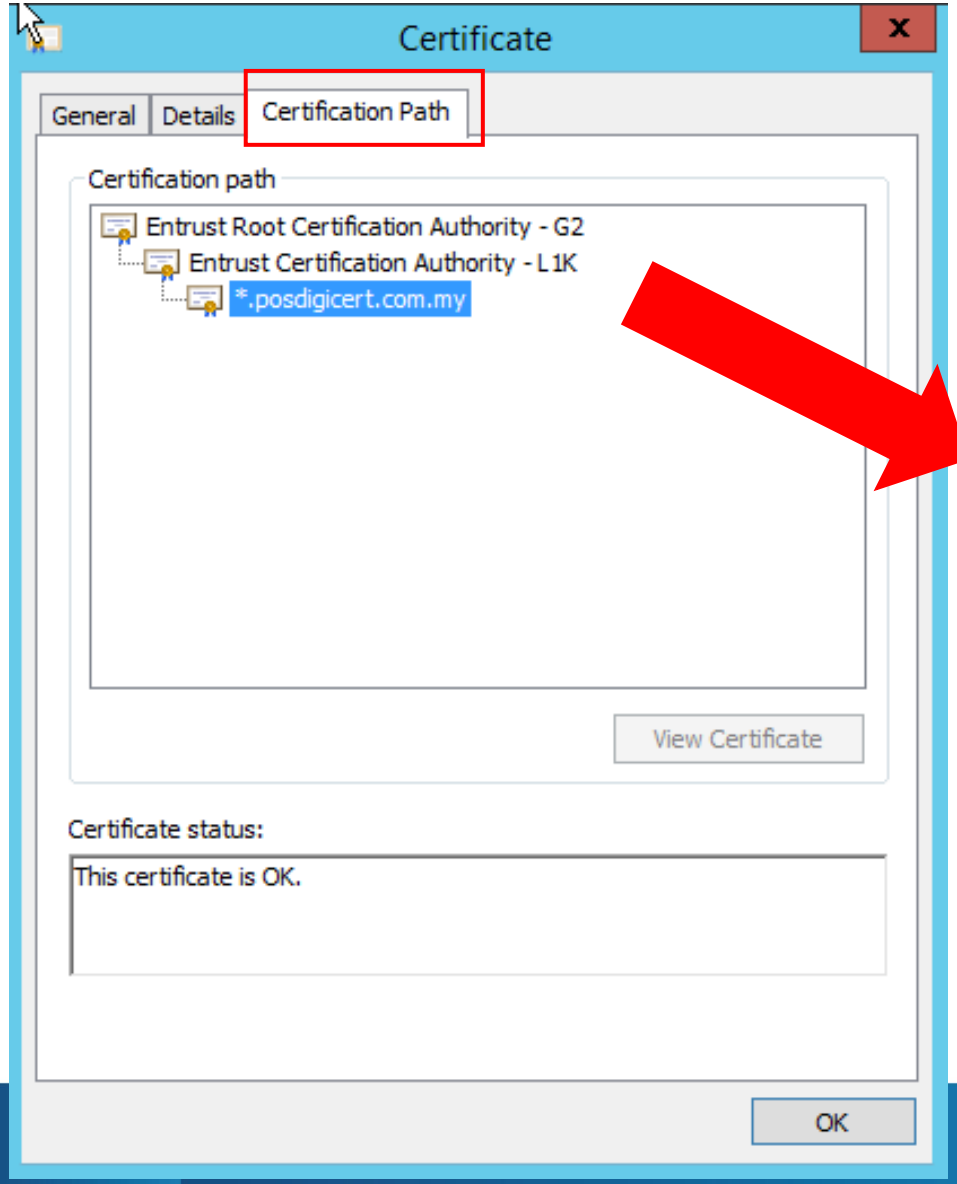
Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web

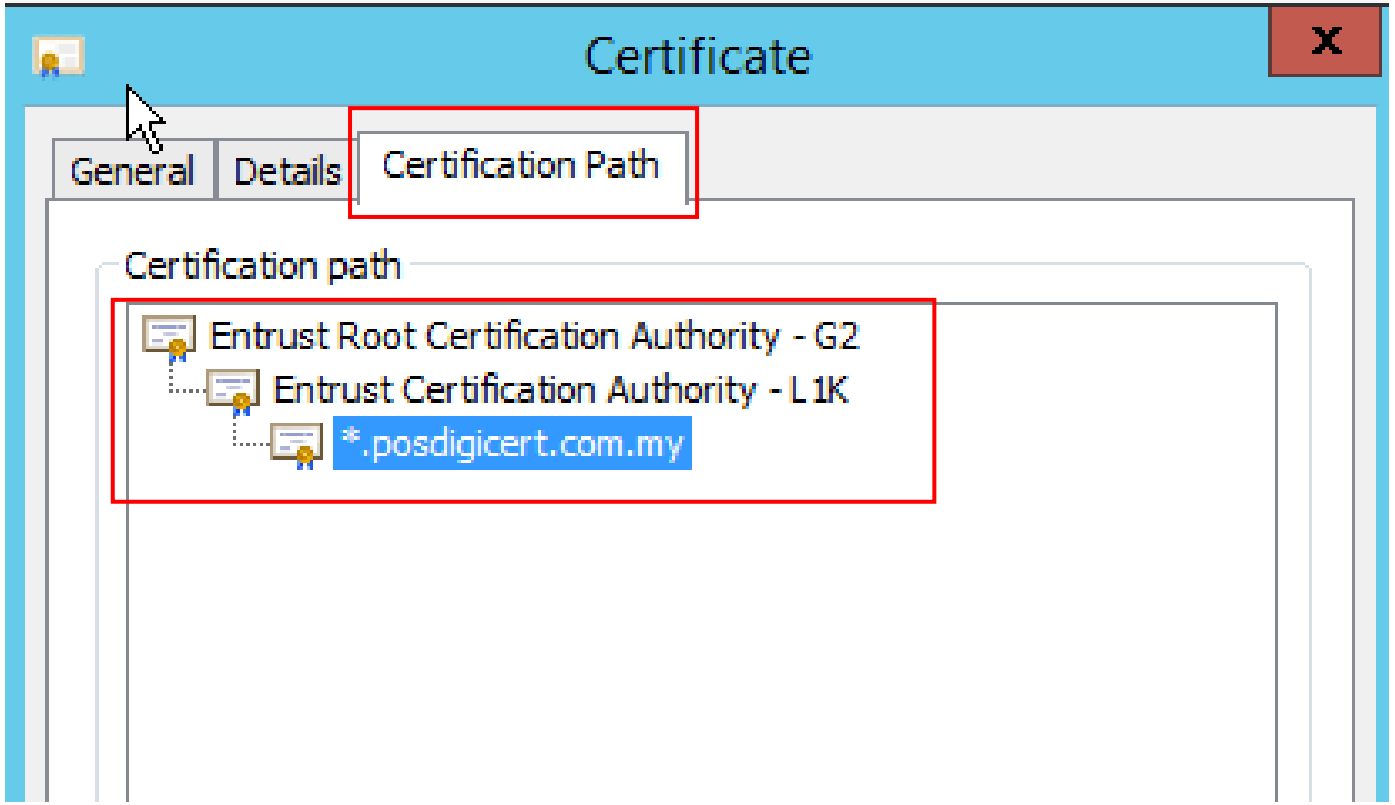


Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web



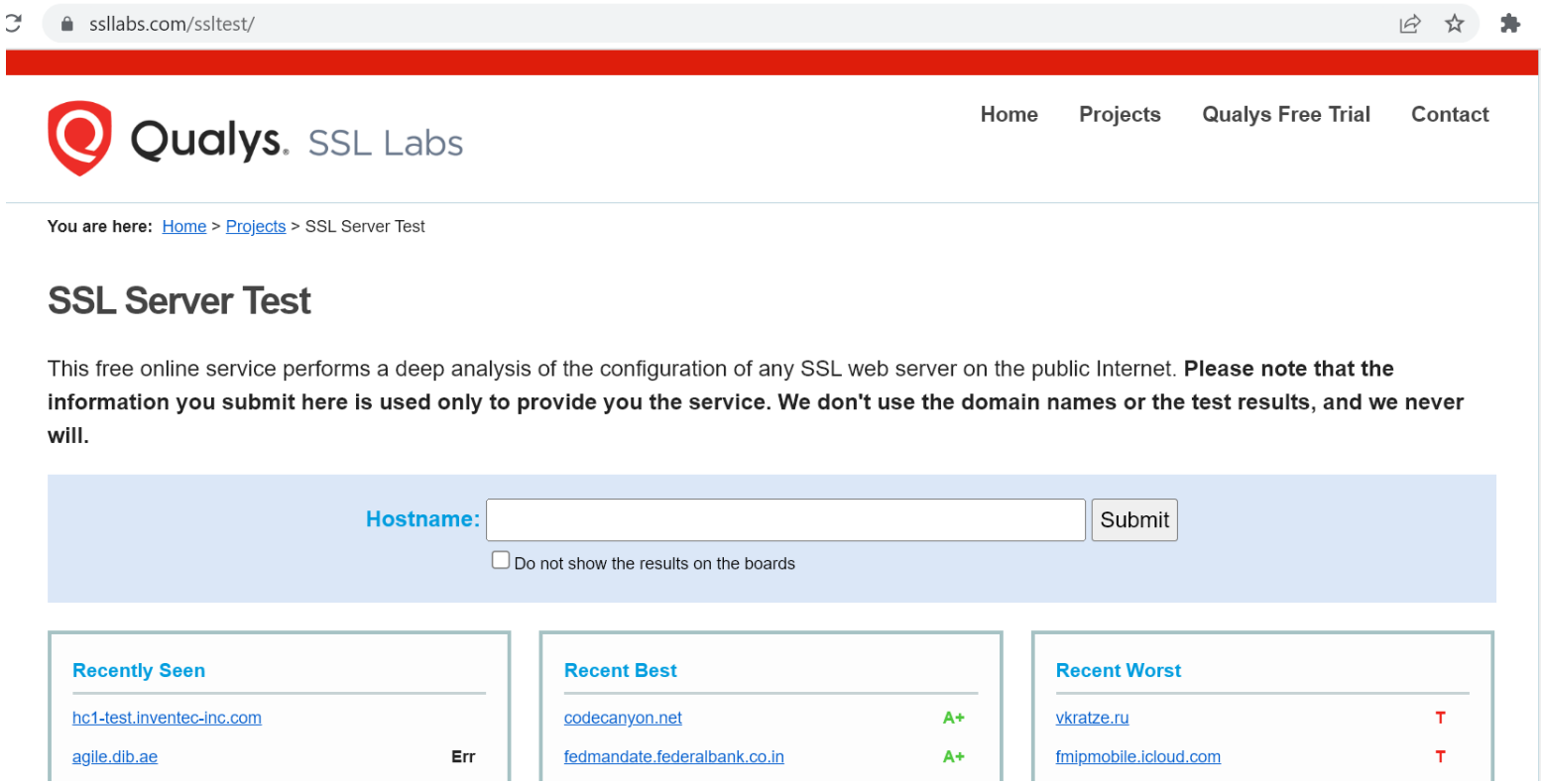
Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web





Bahagian 4: Semak Konfigurasi Sijil Digital

https://www.ssllabs.com/ssltest/



Bahagian 4: Semak Konfigurasi Sijil Digital

Lets Test

Bahagian 4: Semak Konfigurasi Sijil Digital

ssllabs.com/ssltest/

Qualys. SSL Labs

Home Projects

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. I
information you submit here is used only to provide you the service. We don't use the domain names or the
will.

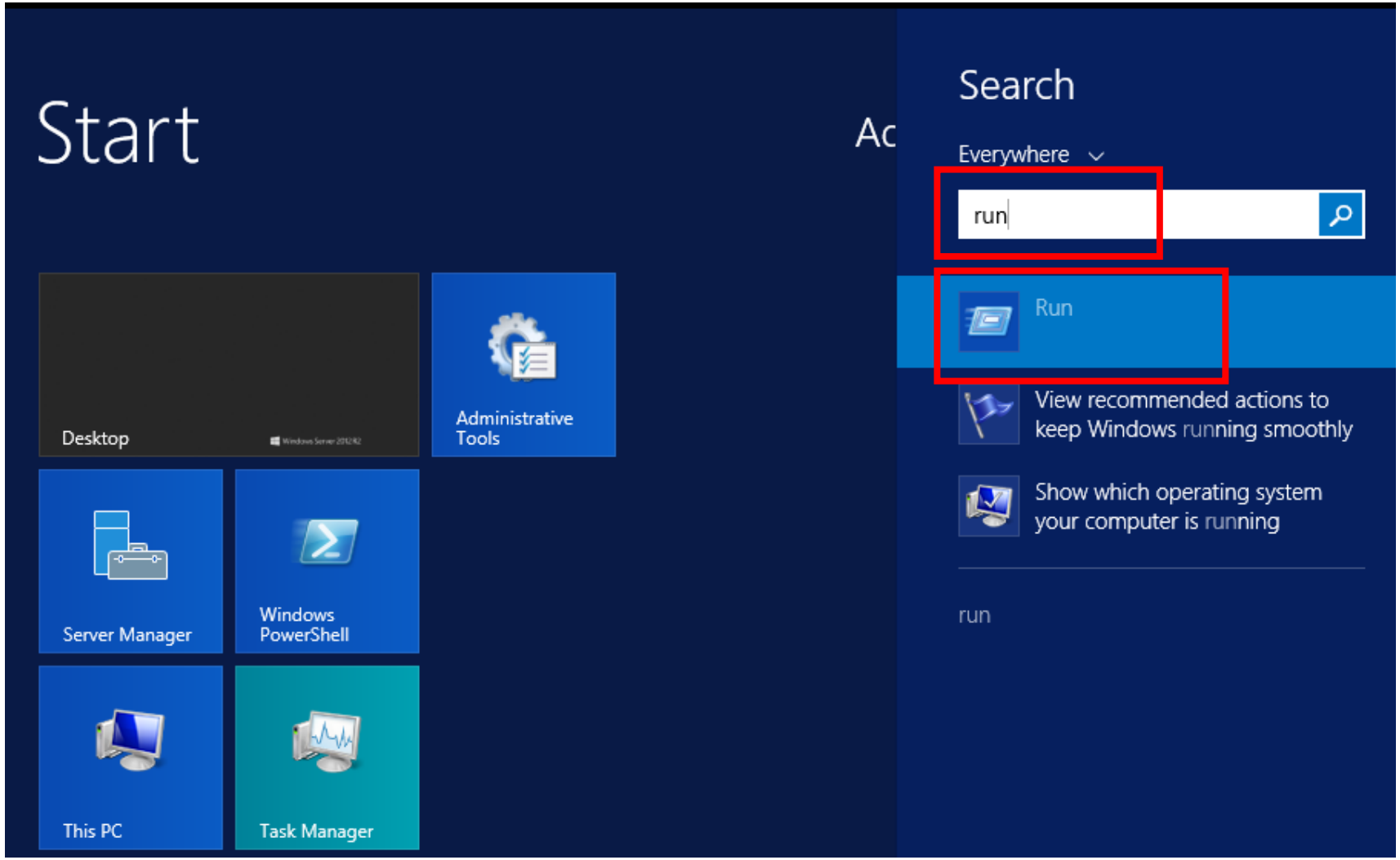
Hostname: Submit

Do not show the results on the boards

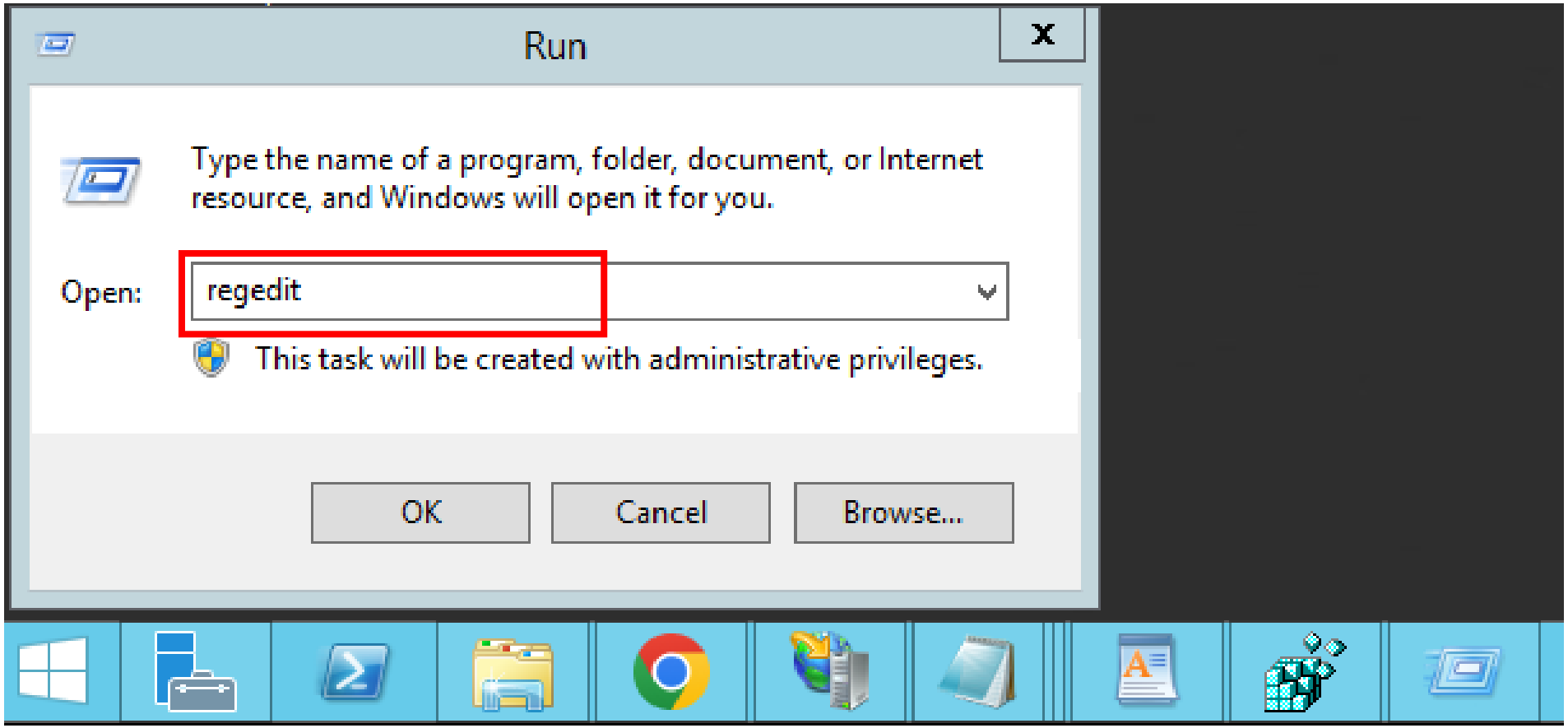
Keputusan Semakan Konfigurasi Sijil Digital

1. https://www.ssllabs.com/ssltest/analyze.html?d=www.posdigicert.com.my

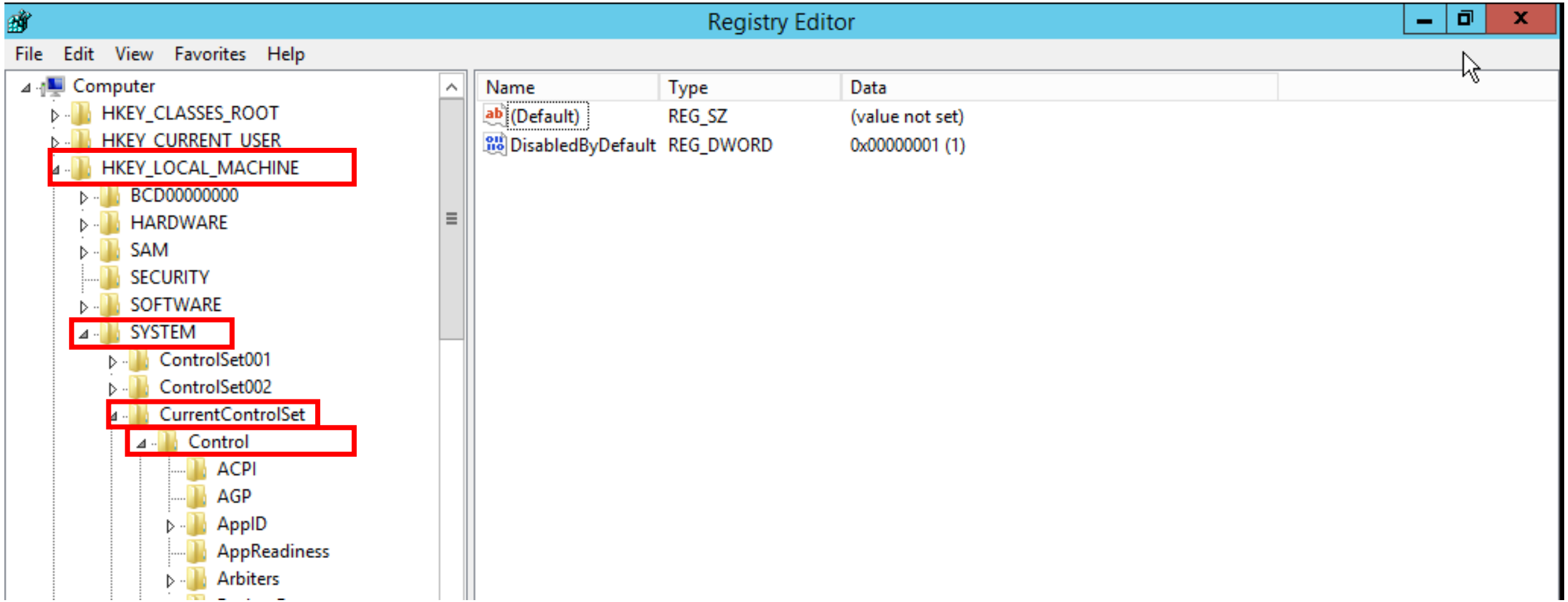
Kemas Kini Konfigurasi



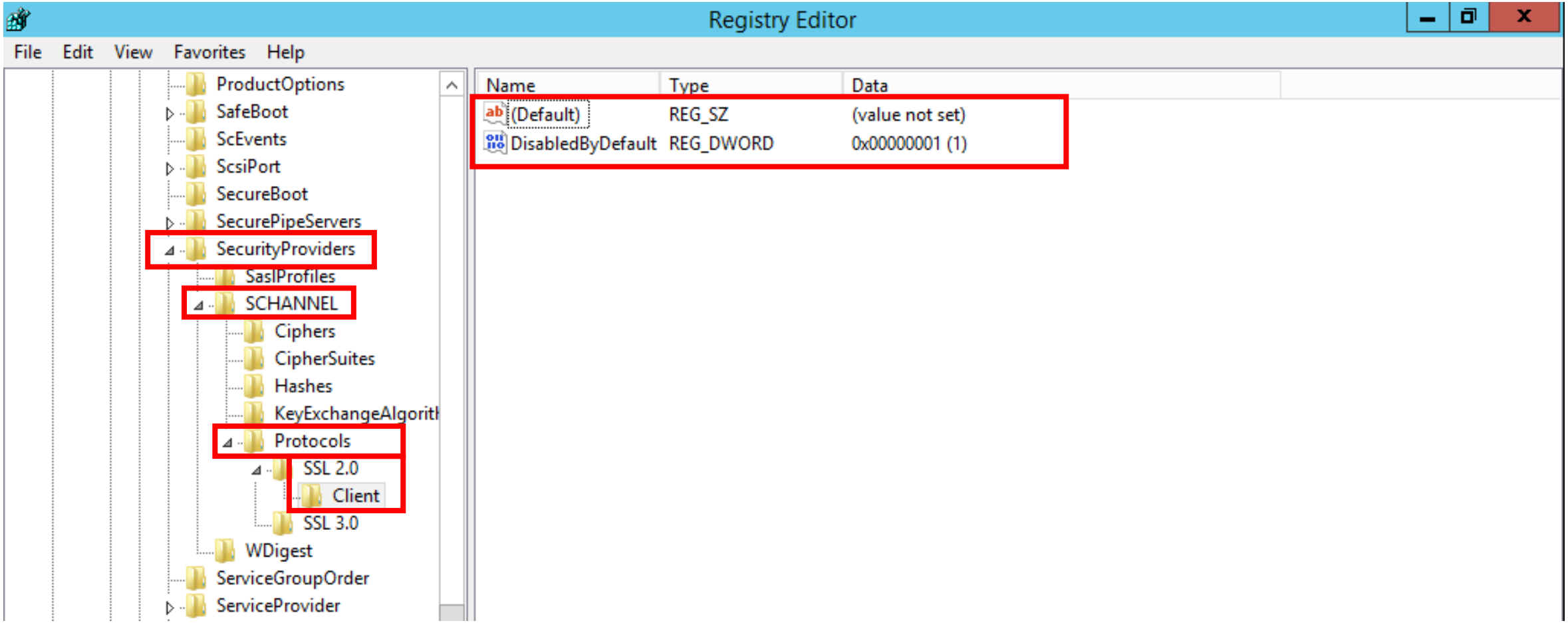
Kemas Kini Konfigurasi



Kemas Kini Konfigurasi



Kemas Kini Konfigurasi



UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

MyGPKI GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Pemasangan Sijil Digital Pelayan

OpenSSL

KeyTool (JSSE)

General Step for SSL Installation

1. Generate Key Pair
2. Generate CSR
3. Submit CSR to CA
4. Receive SSL Certificate from CA
5. Install Certificate
6. Configure SSL on web server or devices

Common Cryptography Software Library

1. Microsoft CryptoAPI (CSP)
2. OpenSSL
3. Java keytool (JKS)
4. IBM Key Management (iKeyMan)
5. Mozilla Network Security Services (NSS)

Crypto Library vs Web Server

Crypto Library	Web Server
SChannel	IIS
OpenSSL	Apache HTTP Server, NGINX
JSSE (Keytool)	Apache Tomcat, JBoss (Wildfly), Weblogic
IBM Java SDK (iKeyMan)	IBM HTTP Server, Websphere
Mozilla NSS (certutil)	Sun Java Web Server

SSL Installation – Apache HTTP (OpenSSL)

- Generate a key pair and CSR

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
-subj "/C=MY/ST=Selangor/L=Cyberjaya/O=MSC
Trustgate.com/CN=www.msctrustgate.com"
```

- Submit CSR file to CA (**server.csr**)
- Receive SSL certificate from CA
- Save SSL certificate as **server.cer**
- Save Intermediate (CA) cert as **cacert.cer**
- Configure httpd.conf or conf.d/ssl.conf

```
SSLCertificateFile /path/to/server.cer
SSLCertificateKeyFile /path/to/server.key
SSLCertificateChainFile /path/to/cacert.cer
```

- Restart Apache (systemctl restart httpd or apachectl –k restart)

Useful OpenSSL command

- Read PEM file

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

- Convert PEM to PKCS#12 (PFX) file

```
openssl pkcs12 -export -out server.pfx -inkey server.key -in server.cer -certfile
cacert.cer
```

- Convert PEM to P7B

```
openssl crl2pkcs7 -nocrl -certfile server.cer -out server.p7b -certfile cacert.cer
```

- Convert PEM to DER

```
openssl x509 -outform der -in server.pem -out server.der
```

- Convert PFX to PEM

```
openssl pkcs12 -in server.pfx -out server.pem -nodes
```

- Convert P7B to PEM

```
openssl pkcs7 -print_certs -in server.p7b -out server.pem
```

- Convert DER to PEM

```
openssl x509 -inform der -in server.der -out server.pem
```

Create a SAN CSR with OpenSSL

- Create an OpenSSL config file with the following content (san.conf)

```
[ 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    = MSC Trustgate.com Sdn. Bhd.
commonName                  = Common Name (e.g. server FQDN or YOUR name)
commonName_max              = 64

[ req_ext ]
subjectAltName = @alt_names

[alt_names]
DNS.1   = www.mytrust365.com
DNS.2   = www.mytrust.biz
DNS.3   = www.mykey.com.my
```

- Use the following command to generate key pair & CSR

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr -subj "/C=MY/ST=Selangor/L=Cyberjaya/O=MSC
Trustgate.com/CN=www.msctrustgate.com" -config san.conf
```

SSL Installation – Apache Tomcat (JKS)

- Generate Key

```
keytool -genkey -keyalg RSA -keysize 2048 -alias tomcat -keystore tomcat.jks
-dname "CN=www.msctrustgate.com, O=MSC Trustgate.com Sdn. Bhd., L=Cyberjaya,
S=Selangor, C=MY"
```

- Generate CSR

```
keytool -certreq -keyalg RSA -alias tomcat -keystore tomcat.jks -file
server.csr
```

- Submit CSR file to CA (server.csr)
- Receive certificates from CA
  - Save SSL certificate as server.cer
  - Save Intermediate (CA) cert as cacert.cer
  - Save Root cert as root.cer

SSL Installation – Apache Tomcat (JKS)

- Install certificate

```
keytool -import -alias root -keystore tomcat.jks -trustcacerts -file
root.cer
keytool -import -alias inter -keystore tomcat.jks -trustcacerts -
file cacert.cer
keytool -import -alias tomcat -keystore tomcat.jks -file server.cer
```

- Update server.xml (Prior Tomcat 8.5)

```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="200" scheme="https" secure="true" SSLEnabled="true"
keystoreFile="/path/to/tomcat.jks" keystorePass="changeit"
clientAuth="false" sslProtocol="TLS"
sslEnabledProtocols="TLSv1.3,TLSv1.2" .../>
```

SSL Installation – Apache Tomcat (JKS)

- Update server.xml (Tomcat 8.5 and later)

```
<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/keystore"
certificateKeystorePassword="changeit" certificateKeyAlias="tomcat"
type="RSA"/>
  </SSLHostConfig>
</Connector>
```

- Restart Tomcat (systemctl restart tomcat)

Useful keytool command

- Read a certificate file

```
keytool -printcert -v -file server.cer
```

- Check certificates in java keystore

```
keytool -list -v -keystore tomcat.jks
```

- Check particular keystore using alias

```
keytool -list -v -keystore tomcat.jks -alias tomcat
```

- Convert PFX to JKS

```
keytool -v -importkeystore -srckeystore server.pfx -srcstoretype PKCS12 -
destkeystore tomcat.jks -deststoretype JKS
```

- Convert JKS to PFX

```
keytool -importkeystore -srckeystore tomcat.jks -srcstoretype JKS -
destkeystore server.pfx -deststoretype PKCS12
```

Create a SAN CSR with Keytool

- Generate Key

```
keytool -genkey -keyalg RSA -keysize 2048 -alias server-cert -keystore server-tomcat.jks -dname "CN=www.msctrustgate.com, O=MSC Trustgate.com Sdn. Bhd., L=Cyberjaya, S=Selangor, C=MY" -ext "SAN=DNS:www.mytrust365.my,DNS:www.mytrust.biz"
```

- Generate CSR

```
keytool -certreq -keyalg RSA -alias server-cert -keystore server-tomcat.jks -file server.csr
```

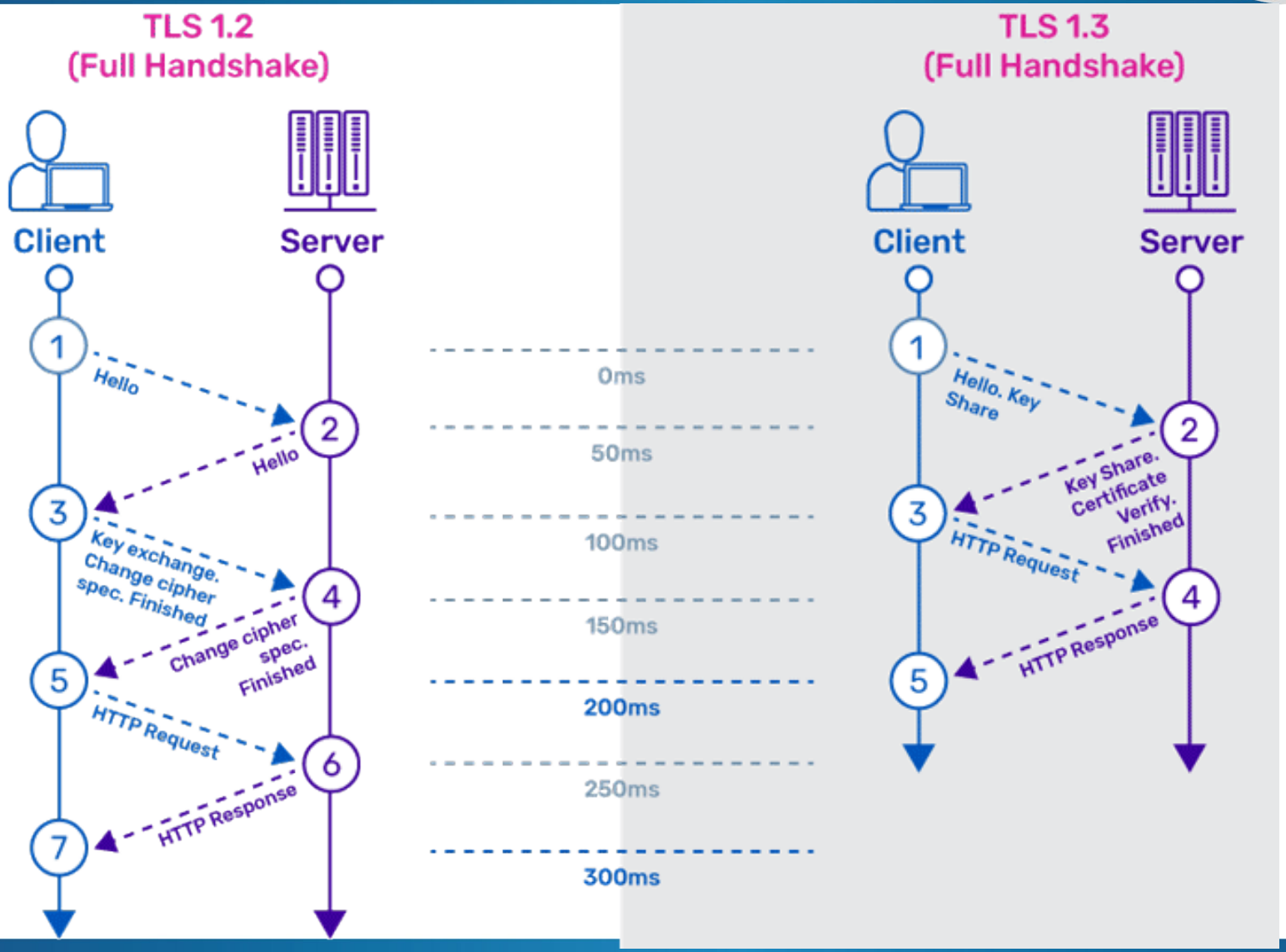
Protocol and Cipher Suites

1. Protocol Security
2. Perfect Forward Secrecy
3. Cipher Suites
4. Best Practices
5. Lab 3 – Securing Web Server Configurations

SSL/TLS Protocol

Protocol	Published	Status	Notes
SSL 1.0	Unpublished	Unpublished	
SSL 2.0	1995	Deprecated in 2011 (RFC 6176)	
SSL 3.0	1996 (RFC 6101)	Deprecated in 2015 (RFC 7568)	2014 – Vulnerable to POODLE attack – affects all block ciphers; RC4 (the only non-block cipher) is also feasibly broken
TLS 1.0	1999 (RFC 2246)	Deprecated in 2020 (RFC 8996)	PCI Council suggest to upgrade to >= TLS 1.1 before 30 June 2018 Oct 2018 – Apple, Microsoft, Google, Mozilla jointly announced to deprecate TLS 1.0 and TLS 1.1 in March 2020
TLS 1.1	2006 (RFC 4346)	Deprecated in 2020 (RFC 8996)	
TLS 1.2	2008 (RFC 5246)		
TLS 1.3	2018 (RFC 8446)		

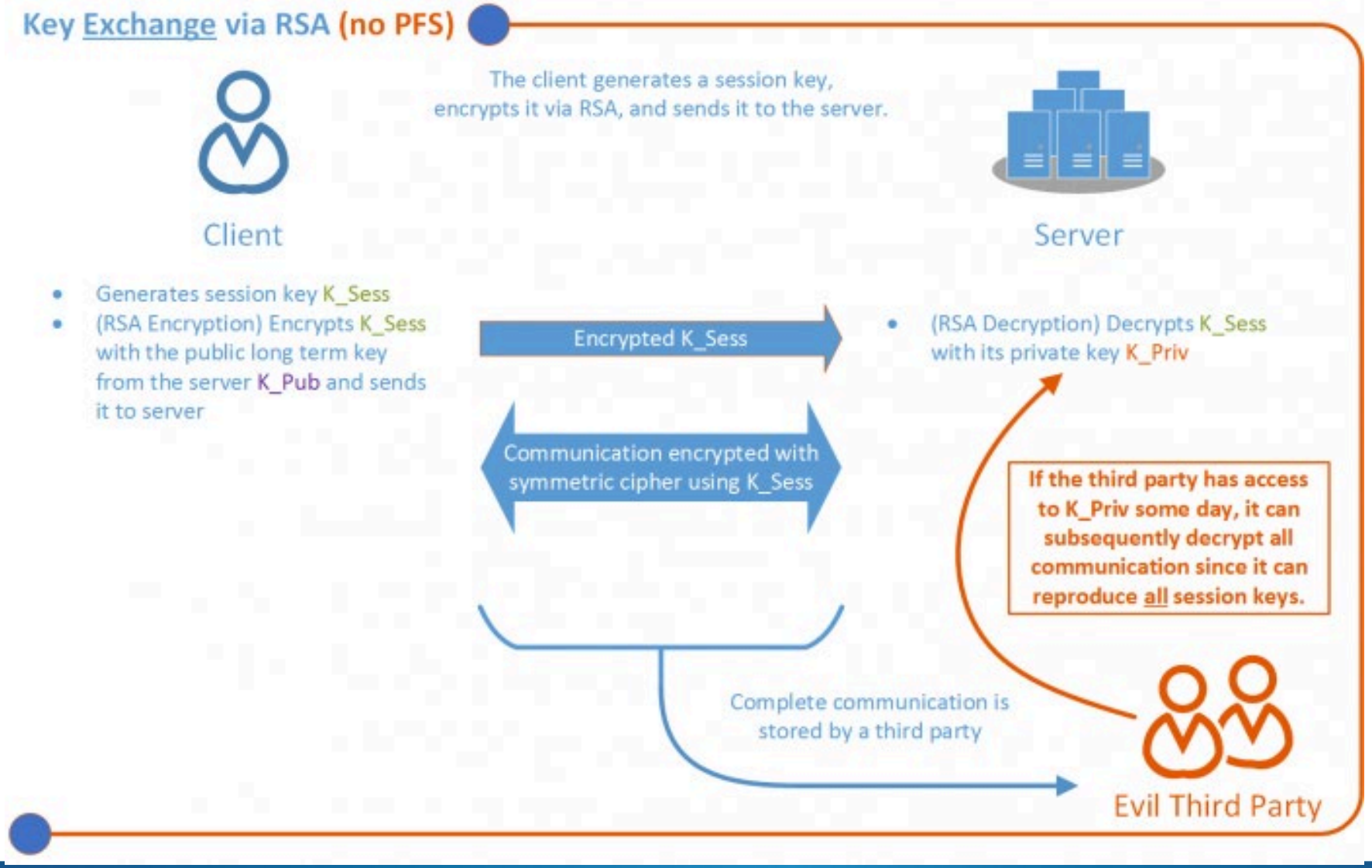
TLS 1.2 vs TLS 1.3



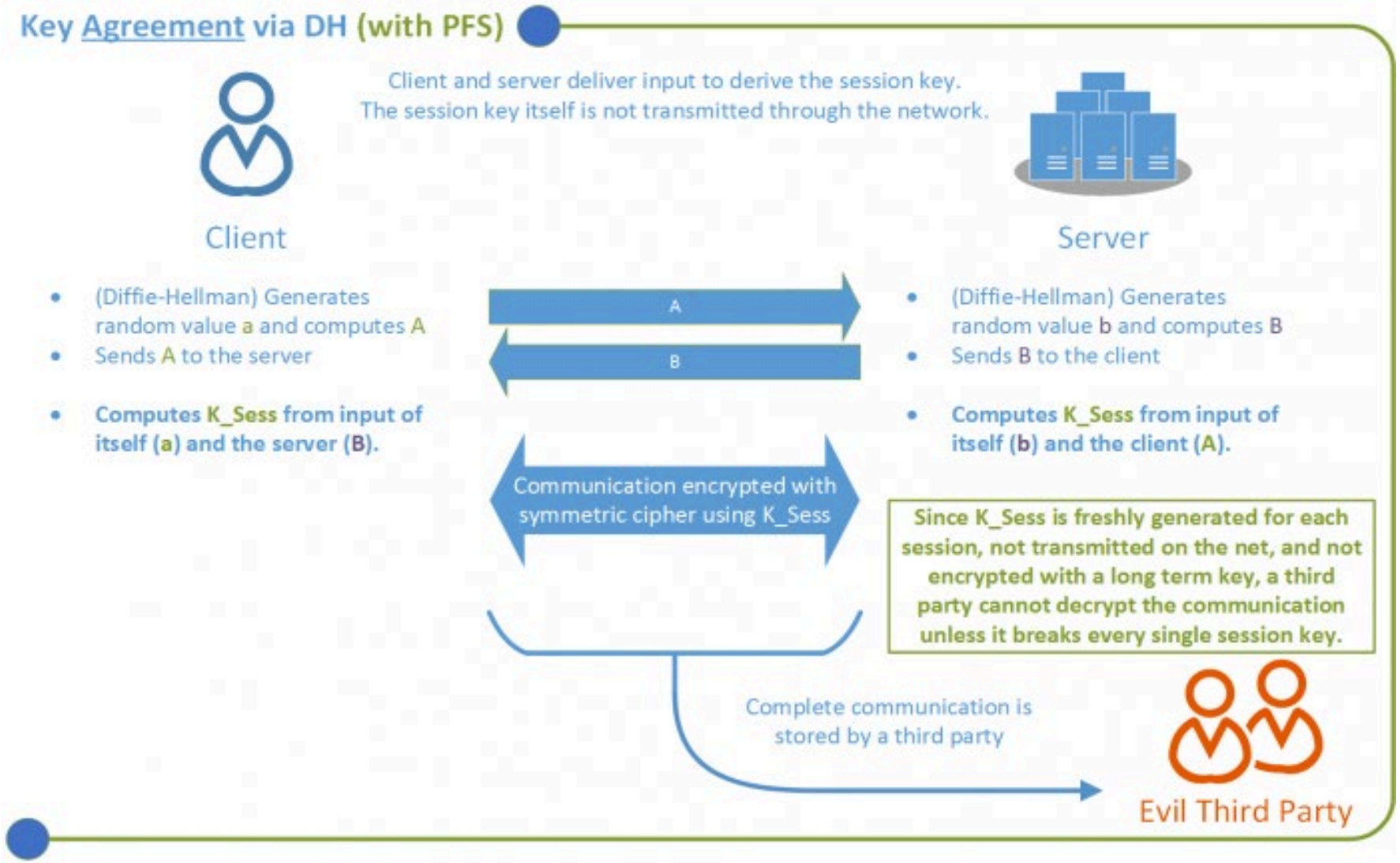
TLS 1.3

- Faster SSL Handshake – lesser packets (0-3 packets) vs 5-7 packets in 1.2
- Simpler, stronger cipher suites – only algorithms no known vulnerabilities and with FPS support
- Zero Round-Trip Time (0-RTT)

Perfect Forward Secrecy (PFS) Overview



Perfect Forward Secrecy (PFS) Overview



SSL Cipher Suites – Naming Scheme TLS 1.2

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Protocol	Key Exchange Algorithm	Key Authentication Algorithm	Bulk Encryption Algorithm	Message Authentication Algorithm
TLS 1.2	Elliptic Curve Diffie-Helman Ephermal	Rivest Shamir Adleman	Algorithm: AES Strength: 128 bit Mode: Galois/Counter Mode	SHA2 256 bit

List of Recommended Cipher (TLS v1.2)

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305

List of Recommended Cipher (TLS v1.3)

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

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

SSL 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

Using Nmap

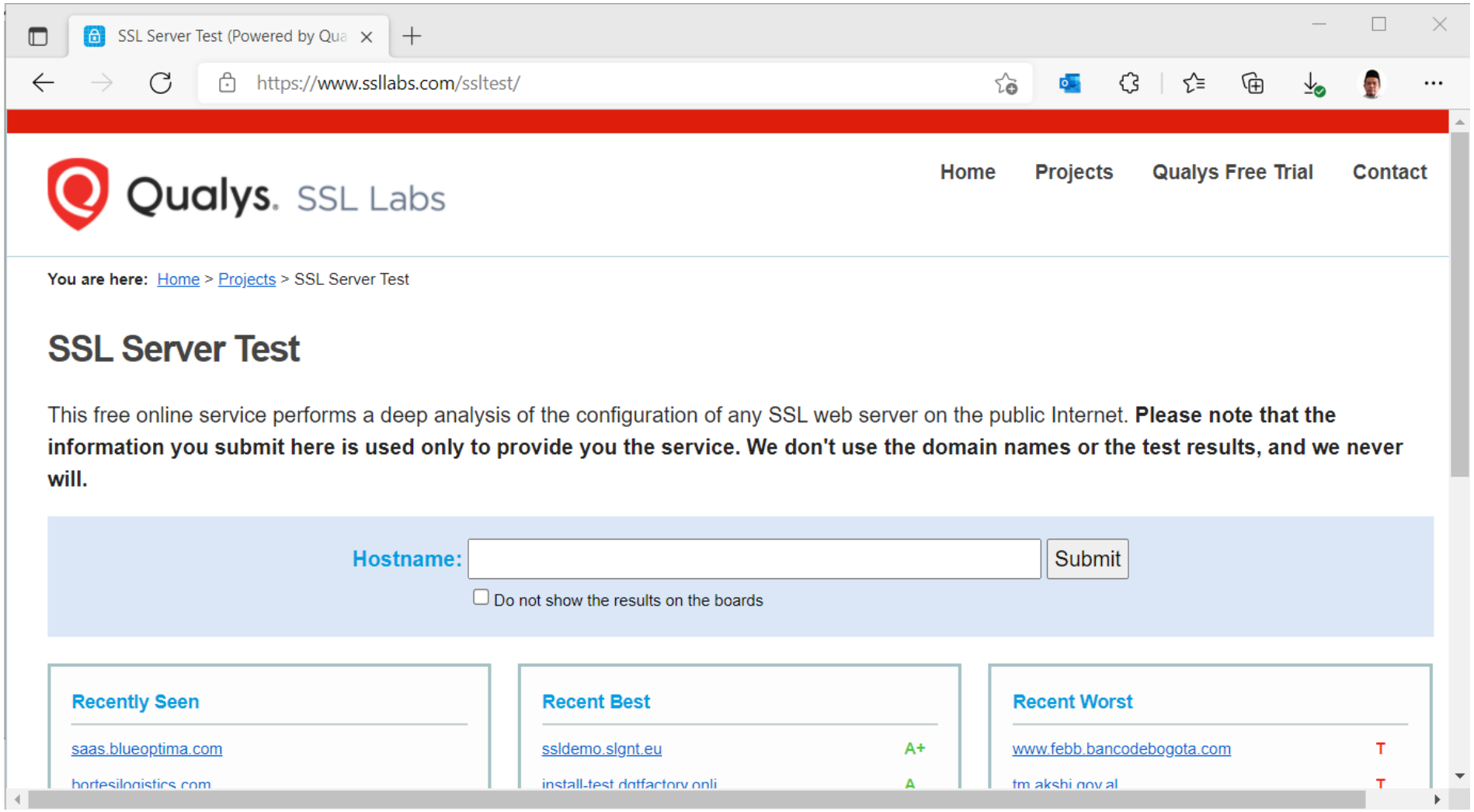
- nmap -sT -PN --script ssl-enum-ciphers.nse <IP Address> [-p <Port>]

```
$ 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
```

Using SSL Server Test



Test SSL connection using OpenSSL

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

Lab 3 – Securing HTTPS Configurations

In this lab, you will enhance HTTPS configuration on previously configured web servers.

- Test SSL connection
- Using nmap to scan for SSL Ciphers Setting
- Enable only TLSv1.2 and TLSv1.3
- Enable server preferences
- Enable ciphers with PFS
- Disable any weak ciphers (Not Grade A)

Bonus – TLS Certificate Lifecycle Management

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

Pengurusan Pentadbir Pelayan & GPKI Mobile

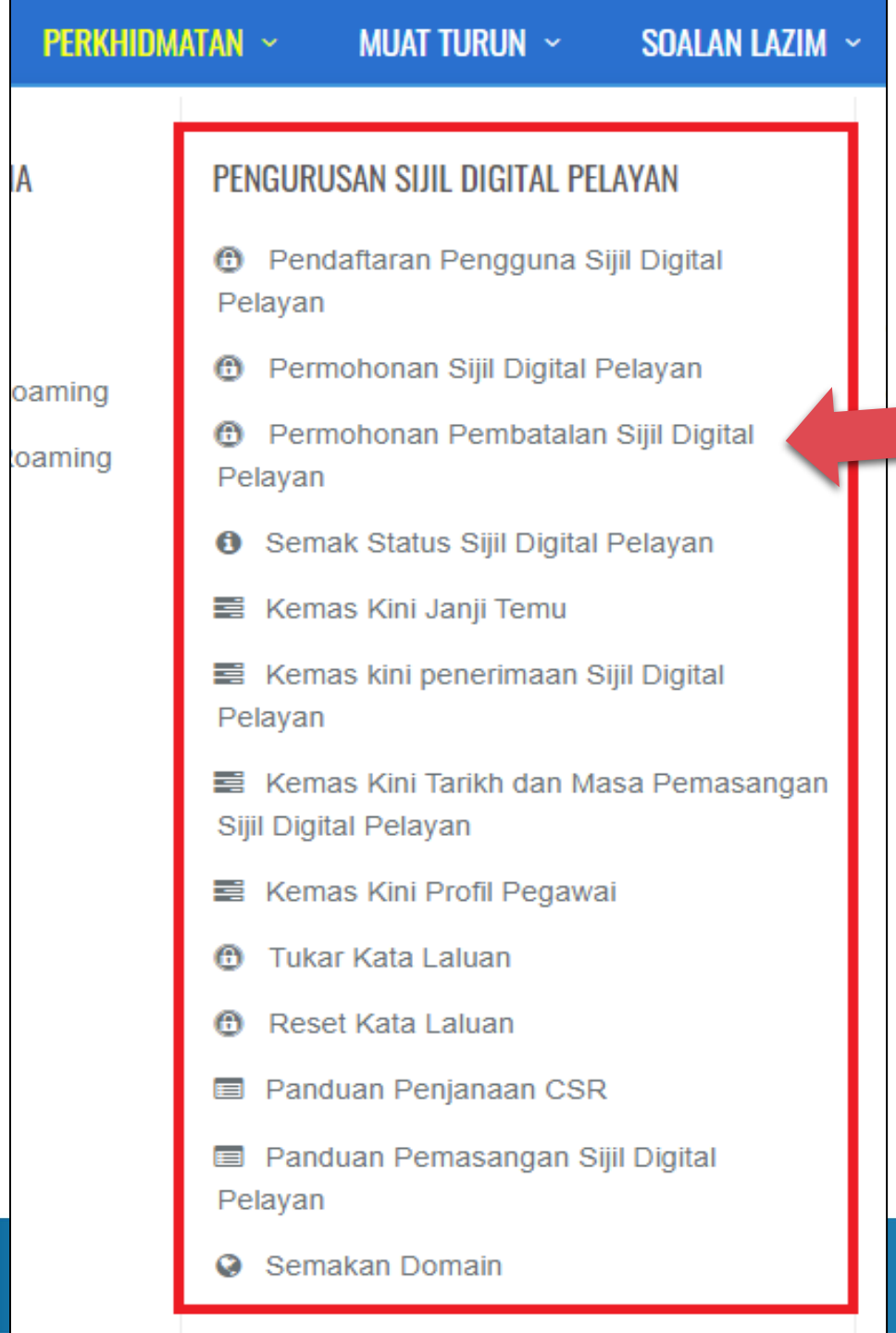
6.1: PENDAFTARAN PENTADBIR PELAYAN DI PORTAL GPKI

6.2: KEMAS KINI PENTADBIR PELAYAN

6.3: GPKI MOBILE UNTUK SSL

6.4: SISTEM GPKI DESK

6.5: SISTEM GPKI 3.0 - PAPARAN SISTEM GPKI eLEARNING

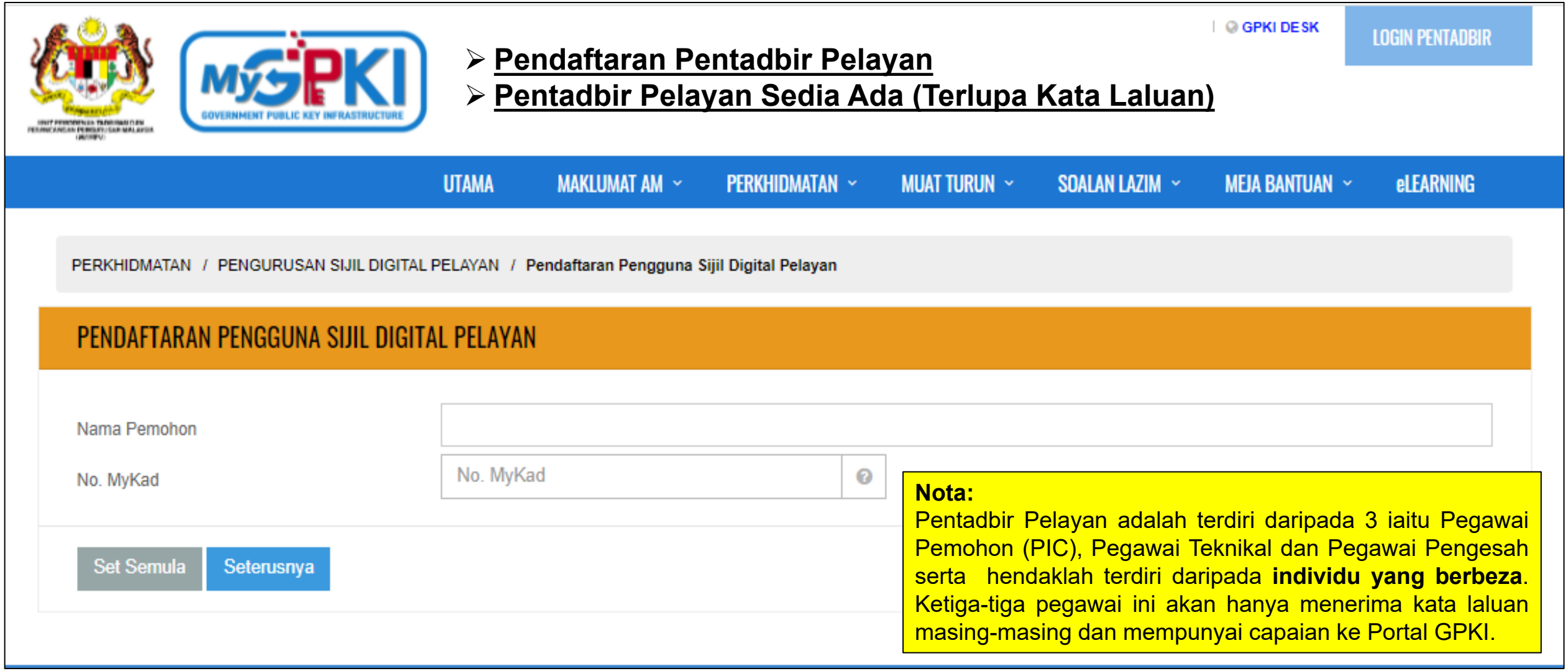


Kesemua 13 menu yang terdapat di bawah Menu "**Pengurusan Sijil Digital Pelayan**" di Portal GPKI 3.0 perlu digunakan oleh pegawai pentabdir pelayan di agensi bagi menguruskan permohonan SSL.

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

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

6.1: PENDAFTARAN PENTADBIR PELAYAN DI PORTAL GPKI



- **Pendaftaran Pentadbir Pelayan**
- **Pentadbir Pelayan Sedia Ada (Terlupa Kata Laluan)**

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 hanya menerima kata laluan masing-masing dan mempunyai capaian ke Portal GPKI.

6.2 KEMAS KINI PENTADBIR PELAYAN

➢ **Pentadbir Pelayan Bertukar atau Berpindah Agensi**

UTAMA | MAKLUMAT AM | PERKHIDMATAN | MUAT TURUN | SOALAN LAZIM | MEJA BANTUAN | eLEARNING

PERKHIDMATAN / PENGURUSAN SIJIL DIGITAL PELAYAN / **Kemas Kini Profil Pegawai**

KEMAS KINI PROFIL PEGAWAI

No. MyKad [redacted]

Kata Laluan ••••••••••••

Set Semula | Seterusnya

Kemas Kini Profil Pegawai / Senarai Permohonan

SENARAI PERMOHONAN PENGGUNA

No.	Nama Pemohon	No. MyKad	Nama Domain	Jenis Sijil Digital Pelayan	Tarikh dan Masa Permohonan	Kementerian / Agensi	Nama Pegawai Teknikal	Nama Pegawai Pengesah	Status	Tindakan
[redacted]	SHAMSUL LAILI BIN MOHAMED YUSOFF	[redacted]	*.mmea.gov.my	Wildcard	26/09/2022 04:07 AM	AGENSI PENGUATKUASAAN MARITIM MALAYSIA	NOOR ASMAH BINTI HALIMI	AIDA BINTI ZULKIFLI	Dalam Tindakan Kelulusan oleh Admin	
[redacted]	SHAMSUL LAILI BIN MOHAMED YUSOFF	[redacted]	www.amsas.gov.my	Single Domain (EV)	30/09/2021 11:14 PM	AGENSI PENGUATKUASAAN MARITIM MALAYSIA	NOOR ASMAH BINTI HALIMI	AIDA BINTI ZULKIFLI	Diterima oleh Pengguna	

6.2 KEMAS KINI PENTADBIR PELAYAN

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)

MyGPKI GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Maklumat Pemohon

Nama	SHAMSUL LAILI BIN MOHAMED YUSOFF
No. MyKad	[redacted]
E-mel	[redacted]
No. Telefon Pejabat	[redacted]
No. Telefon Bimbit	[redacted]
Jawatan	PENOLONG PEGAWAI TEKNOLOGI MAKL
Kementerian / Agensi	AGENSI PENGUATKUASAAN MARITIM MA

Maklumat Pegawai Teknikal

Nama	NOOR ASMAH BINTI HALIMI
No. MyKad	[redacted]
E-mel	[redacted]
No. Telefon Pejabat	[redacted]
No. Telefon Bimbit	[redacted]
Jawatan	PEGAWAI TEKNOLOGI MAKLUMAT
Kementerian / Agensi	AGENSI PENGUATKUASAAN MARITIM MA

Maklumat Sijil Digital | Maklumat Pegawai Terdahulu

Maklumat Pemohon

Maklumat Pegawai Teknikal

Nama	MOHD HAZRI BIN MOHD TAJUDDIN
No. MyKad	[redacted]
E-mel	[redacted]
No. Telefon Pejabat	[redacted]
No. Telefon Bimbit	[redacted]
Jawatan	PENOLONG PENGARAH KANAN
Kementerian / Agensi	KEMENTERIAN DALAM NEGERI

Maklumat Pegawai Pengesah

SEMAK STATUS PERMOHONAN SIJIL

PERKHIDMATAN / PENGURUSAN SIJIL DIGITAL PELAYAN / **Semak Status Sijil Digital Pelayan**

SEMAKAN STATUS SIJIL DIGITAL PELAYAN

No. MyKad [redacted]

Kata Laluan ••••••••••••

Set Semula | Seterusnya

Semakan Status Sijil Digital Pelayan / Maklumat Terperinci

MAKLUMAT TERPERINCI STATUS SIJIL DIGITAL PELAYAN

1	2	3	4	5
Permohonan Sijil Digital	Kelulusan Sijil Digital Pelayan	Proses Sijil Digital Pelayan	Kemas Kini Penerimaan CA	Kemas Kini Penerimaan Pengguna
SHAMSUL LAILI BIN MOHAMED YUSOFF	SABRIYAH BINTI MOHD AKHIR @ KHAIRUDDIN	MOHD AZUAN BIN MOHD ABD KADIR	Pos Digicert	SHAMSUL LAILI BIN MOHAMED YUSOFF
30/09/2021 11:14 PM	01/10/2021 09:08 AM	01/10/2021 05:32 PM	07/10/2021 05:07 PM	07/10/2021 05:10 PM

Maklumat Sijil Digital | Maklumat Arkib Permohonan

Maklumat Permohonan

Jenis Permohonan	**Baharu**
Jenis Sijil Digital Pelayan	**Single Domain (EV)**
Justifikasi Permohonan	**Subdomain ini digunakan bagi Laman web pusat latihan APMM dan knowledge management APMM.**

Maklumat Pemohon

Nama	**SHAMSUL LAILI BIN MOHAMED YUSOFF**
No. MyKad	[redacted]
E-mel	[redacted]
No. Telefon Pejabat	[redacted]
No. Telefon Bimbit	[redacted]
Jawatan	**PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT KANAN**

SEMAK STATUS PERMOHONAN SIJIL

MAKLUMAT TERPERINCI STATUS SIJIL DIGITAL PELAYAN

1	2	3	4	5
Permohonan Sijil Digital	Kelulusan Sijil Digital Pelayan	Proses Sijil Digital Pelayan	Kemas Kini Penerimaan CA	Kemas Kini Penerimaan Pengguna
SHAMSUL LAILI BIN MOHAMED YUSOFF	SABRIYAH BINTI MOHD AKHIR @ KHAIRUDDIN	MOHD AZUAN BIN MOHD ABD KADIR	Pos Digicert	SHAMSUL LAILI BIN MOHAMED YUSOFF
30/08/2021 11:14 PM	01/10/2021 09:08 AM	01/10/2021 05:32 PM	07/10/2021 05:07 PM	07/10/2021 05:10 PM

Maklumat Sijil Digital | **Maklumat Arkib Permohonan**

Rekod Status Permohonan

No.	Tarikh dan Masa Permohonan	Pegawai Bertanggungjawab	Status	Catatan
1	07/10/2021 05:07 PM	890208045011	CA Terima	
2	01/10/2021 05:32 PM	890208045011	Proses	
3	01/10/2021 09:08 AM	700416075426	Diluluskan	New - Diluluskan
4	30/09/2021 11:22 PM	800906045252	Menunggu	Kemas kini Profil Pegawai
5	30/09/2021 10:54 PM	800906045252	KIV	agensi perlu mengemaskini dan memilih klasifikasi dan penilaian risiko yang selaras dengan laporan penilaian risiko yang telah dimuktamadkan.
6	12/10/2021 05:31 PM		Telah Terima	Kemas kini Temu Pemasangan
7	28/09/2021 02:15 PM		Menunggu	
8	30/09/2021 11:14 PM		Menunggu	
9	07/10/2021 10:56 PM		Telah Terima	

KEMAS KINI JANJI TEMU

PERKHIDMATAN / PENGURUSAN SIJIL DIGITAL PELAYAN / **Kemas Kini Janji Temu**

KEMAS KINI JANJI TEMU

No. MyKad: No. MyKad

Kata Laluan:

Cadangan Tarikh dan Masa Janji Temu dengan CA

Cadangan Janji Temu 1: 12/01/2022 03:00 PM

Cadangan Janji Temu 2: 12/01/2022 04:30 PM

Cadangan Janji Temu 3: 13/01/2022 03:00 PM

KEMAS KINI PENERIMAAN SIJIL

PERKHIDMATAN / PENGURUSAN SIJIL DIGITAL PELAYAN / **Kemas Kini Status Penerimaan Sijil Digital Pelayan**

KEMAS KINI STATUS PENERIMAAN SIJIL DIGITAL PELAYAN

No. MyKad [redacted]

Nama Domain direktori.mampu.gov.my

Set Semula | Seterusnya

CA **Telekom Applied Business**

Tarikh dan Masa Penghantaran CA **24/08/2022 03:48 PM**

Tarikh dan Masa Mula Sijil 24/08/2022 03:31 PM

Tarikh dan Masa Akhir Sijil 25/09/2023 03:31 PM

Tarikh dan Masa Penerimaan Sijil

Batal | Hantar

KEMAS KINI PEMASANGAN SIJIL

PERKHIDMATAN / PENGURUSAN SIJIL DIGITAL PELAYAN / **Kemas Kini Tarikh dan Masa Pemasangan**

KEMAS KINI TARIKH DAN MASA PEMASANGAN

No. MyKad: No. MyKad

Kata Laluan:

Set Semula | Seterusnya

No.	Nama Pemohon	No. MyKad	Nama Domain	Jenis Sijil Digital Pelayan	Tarikh dan Masa Permohonan	Tarikh dan Masa Penerimaan	Kementerian / Agensi	Status	Tindakan
1	MUHAMMAD ASRI BIN A BAKAR	821127025191	speks.mampu.gov.my	Multi Domain	26/10/2021 02:37 PM	28/10/2021 12:00 AM	UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA	Diterima oleh Pengguna	

Tarikh dan Masa Pemasangan: Tarikh dan Masa Pemasangan

Catatan:

Batal | Hantar

TUKAR KATA LALUAN

PERKHIDMATAN / PENGURUSAN SIJIL DIGITAL PELAYAN / **Tukar Kata Laluan Pengguna Sijil Digital Pelayan**

TUKAR KATA LALUAN PENGGUNA SIJIL DIGITAL PELAYAN

Nama Pemohon

No. MyKad

Kata Laluan Lama

Kata Laluan Baharu

Set Semula | Hantar

RESET KATA LALUAN

PERKHIDMATAN / PENGURUSAN SIJIL DIGITAL PELAYAN / **Reset Kata Laluan Pengguna Sijil Digital Pelayan**

RESET KATA LALUAN PENGGUNA SIJIL DIGITAL PELAYAN

Nama Pemohon

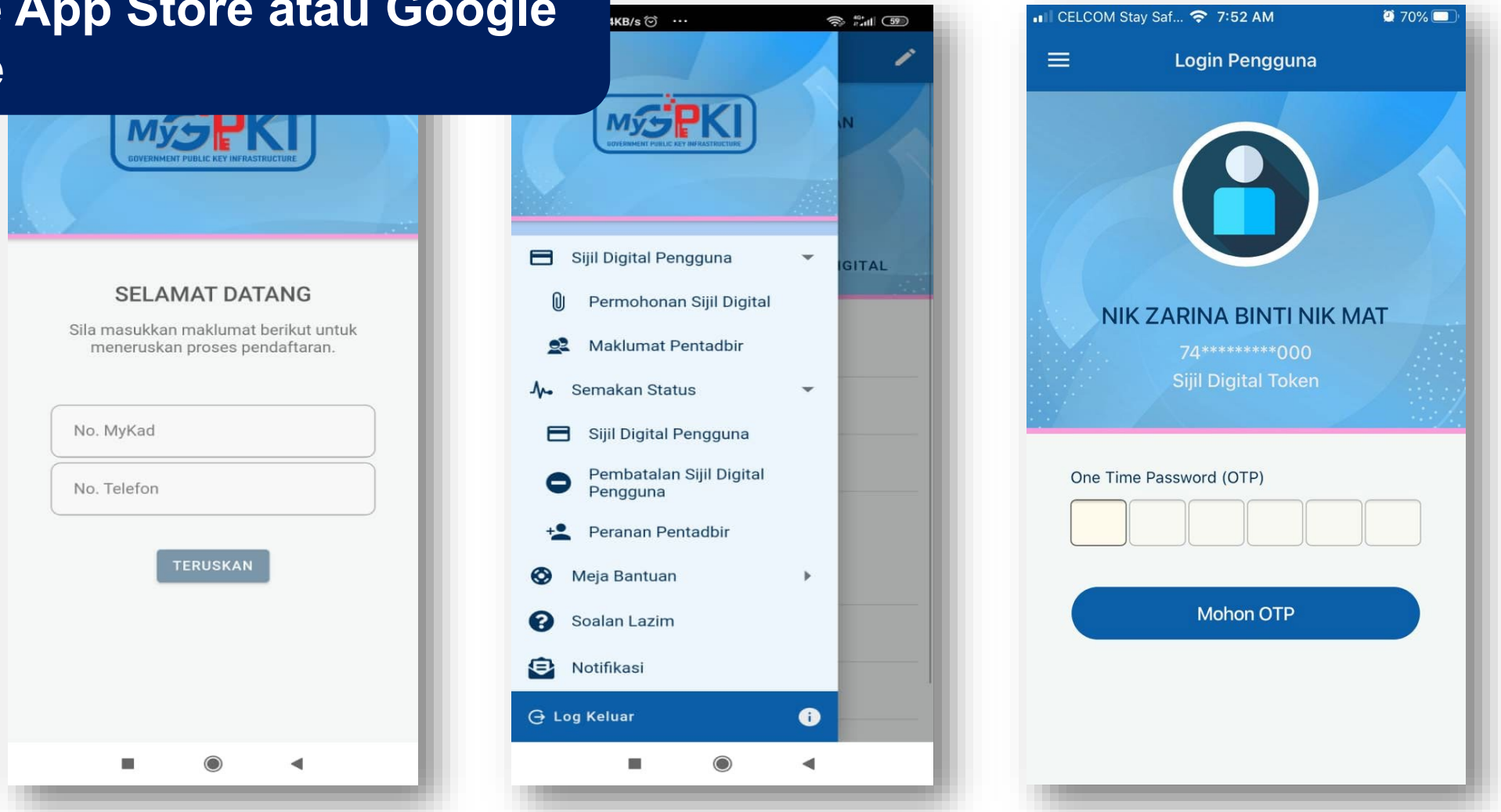
No. MyKad

E-mel

Set Semula | Hantar

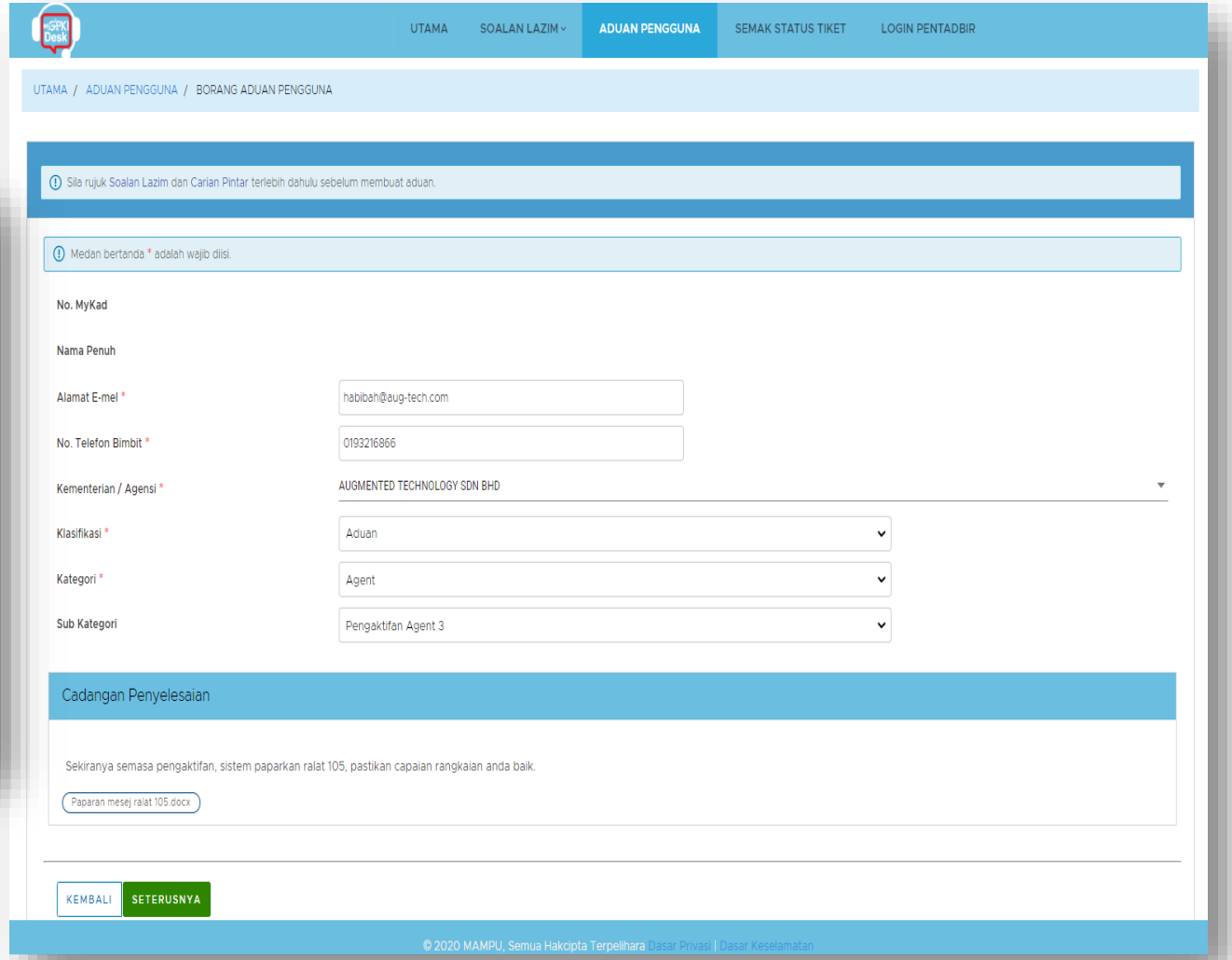
6.3: GPKI MOBILE UNTUK SSL

Muat turun aplikasi GPKI Mobile dari Apple App Store atau Google Play Store



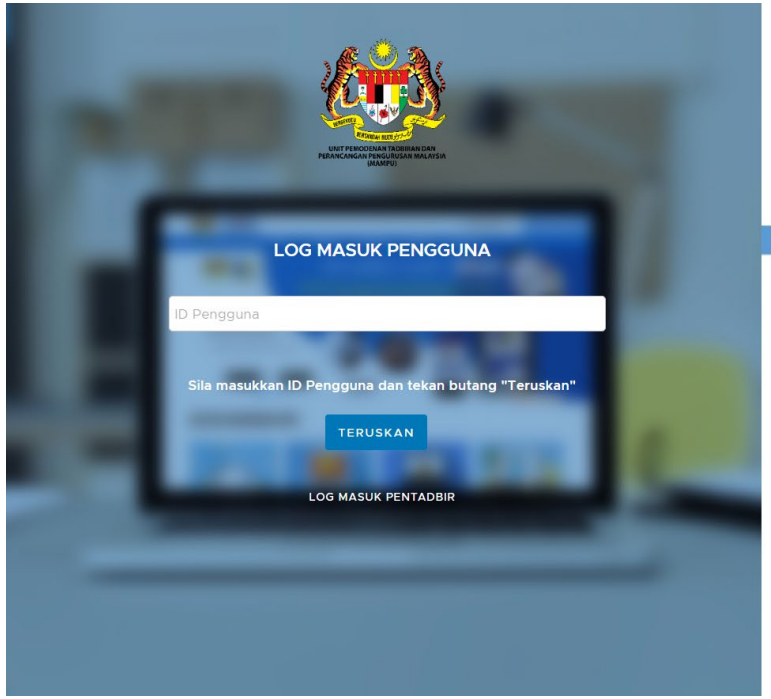
6.4: SISTEM GPKI DESK

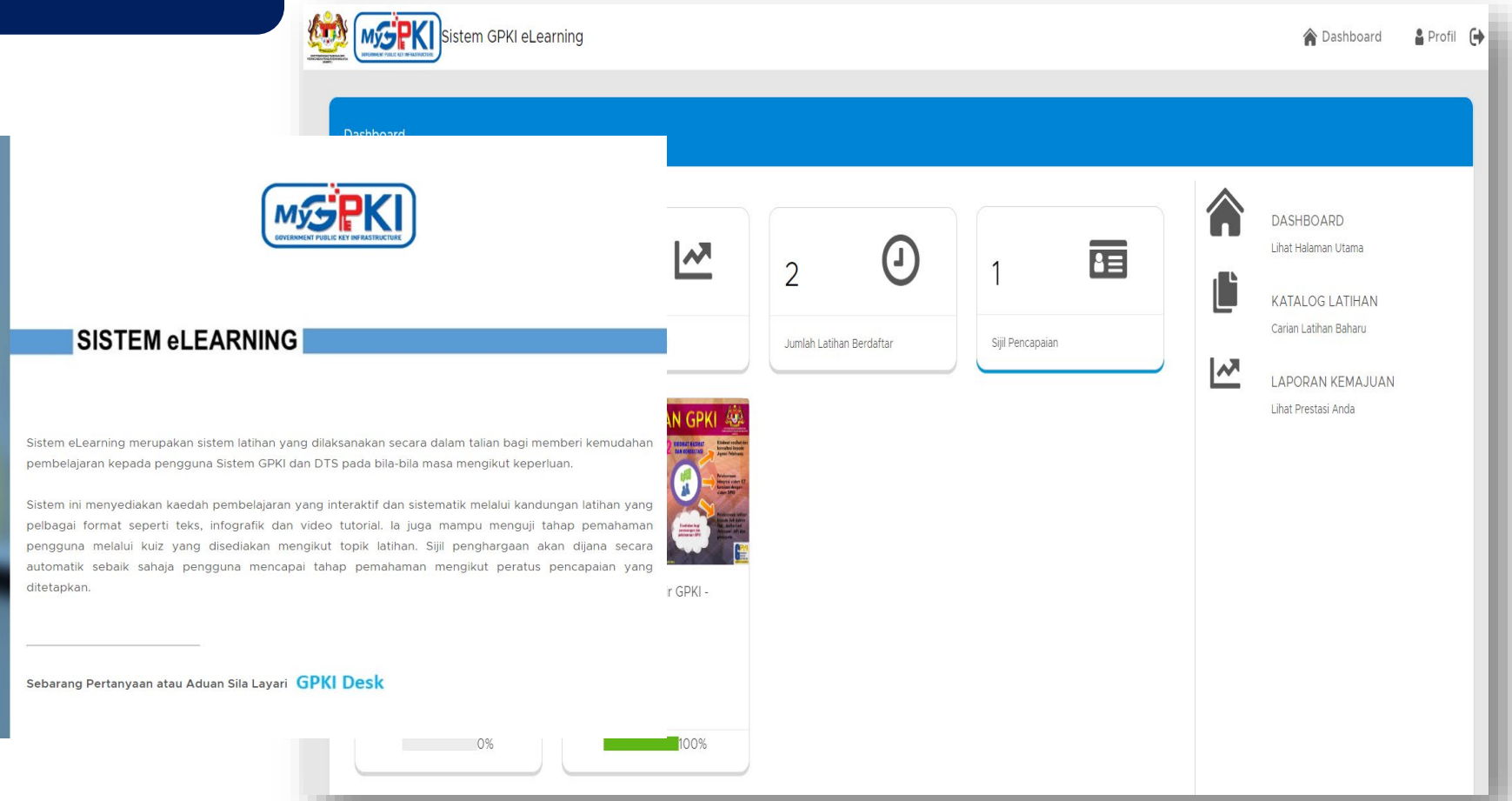
https://gpkidesk.mampu.gov.my



6.5: SISTEM GPKI eLEARNING

https://gpkielearning.mampu.gov.my





TERIMA KASIH