JABATAN PERDANA MENTERI
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA
(MAMPU)

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Seminar Pengurusan Sijil Digital Pelayan (SSL/TLS)

Hotel Marriott Putrajaya
3 Oktober 2023

Agenda

Masa	Agenda
8:00 AM	Pendaftaran Peserta dan Sarapan pagi
9:00 AM	Ucapan Aluan dan Perasmian
9:15 AM	Topik 1: Jom Kenali SSL/TLS
10.00 AM	Topik 2: Sijil Digital Pelayan Perkhidmatan MyGPKI
10:40 AM	Rehat
11:00 AM	Topik 3: Permohonan & Pengurusan Sijil Digital Pelayan
12:45 PM	Makan tengah hari dan Solat
2:15 PM	Topik 4: POV: e-vetting SSL/TLS
3.00 PM	Topik 5: Jom *Install & Test-lah* SSL/TLS
4:45 PM	Penyampaian Hadiah dan Cabutan Bertuah
5:00 PM	Minum Petang dan Bersurai

Kandungan Taklimat Sijil Digital Pelayan

01 Jom Kenali SSL/TLS

02 Sijil Digital Pelayan Perkhidmatan MyGPKI

03 Permohonan & Pengurusan Sijil Digital Pelayan

04 POV: e-vetting SSL/TLS

05 Jom Install & Test-lah SSL/TLS

JABATAN PERDANA MENTERI
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA
(MAMPU)

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Seminar Pengurusan Sijil Digital Pelayan (SSL/TLS)

Hotel Marriott Putrajaya
3 Oktober 2023

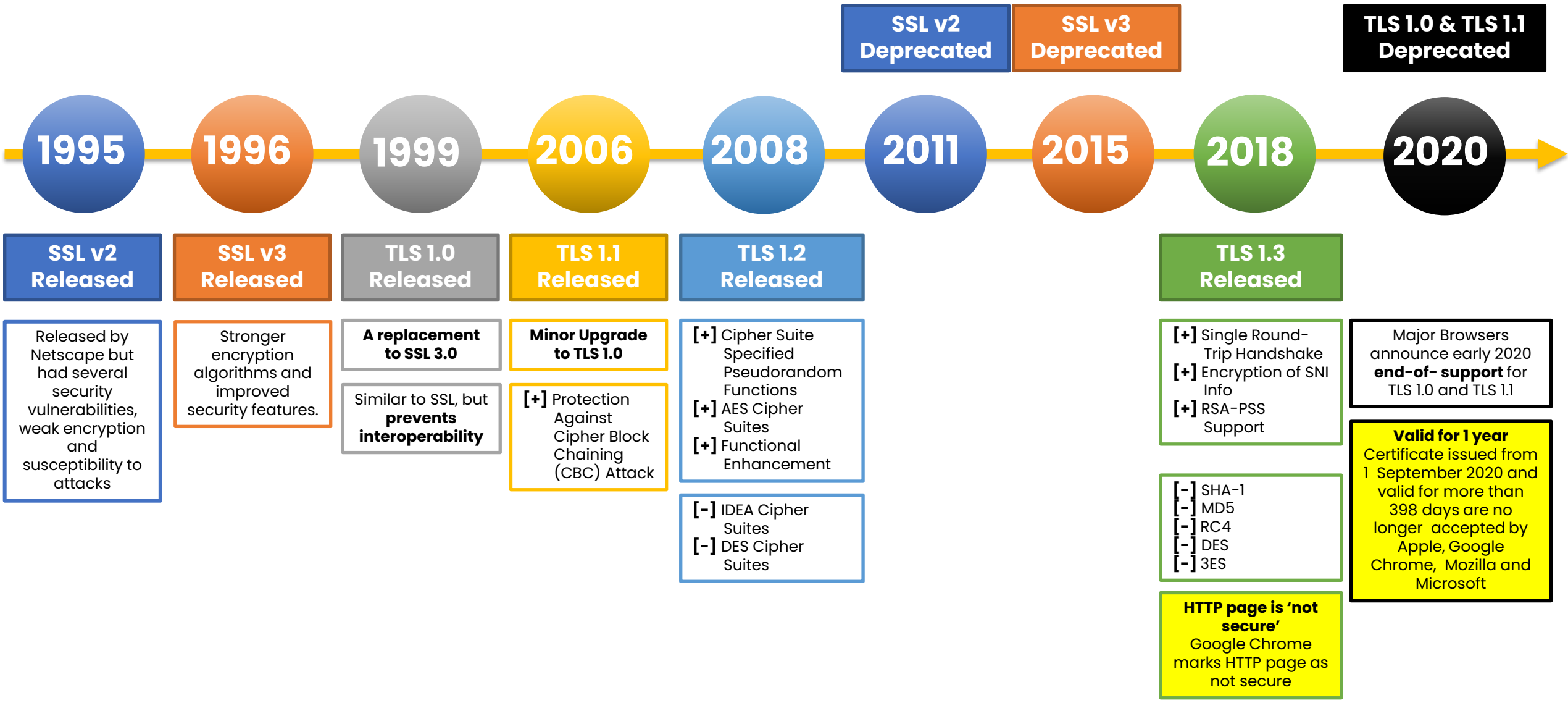
Topik 1:
Jom Kenali SSL/TLS

What is SSL/TLS?

Secure Socket Layer (SSL) / Transport Layer Security (TLS) is a security protocol designed to secure communication between a web browser and web server through authentication and encryption.

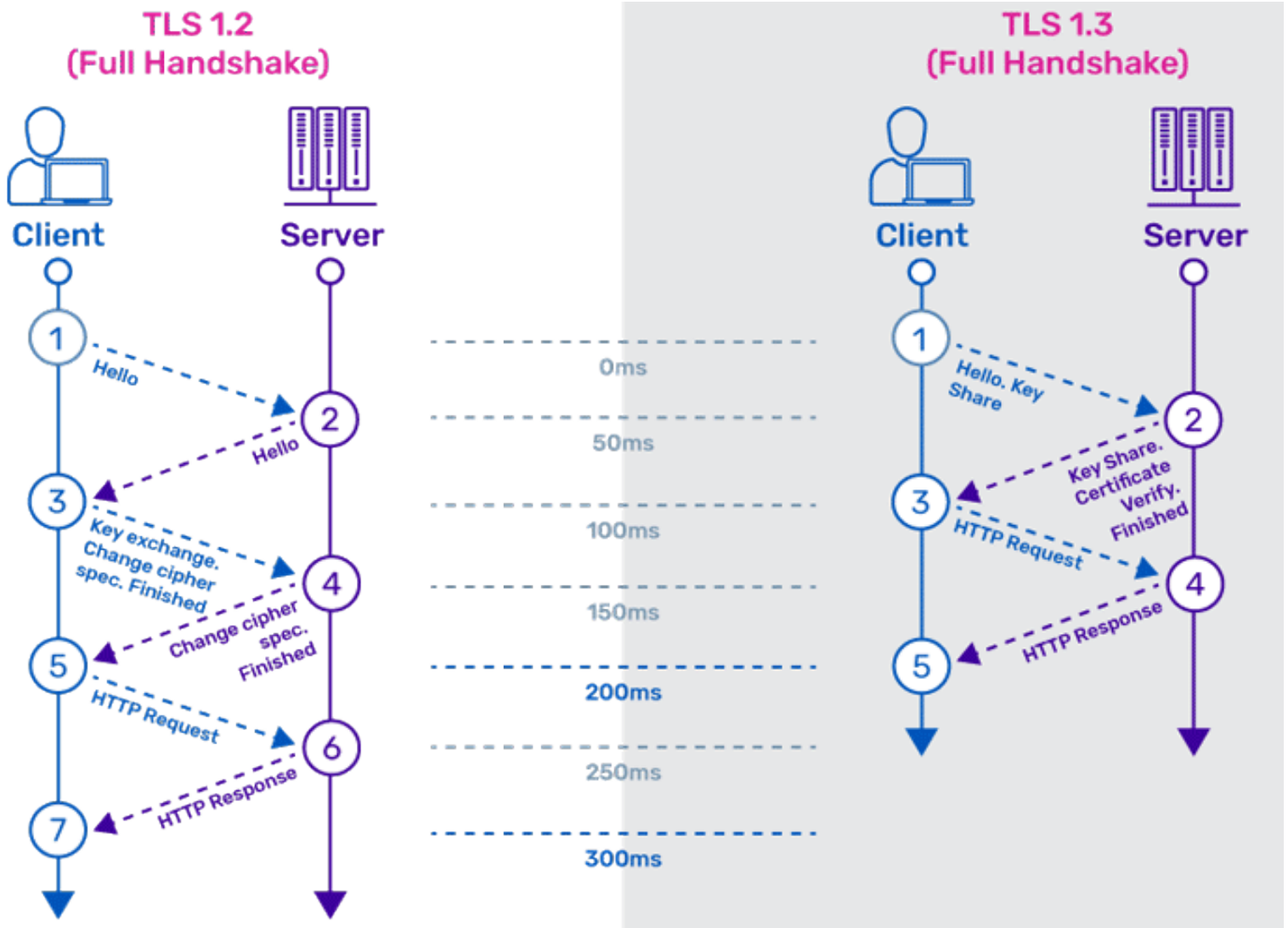
TLS is an upgraded version of the SSL protocol. While both protocols serve the same primary function, there are differences in their security features

The Evolution of SSL/TLS Protocol



	TLS 1.2	TLS 1.3
Handshake Protocol	Longer	Shorter
Cipher Suites	Wide range of cipher suites	Eliminates many older, less secure cipher suites
Security Features	Susceptible to attacks like BEAST and POODLE	Removes legacy features and vulnerabilities present in TLS 1.2
Resumption Mechanism	Session resumption is typically achieved using session IDs or session tickets. This can introduce security and privacy concerns	With "Session 0-RTT" (Zero Round-Trip Time) it allows clients to resume sessions without a full handshake while maintaining security
Key Exchange Algorithms	RSA, DHE, and ECDHE	DHE and ECDHE
Cryptographic Primitives	SHA-1, SHA-256 and MD5	SHA-256 and AEAD

Round-Trip Handshake



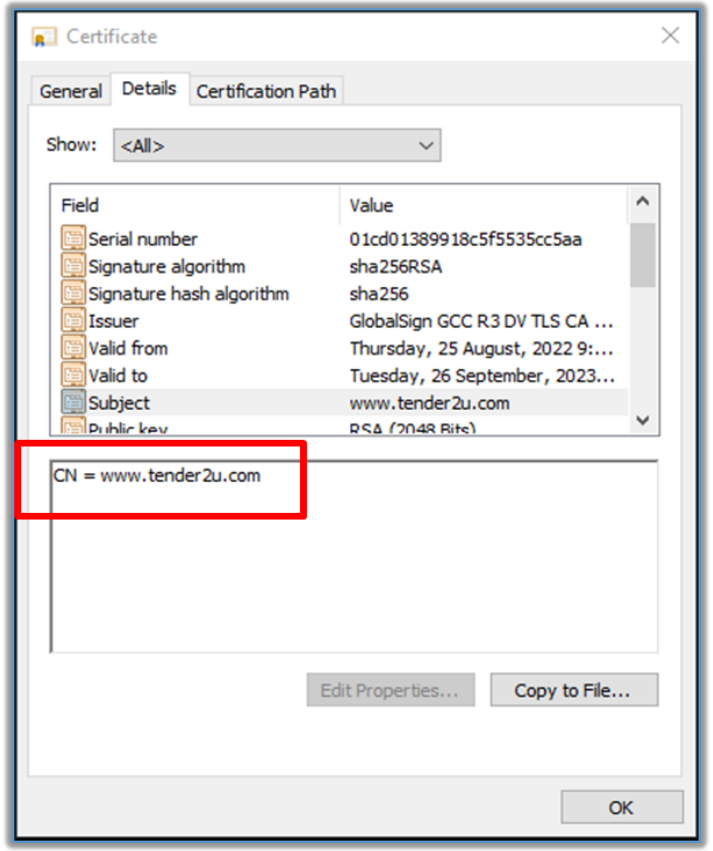
What is TLS/SSL?

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

	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

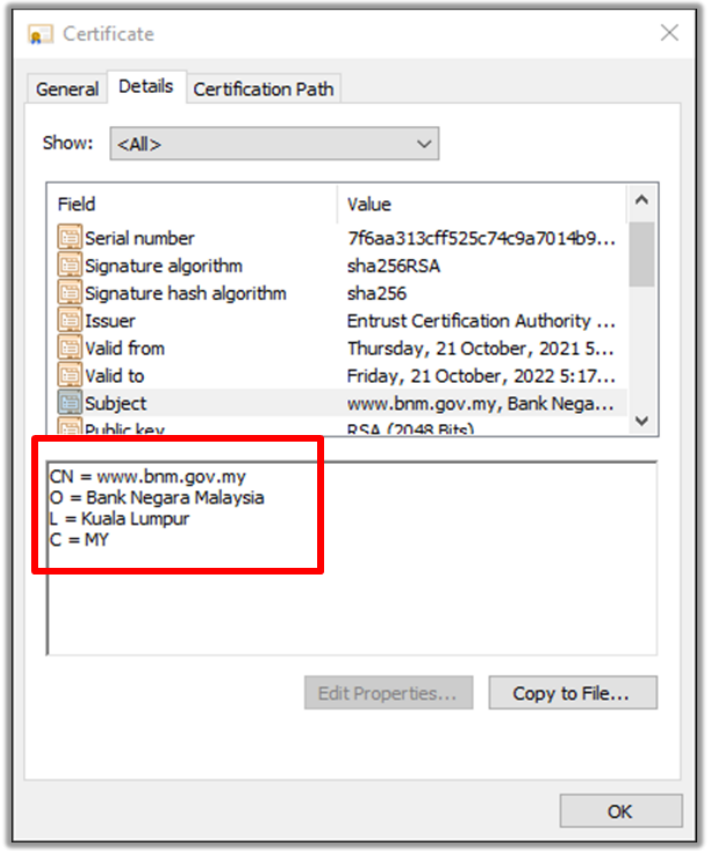
DOMAIN VALIDATED (DV)

- Domain Name



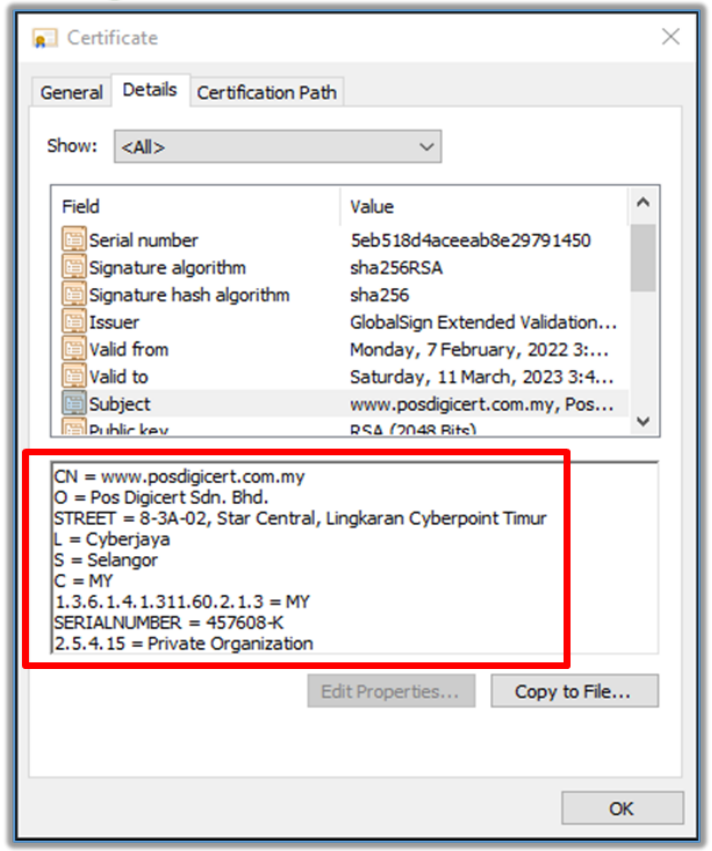
ORGANISATION VALIDATED (OV)

- Domain Name
- Organisation Name

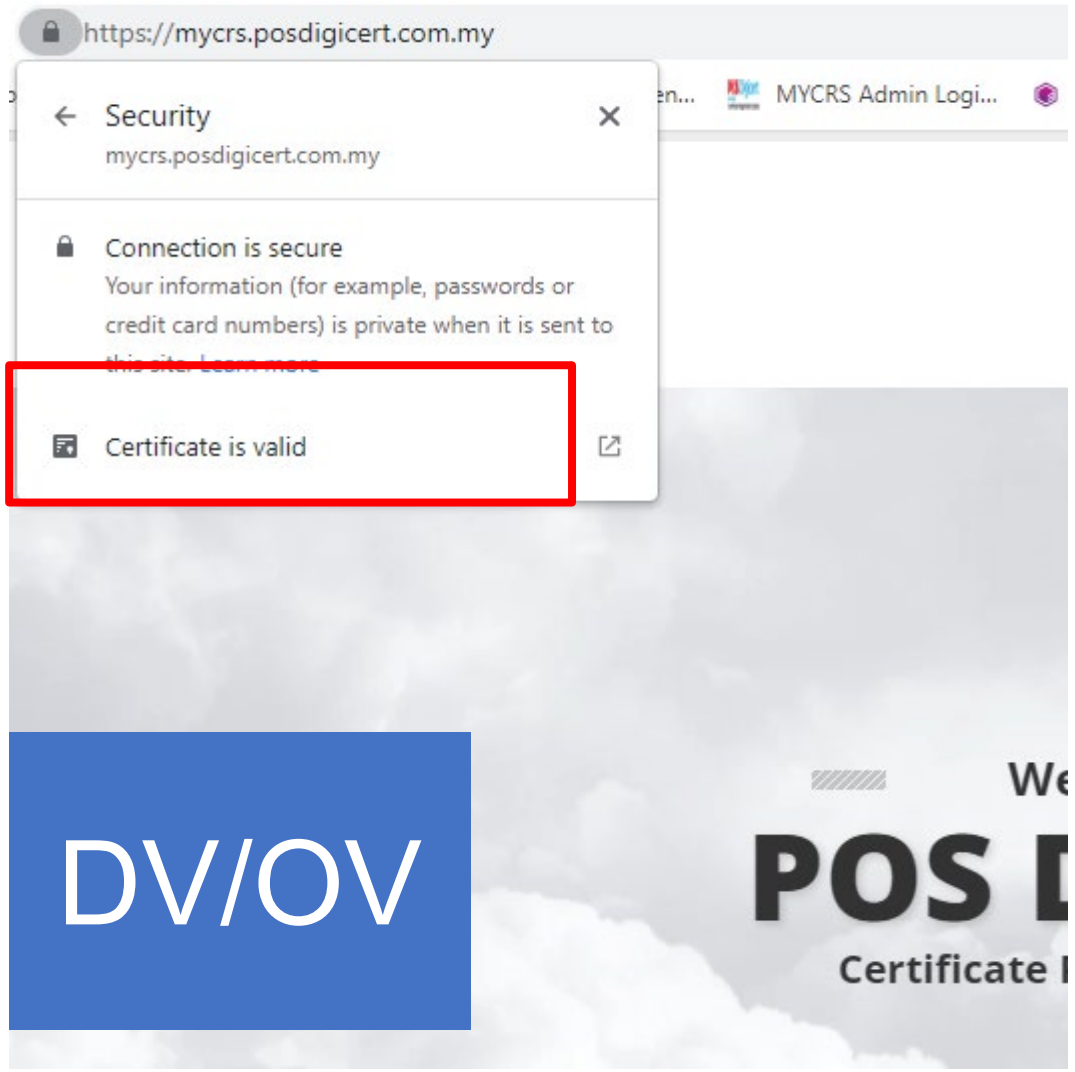


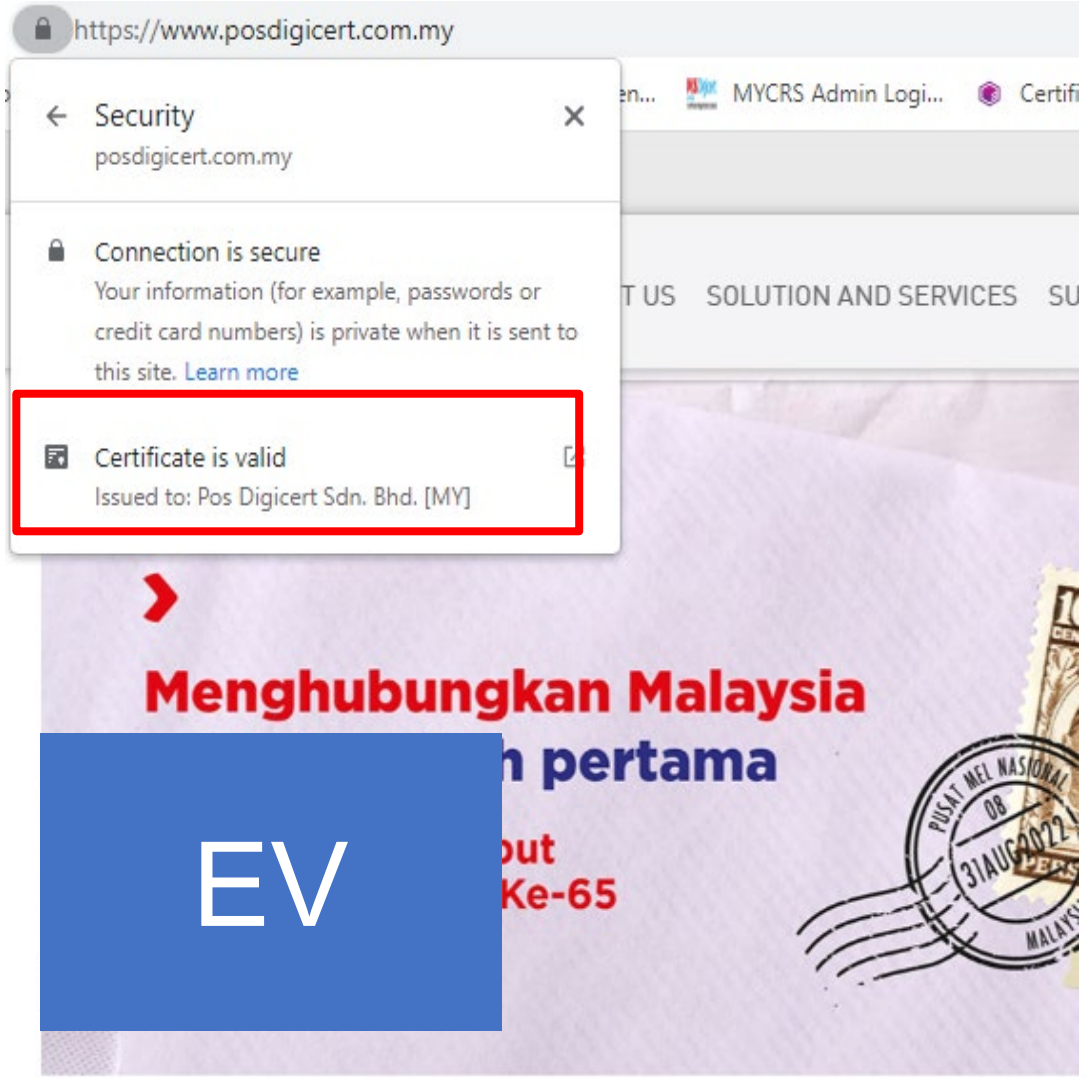
EXTENDED VALIDATION (EV)

- Domain Name
- Organisation Name
- Organisation Address

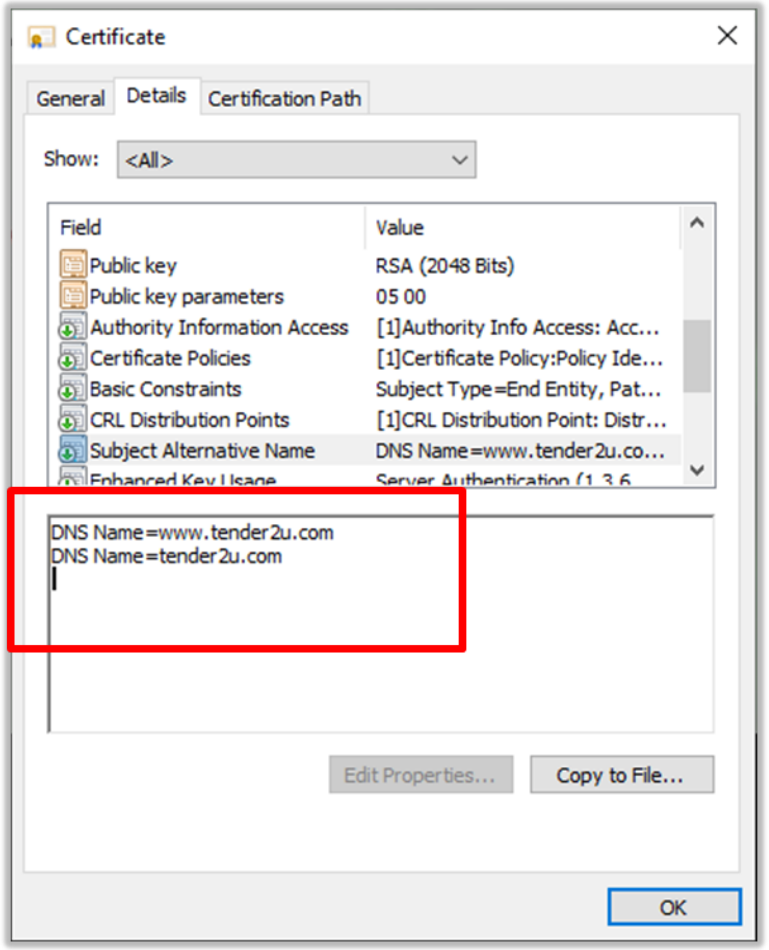


The difference of DV,OV & EV once the SSL certificate is installed in your web browser



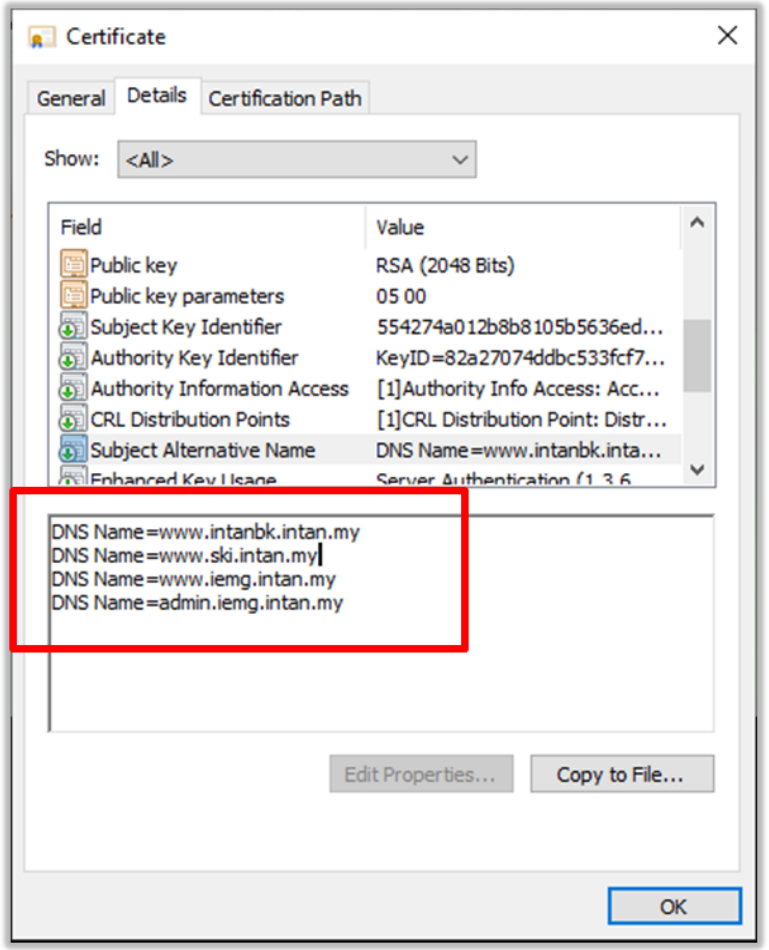


SINGLE DOMAIN



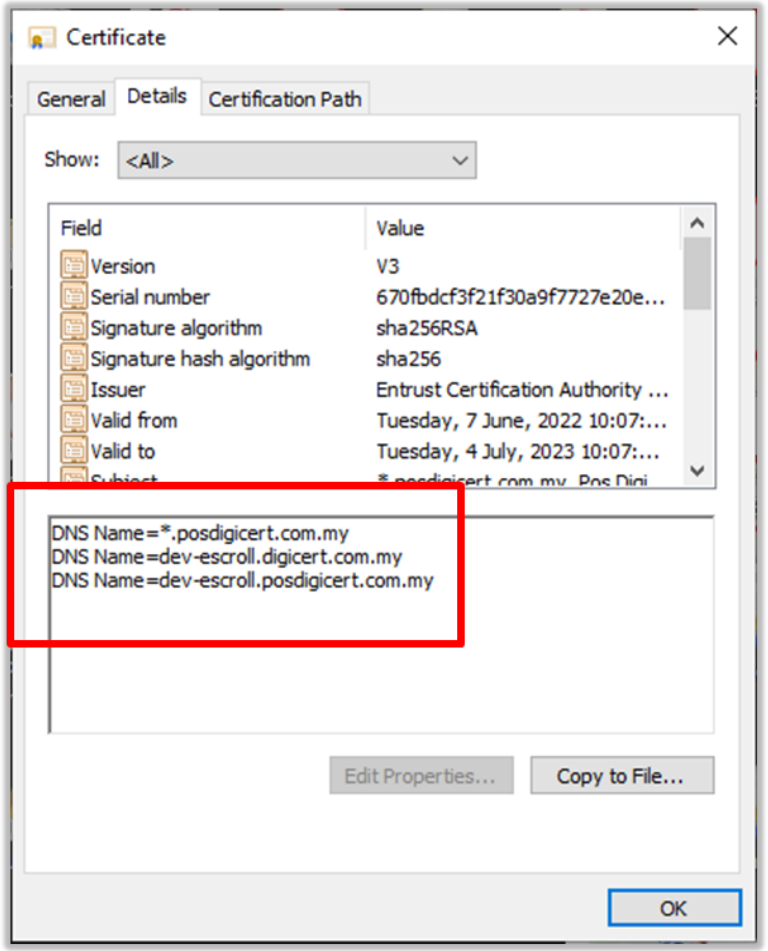
1 domain name
www. is free

MULTI-DOMAIN



More than 2 domain names

WILDCARD



1 root domain
Multiple sub-domains

Algorithms

RSA
(Rivest–Shamir–Adleman)

RSA was first introduced in 1977. RSA involves a protocol called RSA Key Exchange or RSA Key Transport. One party encrypts a symmetric encryption key with the recipient's RSA public key, allowing the recipient to decrypt the symmetric key with their private key and use it for secure communication.

ECC
(Elliptic Curve Cryptography)

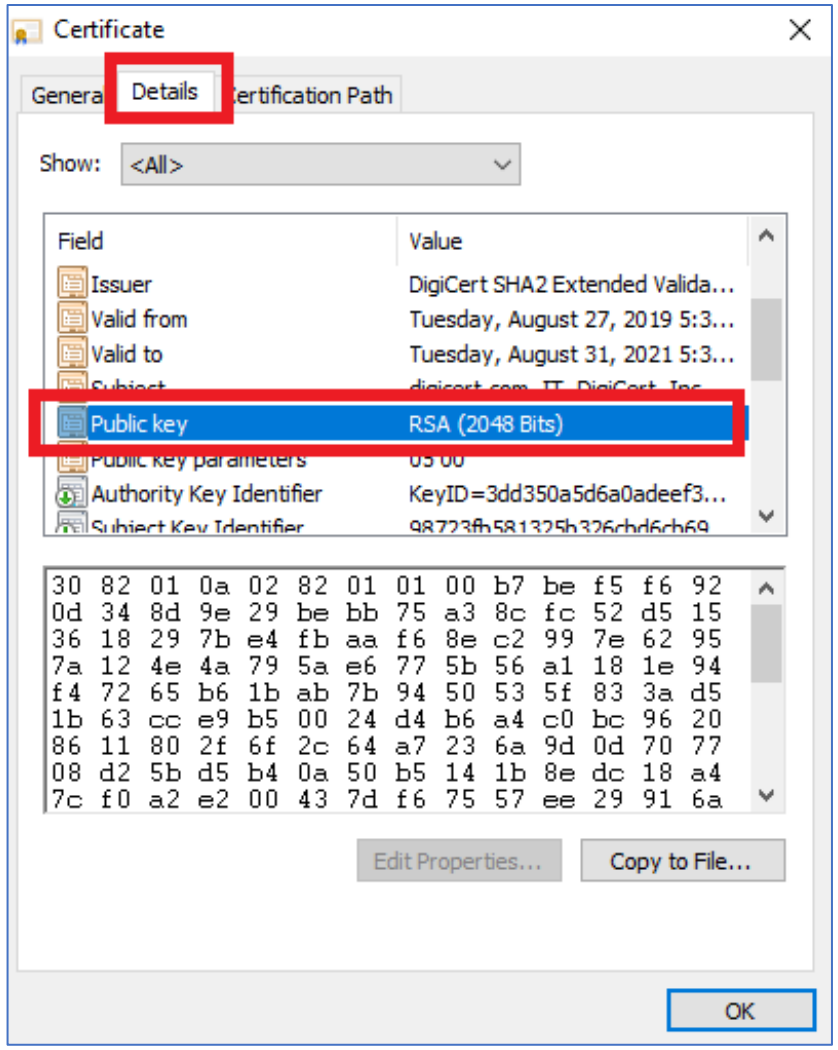
ECC was first introduced in mid 1980s. Key exchange in Elliptic Curve Cryptography (ECC) typically follows a protocol called Elliptic Curve Diffie-Hellman (ECDH). ECDH allows two parties to agree on a shared secret over an insecure communication channel without directly exchanging their private keys.

SSL Certificate Algorithms

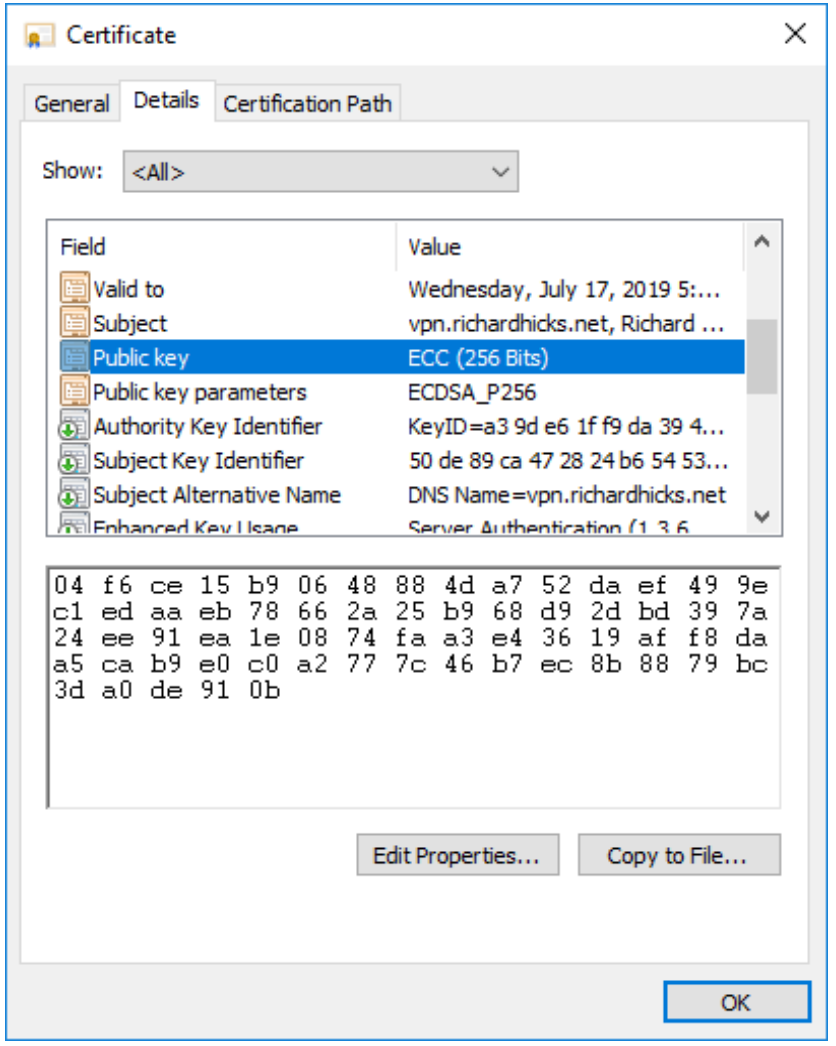
https://youtu.be/4Vq5VCaoUFI

	RSA	ECC
Key Length	Lengthy	Shorter
Efficiency	Increased computational demands	Less computational overhead
Security Strength	Depends on the key size	Well-suited for resource-constrained devices and environments
Resistance to Quantum Attacks	Potential (quantum attack vis Shor's Algorithm)	Secured
Key Management and Storage	Demanding key management	Efficient smaller key size
Standardization	PKCS #1, RFC 8017, FIPS PUB 186, X.509 Certificate Standards, ISO/IEC 18033-2, ANSI X9.31	NIST FIPS PUB 186-4, ANSI X9.62, ISO/IEC 15946-5, SECG, IETF RFC 7748 and RFC 8032, ECC in X.509 Certificates
Patent and Licensing Issues	RSA patent expired	No patent

RSA Certificate



ECC Certificate

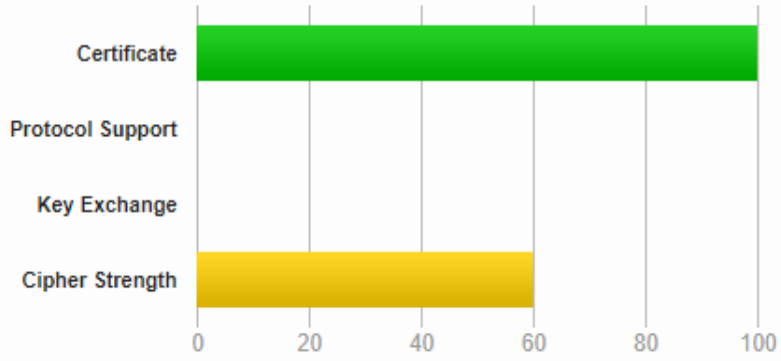


There are primarily two types of encryption methods which are primarily used: "symmetric encryption" and "asymmetric encryption." Both methods use different mathematical algorithms to scramble the data. The encryption list used in SSL certificates as below:

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

Overall Rating

F



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.mampu.gov.my (43.251.19.58)

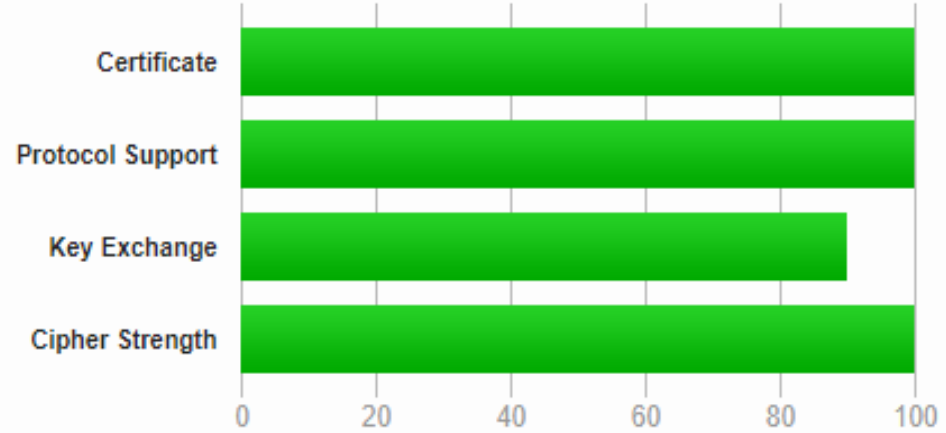
Assessed on: Wed, 27 Sep 2023 13:52:40 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



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

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

www.ssllabs.com/ssltest/

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.

Common reasons for certificate reissuance include:

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

What is Secure Site Seal?

A secure site seal, often referred to as an SSL site seal or trust seal, is a visual indicator displayed as graphical icons or badges on webpages, often in visible locations such as the footer, checkout page, or alongside payment information. It serves several purposes:

Authentication

To display an SSL trust seal, website owners must acquire an SSL certificate from a reputable CA.

Trustworthiness

Signify that a website uses encryption to safeguard sensitive data, like personal details and payment information. This encryption helps prevent unauthorized access to user data.

Visual Confirmation

Visitors are more inclined to trust the website and are more likely to share personal information or complete online transactions.

Clickable Seals

SSL trust seals are clickable, allowing users to access more information about the certificate's validation and the security measures in place.

How to obtain the Secure Site Seal for your website?

1

Purchase SSL Certificate

You can obtain an SSL certificate from a reputable Certificate Authority (CA)

2

Install SSL Certificate

Install it to your web server

3

Configure Your Website

Ensure that your website is configured to use HTTPS protocol

4

Display the SSL Trust Seal

These trust seals are typically provided in the form of HTML code or image files that you can embed on your webpages.

5

Test and Verify

Test your website to ensure that SSL encryption is working correctly and that the trust seal is properly displayed

6

Regular Maintenance

SSL certificates have expiration dates, so make sure to keep track of when your certificate will expire and renew it before it expires to maintain the trust indicators on your site.

	ENTRUST	GlobalSign	GeoTrust
Site Seal Icon / Logo			
How do I get a Site Seal from CA?	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)	26/09/2022-28/10/2023
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

ENTRUST

Sunday 2022-09-18 15:30+0000

buy.entrust.net has been verified by Entrust.

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

This site is secure.

www.digicert.com is validated as a secure site for sending and receiving sensitive data.

English

ENCRYPTED SITE	✓ www.digicert.com
ORGANIZATION NAME	✓ DigiCert, Inc.
LOCATION VERIFIED	✓ UTAH, USA
TLS/SSL CERTIFICATE	✓ Expires: 31-Jul-2024
CERTIFICATE TYPE	✓ DigiCert EV SSL Certificate
REGISTRATION	✓ Confirmed
ADDRESS	✓ Confirmed
PHONE NUMBER	✓ Confirmed
EMAIL ADDRESS	✓ Confirmed
DOMAIN OWNERSHIP	✓ Confirmed
WARRANTY LEVEL	✓ $2 million USD
BLOCKLIST	✓ Checked

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 SSL?

https://youtu.be/UGUmCcVz62A

Sesi Soal Jawab

Topik 2:
Sijil Digital Pelayan Perkhidmatan MyGPKI

2.1: Pengenalan Perkhidmatan MyGPKI

2.2: Dasar Dan Penerangan Umum Mengenai Sijil Digital Pelayan

2.3: Jenis-Jenis Sijil Digital Pelayan yang Dibekalkan

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.

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.

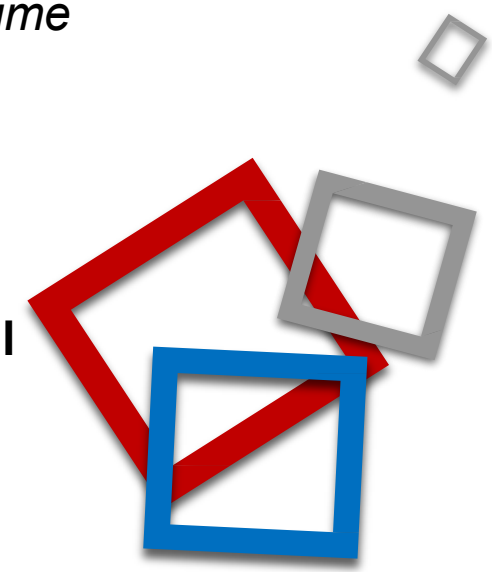
Meningkatkan tahap kepercayaan pengguna untuk melaksanakan transaksi secara dalam talian bagi sebarang urusan Kerajaan.

1 Pengurusan dan Pembekalan Sijil Digital Pengguna

- Token
- *Roaming certificate + One-Time Password (OTP)*
- *Soft certificate*
- *Roaming certificate*

2 Pengurusan dan Pembekalan Sijil Digital Pelayan

- *Single domain*
- *Multi domain*
- *Wildcard*

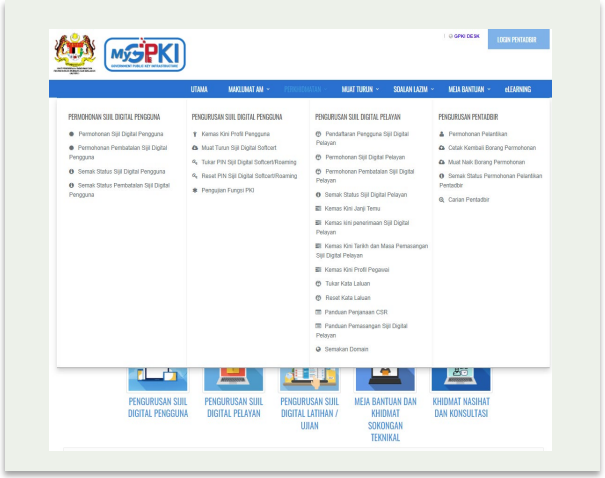


3 Perkhidmatan Meja Bantuan dan Khidmat Sokongan Teknikal

4 Khidmat Nasihat dan Konsultasi bagi Penggunaan PKI

Transformasi Perkhidmatan MyGPKI Bagi Sijil Digital Pelayan

Sistem GPKI 1.0
Permohonan Sijil Digital Pelayan secara **dalam talian** untuk ***Single Domain***



2002

Sijil Digital Pelayan
Hanya jenis ***Single Domain*** sahaja dan dilaksanakan **secara manual**

2011

2017

Sistem GPKI 2.0
Permohonan Sijil Digital Pelayan secara dalam talian dengan tambahan 2 jenis Sijil Digital Pelayan iaitu ***Multi Domain*** dan ***Wildcard***.

2020 - kini

Sistem GPKI 3.0

1. **Penambahan Menu Baharu** - permohonan **pembatalan sijil, semak status , kemaskini penerimaan dan pemasangan, kemaskini profil pegawai, tukar dan reset kata laluan**
2. Sistem **GPKI Desk**
3. Sistem **GPKI eLearning**
4. **GPKI Mobile –** Semak Status

Penggunaan Perkhidmatan MyGPKI – Sijil Digital Pelayan

JPM 855 subdomain	KKM 350 subdomain	MoF 263 subdomain	MoHR 159 subdomain	
MoT 34 subdomain	MoHA 375 subdomain	KPWKM 35 subdomain	KPKT 57 subdomain	
KBS 22 subdomain	EKONOMI 25 subdomain	KPDN 100 subdomain	MoSTI 63 subdomain	
MoHE 10 subdomain	KUSKOP 11 subdomain	KKD 88 subdomain	KPK 10 subdomain	KKDW 71 subdomain
MoD 1 subdomain	KKR 1 subdomain	MoE 39 subdomain	KPKM 27 subdomain	NRECC 141 subdomain

22 kementerian

982 Pentadbir SSL

2,737 subdomain

4 Certification Authority (CA)

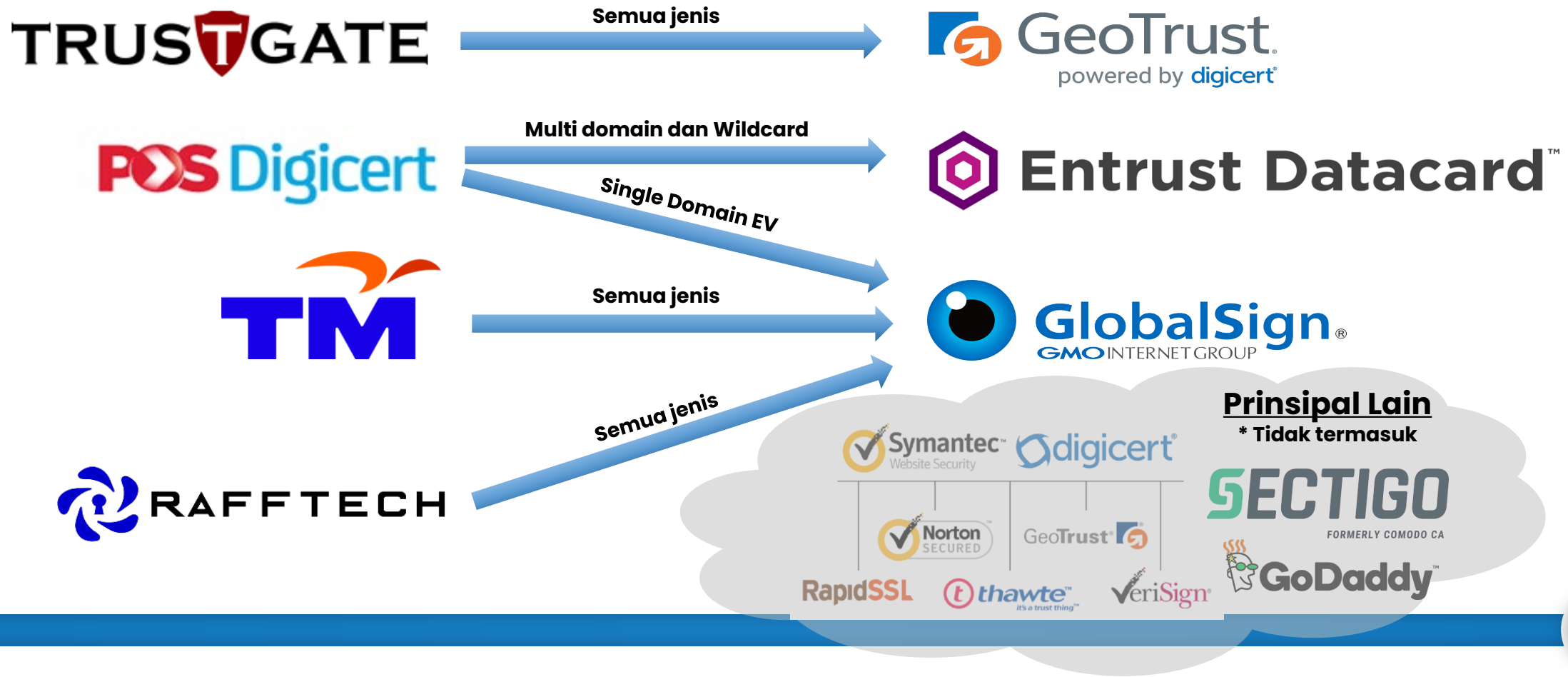
3 prinsipal

Certification Authority (CA)

Pihak Berkuasa 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)



2.2: Dasar Dan Penerangan Umum 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

Sistem ICT Kerajaan

Mestilah beralih kepada GPKI apabila **sistem dinaik taraf/ tempoh kontrak sistem tamat**.

Agensi Sektor Awam

Perlu **ambil kira keperluan** sijil digital pelayan dalam **spesifikasi sistem baharu**.

Perkhidmatan MyGPKI

Hanya akan bekalkan sijil digital pelayan untuk **pembaharuan sedia ada yang akan tamat tempoh.**

Agensi Pusat

Tanggung semua kos bagi perkhidmatan GPKI untuk kementerian dan jabatan persekutuan sahaja.

Agensi Bukan Tanggungan

Semua kos **sijil digital pelayan dalam sistem baharu** akan ditanggung oleh agensi berkenaan.

Agensi yang Berubah Taraf

Agensi pelaksana yang berubah taraf, semua kos di bawah tanggungan agensi berkenaan.

Nota

1. Agensi hendaklah menggunakan sijil digital pelayan SSL **sumber terbuka (*open source*)** bagi kegunaan pelayan, selain pelayan produksi
2. Sistem ICT kerajaan baharu yang dibangunkan secara ***outsource*** perlu mengambil kira kos pemasangan SSL dalam kontrak baharu masing-masing.
3. Sistem ICT Kerajaan yang dibangunkan secara ***inhouse*** akan ditanggung oleh Agensi Pusat.

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

Tanggungan Kos Sijil Digital Pelayan

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	✗ Tidak Ditanggung
		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 Digital Pelayan yang Dibekalkan

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**

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)

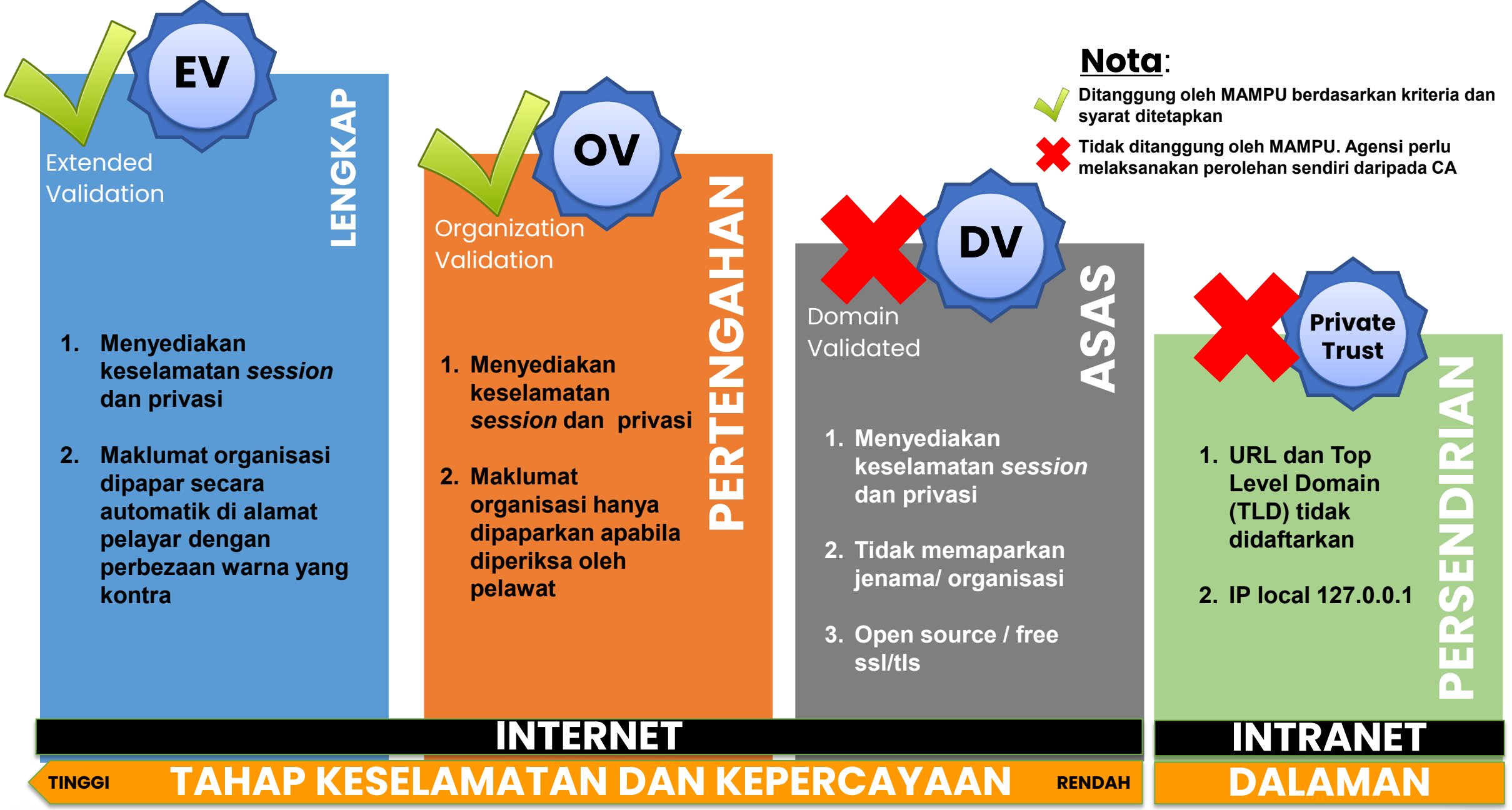
*** Nota:**
Walaupun wildcard mempunyai kelebihan tiada had bilangan subdomain dan boleh menjangkau sehingga melebihi 150 subdomain namun ia hanya meliputi subdomain pada 1 aras hirearki yang sama sahaja dan tidak boleh digunakan bersama dengan jenis multi domain dan single domain atas faktor keselamatan.

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


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
Nota:
Ditanggung oleh MAMPU berdasarkan kriteria dan syarat ditetapkan
Tidak ditanggung oleh MAMPU. Agensi perlu melaksanakan perolehan sendiri daripada CA
INTERNET
INTRANET
TINGGI
TAHAP KESELAMATAN DAN KEPERCAYAAN
RENDAH
DALAMAN

Sesi Soal Jawab

Rehat

Topik 3: Permohonan & Pengurusan Sijil Digital Pelayan

3.1: Proses Permohonan Sijil Digital Pelayan

3.2: Pengurusan Sijil Digital Pelayan Di Portal GPKI

3.3: GPKI Mobile untuk SSL, GPKI Desk dan GPKI eLearning

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 (e-vetting)** dengan Pegawai Agensi

e-vetting = pengesahan organisasi dan pengesahan domain.
e-vetting 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

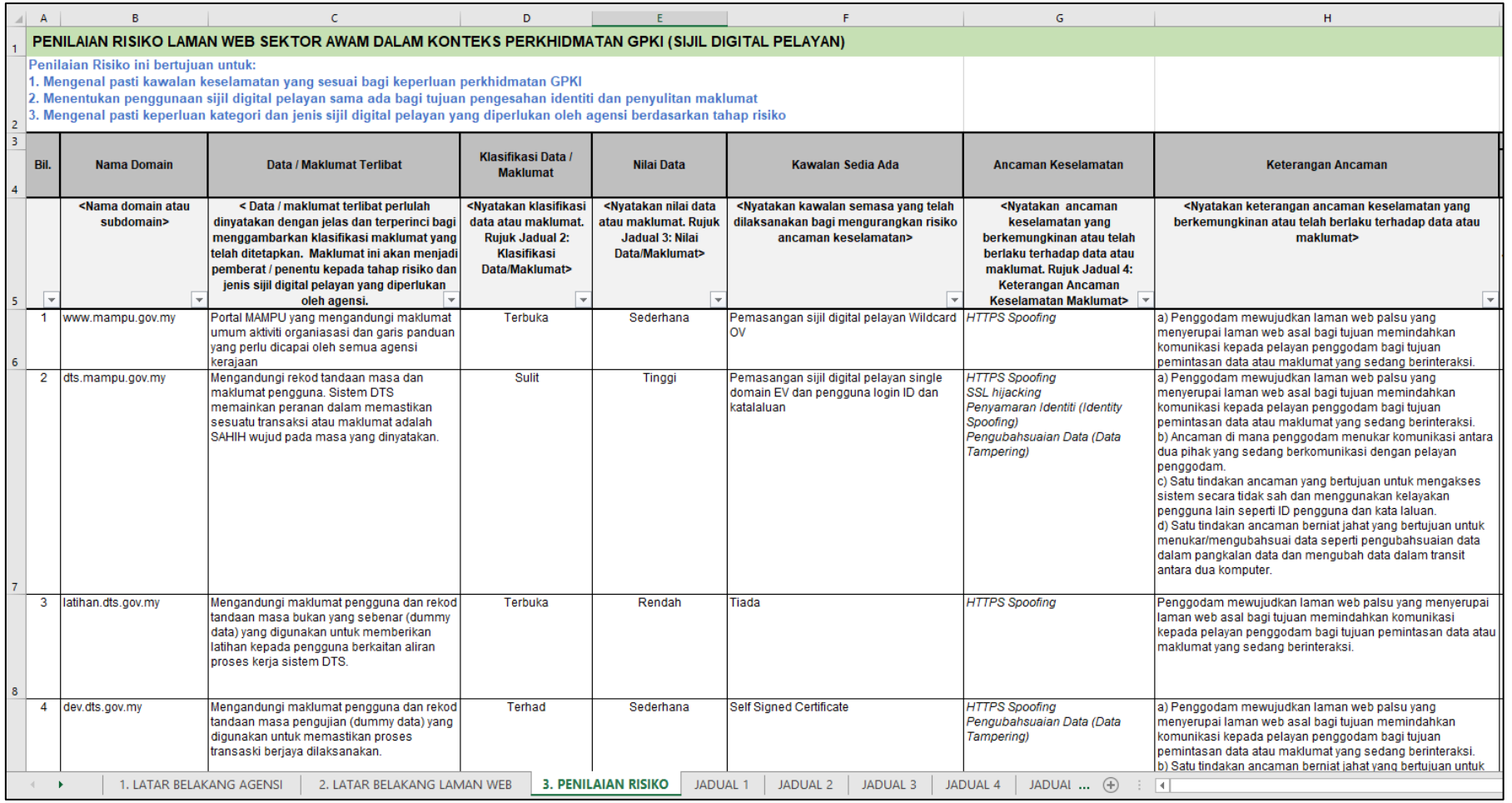
09 Pegawai Agensi membuat pemasangan sijil digital dan **kemas kini tarikh dan taraf pemasangan** di Portal GPKI

Langkah 1: 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 supaya memenuhi **kriteria dan pra-syarat** serta dapat **menentukan jenis sijil digital pelayan** yang sesuai sebelum permohonan di Portal GPKI



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 ...

Kriteria dan Pra Syarat

1

KESELAMATAN

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

2

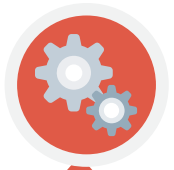
CAPAIAN SISTEM

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.

L02: 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 (e-vetting)** dengan Pegawai Agensi

e-vetting = pengesahan organisasi dan pengesahan domain.
e-vetting 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

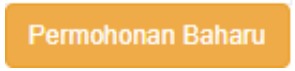
- Sijil MESTI dipasang dalam **tempoh 14 hari** selepas tarikh terimaan sijil daripada CA
- Agensi perlu mengemaskini **tarikh penerimaan dan tarikh pemasangan**

** 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

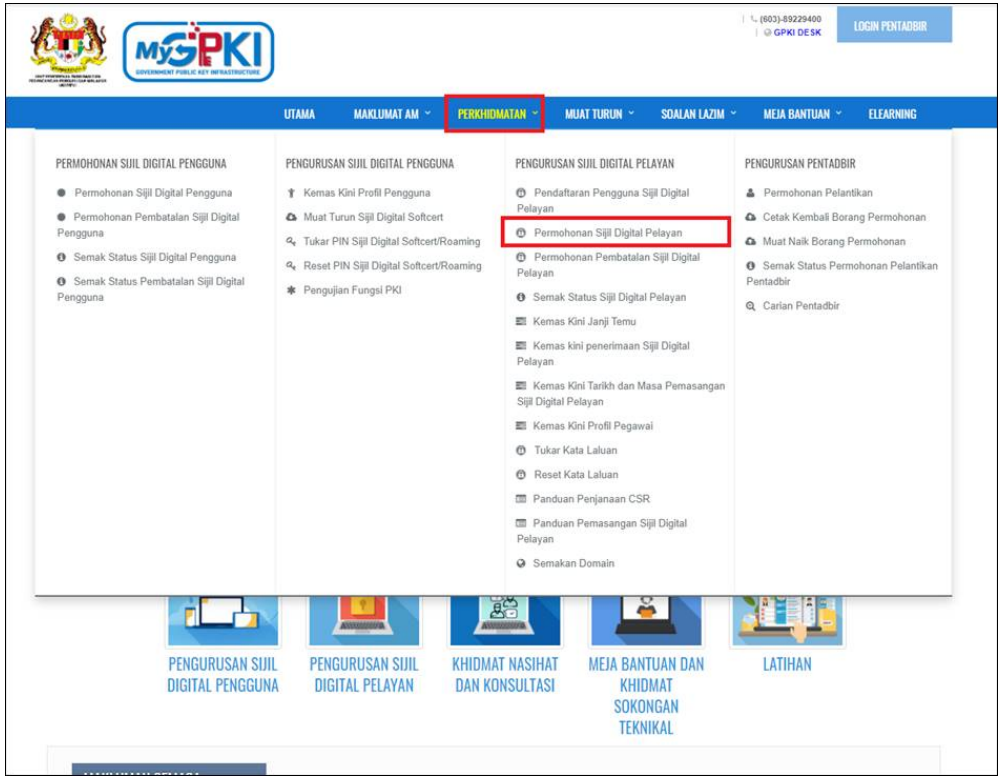
Permohonan Sijil Digital Pelayan di Portal GPKI

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

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

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

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



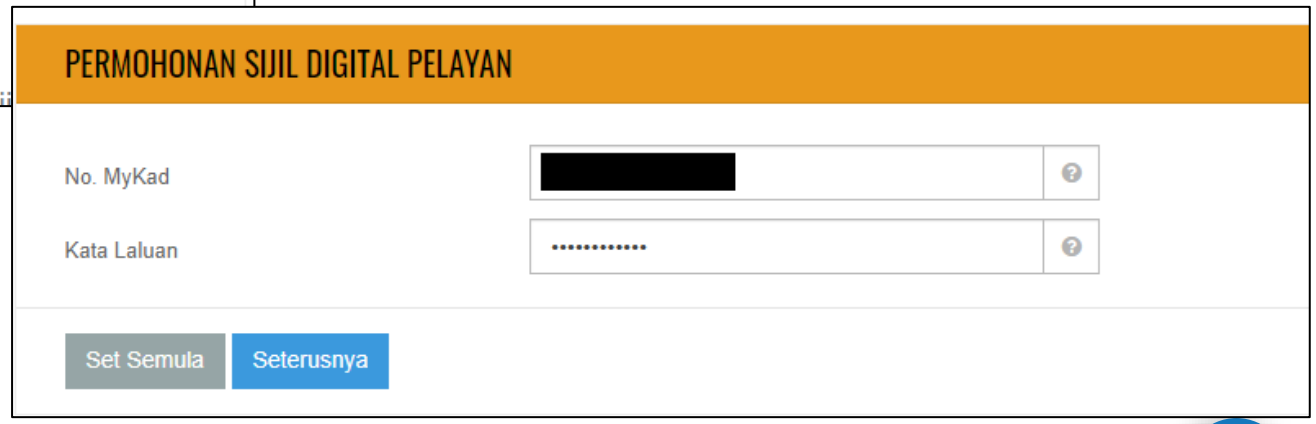
Permohonan Sijil Digital Pelayan di Portal GPKI

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.

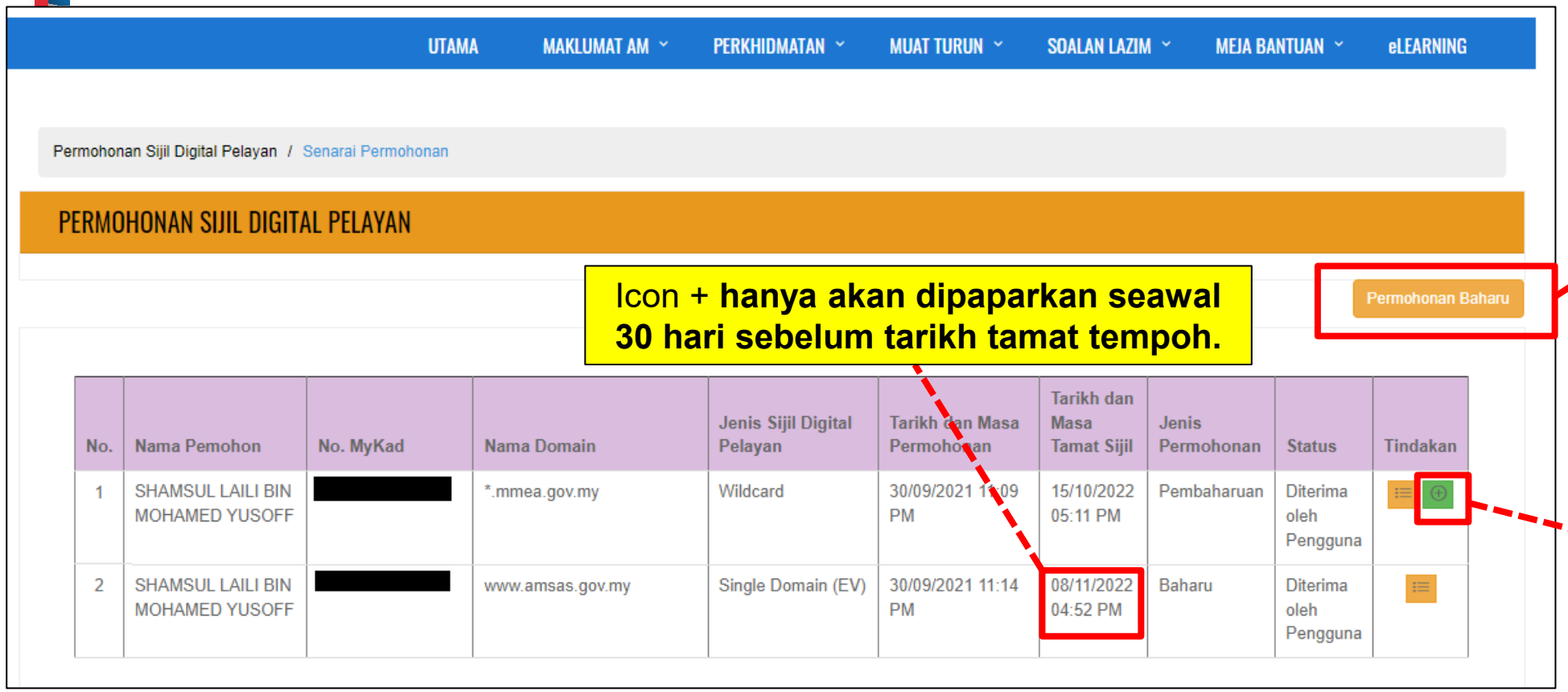
Menu **"Permohonan Sijil Digital Pelayan"** hanya boleh dicapai oleh Pentadbir Pelayan (SSL) sedia ada yang mempunyai ID (No. MyKad) dan kata laluan. Digunakan untuk membuat permohonan pembaharuan atau tambahan bagi domain/subdomain baharu.

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

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



Paparan Senarai Permohonan



Icon + **hanya akan dipaparkan seawal 30 hari sebelum tarikh tamat tempoh.**

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

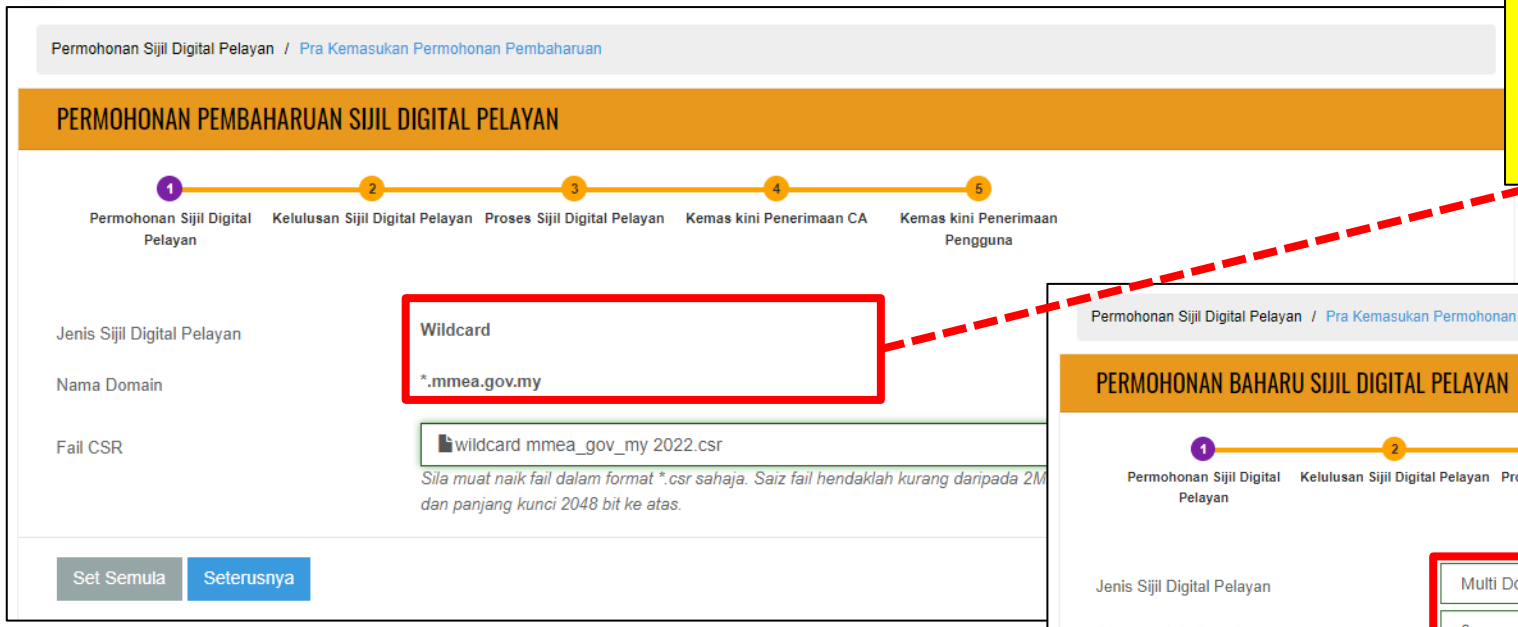
Icon + **digunakan untuk permohonan pembaharuan** domain/ subdomain sedia ada.

Ralat: Tiada Icon +

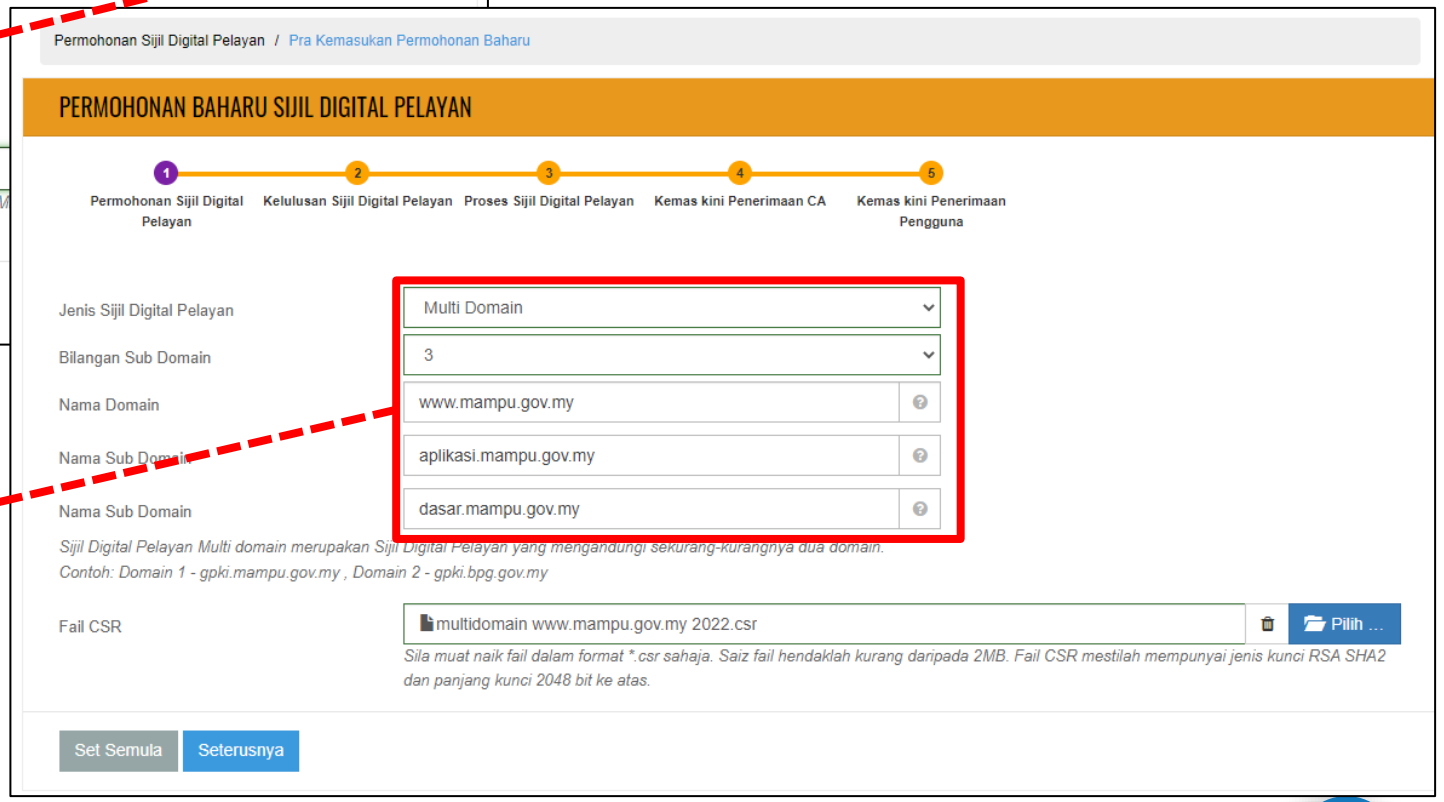
- Ralat icon + pembaharuan masih tidak dipaparkan walaupun tempoh telah kurang dari 30 hari disebabkan **kitaran permohonan terdahulu tidak lengkap atau tidak selesai sepenuhnya**.
- Oleh itu, Pentadbir Pelayan (Pegawai Pemohon sahaja) perlu melaksanakan **mengemas kini tarikh penerimaan dan pemasangan sijil digital pelayan sedia ada** terlebih dahulu oleh agensi.

Borang Permohonan

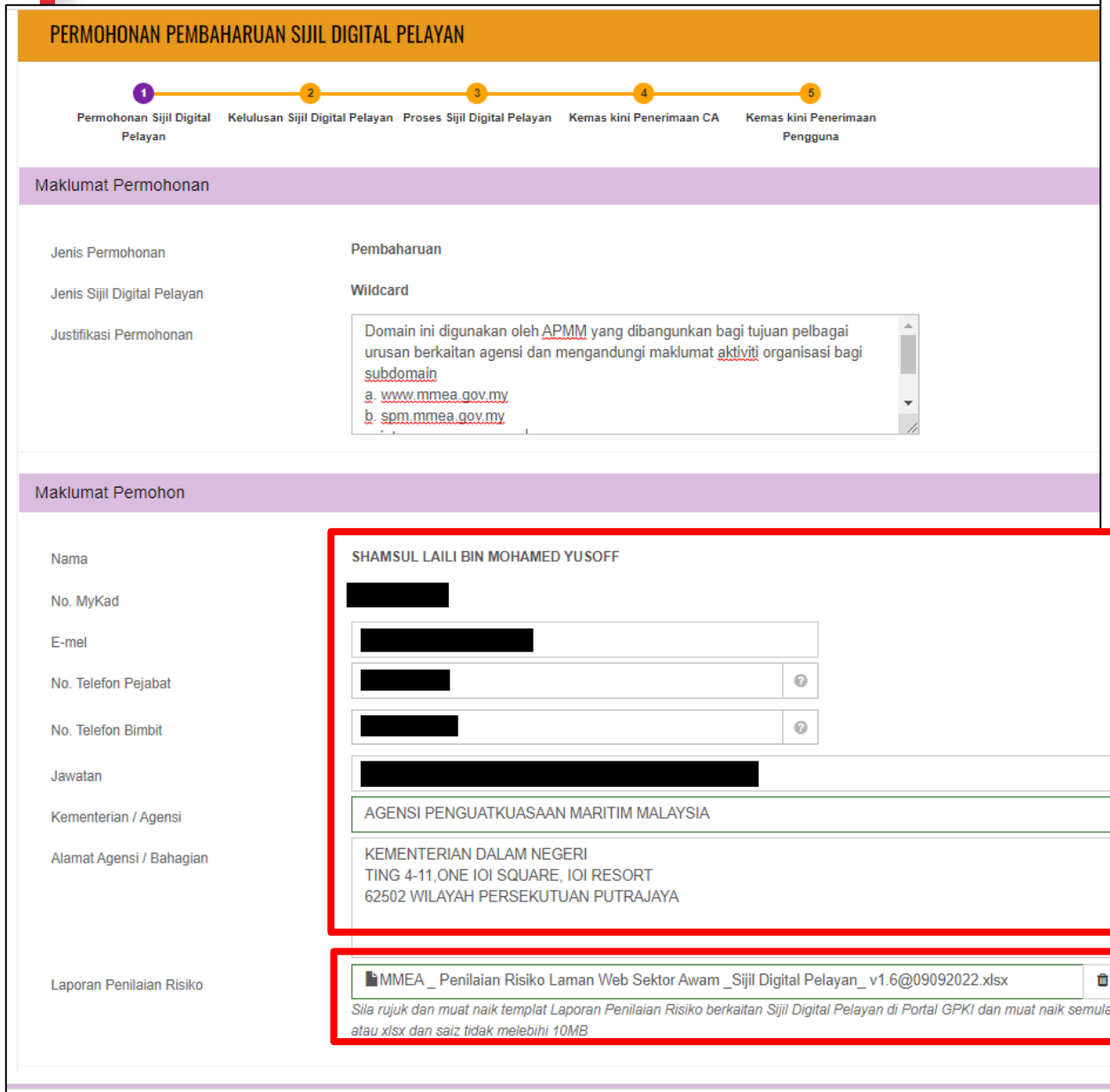
Jenis Single Domain / Wildcard
Kemasukan nama domain/subdomain **MESTILAH** sama dengan kandungan fail CSR yang telah dijana. Bagi wildcard nama domain/subdomain perlulah dimulakan dengan simbol * (contoh: *.mampu.gov.my)

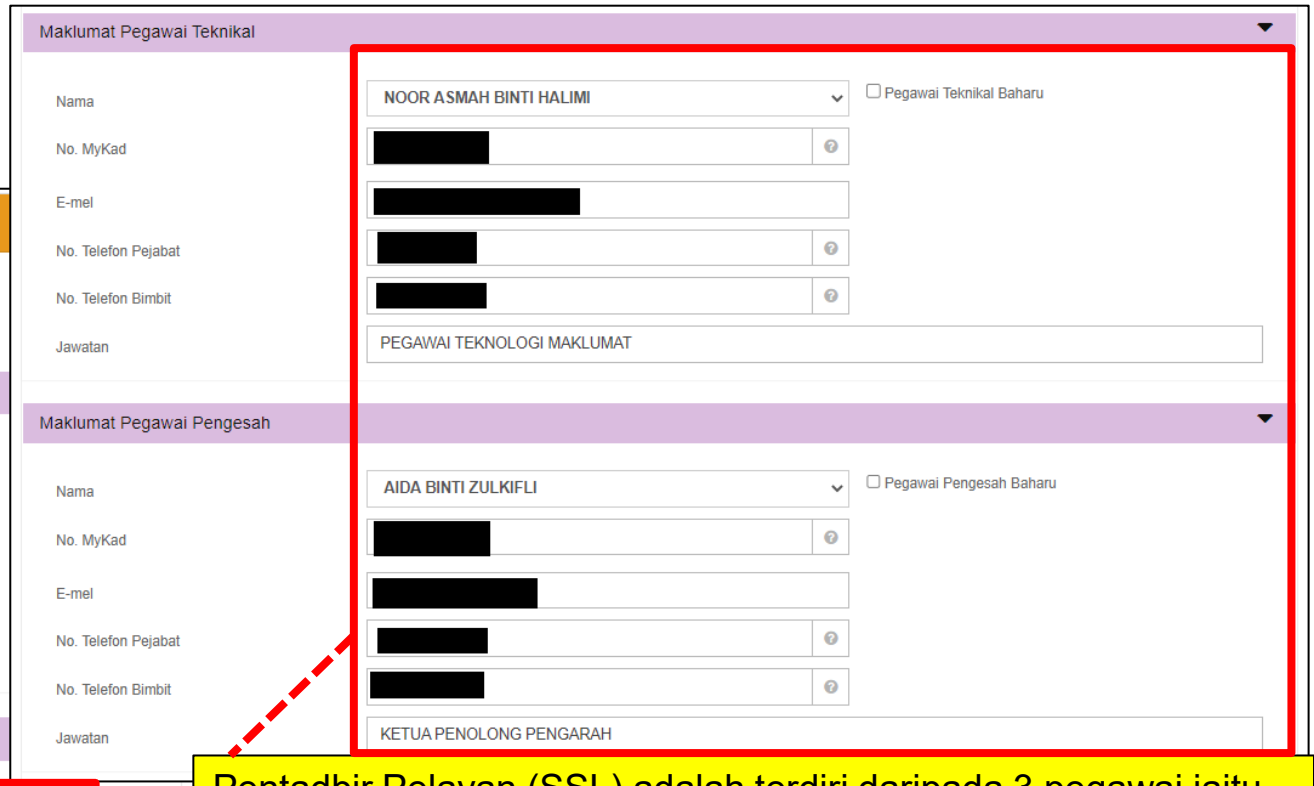


Jenis Multi Domain
Kemasukan nama dan bilangan domain/subdomain **MESTILAH** mengikut susunan dalam kandungan fail CSR yang telah dijana



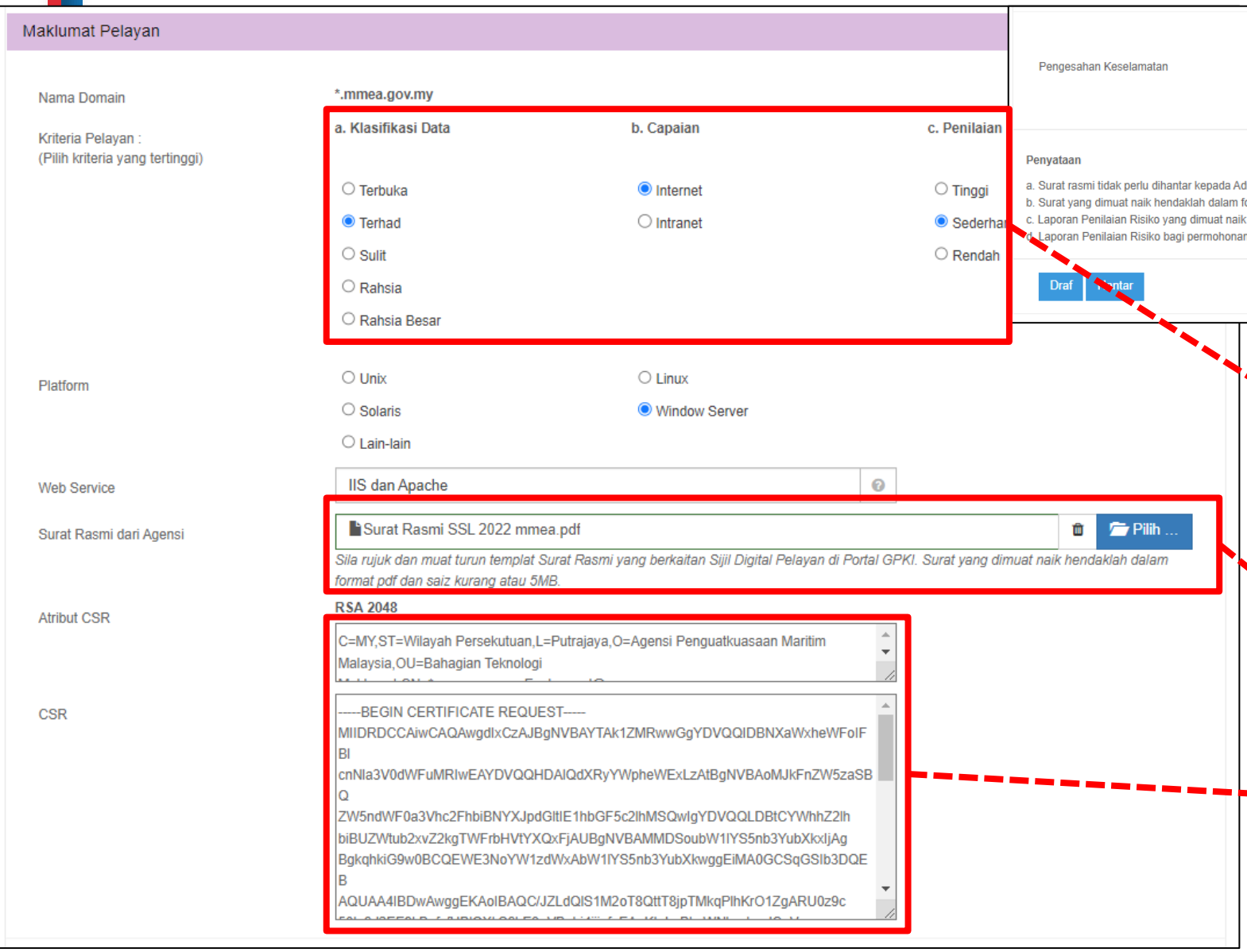
Maklumat Pentadbir Pelayan (SSL)





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.



Pengesahan Keselamatan

p76eb

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

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

Surat rasmi agensi MESTILAH disediakan mengikut format yang telah ditetapkan.

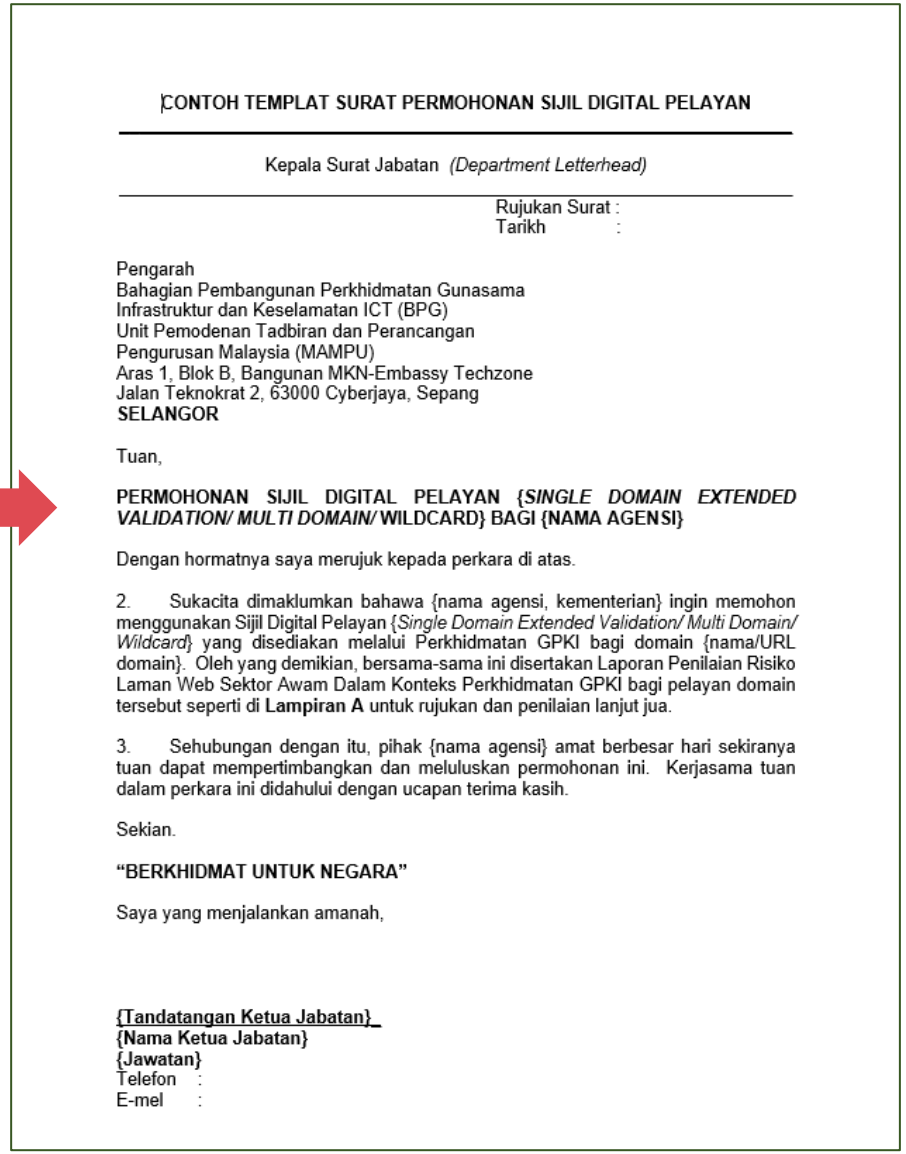
Fail CSR yang telah dimuat naik.

Contoh Surat Rasmi

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 :

Fail CSR

Apa itu 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

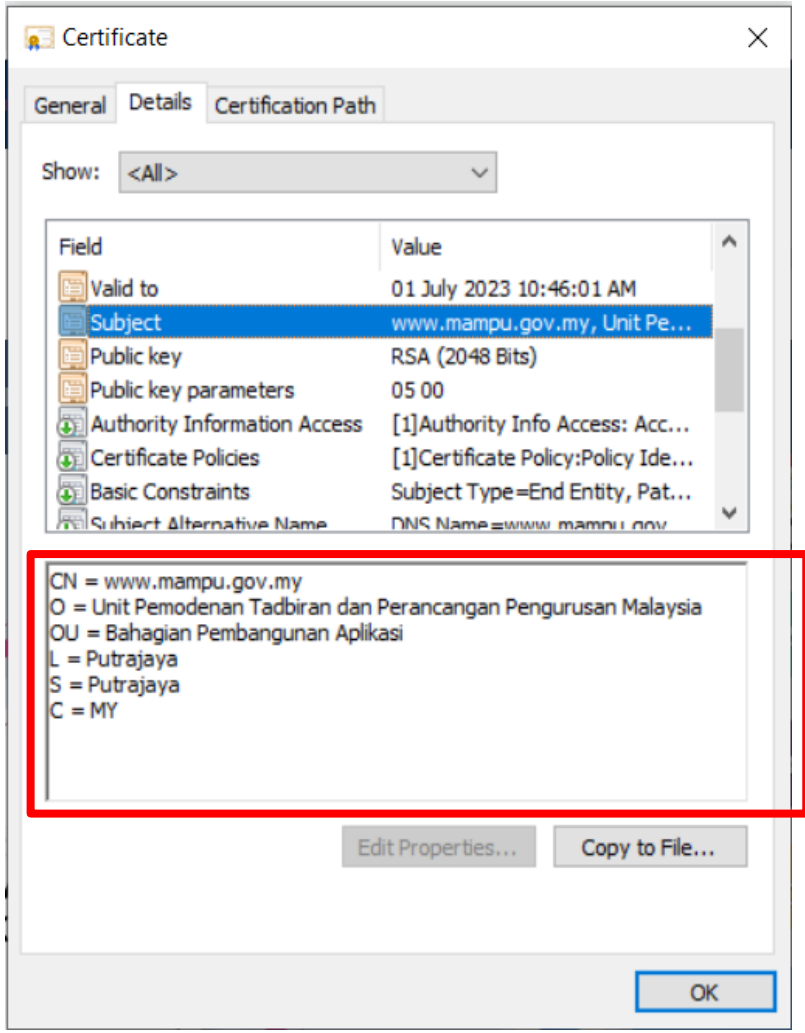
1. Fail CSR yang akan dijana **MESTI** sama dengan maklumat domain yang **TELAH** didaftarkan dengan **Pendaftar Domain (MyNIC)**.
2. Saiz fail hendaklah **kurang daripada 2MB.**
3. Fail CSR mestilah mempunyai jenis kunci **RSA SHA2** dan panjang kunci **2048 bit ke atas**.

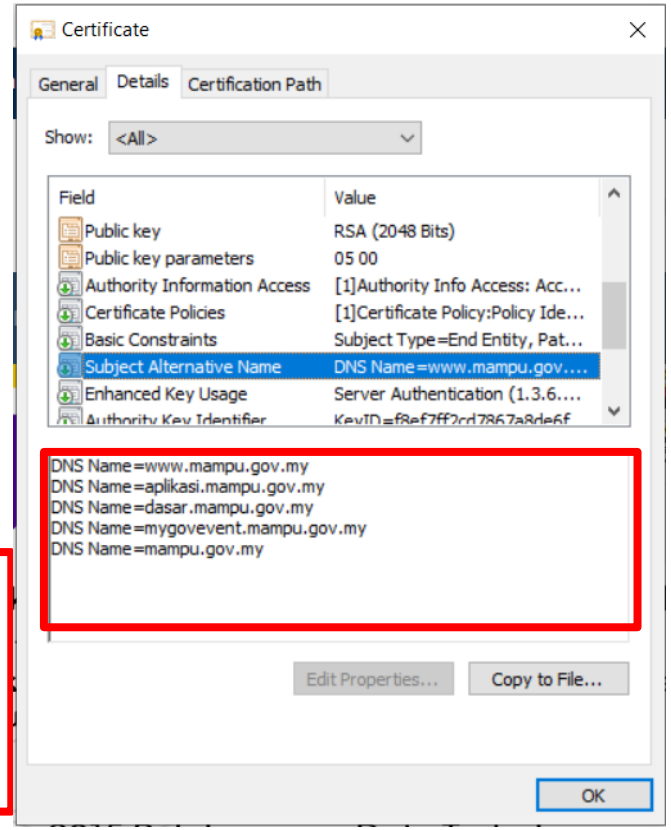
Contoh Format Kandungan CSR (code Base-64)

```
-----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-----
```

Kandungan 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



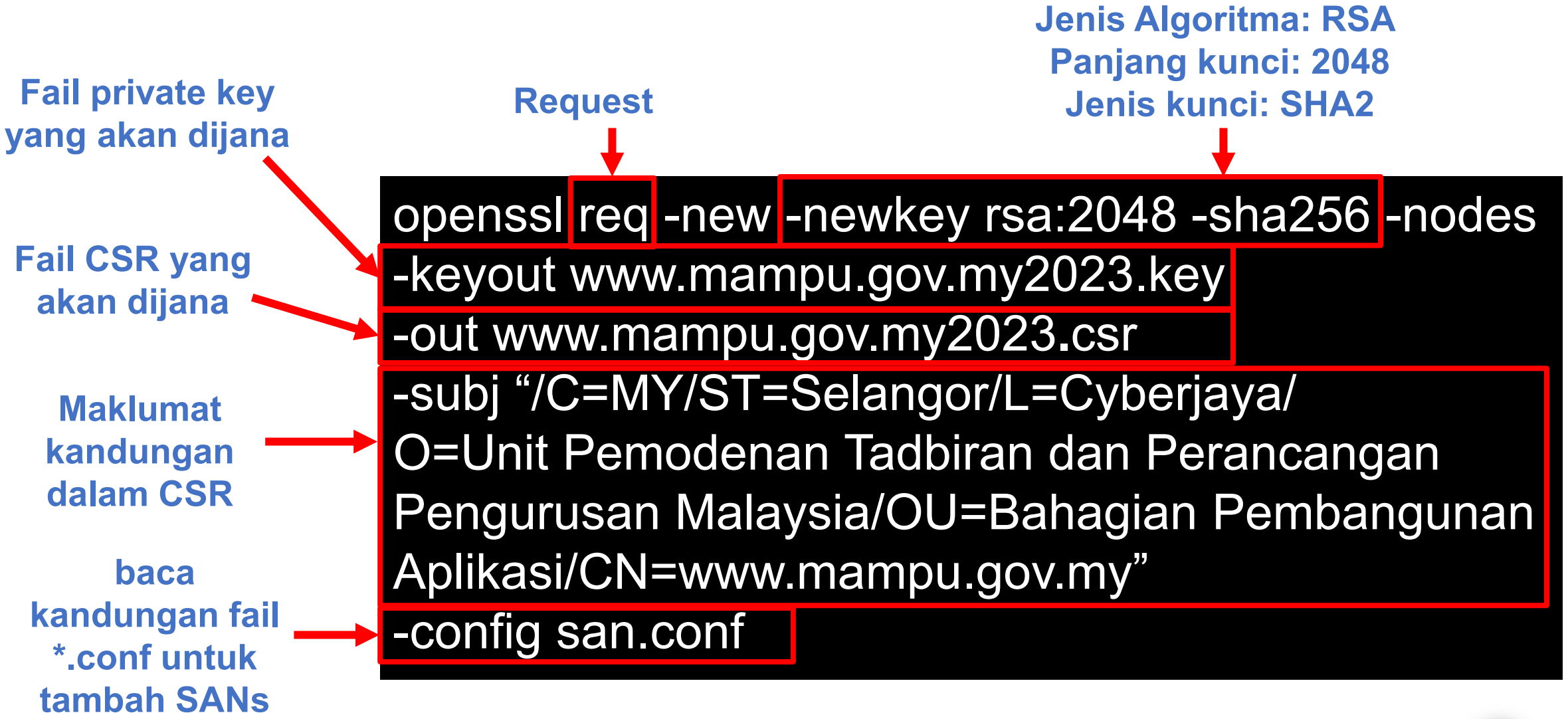


Crypto Library Tool vs Web Service

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

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

Jana Fail CSR - OpenSSL



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)

How to Create a CSR in Apache OpenSSL

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

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

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)	

Jana Fail CSR - Keytool

Generate private key

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

```
keytool -genkey -keyalg RSA -sigalg
SHA256withRSA -keysize 2048 -alias domain –
www.mampu.gov.my2023.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”
```

Fail private key yang akan dijana

Maklumat kandungan dalam CSR

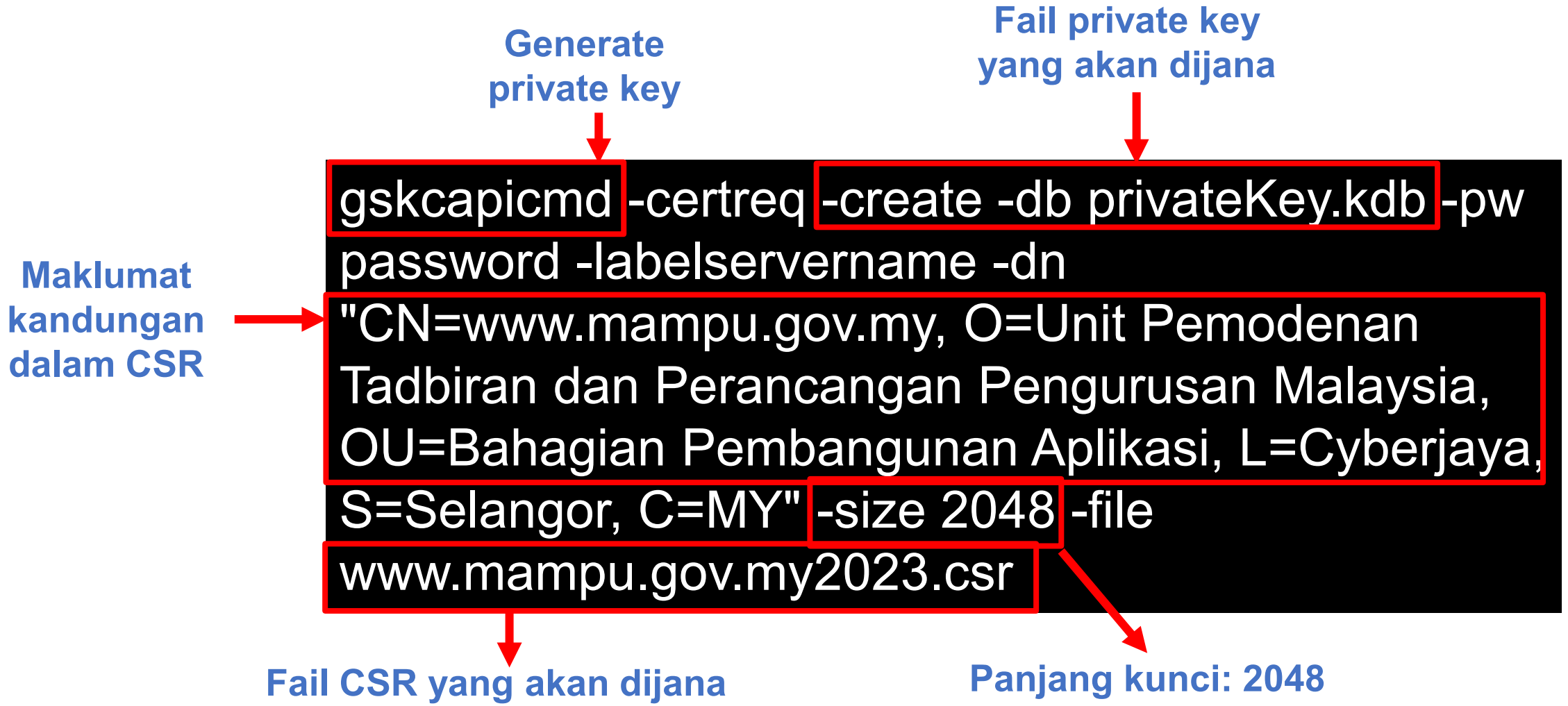
Jana Fail CSR - Keytool (Multi Domain)

How to Create a Java Key Store and Generate a CSR

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

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

Jana Fail CSR – IBM Java SDK (iKeyMan)



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

Jana Fail CSR - Mozilla NSS (certutil)

Jenis Algoritma: RSA
Panjang kunci: 2048

```
certutil -R -k rsa -g 2048 -s
“CN=www.mampu.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
www.mampu.gov.my2023.csr
```

Maklumat kandungan dalam CSR

Fail CSR yang akan dijana

Jana Fail CSR – Schannel (MMC2 Command)

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

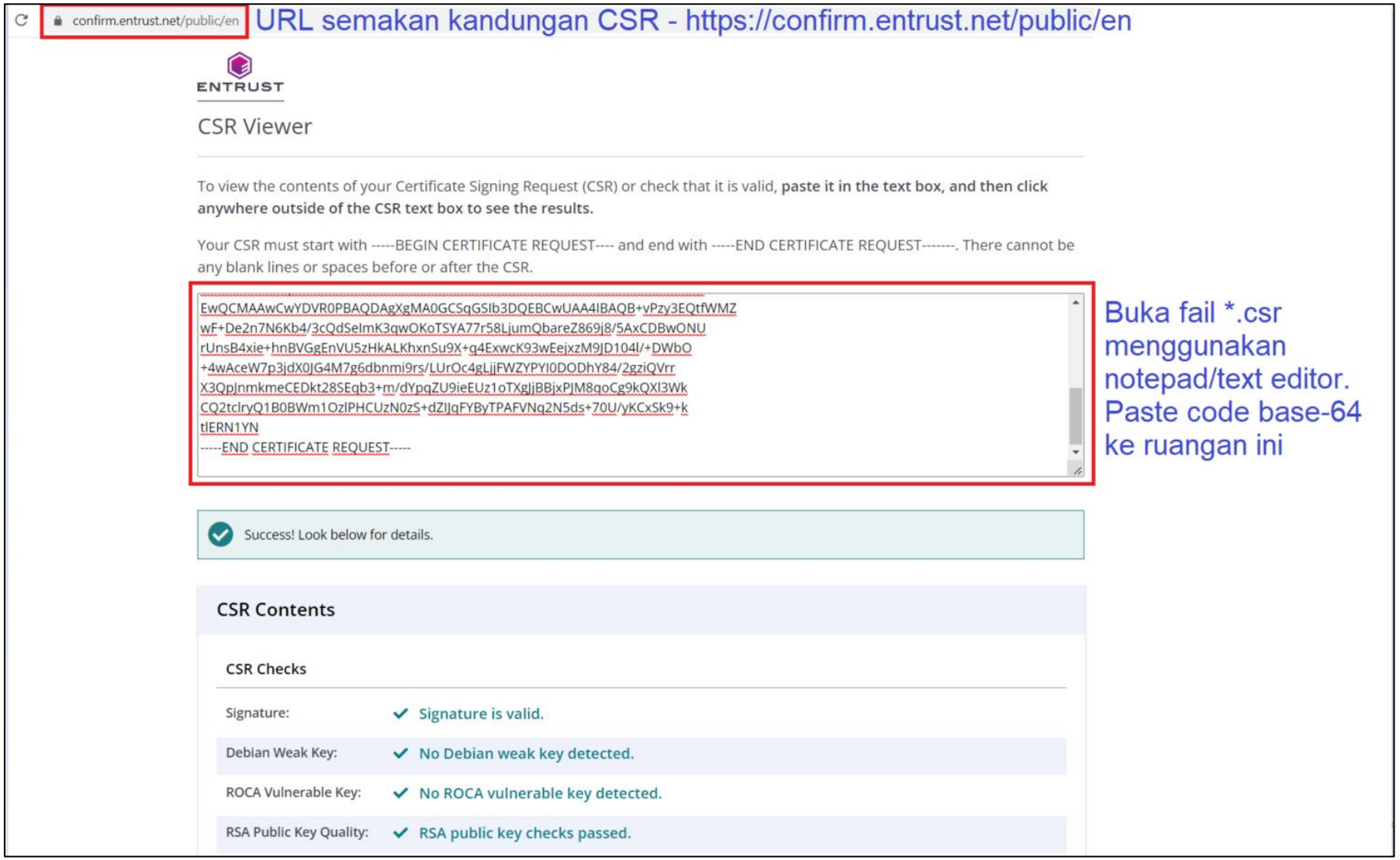
www.youtube.com/watch?v=W2-IphtGcZU

Semakan Kandungan 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
Nama penuh agensi kerana mewakili imej agensi/jabatan kerajaan
Locality: Cyberjaya
State: Selangor
Country: MY
dua aksara kod negara
Subject Alternative Names: aplikasi.mampu.gov.my (dNSName)
dasar.mampu.gov.my (dNSName)
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
perlu memenuhi syarat minimum yang ditetapkan
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
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 t
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.

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.

DO'S

DON'TS

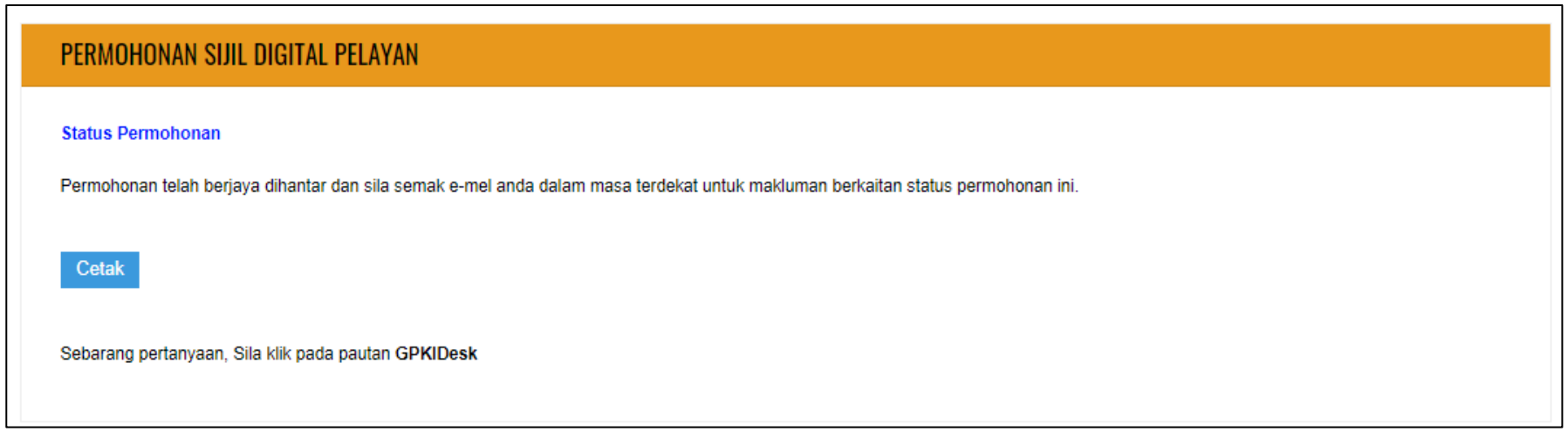
Pastikan **kunci persendirian (*private key*)** (key/ks/pem/jks/keystore/kdb) sijil digital pelayan **tidak hilang atau *corrupt*** dan **disimpan di tempat yang selamat**.

Jangan pindah milik sijil digital pelayan dan *private key*.

Kerja-kerja pemasangan perlu **dilaksanakan sendiri oleh pegawai** di agensi atau pembekal yang **dilantik secara sah sahaja**

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

Pembaharuan Sijil Digital Pelayan



- **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.

L05: 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 (e-vetting)** dengan Pegawai Agensi

e-vetting = pengesahan organisasi dan pengesahan domain.
e-vetting 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

Proses E-vetting – Pengesahan Organisasi

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. 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

c. 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

Proses E-vetting – Pengesahan Domain

KAEDAH PENGESAHAN DOMAIN (*DOMAIN VALIDATION*)

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

- agensi hendaklah memastikan salah satu akaun domain **constructive e-mel default** telah wujud dan aktif iaitu • admin@domainagensi.gov.my, administrator@domainagensi.gov.my, hostmaster@domainagensi.gov.my, webmaster@domainagensi.gov.my atau postmaster@domainagensi.gov.my
- Sekiranya akaun e-mel masih belum wujud, maka pihak agensi perlulah mewujudkan salah satu e-mel tersebut dengan kadar segera

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.

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 (e-vetting)** dengan Pegawai Agensi

e-vetting = pengesahan organisasi dan pengesahan domain.
e-vetting 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

Kaedah Penghantaran Sijil Digital Pelayan kepada Agensi

E-mel notifikasi Sistem GPKI

Format *.cer

E-mel notifikasi berserta lampiran sijil digital pelayan

Portal GPKI

Format *.cer

Muat turun sijil digital pelayan mengikut domain/subdomain masing-masing di Portal GPKI

E-mel CA

Format *.crt, text atau e-mel prinsipal

E-mel kepada Pegawai Pemohon, Pegawai Teknikal dan Pegawai Pengesah

E-mel dan Portal Prinsipal

Lampiran text atau pautan muat turun (dari portal prinsipal)

E-mel kepada Pegawai Pemohon, Pegawai Teknikal dan Pegawai Pengesah

L08 – L09: 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 (e-vetting)** dengan Pegawai Agensi

e-vetting = pengesahan organisasi dan pengesahan domain.
e-vetting 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

Penerimaan dan Pemasangan Sijil Digital Pelayan

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

Pemasangan Sijil Digital Pelayan

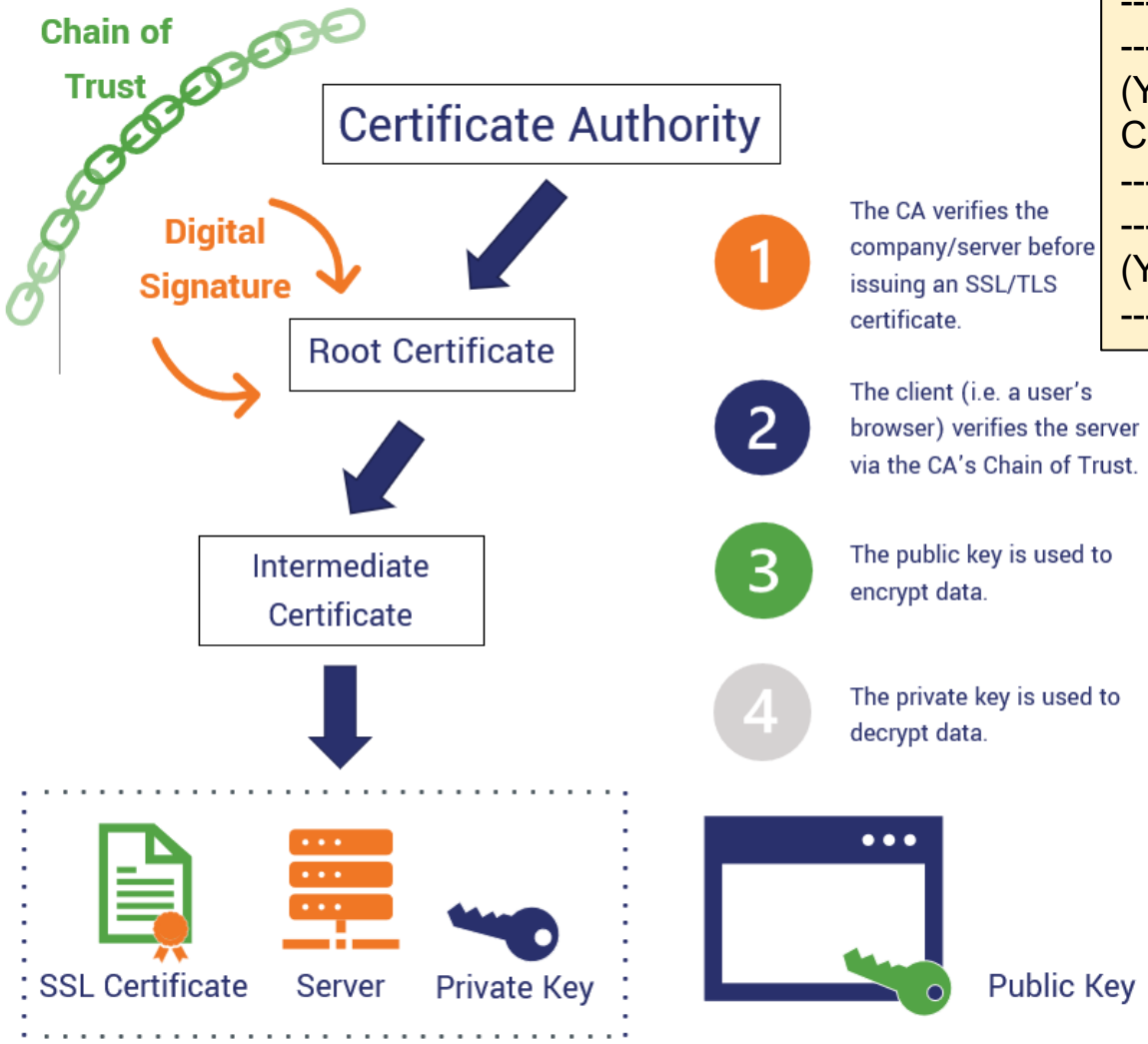
a. Sijil digital pelayan > subdomain yang dimohon

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**".

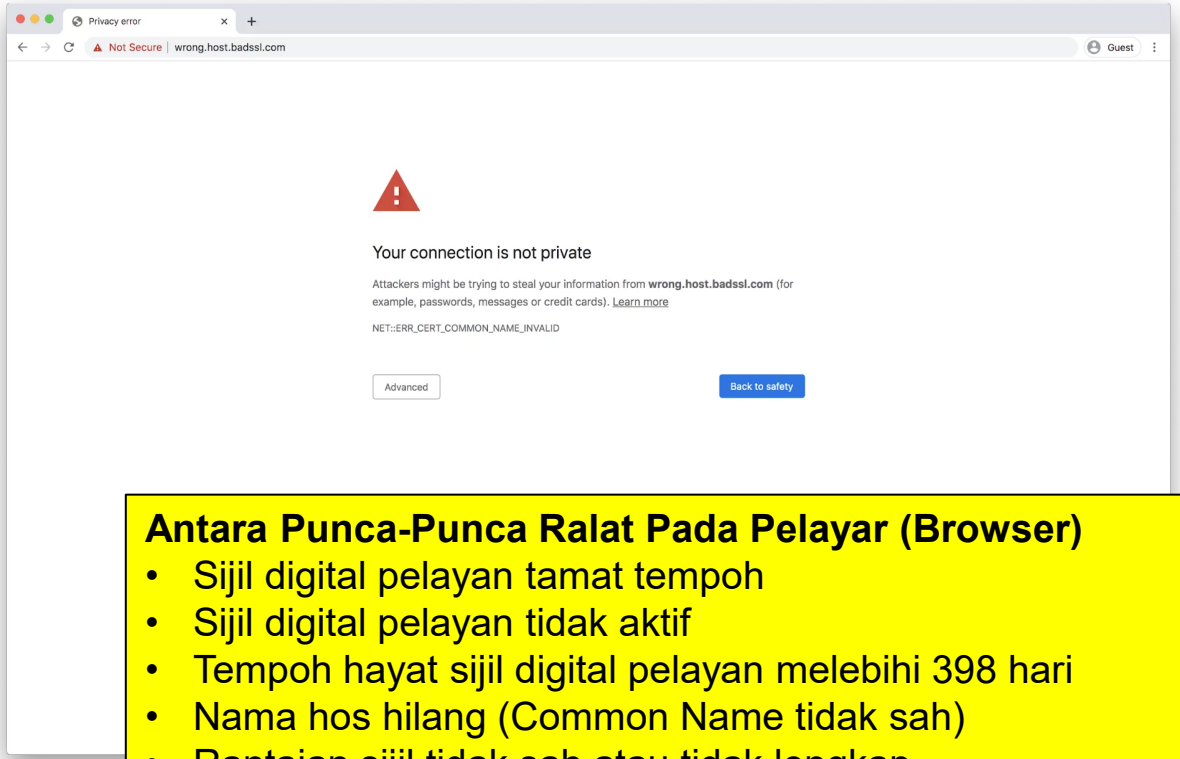


CHAIN COMPLETE
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: Ca_Cert_Intermediate.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: Ca_Cert_Root.crt)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

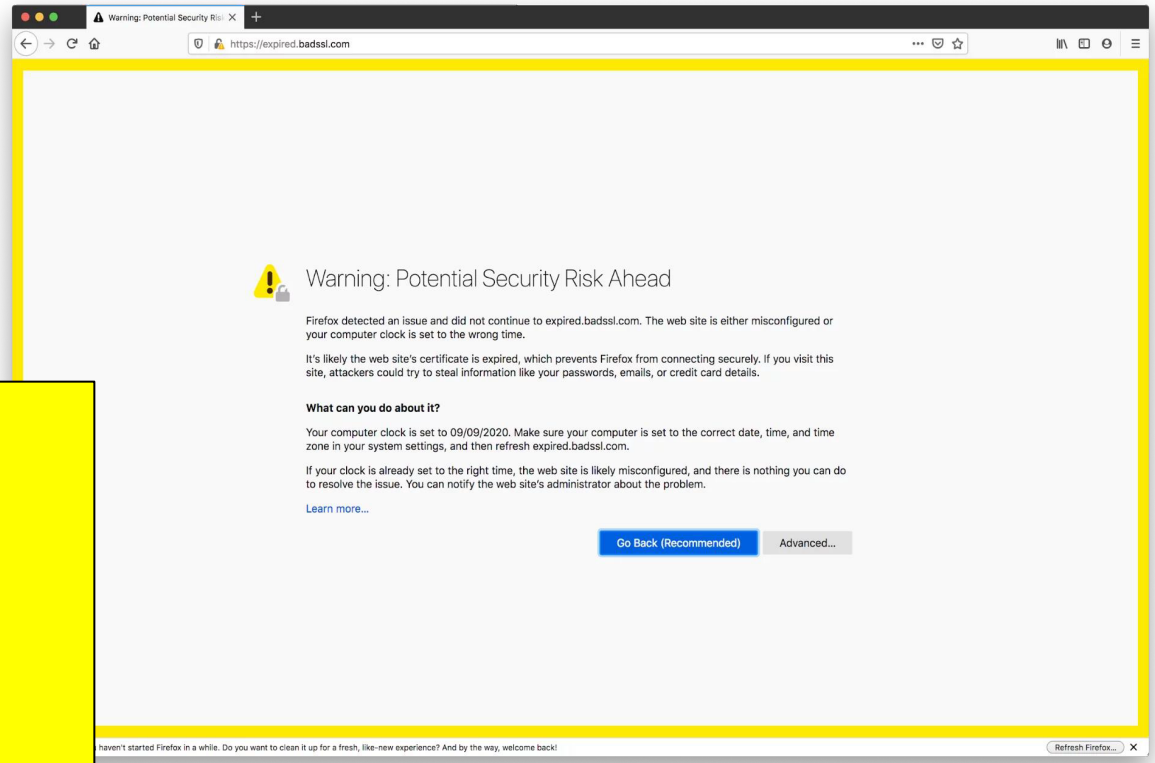
Sijil intermediate dan root CA boleh diperoleh dari pelbagai cara berlainan bergantung kepada kaedah operasi setiap prinsipal sama ada akan diterima dari prinsipal melalui e-mel semasa penghantaran sijil bagi domain/subdomain atau boleh dimuat turun daripada Portal Prinsipal berkenaan.

Ralat Sijil Digital Pelayan

PAPARAN RALAT BAGI GOOGLE CHROME



PAPARAN RALAT BAGI FIREFOX

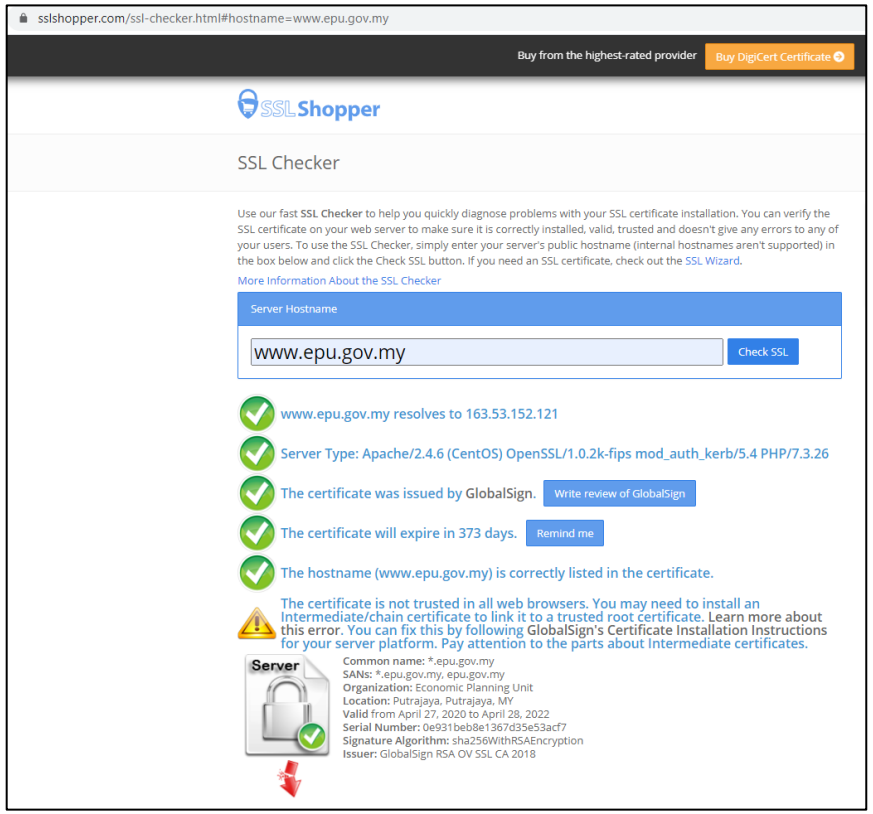


Antara Punca-Punca Ralat Pada Pelayar (Browser)

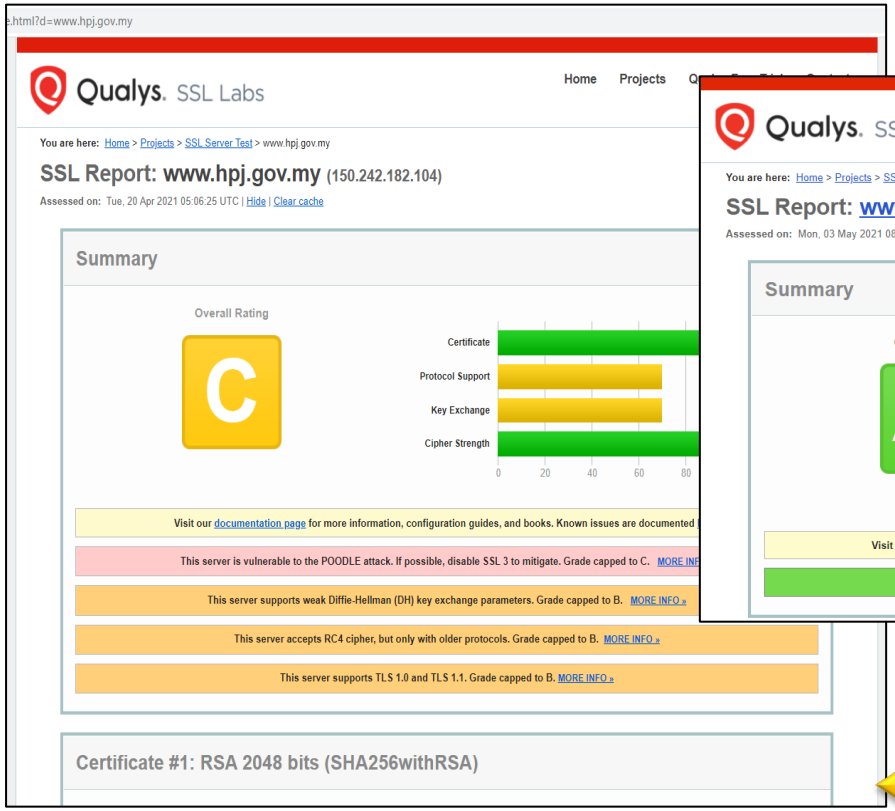
- Sijil digital pelayan tamat tempoh
- Sijil digital pelayan tidak aktif
- Tempoh hayat sijil digital pelayan melebihi 398 hari
- Nama hos hilang (Common Name tidak sah)
- Rantaian sijil tidak sah atau tidak lengkap
- Sijil digital pelayan telah dibatalkan
- *Certification Authority* (CA) yang tidak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

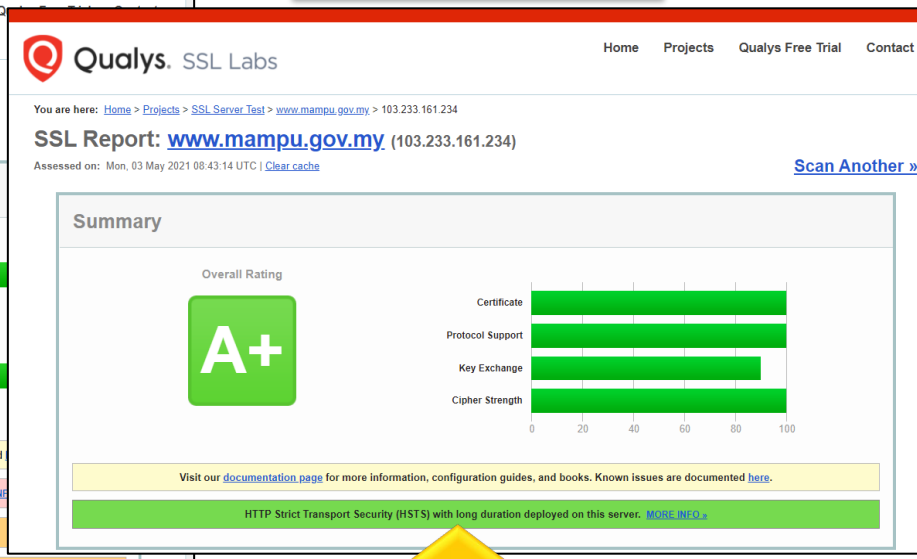
Tools Semakan Pemasangan

SSL Shopper



SSL Labs





Agensi hendaklah mendapat **Taraf A**

Contoh pemasangan sijil dengan konfigurasi yang betul

Tools SSL Labs – Pembetulan Ralat

#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
IIS: Aplikasi iis crypto 3.3 dlm server

#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

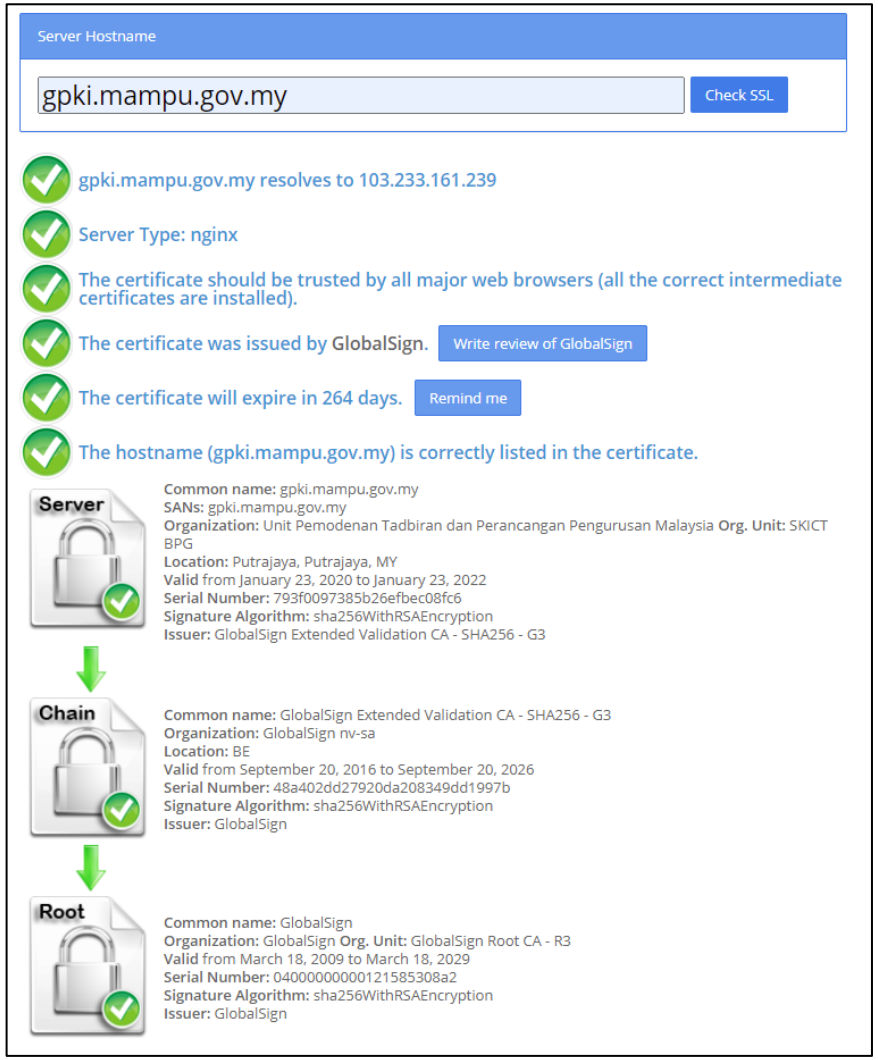
Tools SSL Shopper (Chain Certificate) – Pembetulan Ralat

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

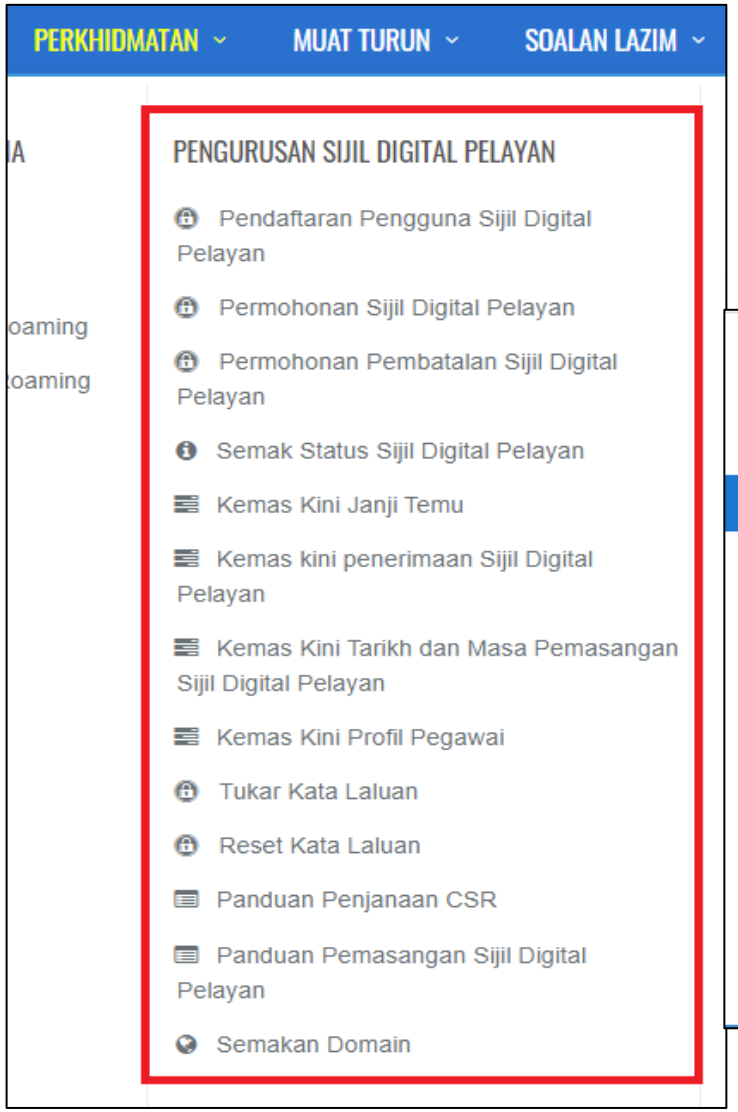
#Finding 2: HTTPS on port 443
=> restricted on firewall/load balancer atau check firewall allow tidak HTTPS connection inbound

#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



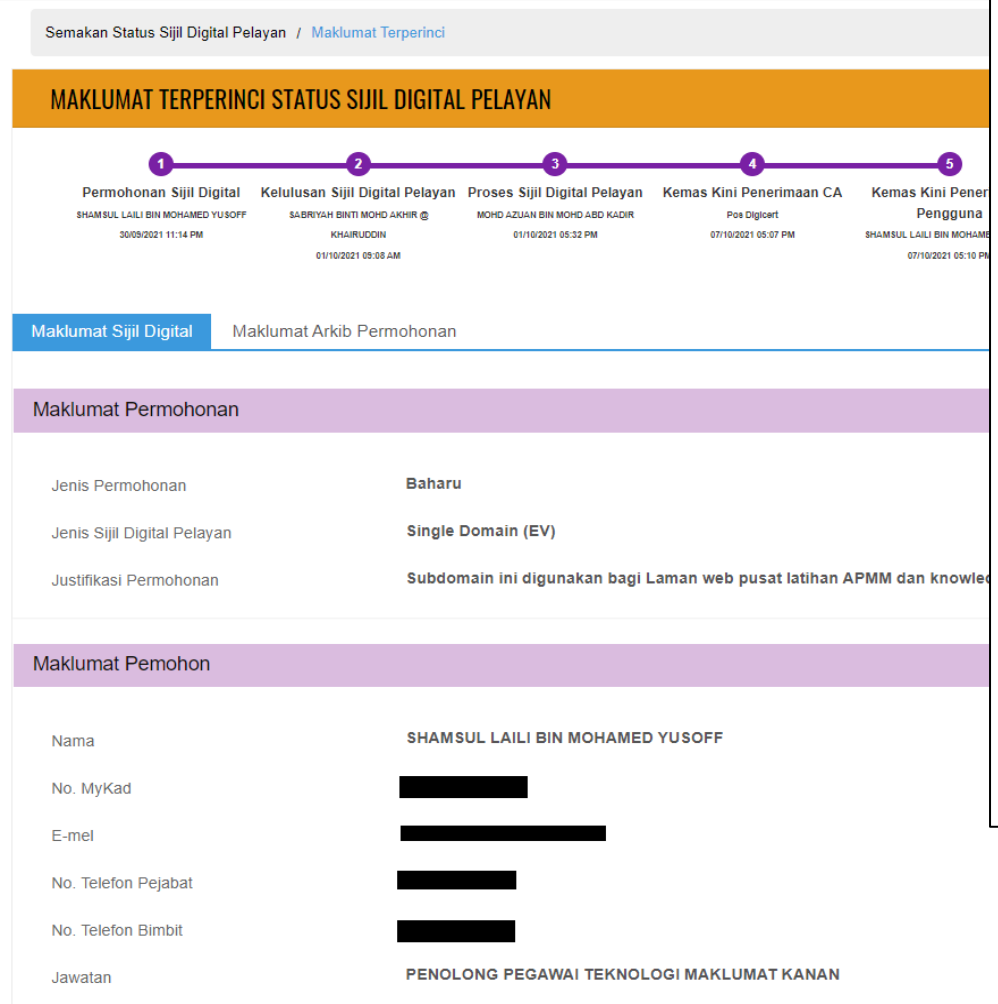
3.2: Pengurusan Sijil Digital Pelayan Di Portal GPKI

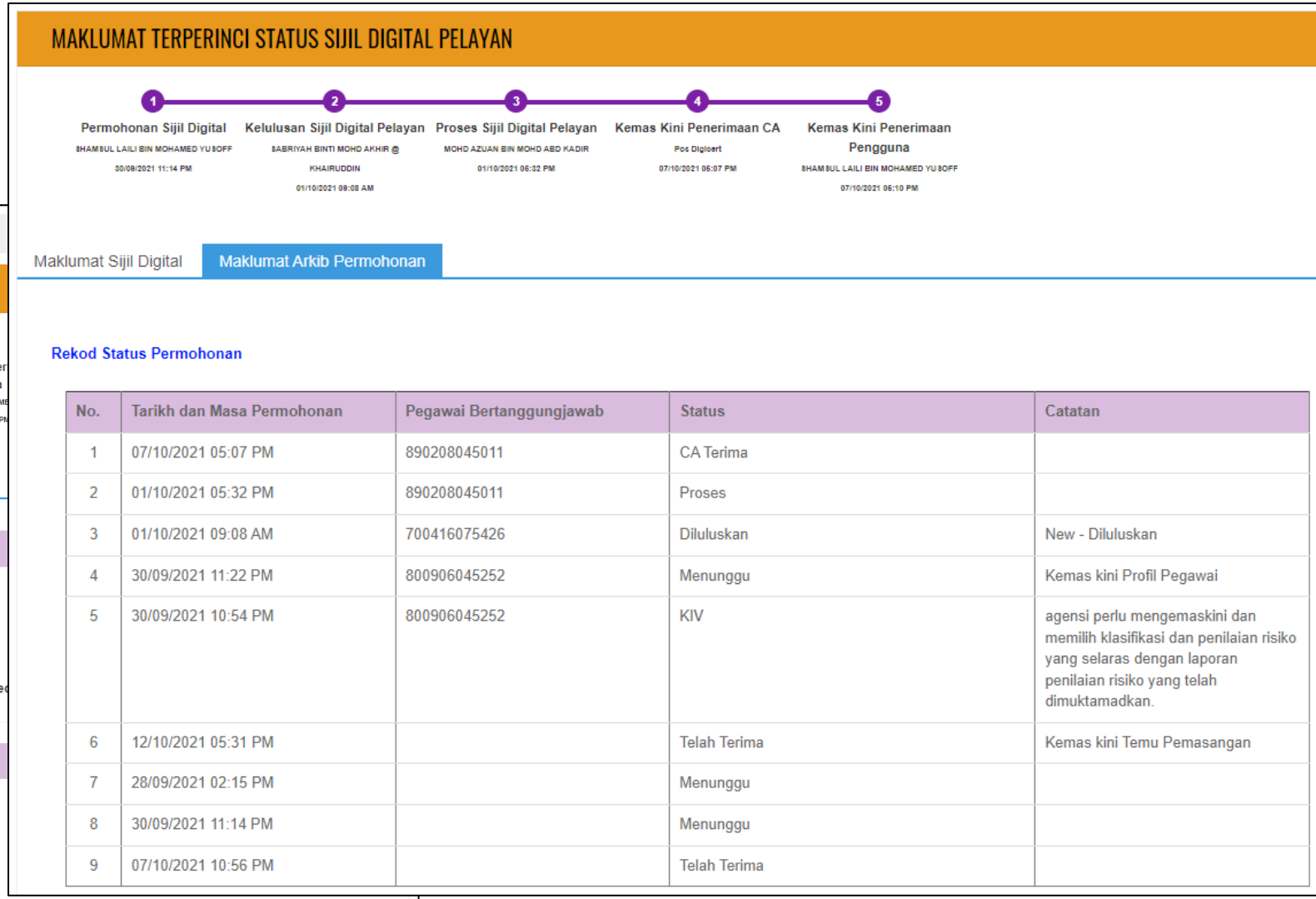


Kesemua 13 menu yang terdapat di bawah Menu "**Pengurusan Sijil Digital Pelayan**" di Portal GPKI 3.0 perlu digunakan oleh pegawai pentabdir pelayan di agensi bagi menguruskan permohonan SSL.

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.

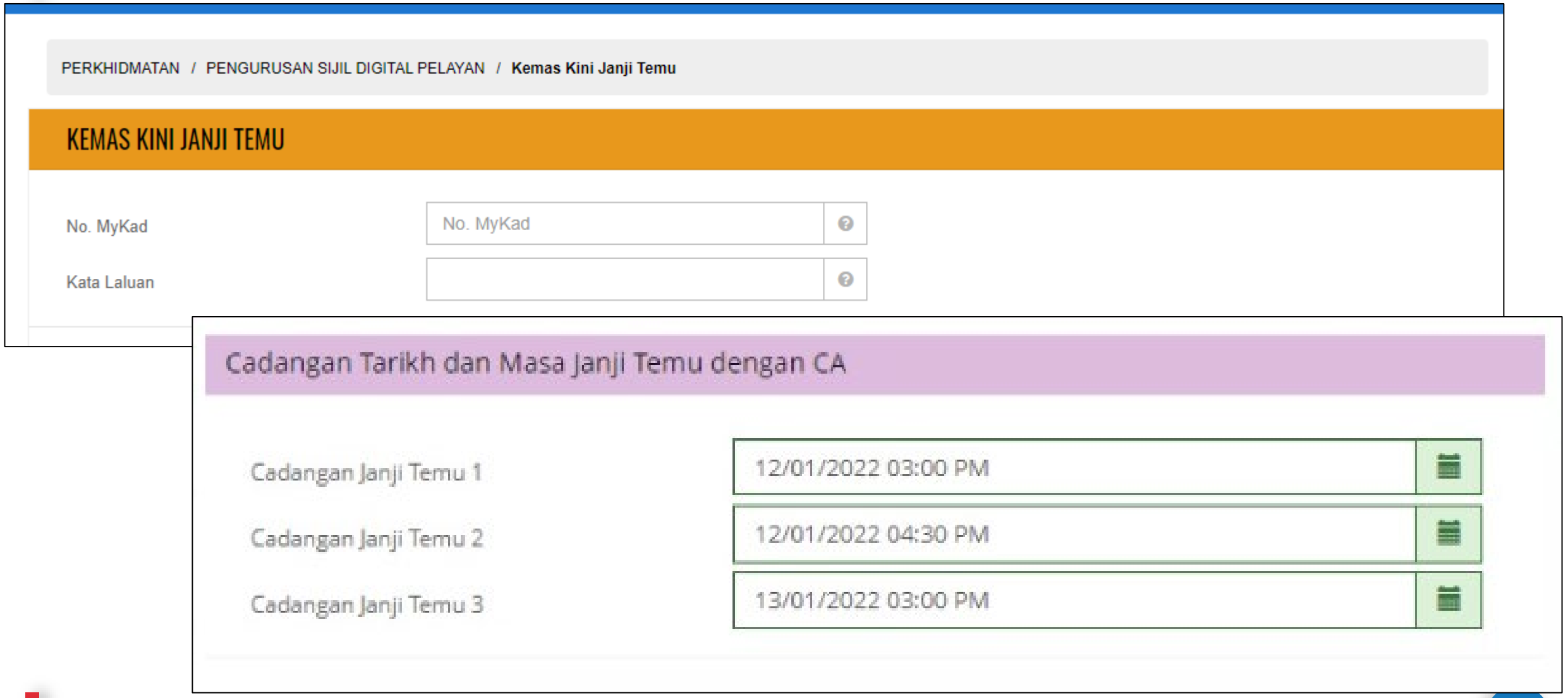
Semak Status Permohonan Sijil



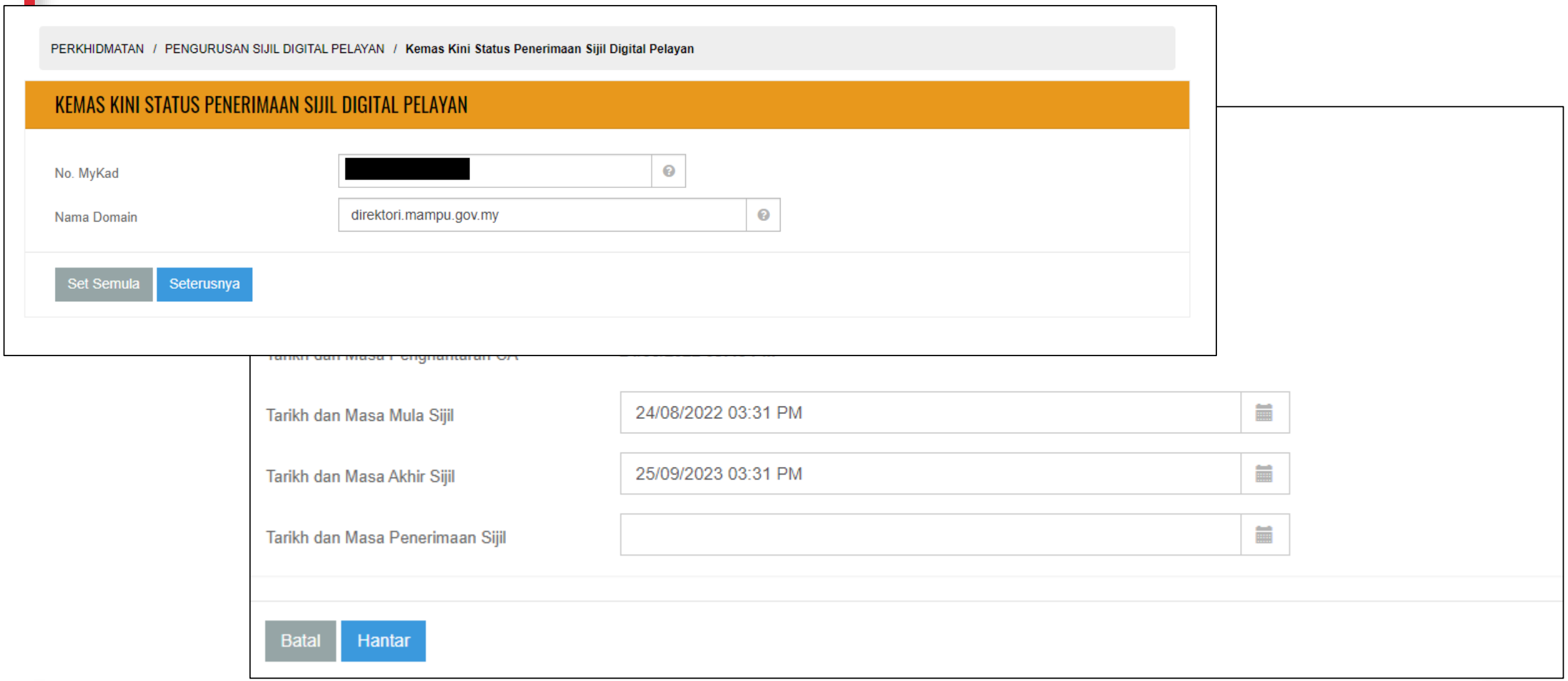


No.	Tarikh dan Masa Permohonan	Pegawai Bertanggungjawab	Status	Catatan
1	07/10/2021 05:07 PM	890208045011	CA Terima	
2	01/10/2021 05:32 PM	890208045011	Proses	
3	01/10/2021 09:08 AM	700416075426	Diluluskan	New - Diluluskan
4	30/09/2021 11:22 PM	800906045252	Menunggu	Kemas kini Profil Pegawai
5	30/09/2021 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	

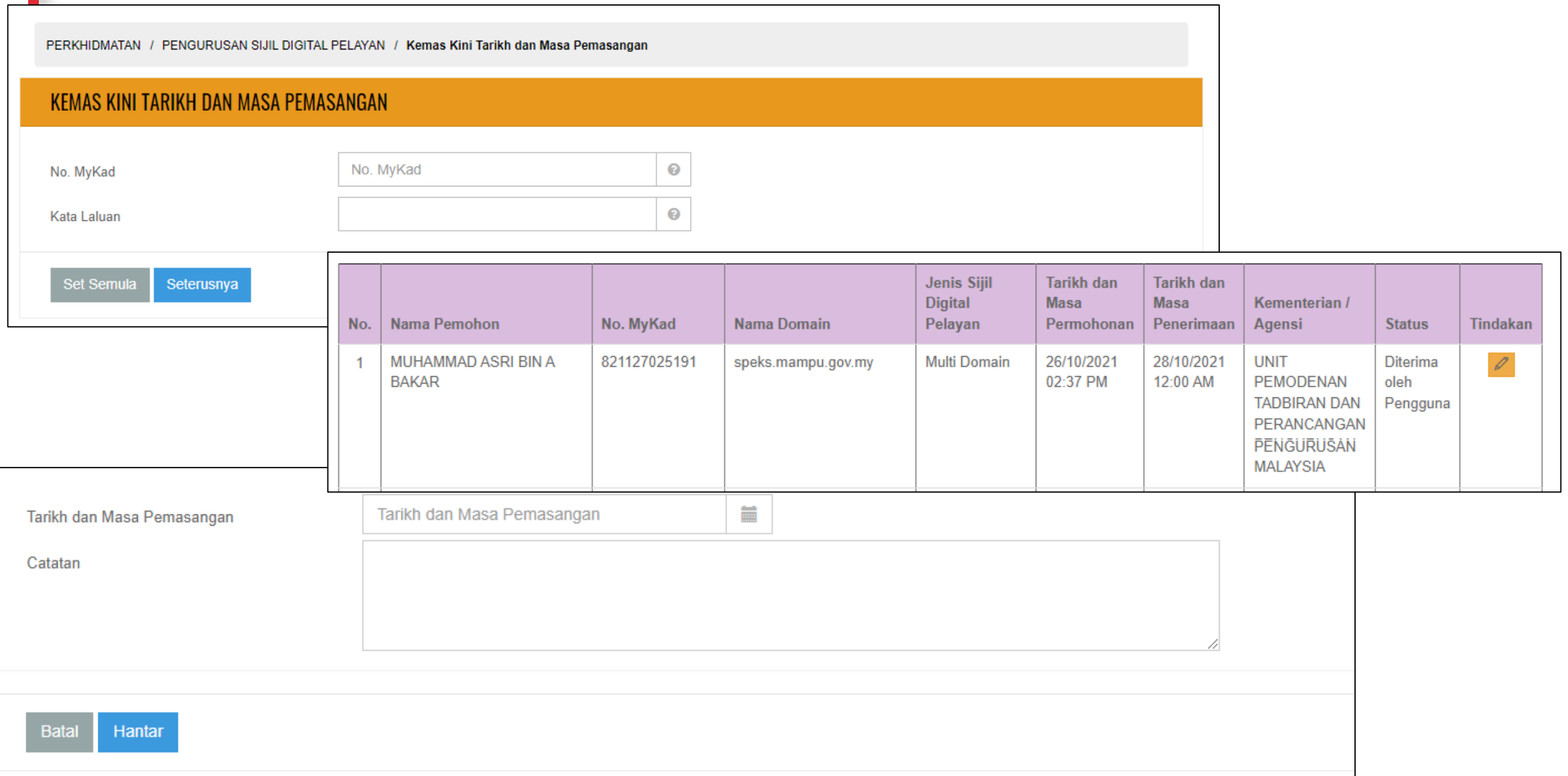
Kemaskini Janji Temu



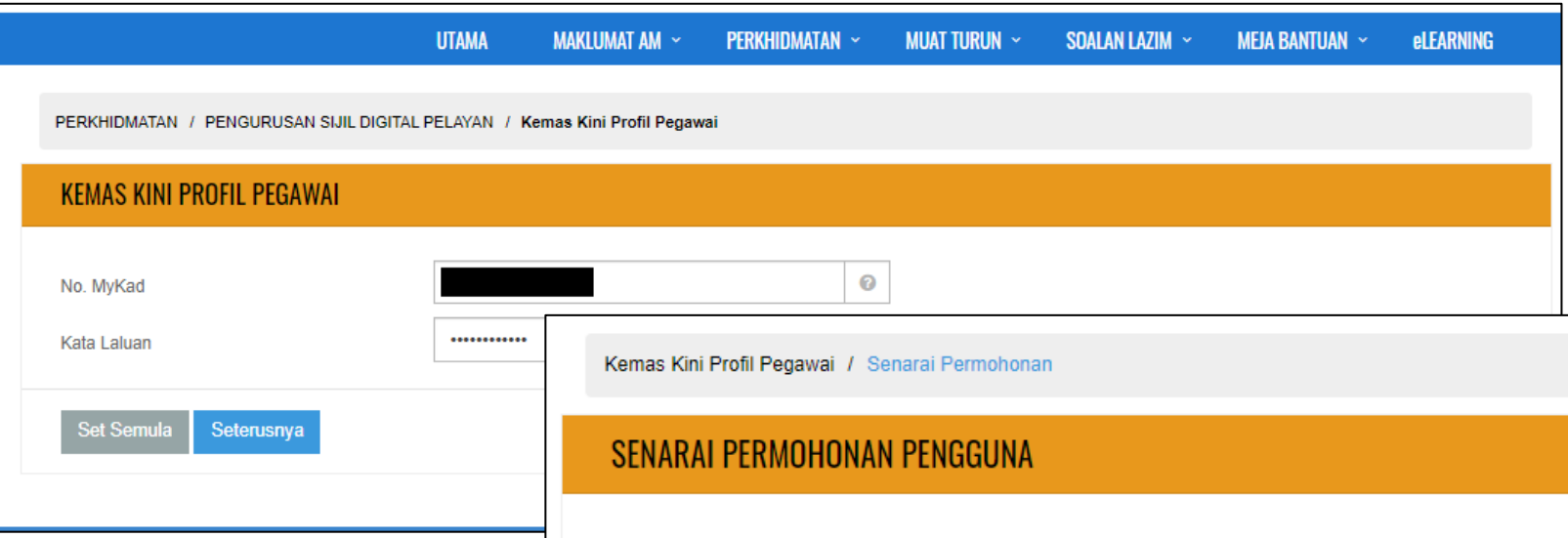
Kemaskini Penerimaan Sijil



Kemaskini Pemasangan Sijil



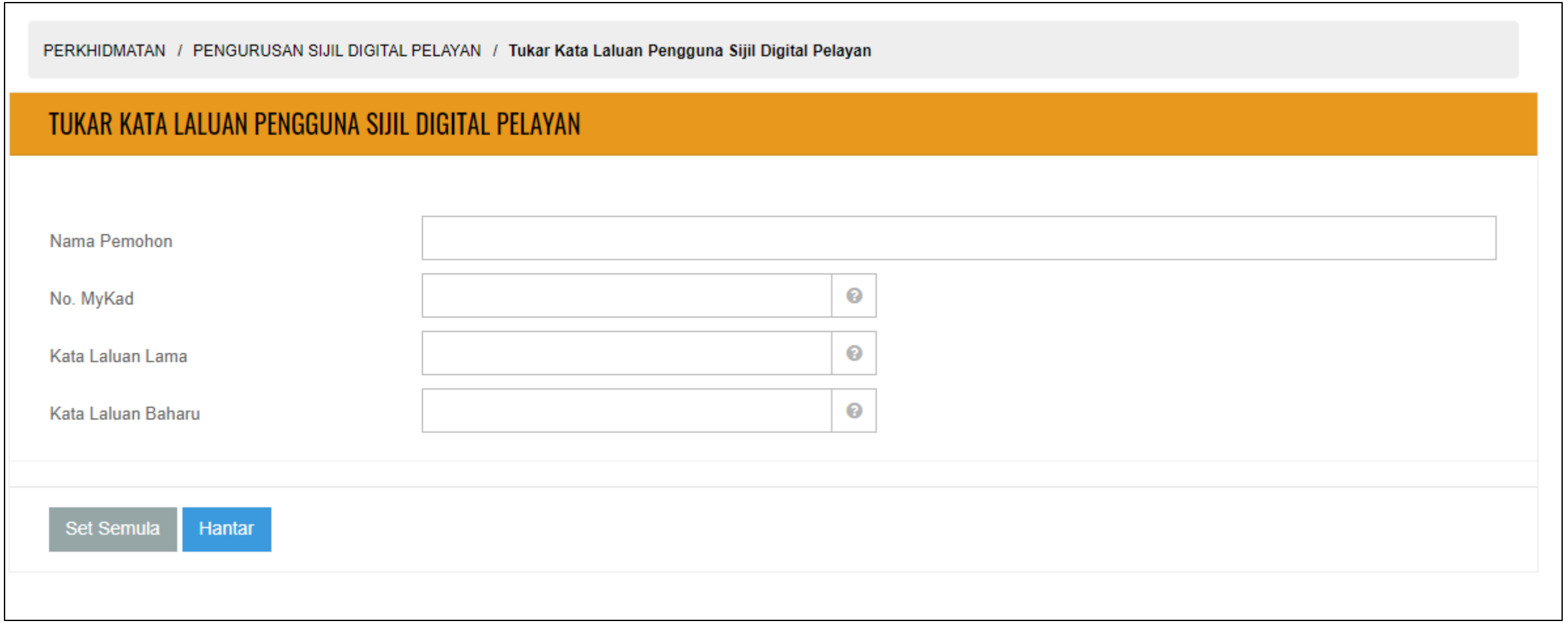
Kemaskini Profil Pegawai



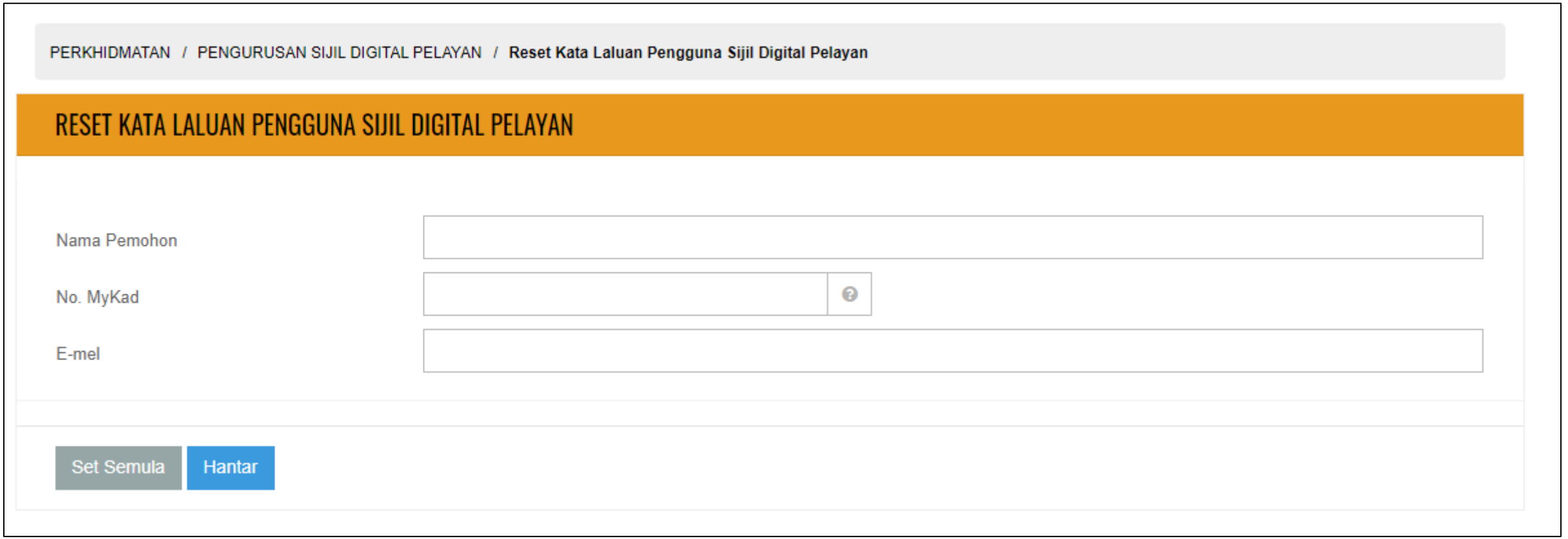
- **Pentadbir Pelayan Bertukar atau Berpindah Agensi**

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	

Tukar Kata Laluan

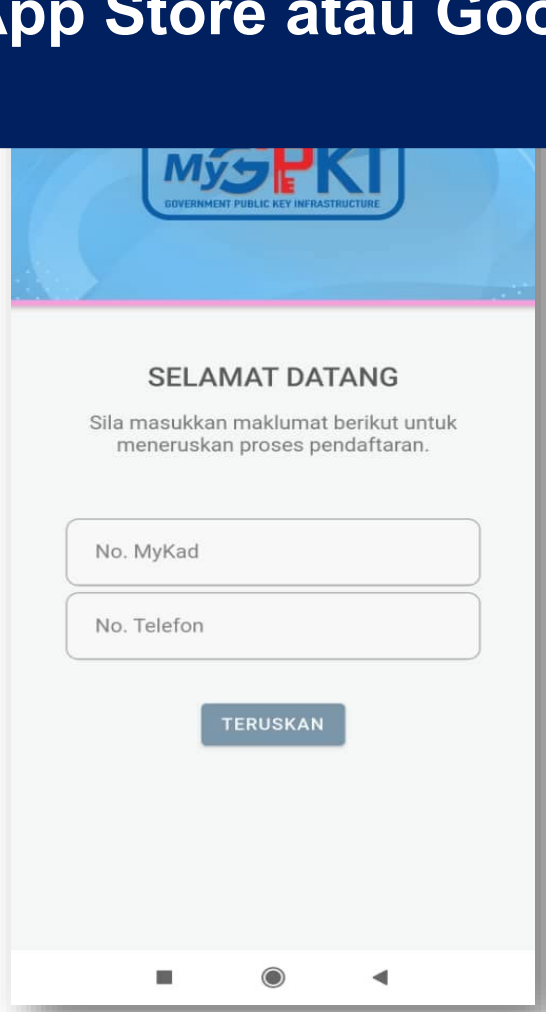


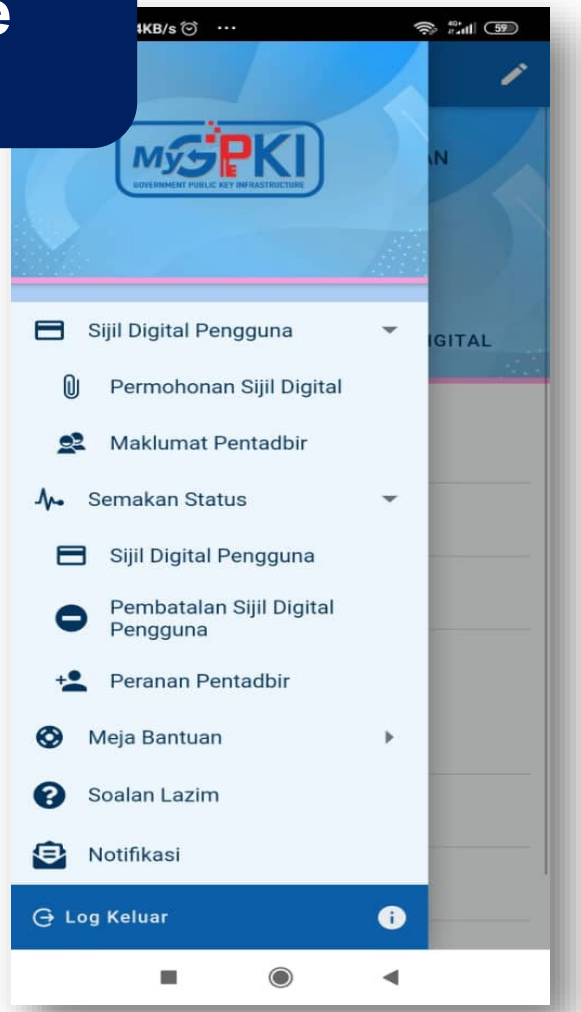
Reset Kata Laluan

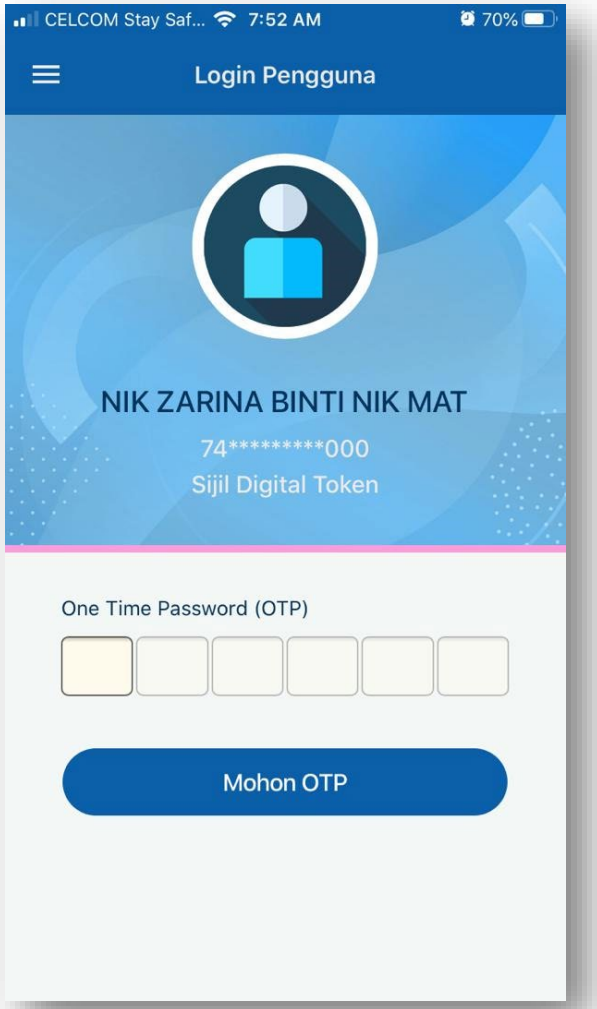


3.3: GPKI Mobile untuk SSL, GPKI Desk dan GPKI eLearning

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

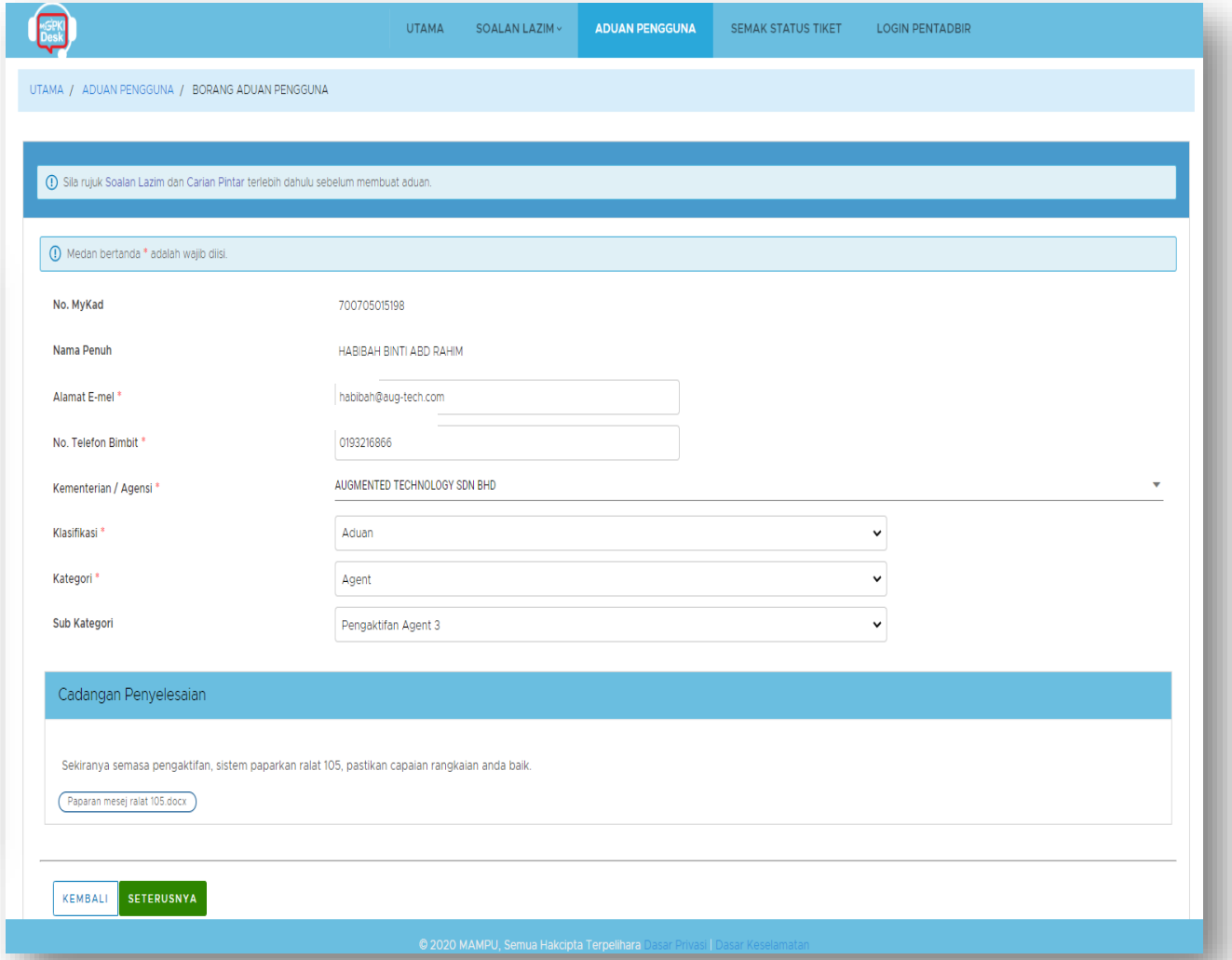






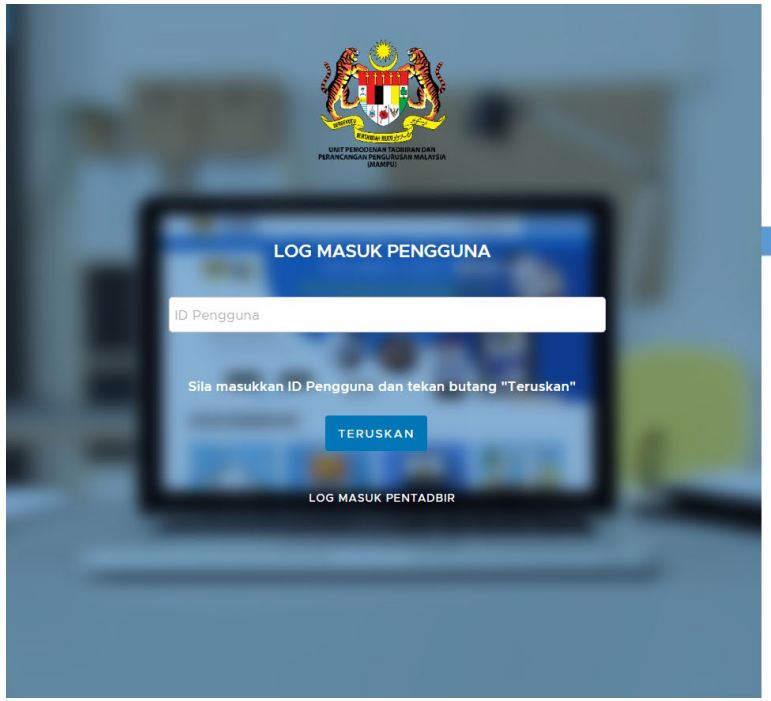
Sistem GPKI Desk

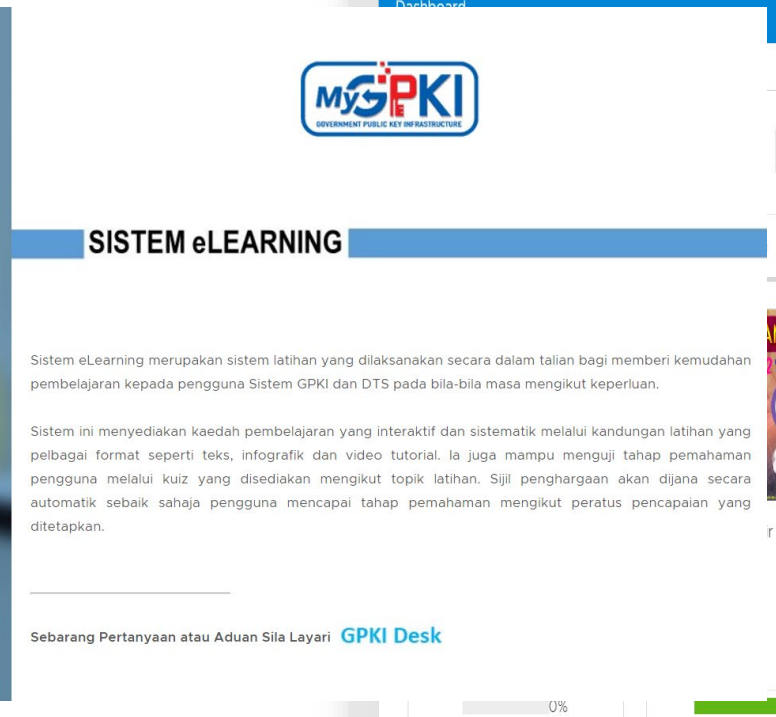
https://gpkidesk.mampu.gov.my



GPKI eLearning

https://gpkielearning.mampu.gov.my





Sesi Soal Jawab

JABATAN PERDANA MENTERI
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA
(MAMPU)

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Seminar Pengurusan Sijil Digital Pelayan (SSL/TLS)

Hotel Marriott Putrajaya
3 Oktober 2023

Topik 4
POV: e-vetting SSL/TLS

RAFFTECH
CERTIFICATION AUTHORITY

Lot 33B-M-04, Block B, Mezzanine Floor,
Villa Putra Condominium, Jalan Tun Ismail
50480 Kuala Lumpur
www.raffcomm.my

TM

TM Technology Services Sdn Bhd.Cybersecurity Division.2nd Floor, TM IT Kompleks,3300, Lingkaran Usahawan 1 Timur,63000 Cyberjaya, Selangor
https://www.tmca.com.my/

Isu-isu Dalam 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.

3 Kemaskini Maklumat agensi dan maklumat pemohon

Portal MyGov **www.malaysia.gov.my**
- GeoTrust

Malaysia Government Call Centre(MyGCC)
- GeoTrust

Proses Verifikasi *Organization Validated* (OV)

CA

CA akan **proses sijil digital pelayan** di Portal GPKI

PRINSIPAL

Prinsipal melaksanakan proses **pengesahan eVetting**:
Agent Authorization Form –Pemohon sahaja

***Organization Vetting* (e-mel)** Pemohon sahaja

Domain Validation:
E-mel dan DNS

PEGAWAI AGENSI

Pegawai agensi **Kemaskini Maklumat penerimaan**

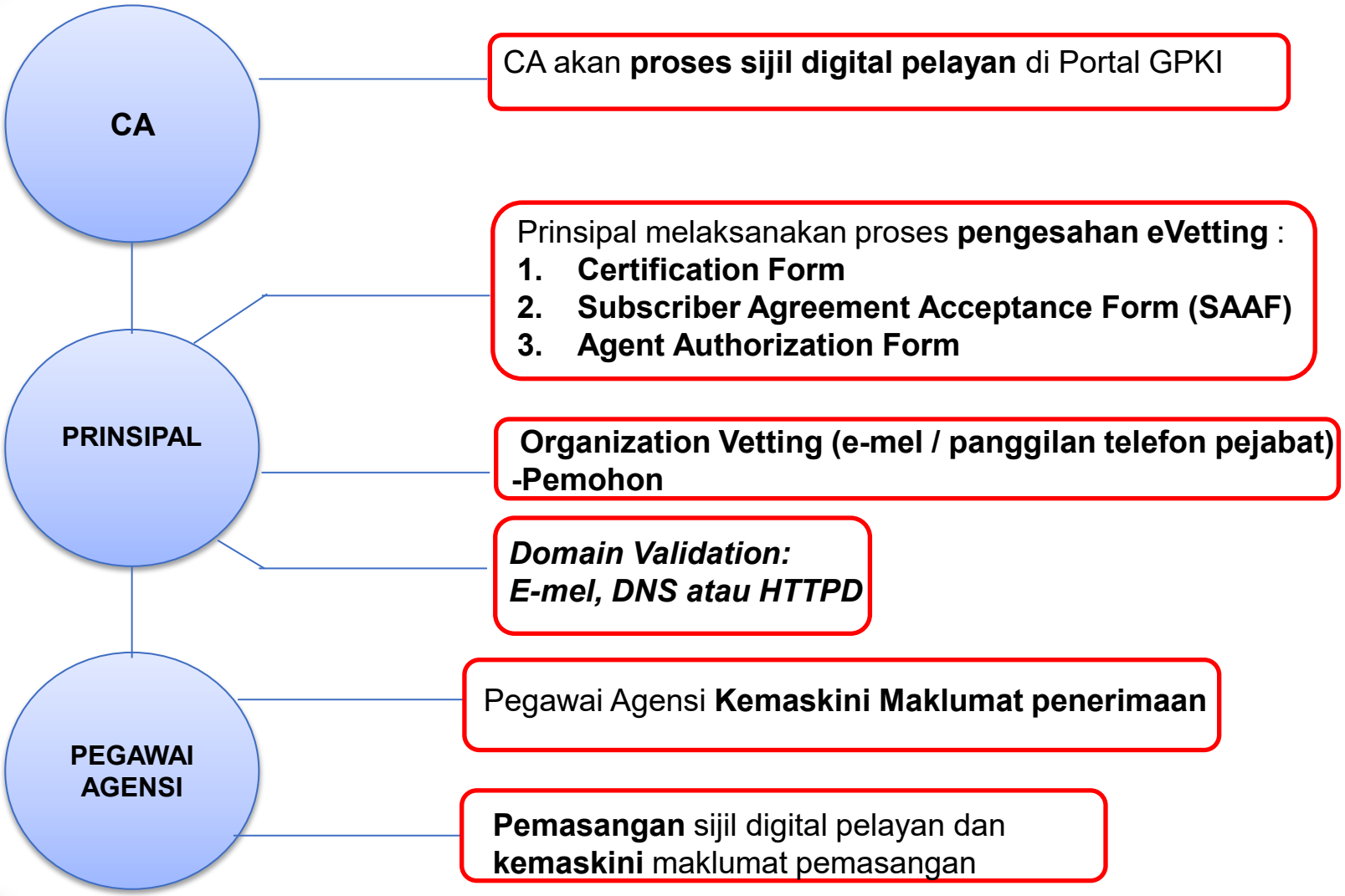
Pemasangan sijil digital pelayan dan **kemaskini** maklumat pemasangan

OV

Organization Validated

1. Agent Authorization Form
2. Organization Vetting
3. Domain Validation

Proses Verifikasi *Extended Validated* (EV)



EV

Extended Validated

1. Certification Form
2. Subscriber Agreement Acceptance Form (SAAF)
3. Agent Authorization Form
4. Organization Vetting
5. Domain Validation

Kaedah Pengesahan Domain

E-mel

1. E-mel Domain constructive e-mel default :

   admin@mampu.gov.my

   administrator@mampu.gov.my

   hostmaster@mampu.gov.my

   webmaster@mampu.gov.my

   postmaster@mampu.gov.my

2. Pengemaskinian maklumat di MyNIC :

   General Line (9 pagi – 6 petang)

   Telefon:603 80082000

   Faksimili:603 80082020

   E-mel: customercare@mynic.my

   Chatbot: MYNIC Live Chat URL: https://mynic.my/contact-us

   Pautan aduan :https://mynic.my/contract

Nota : Akta Perlindungan Data Peribadi 2010 mulai 8 November 2022

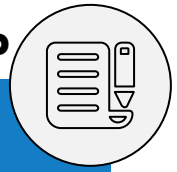
DNS

1. Agensi perlu membuat *random text* yang diberikan oleh principal melalui e-mel.
2. Pengesahan domain hanya akan berjaya sekiranya prinsipal dapat menyemak semula keujudan *random text* di DNS domain/subdomain dengan paparan *random text*

Nota : Sebarang perubahan DNS adalah dibawah kelolaan pihak GITN. Oleh itu,pihak agensi perlu menghubungi terus kepada GITN iaitu https://mygovosf.gitn.net.my

https://support.globalsign.com/ssl/ssl-certificates-life-cycle/performing-domain-verification-dns-txt-record

HTTP

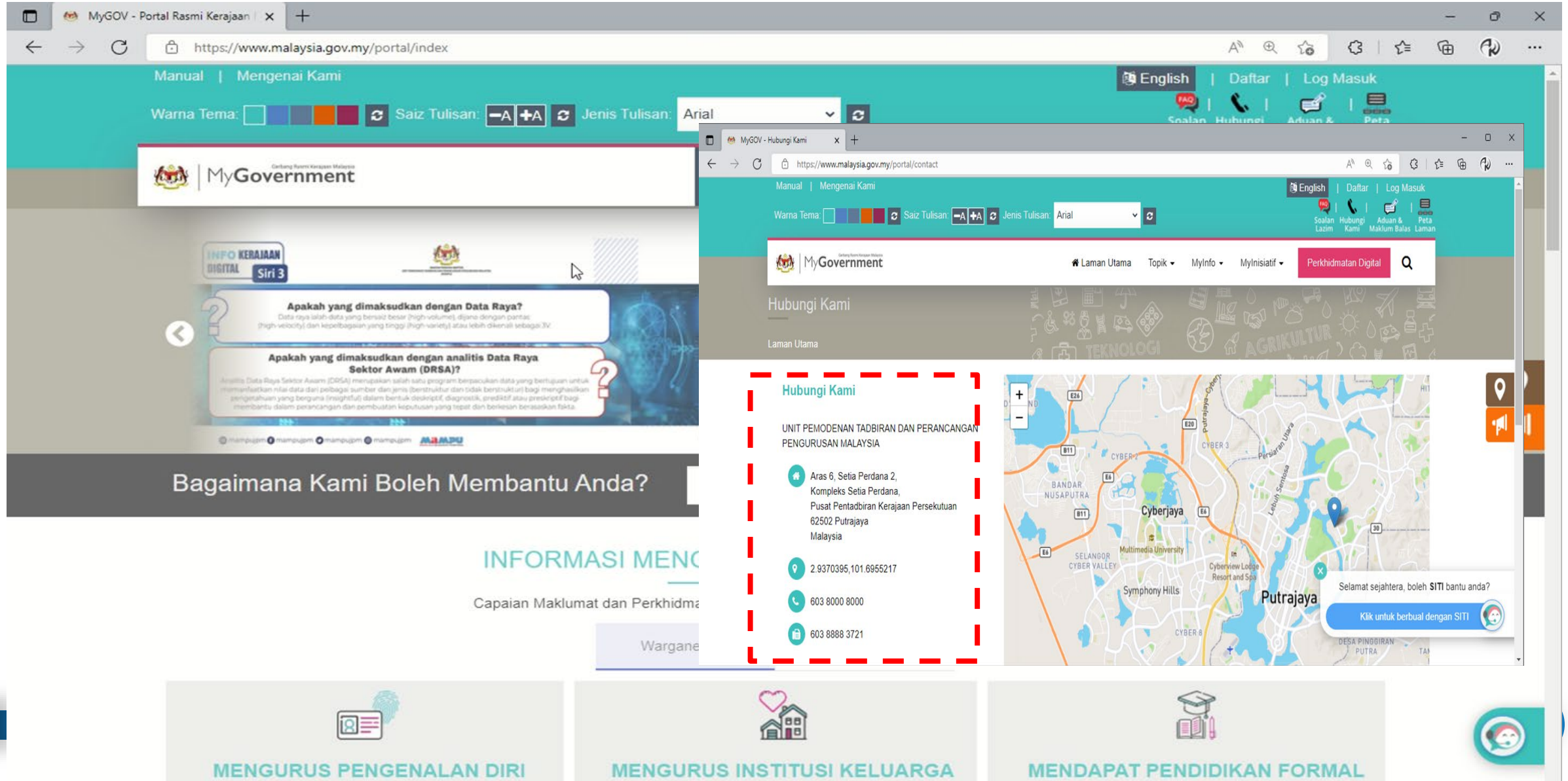


1. Agensi perlu membuat *random text* yang diberikan oleh pihak prinsipal *(well-know*/PKI folder)
2. Pengesahan domain adalah berjaya sekiranya principal dapat menyemak semula *random text*.

Nota : Hanya terpakai untuk *Single Domain Extended validation* sahaja.

https://support.globalsign.com/ssl/ssl-certificates-installation/install-ssl-certificate-overview

Portal MyGovernment



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:

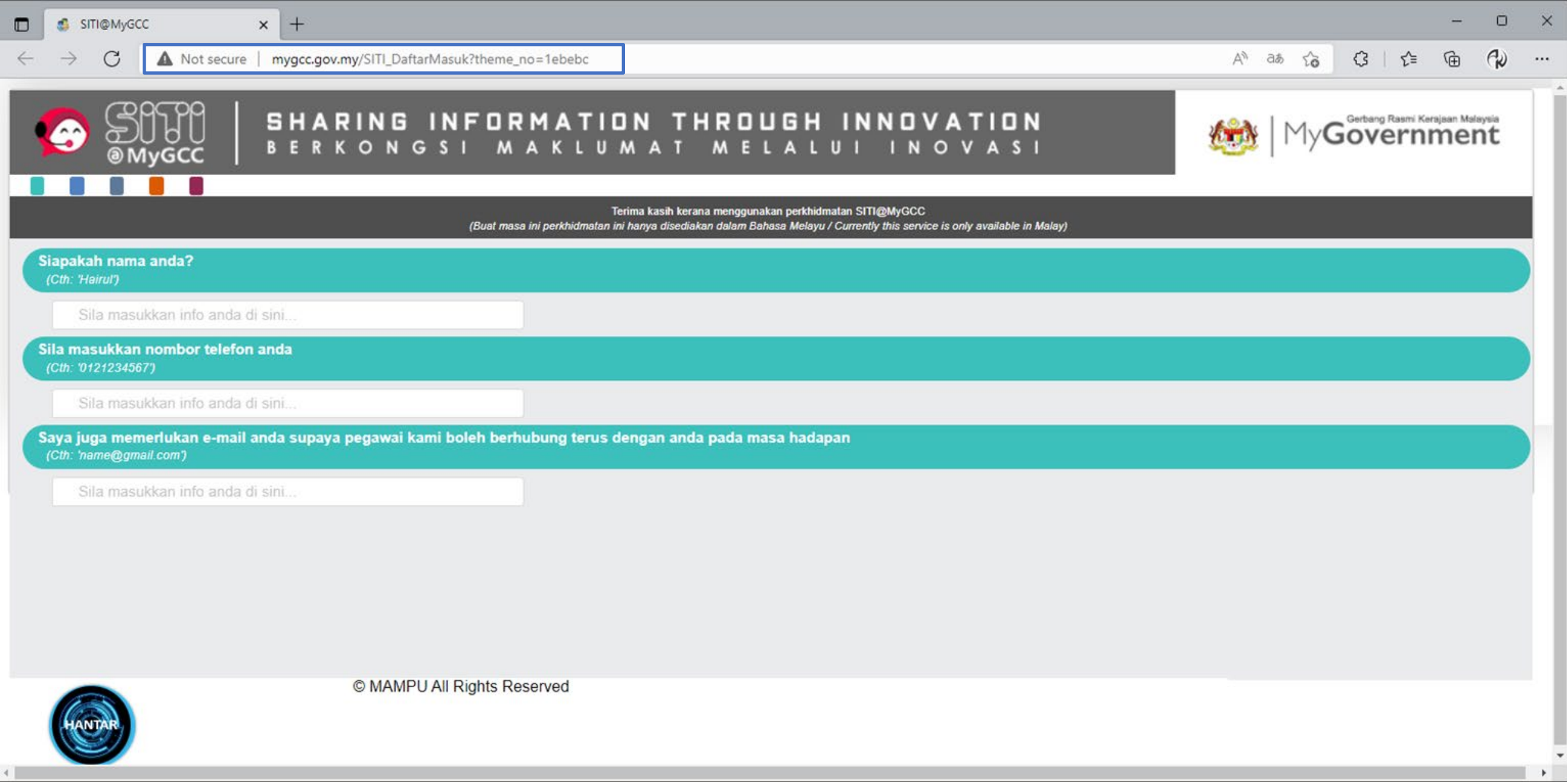
- **Telefon/SMS/IVR : 03-8000 8000**
- **E-mel : 80008000@mygcc.gov.my**
- **Chatbot : SITI@MyGCC**
- **Facebook : facebook.com/MyGCCMalaysia**
- **Instagram : @MyGCCMalaysia**
- **Twitter : twitter.com/MyGCCMalaysia**
- **Portal : www.malaysia.gov.my**

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


SITI@MyGCC
Not secure | mygcc.gov.my/SITI_DaftarMasuk?theme_no=1ebebc
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...
© MAMPU All Rights Reserved
HANTAR

Kembali

Isu-isu Dalam Proses Pengesahan Sijil

4 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.

5 PANGGILAN PENGESAHAN

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

Kemas Kini Janji Temu

Isu-isu Dalam Proses Pengesahan Sijil

6 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.

7 MASALAH PEMASANGAN SIJIL

Bagaimana untuk install?

Tidak cuba untuk buat pemasangan sendiri.

Pemasangan via Remote. ✖

Contoh E-mel Verifikasi oleh Prinsipal

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.

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]

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**.

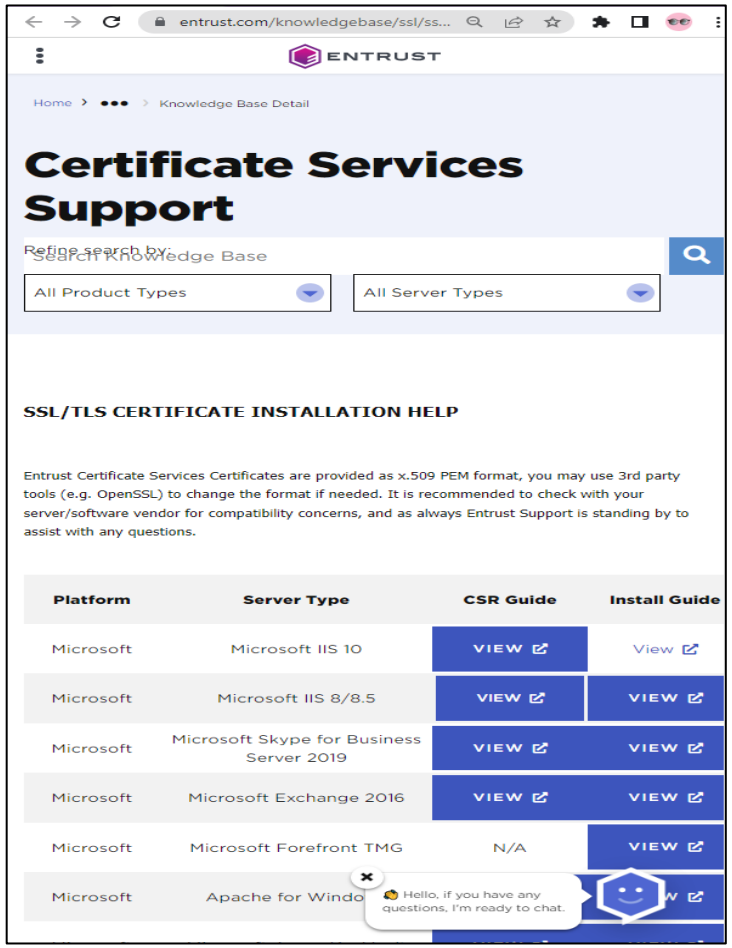
Please attach the document with a reply to this email or fax it to 1-866-842-0223.

Manual Pengguna Untuk Pemasangan SSL

GlobalSign by GMO

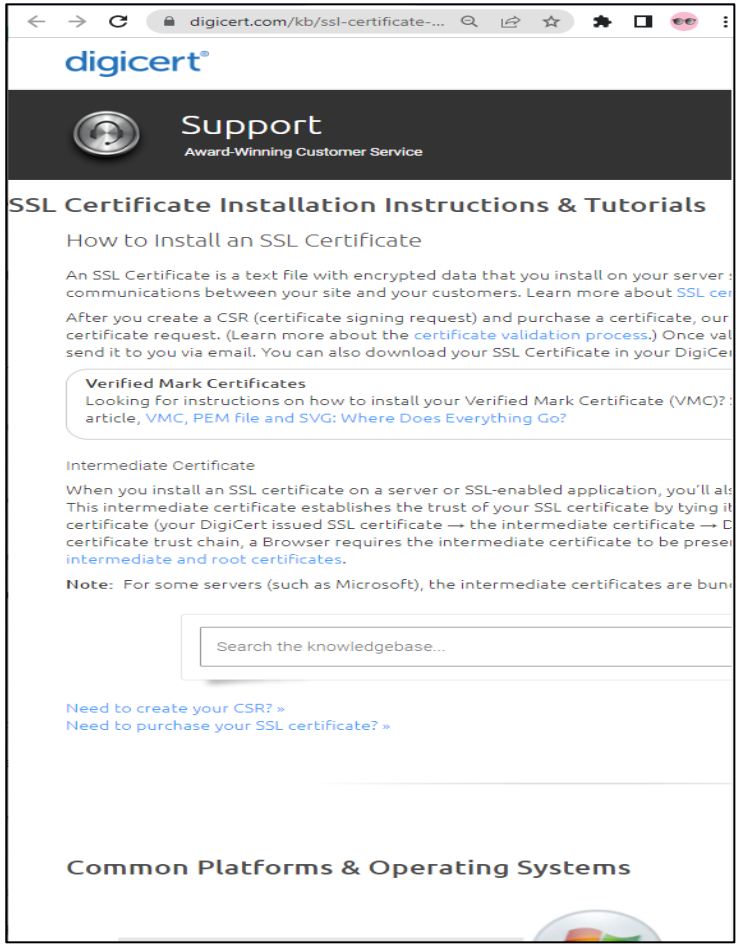
https://support.globalsign.com/ssl/ssl-certificates-installation/install-ssl-certificate-overview

ENTRUST



https://www.entrust.com/knowledgebase/ssl/ssl-tls-certificate-installation-help

GeoTrust powered by digicert



https://www.digicert.com/kb/ssl-certificate-installation.htm

Sesi Soal Jawab

JABATAN PERDANA MENTERI
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA
(MAMPU)

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Seminar Pengurusan Sijil Digital Pelayan (SSL/TLS)

Hotel Marriott Putrajaya
3 Oktober 2023

Topik 5:
Jom *Install* & *Test*-lah SSL/TLS

JABATAN PERDANA MENTERI
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA
(MAMPU)

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

PEMASANGAN SIJIL DIGITAL PELAYAN

Operating System: Unix

OpenSSL dan Java keytool

Langkah Pemasangan Sijil SSL

1. Jana Key
2. Jana CSR
3. Hantar CSR kepada CA
4. Terima Sijil SSL daripada CA
5. Pemasangan Sijil SSL
6. Konfigurasi Tetapan SSL

Common Cryptography Software Library

1 Jana Key

2 Jana CSR

OpenSSL

Java keytool (JKS)

Mozilla Network Security Services (NSS)

Microsoft CryptoAPI

IBM Key Management (iKeyMan)

Web Server

OpenSSL	Apache HTTP Server, NGINX
Java keytool (JKS)	Apache Tomcat, WildFly, JBoss, Oracle Weblogic
Microsoft CryptoAPI	Microsoft Internet Information Services (IIS)
Mozilla Network Security Services (NSS)	Sun Java System Web Server
IBM Key Management (iKeyMan)	IBM HTTP Server (HIS), IBM WebSphere App Server

Jana Key dan CSR

OpenSSL

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
```

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out
server.csr -subj "/C=MY/ST=Wilayah Persekutuan/L=Kuala
Lumpur/O=Raffcomm Technologies Sdn Bhd/CN=www.rafftech.my"
```

Jana Key dan CSR

OpenSSL

GPKI-2023 — openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr — 79×30

```
anais@AnaisMacBookPro2017 GPKI-2023 % openssl req -new -newkey rsa:2048 -nodes
-keyout server.key -out server.csr
..+.....++++++++++++++++++++++++++++++++++++++++*.....+.++++++++++++++++++++++
++++++++++++++++*..........+.+..+....+.........+.............+...+...+......+
...+............+...+..........++++++
...+.........+...........++++++++++++++++++++++++++++++++++++++++*....+........
......+.........+..+.............+....+...+...+..+...+...+....+..+.........
........+.+.....++++++++++++++++++++++++++++++++++++*.+.+.....+............
+..+...........+.++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MY
State or Province Name (full name) [Some-State]:Wilayah Persekutuan
Locality Name (eg, city) []:Kuala Lumpur
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Raffcomm Technologie
s Sdn Bhd
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:www.rafftech.my
```

Jana Key dan SAN CSR

OpenSSL

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out
server.csr -subj "/C=MY/ST=Wilayah Persekutuan/L=Kuala
Lumpur/O=Raffcomm Technologies Sdn Bhd/CN=www.rafftech.my" -config
san.conf
```

Jana Key dan SAN CSR

OpenSSL

GPKI-2023 — -zsh — 79×30

```
anais@AnaisMacBookPro2017 GPKI-2023 % cat 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 = Wilayah Persekutuan
localityName                = Locality Name (eg, city)
localityName_default        = Kuala Lumpur
organizationName            = Organization Name (eg, company)
organizationName_default    = Raffcomm Technologies 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.rafftech.my
DNS.2   = www.rafftech.com
DNS.3   = www.rafftech.com.my
anais@AnaisMacBookPro2017 GPKI-2023 %
```

Jana Key dan CSR

Java keytool (JKS)

Jana Key

```
keytool -genkey -keyalg RSA -keysize 2048 -alias tomcat -keystore
serverkey.jks -dname "CN=www.rafftech.my, O=Raffcomm Technologies
Sdn Bhd, L=Kuala Lumpur, S=Wilayah Persekutuan, C=MY"
```

Jana CSR

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

Jana Key dan SAN CSR

Java keytool (JKS)

Jana Key

```
keytool -genkey -keyalg RSA -keysize 2048 -alias tomcat -keystore
tomcat.jks -dname "CN=www.rafftech.my, O=Raffcomm Technologies Sdn
Bhd, L=Kuala Lumpur, S=Wilayah Persekutuan, C=MY" -ext
"SAN=DNS:www.rafftech.com, DNS:www.rafftech.com.my"
```

Jana CSR

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

Langkah Pemasangan Sijil SSL

1. Jana Key
2. Jana CSR
3. Hantar CSR kepada CA
4. Terima Sijil SSL daripada CA
5. Pemasangan Sijil SSL
6. Konfigurasi Tetapan SSL

Pembekal Sijil Digital Pelayan

3

Hantar CSR kepada CA

Langkah Pemasangan Sijil SSL

1. Jana Key
2. Jana CSR
3. Hantar CSR kepada CA
4. Terima Sijil SSL daripada CA
5. Pemasangan Sijil SSL
6. Konfigurasi Tetapan SSL

Terima Sijil Digital Pelayan Daripada CA

4

Terima Sijil SSL daripada CA

.pem

.crt

.der

.cer

```
-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIMDulMwwAAAABR03eFMA0GCSqGSIb3DQEBCwUAMIG+MQsw
CQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2Vl
IHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMDkg
RW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTIwMAYDVQQD
EylFbnRydXN0IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBHMjAeFw0x
NTEwMDUxOTEzNTZaFw0zMDEyMDUxOTQzNTZaMIG6MQswCQYDVQQGEwJVUzEWMBQG
A1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2VlIHd3dy5lbnRydXN0Lm5l
dC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMTIgRW50cnVzdCwgSW5jLiAt
IGZvciBhdXRob3JpemVkIHVzZSBvbmx5MS4wLAYDVQQDEyVFbnRydXN0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IC0gTDFLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2j+W0E25L0Tn2zlem1DuXKVh2kFnUwmqAJqOV38pa9vH4SEkqjrQ
jUcj0u1yFvCRIdJdt7hLqIOPt5EyaM/OJZMssn2XyP7BtBe6CZ4DkJN7fEmDImiK
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-----
```

Terima Sijil Digital Pelayan Daripada CA

4

Terima Sijil SSL daripada CA

.pem

.crt

.der

.cer

Note:

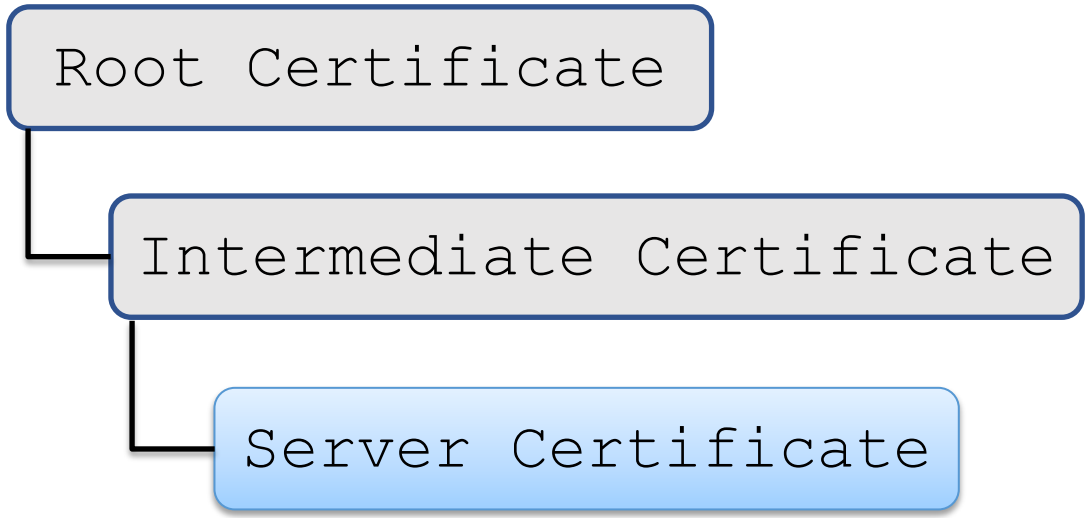
- The PEM format is the most common format used for certificates.
- Extensions used for PEM certificates are cer, crt, and pem.
- They are Base64 encoded ASCII files.

- The DER format is the binary form of the certificate.
- DER formatted certificates do not contain the "BEGIN CERTIFICATE/END CERTIFICATE" statements.
- DER formatted certificates most often use the '.der' extension.

Terima Sijil Digital Pelayan Daripada CA

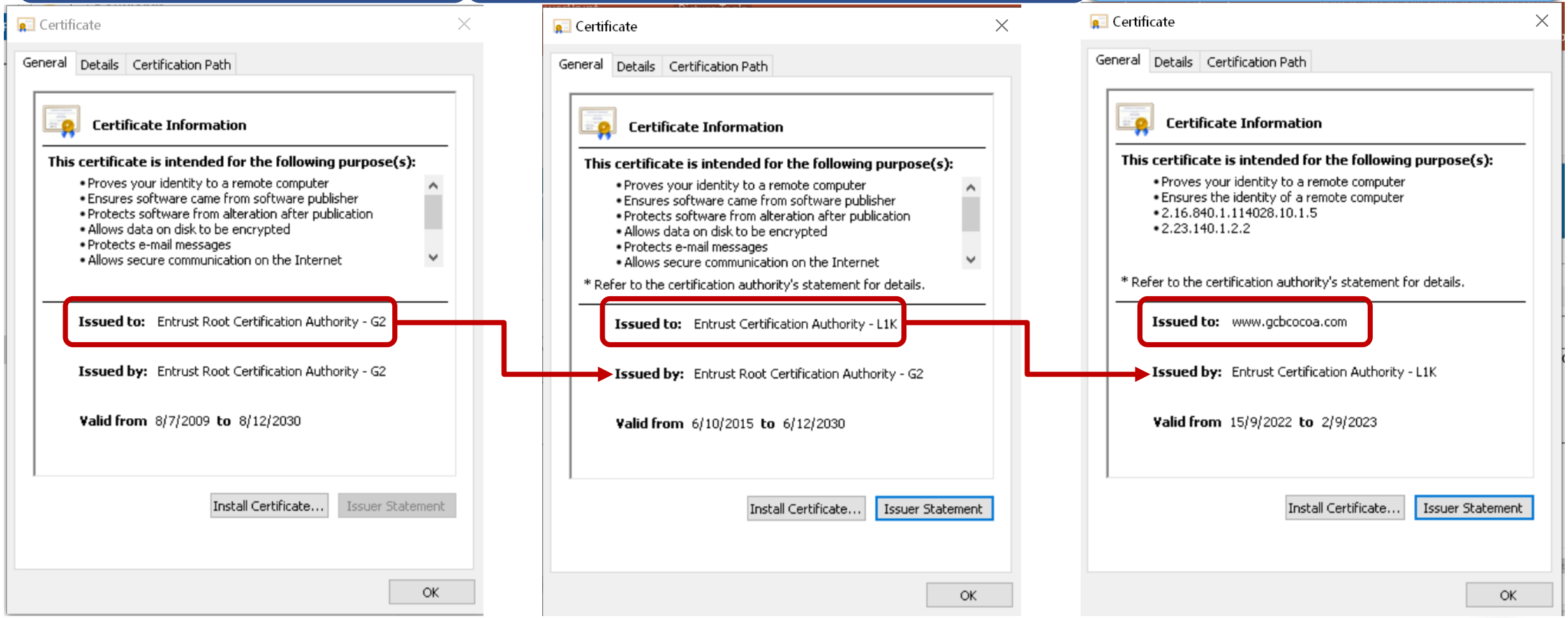
4

Terima Sijil SSL daripada CA



Terima Sijil Digital Pelayan Daripada CA

Root Certificate | Intermediate Certificate | Server Certificate



Langkah Pemasangan Sijil SSL

1. Jana Key
2. Jana CSR
3. Hantar CSR kepada CA
4. Terima Sijil SSL daripada CA
5. Pemasangan Sijil SSL
6. Konfigurasi Tetapan SSL

Langkah Pemasangan Sijil SSL

5 Pemasangan Sijil SSL

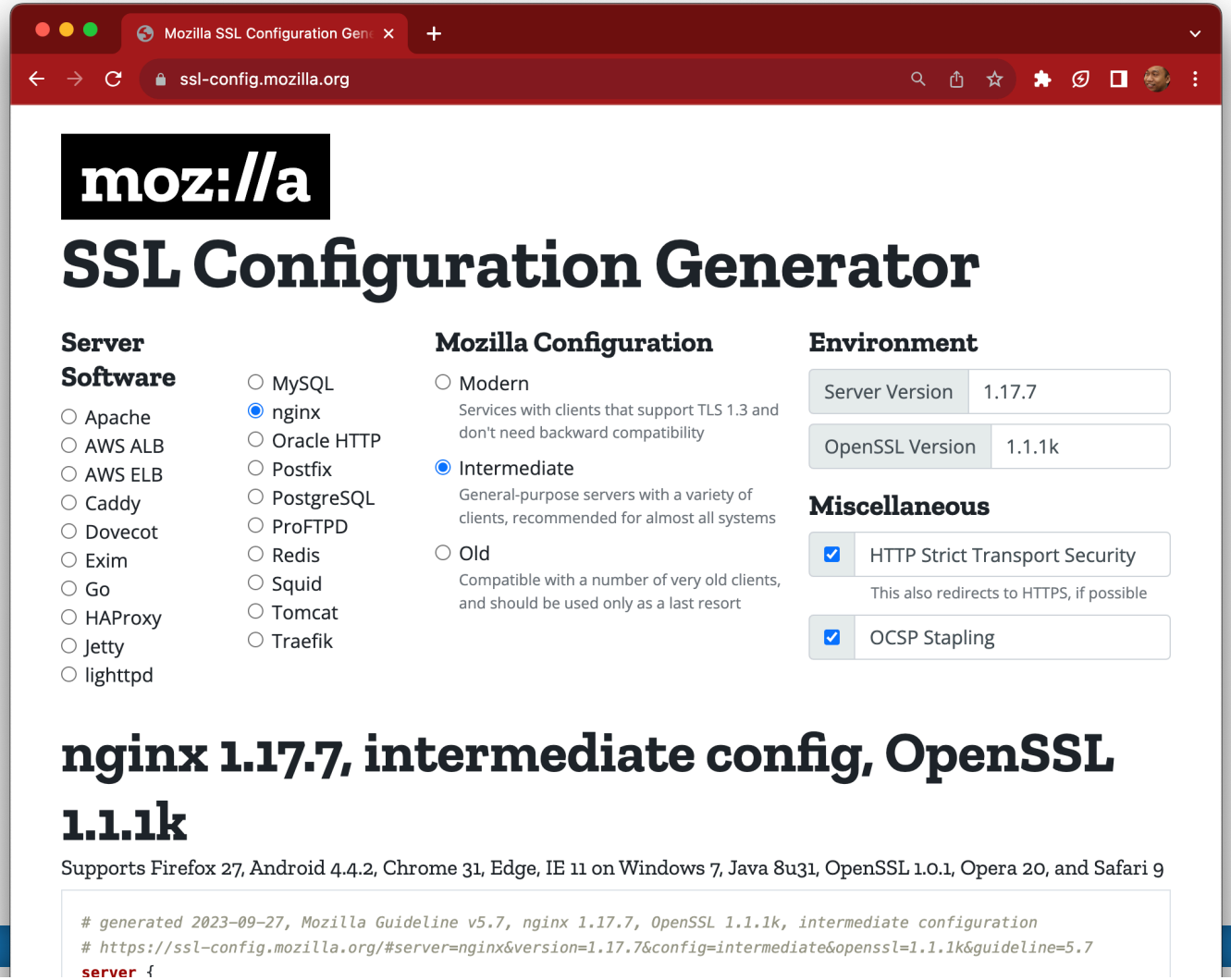
6 Konfigurasi Tetapan SSL

OpenSSL - Rujukan Konfigurasi

`https://ssl-config.mozilla.org/`

OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

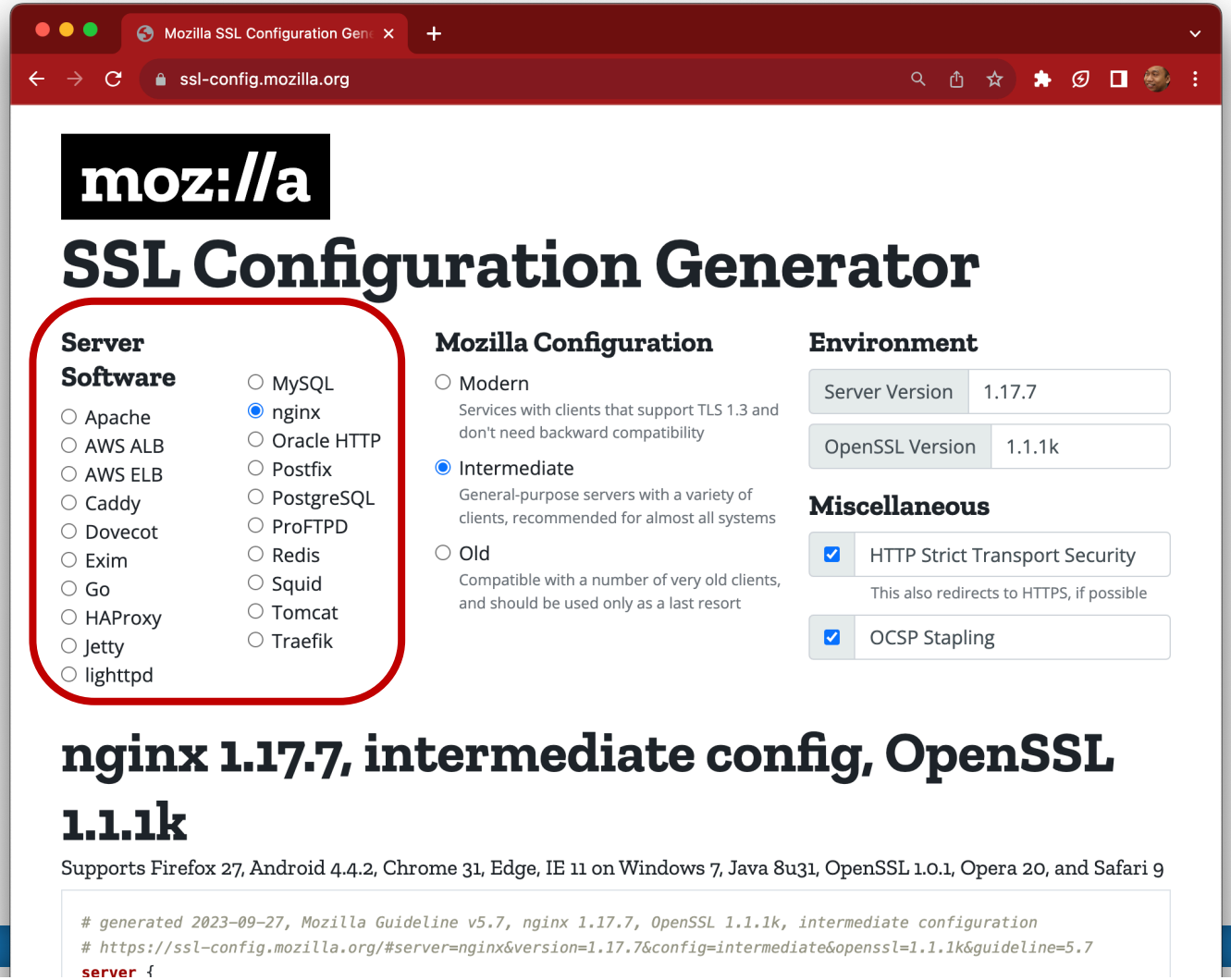


OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

1

Pilih Web Server

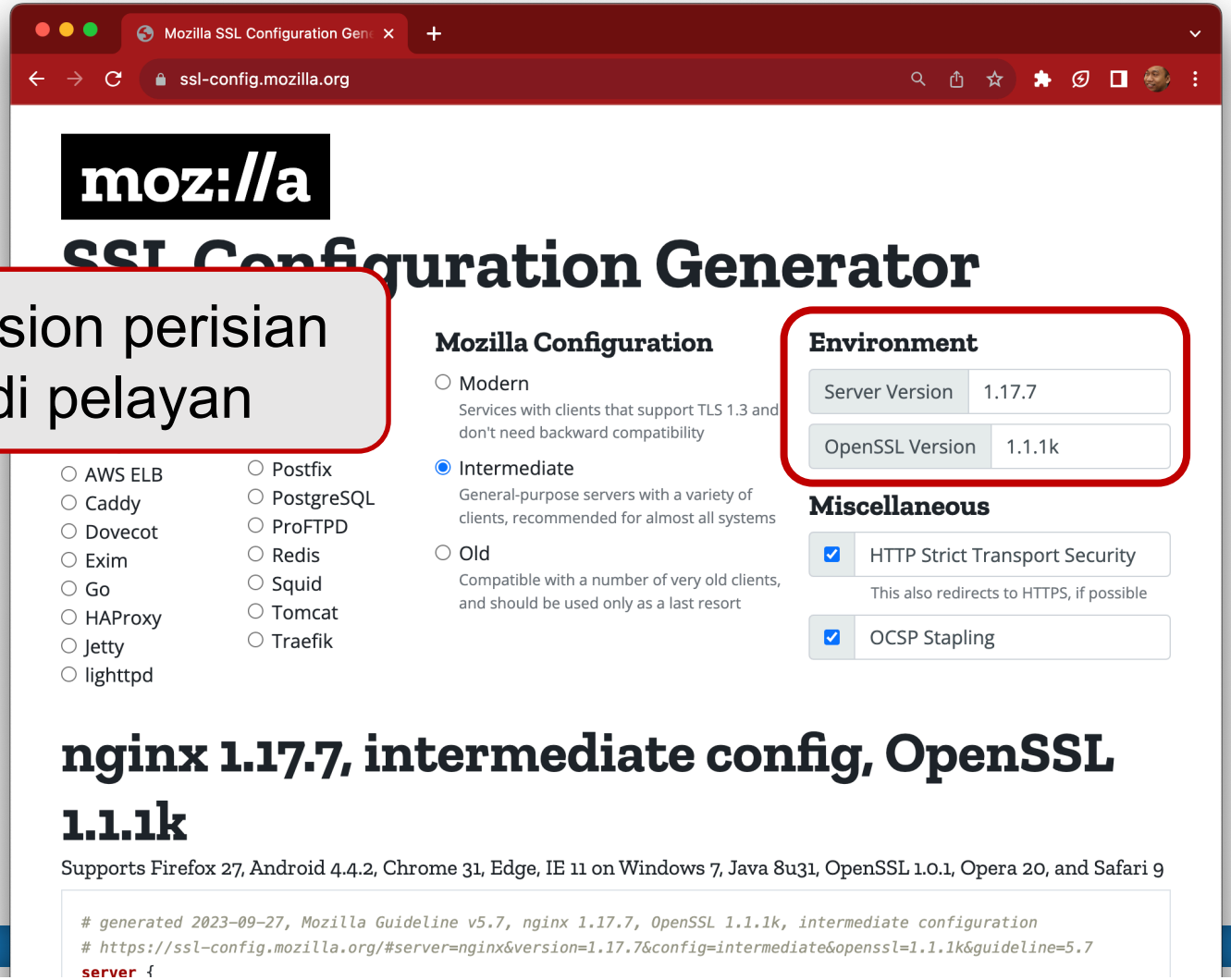


OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

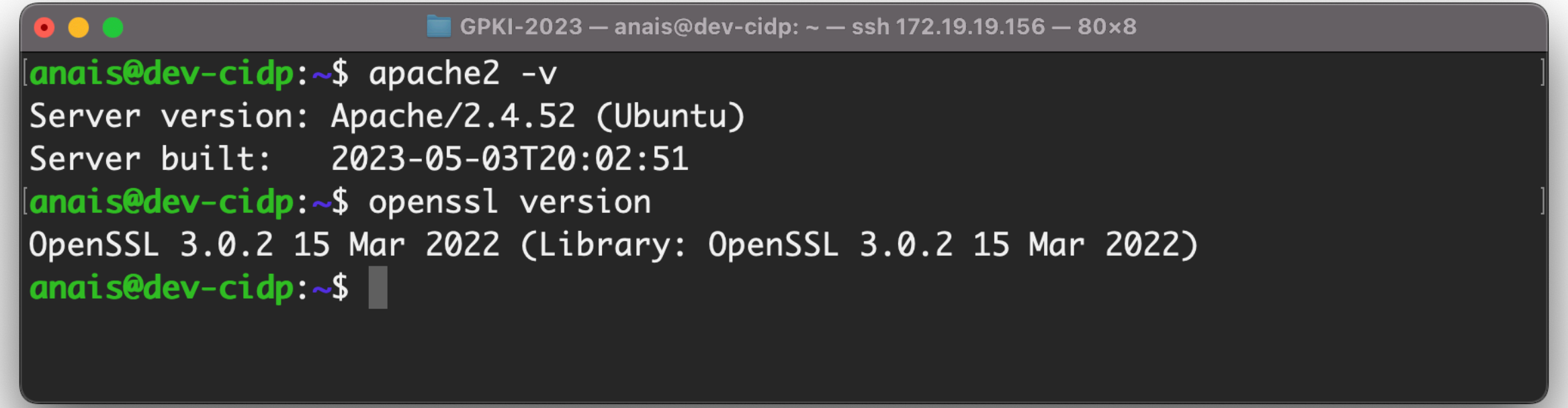
2

Masukkan version perisian terpasang di pelayan



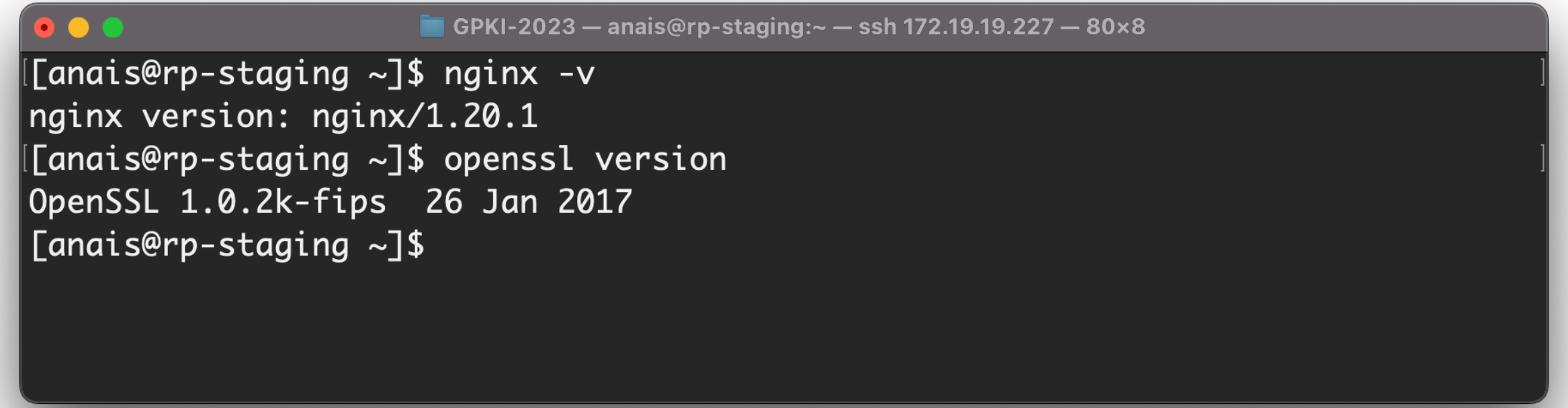
OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/



OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

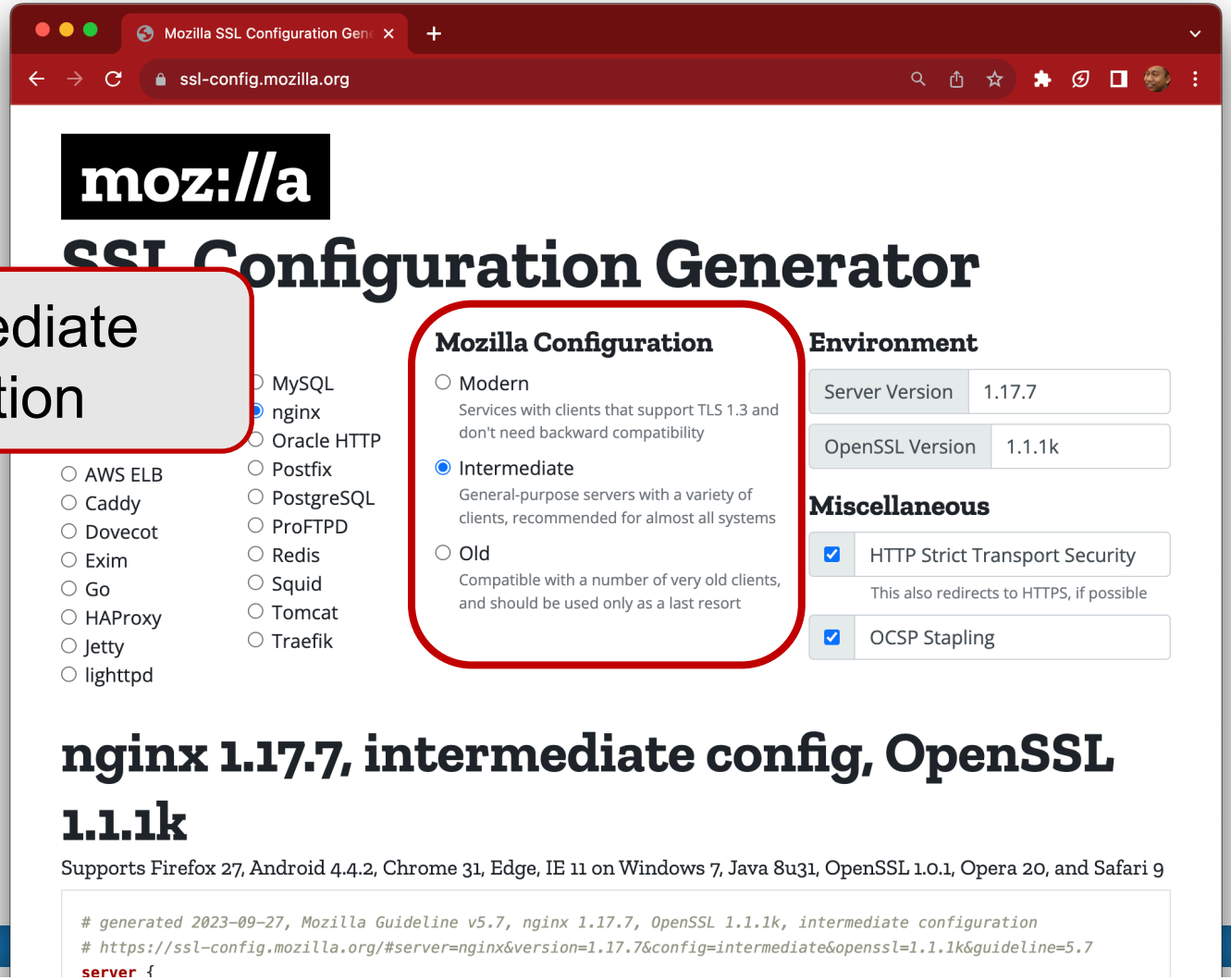


OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

3

Pilih Intermediate Configuration



OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

Intermediate Compatibility (Recommended)

For services that don't need compatibility with legacy clients such as Windows XP or old versions of OpenSSL. This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

Cipher suites (TLS 1.3):
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256

Cipher suites (TLS 1.2): ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-POLY1305

Protocols: TLS 1.2, TLS 1.3
DH parameter size: 2048

OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

Apache HTTP Server

apache 2.4.52, intermediate config, OpenSSL 3.0.2

Supports Firefox 27, Android 4.4.2, Chrome 31, Edge, IE 11 on Windows 7, Java 8u31, OpenSSL 1.0.1, Opera 20, and Safari 9

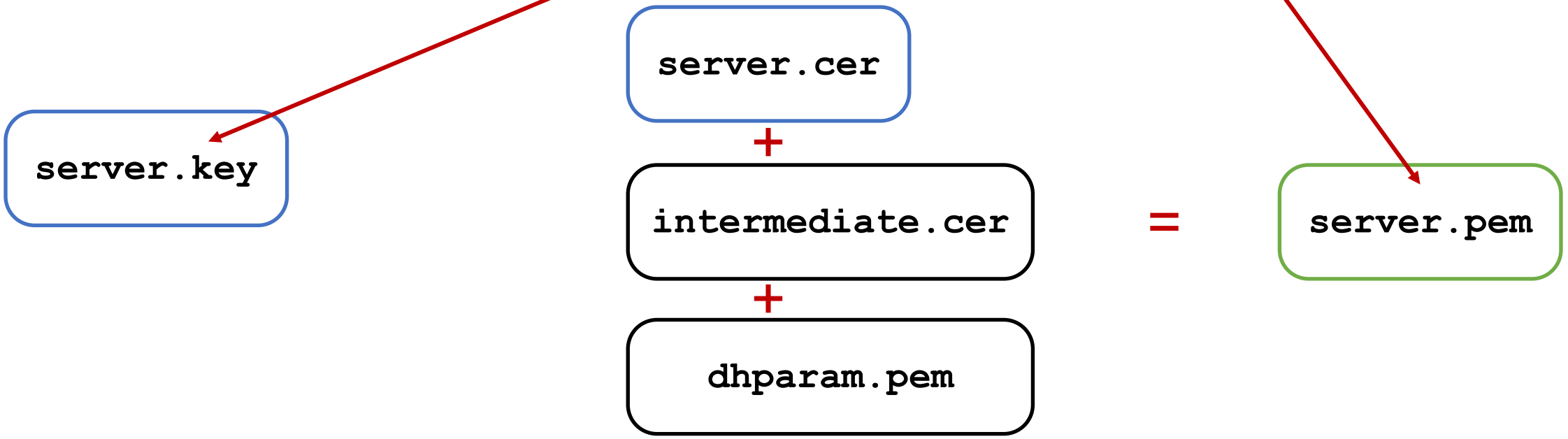
```
# generated 2023-09-29, Mozilla Guideline v5.7, Apache 2.4.52, OpenSSL 3.0.2, intermediate configuration
# https://ssl-config.mozilla.org/#server=apache&version=2.4.52&config=intermediate&openssl=3.0.2&guideline=5.7

# this configuration requires mod_ssl, mod_socache_shmcb, mod_rewrite, and mod_headers
<VirtualHost *:80>
    RewriteEngine On
    RewriteCond %{REQUEST_URI} !^/\.well\-known/acme\-challenge/
    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
</VirtualHost>

<VirtualHost *:443>
    SSLEngine on

    # curl https://ssl-config.mozilla.org/ffdhe2048.txt >> /path/to/signed_cert_and_intermediate_certs_and_dhparams
    SSLCertificateFile      /path/to/signed_cert_and_intermediate_certs_and_dhparams
    SSLCertificateKeyFile   /path/to/private_key
```

OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

Apache HTTP Server

```
SSLCertificateFile      /path/to/signed_cert_and_intermediate_certs_and_dhparams
SSLCertificateKeyFile /path/to/private_key
```



OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

Apache HTTP Server

```
SSLCertificateFile      /path/to/signed_cert_and_intermediate_certs_and_dhparams
SSLCertificateKeyFile /path/to/private_key
```

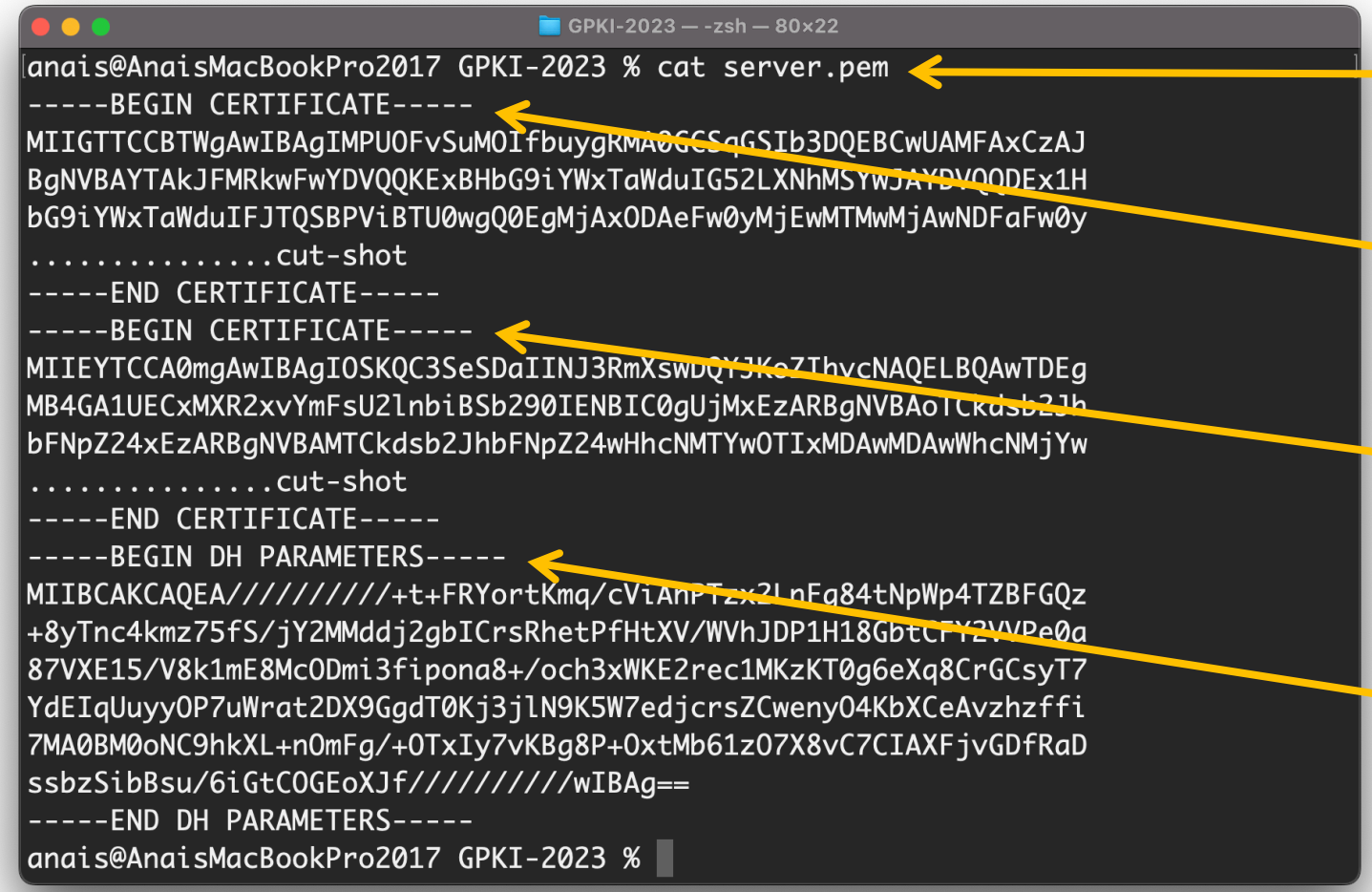
dhparam.pem

```
openssl dhparam -out dhparam.pem 2048
```

OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

Apache HTTP Server



server.pem

server.cer

intermediate.cer

dhparam.pem

How to import an SSL Certificate in Apache Server?

https://youtu.be/Hw2IZkqG5_s
https://youtu.be/zgUshTJa4sc

OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

NGINX

nginx 1.20.1, intermediate config, OpenSSL 1.0.2k-fips

Supports Firefox 27, Android 4.4.2, Chrome 31, Edge, IE 11 on Windows 7, Java 8u31, OpenSSL 1.0.1, Opera 20, and Safari 9

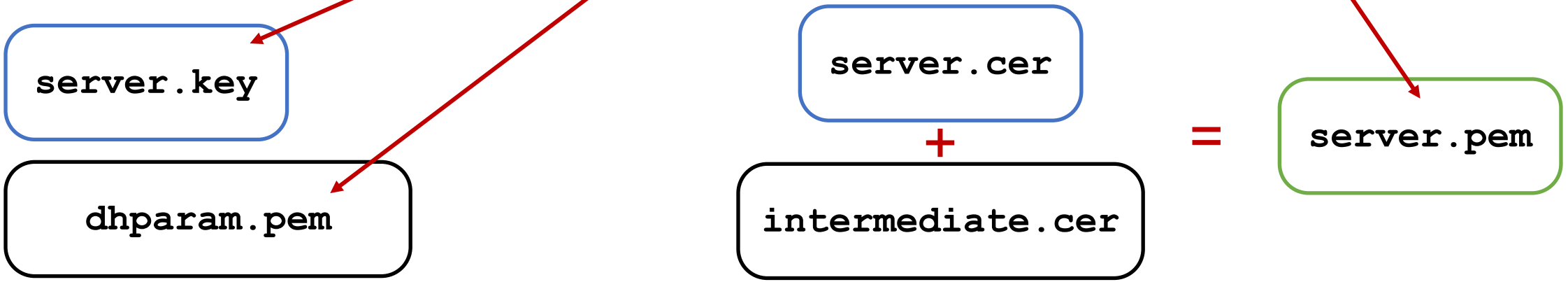
```
# generated 2023-09-29, Mozilla Guideline v5.7, nginx 1.20.1, OpenSSL 1.0.2k-fips, intermediate configuration
# https://ssl-config.mozilla.org/#server=nginx&version=1.20.1&config=intermediate&openssl=1.0.2k-fips&guideline=5.7
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    location / {
        return 301 https://$host$request_uri;
    }
}

server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;

    ssl_certificate /path/to/signed_cert_plus_intermediates;
    ssl_certificate_key /path/to/private_key;
    ssl_session_timeout 1d;
    ssl_session_cache shared:MozSSL:10m;  # about 40000 sessions

    # curl https://ssl-config.mozilla.org/ffdhe2048.txt > /path/to/dhparam
    ssl_dhparam /path/to/dhparam;
```

OpenSSL - Rujukan Konfigurasi Pemasangan SSL

https://ssl-config.mozilla.org/

NGINX

```
ssl_certificate             /path/to/signed_cert_plus_intermediates;
ssl_certificate_key         /path/to/private_key;
ssl_dhparam                 /path/to/dhparam;
ssl_trusted_certificate     /path/to/root_CA_cert_plus_intermediates;
```



How to Install an SSL/TLS Certificate on an NGINX server

https://youtu.be/RwZfDCDuyfg

OpenSSL – Useful Command

Show x509 Certificate

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

Convert PEM to DER

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

Convert DER to PEM

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

OpenSSL – Useful Command

Note: The PKCS#12 or PFX format is a binary format for storing the server certificate, intermediate certificates, and the private key in one encrypt able file. PFX files usually have extensions such as .pfx and .p12. PFX files are typically used on Windows machines to import and export certificates and private keys.

Convert PEM to PFX

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

Convert PFX to PEM

```
openssl pkcs12 -in certificatename.pfx -out certificatename.pem
```

OpenSSL – Useful Command

Note:
The PKCS#7 or P7B format is stored in Base64 ASCII format and has a file extension of .p7b or .p7c. A P7B file only contains certificates and chain certificates (Intermediate CAs), not the private key. The most common platforms that support P7B files are Microsoft Windows and Java Tomcat.

Convert PEM to P7B

```
openssl crl2pkcs7 -nocrl -certfile certificatename.pem -out
certificatename.p7b -certfile CACert.cer
```

Convert P7B to PEM

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

Java keytool (JKS)

Apache Tomcat

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
```

Java keytool (JKS)

Apache Tomcat

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" .../>
```

Java keytool (JKS)

Apache Tomcat

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="/path/to/tomcat.jks"
certificateKeystorePassword="changeit" certificateKeyAlias="tomcat"
type="RSA"/>
  </SSLHostConfig>
</Connector>
```

Java keytool (JKS) – Useful Command

Show x509 Certificate

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

Check Certificate in Java Keystore

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

Check Certificate in Java Keystore using Alias

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

Java keytool (JKS) – Useful Command

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
```

How to install SSL/TLS Certificate on an Apache Tomcat Server

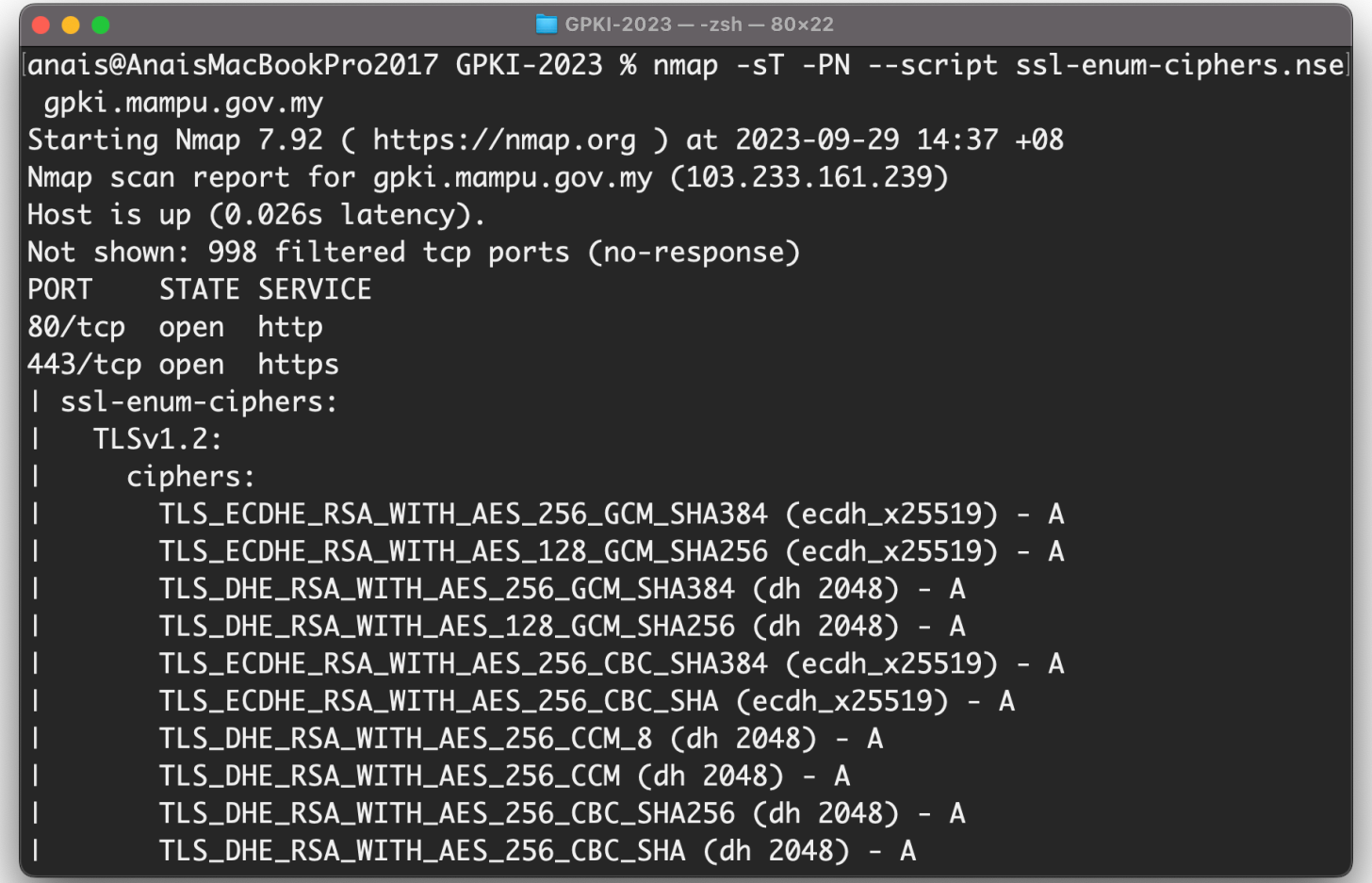
https://youtu.be/kud2Xsz98is

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

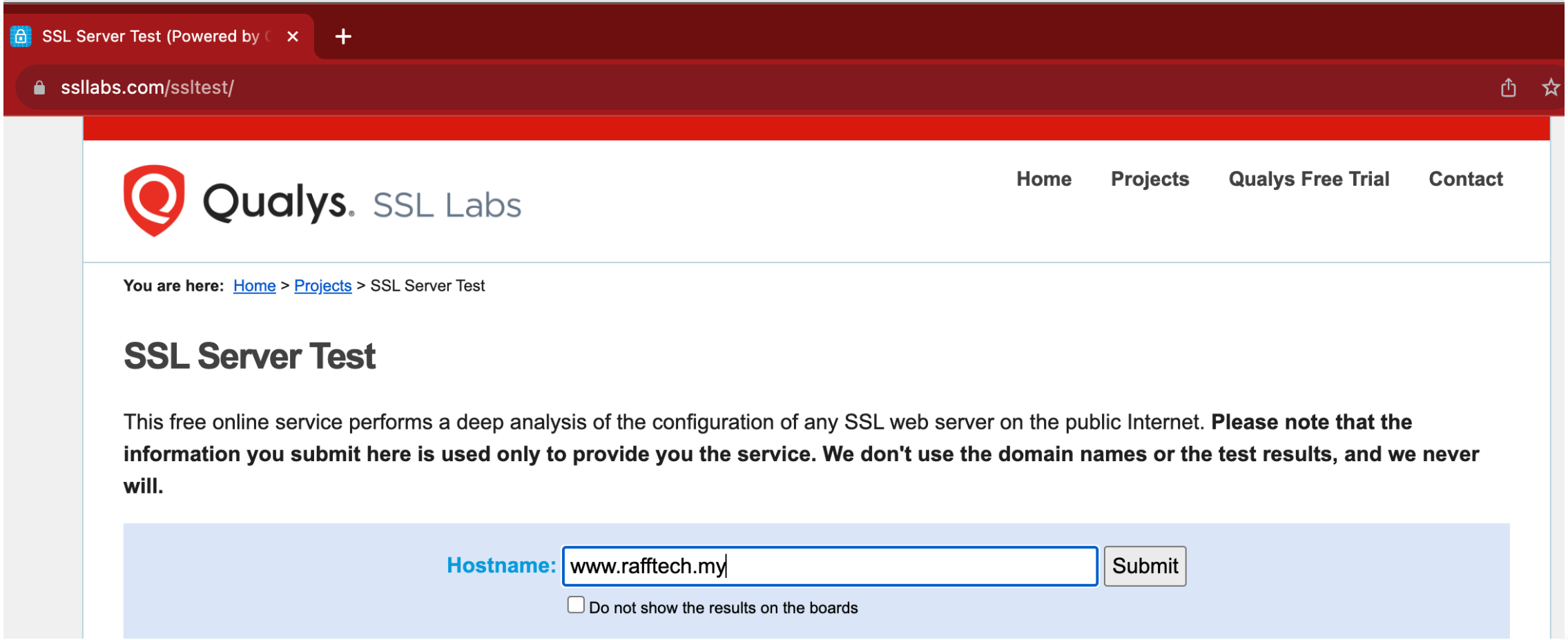
Test – Using NMap

```
nmap -sT -PN --script ssl-enum-ciphers.nse <IP Add/FQDN> [-p <port>]
```



Test – Using Qualys SSL Labs

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



Topik 5: Jom *Install* & *Test*-lah SSL/TLS

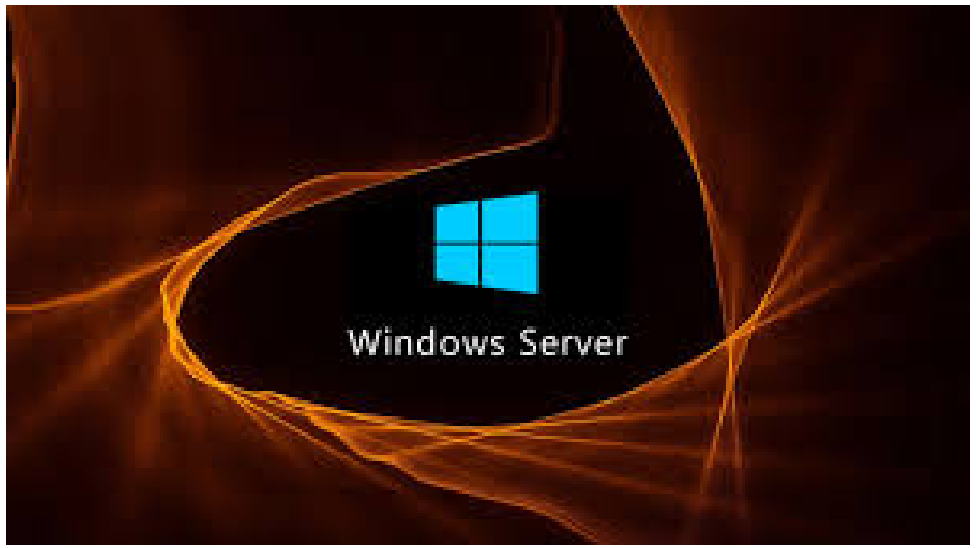
Proses Pemasangan Terbahagi Kepada 4 Bahagian

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

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

Operating System: Windows Server

Web Server:
Internet Information Services (IIS) 6/7/8



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

www.youtube.com/watch?v=W2-IphtGcZU

Bahagian 1: Muat Turun Sijil Digital

auto-notice@entrust.com ⊞ pdsbssl

Entrust Certificate Request Ready etiqa.com.my

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

ENTRUST
SECURING A WORLD IN MOTION

Dear Certificate Requester,

Your account administrator has accepted your request for a SSL Certificate reissue for:
cn=etiqa.com.my, o=Etiqa Family Takaful Berhad, l=Kuala Lumpur, c=MY

The previous certificate (Tracking ID 6281645, Serial Number 66AA185D0C16420F3F595342A2D57F1) will be revoked in 30 days after the replacement was issued.

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 pick up and install your certificate:

https://www.entrust.net/pickup/certificatePickup?ep=E1TcR21j5o56G139vFe4-3tJY1FfH4slld0yqlhXyVOJnYZXoHfCM2XqAdlp0HuMx-EcNrRLpiwUHLyYBTjhHEPdRVN54uJ3cbCT5N5Gaa8kdWdOFhnGDF31XMLgbeCAuU99bWC7-mhkPQPM5A8SCJ8ex0QVhhxaolFv3RBt2eCjSyHyCBh6GCHX19SdYbFY0-Rq8RvkXmY-Xr3GkpsVlX3JtN8Mez-cGPEDavtC0Os

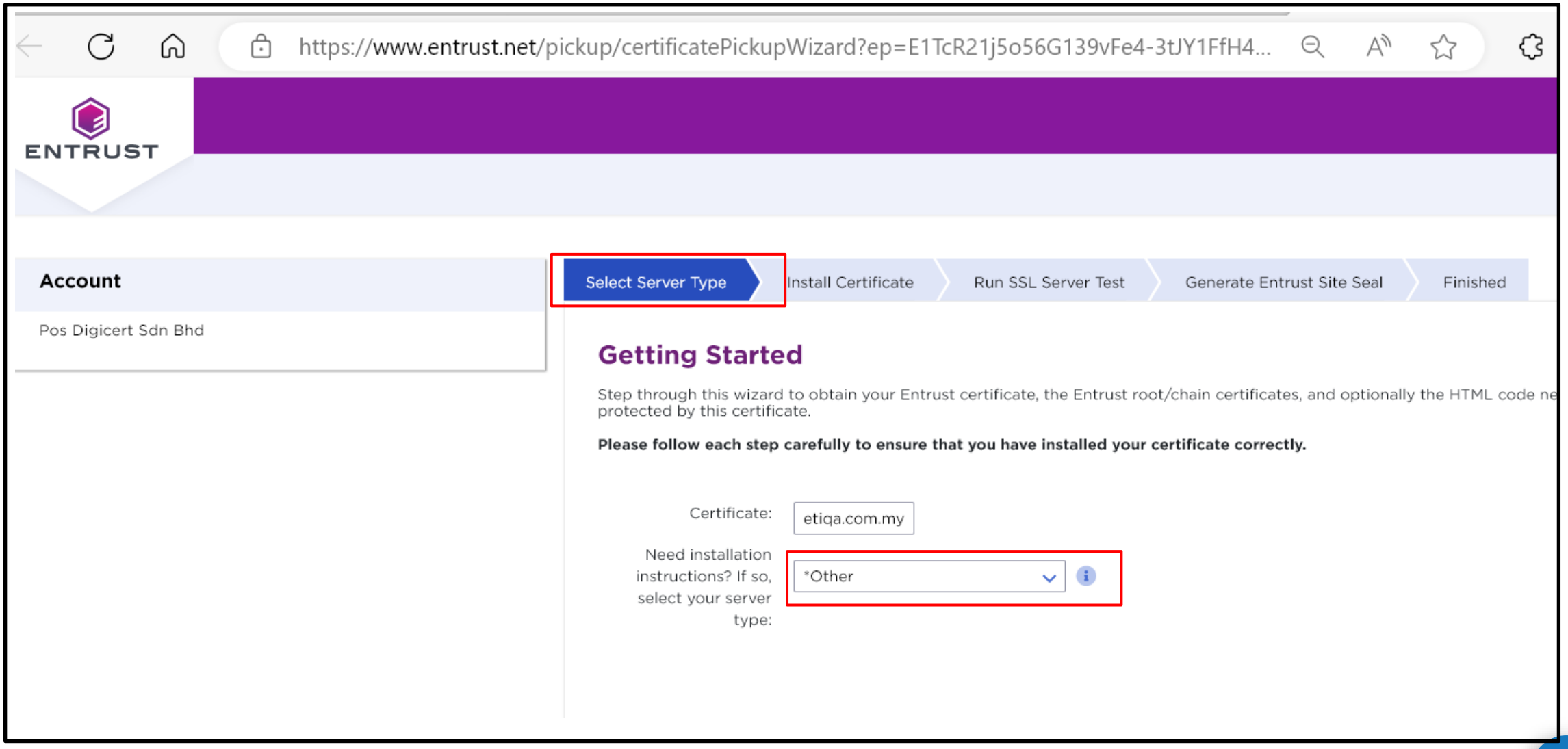
Entrust Certificate Services is ready to assist:

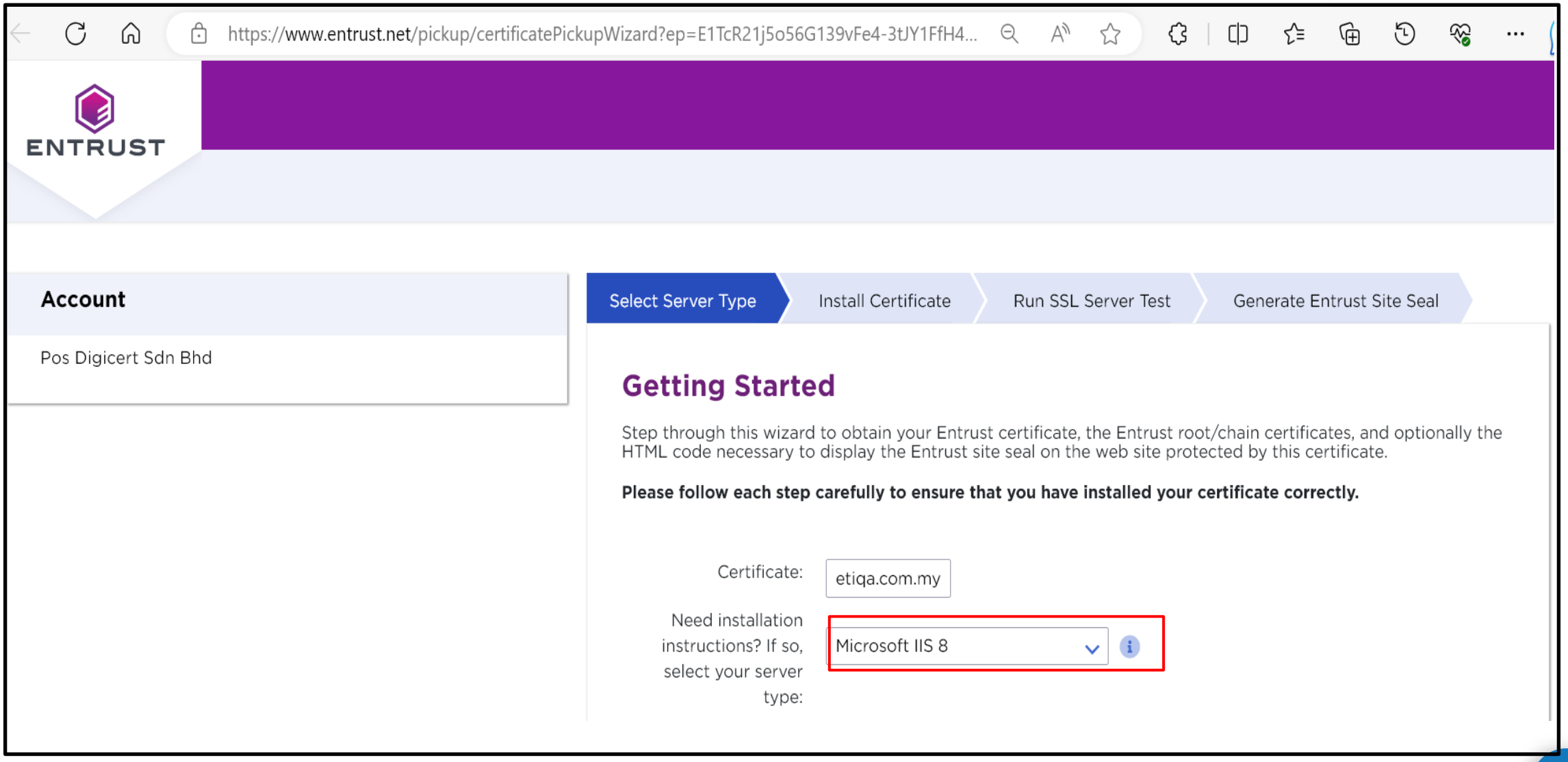
Product and Technical Support: ECS.Support@Entrust.com

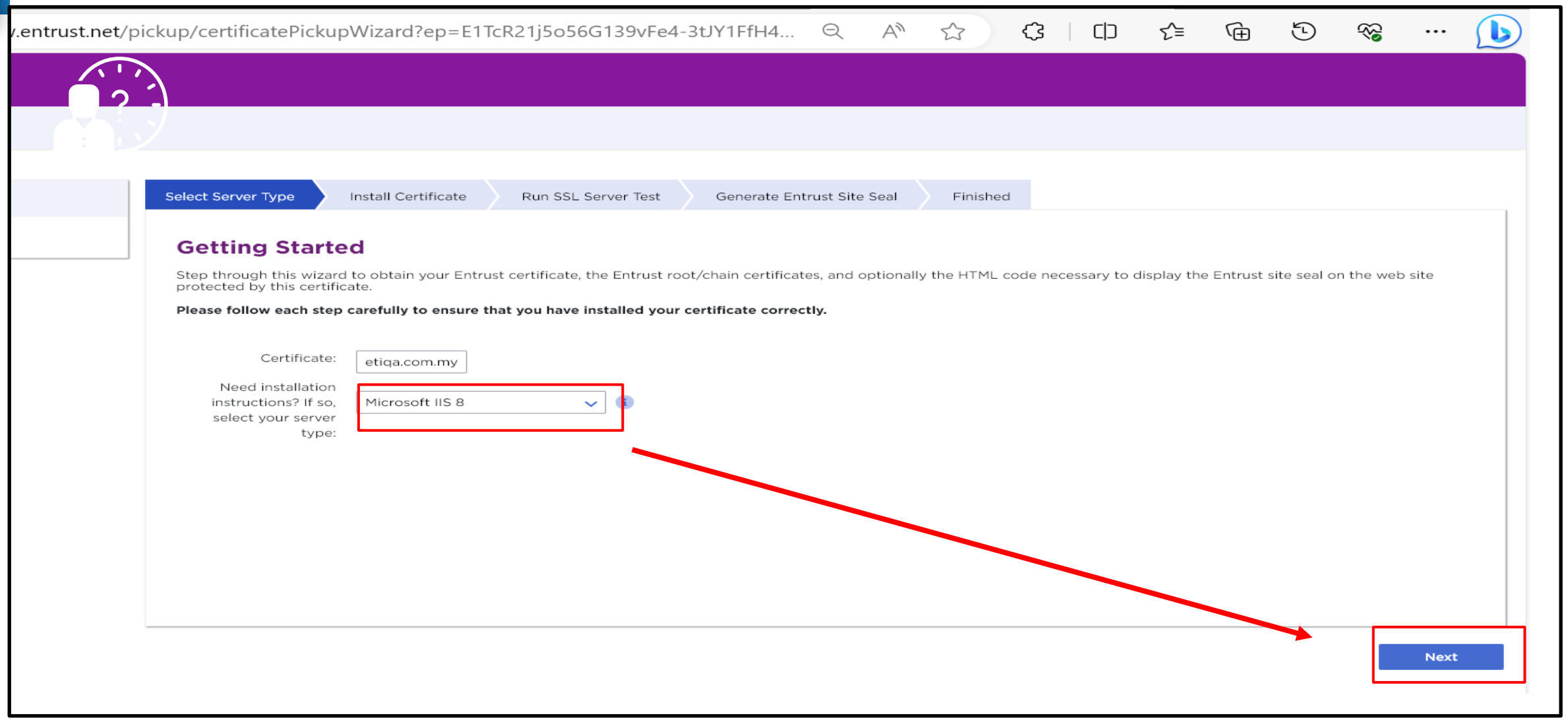
Muat Turun Sijil Digital Pelayan

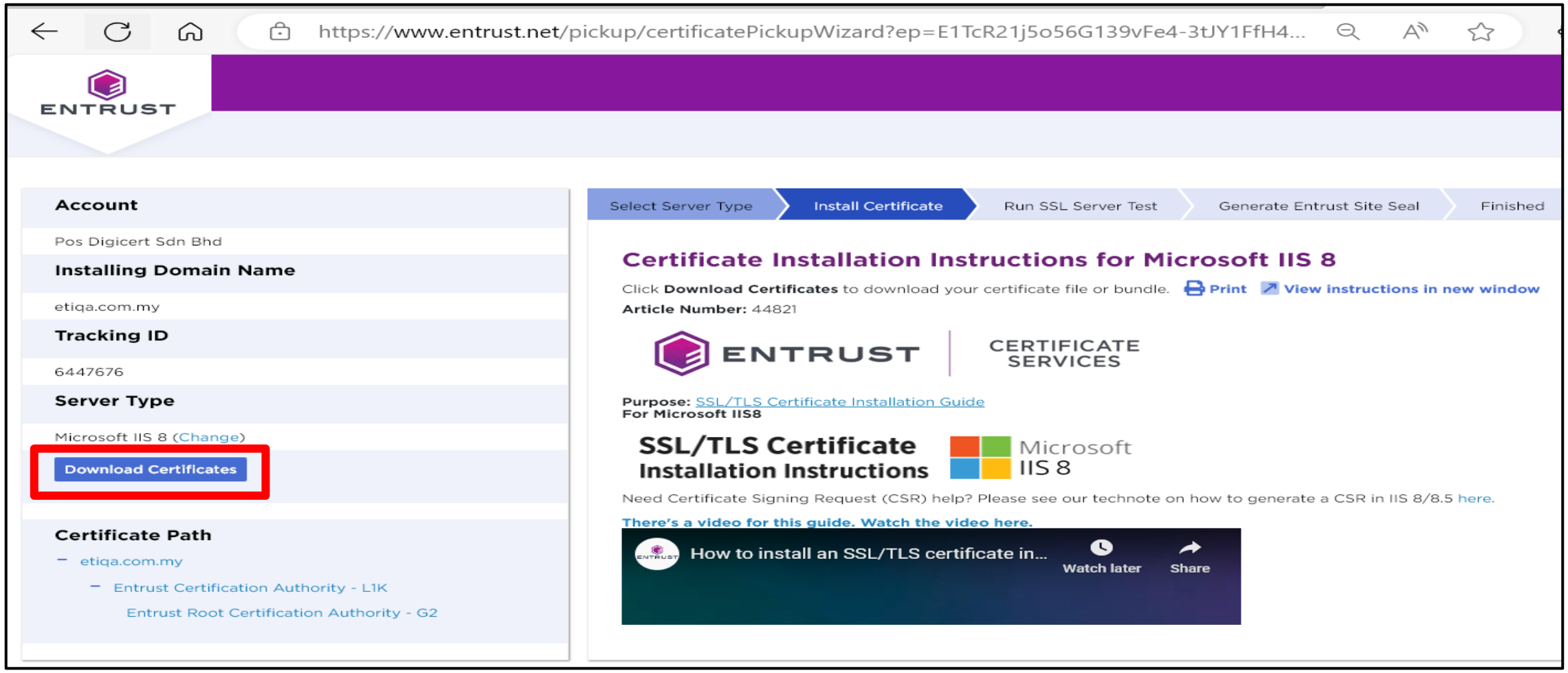
Contoh Pautan Muat Turun Sijil Digital Pelayan

https://www.entrust.net/pickup/certificatePickup?ep=E1TcR21j5o56G139vFe4-3tJY1FfH4sIld0yqlhXyVOJnYZXoHfCM2XqAdlp0HuMx-EcNrRLpiwUHLyYBTjhHEPdRVN54uJ3cbCT5N5Gaa8kdWdOFhnGDF31XMLgbeCAuU99bWC7-mhkPQPM5A8SCJ8ex0QVhhxaoIFv3RBt2eCjSyHyCBh6GCHX19SdYbFY0-Rq8RvkXmY-Xr3GkpsVlX3JtN8Mez-cGPEDavtC0Os

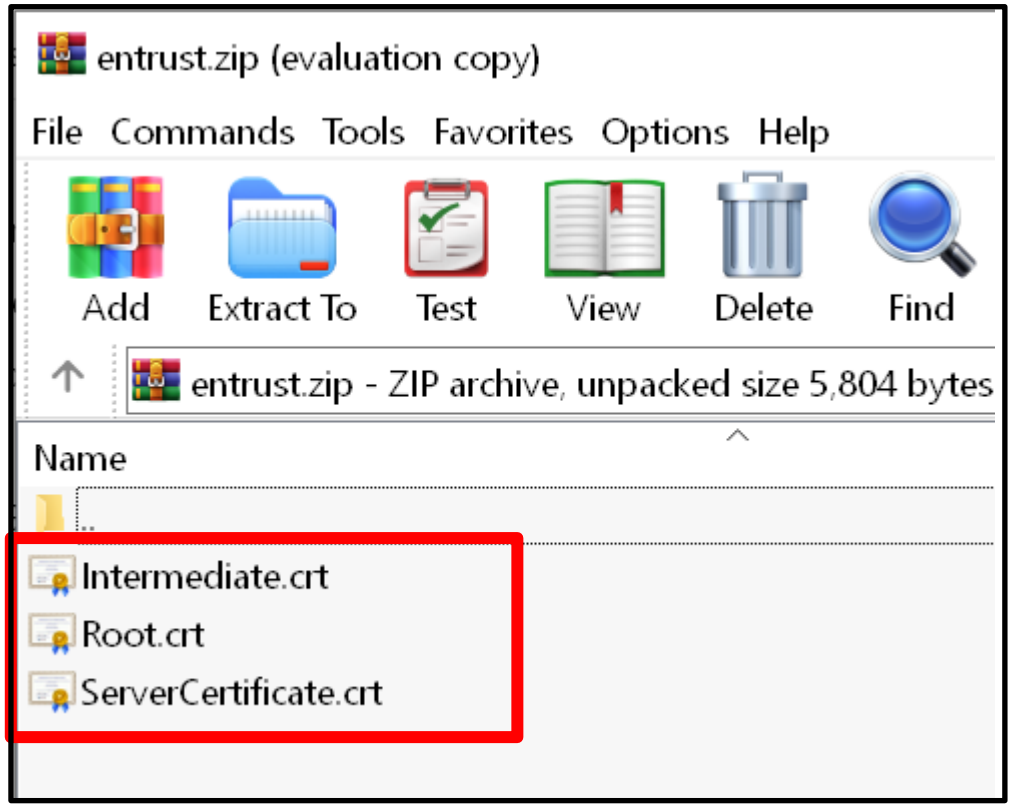

https://www.entrust.net/pickup/certificatePickupWizard?ep=E1TcR21j5o56G139vFe4-3tJY1FfH4...
ENTRUST
Account
Pos Digicert Sdn Bhd
Select Server Type
Install Certificate
Run SSL Server Test
Generate Entrust Site Seal
Finished
Getting Started
Step through this wizard to obtain your Entrust certificate, the Entrust root/chain certificates, and optionally the HTML code ne
protected by this certificate.
Please follow each step carefully to ensure that you have installed your certificate correctly.
Certificate:
etiqa.com.my
Need installation instructions? If so, select your server type:
*Other


https://www.entrust.net/pickup/certificatePickupWizard?ep=E1TcR21j5o56G139vFe4-3tJY1FfH4...
ENTRUST
Account
Pos Digicert Sdn Bhd
Select Server Type
Install Certificate
Run SSL Server Test
Generate Entrust Site Seal
Getting Started
Step through this wizard to obtain your Entrust certificate, the Entrust root/chain certificates, and optionally the HTML code necessary to display the Entrust site seal on the web site protected by this certificate.
Please follow each step carefully to ensure that you have installed your certificate correctly.
Certificate:
etiqa.com.my
Need installation instructions? If so, select your server type:
Microsoft IIS 8


.entrust.net/pickup/certificatePickupWizard?ep=E1TcR21j5o56G139vFe4-3tJY1FfH4...
Select Server Type
Install Certificate
Run SSL Server Test
Generate Entrust Site Seal
Finished
Getting Started
Step through this wizard to obtain your Entrust certificate, the Entrust root/chain certificates, and optionally the HTML code necessary to display the Entrust site seal on the web site protected by this certificate.
Please follow each step carefully to ensure that you have installed your certificate correctly.
Certificate:
etiqa.com.my
Need installation instructions? If so, select your server type:
Microsoft IIS 8
Next


https://www.entrust.net/pickup/certificatePickupWizard?ep=E1TcR21j5o56G139vFe4-3tJY1FfH4...
ENTRUST
Account
Pos Digicert Sdn Bhd
Installing Domain Name
etiqa.com.my
Tracking ID
6447676
Server Type
Microsoft IIS 8 (Change)
Download Certificates
Certificate Path
etiqa.com.my
Entrust Certification Authority - L1K
Entrust Root Certification Authority - G2
Select Server Type
Install Certificate
Run SSL Server Test
Generate Entrust Site Seal
Finished
Certificate Installation Instructions for Microsoft IIS 8
Click Download Certificates to download your certificate file or bundle.
Print
View instructions in new window
Article Number: 44821
ENTRUST
CERTIFICATE SERVICES
Purpose: SSL/TLS Certificate Installation Guide
For Microsoft IIS8
SSL/TLS Certificate Installation Instructions
Microsoft IIS 8
Need Certificate Signing Request (CSR) help? Please see our technote on how to generate a CSR in IIS 8/8.5 here.
There's a video for this guide. Watch the video here.
How to install an SSL/TLS certificate in...
Watch later
Share

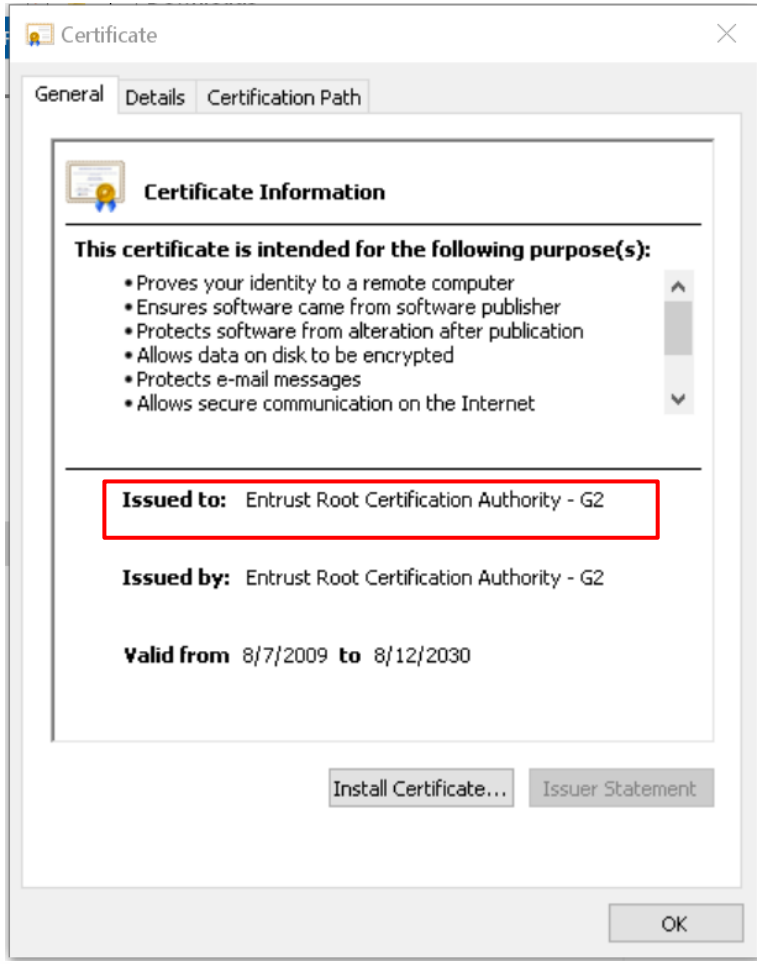

entrust.zip
Type: WinRAR ZIP archive


entrust.zip (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
entrust.zip - ZIP archive, unpacked size 5,804 bytes
Name
..
Intermediate.crt
Root.crt
ServerCertificate.crt

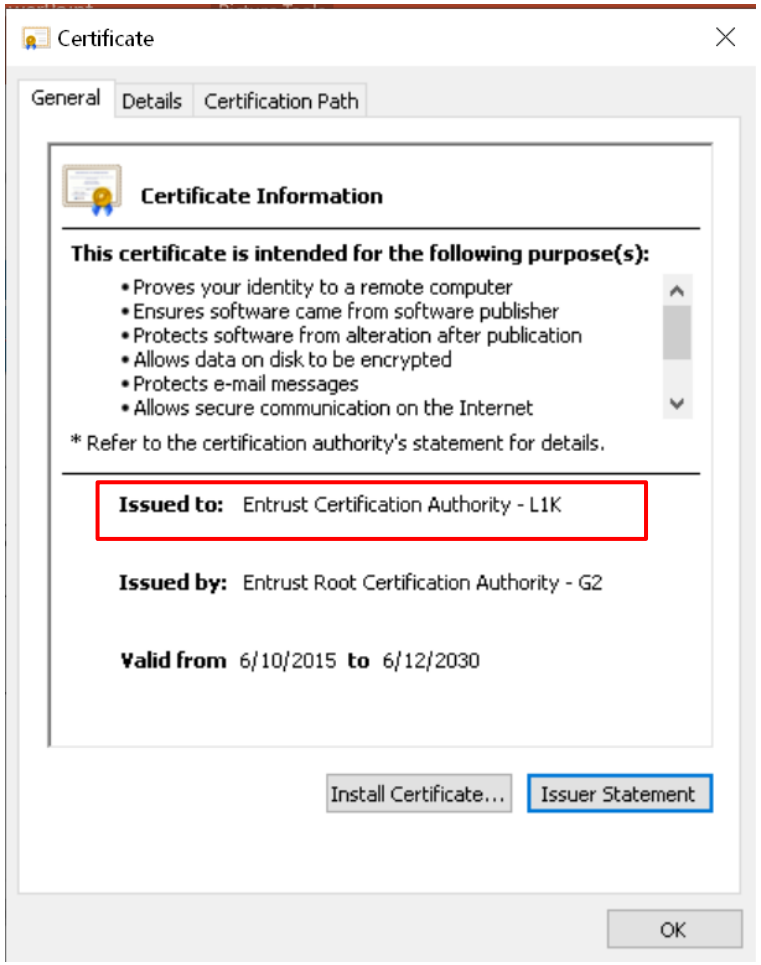
3 Jenis Fail Bagi Windows Server IIS 6/7/8

2 Jenis Fail Bagi Apache

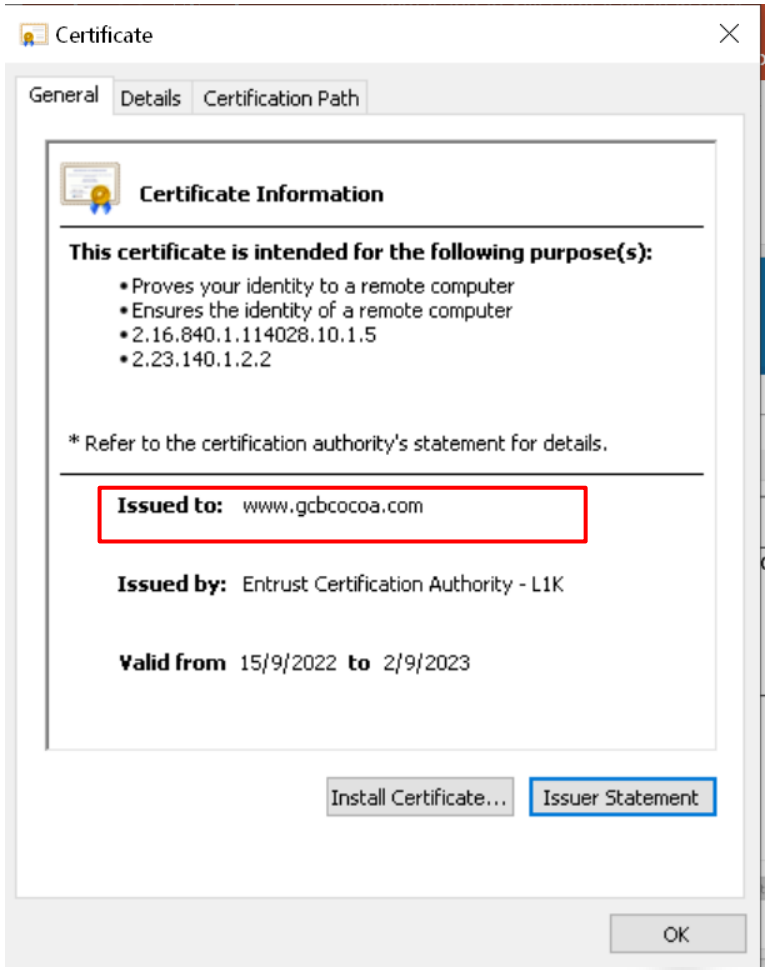
Root



Intermediate

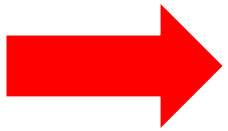


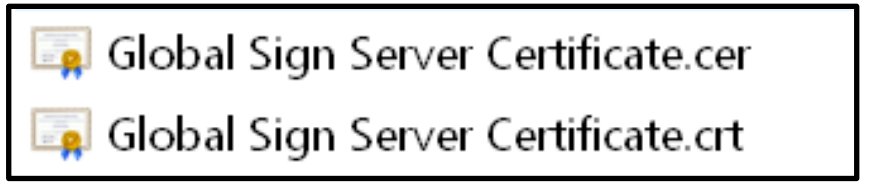
Server Certificate




-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIMDulMwwAAAABR03eFMA0GCSqGSIb3DQEBCwUAMIG+MQsw
CQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2Vl
IHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMDkg
RW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTIwMAYDVQQD
EylFbnRydXN0IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBHMjAeFw0x
NTEwMDUxOTEzNTZaFw0zMDEyMDUxOTQzNTZaMIG6MQswCQYDVQQGEwJVUzEWMBQG
A1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2VlIHd3dy5lbnRydXN0Lm5l
dC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMTIgRW50cnVzdCwgSW5jLiAt
IGZvciBhdXRob3JpemVkIHVzZSBvbmx5MS4wLAYDVQQDEyVFbnRydXN0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IC0gTDFLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2j+W0E25L0Tn2zlem1DuXKVh2kFnUwmqAJqOV38pa9vH4SEkqjrQ
jUcj0u1yFvCRIdJdt7hLqIOPt5EyaM/OJZMssn2XyP7BtBe6CZ4DkJN7fEmDImiK
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/OJZMssn2XyP7BtBe6CZ4DkJN7fEmDImiK
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 Or GeoTrust
SSL Certificate

```
-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIMDulMwwAAAABR03eFMA0GCSqGSIb3DQEBCwUAMIG+MQsw
CQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2Vl
IHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMDkg
RW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTIwMAYDVQQD
EylFbnRydXN0IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBHMjAeFw0x
NTEwMDUxOTEzNTZaFw0zMDEyMDUxOTQzNTZaMIG6MQswCQYDVQQGEwJVUzEWMBQG
A1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2VlIHd3dy5lbnRydXN0Lm5l
dC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMTIgRW50cnVzdCwgSW5jLiAt
IGZvciBhdXRob3JpemVkIHVzZSBvbmx5MS4wLAYDVQQDEyVFbnRydXN0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IC0gTDFLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2j+W0E25L0Tn2zlem1DuXKVh2kFnUwmqAJqOV38pa9vH4SEkqjrQ
jUcj0u1yFvCRIdJdt7hLqIOPt5EyaM/OJZMssn2XyP7BtBe6CZ4DkJN7fEmDImiK
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-----
```





Bahagian 2: Pasang Sijil Digital Pelayan

Pautan Panduan Pemasangan Bagi Jenis IIS 6/7/8

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

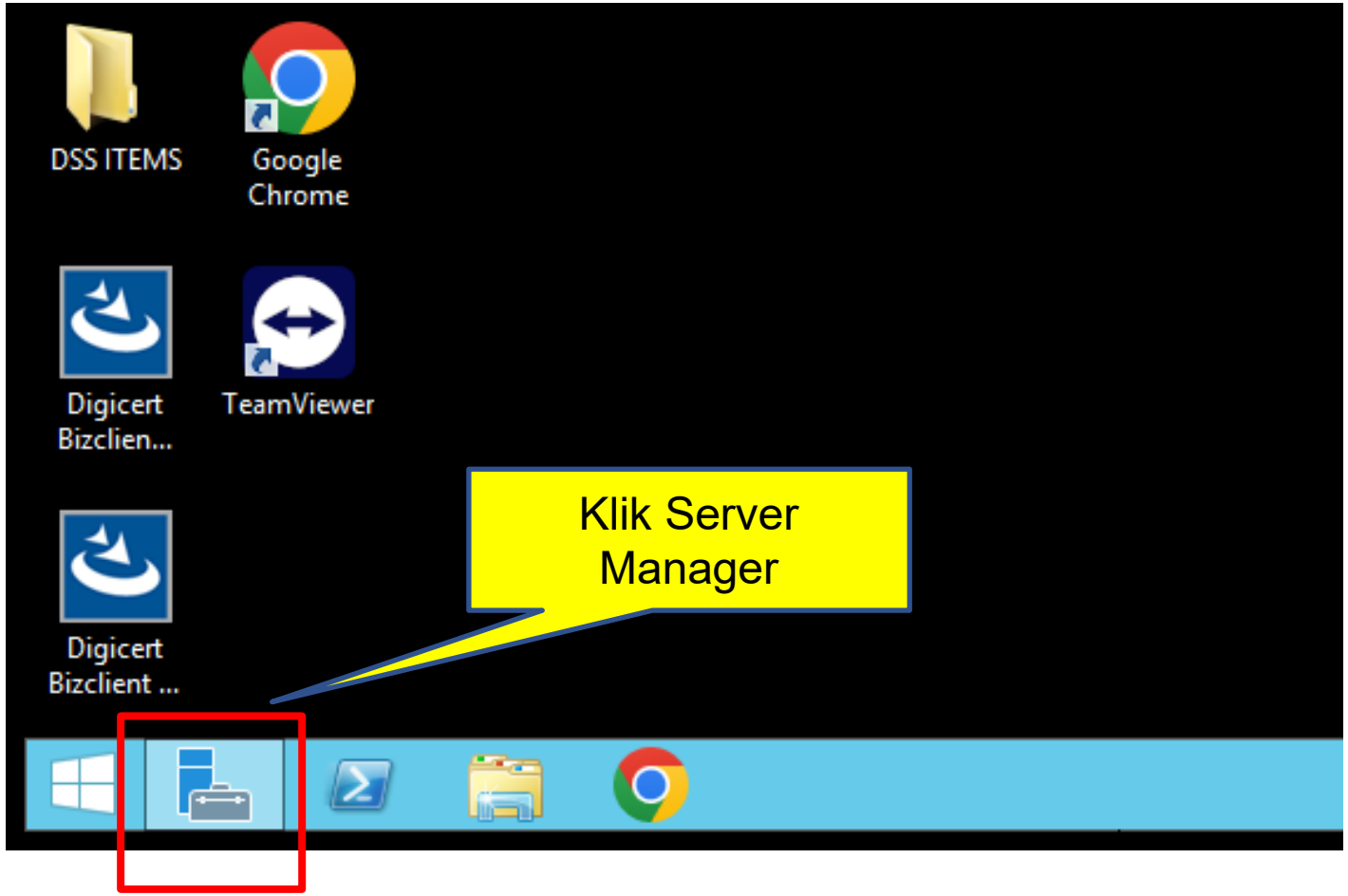
How to install an SSL/TLS certificate in Microsoft IIS8

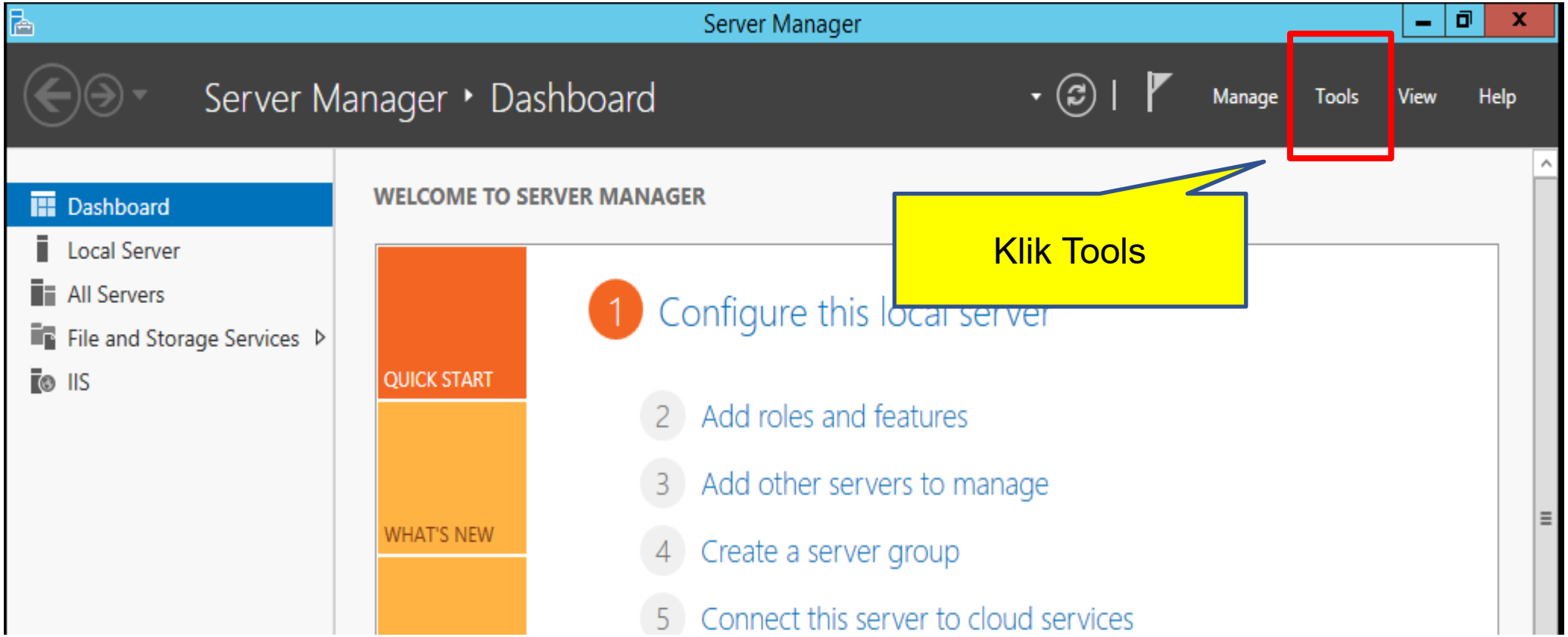
https://youtu.be/nWk1MTFfqWk

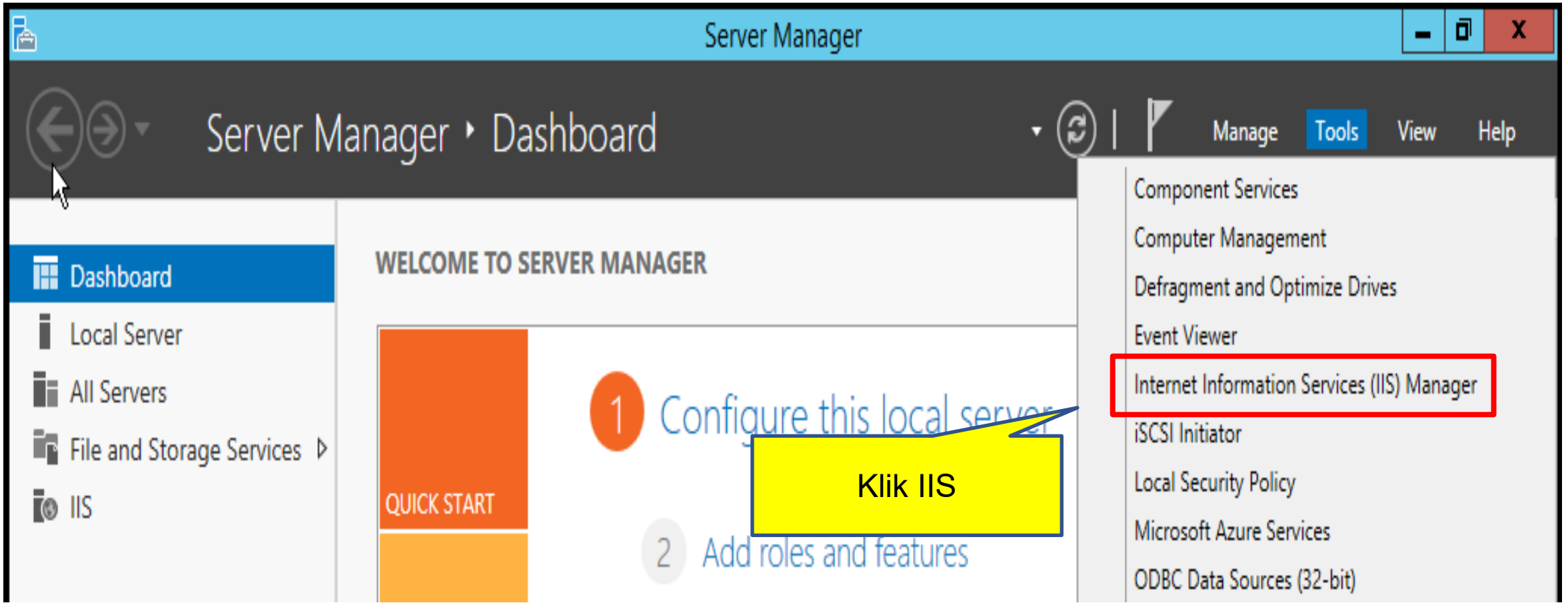
Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web

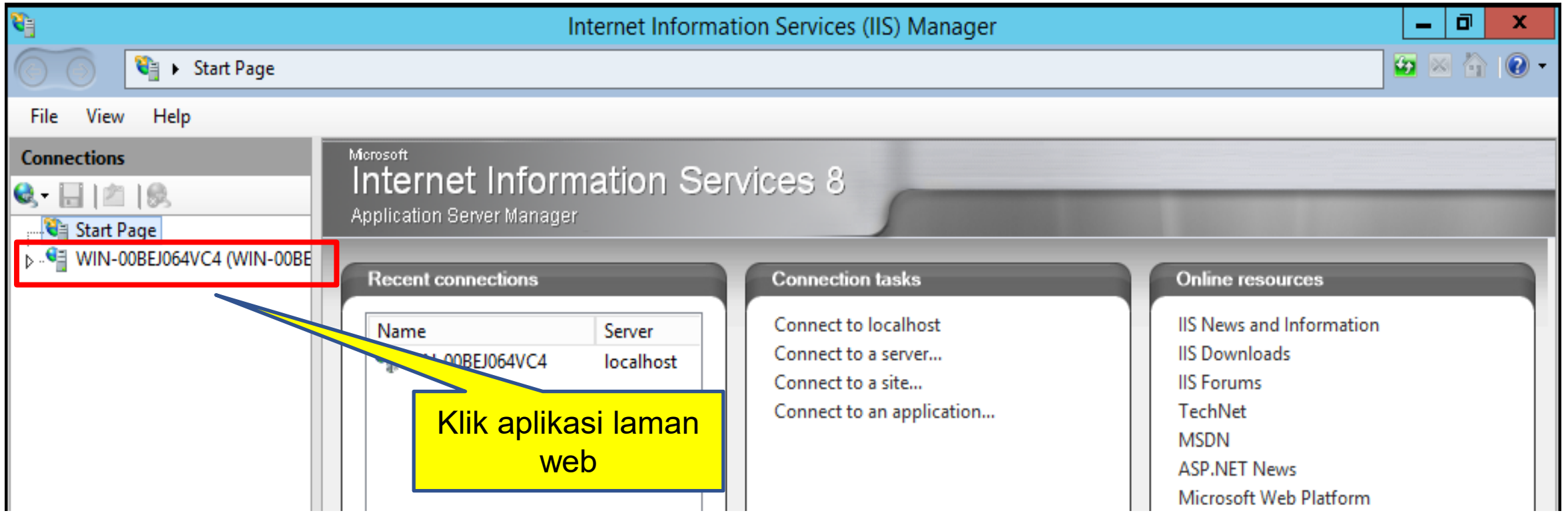
Bagaimanakah Cara Untuk *Bind* Sijil Digital Pelayan Dengan Laman Web?

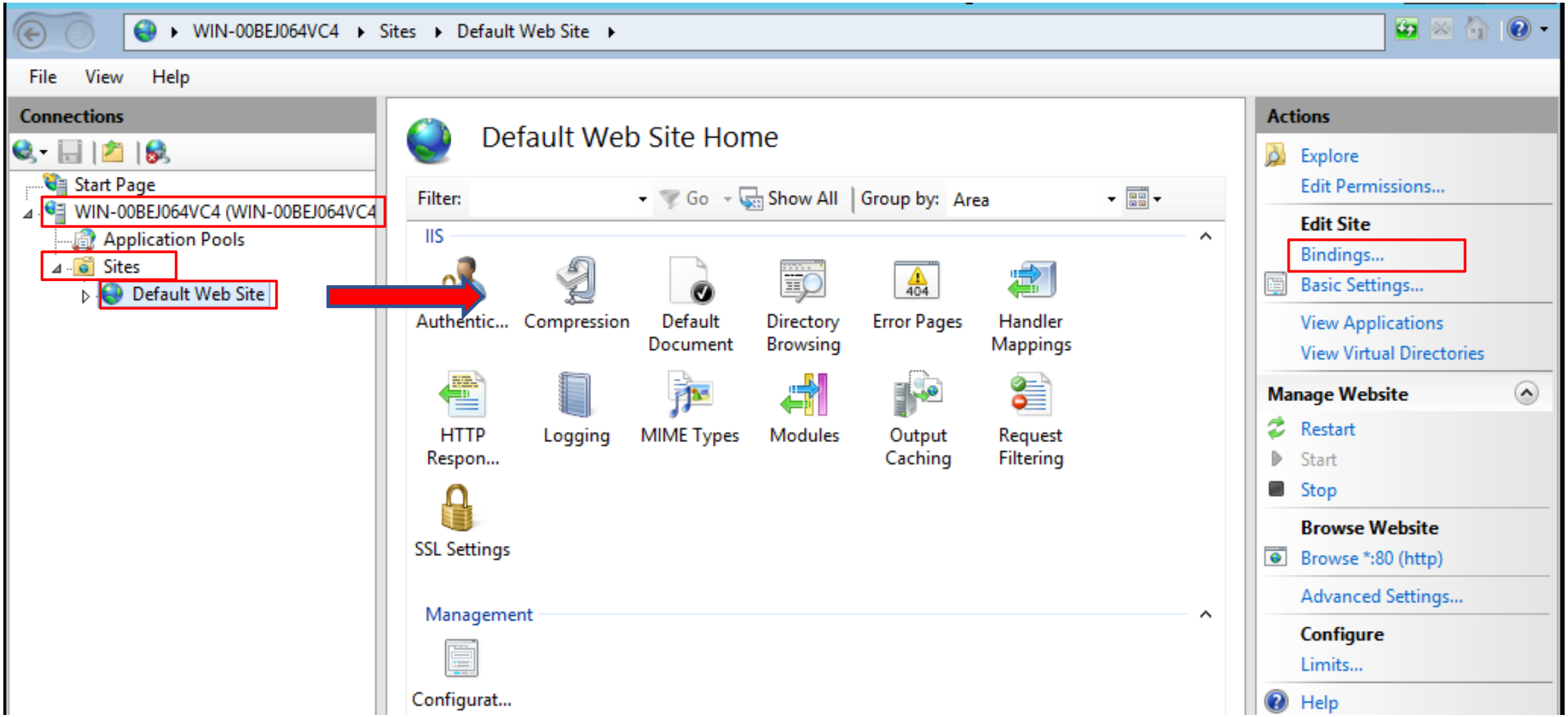
Bahagian 3: *Bind* Sijil Digital Pelayan Dengan Laman Web

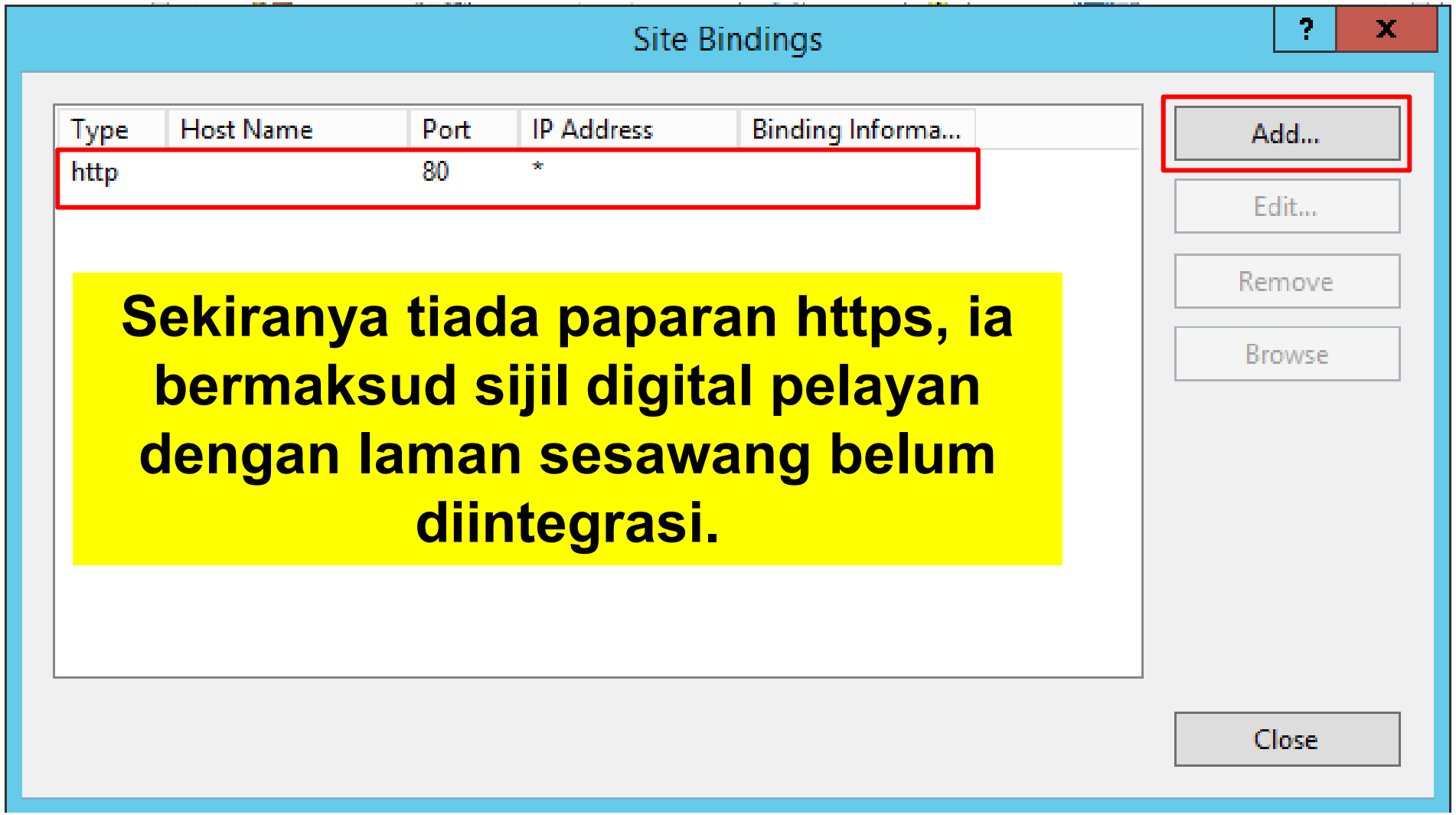



Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Klik Tools

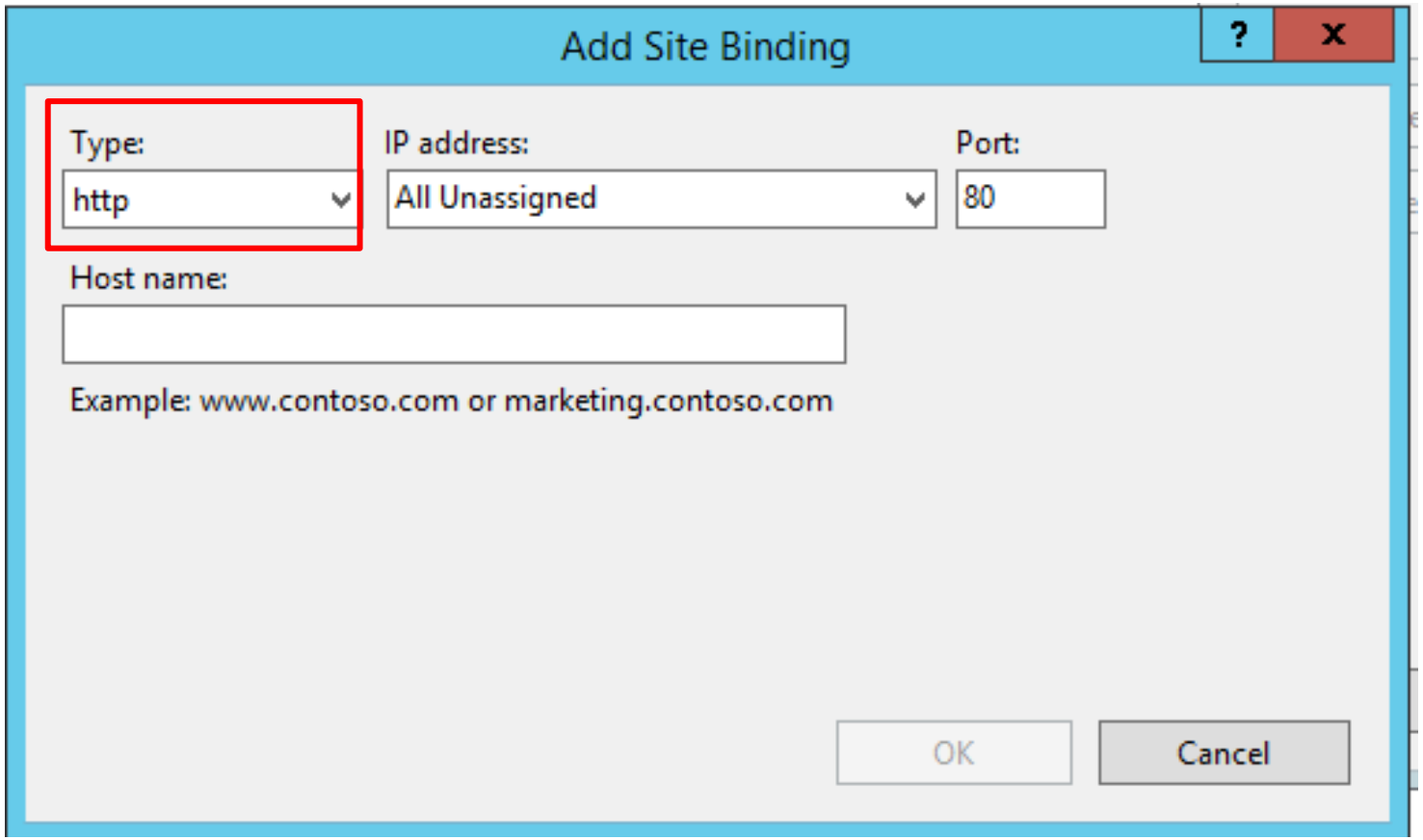

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
1 Configure this local server
2 Add roles and features
Component Services
Computer Management
Defragment and Optimize Drives
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
Klik IIS

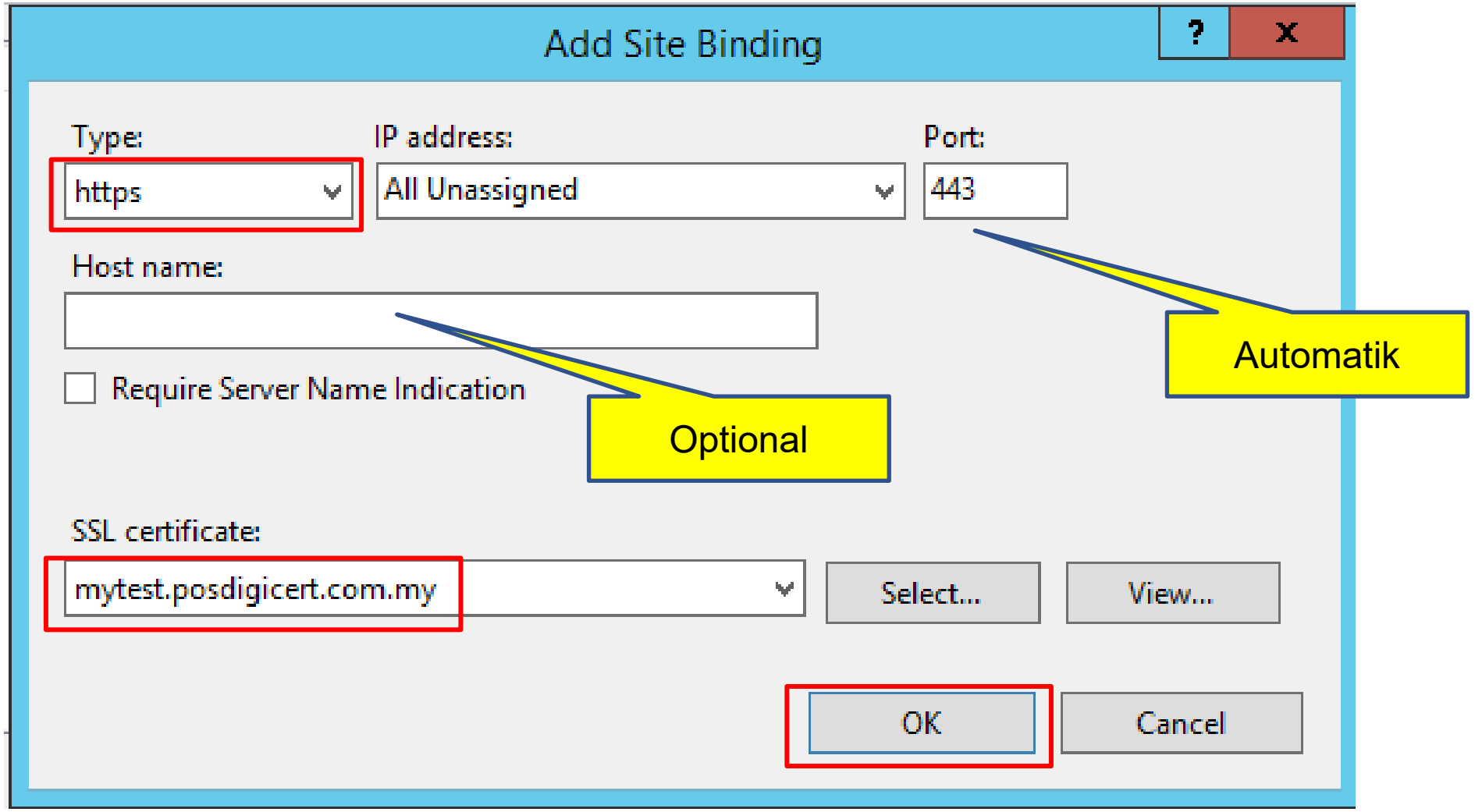

Internet Information Services (IIS) Manager
Start Page
File View Help
Connections
Start Page
WIN-00BEJ064VC4 (WIN-00BE
Microsoft
Internet Information Services 8
Application Server Manager
Recent connections
Name
Server
00BEJ064VC4
localhost
Klik aplikasi laman web
Connection tasks
Connect to localhost
Connect to a server...
Connect to a site...
Connect to an application...
Online resources
IIS News and Information
IIS Downloads
IIS Forums
TechNet
MSDN
ASP.NET News
Microsoft Web Platform

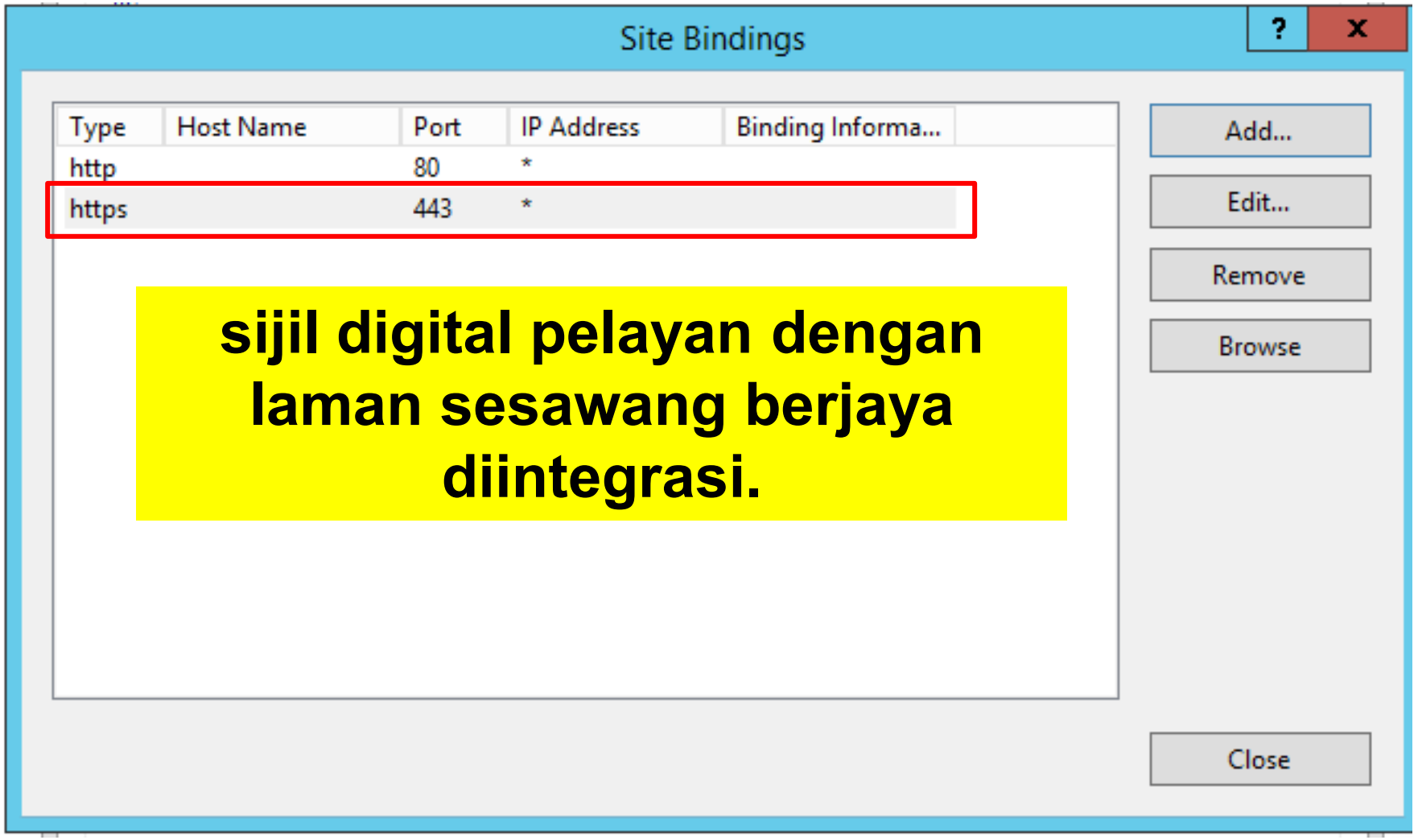

WIN-00BEJ064VC4 ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
WIN-00BEJ064VC4 (WIN-00BEJ064VC4
Application Pools
Sites
Default Web Site
Default Web Site Home
Filter:
Go
Show All
Group by: Area
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Handler Mappings
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

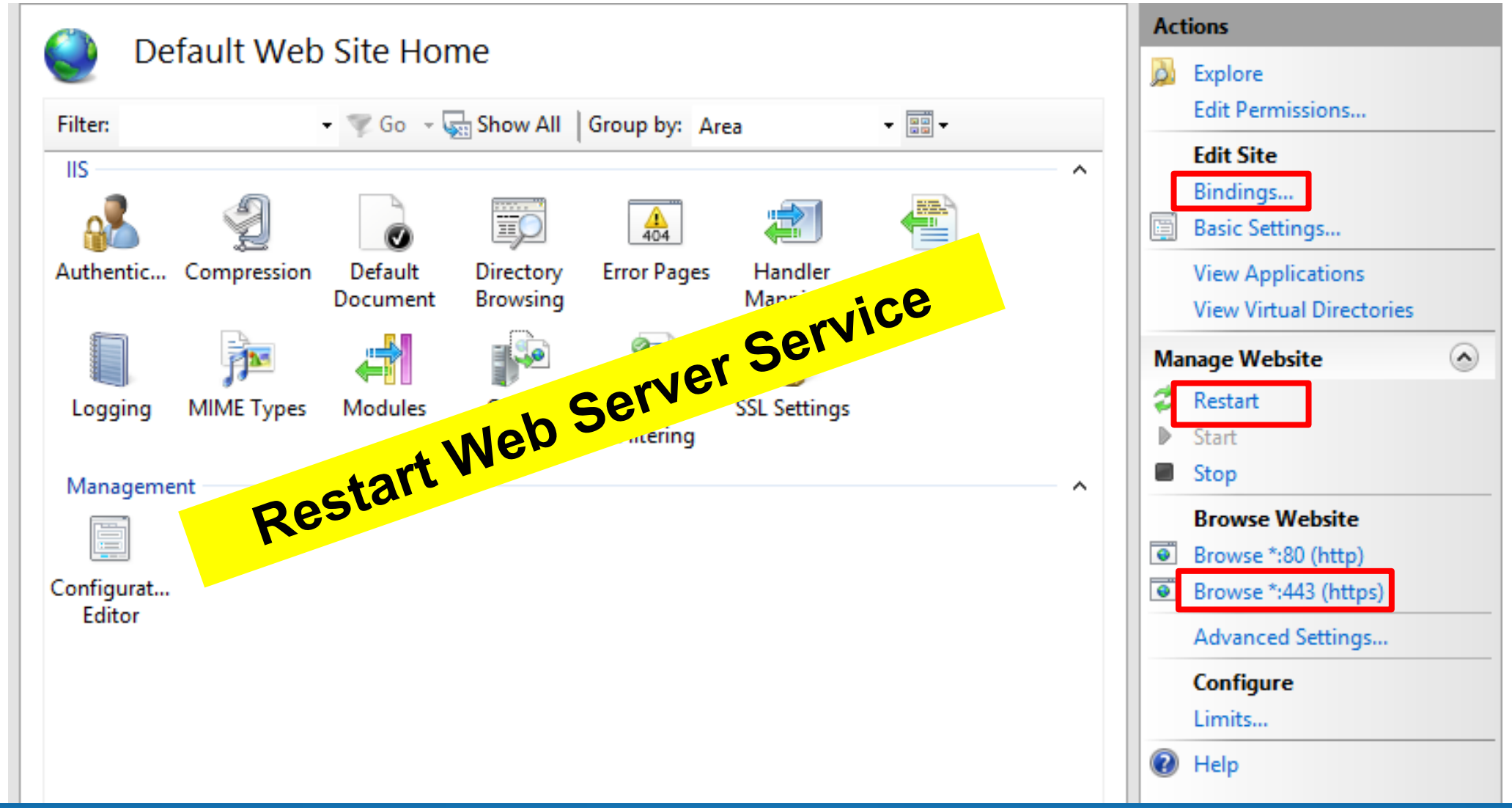


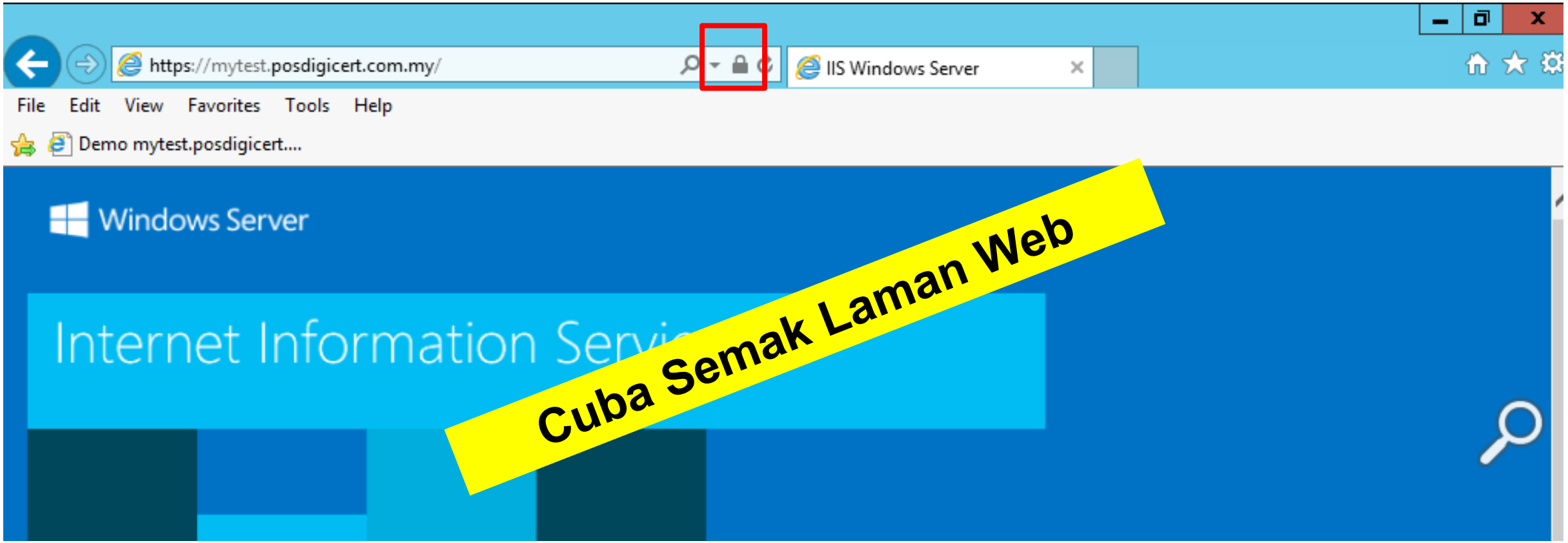
Sekiranya tiada paparan https, ia bermaksud sijil digital pelayan dengan laman sesawang belum diintegrasi.

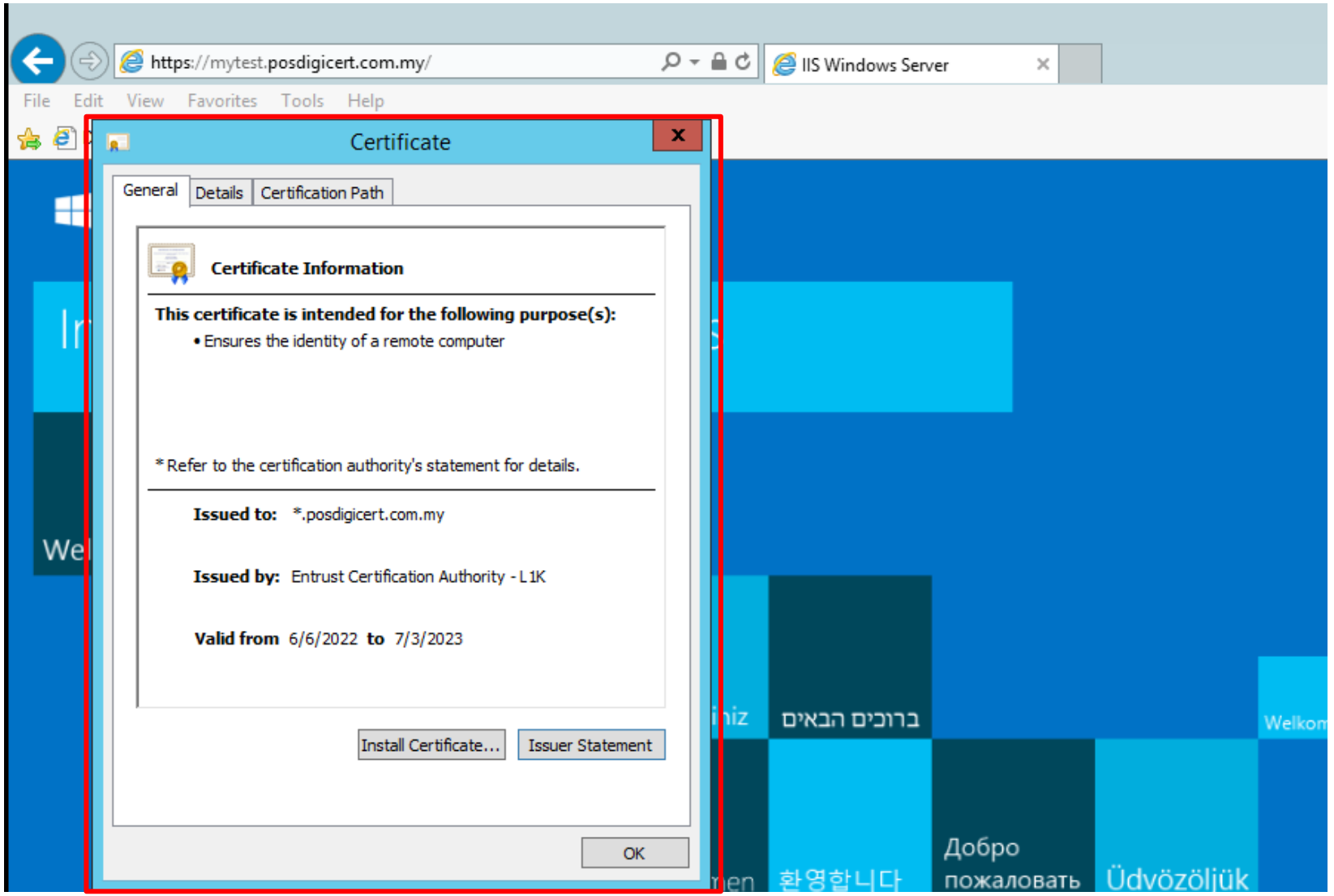

Add Site Binding
?
X
Type:
http
IP address:
All Unassigned
Port:
80
Host name:
Example: www.contoso.com or marketing.contoso.com
OK
Cancel

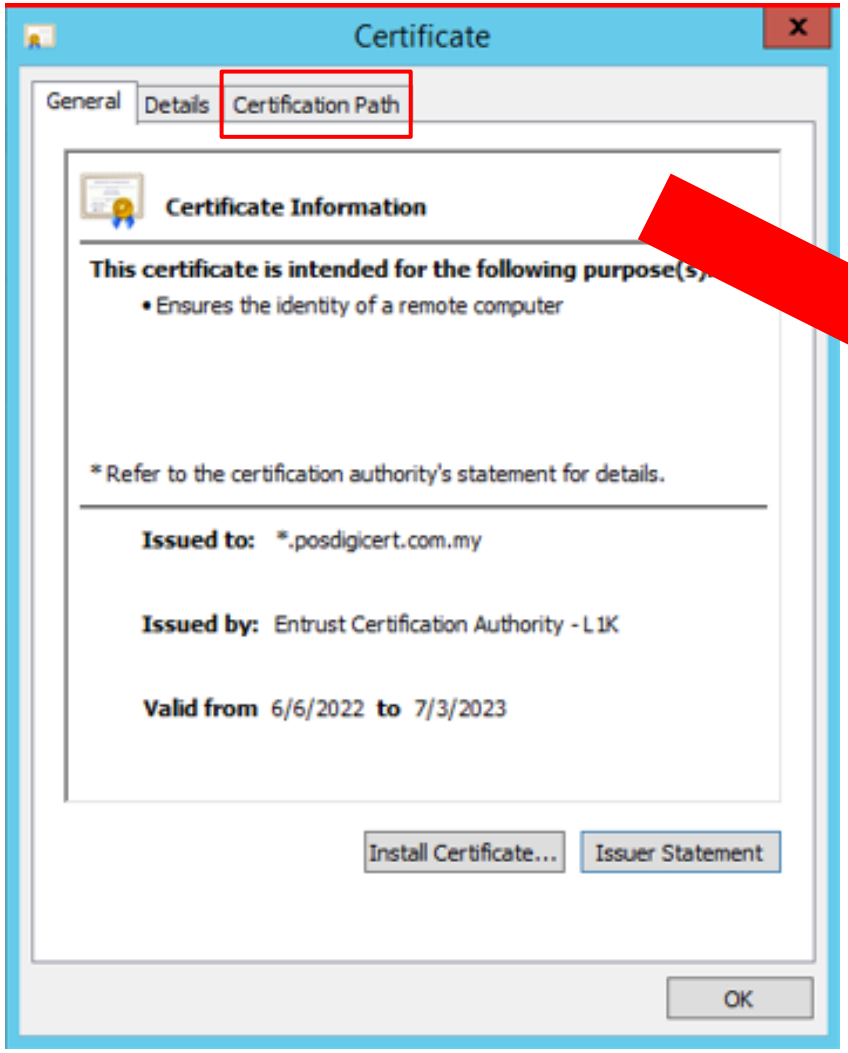

Add Site Binding
Type:
https
IP address:
All Unassigned
Port:
443
Host name:
Require Server Name Indication
Optional
Automatik
SSL certificate:
mytest.posdigicert.com.my
Select...
View...
OK
Cancel

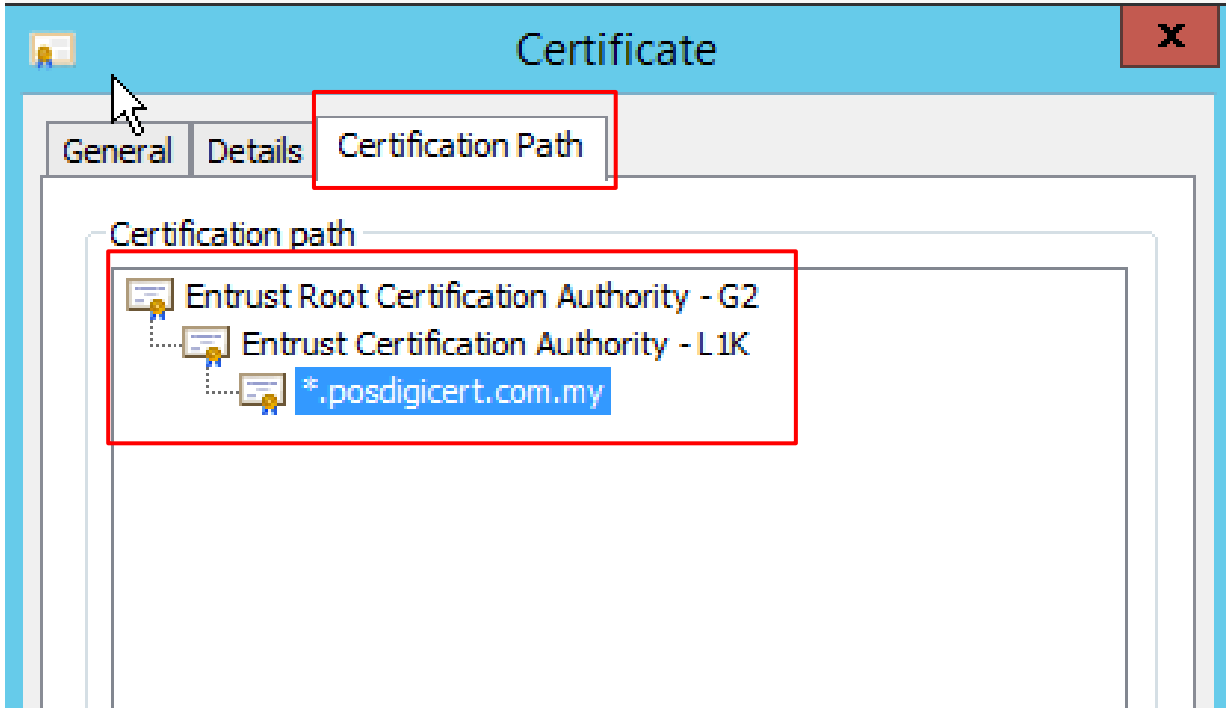

Site Bindings
Type
Host Name
Port
IP Address
Binding Informa...
http
80
*
https
443
*
Add...
Edit...
Remove
Browse
Close
sijil digital pelayan dengan laman sesawang berjaya diintegrasi.


Default Web Site Home
Filter:
Go
Show All
Group by:
Area
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Handler Map...
Logging
MIME Types
Modules
SSL Settings
Management
Configurat... Editor
Restart Web Server Service
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Browse *:443 (https)
Advanced Settings...
Configure
Limits...
Help

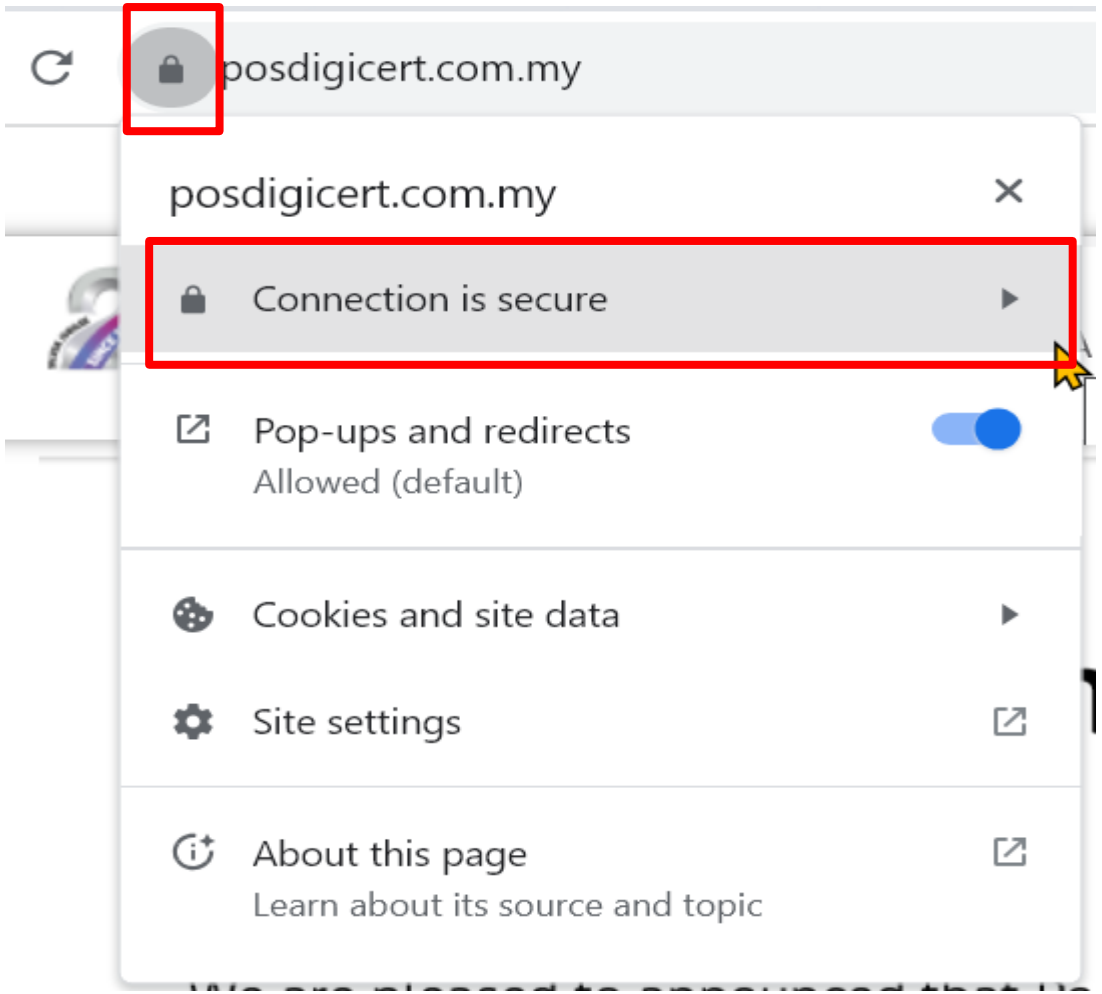

https://mytest.posdigicert.com.my/
IIS Windows Server
File Edit View Favorites Tools Help
Demo mytest.posdigicert....
Windows Server
Internet Information Servi
Cuba Semak Laman Web

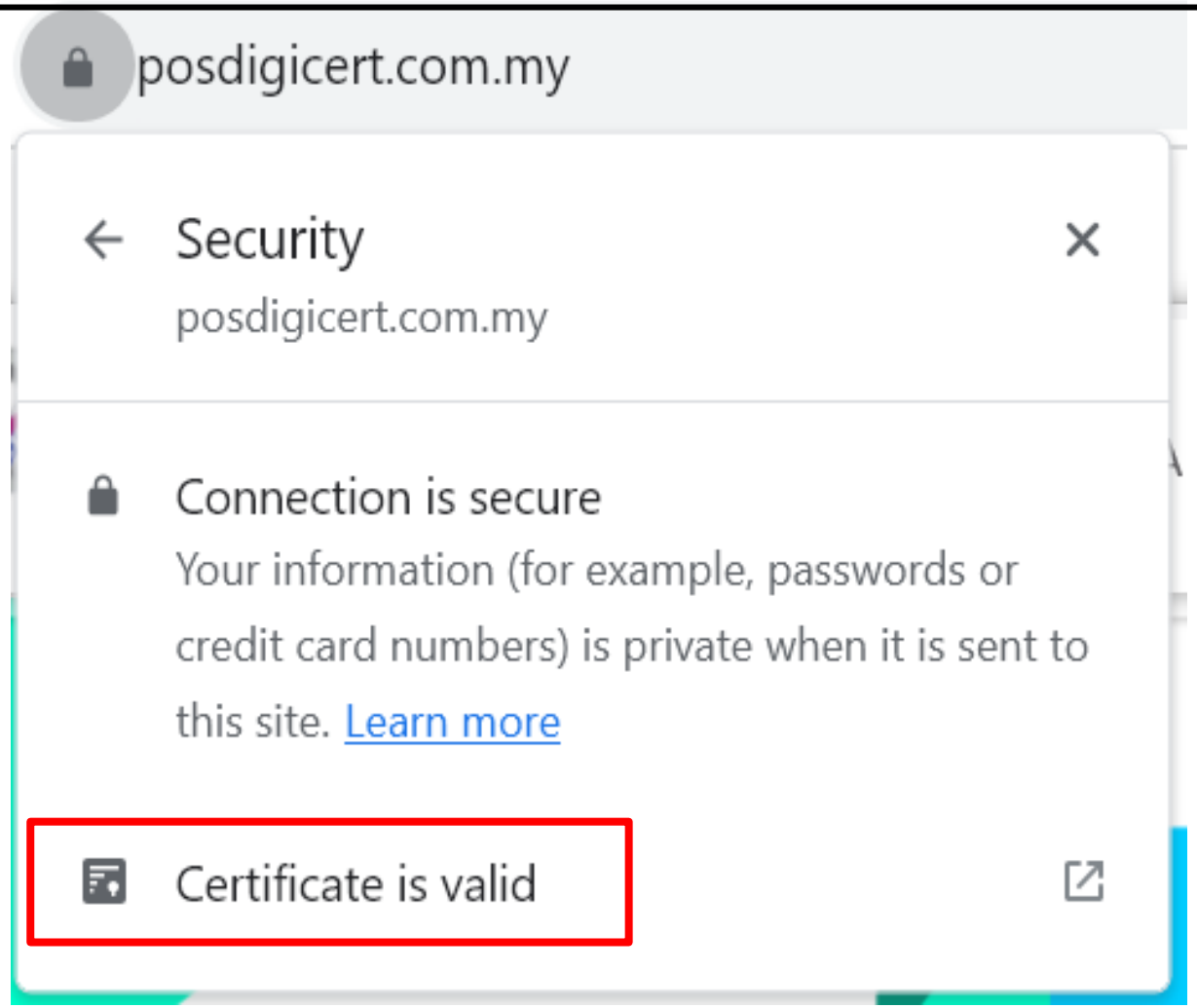

https://mytest.posdigicert.com.my/
IIS Windows Server
File Edit View Favorites Tools Help
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.posdigicert.com.my
Issued by: Entrust Certification Authority - L1K
Valid from 6/6/2022 to 7/3/2023
Install Certificate...
Issuer Statement
OK
ברוכים הבאים
Welkom
Добро пожаловать
환영합니다
Üdvözöljük

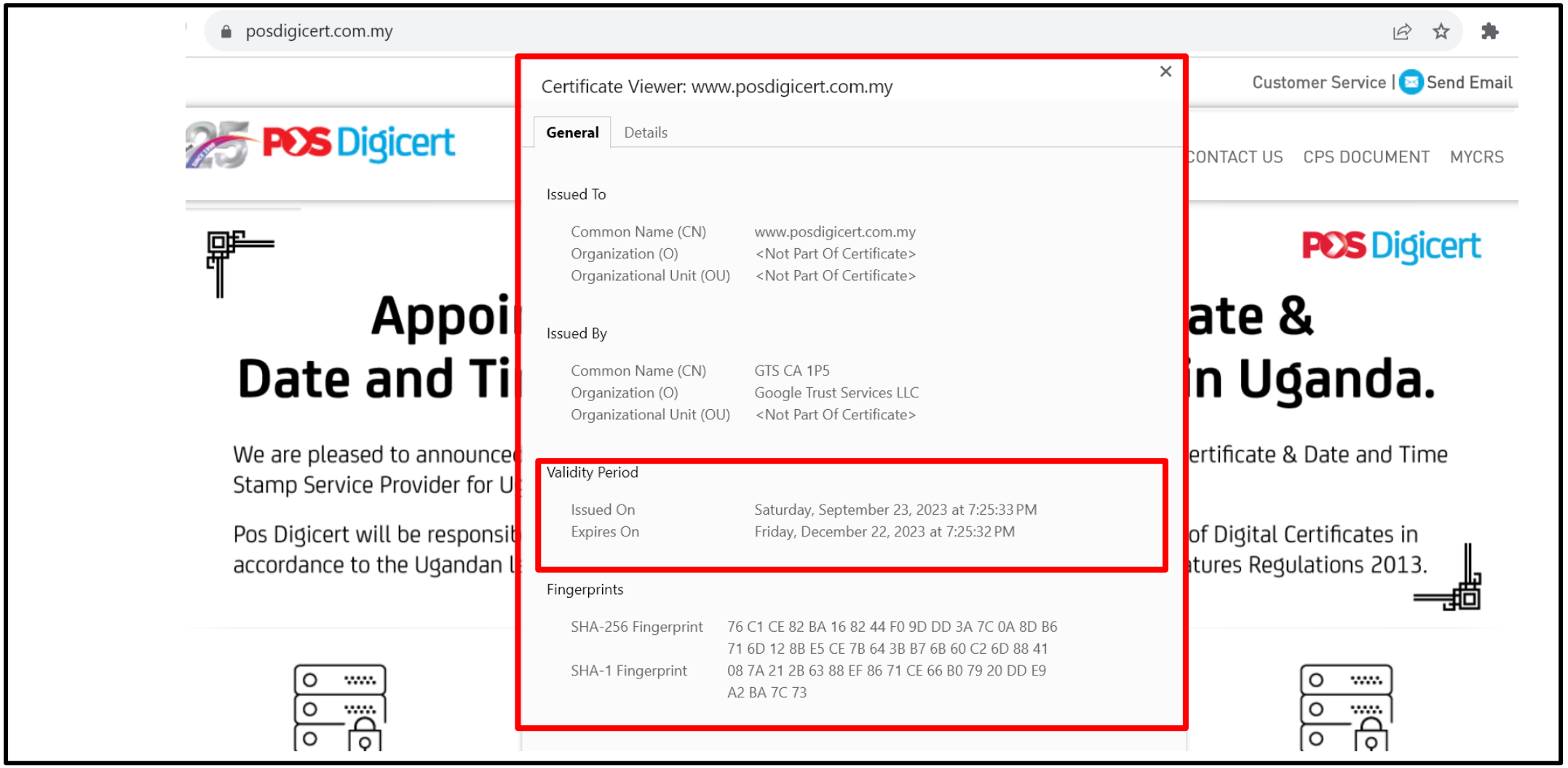

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.posdigicert.com.my
Issued by: Entrust Certification Authority - L1K
Valid from 6/6/2022 to 7/3/2023
Install Certificate...
Issuer Statement
OK


Certificate
General
Details
Certification Path
Certification path
Entrust Root Certification Authority - G2
Entrust Certification Authority - L1K
*.posdigicert.com.my


posdigicert.com.my
Customer Service
POS Digicert
ABOUT US
SOLUTION AND SERVICES
SUPPORT
DOWNLOAD
CPS DOCUMENT
POS Digicert
SILVER JUBILEE
SINCE 1998
Empowering
Your Digital Presence
Sample View SSL Certificate Via Google Chrome


posdigicert.com.my
posdigicert.com.my
Connection is secure
Pop-ups and redirects
Allowed (default)
Cookies and site data
Site settings
About this page
Learn about its source and topic


posdigicert.com.my
Security
posdigicert.com.my
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate is valid

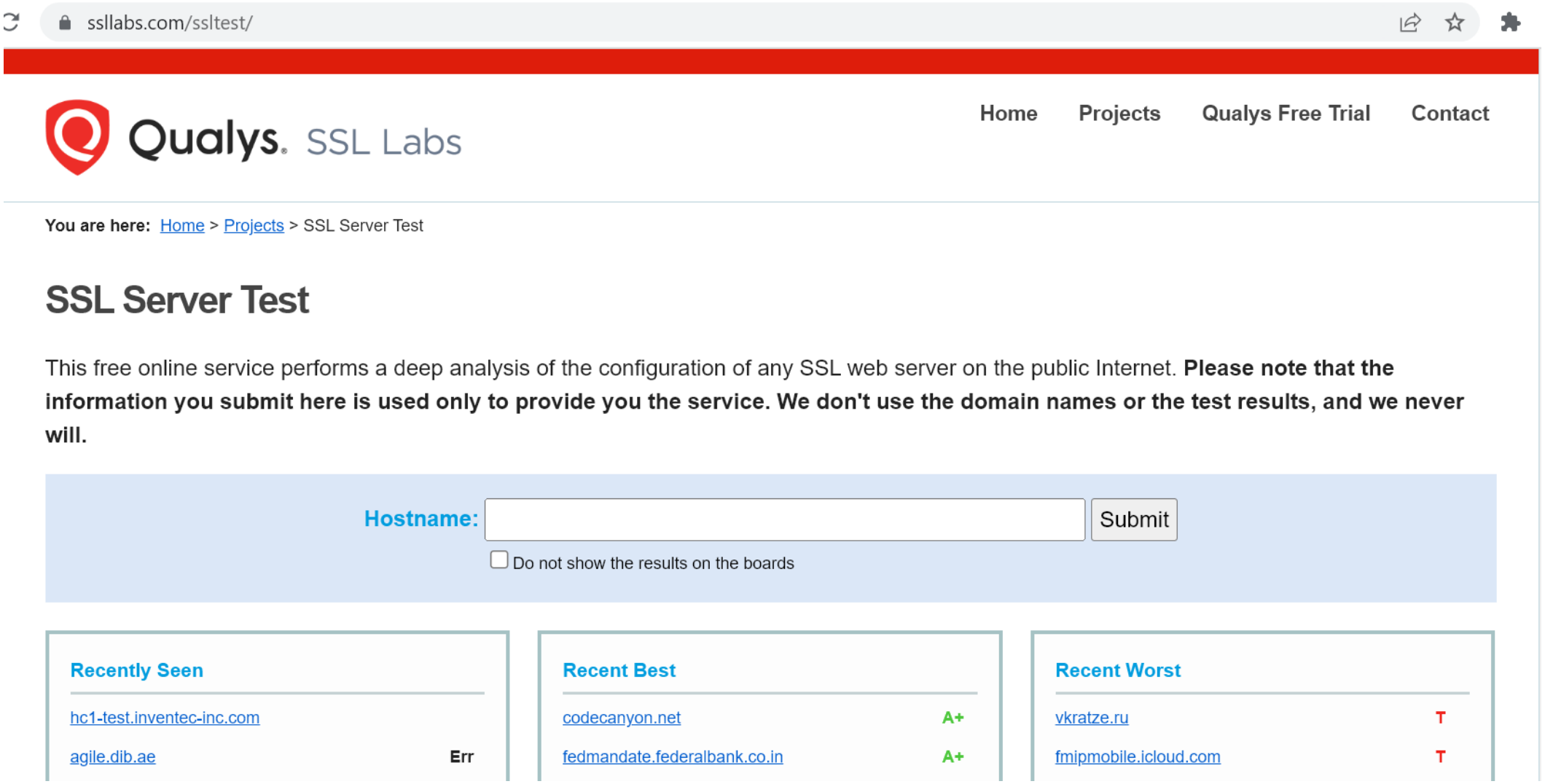

posdigicert.com.my
Customer Service | Send Email
POS Digicert
CONTACT US
CPS DOCUMENT
MYCRS
Certificate Viewer: www.posdigicert.com.my
General
Details
Issued To
Common Name (CN) www.posdigicert.com.my
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) GTS CA 1P5
Organization (O) Google Trust Services LLC
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Saturday, September 23, 2023 at 7:25:33 PM
Expires On Friday, December 22, 2023 at 7:25:32 PM
Fingerprints
SHA-256 Fingerprint 76 C1 CE 82 BA 16 82 44 F0 9D DD 3A 7C 0A 8D B6 71 6D 12 8B E5 CE 7B 64 3B B7 6B 60 C2 6D 88 41
SHA-1 Fingerprint 08 7A 21 2B 63 88 EF 86 71 CE 66 B0 79 20 DD E9 A2 BA 7C 73
POS Digicert
Date and Ti
ate &
n Uganda.
We are pleased to announce
Stamp Service Provider for U
ertificate & Date and Time
Pos Digicert will be responsi
accordance to the Ugandan L
of Digital Certificates in
atures Regulations 2013.

Bahagian 4: Semak Konfigurasi Sijil Digital Pelayan

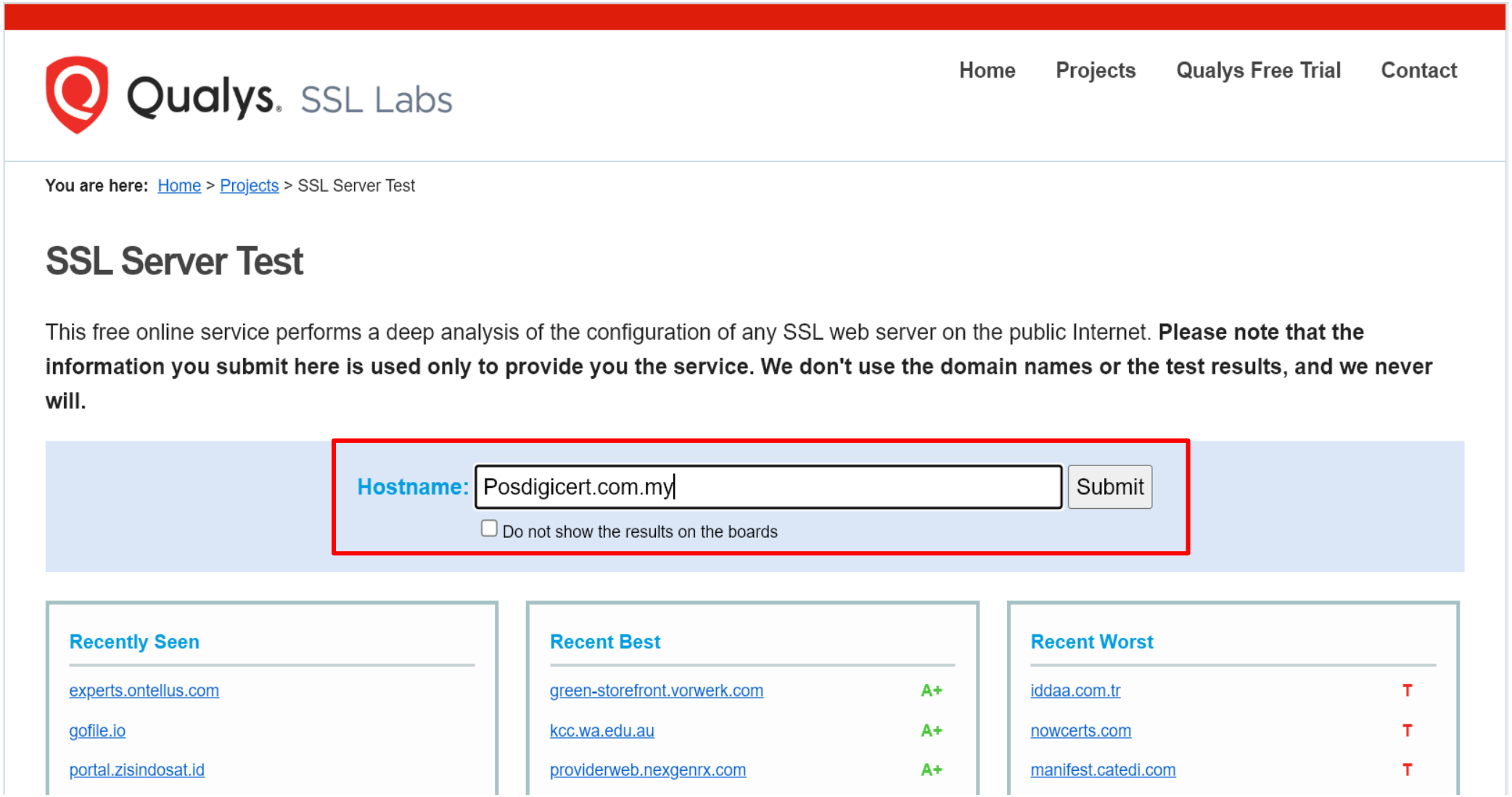
Bagaimanakah Cara Menyemak Konfigurasi Sijil Digital Pelayan?

Pautan Semak Konfigurasi Sijil Digital Pelayan

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


ssllabs.com/ssltest/
Qualys. SSL Labs
Home
Projects
Qualys Free Trial
Contact
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. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.
Hostname:
Submit
Do not show the results on the boards
Recently Seen
hc1-test.inventec-inc.com
agile.dib.ae Err
Recent Best
codecanyon.net A+
fedmandate.federalbank.co.in A+
Recent Worst
vkratze.ru T
fmipmobile.icloud.com T

Lets Test


Qualys. SSL Labs
Home
Projects
Qualys Free Trial
Contact
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. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.
Hostname:
Posdigicert.com.my
Submit
Do not show the results on the boards
Recently Seen
experts.ontellus.com
gofile.io
portal.zisindosat.id
Recent Best
green-storefront.vorwerk.com A+
kcc.wa.edu.au A+
providerweb.nexgenrx.com A+
Recent Worst
iddaa.com.tr T
nowcerts.com T
manifest.catedi.com T

Keputusan Semakan Konfigurasi Sijil Digital

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

SSL Report: www.cimbclicks.com.my (184.30.115.165)

Assessed on: Mon, 02 Oct 2023 02:07:30 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A

Sample Result

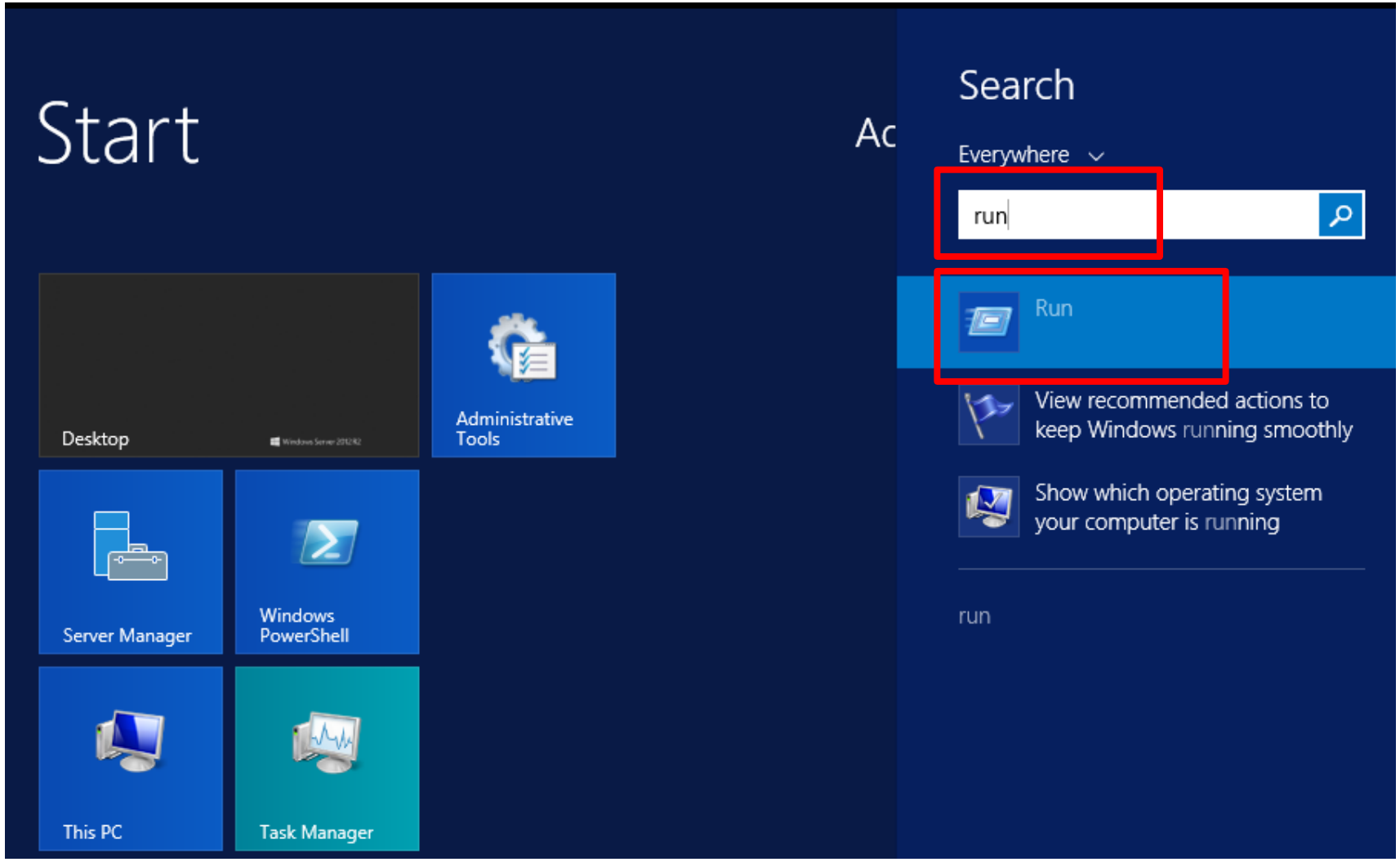
Visit our documentation page for more infor ...guides, and books. Known issues are documented here.

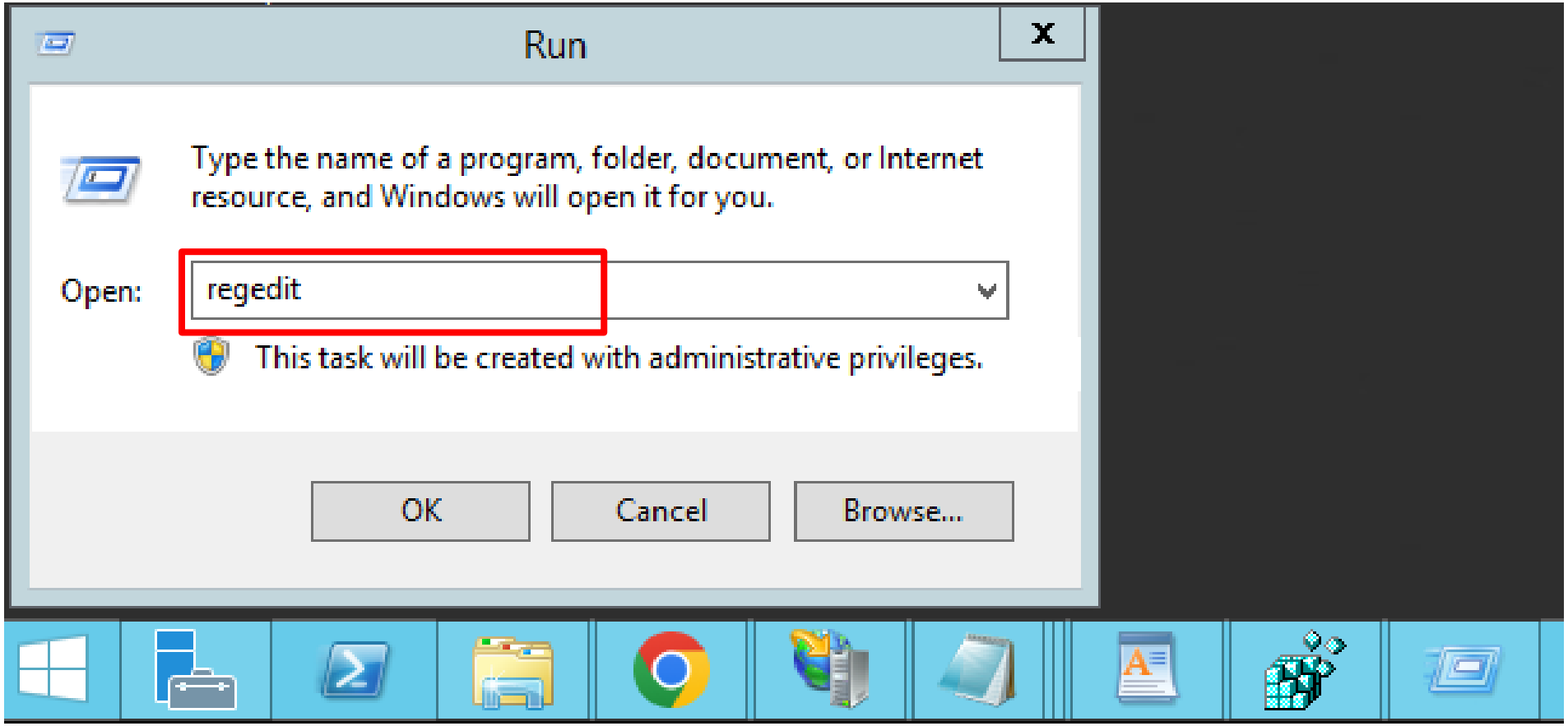
HTTP request t... this server failed, see below for details.

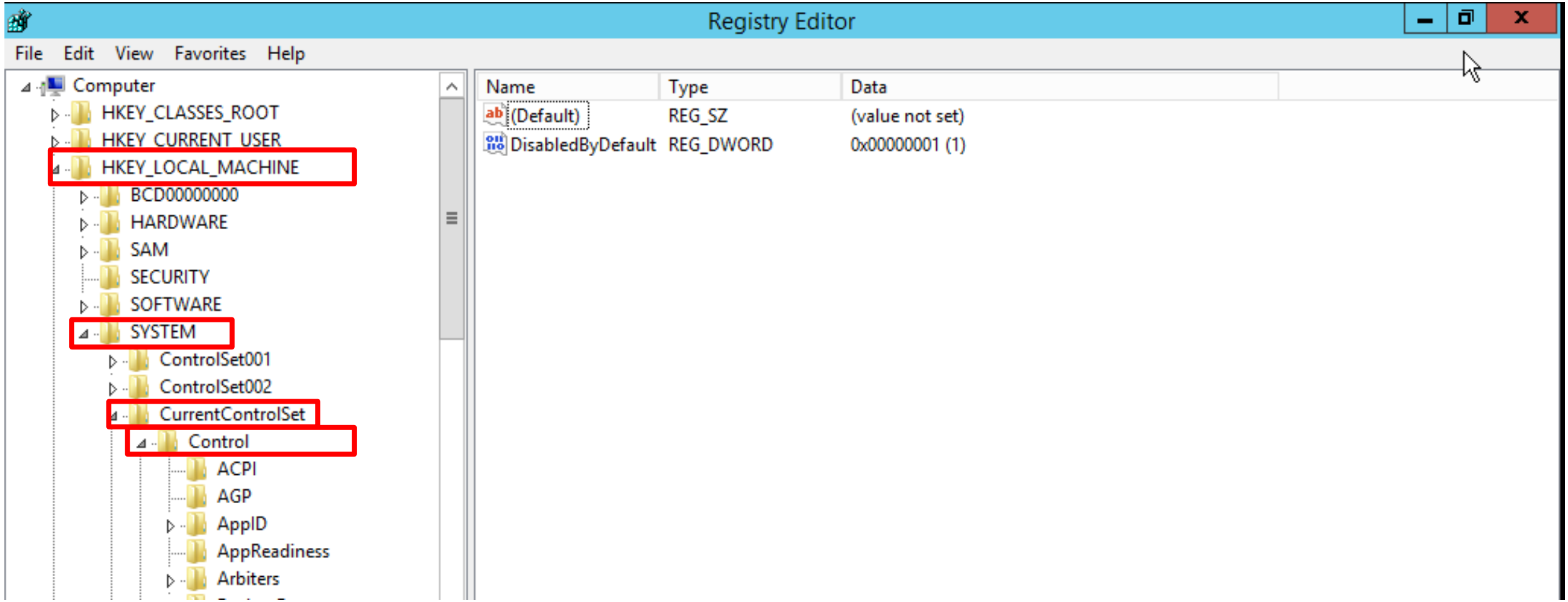
This server supports TLS 1.3.

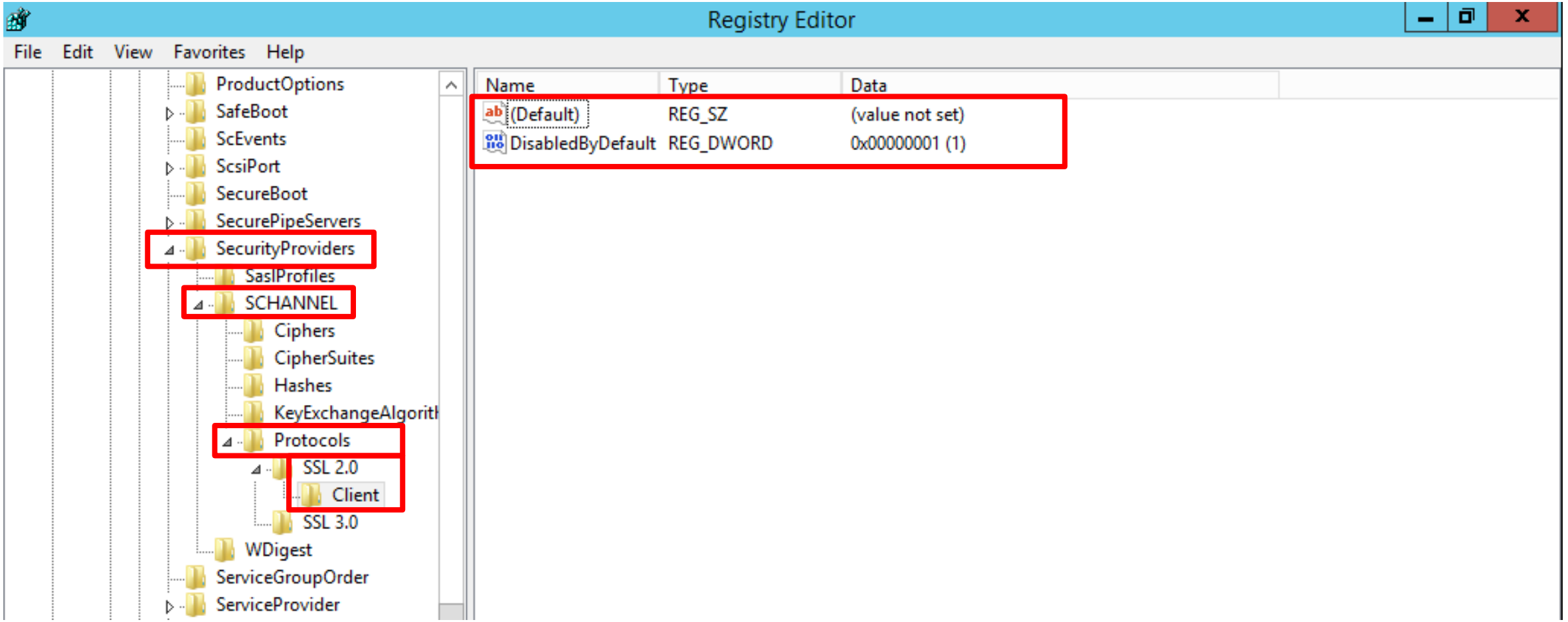
DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Kemas Kini Konfigurasi



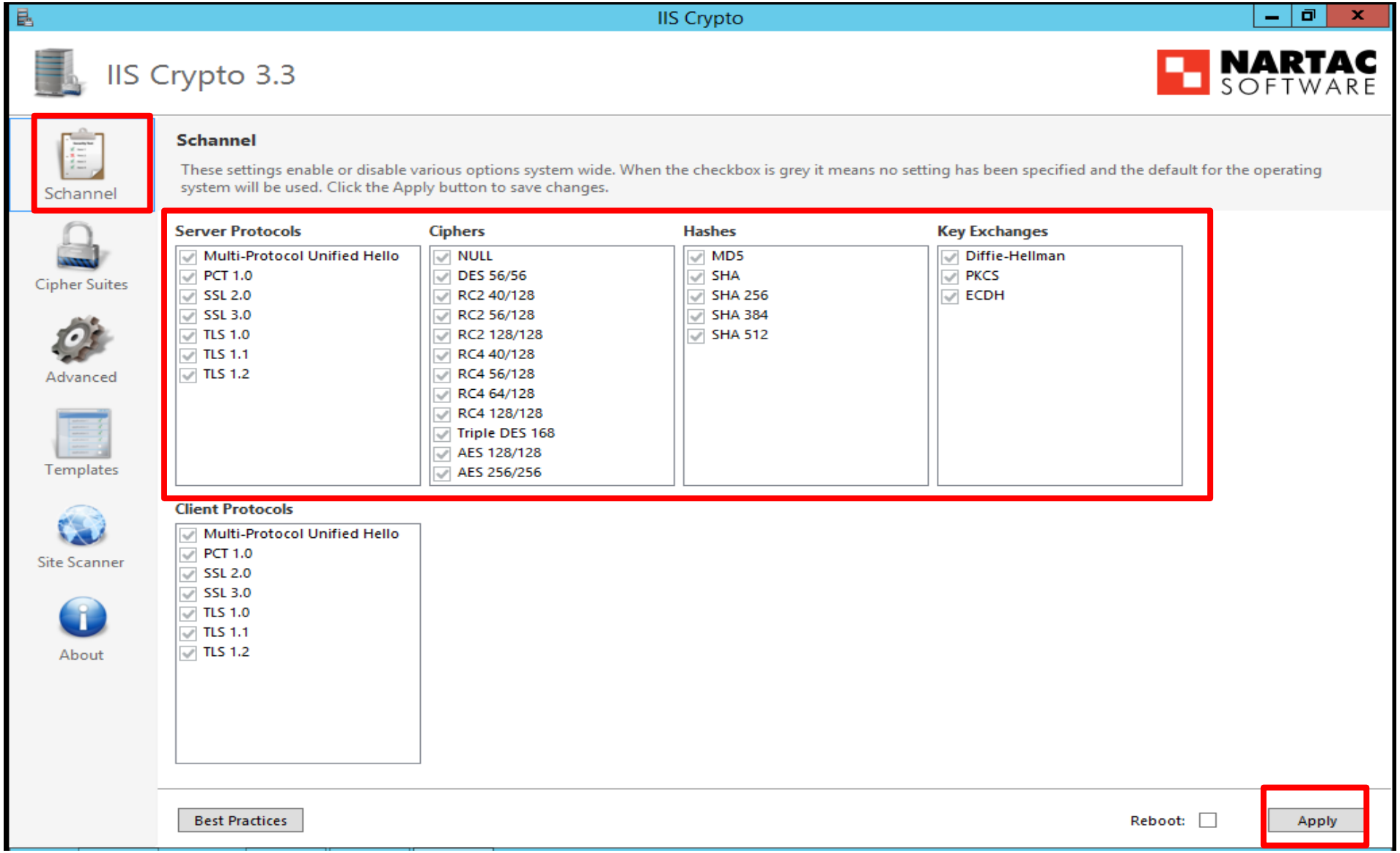

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
regedit
This task will be created with administrative privileges.
OK
Cancel
Browse...

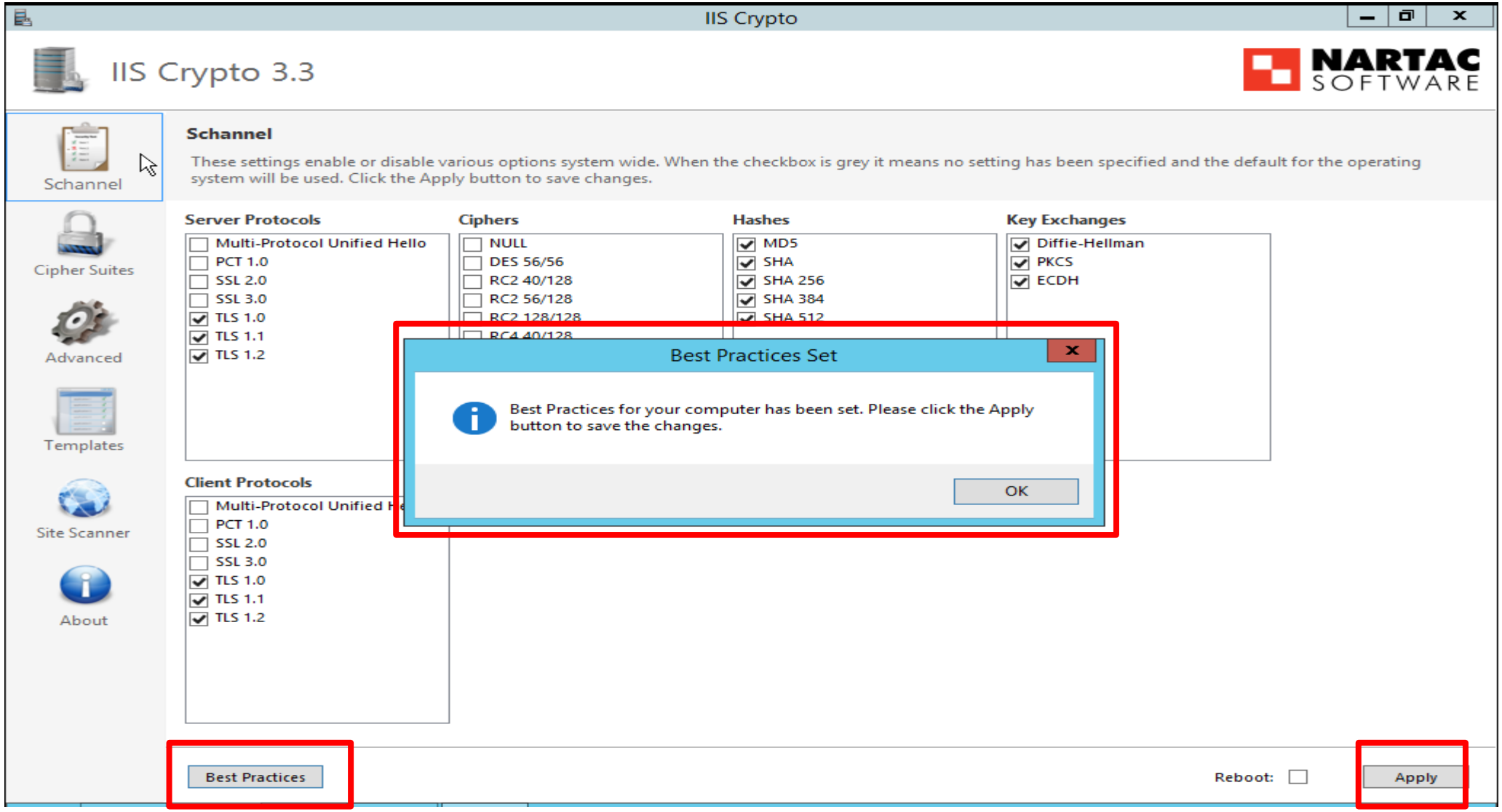

Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ControlSet001
ControlSet002
CurrentControlSet
Control
ACPI
AGP
AppID
AppReadiness
Arbiters
Name
Type
Data
(Default)
REG_SZ
(value not set)
DisabledByDefault
REG_DWORD
0x00000001 (1)

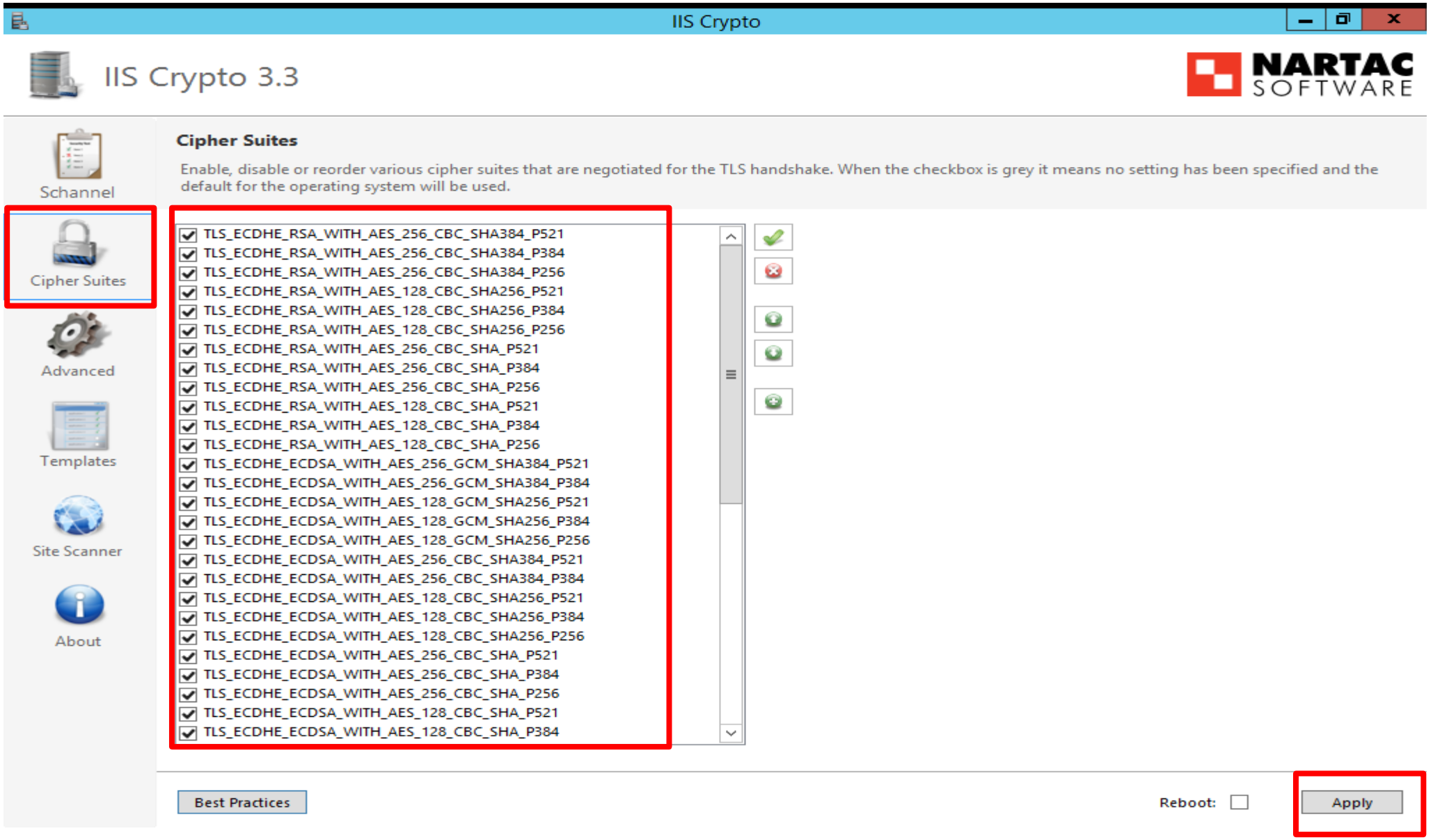

Registry Editor
File
Edit
View
Favorites
Help
ProductOptions
SafeBoot
ScEvents
ScsiPort
SecureBoot
SecurePipeServers
SecurityProviders
SaslProfiles
SCHANNEL
Ciphers
CipherSuites
Hashes
KeyExchangeAlgorith
Protocols
SSL 2.0
Client
SSL 3.0
WDigest
ServiceGroupOrder
ServiceProvider
Name
Type
Data
(Default)
REG_SZ
(value not set)
DisabledByDefault
REG_DWORD
0x00000001 (1)

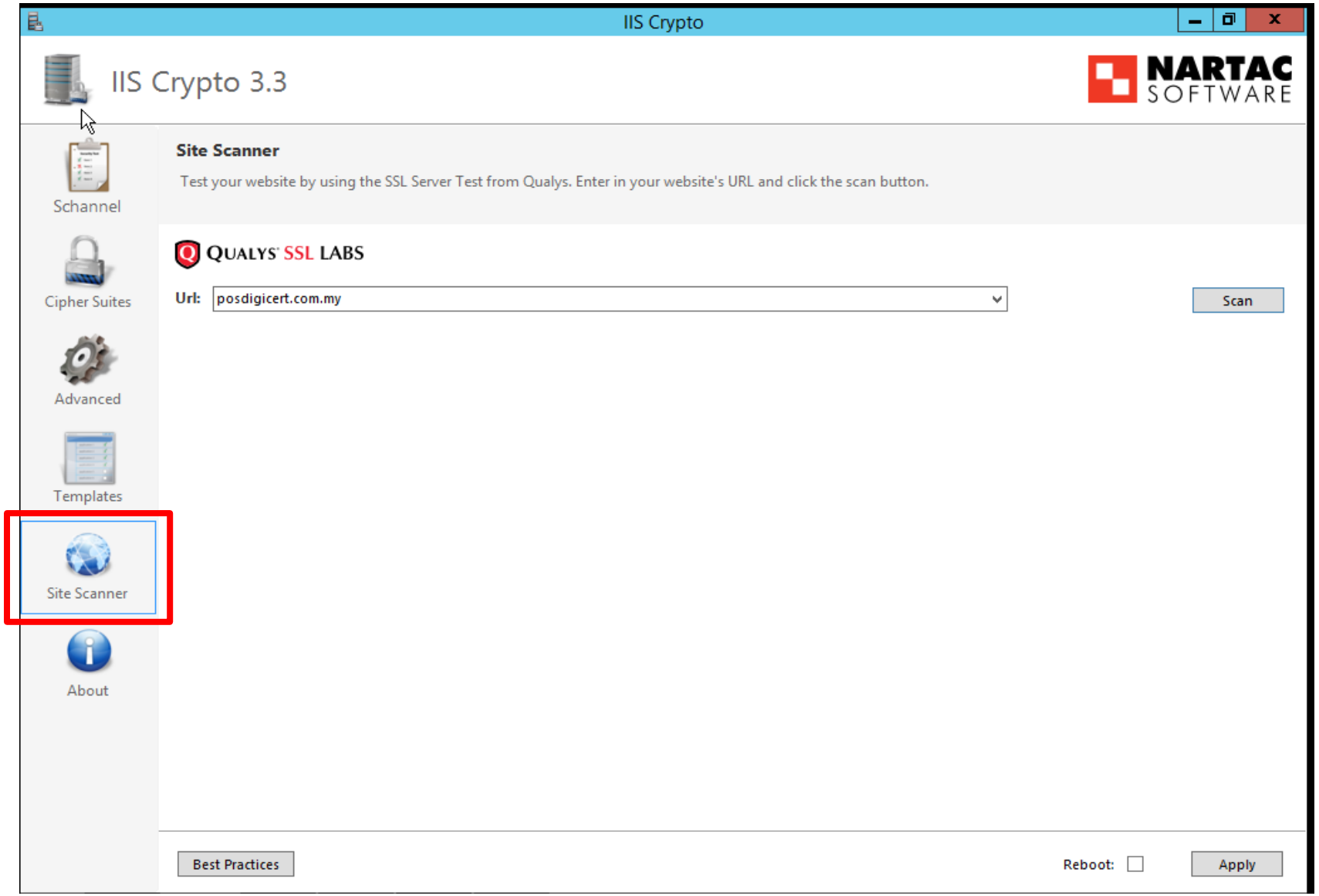
Pautan Kemas Kini TLS Dan Ciphers

https://youtu.be/49yTGXW2wBI?si=d9g1E-b08N8z4oMG


IIS Crypto
IIS Crypto 3.3
NARTAC SOFTWARE
Schannel
Cipher Suites
Advanced
Templates
Site Scanner
About
Schannel
These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used. Click the Apply button to save changes.
Server Protocols
Multi-Protocol Unified Hello
PCT 1.0
SSL 2.0
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2
Ciphers
NULL
DES 56/56
RC2 40/128
RC2 56/128
RC2 128/128
RC4 40/128
RC4 56/128
RC4 64/128
RC4 128/128
Triple DES 168
AES 128/128
AES 256/256
Hashes
MD5
SHA
SHA 256
SHA 384
SHA 512
Key Exchanges
Diffie-Hellman
PKCS
ECDH
Client Protocols
Multi-Protocol Unified Hello
PCT 1.0
SSL 2.0
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2
Best Practices
Reboot:
Apply


IIS Crypto
IIS Crypto 3.3
NARTAC SOFTWARE
Schannel
Cipher Suites
Advanced
Templates
Site Scanner
About
Schannel
These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used. Click the Apply button to save changes.
Server Protocols
Multi-Protocol Unified Hello
PCT 1.0
SSL 2.0
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2
Ciphers
NULL
DES 56/56
RC2 40/128
RC2 56/128
Hashes
MD5
SHA
SHA 256
SHA 384
Key Exchanges
Diffie-Hellman
PKCS
ECDH
Best Practices Set
Best Practices for your computer has been set. Please click the Apply button to save the changes.
OK
Client Protocols
PCT 1.0
SSL 2.0
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2
Best Practices
Reboot:
Apply


IIS Crypto
IIS Crypto 3.3
NARTAC SOFTWARE
Schannel
Cipher Suites
Advanced
Templates
Site Scanner
About
Cipher Suites
Enable, disable or reorder various cipher suites that are negotiated for the TLS handshake. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used.
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
Best Practices
Reboot:
Apply


IIS Crypto
IIS Crypto 3.3
NARTAC SOFTWARE
Schannel
Cipher Suites
Advanced
Templates
Site Scanner
About
Site Scanner
Test your website by using the SSL Server Test from Qualys. Enter in your website's URL and click the scan button.
QUALYS SSL LABS
Url:
posdigicert.com.my
Scan
Best Practices
Reboot:
Apply

TERIMA KASIH