TATACARA INSTALASI SIJIL DIGITAL PELAYAN

SIJIL DIGITAL PELAYAN – *BASIC STEPS*

01

Sijil Digital Pelayan

- *Best Practice*

02

Penjanaan dan Pemasangan Sijil Digital Pelayan

- Apa itu CSR?
- Platform Penjanaan CSR
- Penjanaan dan Pemasangan
  - Apache Tomcat (Single Domain dan Wildcard)
  - IIS (Single Domain dalam persekitaran Windows)
  - Apache Server (Multidomain)

03

Export Sijil Digital Pelayan

- Windows (PEM kepada format .PFX)
- Apache (PKCS#7 kepada format .PFX)
- Apache (PFX kepada format .PEM)

SIJIL DIGITAL PELAYAN – *BEST PRACTICE*

Private Key dan Sijil Digital

- Penggunaan Private key – RSA 2048 bit atau ECDSA 256 bit
- Perlindungan private key – hadkan akses kepada pegawai tertentu sahaja
- Memastikan sijil digital mewakili domain yang betul

Konfigurasi

- Konfigurasi *certificate chain* yang lengkap
- Penggunaa protocol yang selamat – TLS v1.2
- Penggunaan Cipher Suites yang selamat e.g: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Performance

- Penggunaan key - “too short” insecure, “too long” slow operations

HTTP dan Keselamatan Aplikasi

- *Encrypt everything*
- Elakkan Mixed Content

Apache Tomcat (Single Domain dan Wildcard)

PEMASANGAN SIJIL DIGITAL – APACHE TOMCAT

Import sijil digital ke dalam *keystore*

a. Import Certificate Chain

```
keytool -import -alias root -keystore <your_keystore_filename> -trustcacerts -file
<filename_of_the_chain_certificate>
```

b. Import Certificate

```
keytool -import -alias tomcat -keystore <your_keystore_filename> -file
<your_certificate_filename>
```

Konfigurasi pada Apache Tomcat

a. Edit fail server.xml

```
$CATALINA_BASE/conf/server.xml
```

b. Kemaskini fail server.xml untuk konfigurasi keystore

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 --> <Connector
protocol="org.apache.coyote.http11.Http11NioProtocol" port="8443" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true" keystoreFile="${user.home}/.keystore"
keystorePass="changeit" clientAuth="false" sslProtocol="TLS"/>
```

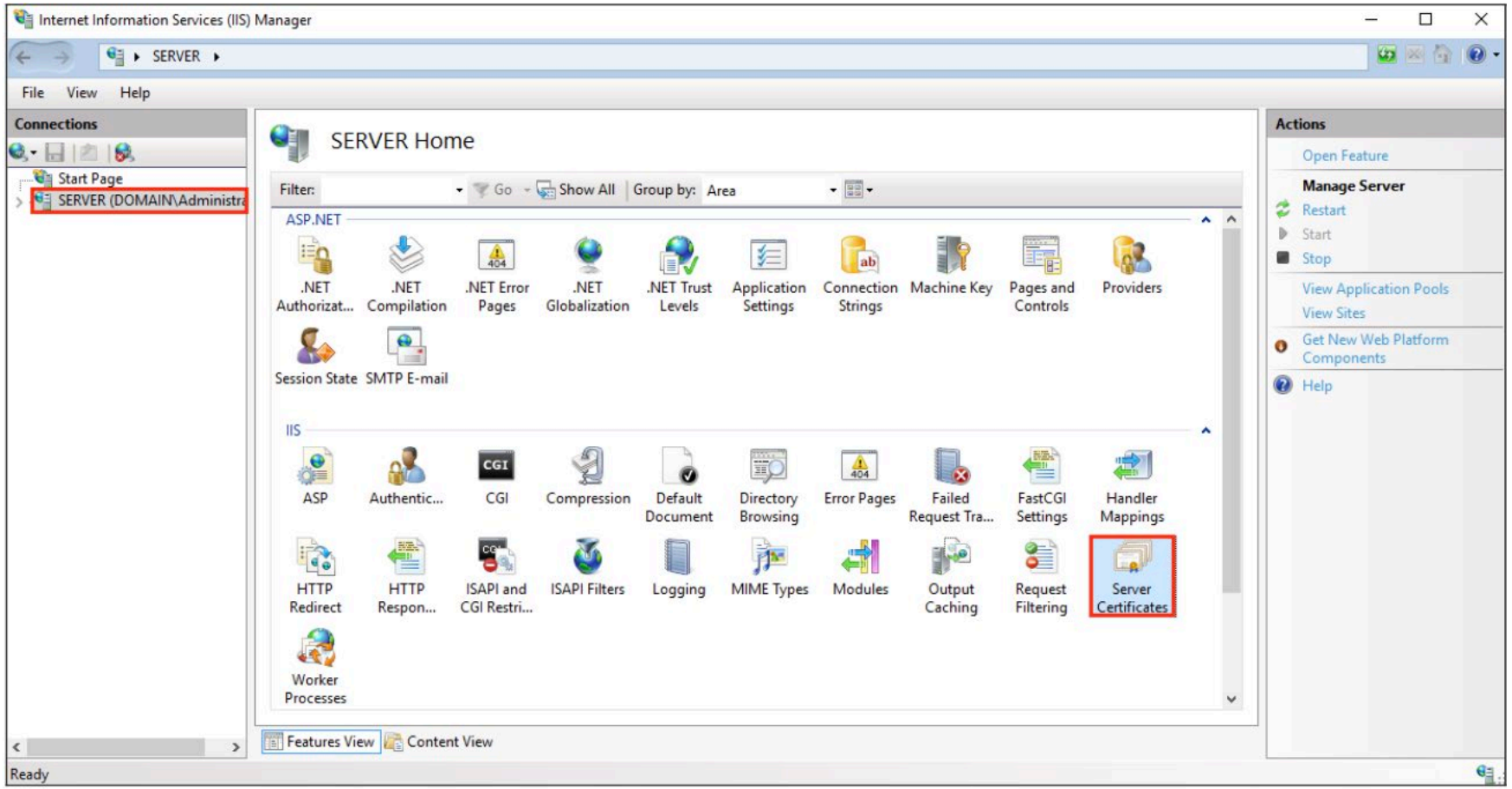
Apache Tomcat 9

IIS (Single Domain dalam persekitaran Windows)

PEMASANGAN SIJIL DIGITAL PELAYAN – IIS 10

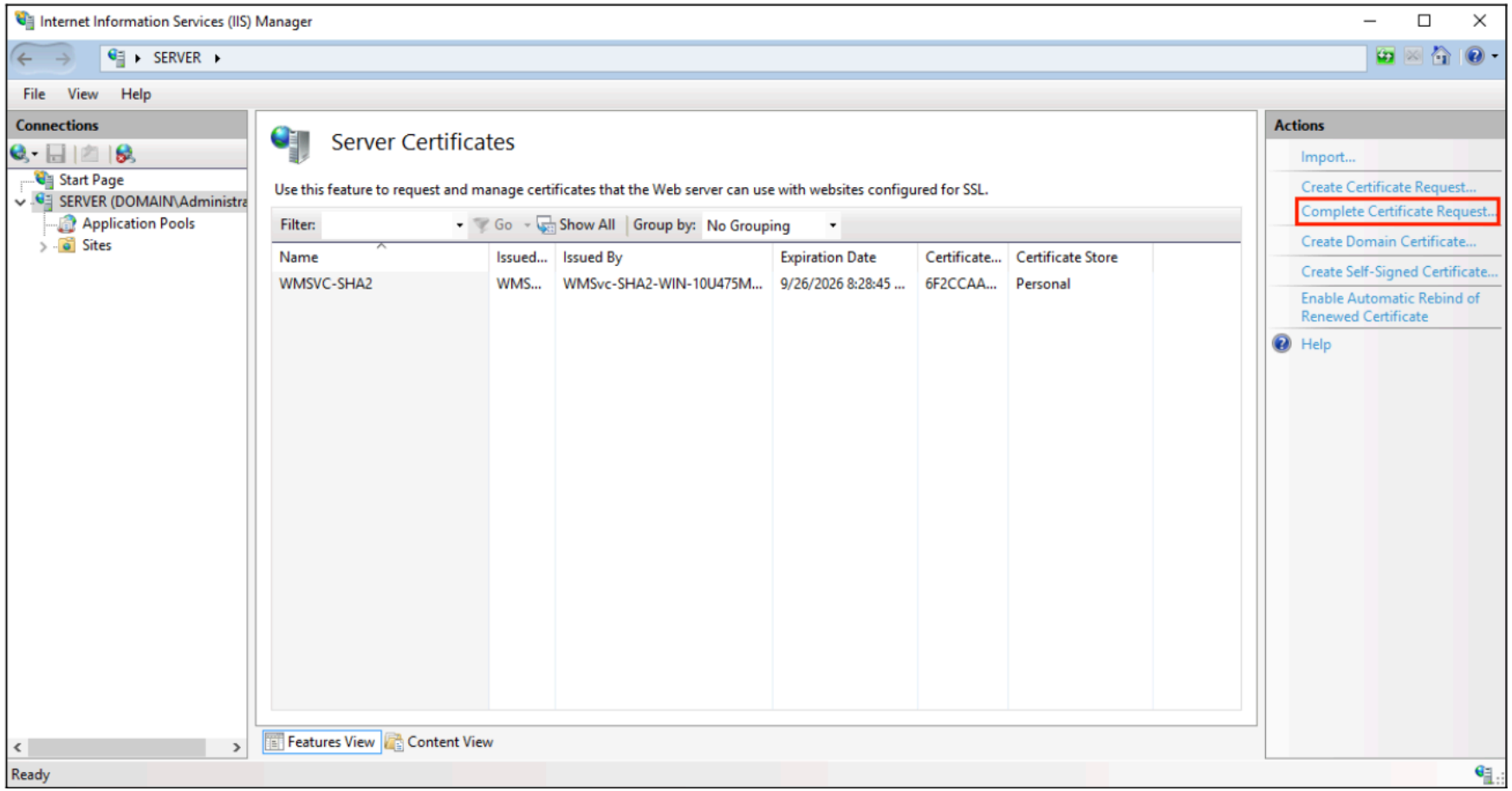
01 Buka skrin ***Internet Information Service (IIS) Manager*** melalui **Windows** start menu**,** taip ***Internet Information Service (IIS) Manager***

02 Pada menu ***Connections***, pilih nama pelayan dan ***double click Server Certificates***



PEMASANGAN SIJIL DIGITAL PELAYAN – IIS 10

03 Klik ‘Complete Certificate Request’ pada menu ***Actions*** (panel kanan)



PEMASANGAN SIJIL DIGITAL PELAYAN – IIS 10

04 Pada paparan ***Specify Certificate Authority Response***:

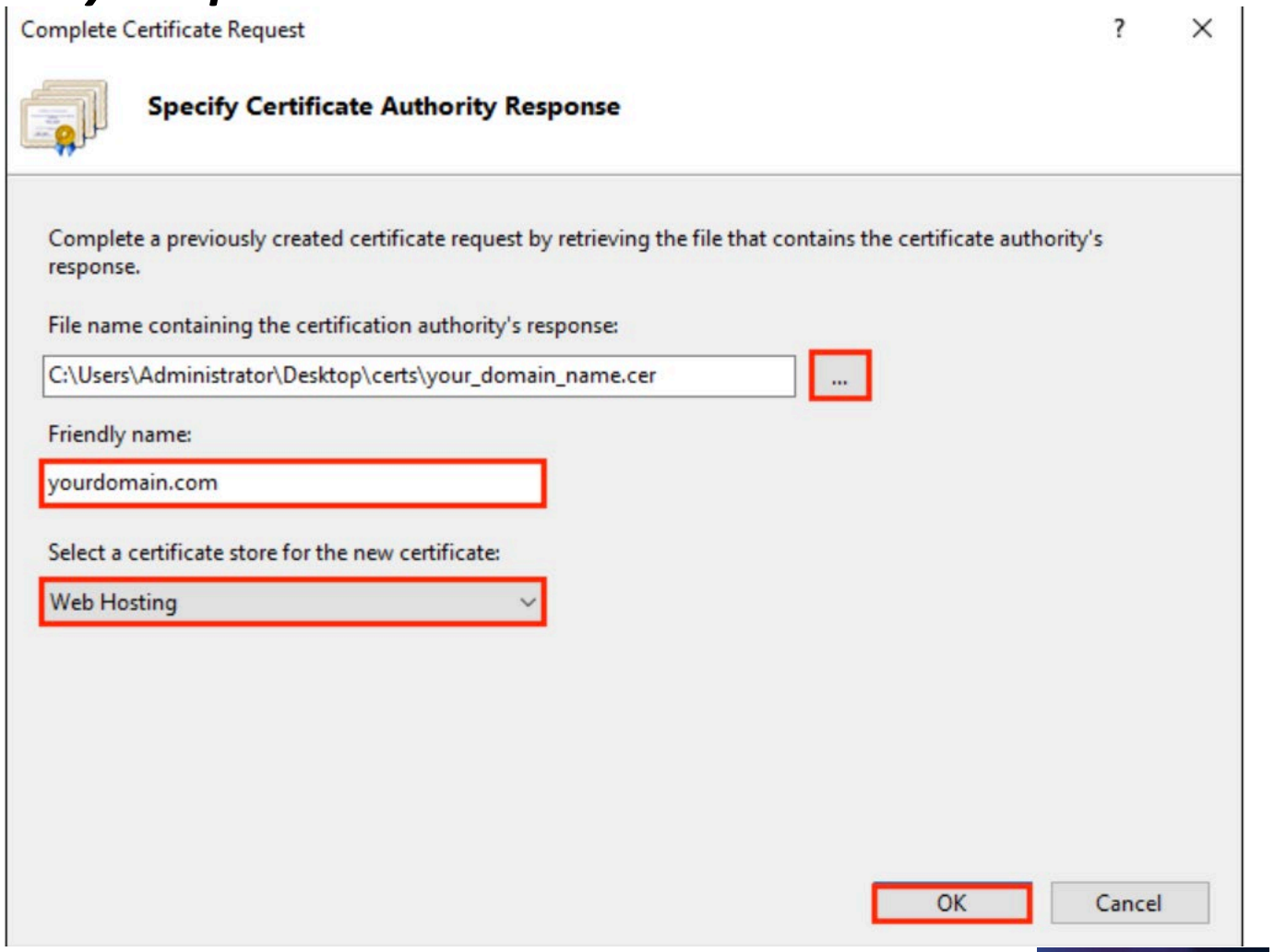
a. Muat naik fail sijil digital

b. Masukkan nama domain

c. Pilih *certificate store* bagi sijil digital tersebut

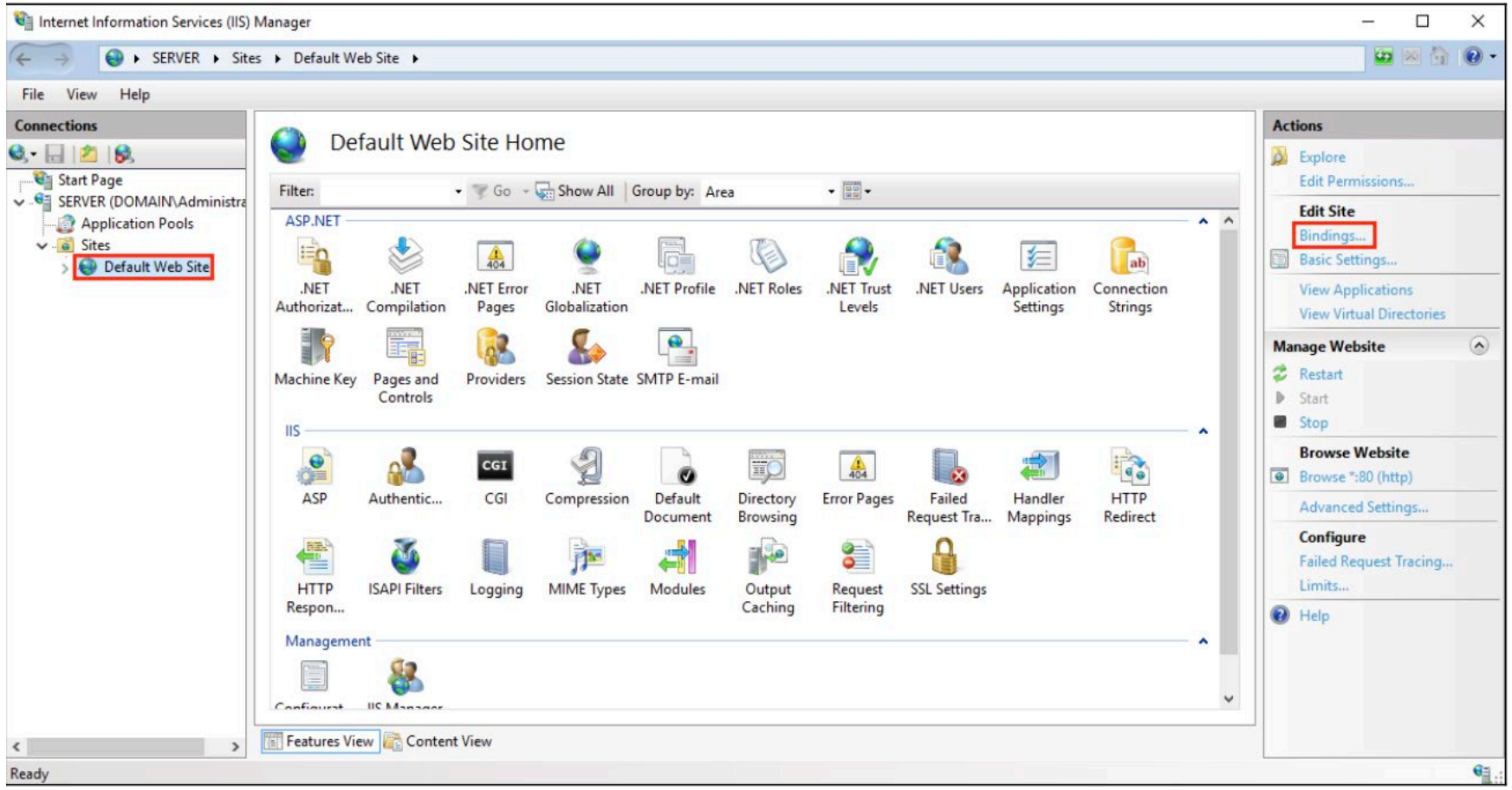
d. Tekan 'OK'

05 Setelah sijil digital dipasang, sijil digital perlu disetkan kepada laman web yang berkaitan.



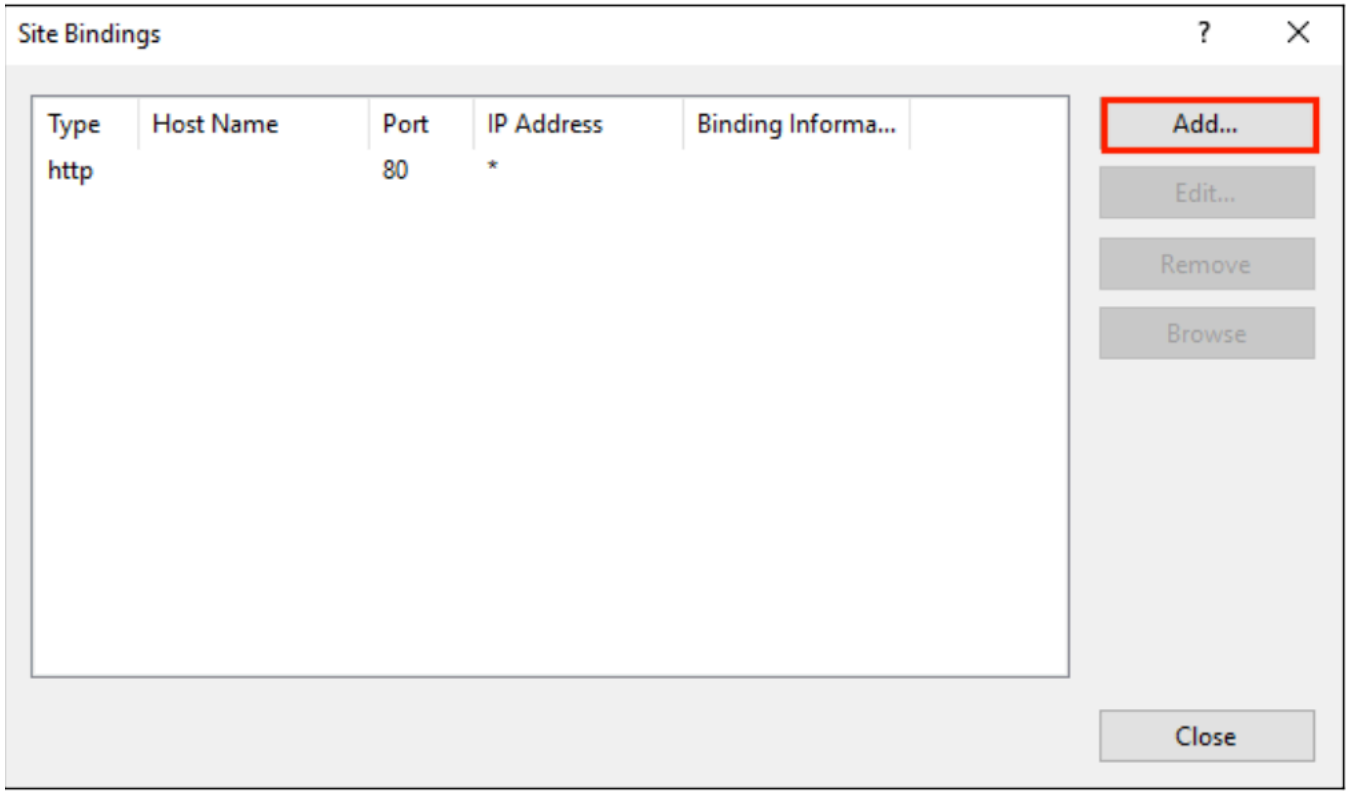
PEMASANGAN SIJIL DIGITAL PELAYAN – IIS 10

06 Klik ‘Binding’ pada menu ***Actions*** (panel kanan)



PEMASANGAN SIJIL DIGITAL PELAYAN – IIS 10

07 Klik ‘Add’ pada paparan ***Site Binding***



PEMASANGAN SIJIL DIGITAL PELAYAN – IIS 10

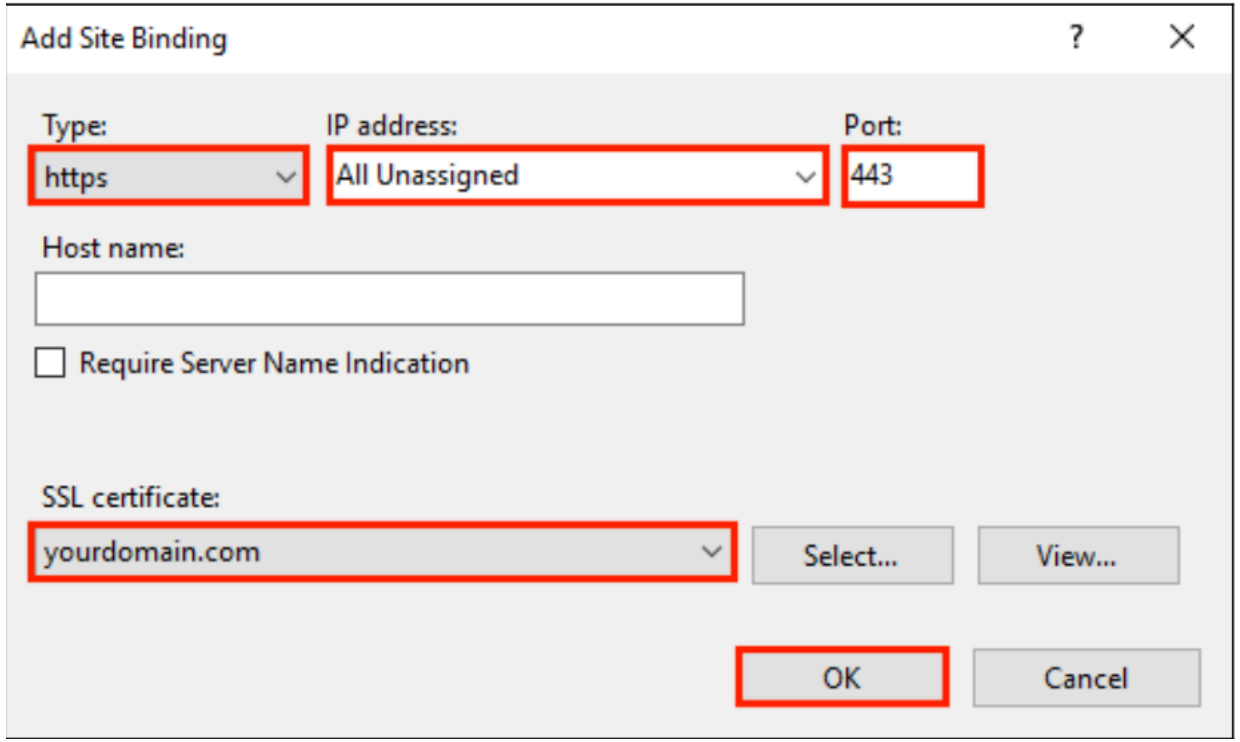
08 Lengkapkan maklumat pada paparan ***Add Site Binding***

a. ***Type –*** pilih “https”

b. ***IP Address –*** pilih ”All Unassigned”

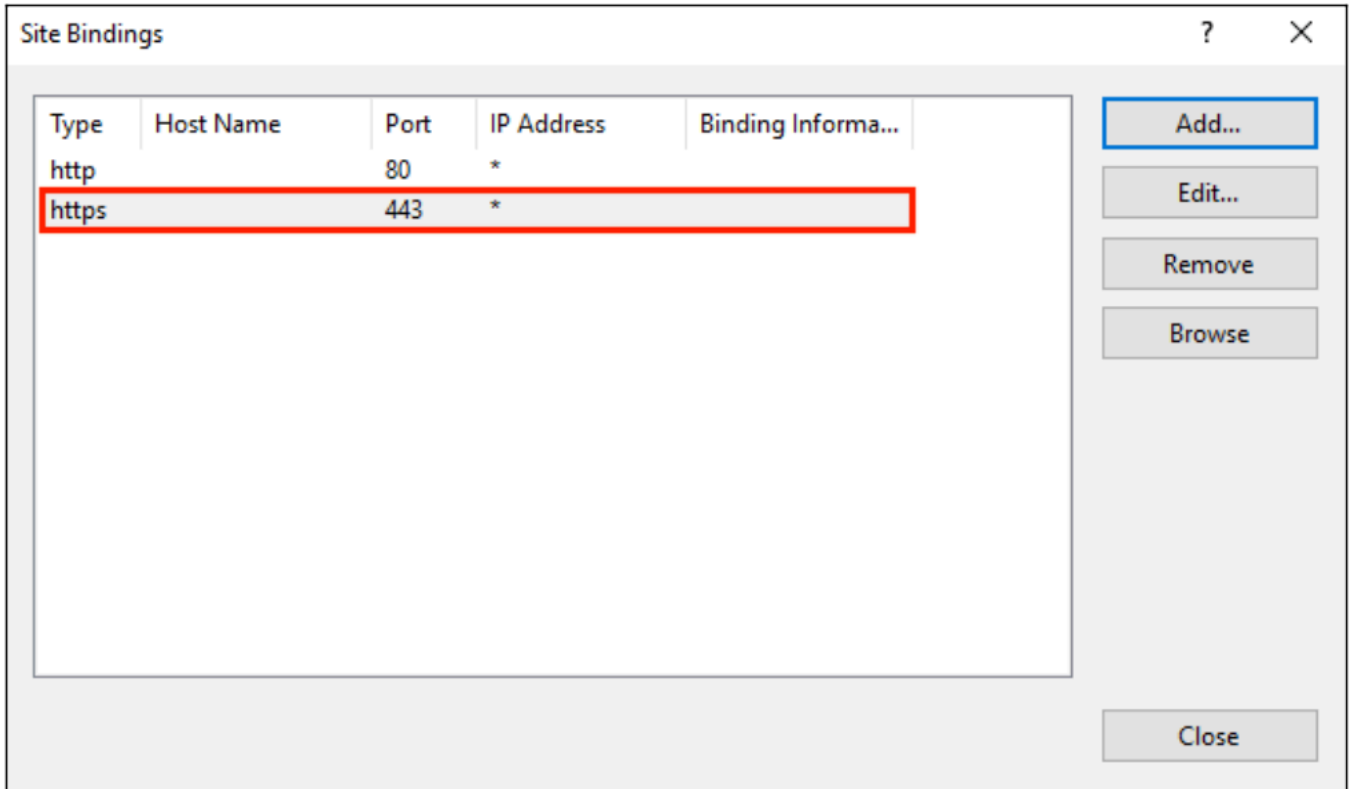
c. ***Port*** - 443

d. ***SSL certificate –*** pilih sijil digital yang telah dipasang



PEMASANGAN SIJIL DIGITAL PELAYAN – IIS 10

09 Sijil digital Berjaya dipasang dan laman web telah Berjaya dikonfigurasi untuk komunikasi secara selamat.



Export - Server Microsoft to Microsoft

EKSPORT SIJIL DIGITAL BAGI FORMAT WINDOWS (.PFX)

Tujuan: *Export* sijil digital SSL pada ***server Microsoft*** ke ***server Microsoft*** yang lain.

Tools yang digunakan: **OpenSSL**

.PFX adalah:

a. fail *binary* dalam format PKCS#12

b. digunakan untuk menyimpan sijil digital pelayan termasuk rantaian sijil dan *private key*

c. fail yang di*encypt*

d. biasanya disimpan di dalam format .pfx dan .p12.

e. digunakan pada persekitaran Windows bagi membolehkan proses import dan eksport sijil digital dan *private keys*.

EKSPORT SIJIL DIGITAL BAGI FORMAT WINDOWS (.PFX)

Prerequisites:

a. private key asal bagi sijil digital terlibat

b. Sijil digital dalam format:
PEM (.pem, .crt, .cer) ke format **PFX** atau **PKCS#7**/P7B(.p7b, .p7c) ke format **PFX**

c. OpenSSL

EKSPORT SIJIL DIGITAL BAGI FORMAT WINDOWS (.PFX)

PEM (.pem, .crt, .cer) kepada format PFX

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -
incertificate.crt -certfile more.crt
```

Keterangan *command:*

Command	Keterangan
openssl	*command* yang digunakan untuk memulakan program OpenSSL
pkcs12	*command* yang digunakan untuk menggunakan fungsi PKCS#12
-export -out	certificate.pfx export and save the PFX file as certificate.pfx
-inkey	privateKey.key – use the private key file privateKey.key as the private key to combine with the certificate.
-certfile	more.crt – This is optional, this is if you have any additional certificates you would like to include in the PFX file.

EKSPORT SIJIL DIGITAL BAGI FORMAT WINDOWS (.PFX)

PKCS#7/P7B (.p7b, .p7c) to PFX

1. Fail P7B tidak boleh digunakan untuk janaan fail PFX.
2. Fail P7B mesti ditukar kepada format PEM.
3. Seterusnya rujuk langkah-langkah untuk eksport fail PEM kepada format PFX.

```
openssl pkcs7 -print_certs -in certificate.p7b -out certificate.crt
```

Keterangan *command:*

Command	**Keterangan**
openssl	*command* yang digunakan untuk memulakan program OpenSSL
pkcs7	*command* yang digunakan untuk menggunakan fungsi PKCS#7
-print_certs –in <nama fail dalam format .p7b>	*Print out* sijil di dalam fail yang disertakan di dalam format .p7b
-out <nama fail dalam format .cer>	Nama fail dalam format .cer

Export - Server Microsoft ke Server Selain Windows

EKSPORT SIJIL DIGITAL BAGI FORMAT APACHE (.PEM)

Tujuan: *Export* sijil digital SSL pada ***server Microsoft*** ke ***server*** **selain Windows (Apache).**

Tools yang digunakan: **OpenSSL**

Langkah-langkah:

a. Tukarkan fail PFX kepada fail yang *compatible* bagi pelayan Apache

b. Untuk mendapatkan *private key,* laksanakan *command* berikut:

```
openssl pkcs12 -in <filename>.pfx  -nocerts -out key.pem
```

c. Untuk mendapatkan *private key,* laksanakan *command* berikut:

```
openssl pkcs12 -in <filename>.pfx -clcerts -nokeys -out cert.pem
```

GOVERNMENT PUBLIC KEY INFRASTRUCTURE
PRASARANA KUNCI AWAM KERAJAAN

Terima Kasih