



TATACARA PENJANAAN FAIL CSR BAGI PELAYAN

01

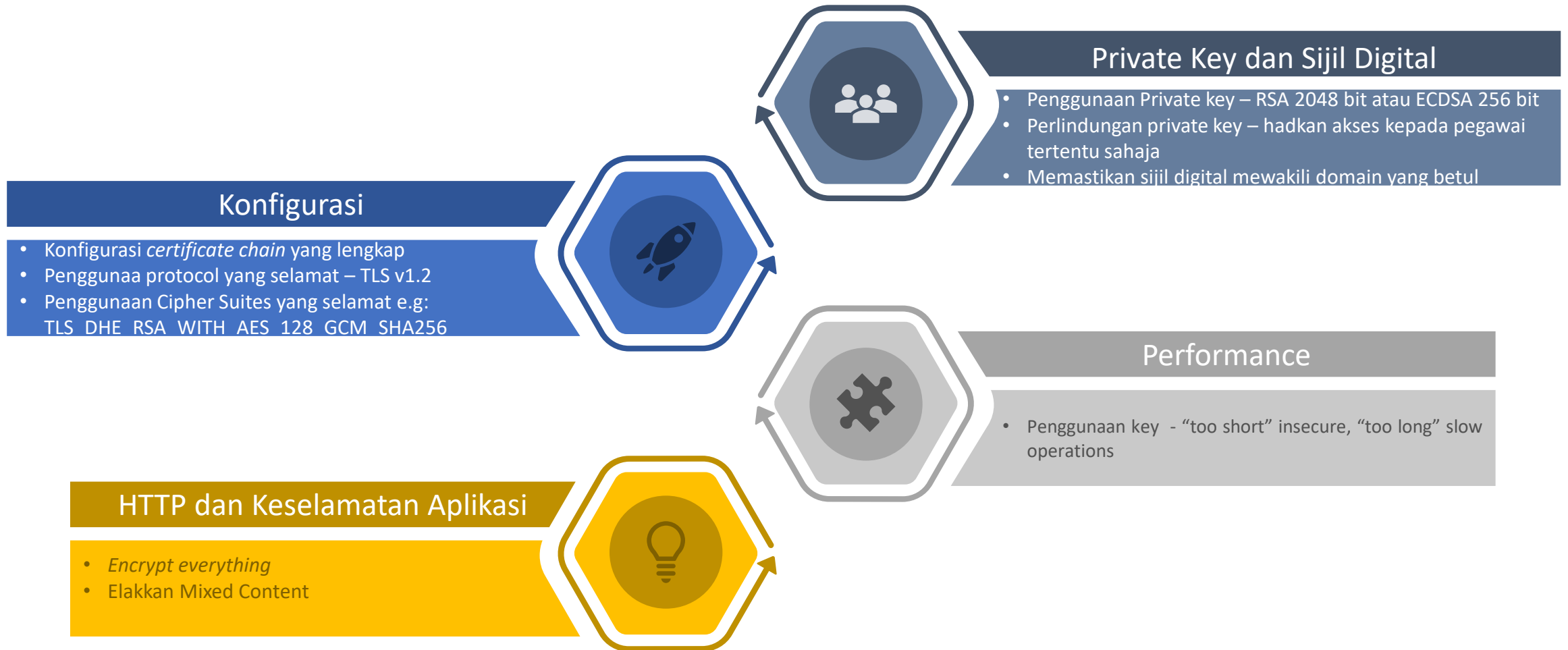
+ Sijil Digital Pelayan

❖ *Best Practice*

02

Penjanaan dan Pemasangan Sijil Digital Pelayan

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



CSR

Certificate Signing Request

❖ Merupakan standard (PKCS#10) yang digunakan untuk penghantaran *public key*, maklumat berkaitan organisasi dan nama domain

❖ Semasa penjanaan CSR, biasanya maklumat berikut diperlukan:

- Common name: <url domain>
- Organization: <nama organisasi>
- Key Algorithm: <RSA>
- Key Size: <2048>


❖ Contoh CSR:

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIICtTCCA0CAQAwQDELMAkGA1UEBhMCTVxHDAaBgNVBAoTE0dvdMvYm1lbnQg
TWFsYXlzaWEzARBgNVBAMTCmdjYS5jb20ubXkwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQcXYfjLSyZ0mjqcIwGjUjeJ2cC27sh8Gg07e9Eu92sEV2F
+83oU920W/KMYTfaSfuCIHoNVzRufx92xPBj0y2da4uJsU+I+QAeKyC9gjkW0UM
9m6htTM4+Y6CK+sytg6UbZpkEqxVubmI4Nw37x0RJGp+fMVuQqWNZg9r0hXq4Kad
l1b1UuS5Yfn7rGASMr7I+uViYXNImRDtUt78CRapvhx5I9W/+sFJ5PgegW+9tDNx
ZYF2bVzpLhK+uIpn7TReK0spV38FhI51ihppL5D+N2uR/vch0dIXeL5Z0iuvGHeH
KvrkV37egGXck2JkyH8wBl7YL8nYGUug2BAeGdIbAgMBAAGgMDAuBgkqhkiG9w0B
CQ4xITAfMB0GA1UdDgQWBBQNJrLTRLRqfPfn39TujQUhw2G6DANBgkqhkiG9w0B
AQsFAA0CAQEAAQd8P5HFhxIQpgGccp2f0Y0QDdzJR6UbI9qGSceLM+LudUmrSEqzv
zw7WGjr8K2CYSnnFqxX2Imqob03JI/q/MCS4h8u5SrTKyXK0IFfcpba50FHD2RZq
ANmHBGgx639YmNPru09npWSHwV6Xy0v/q/qFpk2ZIHibc3h0QBTkhep8nCLD3MBz
yXvdGdwI7basYDsrfLG7Wh882p47nxHSw7M77dniq6ey2Gq2Pi7i93dqPEp+ZsUU
szNA/NiSKYjblDYi6nI6+qBGJeSRm9DIjPgkS/+v7DaEZb64iKo1xousQhCAFjq/
X6KvGX23/jH7x/3cXtJILmdC9jDhI5e5TA==
-----END NEW CERTIFICATE REQUEST-----

```

Antara platform popular yang biasanya digunakan untuk aplikasi web:



Multiplatform

- Apache Tomcat
- Apache Open SSL
- IBM HTTP Web Server
- Oracle Weblogic



Windows

- Microsoft IIS
- Microsoft Exchange

Penjanaan Fail CSR bagi Apache Tomcat (Single Domain dan Wildcard)

Langkah-langkah penjanaan CSR di **Apache Tomcat** menggunakan **keytool**

Windows:

```
"%JAVA_HOME%\bin\keytool"
```

Unix:

```
$JAVA_HOME/bin/keytool
```



01

JANA CERTIFICATE KEYSTORE

```
keytool -genkey -alias tomcat -keyalg RSA -keystore  
<your_keystore_filename>
```

02

JANA CSR

```
keytool -certreq -keyalg RSA -alias tomcat -file  
certreq.csr -keystore <your_keystore_filename>
```



Contoh:

hardiyana-atsb — -bash — 112x24

```
[Hardiyana-ATSBs-MacBook-Pro:~ Nana$ keytool -genkey -alias tomcat -keyalg RSA -keystore orange.ks
[Enter keystore password:
[Re-enter new password:
What is your first and last name?
[Unknown]: www.orange.com
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]: Orange & Co.
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]: Selangor
What is the two-letter country code for this unit?
[Unknown]: MY
Is CN=www.orange.com, OU=Unknown, O=Orange & Co., L=Unknown, ST=Selangor, C=MY correct?
[no]: yes

Enter key password for <tomcat>
[ (RETURN if same as keystore password):
```

Bagi domain wildcard, isi *.<domain> sebagai input 'What is your first and last name?'

 Parameter penting untuk janaan CSR

 Fail *Certificate Keystore* yang dijana

```
-rw-r--r-- 1 Nana staff 2259 Dec 6 12:31 orange.ks
-rw-r--r--@ 1 Nana staff 97411833 Apr 30 2018 out.txt
-rw-r--r--@ 1 Nana staff 1557 Nov 29 2017 test.cer
-rw-r--r--@ 1 Nana staff 460 Feb 12 2018 volog.log
Hardiyana-ATSBs-MacBook-Pro:~ Nana$ █
```


JANA CSR – APACHE TOMCAT SINGLE DOMAIN

```
[Hardiyana-ATSBs-MacBook-Pro:~ Nana$ keytool -certreq -keyalg RSA -alias tomcat -file certrequest.csr -keystore orange.keystore ]
[Enter keystore password: ]
```

```
[Hardiyana-ATSBs-MacBook-Pro:~ Nana$ cat certrequest.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC6TCCAAdECAQAwDELMAkGA1UEBhMCTVxETAPBgNVBAGTCFNBG9w0BBAwT
DgYDVQQHEwdVbmtub3duMRUwEwYDVQQKDAxPcmFuZ2UgJiBDby4xEDA0BgNVBA
B1Vua25vd24xZzAVBgNVBAMTDnd3dy5vcmluZ2UuY29tMIIBIjANBgkqhkiG9w0
AQEFAAOCAQ8AMIIBCgKCAQEAg5X8nwxuUOMwPZFzVac55YqjuZKPFHU34w28/Owz
fxGtv3w2xM6E1+qQBoXOKVnb6++HgqmvvX1EvBnGIAANANhVQpeQh40q05NJsCp1
GP5DCy0ue+yJnmw1AqTxB93Bvon06UqhhbJP/yT3whUtKurhpkymEquU07U/Q9
B4BURbAnsVwuOncoH9i20t2sx+/lcInbhXePFRFLmU5+U+AY/vmAHF66tMDj+Ngg
ssArhy4Gg2E9kva8pX1X0nb8sYEWs8cDHCCSJEu7L1UDu1PpgQieseIPoT8EghSr
9gDPxRKdA010M4YYm4m9g+eF9S5/UBYwPBU7Cc6A0XtpGQIDAQABoDAwLgYJKoZI
hvcNAQkOMSEwHzAdBgNVHQ4EFgQUtPS7LzSPzrGKoZBwCrMY1QkkUwDQYJKoZI
hvcNAQELBQADggEBADUufFaFqecfrm/J5FpBePy09FbiwR0oMadDilucW0QAVogA
PUMSiorj79jJu+me5gvku1BHGbR+GAUwV0Y2dZREeXWln10sKyyYzWXLcU7RNLdo
7Y84nc0OzyAxxp+BwqlaB7kxHgQur2Iz9K+KbqzjJoWYS0nHU+KwkSPRDUY2Z7TA
NvgUXASg8eGLEcKtFN+w0sjlwDlcttJgixwVbbDQ7p2hnpCL7IPn/KgftU7gV+0e
GkOw4qV/aZIkZJi0sz6X0sam9kY9haTrnh/ekSUd1sfxM9p0FCQ/ur72jJ0ltV3S
73C+rbt2dbEITAAKQMPw+jfI6hg3//PS++ibpco=
-----END NEW CERTIFICATE REQUEST-----
```

CSR Information:

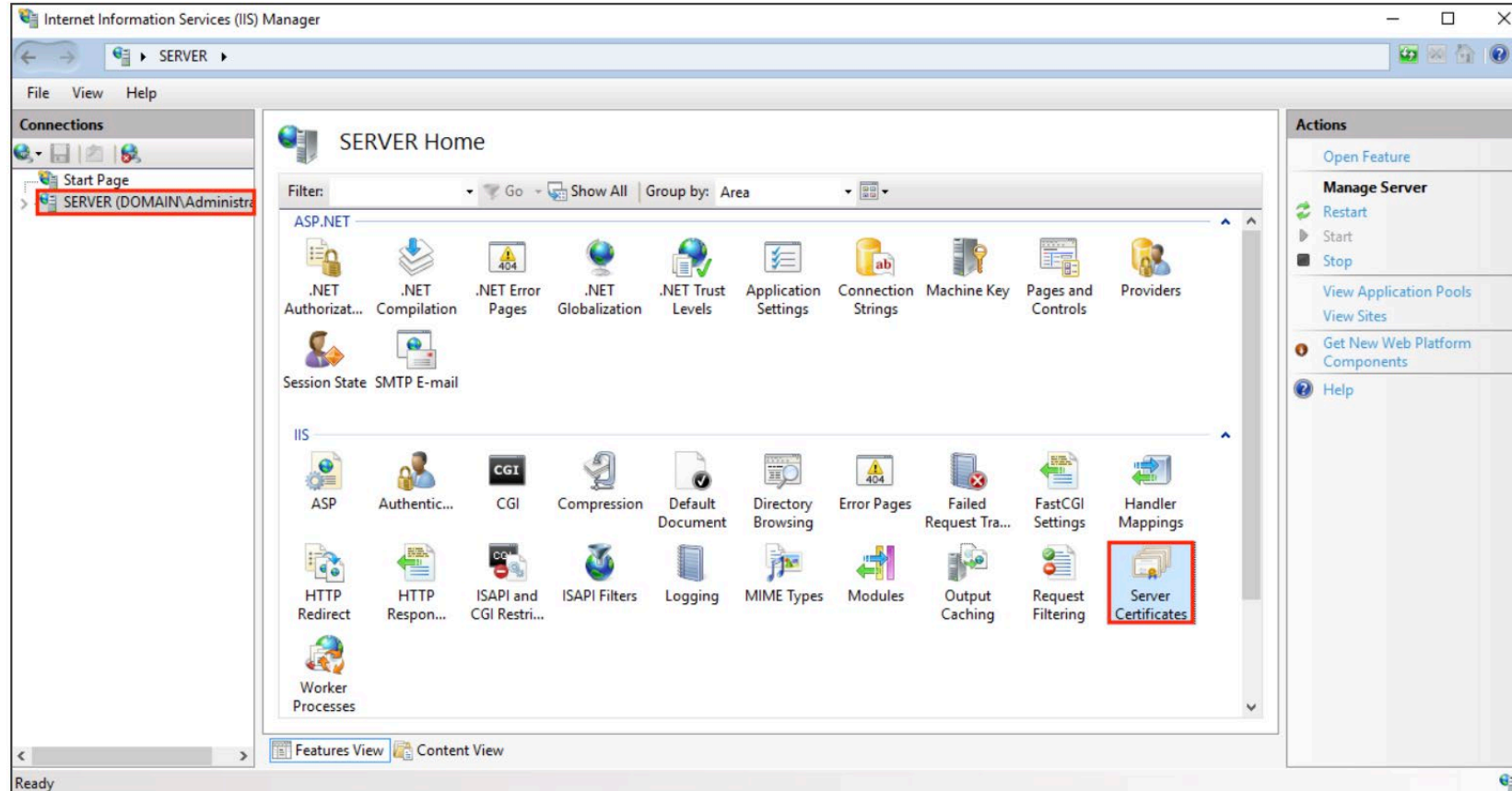
- ✓ Common Name: www.orange.com
- ✓ Organization: Orange & Co.
- ✓ Organization Unit: Unknown
- ✓ Locality: Unknown
- ✓ State: Selangor
- ✓ Country: MY

Fail CSR ini akan dihantar ke CA melalui portal GPKI.

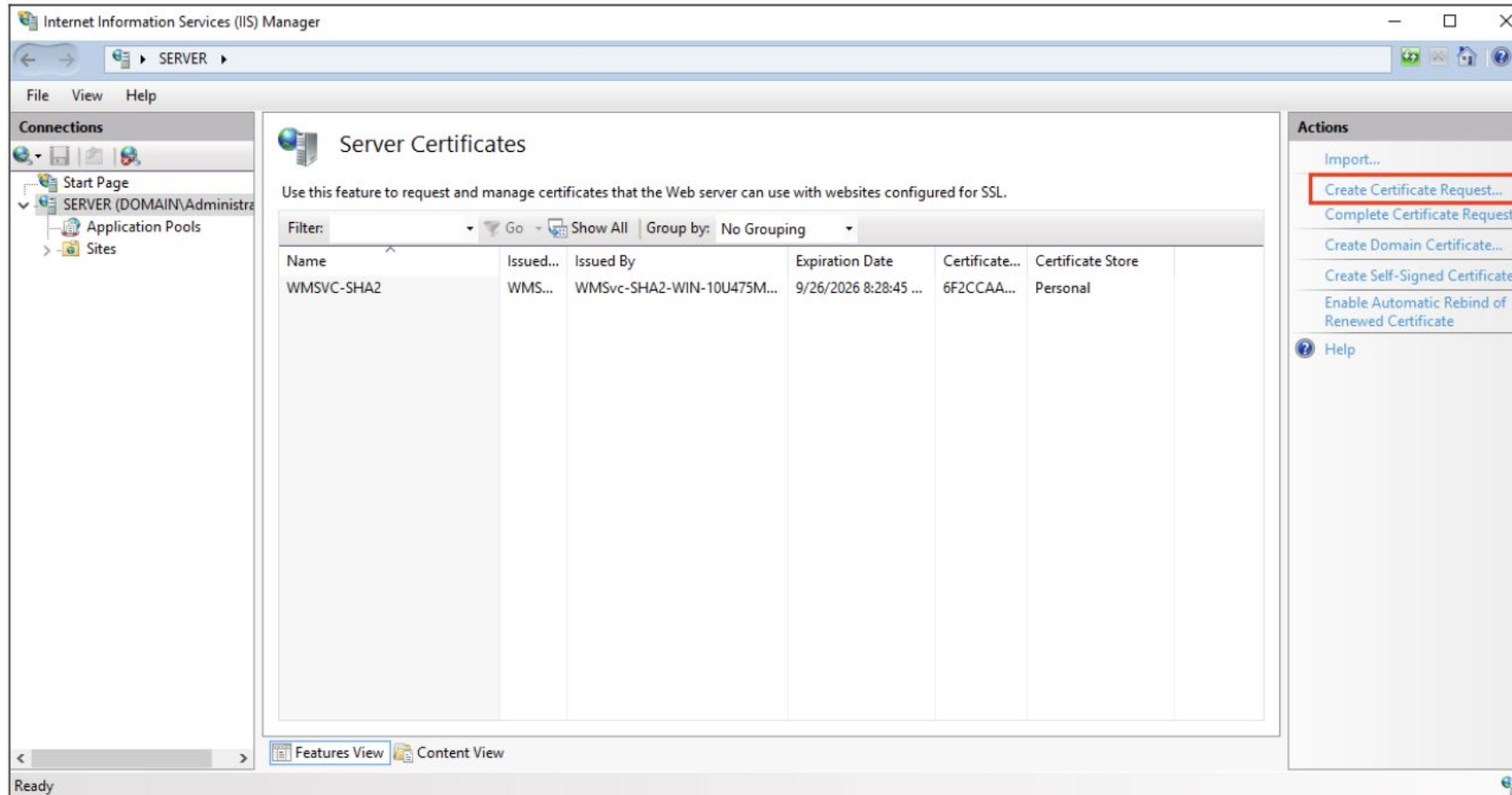
Penjanaan fail CSR bagi IIS (Single Domain dalam persekitaran Windows)

Langkah-langkah penjanaan CSR di IIS 10 menggunakan Windows Server 2016

- 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**



03 Pada menu *Actions* (right pane), klik *Create Certificate Request*



04 Lengkapi maklumat berikut:

Common Name <Nama domain>

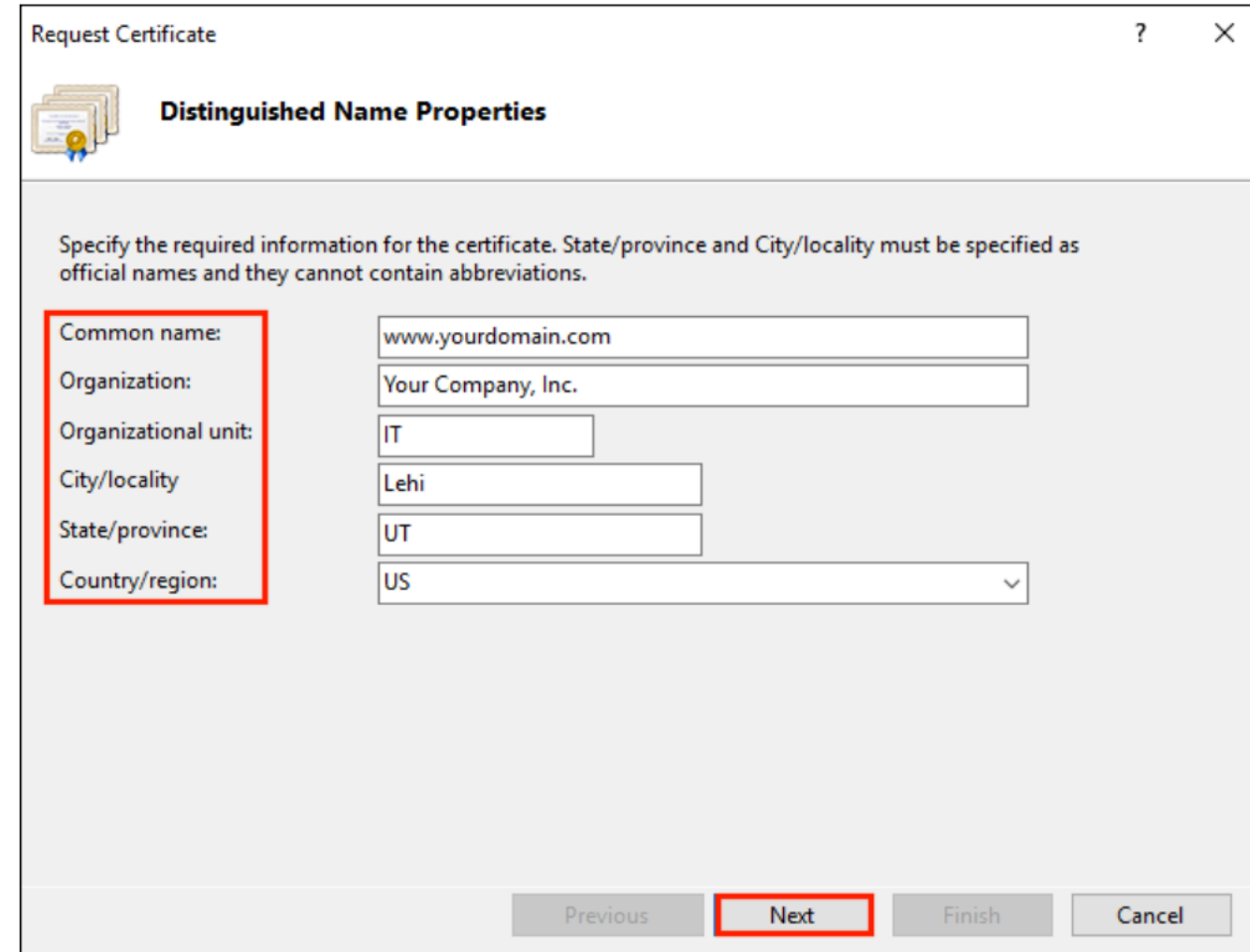
Organization <Nama organisasi>

Organization Unit <Unit organisasi>

City/locality <Bandar tempat organisasi didaftarkan>

State/province <Negeri tempat organisasi didaftarkan>

Country <Kod negara e.g: MY>



Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

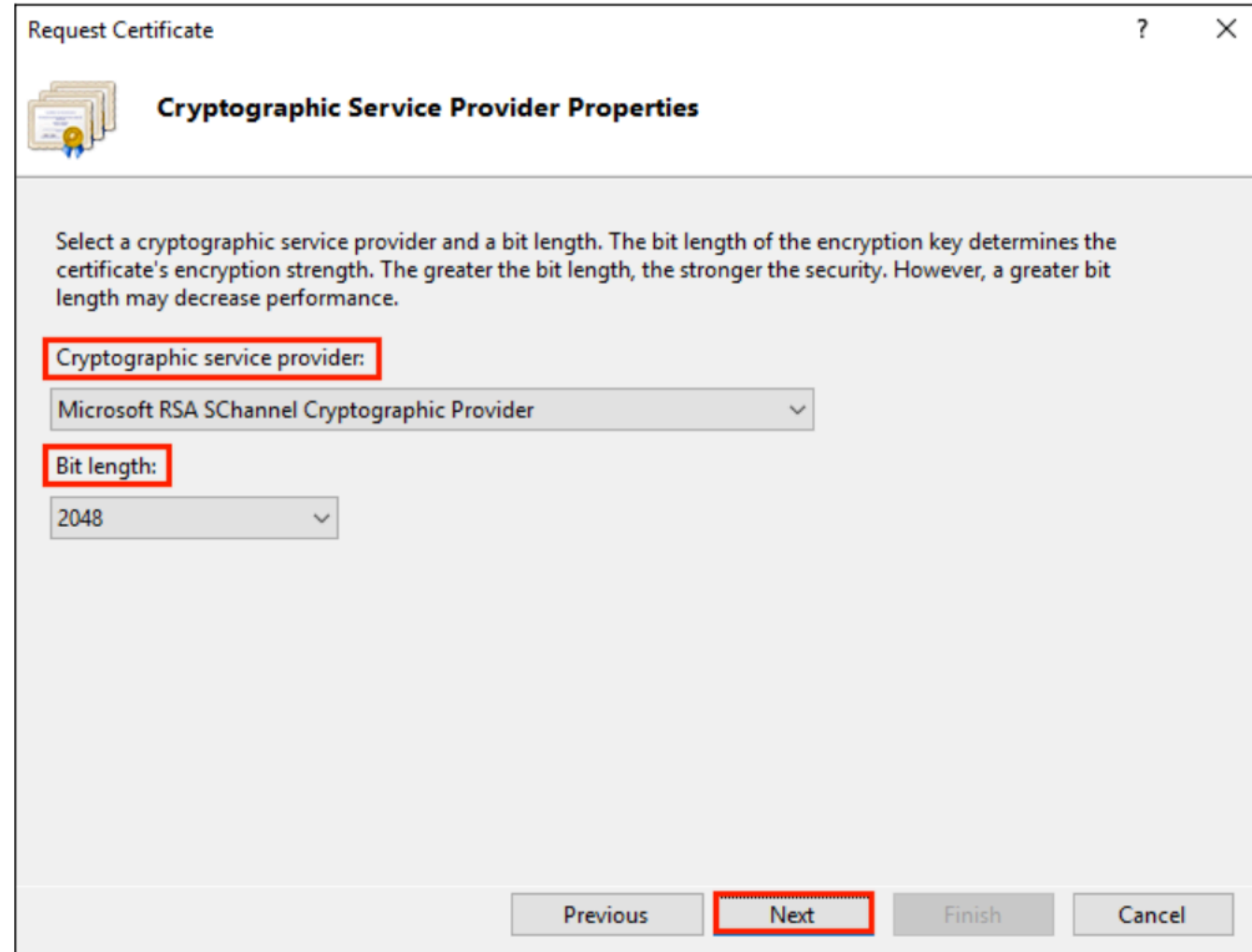
Common name:	www.yourdomain.com
Organization:	Your Company, Inc.
Organizational unit:	IT
City/locality	Lehi
State/province:	UT
Country/region:	US

Previous **Next** Finish Cancel

05 Lengkapkan maklumat seterusnya:

Cryptographic service provider - Pilih
Microsoft RSA SChannel Cryptographic
Provider

Bit length - 2048



Request Certificate

Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:
Microsoft RSA SChannel Cryptographic Provider

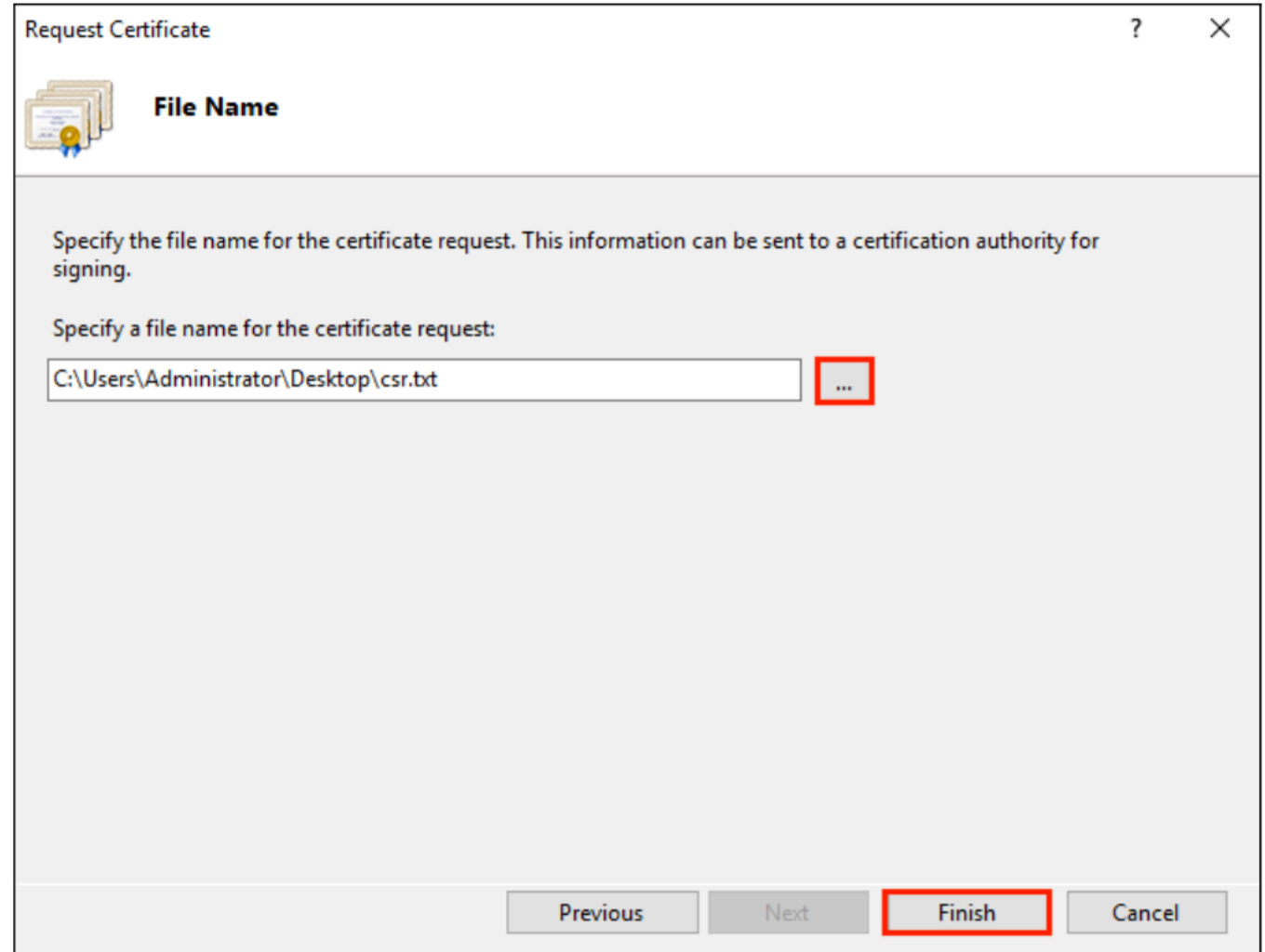
Bit length:
2048

Previous Next Finish Cancel


06 Lengkapi maklumat seterusnya:

Lengkapi nama fail dan lokasi fail untuk disimpan.

Seterusnya klik “Finish”.



Request Certificate

 **File Name**

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

C:\Users\Administrator\Desktop\csr.txt

...

Previous Next **Finish** Cancel

07 Paparan CSR seperti berikut:

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIICvDCCAAQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJITdGF0ZTER  
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t  
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG  
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32  
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0  
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEoX4VvALBOMLHVrB5/vhYfGECLJbc31  
RdEbdXyHDtHk1RAoIVQCfjTwBwGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywgwx  
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf  
m6rMEYm9o65j7vEYaKEJU0JtA5MIz/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ  
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB  
/qdTYR+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEb08GA0Fc4rw  
ix7vb15vSXE3shGijRGIzzHVGRoR3r7xQtIuMaDar3x1V8jHbcvZTcpx0Kbq6H1G  
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk  
M2eDsvPhMx/pENGBnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI  
obf5ziuNm1Df24NBt5tpCNzfGviKT6/Ryfwg3dMaKxc=  
-----END NEW CERTIFICATE REQUEST-----
```

08 CSR dihantar ke CA untuk tujuan pengeluaran sijil SSL.

Penjanaan fail CSR bagi Apache Server (Multidomain)

Langkah-langkah penjaan CSR multidomain melalui **OpenSSL**

01 Secara amnya, OpenSSL menggunakan konfigurasi seperti di dalam fail:

```
/etc/ssl/openssl.cnf
```

02 Bagi konfigurasi ke atas lebih dari satu pelayan, laksanakan proses salinan fail konfigurasi seperti berikut:

```
cp /etc/ssl/openssl.cnf /var/www/latihan.com/cert/latihan.com.cnf
```

03 Edit fail konfigurasi `/var/www/latihan.com/cert/latihan.com.cnf` di bahagian `[req]` .

04 *Uncomment* `req_extensions = v3_req`

Tambah maklumat berikut `subjectAltName = @alt_names`
di bahagian `[v3_req]` . Perubahan adalah seperti berikut:

```
[ v3_req ]  
# Extensions to add to a certificate request  
basicConstraints = CA:FALSE  
keyUsage = nonRepudiation, digitalSignature, keyEncipherment  
subjectAltName = @alt_names
```

05 Tambah bahagian `[alt_names]` seperti berikut:

```
[ alt_names ]  
DNS.1 = www.latihan.com  
DNS.2 = training.com
```

01 Tukar direktori ke cert folder

```
cd /var/www/latihan.com/cert/
```

02 Laksanakan *command* berikut untuk jana *private key*

```
openssl genrsa -out latihan.com.key 2048
```

03 Laksanakan *command* berikut untuk jana CSR

```
openssl req -new -key latihan.com.key -out latihan.com.csr -  
config latihan.com.cnf
```

04 Laksanakan *command* berikut untuk *verify* CSR

```
openssl req -in latihan.com.csr -noout -text
```

Terima Kasih