《使用 OpenSSL 建立自簽根憑證與簽發終端憑證指南》

➢ 自簽根憑證產生步驟

https://blog.miniasp.com/post/2019/02/25/Creating-Self-signed-Certificate-using-OpenSSL

Organization Name (eg, company) ===> Executive Yuan

Organizational Unit Name (eg, section) ===> Ministry of Digital Affairs

Organizational Unit Name (eg, section) ===> Ministry of Digital Affairs Root Certification Authority - G1

- ✓ 本文件操作需使用 Windows OpenSSL，故請先至以下連結下載 Windows OpenSSL 安裝才能操作。
  https://slproweb.com/products/Win32OpenSSL.html
- ✓ 調整 openssl\bin 目錄下 openssl.cfg (已改好的檔為 openssl_RootCAPRofile.cfg, 可將 openssl_RootCAPRofile.cfg 改檔名 openssl.cfg 直接使用, 但預設組織及預設組織單位為前述 Executive Yuan 及 Ministry of Digital Affairs, 可自行在用記事本打開修改預設組織及預設組織單位)

  ※ 將 stateOrProvinceName, commonName, emailAddress 這三項前加#註記掉

```
# For the CA policy
[ policy_match ]
countryName              = match
#stateOrProvinceName     = match
organizationName         = match
organizationalUnitName   = optional
#commonName              = supplied
#emailAddress            = optional
```

```
# For the CA policy
[ policy_match ]
countryName              = match
#stateOrProvinceName     = match
organizationName         = match
organizationalUnitName   = optional
#commonName              = supplied
#emailAddress            = optional
```

※ 將 countryName_default, stateOrProvinceName, stateOrProvinceName_default, localityName, 0.organizationName_default, commonName, emailAddress 這六項前加#註記掉; organizationalUnitName 改為 0.organizationalUnitName; organizationName_default 改為 0.organizationName_default 加入機關名稱; 新增 1.organizationalUnitName; 新增 1.organizationalUnitName_default 加入單位名稱。

```
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
#countryName_default            = AU
countryName_default             = TW
countryName_min                 = 2
countryName_max                 = 2

#stateOrProvinceName            = State or Province Name (full name)
#stateOrProvinceName_default    = Some-State

#localityName                   = Locality Name (eg, city)

0.organizationName              = Organization Name (eg, company)
#0.organizationName_default     = Internet Widgits Pty Ltd
0.organizationName_default      = Executive Yuan

# we can do this but it is not needed normally :-)
#1.organizationName             = Second Organization Name (eg, company)
#1.organizationName_default     = World Wide Web Pty Ltd

0.organizationalUnitName        = Organizational Unit Name (eg, section)
#organizationalUnitName_default  =
0.organizationalUnitName_default = Ministry of Digital Affairs Root

1.organizationalUnitName        = Organizational Unit Name (eg, section)
1.organizationalUnitName_default = Ministry of Digital Affairs Root
Certification Authority - G1

#commonName                     = Common Name (e.g. server FQDN or YOUR
name)
commonName_max                  = 64
```

```
#emailAddress                    = Email Address
emailAddress_max                 = 64
```

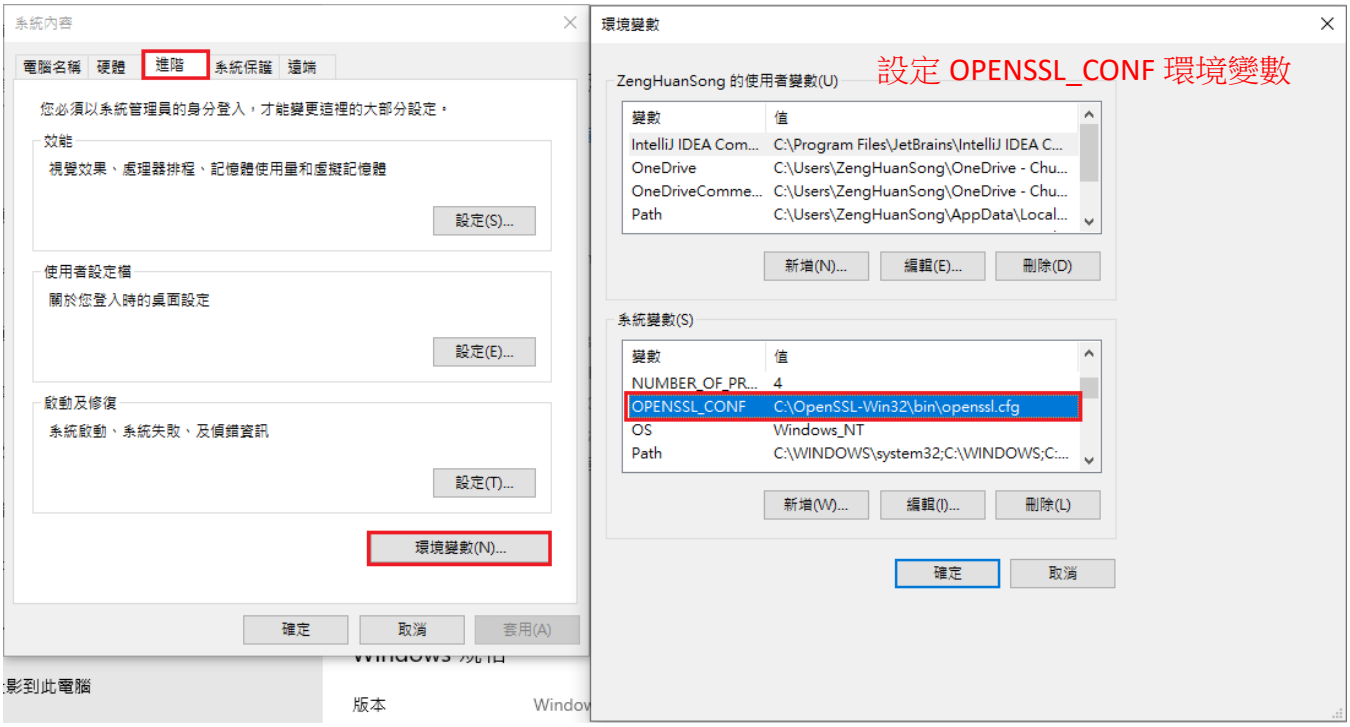
```
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
#countryName_default            = AU
countryName_default             = TW
countryName_min                 = 2
countryName_max                 = 2

#stateOrProvinceName            = State or Province Name (full name)
#stateOrProvinceName_default    = Some-State

#localityName                   = Locality Name (eg, city)

0.organizationName              = Organization Name (eg, company)
#0.organizationName_default     = Internet Widgits Pty Ltd
0.organizationName_default      = Executive Yuan

# we can do this but it is not needed normally :-)
#1.organizationName             = Second Organization Name (eg, company)
#1.organizationName_default     = World Wide Web Pty Ltd

0.organizationalUnitName                = Organizational Unit Name (eg, section)
#0.organizationalUnitName_default       =
0.organizationalUnitName_default        = Ministry of Digital Affairs

1.organizationalUnitName                = Organizational Unit Name (eg, section)
1.organizationalUnitName_default        = Ministry of Digital Affairs Root Certification Authority - G1

#commonName                     = Common Name (e.g. server FQDN or YOUR name)
commonName_max                  = 64

#emailAddress                   = Email Address
emailAddress_max                = 64
```

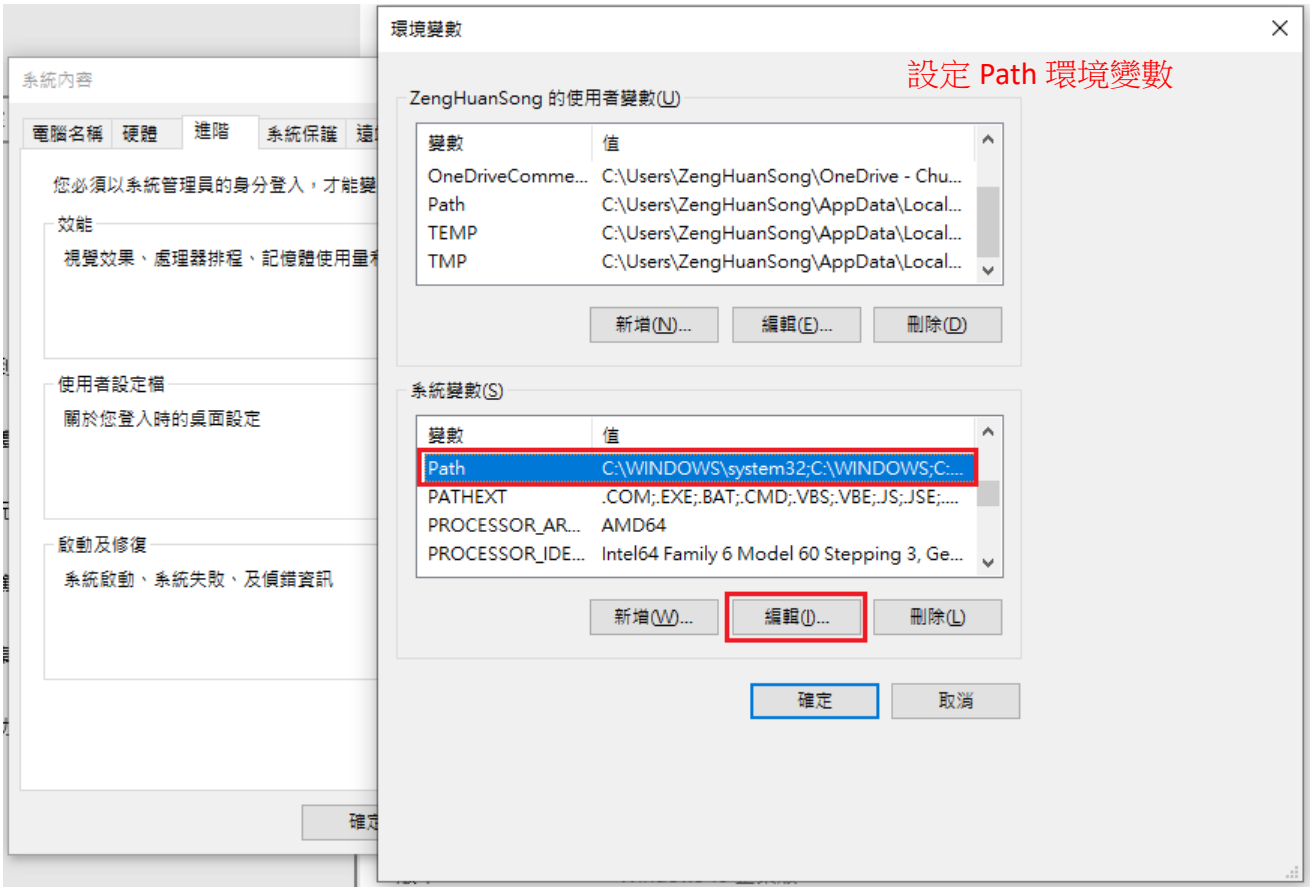
※ 將 authorityKeyIdentifier 這項前加#註記掉；新增 keyUsage 並加入 digitalSignature

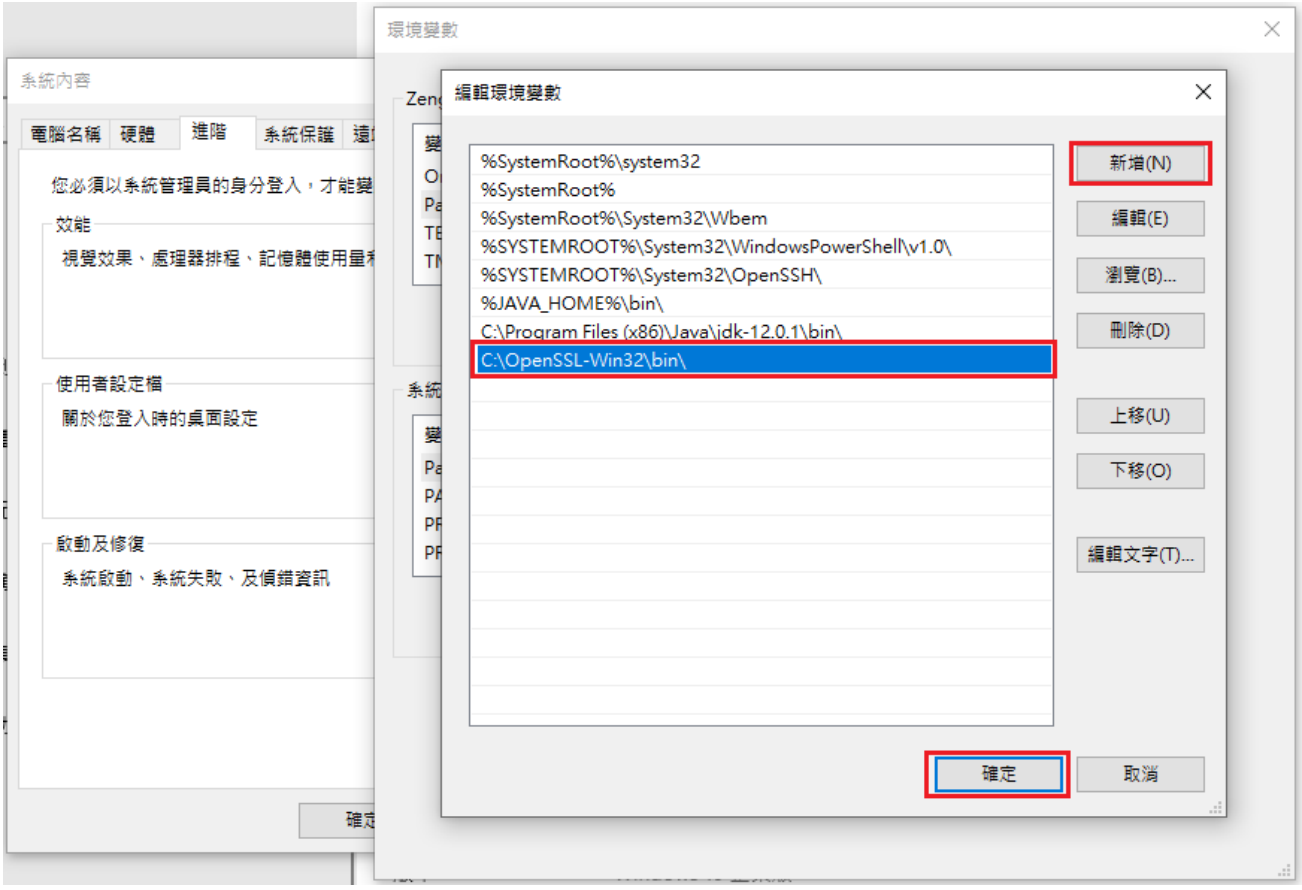
```
[ v3_ca ]
# Extensions for a typical CA
# PKIX recommendation.
subjectKeyIdentifier=hash
# authorityKeyIdentifier=keyid:always,issuer
.
.
.
# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
# keyUsage = cRLSign, keyCertSign
keyUsage = digitalSignature, cRLSign, keyCertSign
```

```
[ v3_ca ]

# Extensions for a typical CA

# PKIX recommendation.

subjectKeyIdentifier=hash

# authorityKeyIdentifier=keyid:always,issuer

# This is what PKIX recommends but some broken software chokes on critical
# extensions.
#basicConstraints = critical,CA:true
# So we do this instead.
basicConstraints = CA:true

# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
# keyUsage = cRLSign, keyCertSign
keyUsage = digitalSignature, cRLSign, keyCertSign
```

- ✓ 打開 命令提示字元 執行以下指令
- ✓ C:\WINDOWS\system32>**cd C:\OpenSSL-Win32\bin**
- ✓ C:\OpenSSL-Win32\bin>**mkdir MODA**
- ✓ C:\OpenSSL-Win32\bin>**cd MODA**
- ✓ C:\OpenSSL-Win32\bin\MODA>**openssl req -x509 -new -nodes -sha256 -utf8 -days 3650 -newkey rsa:4096 -keyout MODARoot.key -out MODARoot.crt**
- ✓ 若有組織有架設 Windows Active Directory (AD)環境，可先將根憑證 MODARoot.crt 匯入 AD 主機中，用派送的方式將根憑證 MODARoot.crt 派送至各個終端電腦中，即可讓所有控管的終端電腦信賴簽發出來的自簽根憑證；若沒有架設 Windows Active Directory (AD)環境，則只能至需要信賴憑證的終端電腦匯入自簽根憑證，可參考後面在 Windows 植入簽發出來的根憑證指令在需要信賴憑證的終端進行匯入動作。
  - ※ 若沒有設定環境變數，執行 openssl 有可能會出現 'openssl' 不是內部或外部命令、可執行的程式或批次檔。。請在 Windows 設定 -> 系統 -> 左邊選項最下方 關於 -> 右邊選項 進階系統設定，設定 OPENSSL_CONF 及 path 環境變數。
  - ※ 若沒有設定環境變數，可用指定 openssl.exe 程式全路徑並指定 openssl.cfg 檔案位置執行，如 C:\OpenSSL-Win32\bin\MODA> **"C:\OpenSSL-Win32\bin\openssl.exe" req -config "C:\OpenSSL-Win32\bin\openssl.cfg" -x509 -new -nodes -sha256 -utf8 -days 3650 -newkey rsa:4096 -keyout MODARoot.key -out MODARoot.crt**
  - ※ -days 3650 為簽發憑證效期天數約 10 年，3650 可自行調整。
  - ※ 若單位內有嚴格的資安管控，如 Active Directory (AD)，建議安裝 OpenSSL 時將 OpenSSL 在本機可以控管的目錄下，否則在操作上要放 openssl.cfg 檔案或改檔名需要由管理者開放權限，操作上會比較麻煩。




設定 Path 環境變數
環境變數
系統內容
電腦名稱
硬體
進階
系統保護
您必須以系統管理員的身分登入，才能變
效能
視覺效果、處理器排程、記憶體使用量
使用者設定檔
關於您登入時的桌面設定
啟動及修復
系統啟動、系統失敗、及偵錯資訊
ZengHuanSong 的使用者變數(U)
變數
值
OneDriveComme...
C:\Users\ZengHuanSong\OneDrive - Chu...
Path
C:\Users\ZengHuanSong\AppData\Local...
TEMP
C:\Users\ZengHuanSong\AppData\Local...
TMP
C:\Users\ZengHuanSong\AppData\Local...
新增(N)...
編輯(E)...
刪除(D)
系統變數(S)
變數
值
Path
C:\WINDOWS\system32;C:\WINDOWS;C:...
PATHEXT
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;...
PROCESSOR_AR...
AMD64
PROCESSOR_IDE...
Intel64 Family 6 Model 60 Stepping 3, Ge...
新增(W)...
編輯(I)...
刪除(L)
確定
取消


環境變數
系統內容
電腦名稱
硬體
進階
系統保護
您必須以系統管理員的身分登入，才能變
效能
視覺效果、處理器排程、記憶體使用量
使用者設定檔
關於您登入時的桌面設定
啟動及修復
系統啟動、系統失敗、及偵錯資訊
編輯環境變數
%SystemRoot%\system32
%SystemRoot%
%SystemRoot%\System32\Wbem
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
%SYSTEMROOT%\System32\OpenSSH\
%JAVA_HOME%\bin\
C:\Program Files (x86)\Java\jdk-12.0.1\bin\
C:\OpenSSL-Win32\bin\
新增(N)
編輯(E)
瀏覽(B)...
刪除(D)
上移(U)
下移(O)
編輯文字(T)...
確定
取消

系統管理員: 命令提示字元

```
Microsoft Windows [版本 10.0.19045.5487]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\WINDOWS\system32>cd C:\OpenSSL-Win32\bin

C:\OpenSSL-Win32\bin>mkdir MODA

C:\OpenSSL-Win32\bin>cd MODA

C:\OpenSSL-Win32\bin\MODA>openssl req -x509 -new -nodes -sha256 -utf8 -days 3650 -newkey rsa:4096 -keyout MODARoot.key -out MODARoot.crt
Loading 'screen' into random state - done
Generating a 4096 bit RSA private key
...++
.++
writing new private key to 'MODARoot.key'
-----
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) [TW]:
Organization Name (eg, company) [Executive Yuan]:
Organizational Unit Name (eg, section) [Ministry of Digital Affairs]:
Organizational Unit Name (eg, section) [Ministry of Digital Affairs Root Certification Authority - G1]:

C:\OpenSSL-Win32\bin\MODA>
```

憑證

一般 | 詳細資料 | 憑證路徑

顯示(S): <全部>

欄位	值
版本號	V3
序號	00f5b2d5a3229bf9bf
簽章演算法	sha256RSA
簽章雜湊演算法	sha256
簽發者	Ministry of Digital Affairs Root Certification Authorit
有效期自	2025年3月17日 下午 05:25:32
有效期到	2035年3月15日 下午 05:25:32

OU = Ministry of Digital Affairs Root Certification Authority - G1
OU = Ministry of Digital Affairs
O = Executive Yuan
C = TW

編輯內容(E)... 複製到檔案(C)...

確定

憑證

一般 | 詳細資料 | 憑證路徑

顯示(S): <全部>

欄位	值
主體	Ministry of Digital Affairs Root Certification Authorit
公開金鑰	RSA (4096 Bits)
公開金鑰參數	05 00
主體金鑰識別碼	d246d51fc0a8cd83418e77826124c4b5f0d65065
基本限制	Subject Type=CA, Path Length Constraint=None
金鑰使用方法	Digital Signature, Certificate Signing, Off-line CRL S
憑證指紋	693e28971c494ab394a4b7377309567157dffe85

Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

編輯內容(E)... 複製到檔案(C)...

確定

➢ 以自簽根憑證簽發下屬終端憑證步驟

https://blog.davy.tw/posts/use-openssl-to-sign-intermediate-ca/

Organization Name (eg, company) ===> Executive Yuan

Organizational Unit Name (eg, section) ===> Ministry Of Digital Affairs

Common Name (e.g. server FQDN or YOUR name) ===> www.moda.gov.tw

✓ 調整 openssl\bin 目錄下 openssl.cfg (已改好的檔為 openssl_EndEntityProfile.cfg, 可將 openssl_EndEntityProfile.cfg 改檔名 openssl.cfg 直接使用, 但預設組織及預設組織單位為前述 Executive Yuan 及 Ministry of Digital Affairs, 可自行在用記事本打開修改預設組織及預設組織單位)

※ 將 dir 前加#註記掉; 新增 dir = .; 將 new_certs_dir 前加#註記掉; 新增 new_certs_dir = $dir

```
[ CA_default ]

#dir            = ./demoCA              # Where everything is kept
dir             = .                     # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject = no                    # Set to 'no' to allow creation of
                                        # several ctificates with same subject.
#new_certs_dir  = $dir/newcerts         # default place for new certs.
new_certs_dir   = $dir

certificate     = $dir/cacert.pem       # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem# The private key
RANDFILE        = $dir/private/.rand    # private random number file

x509_extensions = usr_cert              # The extentions to add to the cert
```

※ 將 commonName 前加註的#取消

```
# For the CA policy
[ policy_match ]
countryName             = match
#stateOrProvinceName    = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
#emailAddress           = optional
```

```
# For the CA policy
[ policy_match ]
countryName             = match
#stateOrProvinceName    = match
organizationName        = match
organizationalUnitName  = optional
```

```
commonName                      = supplied
#emailAddress                   = optional
```

※ 將 1.organizationalUnitName，1.organizationalUnitName_default 這兩項前加#註記掉；commonName 前加註的#取消

```
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
#countryName_default            = AU
countryName_default             = TW
countryName_min                 = 2
countryName_max                 = 2

#stateOrProvinceName            = State or Province Name (full name)
#stateOrProvinceName_default    = Some-State

#localityName                   = Locality Name (eg, city)

0.organizationName              = Organization Name (eg, company)
#0.organizationName_default     = Internet Widgits Pty Ltd
0.organizationName_default      = Executive Yuan

# we can do this but it is not needed normally :-)
#1.organizationName             = Second Organization Name (eg, company)
#1.organizationName_default     = World Wide Web Pty Ltd

0.organizationalUnitName                = Organizational Unit Name (eg, section)
#0.organizationalUnitName_default       =
0.organizationalUnitName_default        = Ministry Of Digital Affairs

#1.organizationalUnitName               = Organizational Unit Name (eg, section)
#1.organizationalUnitName_default       = Ministry Of Digital Affairs Root Certification Authority - G1

commonName                      = Common Name (e.g. server FQDN or YOUR name)
commonName_max                  = 64

#emailAddress                   = Email Address
emailAddress_max                = 64
```


```
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
#countryName_default            = AU
countryName_default             = TW
countryName_min                 = 2
countryName_max                 = 2

#stateOrProvinceName            = State or Province Name (full name)
#stateOrProvinceName_default    = Some-State

#localityName                   = Locality Name (eg, city)

0.organizationName              = Organization Name (eg, company)
#0.organizationName_default     = Internet Widgits Pty Ltd
0.organizationName_default      = Executive Yuan

# we can do this but it is not needed normally :-)
#1.organizationName             = Second Organization Name (eg, company)
#1.organizationName_default     = World Wide Web Pty Ltd
```

```
0.organizationalUnitName          = Organizational Unit Name (eg, section)
#organizationalUnitName_default   =
0.organizationalUnitName_default = Ministry Of Foreign Affairs Root

#1.organizationalUnitName         = Organizational Unit Name (eg, section)
#1.organizationalUnitName_default = Ministry Of Foreign Affairs Root
Certification Authority - G1

commonName                       = Common Name (e.g. server FQDN or YOUR
name)
commonName_max                    = 64

#emailAddress                     = Email Address
emailAddress_max                  = 64
```

※ 將 usr_cert 加入 # PKIX recommendations harmless if included in all certificates. …… extendedKeyUsage = critical,serverAuth,clientAuth 這個區段內容; 將 basicConstraints 前加#註記掉; # This is typical in keyUsage for a client certificate. # keyUsage = nonRepudiation, digitalSignature, keyEncipherment 這兩行刪除; nsComment 前加#註記掉; # PKIX recommendations harmless if included in all certificates. # subjectKeyIdentifier=hash # authorityKeyIdentifier=keyid,issuer 這兩行刪除; # This is required for TSA certificates. # extendedKeyUsage = critical,timeStamping 這兩行刪除

```
[ usr_cert ]

# These extensions are added when 'ca' signs a request.

# PKIX recommendations harmless if included in all certificates.
authorityKeyIdentifier=keyid,issuer
subjectKeyIdentifier=hash

# authorityInfoAccess = caIssuers;URI:https://www.moda.gov.tw/MOFARootCA.p7b

certificatePolicies = 2.16.886.101.0.3.3, 2.23.140.1.2.2

# multidomain certificate
subjectAltName  = @alt_names

# crlDistributionPoints = URI:http://www.moda.gov.tw/ca.crl

# This is typical in keyUsage for a client certificate.
# keyUsage = nonRepudiation, digitalSignature, keyEncipherment
keyUsage = critical, digitalSignature, keyEncipherment

# This is required for TSA certificates.
# extendedKeyUsage = critical,timeStamping
extendedKeyUsage = critical,serverAuth,clientAuth

# This goes against PKIX guidelines but some CAs do it and some software
# requires this to avoid interpreting an end user certificate as a CA.

# basicConstraints = CA:FALSE

# Here are some examples of the usage of nsCertType. If it is omitted
# the certificate can be used for anything *except* object signing.

# This is OK for an SSL server.
# nsCertType                      = server

# For an object signing certificate this would be used.
# nsCertType = objsign

# For normal client use this is typical
# nsCertType = client, email

# and for everything including object signing:
# nsCertType = client, email, objsign

# This will be displayed in Netscape's comment listbox.
# nsComment                       = "OpenSSL Generated Certificate"

# This stuff is for subjectAltName and issuerAltname.
# Import the email address.
# subjectAltName=email:copy
# An alternative to produce certificates that aren't
# deprecated according to PKIX.
# subjectAltName=email:move

# Copy subject details
# issuerAltName=issuer:copy

#nsCaRevocationUrl              = http://www.domain.dom/ca-crl.pem
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName
```

```
[ usr_cert ]

# These extensions are added when 'ca' signs a request.

# PKIX recommendations harmless if included in all certificates.
authorityKeyIdentifier=keyid,issuer
subjectKeyIdentifier=hash

# authorityInfoAccess =
caIssuers;URI:https://www.moda.gov.tw/MODARootCA.p7b

certificatePolicies = 2.16.886.101.0.3.3, 2.23.140.1.2.2

# multidomain certificate
subjectAltName  = @alt_names

# crlDistributionPoints = URI:http://www.moda.gov.tw/ca.crl

# This is typical in keyUsage for a client certificate.
# keyUsage = nonRepudiation, digitalSignature, keyEncipherment
keyUsage = critical, digitalSignature, keyEncipherment

# This is required for TSA certificates.
# extendedKeyUsage = critical,timeStamping
extendedKeyUsage = critical,serverAuth,clientAuth

# This goes against PKIX guidelines but some CAs do it and some software
# requires this to avoid interpreting an end user certificate as a CA.

# basicConstraints = CA:FALSE

# This is typical in keyUsage for a client certificate.
# keyUsage = nonRepudiation, digitalSignature, keyEncipherment

# This will be displayed in Netscape's comment listbox.
# nsComment             = "OpenSSL Generated Certificate"

# PKIX recommendations harmless if included in all certificates.
```

~~# subjectKeyIdentifier=hash~~
~~# authorityKeyIdentifier=keyid,issuer~~

.

.

.

~~# This is required for TSA certificates.~~
~~# extendedKeyUsage = critical,timestamping~~

※ 將keyUsage前加#註記掉；新增keyUsage = digitalSignature, keyEncipherment 及 subjectAltName = @alt_names 這兩行，並加入[alt_names]區段資料

```
[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
keyUsage = digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = www.moda.gov.tw
#IP.1 = 104.18.23.126
#email = service@moda.gov.tw
```

```
[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
keyUsage = digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = www.moda.gov.tw
#IP.1 = 203.66.32.136
#email = service@moda.gov.tw
```

※ 加入 certificatePolicies 及 Key usage …… keyUsage = critical, cRLSign, keyCertSign 區段; authorityKeyIdentifier 前加註的#取消; # Key usage: this is typical for a CA certificate. However since it will …… # keyUsage = digitalSignature, cRLSign, keyCertSign 這四行刪除

```
[ v3_ca ]

# Extensions for a typical CA

certificatePolicies = 2.16.886.101.0.3.3, 2.23.140.1.2.2

# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
# keyUsage = cRLSign, keyCertSign
# keyUsage = digitalSignature, cRLSign, keyCertSign
keyUsage = critical, cRLSign, keyCertSign

# PKIX recommendation.

subjectKeyIdentifier=hash

authorityKeyIdentifier=keyid:always,issuer

# This is what PKIX recommends but some broken software chokes on critical
# extensions.
#basicConstraints = critical,CA:true
# So we do this instead.
# basicConstraints = CA:true
basicConstraints=CA:TRUE,pathlen:0

# Some might want this also
# nsCertType = sslCA, emailCA

# Include email address in subject alt name: another PKIX recommendation
# subjectAltName=email:copy
# Copy issuer details
# issuerAltName=issuer:copy

# DER hex encoding of an extension: beware experts only!
# obj=DER:02:03
# Where 'obj' is a standard or added object
# You can even override a supported extension:
# basicConstraints= critical. DER:30:03:01:01:FF
```

```
[ v3_ca ]

# Extensions for a typical CA

certificatePolicies = 2.16.886.101.0.3.3, 2.23.140.1.2.2

# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
# keyUsage = cRLSign, keyCertSign
# keyUsage = digitalSignature, cRLSign, keyCertSign
keyUsage = critical, cRLSign, keyCertSign

# PKIX recommendation.

subjectKeyIdentifier=hash

authorityKeyIdentifier=keyid:always,issuer

# This is what PKIX recommends but some broken software chokes on critical
# extensions.
#basicConstraints = critical,CA:true
# So we do this instead.
# basicConstraints = CA:true
basicConstraints=CA:TRUE,pathlen:0

# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
# keyUsage = cRLSign, keyCertSign
# keyUsage = digitalSignature, cRLSign, keyCertSign
```

- ✓ C:\OpenSSL-Win32\bin\MODA>**openssl genrsa -out server.key 4096**
- ✓ C:\OpenSSL-Win32\bin\MODA>**openssl req -sha256 -new -key server.key -out server.csr**
- ✓ C:\OpenSSL-Win32\bin\MODA>**openssl ca -in server.csr -cert MODARoot.crt -keyfile MODARoot.Key -out server.crt -days 3652**
- ✓ ……Certificate is to be certified until Mar 17 09:52:16 2035 GMT (3652 days)
  Sign the certificate? [y/n]:**y**
- ✓ 1 out of 1 certificate requests certified, commit? [y/n]**y**

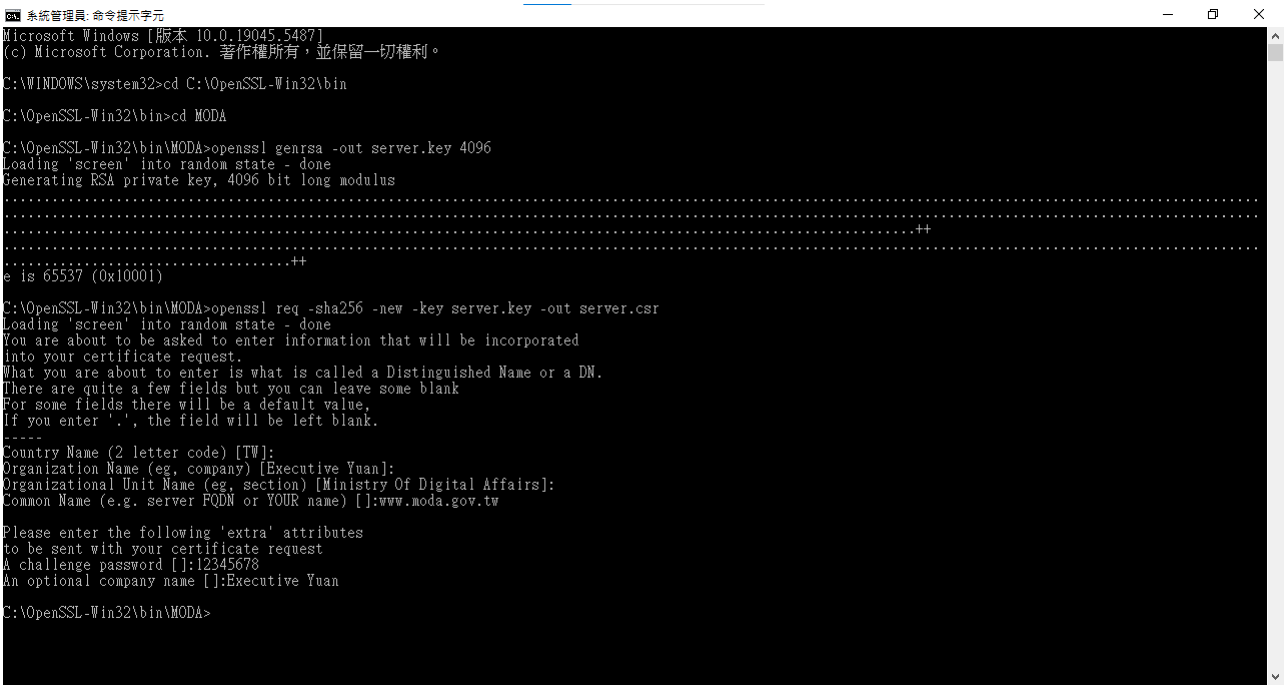
※ 若沒有設定環境變數，可用指定 openssl.exe 程式全路徑並指定 openssl.cfg 檔案位置執行，如

C:\OpenSSL-Win32\bin\MODA>**"C:\OpenSSL-Win32\bin\openssl.exe" genrsa -out server.key 4096**

C:\OpenSSL-Win32\bin\MODA>**"C:\OpenSSL-Win32\bin\openssl.exe" req -config "C:\OpenSSL-Win32\bin\openssl.cfg" -sha256 -new -key server.key -out server.csr**

C:\OpenSSL-Win32\bin\MODA>**"C:\OpenSSL-Win32\bin\openssl.exe" ca -config "C:\OpenSSL-Win32\bin\openssl.cfg" -in server.csr -cert MODARoot.crt -keyfile MODARoot.Key -out server.crt -days 3652**

※ 以上 server.key 及 server.pem，若簽多張，請用不同檔案取代，否則在相同目錄下執行會一直蓋檔過去。



系統管理員: 命令提示字元

```
C:\OpenSSL-Win32\bin\MODA>openssl ca -in server.csr -cert MODARoot.crt -keyfile MODARoot.Key -out server.crt -days 3652
Using configuration from C:\OpenSSL-Win32\bin\openssl.cfg
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            38:44:19:92:9e:52:9b:22:0a:58:d4:26:34:94:24:82
        Validity
            Not Before: Mar 17 09:52:16 2025 GMT
            Not After : Mar 17 09:52:16 2035 GMT
        Subject:
            countryName               = TW
            organizationName          = Executive Yuan
            organizationalUnitName    = Ministry Of Digital Affairs
            commonName                = www.moda.gov.tw
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:D2:46:D5:1F:C0:A8:CD:83:41:8E:77:82:61:24:C4:B5:F0:D6:50:65

            X509v3 Subject Key Identifier:
                D2:B8:4F:52:1E:73:D2:B7:4B:88:F0:CE:E0:01:59:A4:9B:F1:8F:57
            X509v3 Certificate Policies:
                Policy: 2.16.886.101.0.3.3
                Policy: 2.23.140.1.2.2

            X509v3 Subject Alternative Name:
                DNS:www.mofa.gov.tw
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage: critical
                TLS Web Server Authentication, TLS Web Client Authentication
Certificate is to be certified until Mar 17 09:52:16 2035 GMT (3652 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\OpenSSL-Win32\bin\MODA>
```

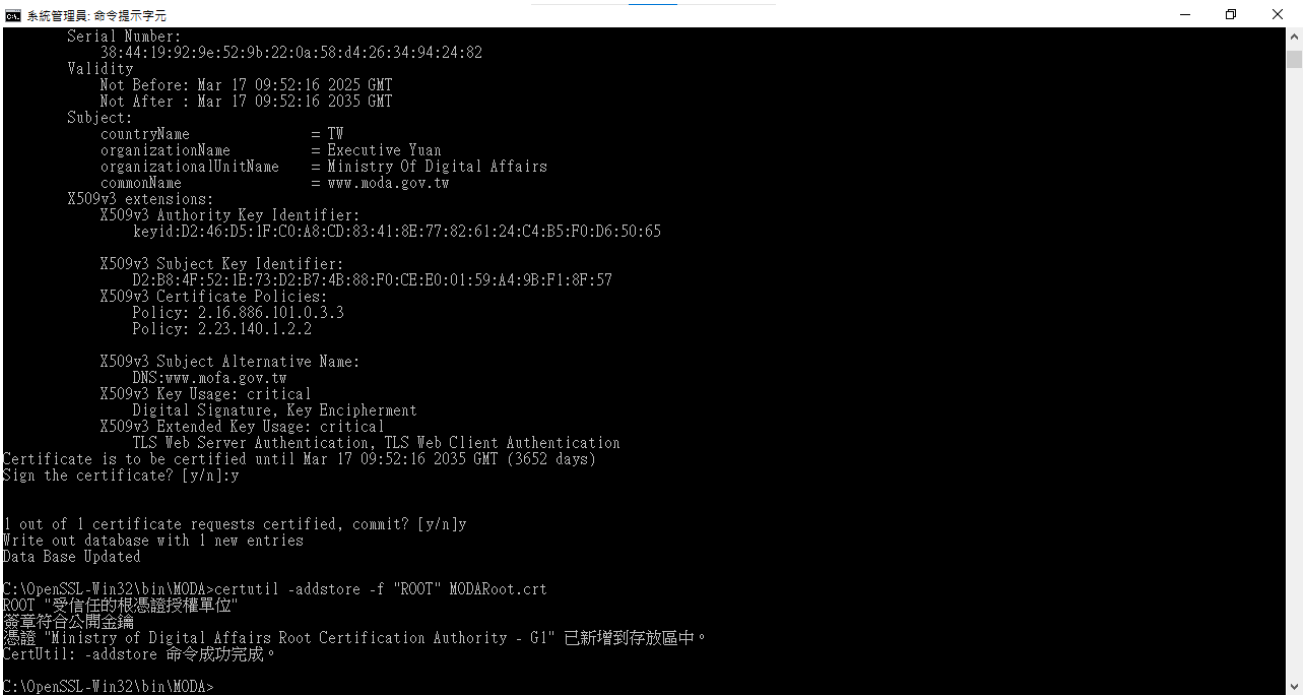
- 在 Windows 植入簽發出來的根憑證
  - ✓ C:\OpenSSL-Win32\bin\MODA>**certutil -addstore -f "ROOT" MODARoot.crt**

    ROOT "受信任的根憑證授權單位"

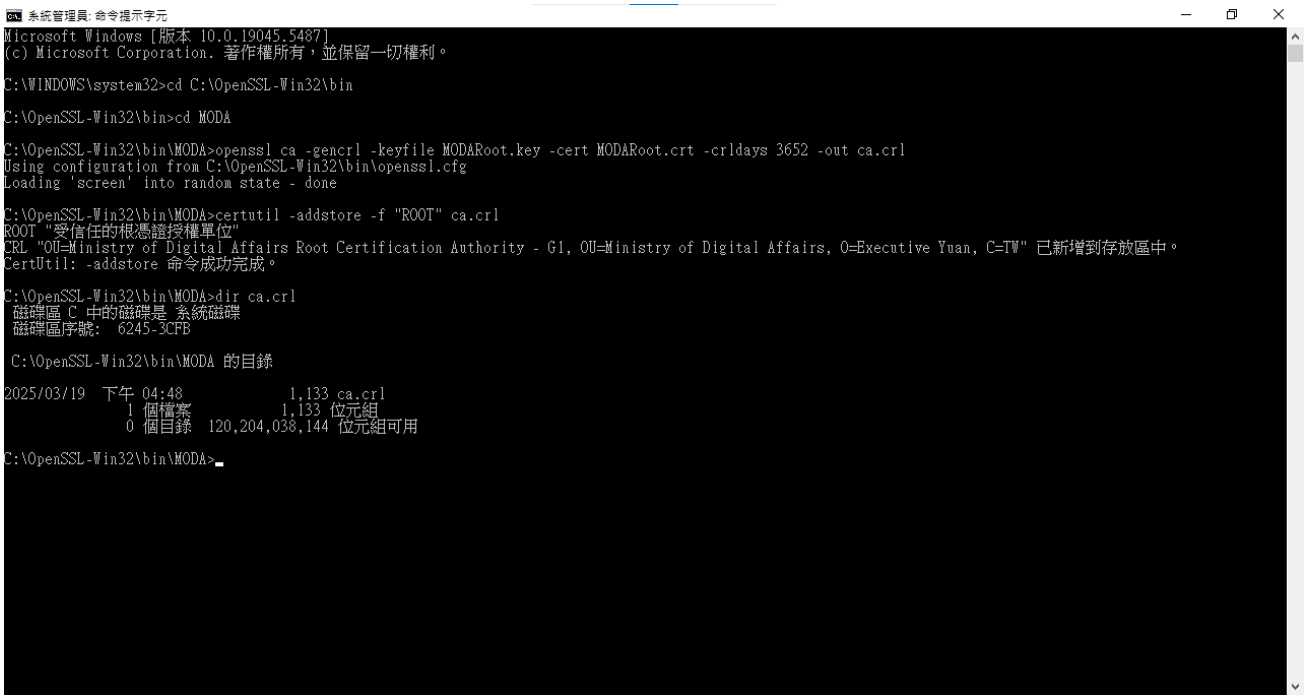
    簽章符合公開金鑰

    憑證 "Ministry of Digital Affairs Root Certification Authority" 已新增到存放區中。

    CertUtil: -addstore 命令成功完成。

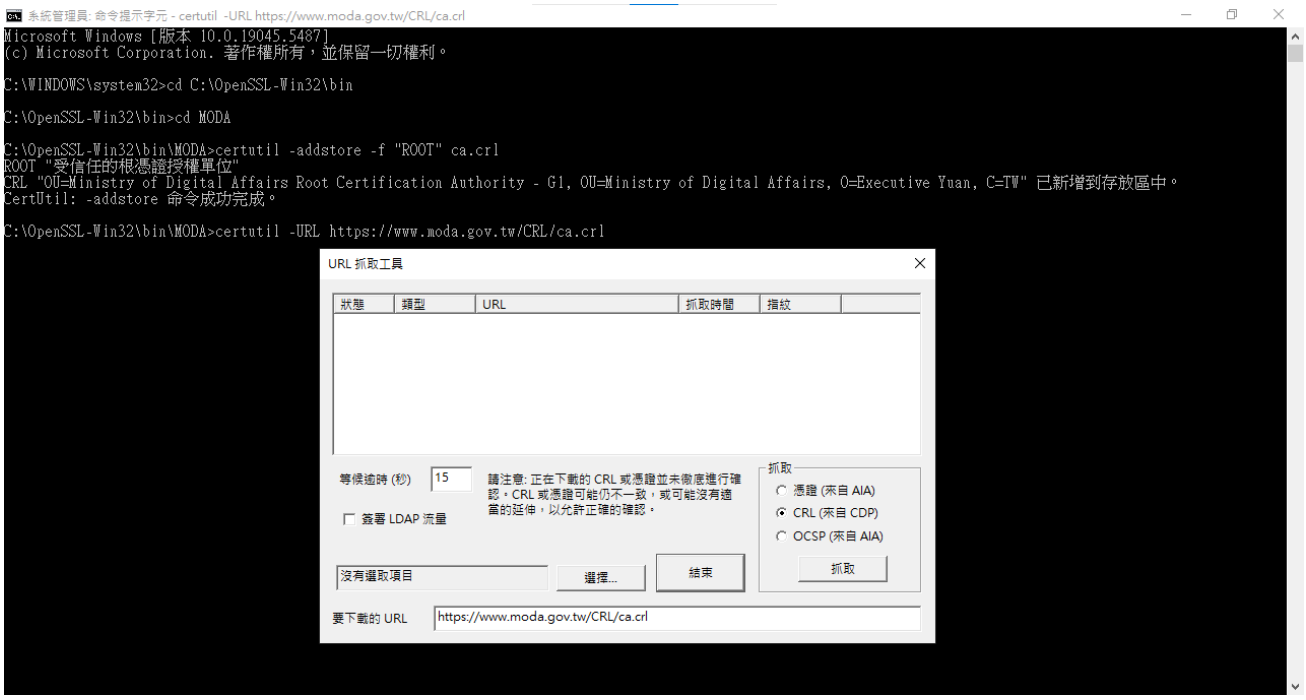


- 產製 ca.crl，在 Windows 植入憑證廢止清冊 ca.crl。
  - ✓ C:\OpenSSL-Win32\bin\MODA>**openssl ca -gencrl -keyfile MODARoot.key -cert MODARoot.crt -crldays 3652 -out ca.crl**
    Using configuration from C:\OpenSSL-Win32\bin\openssl.cfg
    Loading 'screen' into random state - done
    ※ -crldays 3650 為簽發憑證廢止清冊效期天數約 10 年，3650 可自行調整。
  - ✓ C:\OpenSSL-Win32\bin\MODA>**certutil -addstore -f "ROOT" ca.crl**
    ROOT "受信任的根憑證授權單位"
    CRL "OU=Ministry of Digital Affairs Root Certification Authority - G1, OU=Ministry of Digital Affairs, O=Executive Yuan, C=TW" 已新增到存放區中。
    CertUtil: -addstore 命令成功完成。

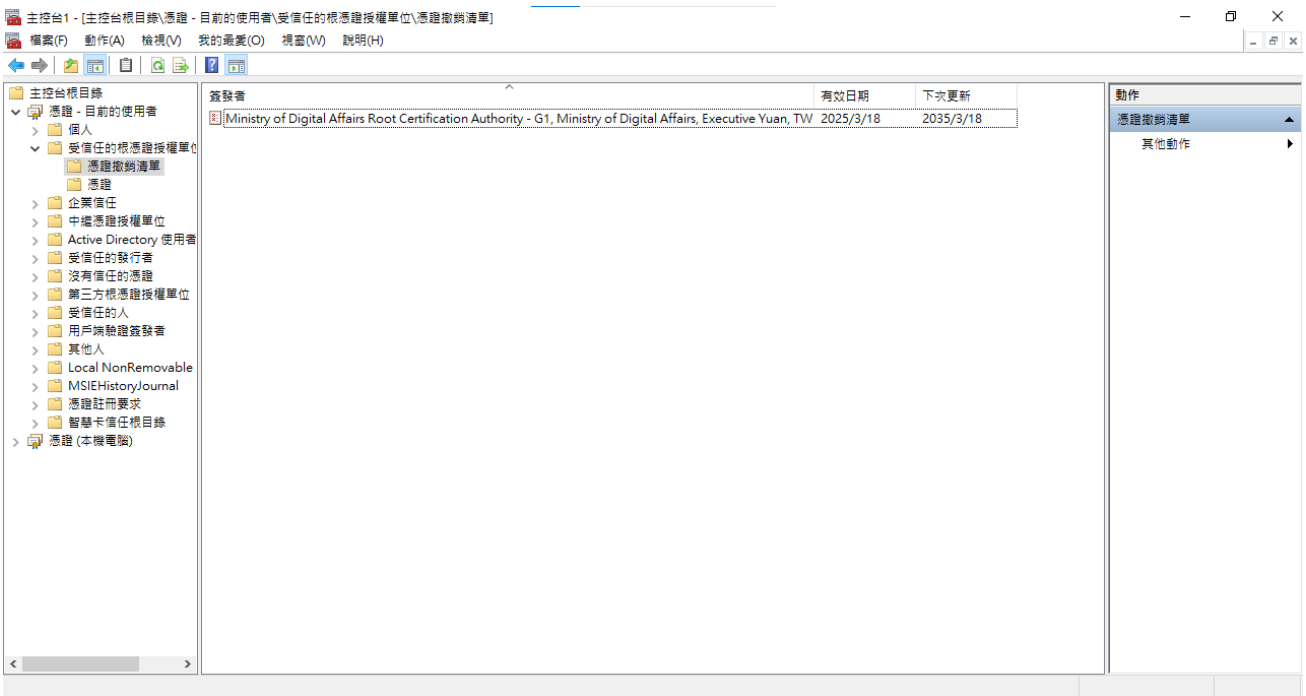


✓ C:\OpenSSL-Win32\bin\MODA>**certutil -URL https://www.moda.gov.tw/CRL/ca.crl**
CertUtil: -URL 命令成功完成。

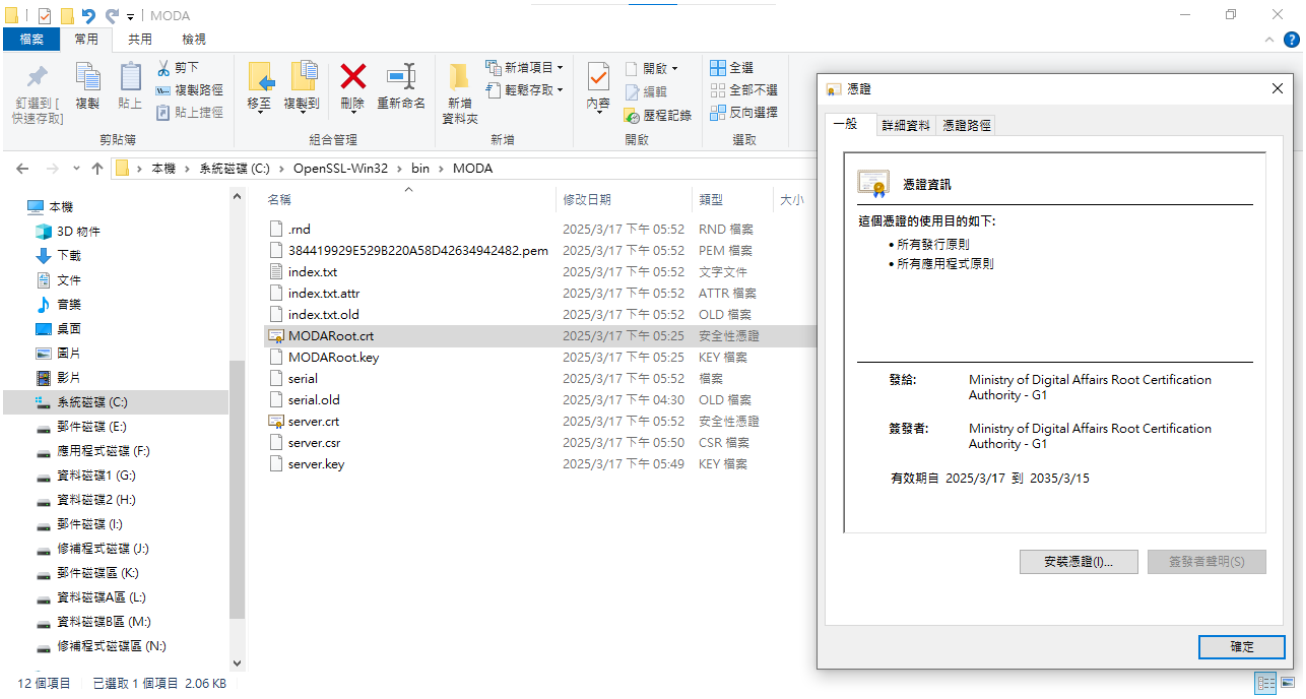
※ 請自行找一台內部主機放置產製出來的 ca.crl；上述指令自 FQDN 自行改為自己放置的內部主機 FQDN 或 IP；確認終端電腦可以透過 certutil -URL 抓取該 CRL。



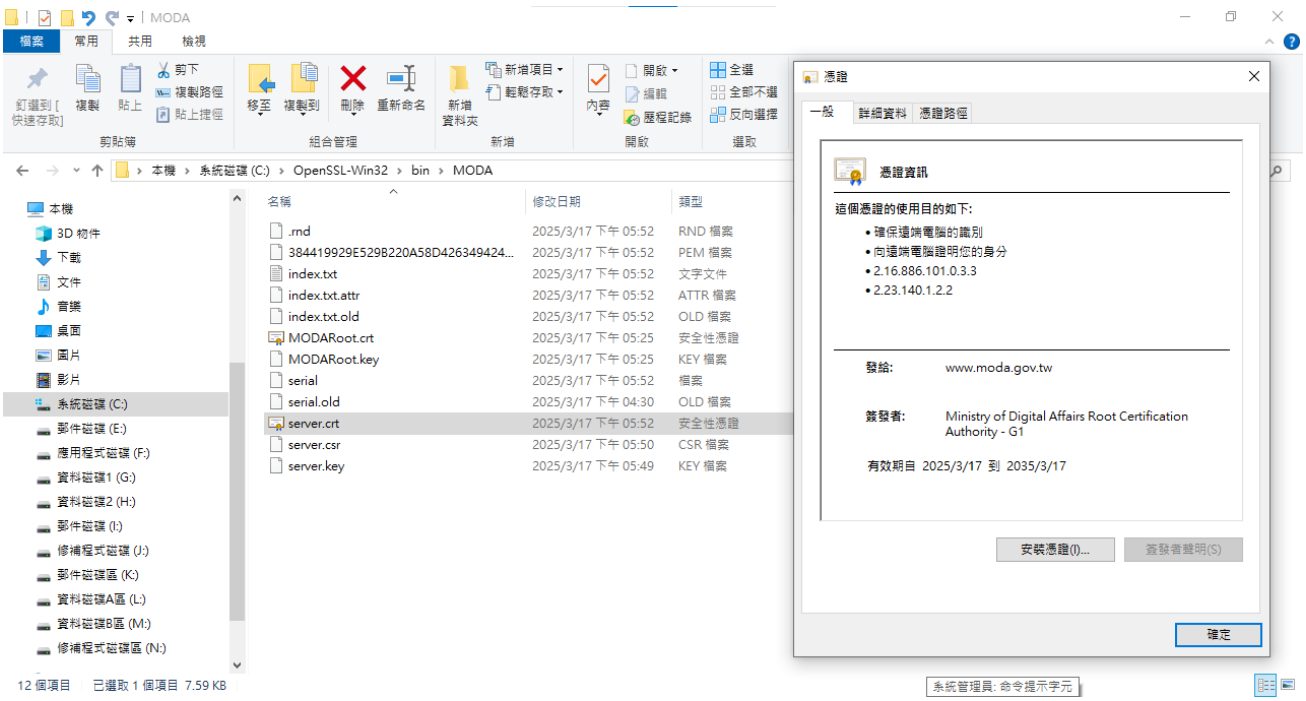
- ✓ 在 命令列 或 命令提示字元 下輸入 mmc Enter; 選檔案 -> 新增/移除嵌入式管理單元(M) -> 可用式嵌入式管理單元(S) 選擇 憑證 -> 新增; 這個嵌入式管理單元將自動管理下列帳戶的憑證: 選 我的使用者帳戶(M) -> 完成 -> 確定
- ✓ 點選 憑證-目前的使用者 -> 受信任的根憑證授權單位 -> 憑證撤銷清單，在右邊視窗中可找到植入的憑證撤銷清單

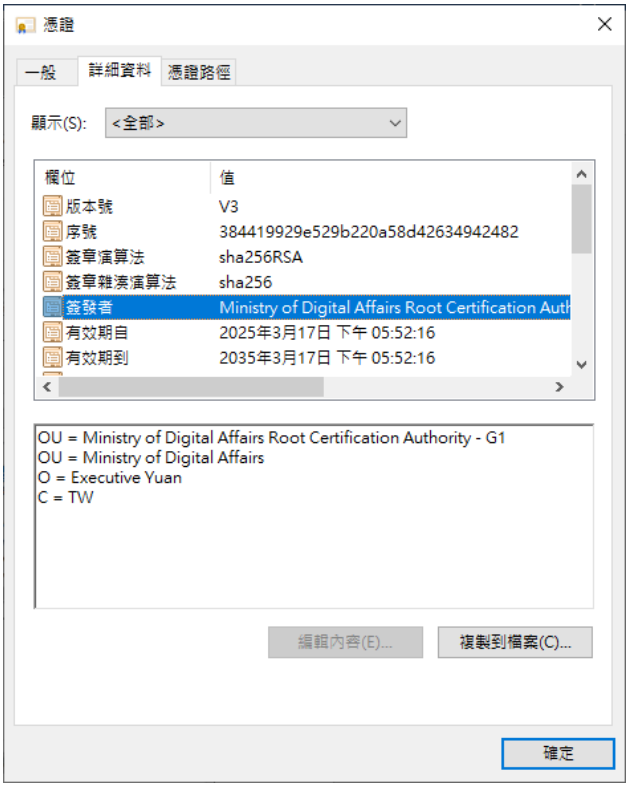


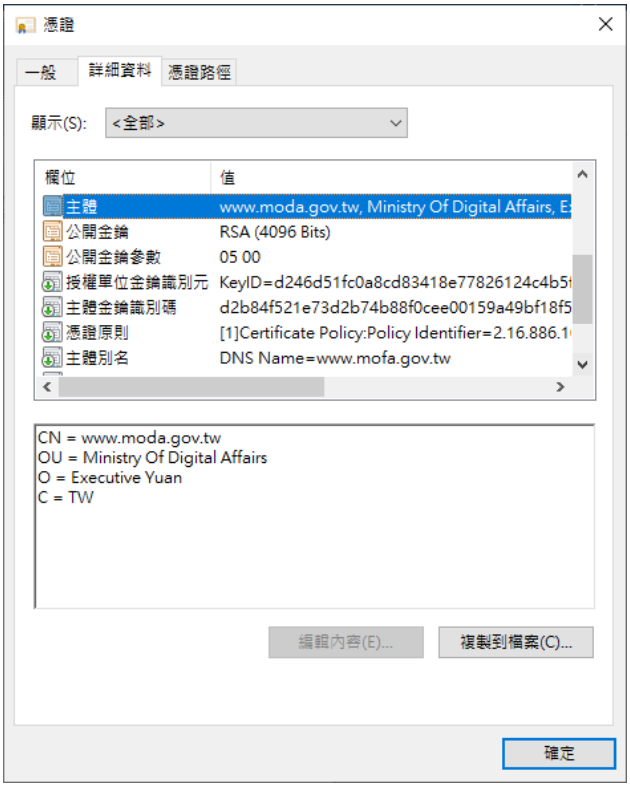
➢ 確認簽出來的根憑證植入 Windows 的狀態，正常會如下圖並沒有任何錯誤或驚嘆號

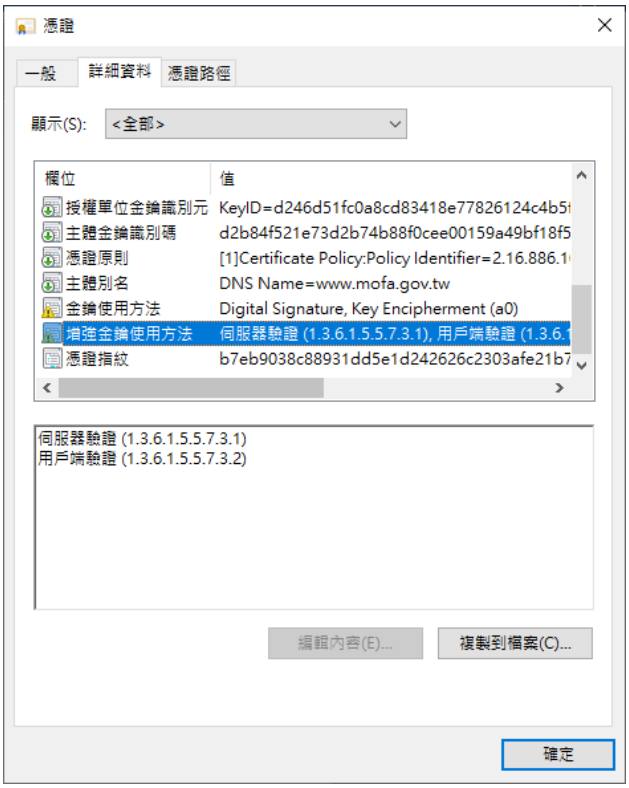


➢ 確認簽出來的終端憑證狀態，正常會如下圖並沒有任何錯誤或驚嘆號，發給會出現簽發的 Domain Name







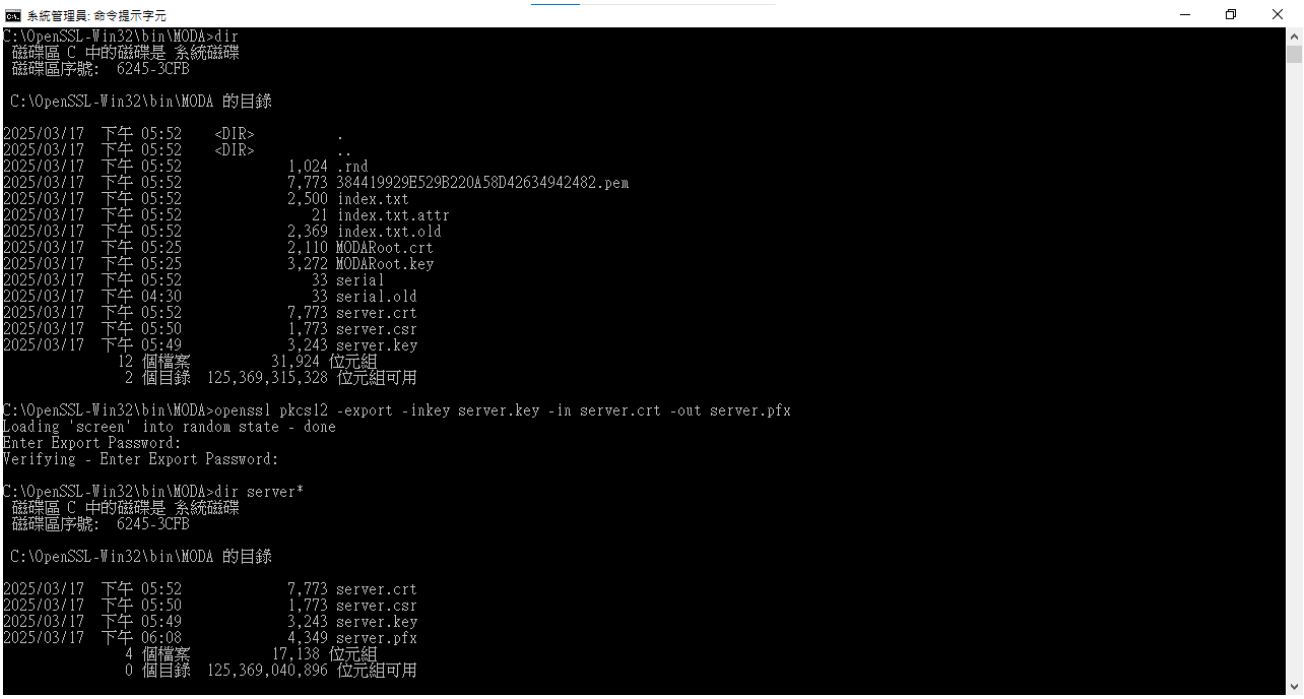

憑證
一般
詳細資料
憑證路徑
顯示(S):
<全部>
欄位
值
授權單位金鑰識別元
KeyID=d246d51fc0a8cd83418e77826124c4b5
主體金鑰識別碼
d2b84f521e73d2b74b88f0cee00159a49bf18f5
憑證原則
[1]Certificate Policy:Policy Identifier=2.16.886.1
主體別名
DNS Name=www.mofa.gov.tw
金鑰使用方法
Digital Signature, Key Encipherment (a0)
增強金鑰使用方法
伺服器驗證 (1.3.6.1.5.5.7.3.1), 用戶端驗證 (1.3.6.
憑證指紋
b7eb9038c88931dd5e1d242626c2303afe21b7
伺服器驗證 (1.3.6.1.5.5.7.3.1)
用戶端驗證 (1.3.6.1.5.5.7.3.2)
編輯內容(E)...
複製到檔案(C)...
確定

➢ 將 OpenSSL 產製的私密金鑰及自簽憑證合併成 PKCS12 檔案格式(PFX 檔)

openssl pkcs12 -export -inkey server.key -in server.crt -out server.pfx

※ 若沒有設定環境變數，可用指定 openssl.exe 程式全路徑並指定 openssl.cfg 檔案位置執行，如

C:\OpenSSL-Win32\bin\MODA>**"C:\OpenSSL-Win32\bin\openssl.exe"** pkcs12 -export -inkey server.key -in server.crt -out server.pfx



```
系統管理員: 命令提示字元
C:\OpenSSL-Win32\bin\MODA>dir
 磁碟區 C 中的磁碟是 系統磁碟
 磁碟區序號:  6245-3CFB

 C:\OpenSSL-Win32\bin\MODA 的目錄

2025/03/17  下午 05:52    <DIR>          .
2025/03/17  下午 05:52    <DIR>          ..
2025/03/17  下午 05:52             1,024 .rnd
2025/03/17  下午 05:52             7,773 384419929E529B220A58D42634942482.pem
2025/03/17  下午 05:52             2,500 index.txt
2025/03/17  下午 05:52                21 index.txt.attr
2025/03/17  下午 05:52             2,369 index.txt.old
2025/03/17  下午 05:25             2,110 MODARoot.crt
2025/03/17  下午 05:25             3,272 MODARoot.key
2025/03/17  下午 05:52                33 serial
2025/03/17  下午 04:30                33 serial.old
2025/03/17  下午 05:52             7,773 server.crt
2025/03/17  下午 05:50             1,773 server.csr
2025/03/17  下午 05:49             3,243 server.key
              12 個檔案          31,924 位元組
               2 個目錄  125,369,315,328 位元組可用

C:\OpenSSL-Win32\bin\MODA>openssl pkcs12 -export -inkey server.key -in server.crt -out server.pfx
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:

C:\OpenSSL-Win32\bin\MODA>dir server*
 磁碟區 C 中的磁碟是 系統磁碟
 磁碟區序號:  6245-3CFB

 C:\OpenSSL-Win32\bin\MODA 的目錄

2025/03/17  下午 05:52             7,773 server.crt
2025/03/17  下午 05:50             1,773 server.csr
2025/03/17  下午 05:49             3,243 server.key
2025/03/17  下午 06:08             4,349 server.pfx
               4 個檔案          17,138 位元組
               0 個目錄  125,369,040,896 位元組可用
```

- 將 PKCS12 檔案格式(PFX 檔)轉成 JAVA 常用的 keystore 檔，但必須要有安裝 OpenJDK 或 Oracle JAVA JDK 才能操作

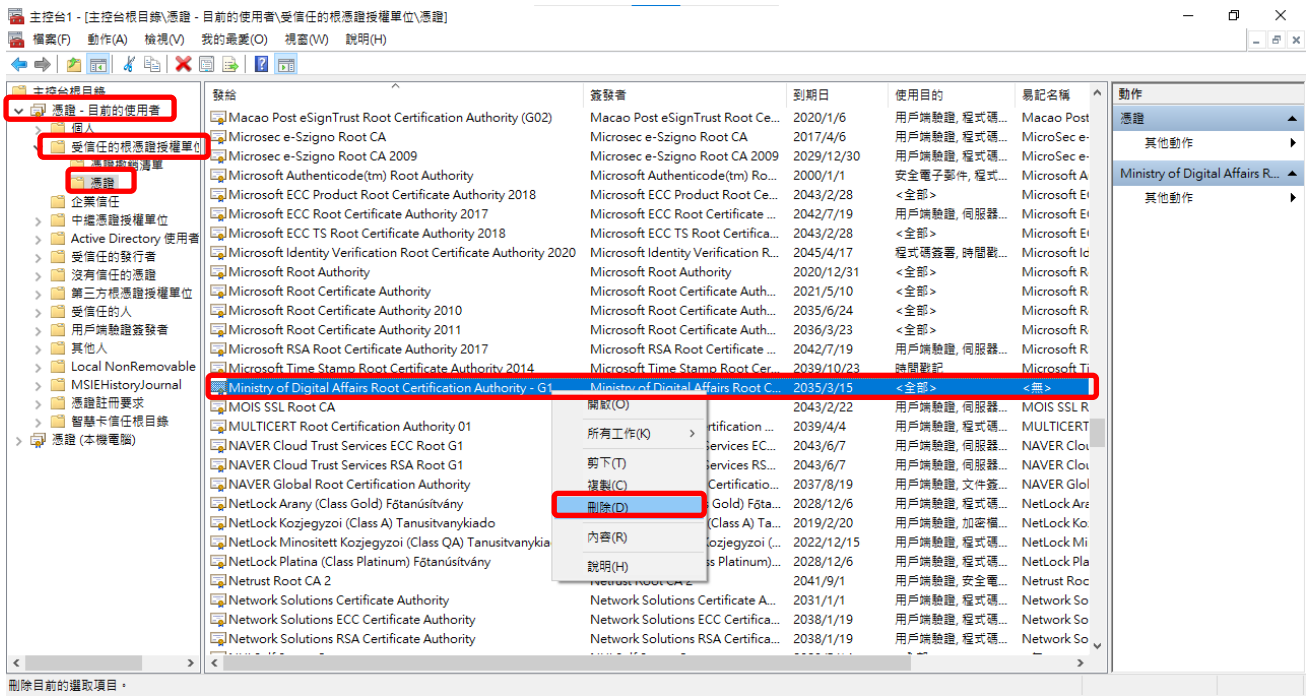
  keytool -importkeystore -srckeystore server.pfx -destkeystore tomcat.jks -srcstoretype pkcs12 -deststoretype jks -srcalias 1 -destalias tomcat

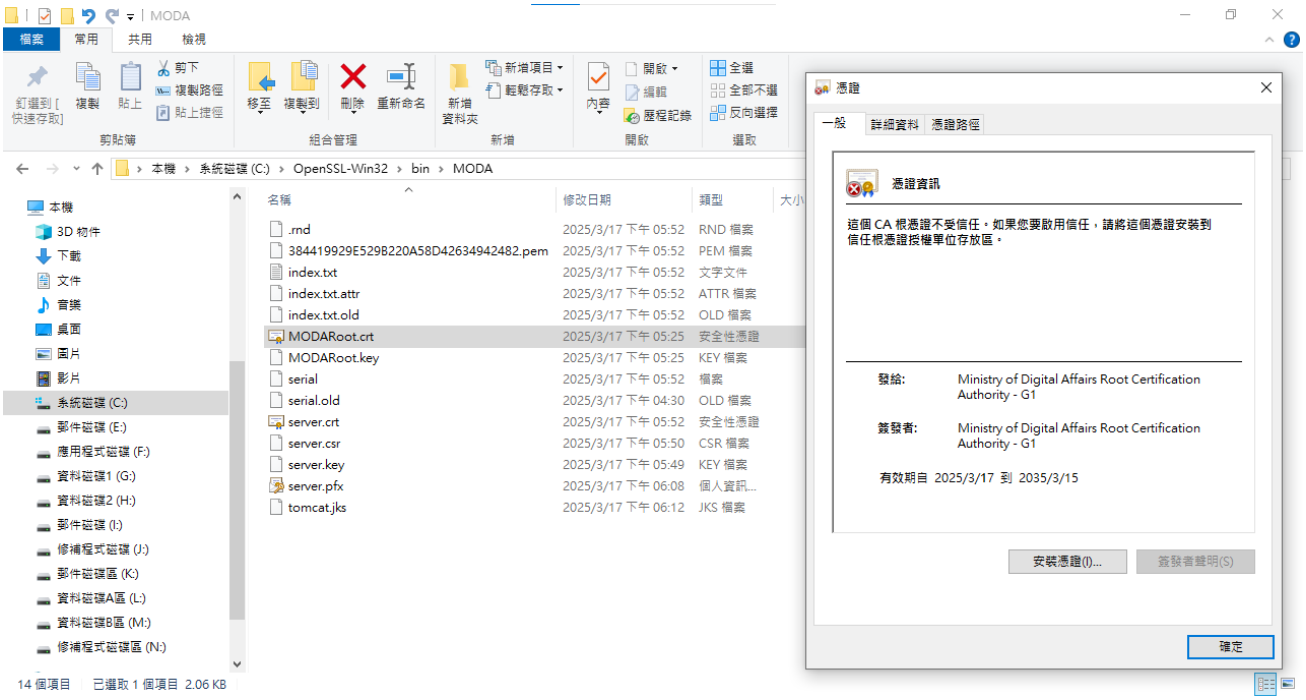
```
系統管理員: 命令提示字元
Enter Export Password:
Verifying - Enter Export Password:

C:\OpenSSL-Win32\bin\MODA>dir server*
 磁碟區 C 中的磁碟是 系統磁碟
 磁碟區序號:  6245-3CFB

 C:\OpenSSL-Win32\bin\MODA 的目錄

2025/03/17  下午 05:52             7,773 server.crt
2025/03/17  下午 05:50             1,773 server.csr
2025/03/17  下午 05:49             3,243 server.key
2025/03/17  下午 06:08             4,349 server.pfx
               4 個檔案          17,138 位元組
               0 個目錄  125,369,040,896 位元組可用

C:\OpenSSL-Win32\bin\MODA>keytool -importkeystore -srckeystore server.pfx -destkeystore tomcat.jks -srcstoretype pkcs12 -deststoretype jks -srcalias 1 -desta
lias tomcat
Importing keystore server.pfx to tomcat.jks...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srcke
ystore tomcat.jks -destkeystore tomcat.jks -deststoretype pkcs12".

C:\OpenSSL-Win32\bin\MODA>dir server*
 磁碟區 C 中的磁碟是 系統磁碟
 磁碟區序號:  6245-3CFB

 C:\OpenSSL-Win32\bin\MODA 的目錄

2025/03/17  下午 05:52             7,773 server.crt
2025/03/17  下午 05:50             1,773 server.csr
2025/03/17  下午 05:49             3,243 server.key
2025/03/17  下午 06:08             4,349 server.pfx
               4 個檔案          17,138 位元組
               0 個目錄  125,367,795,712 位元組可用

C:\OpenSSL-Win32\bin\MODA>
```

➢ 刪除植入 Windows 根憑證方法

✓ 在 命令列 或 命令提示字元 下輸入 mmc Enter; 選檔案 -> 新增/移除嵌入式管理單元(M) -> 可用式嵌入式管理單元(S) 選擇 憑證 -> 新增; 這個嵌入式管理單元將自動管理下列帳戶的憑證: 選 我的使用者帳戶(M) -> 完成 -> 確定

✓ 點選 憑證-目前的使用者 -> 受信任的根憑證授權單位 -> 憑證，在右邊視窗中找到植入的根憑證名稱，按滑鼠右鍵選刪除，刪除後根憑證就會變成不受信賴





➢ openssl.cfg 設定 req_distinguished_name 說明

[req_distinguished_name]

countryName = Country Name (2 letter code)

#countryName_default = AU ##### comment Default

countryName_default = TW ##### Change

===> 可改 Executive Yuan，或產生請求檔自行輸入即可

#localityName = Locality Name (eg, city) ##### uncomment Default

localityName_default = Taipei City

0.organizationName = Organization Name (eg, company)

#0.organizationName_default = Internet Widgits Pty Ltd ##### comment Default

0.organizationName_default = Chunghwa Telecom Co., Ltd.

===> 可改 Executive Yuan，或產生請求檔自行輸入即可

1.organizationName = Second Organization Name (eg, company)

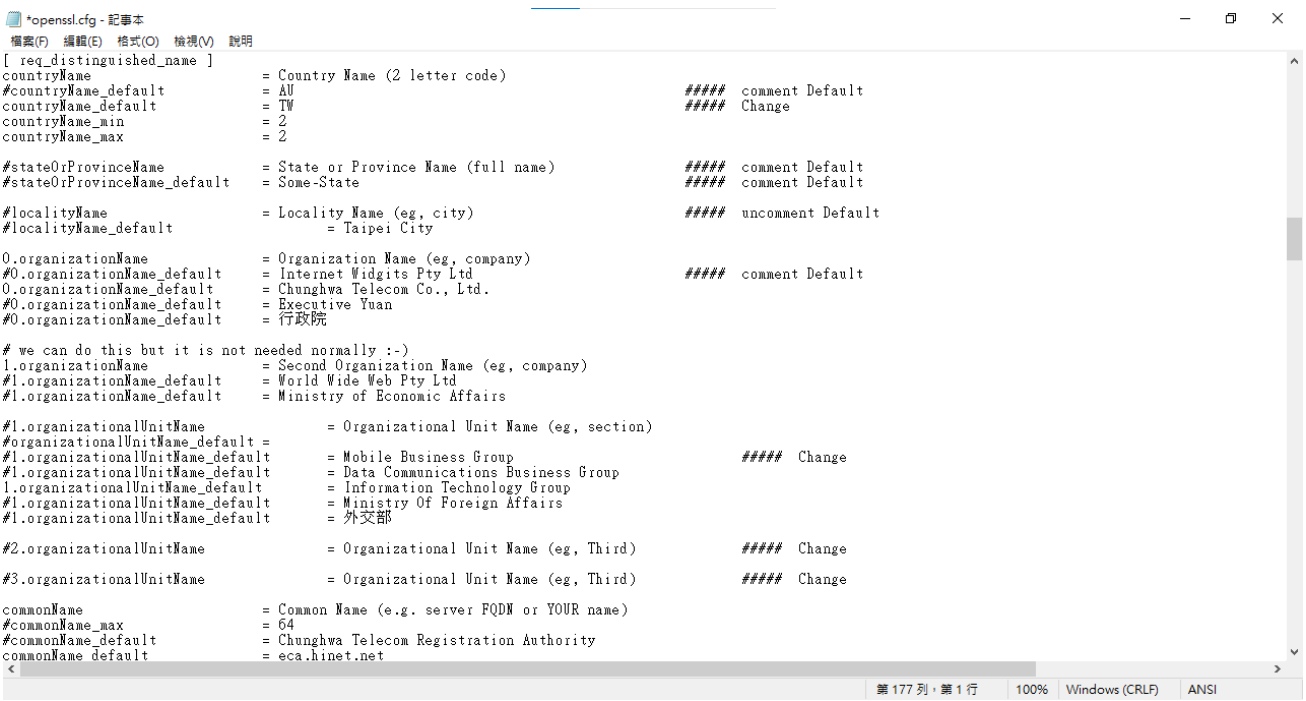
1.organizationalUnitName_default = Information Technology Group

===> 可改 Ministry Of Foreign Affairs，或產生請求檔自行輸入即可

commonName = Common Name (e.g. server FQDN or YOUR name)

commonName_default = eca.hinet.net

===> 可改也可不用改，產生請求檔自行輸入即可



```
*openssl.cfg - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
#countryName_default            = AU                                    #####  comment Default
countryName_default             = TW                                    #####  Change
countryName_min                 = 2
countryName_max                 = 2

#stateOrProvinceName            = State or Province Name (full name)    #####  comment Default
#stateOrProvinceName_default    = Some-State                            #####  comment Default

#localityName                   = Locality Name (eg, city)              #####  uncomment Default
#localityName_default                   = Taipei City

0.organizationName              = Organization Name (eg, company)
#0.organizationName_default     = Internet Widgits Pty Ltd              #####  comment Default
0.organizationName_default      = Chunghwa Telecom Co., Ltd.
#0.organizationName_default     = Executive Yuan
#0.organizationName_default     = 行政院

# we can do this but it is not needed normally :-)
1.organizationName              = Second Organization Name (eg, company)
#1.organizationName_default     = World Wide Web Pty Ltd
#1.organizationName_default     = Ministry of Economic Affairs

#1.organizationalUnitName               = Organizational Unit Name (eg, section)
#organizationalUnitName_default =
#1.organizationalUnitName_default       = Mobile Business Group                         #####  Change
#1.organizationalUnitName_default       = Data Communications Business Group
1.organizationalUnitName_default        = Information Technology Group
#1.organizationalUnitName_default       = Ministry Of Foreign Affairs
#1.organizationalUnitName_default       = 外交部

#2.organizationalUnitName               = Organizational Unit Name (eg, Third)          #####  Change

#3.organizationalUnitName               = Organizational Unit Name (eg, Third)          #####  Change

commonName                      = Common Name (e.g. server FQDN or YOUR name)
#commonName_max                 = 64
#commonName_default             = Chunghwa Telecom Registration Authority
commonName_default              = eca.hinet.net
第 177 列，第 1 行   100%   Windows (CRLF)   ANSI
```

➢ openssl.cfg 設定 alt_names 說明

[alt_names]

DNS.1 = eca.hinet.net

DNS.2 = epki.com.tw

#IP.1 = 172.16.1.1

#IP.2 = 10.10.10.1

#IP.3 = 192.168.1.1

要加主體別名在 alt_names 這個區段，若多網域則用 DNS.1、DNS.2 或 IP.1、IP.2、IP.3 等，若只有單網域只要加 DNS.1 或 IP.1。