《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)
#O.organizationName_default	= Internet Widgits Pty Ltd
0.organizationName_default	= Executive Yuan
# we can do this but it is not no	eeded 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 name)	= Common Name (e.g. server FQDN or YOUR
commonName_max	= 64
第3]	頁, 共32頁

#emailAddress	= Email Address
emailAddress_max	= 64
[req_distinguished_name]	
countryNamedefault	= Country Name (2 letter code) = AU
countryName default	
countryName_min countryName_max	= 2 = 2
#stateOrProvinceName	= State or Province Name (full name)
#stateOrProvinceName_default	= Some-State
#localityName	= Locality Name (eg, city)
O.organizationName	= Organization Name (eg. company)
#0.organizationName_default	= Internet Widgits Pty Ltd - Executive Ynan
# we can do this but it is not #1.organizationName	needed normally :-) = Second Organization Name (eg. company)
#1.organizationName_default	= World Wide Web Pty Ltd
0.organizationalUnitName	= Organizational Unit Name (eg, section)
O.organizationalUnitName_defau	lt = Ministry of Digital Affairs
1.organizationalUnitName	= Organizational Unit Name (eg. section)
1.organizationalUnitName_defau	lt = Ministry of Digital Affairs Root Certification Authority - G1
#commonName	= Common Name (e.g. server FQDN or YOUR name)
commonName_max	= 04
#emailAddress	= Email Address
emaılAddress_max	= 04

※ 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.
# keyllsage = cRLSign, keyCertSign
```

```
keyUsage = digitalŠignature, 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 <u>'openssl' 不是內部或外部命令、</u>
 <u>可執行的程式或批次檔。</u>。請在 <u>Windows 設定</u> -> <u>系統</u> -> 左邊選項最下方 <u>關於</u>
 -> 右邊選項 <u>進階系統設定</u>,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。

条統內容 ×	環境變數	×
電腦名稱 硬體 進階 未統保護 遠端 您必須以系統管理員的身分登入,才能變更這裡的大部分設定。	建文 值 建款 值 Intellij IDEA Com C:\Users\ZengHuanSong\OneDrive - Chu OneDrive C:\Users\ZengHuanSong\OneDrive - Chu OneDriveComme C:\Users\ZengHuanSong\AppData\Local	Ţ
使用者設定檔 關於您登入時的桌面設定 設定(E)	新增(N) 編輯(E) 刪除(D) 条統變數(S) 變數 值 ^	
啟動及修復 系統啟動、系統失敗、及偵錯資訊 設定(T) 環境磁動(AD)	NUMBER_OF_PR 4 OPENSSL_CONF C:\OpenSSL-Win32\bin\openssl.cfg OS Windows_NT Path C:\WINDOWS\system32;C:\WINDOWS;C: v 新增(W) 編輯(I) 刪除(L)	
	· 程定 取消	

	環境變數	×
系統內容	ZengHuanSong 的使用者變數(U) 設定 Path 環境變數	
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 效能 視覺效果、處理器排程、記憶體使用	 22 22 22 22 23 24 24 25 25 26 27 28 28 28 29 20 20 21 	
● 使用者設定檔 關於您登入時的桌面設定	新增(1) 編輯(E) 刪除(D) 条統變數(S)	
↓ □ 啟動及修復 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	PROCESSOR_AR AMD64 PROCESSOR_IDE Intel64 Family 6 Model 60 Stepping 3, Ge 、 新增W 編輯() 刪除(L) 確定 取消	
	童茂	.1



■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	-	٥	×
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 rss 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. Thore ore suite a few fields but were non Leove area block of Name or a DN.	:4096 -keyout MODARoot.key -out MODARoot.crt		
Inere are quite a rew fields but you can reave some brank 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 Mame (eg, company) [Executive Yuan]: Organizational Unit Name (eg, section) [Ministry of Digital Affairs]: Organizational Unit Name (eg, section) [Ministry of Digital Affairs Root Certification Auth«	brity - G1]:		
C:\OpenSSL-Win32\bin\MODA>			

5 憑證		× 🇔 🤅	題		×
一般詳細	資料 憑證路徑	— <u>A</u>	} 計細資料 ∦	長證路徑	
顯示(S): <	全部> ~	Đ	示(S): <全部>	~	
欄位	值	^	闌位	值	^
🖺 版本號	V3		副主體	Ministry of Digital Affairs Root Certification Aut	horit
📴 序號	00f5b2d5a3229bf9bf		公開金鑰	RSA (4096 Bits)	
🔚 簽章演算	誌 sha256RSA		▋公開金鑰參數	05 00	
☐ 簽章雜》	[演算法 sha256		🗊 主體金鑰識別碼	d246d51fc0a8cd83418e77826124c4b5f0d650	65
፼ 簽發者	Ministry of Digital Affairs Root Certification	on Authority	3 基本限制	Subject Type=CA, Path Length Constraint=Nor	ie
🔄 有效期目	2025年3月17日下午 05:25:32		金鑰使用方法	Digital Signature, Certificate Signing, Off-line C	RL Si
一 有效期到] 2035年3月15日下午 05:25:32	✓	圖憑證指紋	693e28971c494ab394a4b7377309567157dffe	85 🗸
<		>			>
OU = Minis OU = Minis O = Execut C = TW	try of Digital Affairs Root Certification Authority - try of Digital Affairs ve Yuan 编輯內容(E) 複纂	G1	igital Signature, (6)	Certificate Signing, Off-line CRL Signing,	iing [(C)
		確定			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) ===> <u>www.moda.gov.tw</u>

- ✓ 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
                                         # Where everything is kept
dir
                =
                = $dir/certs
                                         # Where the issued certs are kept
certs
                = $dir/crl
                                         # Where the issued crl are kept
crl_dir
                = $dir/index.txt
                                         # database index file.
database
#unique_subject = no
                                         # Set to 'no' to allow creation of
                                         # several ctificates with same subject.
                = $dir/newcerts
#new_certs_dir
                                         # default place for new certs.
new_certs_dir
                = $dir
                                         # The CA certificate
                = $dir/cacert.pem
certificate
                = $dir/serial
                                         # The current serial number
serial
                = $dir/crlnumber
crlnumber
                                         # the current crl number
                                         # must be commented out to leave a V1 CRL
                                         # The current CRL
                = $dir/crl.pem
crl
                = $dir/private/cakey.pem# The private key
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
                              第9頁, 共32頁
```

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 #countryName_default countryName_default countryName_min countryName_max	= Coun = AV = TW = 2 = 2	try Name (2 letter code)
#stateOrProvinceName #stateOrProvinceName_default	= Stat = Some	e or Province Name (full name) -State
#localityName	= Loca	lity Name (eg, city)
O.organizationName #O.organizationName_default O.organizationName_default	= Orga = Inte = Exec	nization Name (eg, company) rnet Widgits Pty Ltd utive Yuan
# we can do this but it is not n #1.organizationName #1.organizationName_default	needed = Seco = Worl	normally :-) nd Organization Name (eg, company) d Wide Web Pty Ltd
O.organizationalUnitName #O.organizationalUnitName_defau O.organizationalUnitName_defaul	lt t	= Organizational Unit Name (eg, section) = = Ministry Of Digital Affairs
#1.organizationalUnitName #1.organizationalUnitName_defau	lt	= Organizational Unit Name (eg, section) = Ministry Of Digital Affairs Root Certification Authority – G1
commonName	= Comm	on Name (e.g. server FQDN or YOUR name)
#emailAddress emailAddress_max	= Emai = 64	l Address
[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_defa	ult	= Some-State
#localityName		= Locality Name (eg, city)
0.organizationName		= Organization Name (eg, company)
#0.organizationName_defau	ılt	= Internet Widgits Pty Ltd
0.organizationName_defaul	t	= Executive Yuan
# we can do this but it i #1.organizationName	s not	needed normally :-) = Second Organization Name (eg, company)
<pre>#1.organizationName_defau</pre>	ılt	= 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 = calssuers;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.
                                  = "OpenSSL Generated Certificate"
# nsComment
 # 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
 #nsBase∬rl
 #nsRevocationUrl
 #nsRenewalUrl
 #nsCaPolicvUrl
 #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 =
calssuers;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 will be displayed in Netscape's comment listbox.
                      = "OpenSSL Generated Certificate"
# nsComment
 DVIV
                             第15頁, 共32頁
```

<mark>#_subjeetKeyIdentifier=hash</mark> #_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。

■ 朱統管理員:命令提示字元	-	٥	×
Microsoft Windows [版本 10.0.19045.5487] (c) Microsoft Corporation. 著作權所有,並保留一切權利。			Â
C:\WINDOWS\system32>cd C:\OpenSSL-Win32\bin			
C:\OpenSSL-Win32\bin>cd MODA			
C:\OpenSSL-Win32\bin\MODA>openssl genrsa -out server.key 4096 Loading 'screen' into random state – done Generating RSA private key, 4096 bit long modulus			
e is 65537 (0x10001)			
C:\OpenSSL-Win32\bin\MODA>openssl req -sha256 -new -key server.key -out server.csr Loading 'screen' into random state - done 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, server FQDN or YOUR name) []:www.moda.gov.tw			
Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:12345678 An optional company name []:Executive Yuan			
C:\OpenSSL-Win32\bin\MODA>			

📼 系統管理員: 命令提示字元	-	D	×
C:\OpenSSL-Win32\bin\MODA>openssl ca -in server.csr -cert MODARoot.crt -keyfile MODARoot.Key -out server.crt -days 3652 Weing configuration from C:\OpenSSL Win32\bin\opensel ofg			
Loading Configuration from C. Openado and Taxon Nopenson. Crg			
Check that the request matches the signature			
Signature ok			
Certificate Details:			
Serial Number:			
<u>38:44:19:92:9e:52:9b:22:0a:58:d4:26:34:94:24:82</u>			
Validity			
Not Before: Mar 17 09:52:16 2025 GMT			
wot After : Mar 17 09:52:10 2055 GMI			
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:52:1É: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			
X5U9y3 Extended Key Usage: critical			
ILS web Server Authentication, ILS web Client Authentication			
Certificate is to be certified until mar 17 09:52:10 2055 Gml (5052 Gays)			
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。

■ 条统管理員: 命令提示字元	_	٥	×
Serial Number: 38:44:19:92:9e:52:9b:22:0a:58:d4:26:34:94:24:82			^
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 Authority Key Identifier: k509v3 Authority Key Identifier: keyid:D2:46:D5:IP:CO: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:A86.101.0.3.3 Policy: 2.23.140.1.2.2			
X509v3 Subject Alternative Name: DNS:www.msfa.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			
l out of 1 certificate requests certified, commit? [y/n]y Write out database with 1 new entries Data Base Updated			
2:\OpenSSL-Win32\bin\MODA>certutil -addstore -f "ROOT" MODARoot.crt ROOT "愛信任的根憑證授權單位" 簽章符合公開金鎬 簽證 "Ministry of Digital Affairs Root Certification Authority - G1" 已新增到存放區中。 CertUtil: -addstore 命令成功完成。 C:\OpenSSL-Win32\bin\MODA>			~

- ▶ 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。

The set # # # # # # # # # # # # # # # # # # #				
A (croseft ¥indows [版本 10.0.19045.5487) (c) Microsoft Zynadows - WirkBard W W W W W W W W W W W W W W W W W W W	■ 条纸管理具: 命令提示字元 - certutil -URL https://www.moda.gov.tw/CRL/ca.crl	-	Ő	\times
C:\UPENDUWS\system2>cd C:\UPENSU.Fin32\bin C:\UPENSU.Fin32\bin\UDA>certuil = addstore =f "ROOT" ca.crl ROOT "%defratR&maisty af Digital Affairs Root Certification Authority = G1, OU=Ministry of Digital Affairs, O=Executive Yuan, C=TW" 已新增到存放區中。 CertUil: = addstore 命令放放完成。 C:\UPENSU.Fin32\bin\UDA>certuil =URL https://www.moda.gov.tw/CRL/ca.crl URL%bing Fgguip (0) 15 描述會 正在下動的CRL或是整法物意地行動 E: CRL或是整正和影響 建成 「 委員LDAP 完量	Microsoft Windows [版本 10.0.19045.5487] (c) Microsoft Corporation. 著作權所有,並保留一切權利。			
C: VopenSSL-Vin32\bin\WODA>certutil =addstore =f "ROOT" ca.crl ROOT " ghtfthHK是超技程程U" C: VopenSSL-Vin32\bin\WODA>certutil =addstore =f "ROOT" ca.crl CertUtil: =addstore 命令成功完成。 C: VopenSSL-Vin32\bin\WODA>certutil =URL https://www.moda.gov.tw/CRL/ca.crl URL 抓取工具 × 「 新聞 課題 URL	C:\WINDOWS\system32>cd C:\OpenSSL-Win32\bin			
E: V0penSSL-Vin32Vbin/WODA>certutil -addstore -f "ROOT" ca.crl ROOT " 咬信任的根處證技構單位" E: "U0PenSSL-Vin32Vbin/WODA>certutil - URL https://www.moda.gov.tw/CRL/ca.crl URL 新設工具 X 家保協時(5) 15 藤注意: 正在下着的(CRL或通程立未能定進行確 路(CRL 或通程可能仍不一般) 或可能及其语 定 CRL 或通程可能仍不一般) 或可能及其语 定 家著 LDAP 质量 超短语: 以CRL 或通程立体的不一般 或可能及其语 更下能的(URL https://www.moda.gov.tw/CRL/ca.crl	C:\OpenSSL-Win32\bin>cd MODA			
C:\OpenSSL-Vin32\bin\MODA>certutil -URL https://www.moda.gov.tw/CRL/ca.crl X URL 新取其 X 就應 編型 URL 新取時簡 指紋 等候脑時(彩) 15 醫生會:正在下醫的CRL或過酸盐未能應變行確 節於CRL或過酸盐未能應變行確 當該任命,以允許正確的確認。 所取 ○ 管證(來自ALA) ○ KEL (來自 CDP) ○ OCSP (來自ALA) 沒有趨款項目 選擇 紙束 要下點的 URL https://www.moda.gov.tw/CRL/ca.crl	C:\OpenSSL-Win32\bin\MODA>certutil -addstore -f "ROOT" ca.crl ROOT "受信任的報憑證授權單位" C2L "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。			
URL 浙亚 其	C:\OpenSSL-Win32\bin\MODA>certutil -URL https://www.moda.gov.tw/CRL/ca.crl			
就種 類型 URL 抓取時間 指紋 等候诡時(参) 15 講注意: 正在下載的 CRL 或過證並未錄應進行確 認 · CRL 或過證如未錄應進行確 認 · CRL 或過證如年錄應進行確 認 · CRL 或過證如年錄應進行確 語的延伸 · 以允許正確的確認 · 抓取 C 憑證 (來自 AIA) 「 簽署 LDAP 法量 · CRL (來自 CDP) [沒有違取項目 違理 要下載的 URL https://www.moda.gov.tw/CRL/ca.crl	URL 抓取工具 X			
等侵៉途時(約) 15 請注意:正在下載的 CRL或通證並未徹底進行確 認・CRL或通道可能仍不一致,或可能沒有適 當的延伸,以允許正確的確認。 (○ CRL(來自 AIA) ○ CRL(來自 CDP) ○ OCSP(來自 AIA) ②有違取項目 違揮	狀態 類型 URL 抓取時間 指紋			
等候៉適時(ぎ) 15 諸注意:正在下載的 CRL 或通證並未像應進行準 認 · CRL 或通證可能仍不一致,或可能沒有適 當的延伸,以允許正確的確認。 「 簽署 LDAP 流量 室的延伸,以允許正確的確認。 ○ CRL (來自 AIA) 「 沒有違取項目 違理 追索 要下載的 URL https://www.moda.gov.tw/CRL/ca.crl				
沒有違取項目 違律 結束 抓取 要下動的 URL https://www.moda.gov.tw/CRL/ca.crl	等候逾時(秒) 15 諸注意:正在下載的 CRL 或憑證並未徹底憶行確 該。CRL 或憑證可能仍不一致,或可能沒有適 當的延伸,以允許正確的確認。 CRL (來自 AIA) ○ CRL (來自 CDP) ○ CCSP (來自 AIA)			
要下動的 URL https://www.moda.gov.tw/CRL/ca.crl	沒有攜取項目			
	要下載的 URL https://www.moda.gov.tw/CRL/ca.crl			
				,

■ 系統管理員: 命令提示字元 - certutil -URL https://www.moda.gov.tw/CRL/ca.crl	_	D	\times
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>cd MODA			
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—TV" 已新增到存放區中 CertUtil: -addstore 命令成功完成。	1 0		
C:\OpenSSL-Win32\bin\MODA>certutil -URL https://www.moda.gov.tw/CRL/ca.crl			
URL 抓取工具 X			
詳し 1181 1181 1161 確定 基本 CRL (780bd392) [0.0] http://www.moda.gov.tw/CRL/ca.crl 0 く 等候地時(参) 15 腸注意: 正在下飯的 CRL 或憑證並未彻底進行確 影・CRL 或憑證可能以不一致,或可能沒有適 (*) 小取			
□ 簽署 LDAP 流量			
沒有繼取項目 邊宿 結束 抓取			
要下載的 URL http://www.moda.gov.tw/CRL/ca.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

🚟 主控台1 - [主控台根目錄\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]				-	ð ×
🚟 檔案(F) 動作(A) 檢視(V)	我的最爱(O) 視窗(W) 說明(H)					_ 8 ×
🗢 🄿 🙍 🔂 🖬 🙆						
主控台根目錄		有效日期	下次更新		動作	
✓ □ 憑證 - 目前的使用者	E Ministry of Digital Affairs Root Certification Authority - G1, Ministry of Digital Affairs, Executive Yuan, TW	2025/3/18	2035/3/18		慿證撤銷清單	
> 個人 < 1 番信任的規馮證授權單(其他動作	•
□ 憑證撤銷清單						
── 憑證						
> 📫 企業信任						
> P 甲種憑證授權単位						
> Call Active Directory 使用者						
> 🧾 沒有信任的憑證						
> 📔 第三方根憑證授權單位						
> 🧮 受信任的人						
> 用尸喃歌超或张音						
> Cocal NonRemovable						
> 📔 MSIEHistoryJournal						
> 🧰 憑證註冊要求						
> 2 智慧卞信仕根日臻 、 (二) 馮晓 (大將秦際)						
> 「」 22世(平)(21世(中))						
	JI]]		

▶ 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

1 2 2 1 MODA 確認 常用 共用 檢視 第用 技用 技用 検視 第目 (編集) 時上 (編集) 第上 「該違到」[(編集) 時上 (注意) 所上 (注意) 「訪比簿 (注意) (注意) (注意) (注意)		 ○ 間飯・ ○ 環銀 ○ 環銀 ○ 環銀 ○ 環盤記錄 ○ 関飲 	 全選 ○ 全部不選 ○ 定部不選 ○ 反向選擇 選取 	- □ × へ ● 原 ● 詳細資料 憑證第徑
 ← → ◇ ↑ → 本機 → 未規 → 未規 本機 本機 30 約件 下式 文件 う 音獎 桌面 眞川 夏片 夏片 夏川 第5 三 原用程式巡議(C) 三 算料巡議(C) 三 算料 三 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	(C:) > OpenSL-Win32 > bin > MODA Sime and the second sec	修改日期 2025/3/17 下午 05:52 2025/3/17 下午 05:52 2025/3/17 下午 05:52 2025/3/17 下午 05:52 2025/3/17 下午 05:25 2025/3/17 下午 05:25 2025/3/17 下午 05:52 2025/3/17 下午 05:52 2025/3/17 下午 05:50 2025/3/17 下午 05:50 2025/3/17 下午 05:49	環型 大川 RND 備業 PEM 備業 文字文件 ATTR 備業 CDLD 備業 CDLD 備業 CDLD 備業 CDLD 備業 CDLD 備業 CDLD 備業 CDL 備業 CDL 備業 CDL 備業 KEY 備業 KEY 備業 CDL 情報 CDL ft	遊館変融 遊園の設備用目的如下: 単、病有發行原則 予、所有應用電式原則 一 就 部: Ministry of Digital Affairs Root Certification 通報語: Ministry of Digital Affairs Root Certification 通知的では、-G1 - 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一

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



		>
-般 詳細資料 憑證路	各徑	
顯示(S): <全部>	~	
欄位 授權單位金鎢識別元 主體金鎢識別碼 主體別名 主體別名 金鑰使用方法 描述金鑰使用方法 通過證損約	值 KeyID=d246d51fc0a8cd83418e77826124c4b5i d2b84f521e73d2b74b88f0cee00159a49bf18f5 [1]Certificate Policy:Policy Identifier=2.16.886.11 DNS Name=www.mofa.gov.tw Digital Signature, Key Encipherment (a0) 伺服器驗證 (1.3.6.1.5.5.7.3.1), 用戶情驗證 (1.3.6.1 b7eb9038c88931dd5e1d242626c2303afe21b7 >	
伺服器驗證 (1.3.6.1.5.5. 用戶端驗證 (1.3.6.1.5.5.	7.3.1) 7.3.2)	
伺服器驗證 (1.3.6.1.5.5. 用戶端驗證 (1.3.6.1.5.5.	7.3.1) 7.3.2) 编輯內容(E) 複製到檔案(C)	

▶ 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: 6	命令提示字元		-	o x
C:NOpenSSL-₩ 磁碟區_C_中	₩In32\bin\MUUB>d1r h的磁碟是_系統磁碟			
磁埰區序號:	: 6245-3UFB			
C:\OpenSSL-	-Win32\bin\MODA 的目标			
2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17	下午 05:52 <dir> 下午 05:52 <dir> 下午 05:52 <1,024 .rnd 下午 05:52 7,773 384419929E529B220A58D42634942482.pem 下午 05:52 7,773 384419929E529B220A58D42634942482.pem 下午 05:52 7,773 384419929E529B220A58D42634942482.pem 下午 05:52 2,100 MODARoot.xtt 下午 05:25 2,100 MODARoot.crt 下午 05:52 3,272 MODARoot.key 下午 05:52 3,272 MODARoot.key 下午 05:52 7,773 server.crt 下午 05:50 1,773 server.csr 下午 05:50 1,773 server.csr 下午 05:49 3,243 server.key 12 個智録 125.369.315.328 (万定封甲) 田</dir></dir>			
C:\OpenSSL-W Loading 'scr Enter Export Verifying -	Win32\bin\MODA>openss1 pkcs12 -export -inkey server.key -in server.crt -out ser reen' into random state - done t Password: Enter Export Password:	ver.pfx		
C:\OpenSSL-W 磁碟區 C 中 磁碟區序號:	₩in32\bin\MODA>dir server* 中的磁碟是 系統磁碟 : 6245-3CPB			
C:\OpenSSL-	-Win32\bin\MODA 的目錄			
2025/03/17 2025/03/17 2025/03/17 2025/03/17 2025/03/17	下午 05:52 7.773 server.crt 下午 05:50 1.773 server.csr 下午 06:08 4.349 server.key 下午 06:08 4.349 server.pfx 4 個檔案 17.138 位元組 0 個目録 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	— ć		×
Enter Export Password: Verifying - Enter Export Password:			^
C:\OpenSSL-Win32\bin\MODA>dir server* 磁碟區 C 中的磁碟是 条統磁碟 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 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 -srcal lias tomcat Importing keystore server.pfx to tomcat.jks Enter destination keystore password: Re-enter new password: Enter source keystore password:	ias 1	-desta	
Warning: The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkey ystore tomcat.jks -destkeystore tomcat.jks -deststoretype pkcs12".	store	-srcke	2
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-Vin32\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

📸 王控台1 - [王控台根目錄\憑證 -	日前的使用者\受信任的根憑證授權單位\憑證]					- 0	. ×
🚟 檔案(F) 動作(A) 檢視(V)	我的最爱(O) 視畜(W) 說明(H)						- 8 ×
- 🗢 🔿 📶 🔏 🖬 🗙 🛛							
11 主控台根目籍	發給 ^	簽發者	到期日	使用目的	易記名稱 ^	動作	
🗸 🗔 憑證 - 目前的使用者	🔄 Macao Post eSignTrust Root Certification Authority (G02)	Macao Post eSignTrust Root Ce	2020/1/6	, 用戶端驗證,程式碼	Macao Post	憑證	
	🔄 Microsec e-Szigno Root CA	Microsec e-Szigno Root CA	2017/4/6	用戶端驗證,程式碼	MicroSec e-	首他動作	•
受信任的根您證按權単位	🔄 Microsec e-Szigno Root CA 2009	Microsec e-Szigno Root CA 2009	2029/12/30	用戶端驗證,程式碼	MicroSec e-	STIDE/IF	,
一 准均	🔄 Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Ro	2000/1/1	安全電子郵件,程式	Microsoft A	Ministry of Digital Affa	irs R 🔺
	GMicrosoft ECC Product Root Certificate Authority 2018	Microsoft ECC Product Root Ce	2043/2/28	<全部>	Microsoft E	其他動作	•
止未自止 、 □□ 止未自止 、 □□ 止患痛酸指摘 ■ 位	Microsoft ECC Root Certificate Authority 2017	Microsoft ECC Root Certificate	2042/7/19	用戶端驗證, 伺服器	Microsoft E		
→ Crive Directory 使用者	G Microsoft ECC TS Root Certificate Authority 2018	Microsoft ECC TS Root Certifica	2043/2/28	<全部>	Microsoft E		
> □ 受信任的發行者	Microsoft Identity Verification Root Certificate Authority 2020	Microsoft Identity Verification R	2045/4/17	程式碼簽署, 時間戳	Microsoft Id		
> 2 沒有信任的憑證	🔄 Microsoft Root Authority	Microsoft Root Authority	2020/12/31	<全部>	Microsoft R		
> 🧰 第三方根憑證授權單位	🔄 Microsoft Root Certificate Authority	Microsoft Root Certificate Auth	2021/5/10	<全部>	Microsoft R		
> 🧰 受信任的人	🔄 Microsoft Root Certificate Authority 2010	Microsoft Root Certificate Auth	2035/6/24	<全部>	Microsoft R		
> 📔 用戶端驗證簽發者	🔄 Microsoft Root Certificate Authority 2011	Microsoft Root Certificate Auth	2036/3/23	<全部>	Microsoft R		
> 🔛 其他人	🔄 Microsoft RSA Root Certificate Authority 2017	Microsoft RSA Root Certificate	2042/7/19	用戶端驗證, 伺服器	Microsoft R		
> 📔 Local NonRemovable	Microsoft Time Stamp Root Certificate Authority 2014	Microsoft Time Stamp Root Cer	2039/10/23	時間戳記	Microsoft Ti		
> MSIEHistoryJournal	Ministry of Digital Affairs Root Certification Authority - G1	Ministry of Digital Affairs Root C	2035/3/15	<全部>	<無>		
> 🔛 憑證註冊要求	MOIS SSL Root CA	開啟(O)	2043/2/22	用戶端驗證, 伺服器	MOIS SSL R		
> 🔛 智慧卡信任根目錄	MULTICERT Root Certification Authority 01	新有工作(K) 、rtification	2039/4/4	用戶端驗證,程式碼	MULTICERT		
> 🔛 憑證 (本機電腦)	RAVER Cloud Trust Services ECC Root G1	Services EC	2043/6/7	用戶端驗證, 伺服器	NAVER Clou		
	RAVER Cloud Trust Services RSA Root G1	剪下(T) Services RS	2043/6/7	用戶端驗證, 伺服器	NAVER Clou		
	Root Certification Authority	複製(C) Certificatio	2037/8/19	用戶端驗證, 文件簽	NAVER Glol		
	🔄 NetLock Arany (Class Gold) Főtanúsítvány	刪除(D) Gold) Főta	2028/12/6	用戶端驗證,程式碼	NetLock Are		
	🔄 NetLock Kozjegyzoi (Class A) Tanusitvanykiado	(Class A) Ta	2019/2/20	用戶端驗證, 加密檔	NetLock Ko:		
	🔄 NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykia	内晉(R) iozjegyzoi (2022/12/15	用戶端驗證,程式碼	NetLock Mi		
	🔄 NetLock Platina (Class Platinum) Főtanúsítvány	說明(H) is Platinum)	2028/12/6	用戶端驗證,程式碼	NetLock Pla		
	Root CA 2	NEUDSCHOOL CA 2	2041/9/1	用戶端驗證, 安全電	Netrust Roc		
	Retwork Solutions Certificate Authority	Network Solutions Certificate A	2031/1/1	用戶端驗證,程式碼	Network So		
	Retwork Solutions ECC Certificate Authority	Network Solutions ECC Certifica	2038/1/19	用戶端驗證,程式碼	Network So		
	RSA Certificate Authority	Network Solutions RSA Certifica	2038/1/19	用戶端驗證,程式碼	Network So 🗸		
< >	<				>		
						,	

刪除目前的選取項目・

□ □ w 複製路徑 」[複製 貼上 取] 剪貼簿		A ▲ ○ 編輯 内容 ● 極程記錄 開啟		-8	憑證 詳細資料 憑證路徑	
	蝴蝶 (C:) → OpenSSL-Win32 → bin → MODA				· · · · · · · · · · · · · · · · · · ·	
本機	^ 名稱	修改日期	類型 大	:/J/	w#	
3D 物件	rnd	2025/3/17 下午 05:52	RND 檔案		這個 CA 根憑證不受信任。如果您要啟用信任,請將這個憑證安裝到	1
下載	384419929E529B220A58D42634942482.pem	2025/3/17 下午 05:52	PEM 檔案		信任恨您證授懼単位仔放區。	
文件	index.txt	2025/3/17 下午 05:52	文字文件			
~!!	index.txt.attr	2025/3/17 下午 05:52	ATTR 檔案			
自示	index.txt.old	2025/3/17 下午 05:52	OLD 檔案			
	MODARoot.crt	2025/3/17 下午 05:25	安全性憑證			
	MODARoot.key	2025/3/17下午 05:25	KEY 檔案			
影片	serial	2025/3/17 下午 05:52	福業		發縮: Ministry of Digital Affairs Root Certification Authority - G1	
, 系統經經 (C:)		2025/3/17 下十 04:30	OLD 佃菜 安全計運路		,	
郵件磁碟 (E:)	server ctr	2025/3/17下午 05:52	メエロ ²⁰¹⁰ CCR 横安		簽發者: Ministry of Digital Affairs Root Certification	
應用程式磁碟 (F:)		2025/3/17 下午 05:50	KFY 檔室		Automy Gr	
資料磁碟1 (G:)	server.pfx	2025/3/17 下午 06:08	個人資訊		有效期自 2025/3/17 到 2035/3/15	
資料磁碟2 (H:)	tomcat.jks	2025/3/17 下午 06:12	JKS 檔案			
郵件磁碟 (I:)						
修補程式磁碟 (J:)					安排運動(A) 参照系統	B(C)
郵件磁碟區 (K:)					女教燈籠(I) 短股有章	
資料磁碟A區 (L:)						
資料磁碟B區 (M:)						
。 修诸程式磁磁度 (NF)						確定

▶ openssl.cfg 設定 re	q_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	訪求檔自行輸入即可

🥘 *openssl.cfg - 記事本							- ć) ×	
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明									
req_distinguished_name] countryName #countryName_default countryName_default countryName_min countryName_max	= Country Name (2 letter code) = AU = T₩ = 2 = 2	****	comment Default Change						^
#stateOrProvinceName #stateOrProvinceName_default	= State or Province Name (full name) = Some-State	##### #####	comment Default comment Default						
#localityName #localityName_default	= Locality Name (eg, city) = Taipei City	#####	uncomment Defau	lt					ł
0.organizationName #0.organizationName_default 0.organizationName_default #0.organizationName_default #0.organizationName_default	= Organization Name (eg, company) = Internet Vidgits Pty Ltd = Chunghwa Telecom Co., Ltd. = Executive Yuan = 行政院	****	comment Default						l
# we can do this but it is not 1.organizationName #1.organizationName_default #1.organizationName_default	needed normally :-) = Second Organization Name (eg, company) = World Wide Web Pty Ltd = Ministry of Economic Affairs								
#1.organizationalUnitName #organizationalUnitName_default #1.organizationalUnitName_defau #1.organizationalUnitName_defau 1.organizationalUnitName_defau #1.organizationalUnitName_defau #1.organizationalUnitName_defau	= Organizational Unit Name (eg, section) := lt = Mobile Business Group lt = Data Communications Business Group t = Information Technology Group lt = Ministry Of Foreign Affairs lt = 外交部		<i>#####</i> Change						
#2.organizationalUnitName	= Organizational Unit Name (eg, Third)		##### Change						
#3.organizationalUnitName	= Organizational Unit Name (eg, Third)		##### Change						
commonName #commonName_max #commonName_default commonName_default ≤	= Common Name (e.g. server FQDN or YOUR name) = 64 = Chunghwa Telecom Registration Authority = 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。

🥘 *openssl.cfg - 記事本 - 0 \times 檔案(F) 編輯(E) 格式(O) 檢視(V) 說明 [v3_req] # Extensions to add to a certificate request # asicConstraints = CA:FALSE
basicConstraints=CA:TRUE,pathlen:0
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
keyUsage = digitalSignature, keyEncipherment
keyUsage = digitalSignature
keyUsage = digitalSignature
subjectAltName = @alt_names *#####* Default ##### Change ##### Change ##### 「uncomment Multi-Domain SSL Setup with "Subject Alternative Names"」 [alt_names] DNS.1 = eca.hinet.net DNS.2 = pki.hinet.net #IP.1 = 172.16.1.1 #IP.1 = 10.10.10.1 #IP.1 = 192.168.1.1 #email = caservice@cht.com.tw #email = jianminyao@cht.com.tw #email = publicca@publicca.hinet.net [v3_ca] # Extensions for a typical CA # certificatePolicies= 1.3.6.1.4.1.23459.100.0.1, 1.3.6.1.4.1.23459.100.0.2, 1.3.6.1.4.1.23459.100.0.3, 2.16.886.1.100.0.1, 2.16.886.1.100.0.2, 2.16.886.1.100 certificatePolicies= 2.23.140.1.2.2, 1.3.6.1.4.1.23459.100.0.3 # 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 = critical, cRLSign, keyCertSign ##### 「uncomment keyUsage」 # PKIX recommendation. < 第 277 列 [,] 第 1 行 100% Windows (CRLF) ANSI