

中華電信通用憑證管理中心(PublicCA)

IBM Domino Server憑證請求檔製作與憑證安裝手冊

聲明：本說明文件之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本說明文件所敘述的程序係將本公司安裝相關軟體的經驗分享供申請 SSL 伺服器軟體憑證用戶參考，若因參考本說明文件所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

本說明書的申請程序，已經在Windows系統 + Domino Server 9.0 + Domino Admin 9.0測試過，您所使用的版本或環境可能與本版本有所差異，若是如此則請參考您的Domino相關使用手冊，適度調整申請步驟。

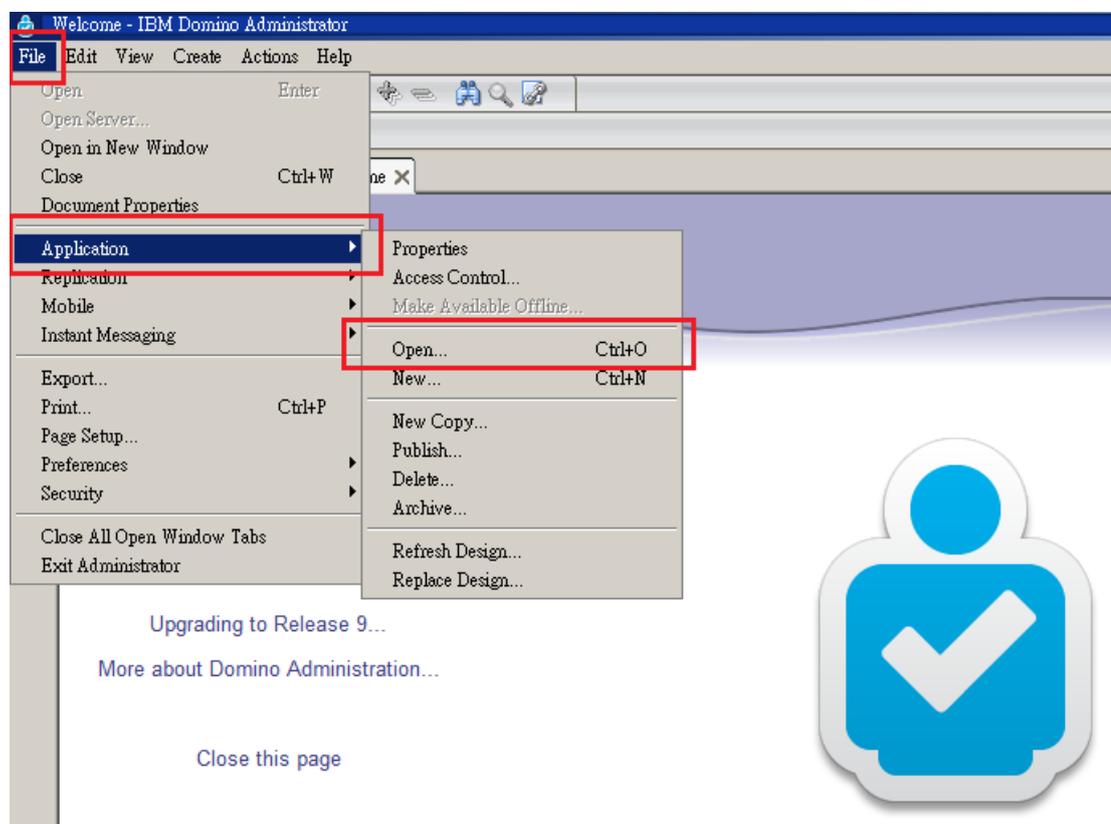
Domino 8.5不支援SHA-256憑證，需至少升級至Domino 9並安裝Fix Pack才可支援SHA-256憑證。

目錄

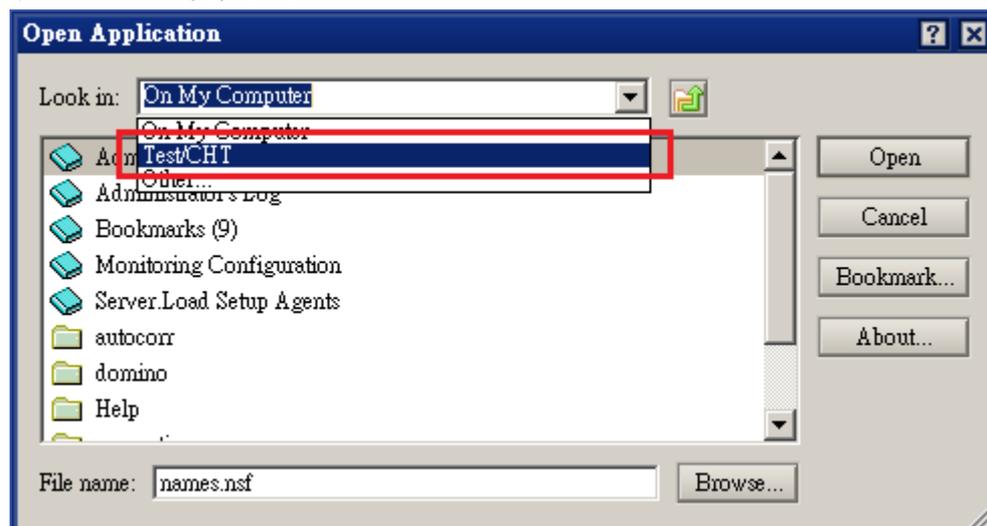
Domino Server SSL 憑證請求檔製作手冊	2
Domino Server SSL 憑證安裝操作手冊	9

Domino Server SSL 憑證請求檔製作手冊

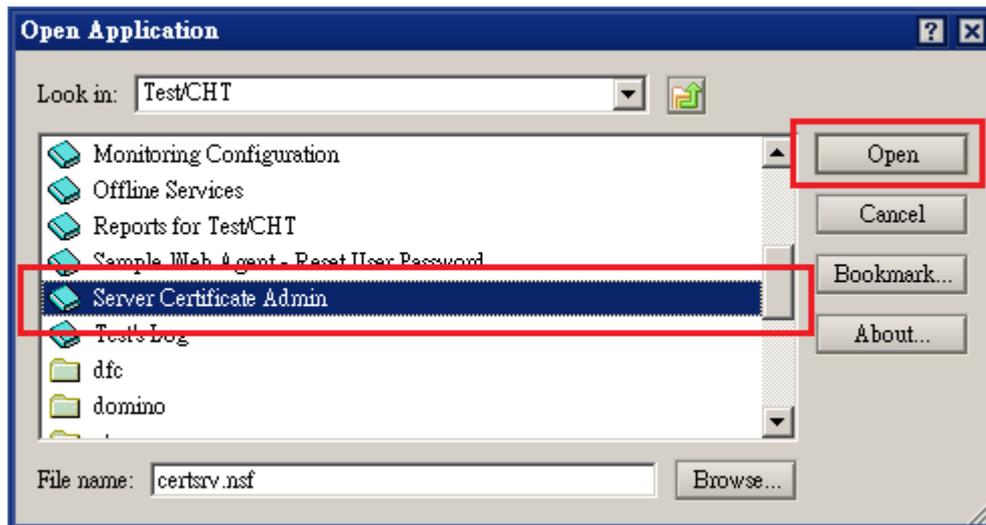
- 一、開啟 IBM Domino Admin，並連線到 Domino Server。
- 二、點選「File」→「Applications」→「Open」。



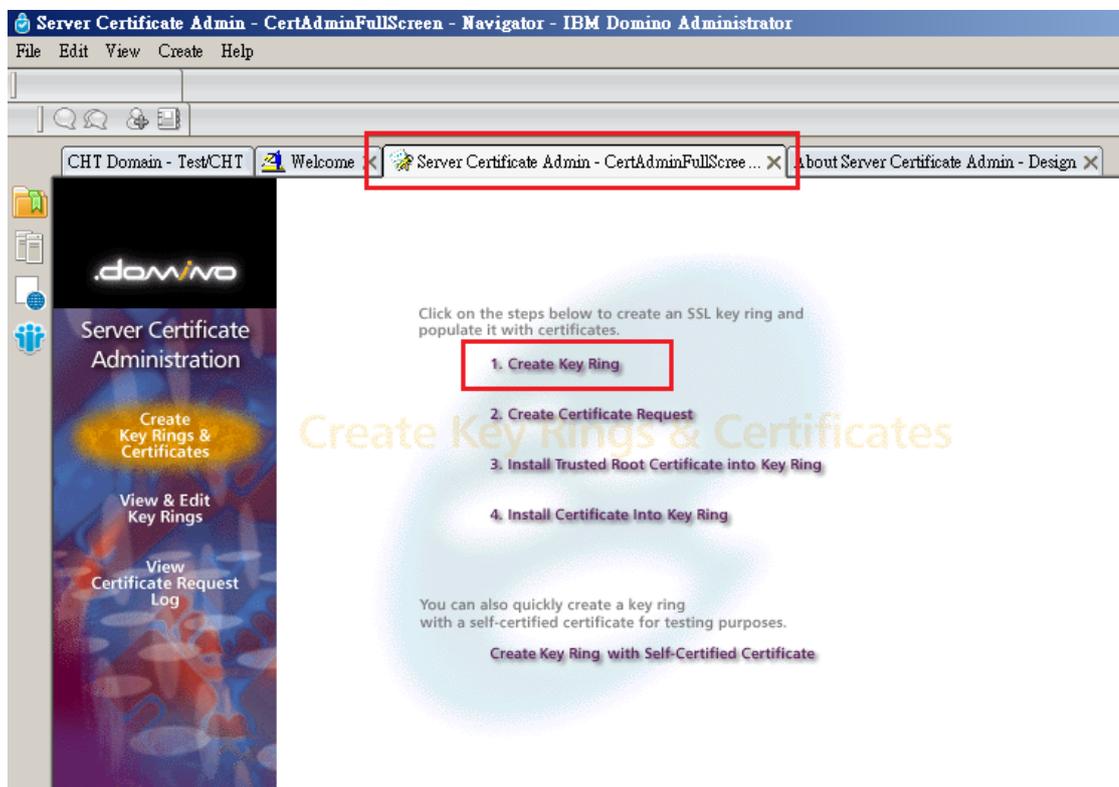
- 三、在 Look in 選擇您的 Domino Server



選擇「Server Certificate Admin」→「Open」



四、點選「Create Key Ring」。



五、依序將資料填入

Key Ring File Name：金鑰儲存的位置，可修改

Key Ring Password、Confirm Password：保護金鑰的密碼

Key Size：金鑰長度，選擇 2048，使用 2048 位元的金鑰長度（請注意依照國際密碼學趨勢，請使用 RSA 2048 位元(含)以上金鑰長度。）

Common Name：填入完全吻合網域名稱(FQDN)

Organization：公司名稱

Organization Unit：組織單位

City or Locality：城市

Country : TW

最後按下 Create Key Ring。

Create Key Ring

The first step in setting up SSL on a server is to create the key ring.
When the key ring is created, a public/private keypair is automatically generated and stored in the key ring.

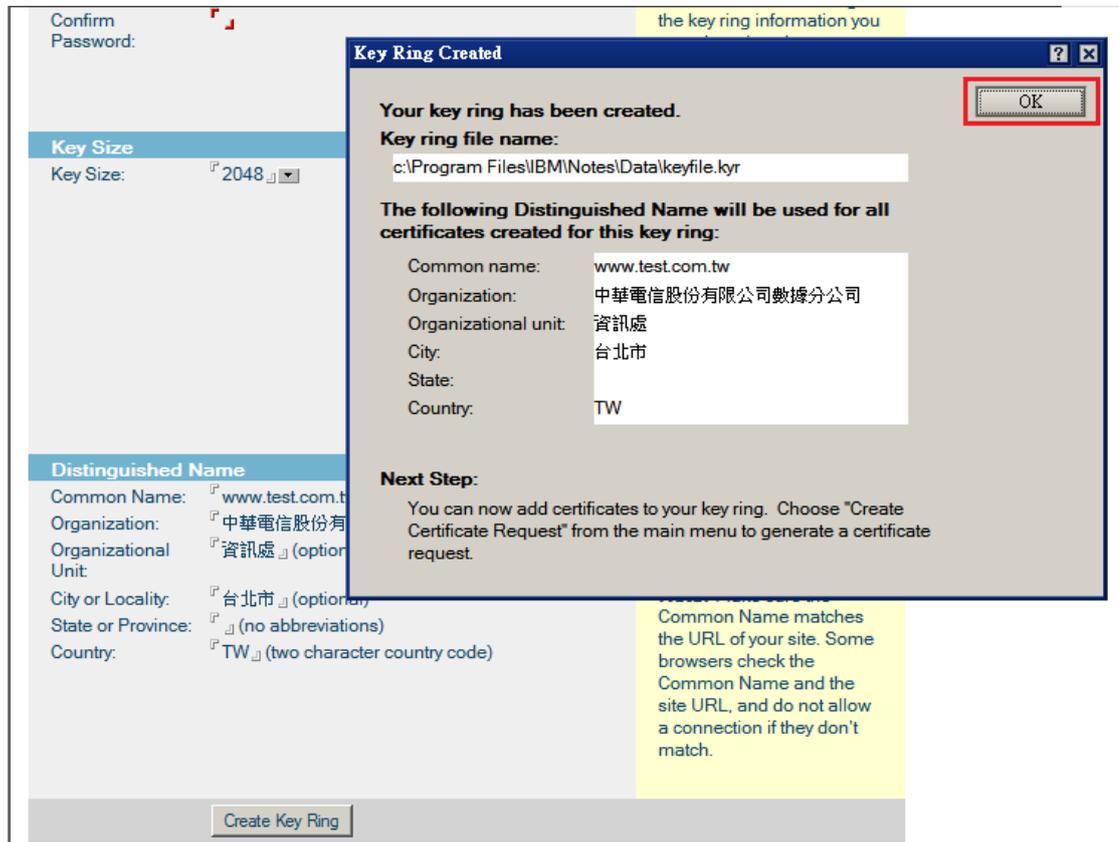
Key Ring Information	Quick Help
<p>Key Ring File Name: 『keyfile.kyr』</p> <p>Key Ring Password: 『*****』</p> <p>Confirm Password: 『*****』</p>	<p>Specify the name and password for the key ring file.</p> <p>Note: You'll be referring to the key ring information you enter here in subsequent steps as you create and install certificates into the key ring.</p>
Key Size	Quick Help
<p>Key Size: 『2048』</p>	<p>Key Size is the size of the public/private key pair in bits. The larger the key size, the greater the encryption strength.</p> <p>Note: This Edition of Domino provides the ability to generate RSA keys at both 1024 bits and 512 bits, in accordance with export regulations worldwide.</p>
Distinguished Name	Quick Help
<p>Common Name: 『www.test.com.tw』</p> <p>Organization: 『中華電信股份有限公司數據分公司』</p> <p>Organizational Unit: 『資訊處』 (optional)</p> <p>City or Locality: 『台北市』 (optional)</p> <p>State or Province: 『』 (no abbreviations)</p> <p>Country: 『TW』 (two character country code)</p>	<p>The Distinguished Name is the information about your site that will appear in any certificates you create.</p> <p>Note: Make sure the Common Name matches the URL of your site. Some browsers check the Common Name and the site URL, and do not allow a connection if they don't match.</p>

Create Key Ring

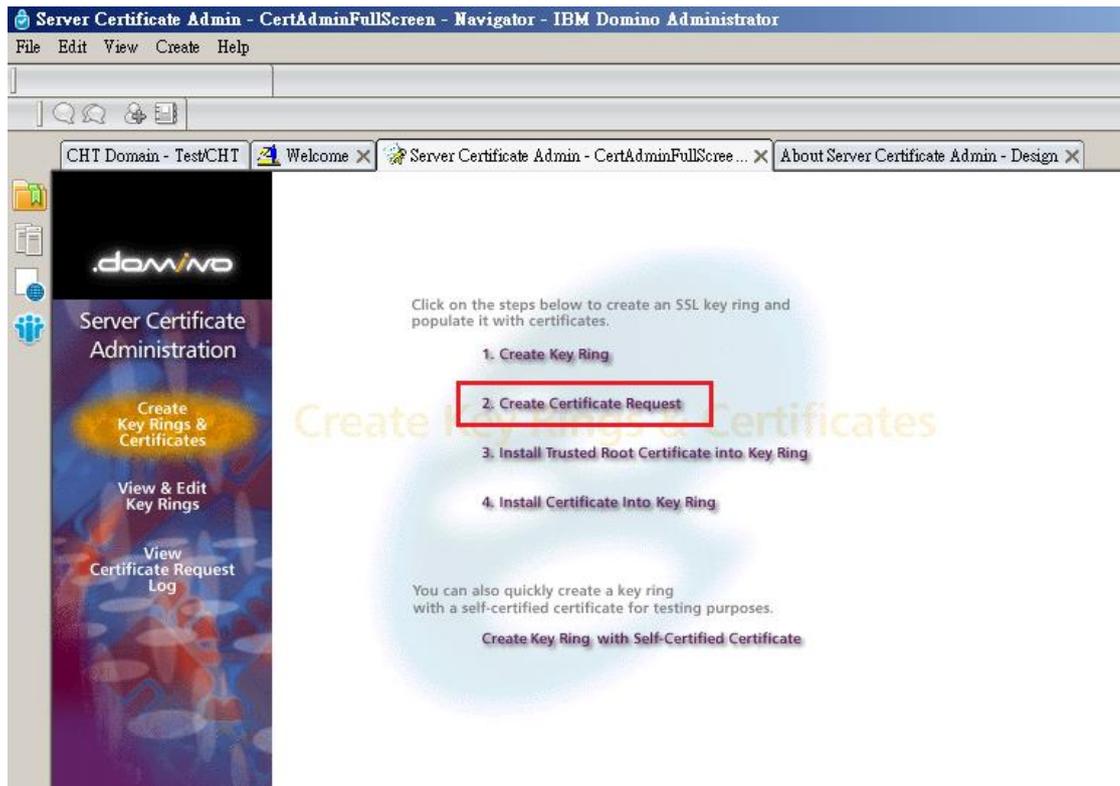
補充說明 1: 中華電信通用憑證管理中心之程式會擷取憑證請求檔中的公開金鑰, 但不會使用憑證請求檔中於步驟五所輸入之資訊, 而是以於申請網頁上所填入的組織資訊與完全吻合網域名稱(Fully Qualified Domain Name, FQDN)為準, 並記載於所簽發的 SSL 憑證裡面的欄位[如

憑證主體名稱(Subject Name)之一般名稱(Common Name)或憑證主體別名(Subject Alternative Name)等欄位]。

六、按下確定。



七、點選「Create Certificate Request」。



八、依照預設值，按下「Create Certificate Request」，此時會要求輸入金鑰保護密碼，輸入完成後，按下確定。

A certificate is required for the public key in the key ring you created. To obtain a certificate, you create a certificate request, and provide it to a Certificate Authority for signing. Use this form to create the certificate request.

Note: Before proceeding you should read the documentation provided by the Certificate Authority you are using to see how they require the certificate request to be delivered.

Key Ring Information	Quick Help
Key Ring File Name <input type="text" value="c:\Program Files\IBM\Notes\Data\keyfile.kyr"/>	Specify the key ring file. Note: The key ring contains the Distinguished Name information that will be included in the certificate request.
Certificate Request Information	
Log Certificate Request <input type="text" value="Yes"/>	Log certificate requests for future reference. Note: Choose "View Certificate Request Log" in the main menu page to see a listing of all logged requests.
Method <input checked="" type="radio"/> Paste into form on CA's site <input type="radio"/> Send to CA by e-mail	Choose how to submit the certificate request to the Certificate Authority. Note: The "Paste" method is recommended if it is supported by the Certificate Authority you are using.
<input type="button" value="Create Certificate Request"/>	

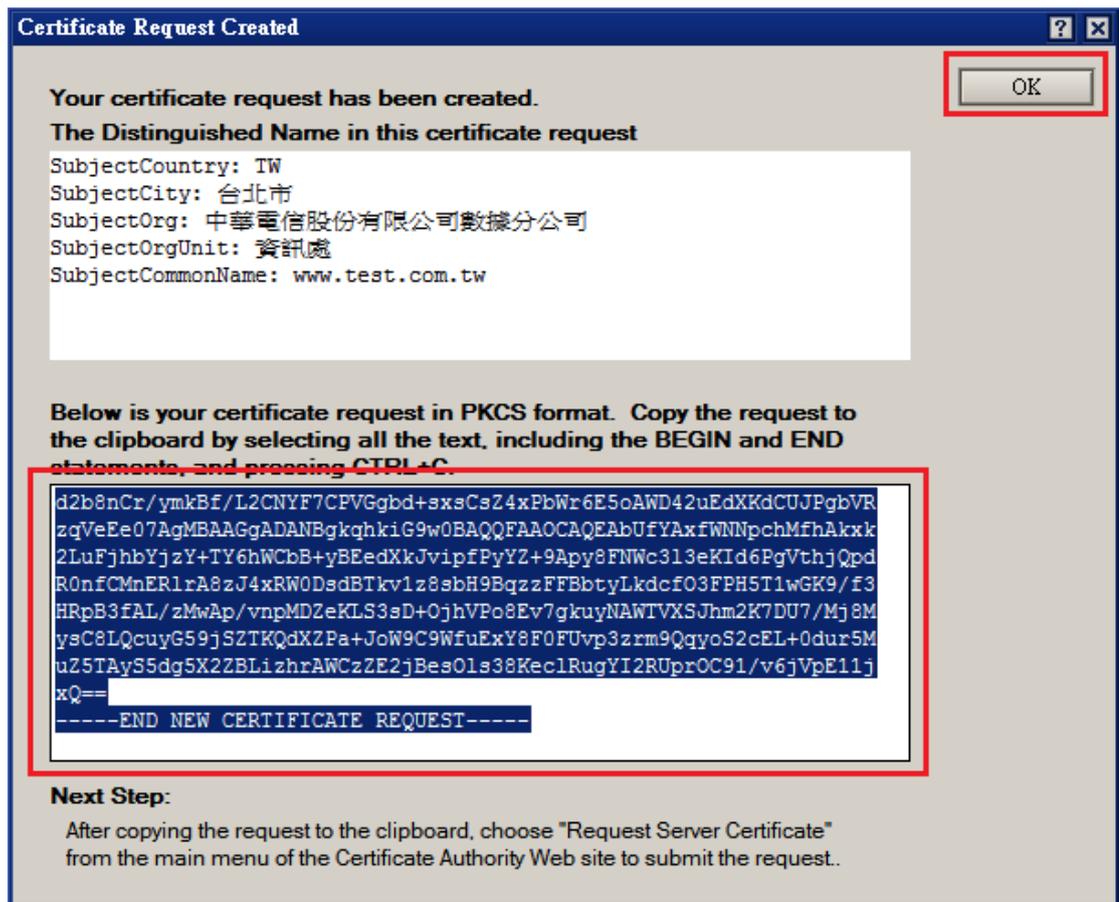
Password Input [?] [X]

Input password for c:\Program Files\IBM\Notes\Data\keyfile.kyr

Warning: An application that is not IBM Notes or Domino may be prompting you for this password. If you do not know the source of this prompt, providing a password may be a security risk.

OK Cancel

九、將下列文字複製到記事本，並儲存成 certreq.txt 後，憑證請求檔就製作完成。



- 十、請持憑證請求檔(certreq.txt)至中華電信通用憑證管理中心網站 (<https://publicca.hinet.net/>) 依照網頁說明申請 SSL 憑證。(若使用 Windows 作業系統可使用記事本(Notepad 程式)開啟憑證請求檔，全選、複製與貼上憑證請求檔內的內容至申請頁面”請貼上憑證請求檔”的表格內。若使用 Mac OS 則可使用”文字編輯”之程式。)
- 十一、若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站電子表單之資訊表單的 IS14-伺服器應用軟體憑證申請/異動單閱讀申請規定後提出申請。

補充說明 2:若您是申請多網域 SSL 憑證或萬用網域 SSL 憑證，僅需要產生 1 個憑證請求檔(產生憑證請求檔之過程就是幫您的伺服器產製 1 對金鑰對，私密金鑰與密碼由伺服器管理者保管，公開金鑰會包含在憑證請求檔內，憑證管理中心審驗您的身分與網域名稱擁有權或控制權後，所簽發的憑證會記載申請者的組織資訊、完全吻合網域名稱與公開金鑰在 SSL 憑證內。後續先安裝 SSL 憑證串鍊於產生憑證請求檔之站台，再將私密金鑰與憑證備份後匯入其他站台，不同廠牌伺服器之匯出與匯入可參考手冊或寫電子郵件給本管理中心技術客服信箱 caservice@cht.com.tw 詢問，不需要每個網站站台都分別產生憑證請求檔。)

Domino Server SSL 憑證安裝操作手冊

一、下載憑證串鏈，包含 3 張憑證，分別是(1)eCA 根憑證(ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證)、(2)PublicCA 中繼憑證(中華電信通用憑證管理中心自身憑證)與(3)PublicCA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：

1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、PublicCA 中繼憑證(檔名為 PublicCA2_64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈 3 個檔案。

2. 從網站查詢與下載：

eCA 憑證：

http://epki.com.tw/download/ROOTeCA_64.crt

PublicCA G2 憑證：

http://epki.com.tw/download/PublicCA2_64.crt

SSL 憑證下載：您若是本公司之客戶，請至 PublicCA 網站點選「SSL 憑證服務」再點選「SSL 憑證查詢及下載」，進行 SSL 憑證下載。

若您是中華電信之員工，負責管理單位之伺服器，請至

<http://chtra.cht.com.tw/> 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證。

二、開啟 IBM Domino Admin 並開啟 Server Certificate Admin。

三、點選「Install Trusted Root Certificate into Key Ring」，進入憑證安裝畫面。



四、安裝 eCA 根憑證

Certificate Label：可填入 ROOTeCA

Certificate Source：選擇 File

File Name：eCA 根憑證的位置

File Format：選擇 Base64 encoding

最後點選「Merge Trusted Root Certificate into Key Ring」並輸入密碼。

Install Trusted Root Certificate

Use this form to install the Certificate Authority Trusted Root certificate into the server key ring. If you haven't already done so, first obtain the Certificate Authority Trusted Root certificate by choosing "Accept This Authority In Your Server" from the main menu of Certificate Authority Web site. **Note:** This step of installing the Certificate Authority Trusted Root certificate into your server key ring is recommended before installing certificates signed by this Certificate Authority into the key ring.

Key Ring Information	Quick Help
Key Ring File Name <input type="text" value="c:\Program Files\IBM\Notes\Data\keyfile.kyr"/>	Specify the key ring file.
Certificate Information	
Certificate Label <input type="text" value="ROOTeCA"/>	The identifier you'll see for this certificate when you choose "View & Edit Key Ring" from the main menu.
Certificate Source <input checked="" type="radio"/> File <input type="radio"/> Clipboard	The source of the certificate can be from a file or from the clipboard.
File Name <input type="text" value="C:\ROOTeCA_64.crt"/>	The name of the file containing the CA's Trusted Root certificate.
File Format <input checked="" type="radio"/> Base 64 encoding <input type="radio"/> Binary file format	Base 64 encoding is most common. Binary format is used by some CA's (e.g., CAs based on the Microsoft CA Server).
<input type="button" value="Merge Trusted Root Certificate into Key Ring"/>	

Password Input [?] [X]

Input password for c:\Program Files\IBM\Notes\Data\keyfile.kyr

Warning: An application that is not IBM Notes or Domino may be prompting you for this password. If you do not know the source of this prompt, providing a password may be a security risk.

OK

Cancel

查看憑證訊息，並按下確定。



五、再次點選「Install Trusted Root Certificate into Key Ring」，安裝 PublicCA G2 中繼憑證，如 eCA 根憑證安裝步驟。

Install Trusted Root Certificate

Use this form to install the Certificate Authority Trusted Root certificate into the server key ring. If you haven't already done so, first obtain the Certificate Authority Trusted Root certificate by choosing "Accept This Authority In Your Server" from the main menu of Certificate Authority Web site. **Note:** This step of installing the Certificate Authority Trusted Root certificate into your server key ring is recommended before installing certificates signed by this Certificate Authority into the key ring.

Key Ring Information	Quick Help
Key Ring File Name <input type="text" value="c:\Program Files\IBM\Notes\Data\keyfile.kyr"/>	Specify the key ring file.
Certificate Information	
Certificate Label <input type="text" value="PublicCA2"/>	The identifier you'll see for this certificate when you choose "View & Edit Key Ring" from the main menu.
Certificate Source <input checked="" type="radio"/> File <input type="radio"/> Clipboard	The source of the certificate can be from a file or from the clipboard.
File Name <input type="text" value="C:\PublicCA2_64.crt"/>	The name of the file containing the CA's Trusted Root certificate.
File Format <input checked="" type="radio"/> Base 64 encoding <input type="radio"/> Binary file format	Base 64 encoding is most common. Binary format is used by some CA's (e.g., CAs based on the Microsoft CA Server).
<input type="button" value="Merge Trusted Root Certificate into Key Ring"/>	

Merge Trusted Root Certificate Confirmation

This certificate will be merged into your key ring as a Trusted Root. Check the information below, then click OK to install the certificate, or Cancel to stop the operation.

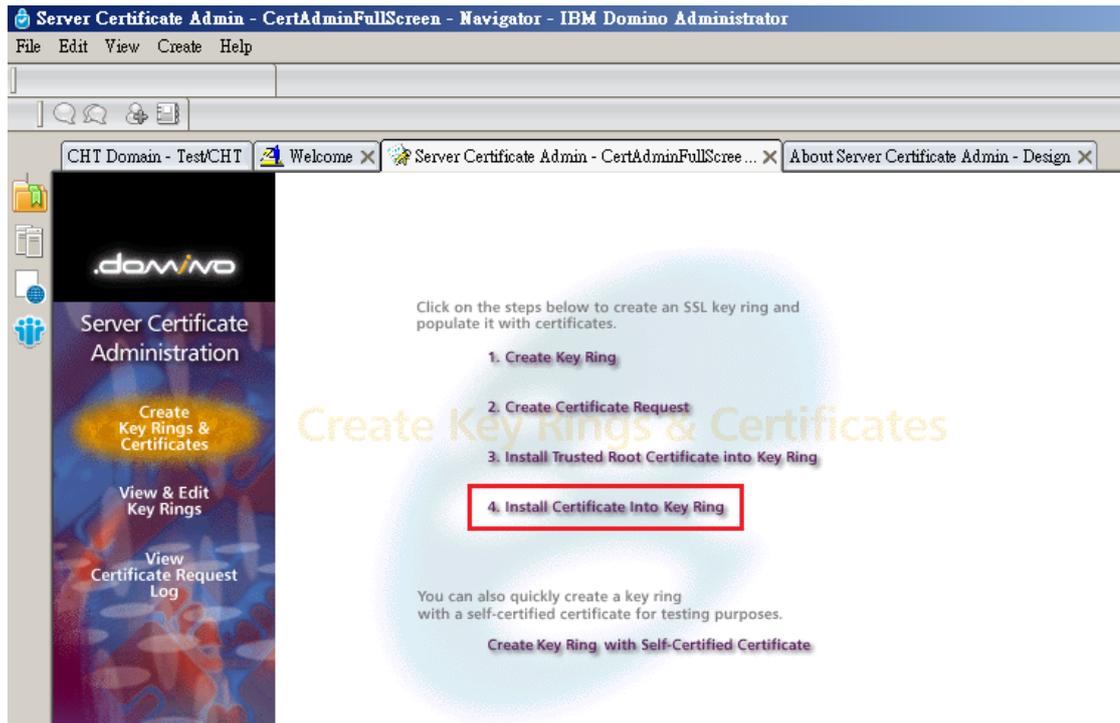
Key ring file name:

Certificate Subject:	Certificate Issuer:
SubjectCountry: TW SubjectOrg: Chunghwa Telecom Co., Ltd. SubjectOrgUnit: Public Certification Authority - G2	IssuerCountry: TW IssuerOrg: Chunghwa Telecom Co., Ltd. IssuerOrgUnit: ePKI Root Certification Authority

StartDate:

EndDate:

六、點選「Install Certificate into Key Ring」，進入憑證安裝畫面。



七、安裝 SSL 憑證

Certificate Source：選擇 File

File Name：SSL 憑證的存放位置

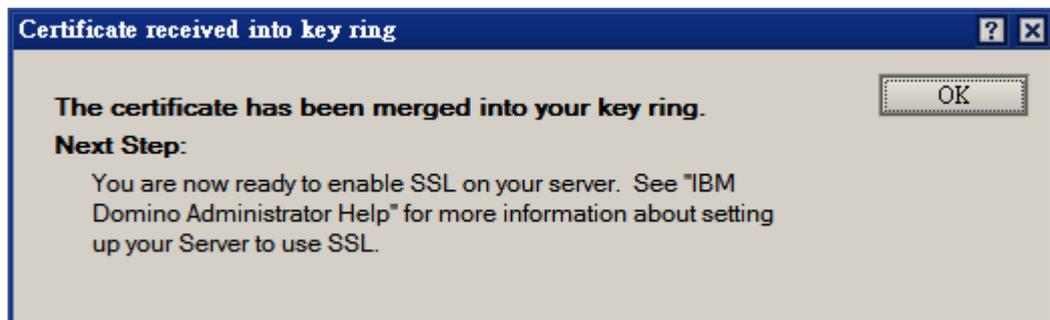
最後點選「Merge Certificate into Key Ring」並輸入密碼。

Install Certificate into Key Ring

The Certificate Authority will notify when your signed certificate is ready. The specifics depend on the Certificate Authority, but typically you will receive an e-mail specifying a URL where you can pick up the certificate. Once you have obtained the signed certificate, this form lets you install it into your key ring. **Note:** Before installing this certificate, it is recommended that you install the certificate of the signing Certificate Authority in your key ring as a Trusted Root. If you haven't already done so, choose "Accept This Authority In Your Server" from the main menu of the Certificate Authority Web site to obtain the CA certificate.

Key Ring Information	Quick Help
Key Ring File Name <input type="text" value="c:\Program Files\IBM\Notes\Data\keyfile.kyr"/>	Specify the key ring file.
Certificate Information	
<div style="border: 2px solid red; padding: 5px;"> Certificate Source <input checked="" type="radio"/> File <input type="radio"/> Clipboard </div>	The source of the certificate can be from a file or from the clipboard.
File Name <input type="text" value="C:\67BCB6D616FA8EF6FC95DD51FA8E02CD.cer"/>	The name of the file that holds the signed certificate.
<div style="border: 2px solid red; display: inline-block; padding: 5px 20px; font-weight: bold;">Merge Certificate into Key Ring</div>	

確認資訊後，按下 OK。



八、最後，請將 key.kyr、key.sth 由 Notes\Data 下，移至 Domino\Data 下，即完成 SSL 憑證之安裝。

另外，您可能需要開啟 Domino Server 上的 https 功能。

九、依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。

十、安裝 SSL 安全認證標章：

請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。

請中華電信公司負責維護網站的同仁，參考從電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。