

中華電信通用憑證管理中心 (PublicCA)

IBM Websphere Application Server 8.5 伺服器憑證請求檔製作

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起的任何損害，本公司不負任何損害賠償責任。

程式使用版本：Websphere Application Server 8.5

- 一、 透過瀏覽器連線到 Websphere Integrated Solutions Console。
- 二、 依步驟點選「安全」→「SSL 憑證和金鑰管理」→「金鑰儲存庫和憑證」。

The screenshot shows the Websphere Integrated Solutions Console interface. On the left is a navigation tree with the following items: 歡迎使用, 引導活動, 伺服器, 應用程式, 服務, 資源, 安全 (highlighted with a red circle), 廣域安全, 安全網域, 管理授權群組, SSL 憑證和金鑰管理 (highlighted with a red circle), 安全審核, 匯流排安全, 環境, 系統管理, 使用者和群組, 監視和調整, 疑難排解, 服務整合. The main content area is titled 'SSL 憑證和金鑰管理' and contains sections for 'SSL 配置', '配置設定', and '管理端點安全配置'. A '相關項目' sidebar on the right lists: SSL 配置, 動態出埠端點 SSL 配置, 金鑰儲存庫和憑證 (highlighted with a red circle), 金鑰基, 金鑰集群組, 金鑰管理程式, 信任管理程式, 憑證管理中心 (CA) 用戶端配置. At the bottom of the main content area are buttons for '套用' and '重設'.

- 三、 點選「新建...」後，依序填入必要資訊後，按下套用→確定。

SSL 憑證和金鑰管理 > 金鑰儲存庫和憑證 > 新建...

定義金鑰儲存庫類型，其中包括加密法、RACF(R)、CMS、Java(TM)，以及所有信任儲存庫類型。

一般內容

* 名稱

sslkeystore

說明

SSL金鑰儲存庫

管理範圍

(cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01

* 路徑

D:\sslkeystore.p12

* 密碼

●●●●●●

* 確認密碼

●●●●●●

類型

PKCS12

 唯讀 啟動時起始設定 啟用硬體裝置的加密作業

套用

確定

重設

取消

返回原畫面後，點選儲存。

消息

- 已對您的本端配置做了變更。您可以：
- 直接儲存至主要配置中。
 - 在儲存或捨棄之前，檢閱變更。
- 伺服器可能需要重新啟動，這些變更才能生效。

SSL 憑證和金鑰管理 > 金鑰儲存庫和憑證

定義金鑰儲存庫類型，其中包括加密法、RACF(R)、CMS、Java(TM)，以及所有信任儲存庫類型。

Keystore 用法

SSL 金鑰儲存庫

喜好設定

新建...

刪除

變更密碼...

交換簽章者...

四、點選剛剛建立的儲存庫後，按下畫面右邊的「個人憑證要求」。

SSL 憑證和金鑰管理

[SSL 憑證和金鑰管理](#) > [金鑰儲存庫和憑證](#) > [sslkeystore](#)

定義金鑰儲存庫類型，其中包括加密法、RACF(R)、CMS、Java(TM)，以及所有信任儲存庫類型。

一般內容	其他內容
<p>名稱 sslkeystore</p> <p>說明 SSL金鑰儲存庫</p> <p>管理範圍 (cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01</p> <p>路徑 D:\sslkeystore.p12</p> <p>* 密碼 <input type="password"/></p> <p>類型 PKCS12</p>	<ul style="list-style-type: none"> ■ 簽章者憑證 ■ 個人憑證 ■ 個人憑證要求 ■ 自訂內容

五、 依序輸入所需資訊：

憑證要求檔案：憑證請求檔存放的位置

金鑰標籤：識別名

簽章演算法：SHA1withRSA

金鑰大小：2048。請注意依照國際密碼學趨勢，請使用 2048 位元(含)以上金鑰長度。

一般名稱：輸入網站的 domain name

按下「套用」後，會顯示憑證請求檔的相關資訊。

[SSL 憑證和金鑰管理](#) > [金鑰儲存庫和憑證](#) > [sslkeystore](#) > [個人憑證要求](#) > 新建...

管理個人憑證要求，這些要求是憑證管理中心 (CA) 將要簽章之憑證的暫時位置保留區。

一般內容

* 憑證要求的檔案

D:\certreq.txt

憑證資訊

* 金鑰標籤

ssl

簽章演算法

SHA1withRSA

金鑰大小

2048 位元

* 一般名稱

www.test.com.tw

組織

中華電信股份有限公司數據分公司

組織單位

政府網路處

地區

州/省 (縣/市)

台北市

郵遞區號

國家或地區

TW

[SSL 憑證和金鑰管理](#) > [金鑰儲存庫和憑證](#) > [sslkeystore](#) > [個人憑證要求](#) > [ssl](#)

管理個人憑證要求，這些要求是憑證管理中心 (CA) 將要簽章之憑證的暫時位置保留區。

一般內容

憑證要求的檔案

D:/certreq.txt

金鑰標籤

ssl

金鑰大小

2048 位元

要求者

CN=www.test.com.tw, OU=政府網路處, O=中華電信股份有限公司數據分公司, ST=台北市, C=TW

指紋 (SHA 摘要)

17:F5:71:87:BD:EF:30:C7:BF:FE:F7:41:AB:99:3E:A0:33:55:5F:6F

簽章演算法

SHA1withRSA(1.2.840.113549.1.1.5)

上一步

- 六、 此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至中華電信通用憑證管理中心網站 (<http://publicca.hinet.net/>) 依照網頁說明申請 SSL 憑證。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 IS14-伺服器應用軟體憑證申請/異動單提出申請。