中華電信通用憑證管理中心（Public**CA**）

IBM Websphere Application Server 8.5 伺服器憑證安裝操作

程式使用版本：IBM Websphere Application Server 8.5

一、 下載 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)與 PublicCA 中繼憑證(中華電信通用憑證管理中心自身憑證)有以下兩種方式：

1. eCA：http://epki.com.tw/download/ROOTeCA_64.crt
   PublicCA：http://publicca.hinet.net/CHTM/download/PublicCA_64.crt
2. 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，解壓縮後包括三個檔案，分別是 eCA 跟憑證(檔名爲 b64.cer)、PublicCA 中繼憑證 pubcab64.cer 與 xxHDxxxxxxxx.crt 是簽發給用戶的 SSL 伺服器軟體憑證，其中 xxHDxxxxxxxx 是案件流水號。
   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。解壓縮後可以進行安裝。

二、 開啓 Websphere Integrated Solutions Console，登錄後並開啓 SSL 憑證與金鑰管理介面。

三、　　點選「金鑰儲存庫和憑證」→先前建立的 keystore→點選右邊的「簽章者憑證」。

SSL 配置

Secure Socket Layer (SSL) 通訊協定提供遠端伺服器程序或端點之間的安全通訊。SSL 安全可用來建立端點的入埠和出埠通訊。如果要建立安全通訊，必須為端點指定憑證和 SSL 配置。

在本產品的舊版中，必須手動為 Secure Sockets Layer (SSL) 配置每一個端點。但在本版中，您可以為整個應用程式服務環境定義單一配置。這項功能可讓您集中管理安全通訊。此外，您可以置換預設的 Cell 層次 SSL 配置，以便在多個節點環境中建立信任區域。

如果您使用了移轉公用程式將安全環境移轉至本版，則會還原各個不同端點的舊有 Secure Sockets Layer (SSL) 配置。不過，您必須重新配置 SSL，才能得到集中管理功能的好處。

配置設定

管理端點安全配置

管理憑證有效期限

管理 FIPS

☑ 當發生 SSL 配置變更時，動態更新執行時期

套用 重設

相關項目

- SSL 配置
- 動態出埠端點 SSL 配置
- 金鑰儲存庫和憑證
- 金鑰集
- 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

⊞ 喜好設定

新建... 刪除 變更密碼... 交換簽章者...

選取	名稱	說明	管理範圍	路徑
您可以管理下列資源：				
☐	NodeDefaultKeyStore	CHT-HP49R5ZDNode01 的預設金鑰儲存庫	(cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01	${CONFIG_ROOT}/cells/CHT-HP49R5ZDNode01Cell/nodes/CHT-HP49R5ZDNode01/key.p12
☐	NodeDefaultTrustStore	CHT-HP49R5ZDNode01 的預設信任儲存庫	(cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01	${CONFIG_ROOT}/cells/CHT-HP49R5ZDNode01Cell/nodes/CHT-HP49R5ZDNode01/trust.p12
☐	sslkeystore	SSL金鑰儲存庫	(cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01	D:\sslkeystore.p12
☐	test		(cell):CHT-HP49R5ZDNode01Cell:(node):CHT-HP49R5ZDNode01	D:\test.p12

總計 4

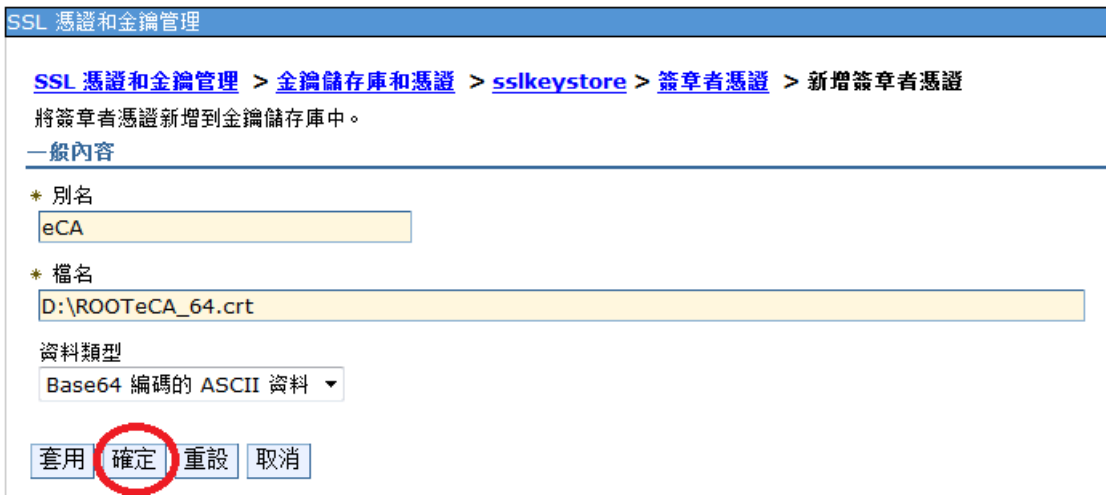
四、 安裝 eCA 根憑證與 PublicCA 中繼憑證

點選「新增」

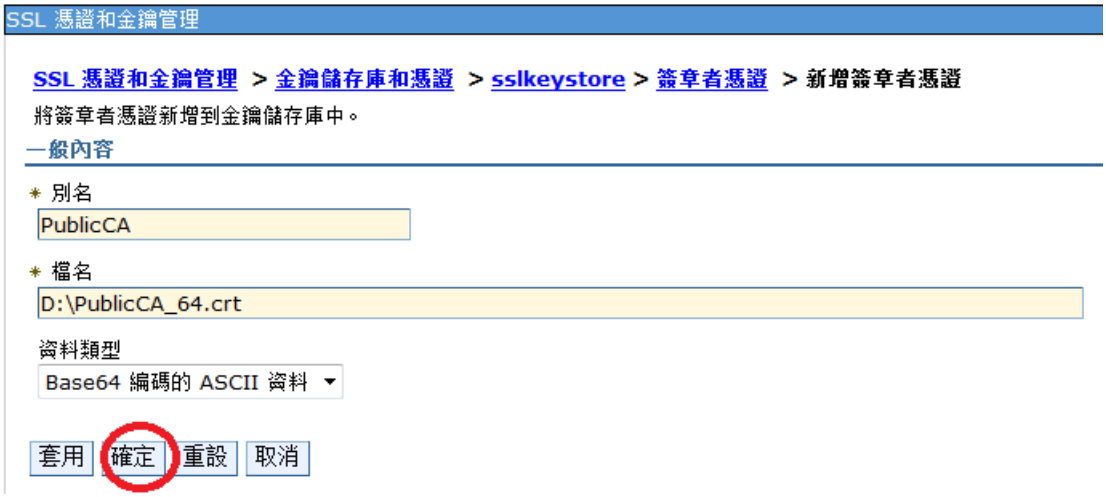
別名：eCA 憑證的名稱

檔名：eCA 憑證位置

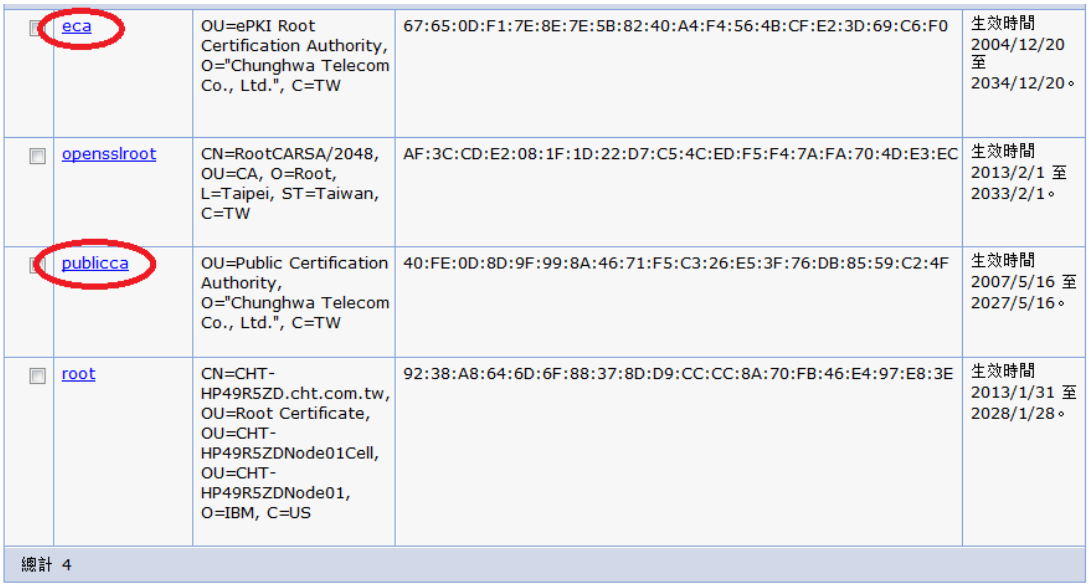
填寫完成後，按下確定鍵。



以相同方法安裝 PublicCA 中繼憑證。



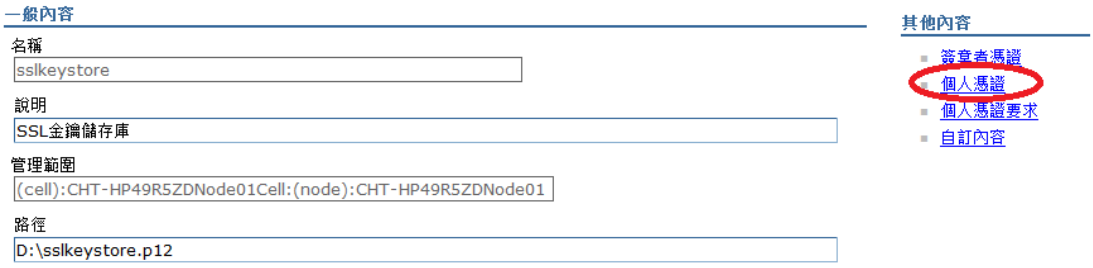
完成後，將可在以下畫面看到 eCA 與 PublicCA 的憑證資訊。



	eca	OU=ePKI Root Certification Authority, O="Chunghwa Telecom Co., Ltd.", C=TW	67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0	生效時間 2004/12/20 至 2034/12/20。
	openssIroot	CN=RootCARSA/2048, OU=CA, O=Root, L=Taipei, ST=Taiwan, C=TW	AF:3C:CD:E2:08:1F:1D:22:D7:C5:4C:ED:F5:F4:7A:FA:70:4D:E3:EC	生效時間 2013/2/1 至 2033/2/1。
	publicca	OU=Public Certification Authority, O="Chunghwa Telecom Co., Ltd.", C=TW	40:FE:0D:8D:9F:99:8A:46:71:F5:C3:26:E5:3F:76:DB:85:59:C2:4F	生效時間 2007/5/16 至 2027/5/16。
	root	CN=CHT-HP49R5ZD.cht.com.tw, OU=Root Certificate, OU=CHT-HP49R5ZDNode01Cell, OU=CHT-HP49R5ZDNode01, O=IBM, C=US	92:38:A8:64:6D:6F:88:37:8D:D9:CC:CC:8A:70:FB:46:E4:97:E8:3E	生效時間 2013/1/31 至 2028/1/28。

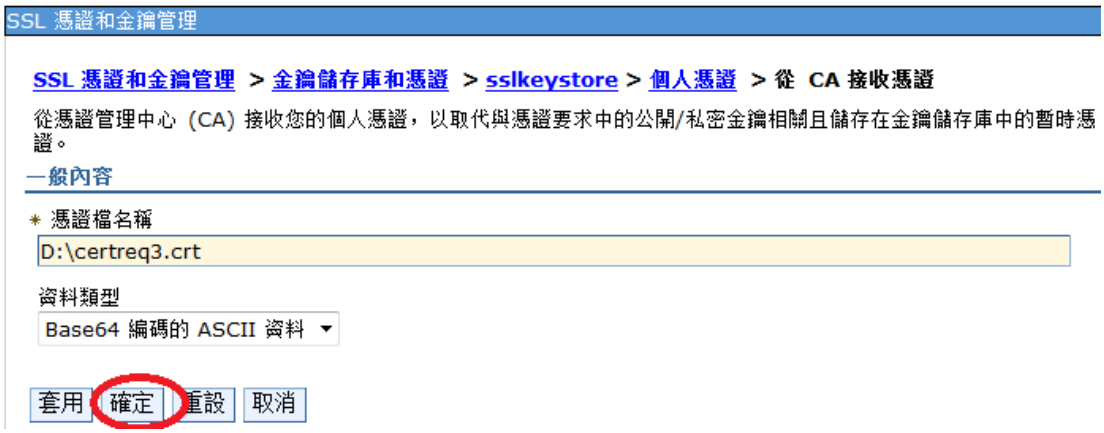
總計 4

五、 回到上一頁後，點選個人憑證。



點選「從憑證管理中心接收・・・」

填入個人憑證位置後，按下「確定」鍵。



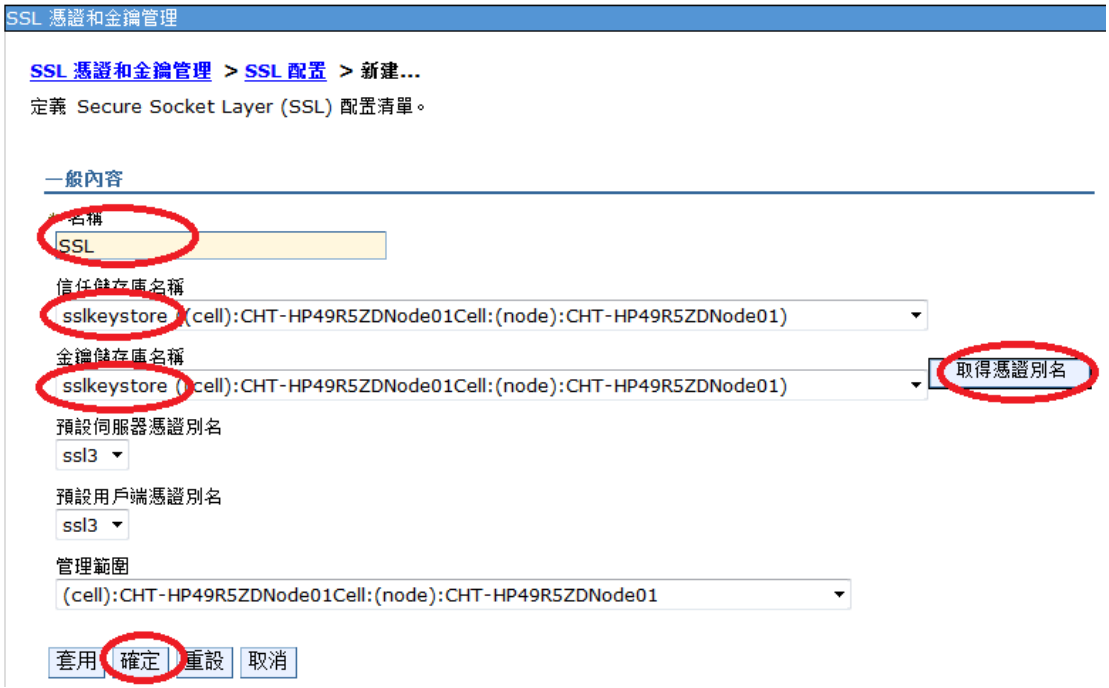
若跟憑證、中繼憑證、個人憑證皆有效的情況下，系統會自動將憑證串列建立起來。

(下圖以 OpenSSL 的自簽憑證當 root CA 簽發 SSL 憑證給 www.test.com.tw。)

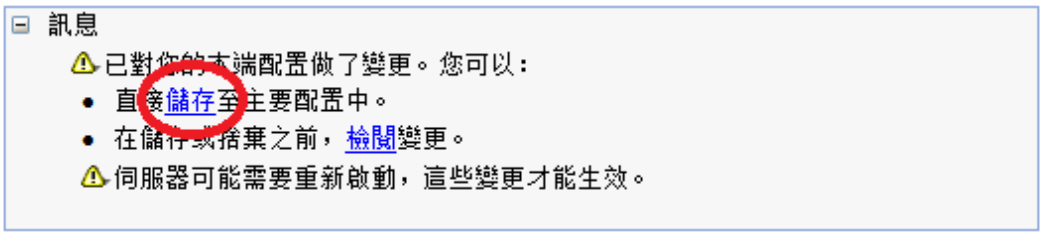
六、　回到 SSL 憑證和金鑰管理，接著點選「SSL 配置」

點選「新建」。

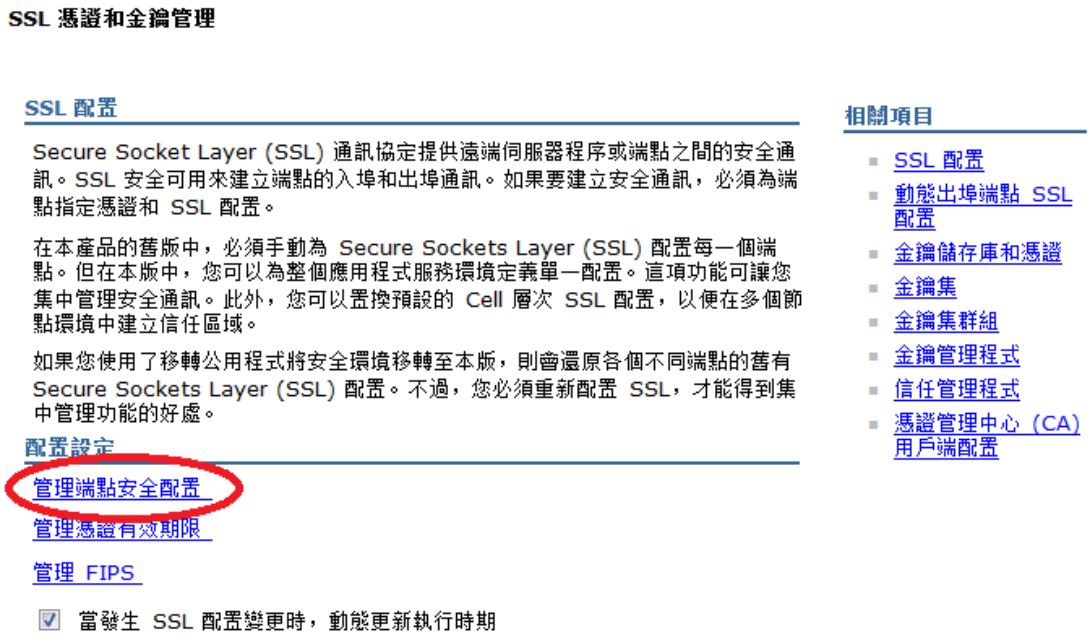
依序填入「名稱」，下拉式選擇之前有建立 SSL 憑證的儲存庫，按下「取得憑證別名」，確認資訊無誤後，方可按下「確定鍵」鍵。



點選「儲存」。



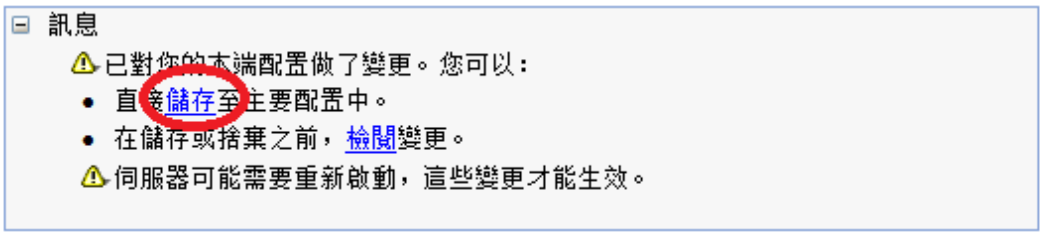
七、 最後點選「管理端點安全配置」



對需要的入埠與出埠做設定。

以入埠爲例，下拉式選單選擇剛剛在 SSL 配置完成的名稱，之後按下「更新憑證別名清單」，最後按下「確定」。

設定完成後，點選「儲存」。



八、　　到此爲止，已完成 SSL 憑證之安裝與設定，可以嘗試以「https」的方式瀏覽網頁，確認 SSL 憑證已經安裝成功。