

# 中華電信通用憑證管理中心(PublicCA)

Redhat Enterprise 4 + Oracle Application Server 10.1.3 HTTP 2.0

## SSL 憑證請求檔製作與安裝手冊

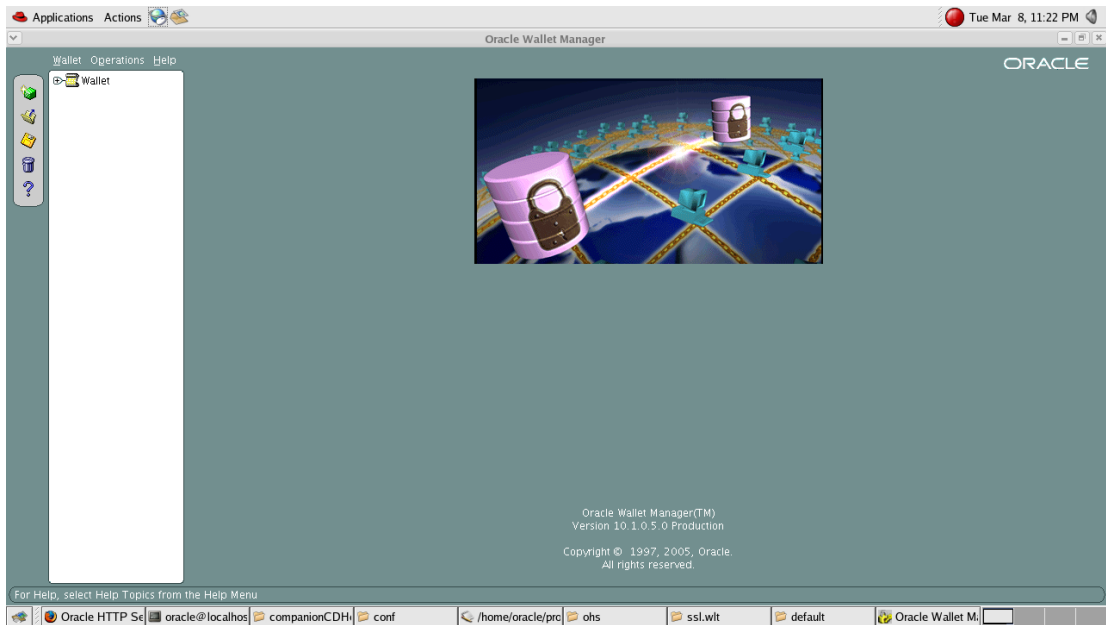
聲明：本說明文件之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本說明文件所敘述的程序係將本公司安裝相關軟體的經驗分享供申請 SSL 伺服器軟體憑證用戶參考，若因參考本說明文件所敘述的程序而起的任何損害，本公司不負任何損害賠償責任。

1. 進入安裝 Oracle Applications Server 的路徑，進入 bin 資料

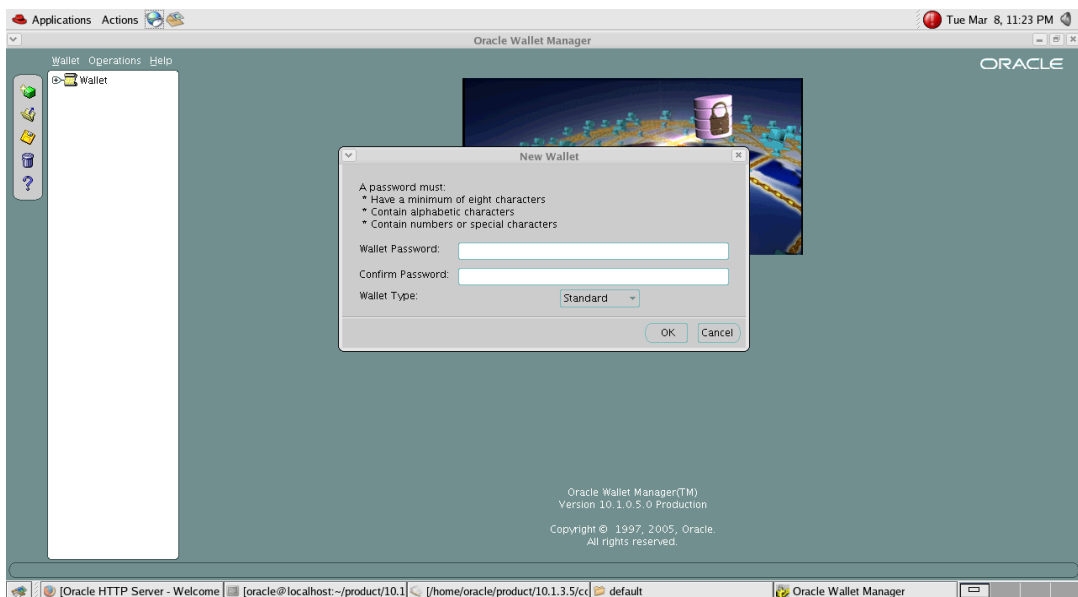
夾，找到 owm 執行後開啟 Oracle Wallet Manager

```
localhost.localdomain> cd $ORACLE_HOME
localhost.localdomain> ls
assistants  install.platform  ldap      opmn      plsql      slax
bin         inventory        lib       oracore   precomp    sqlplus
cfgtoollogs jdbc             network   oraInst.loc rdbms      srvn
dcm        jdk              nls       oui        relnotes   sysman
diagnostics jlib            ohs       owm        root.sh    uix
install    jre             OPatch    perl       root.sh.old xdk
localhost.localdomain> cd bin
localhost.localdomain> ./owm
□
```

---

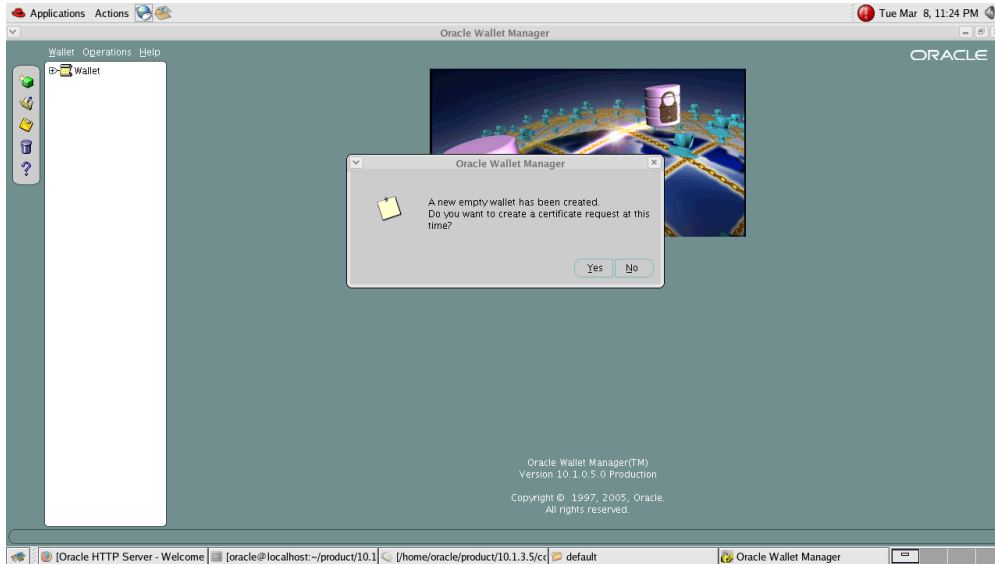


2. 您可以從左邊的 ICON 選擇新增 Wallet 或開啟舊有的 Wallet，本手冊以新增一個 New Wallet 說明。



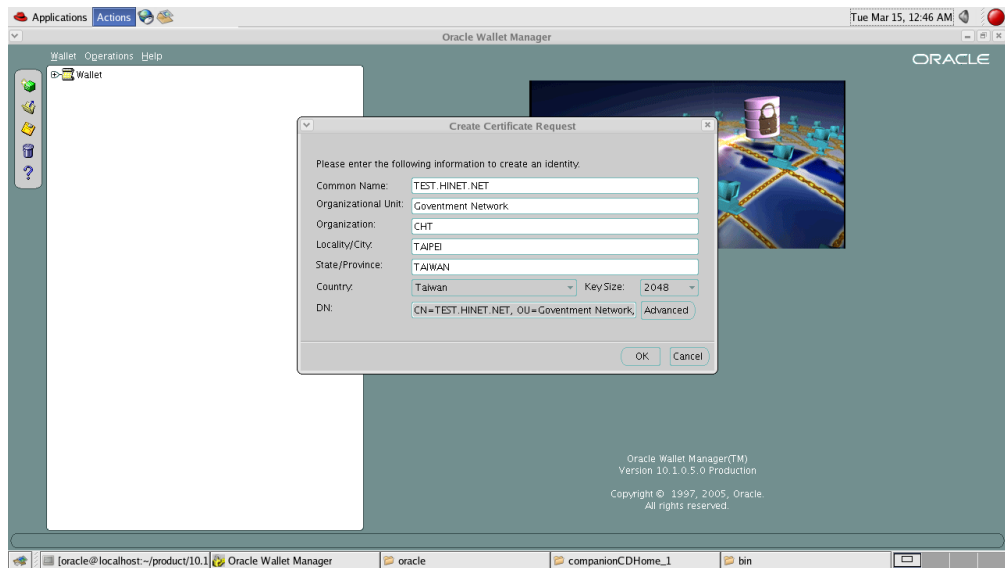
3. 新增 Wallet 後，會問您要不要順便產製一個新的憑證請求檔（一種包含伺服器公鑰與基本資訊，以利進行憑證申請的檔案），也可

稍候在圖形介面上方的 Function Bar > Operations 去新增憑證請求檔。

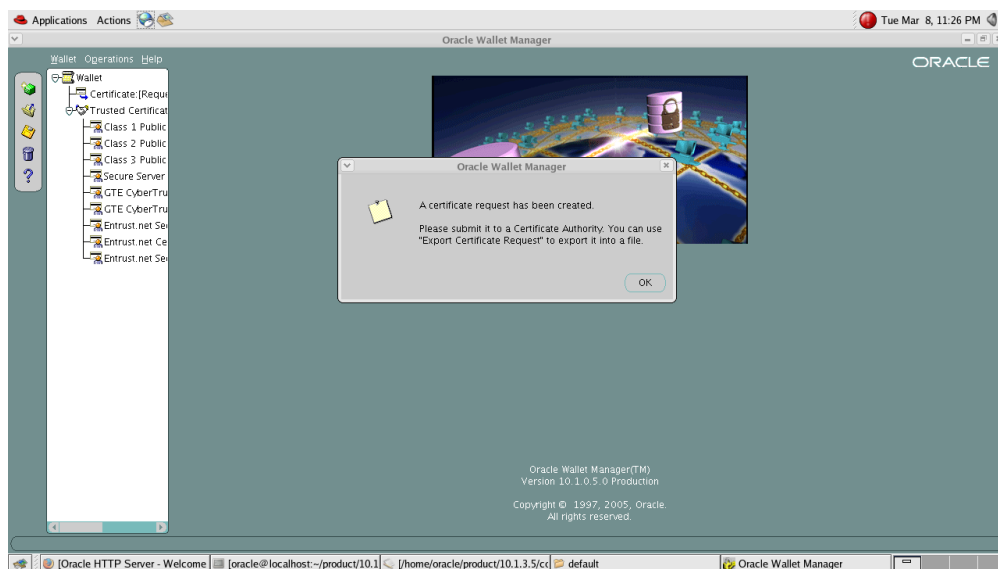


4. 進行 Wallet 所要求的 SSL 憑證申請的唯一識別資料填寫。

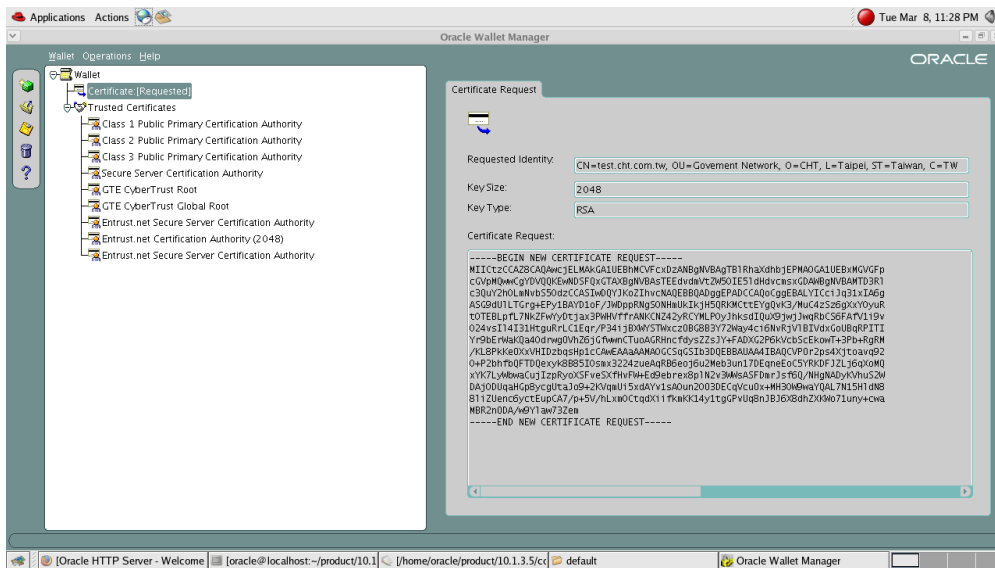
PublicCA SSL 憑證會採用憑證請求檔之公鑰資訊，但不會使用下圖所填寫之資訊(例如 Common Name、Organizational Unit、Organization、Locality/City)於所簽發之 SSL 憑證的資訊欄位中，憑證註記之唯一識別資訊是以要於 PublicCA 網站之申請介面填寫並經過認證的資訊為主。此介面右下方之金鑰長度(key size)可選取 1024 位元、2048 位元或 4096 位元，請選取目前安全性較佳且符合各大瀏覽器或作業系統建議之 2048 位元(含)以上的金鑰長度。



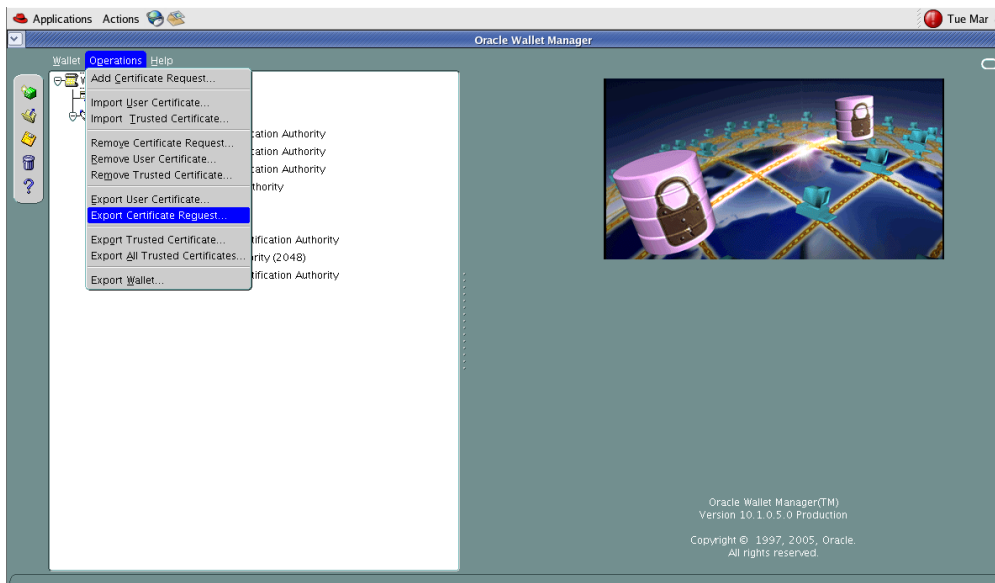
5. 資料輸入完畢後，請點選 OK，系統會提示您可以將憑證請求檔匯出以便申請憑證。



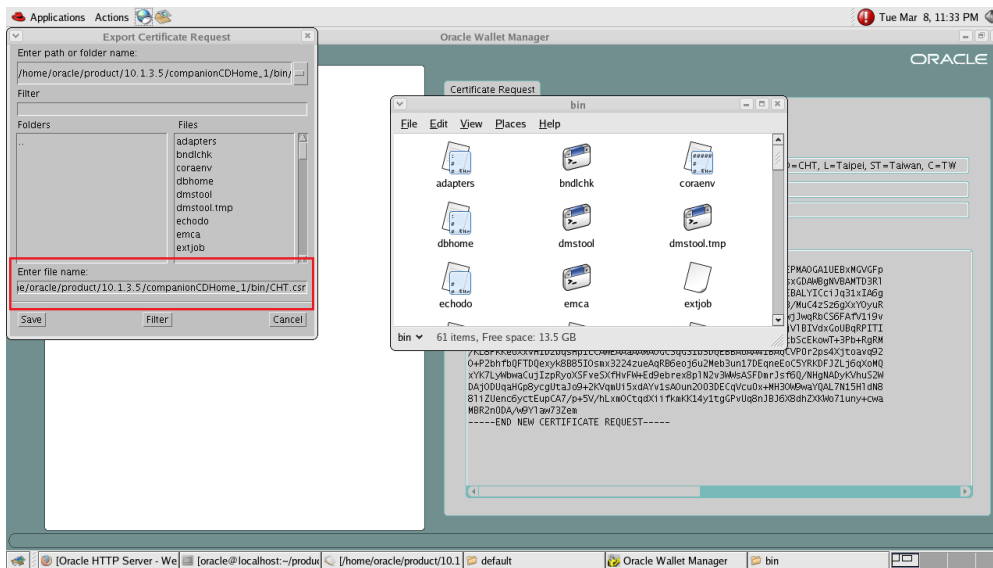
6. 您可以點一下左邊的樹狀圖中 Certificate:[Requested] 確認一下剛才輸入的資料是否有誤：



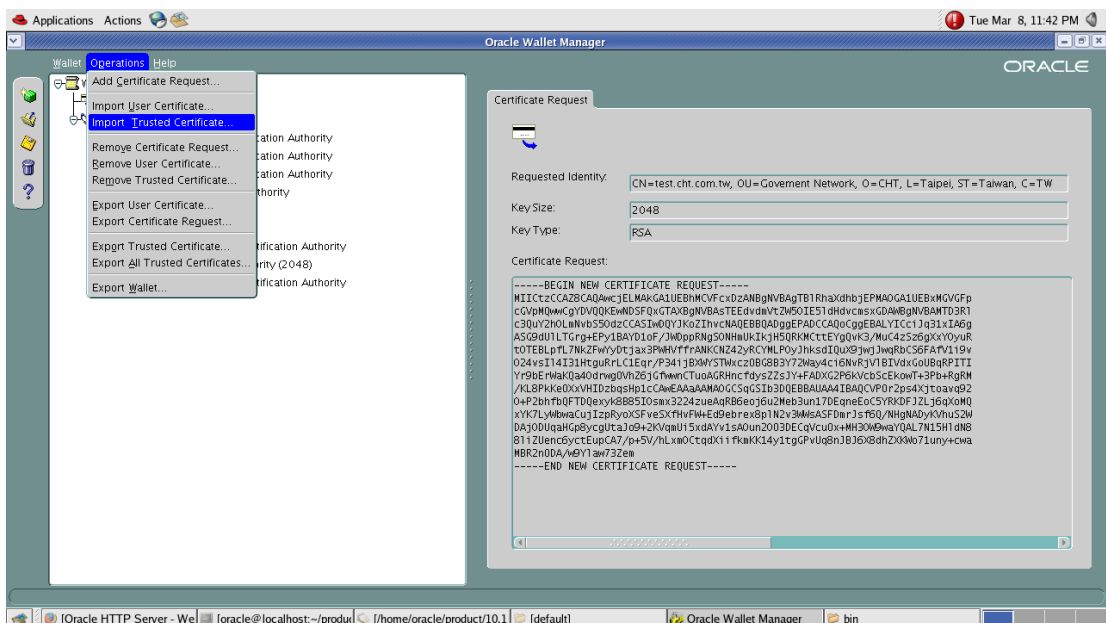
7. 點選上方 Operations > Export Certificate Request，將憑證請求檔匯出。



8. 選擇憑證請求檔之儲存路徑，在 Enter file name 的欄位打上匯出檔名 <filename>.csr



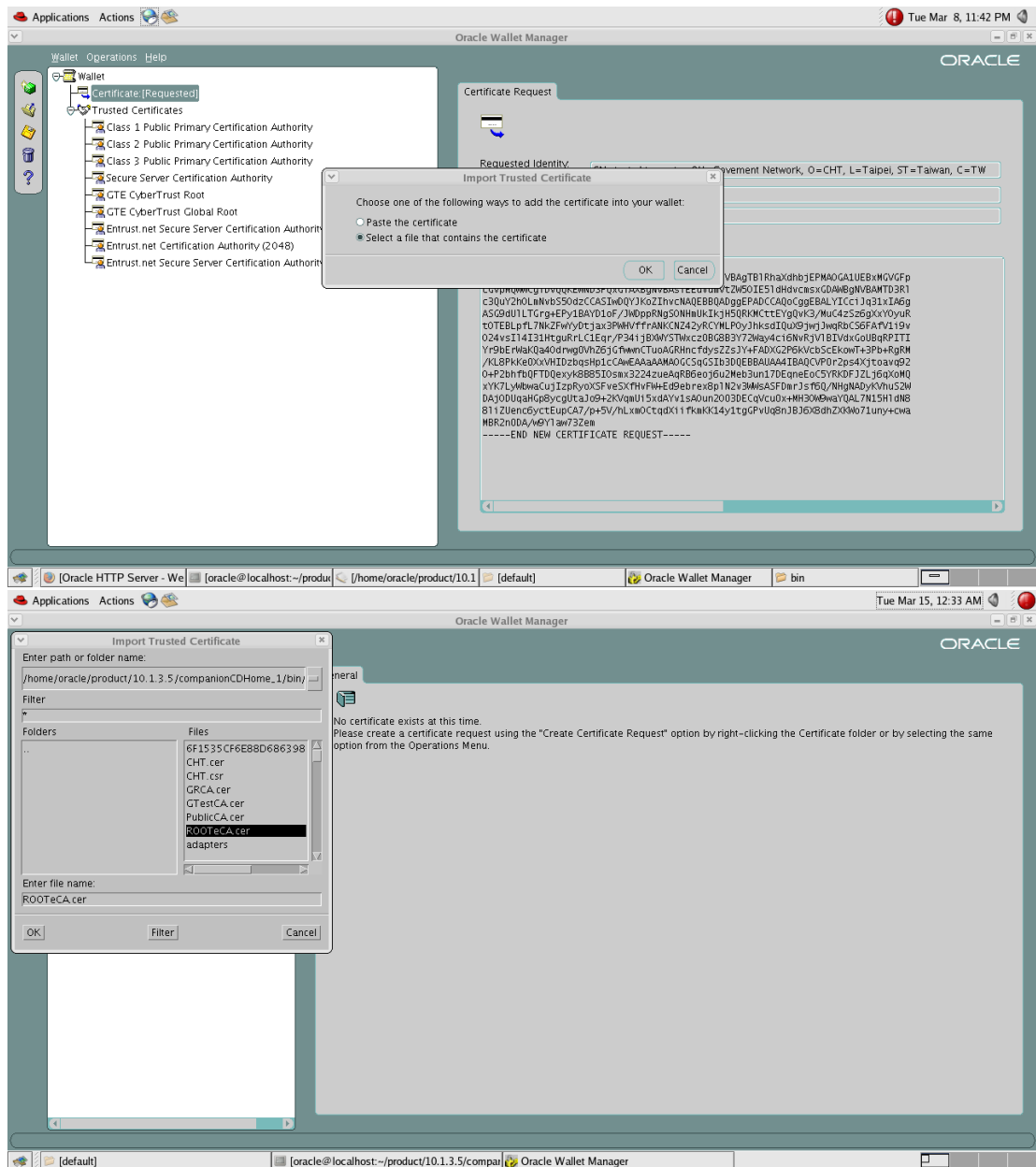
9. 請將申請到的 SSL 伺服器憑證、根憑證 (Root CA Certificate)、中繼憑證 (Intermedi CA Certificate) 存到任一目錄，進行憑證匯入動作。首先進行根憑證、中繼憑證的匯入，點選上方的 Operations > Import Trusted Certificate



10. 選擇要匯入的根憑證，本操作範例之根憑證為 ePKI Root CA 憑

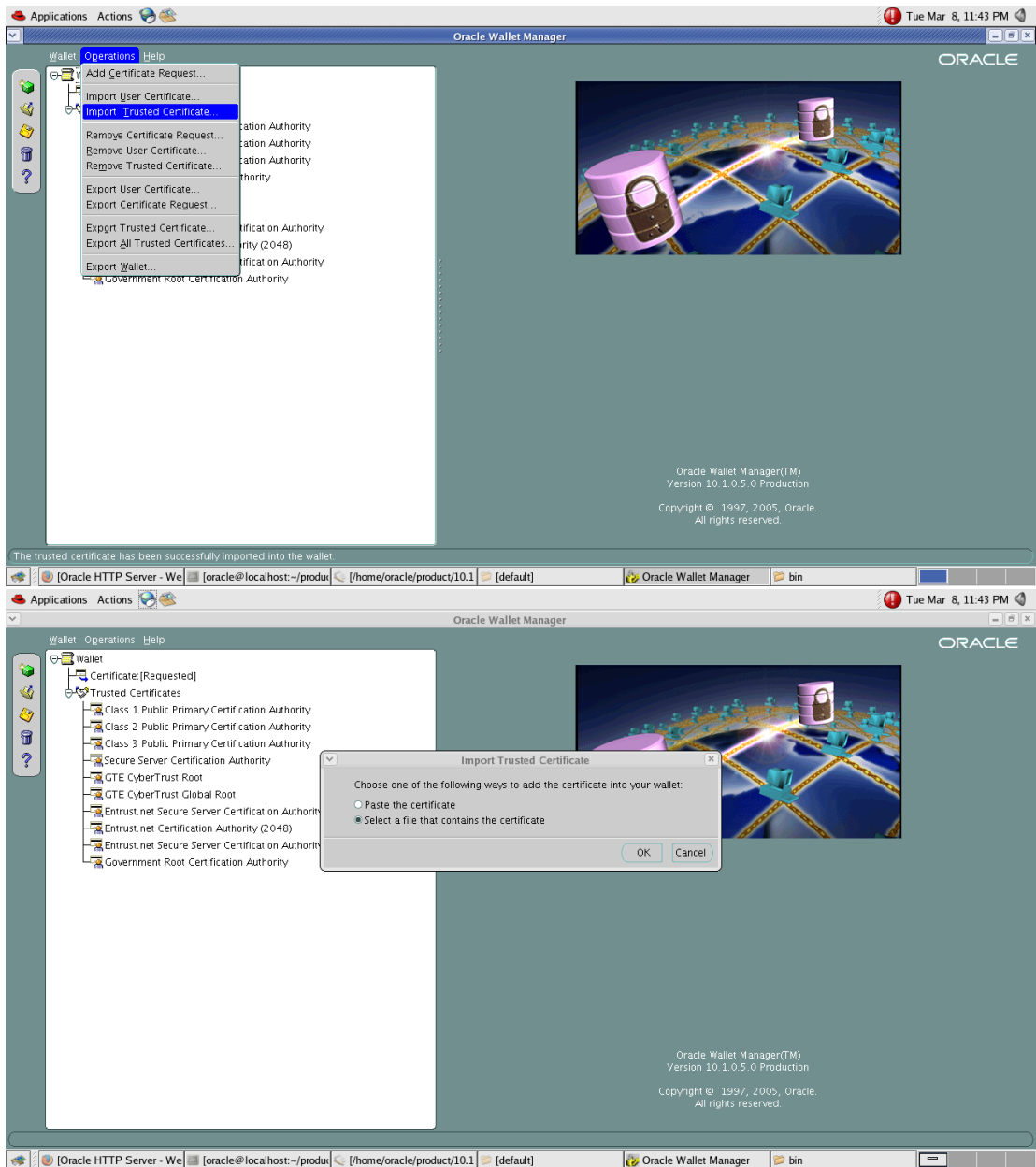
證(eCA 自簽憑證)： ePKIb64.cer(隨核發憑證之電子郵件一同附在 ZIP 檔內)，或直接由 PublicCA 網站之儲存庫下載為 ROOT...

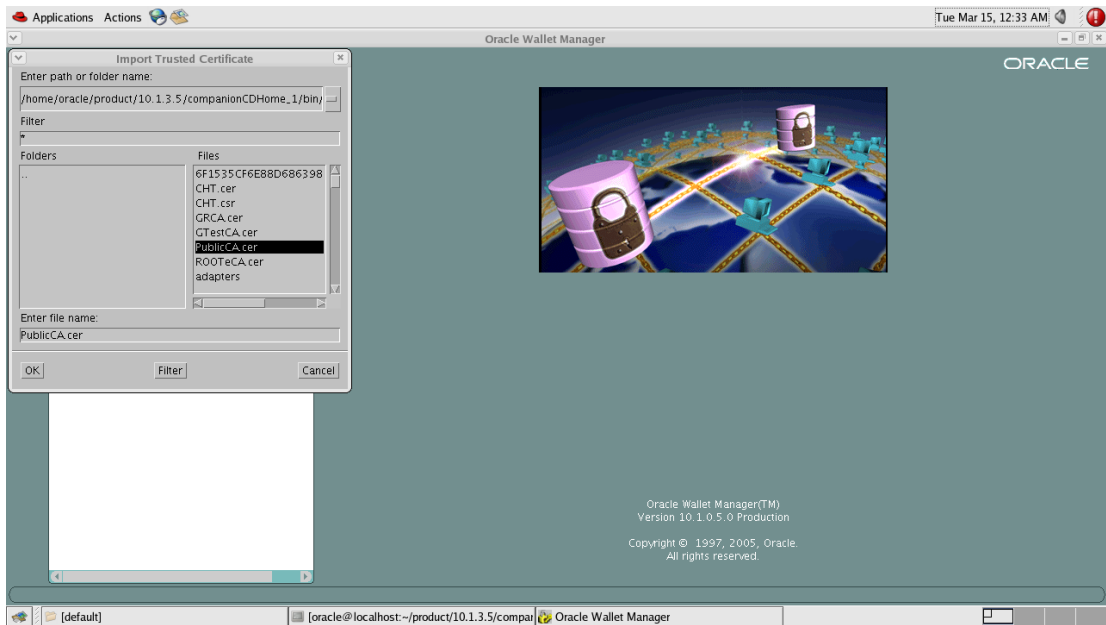
eCA.cer



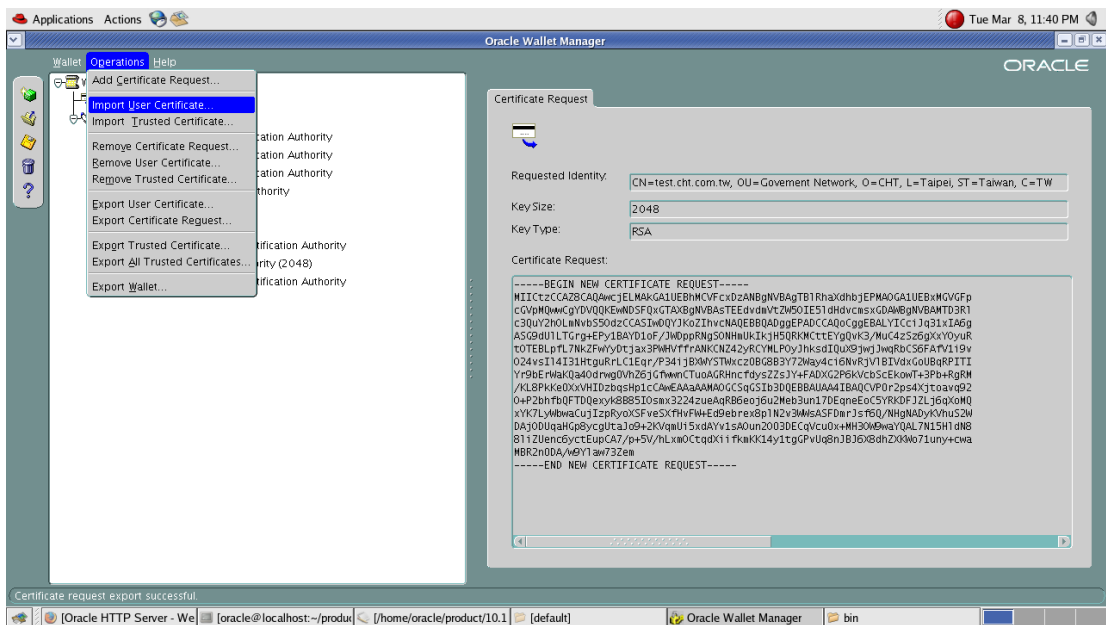
11. 再次重複上述動作匯入中繼憑證，本操作範例之中繼憑證為中華電信通用憑證管理中心的 CA 憑證，檔名為 pubcab64.cer(隨核發憑證一同附在 ZIP 檔內)。或直接由 PublicCA 網站之儲存庫下載

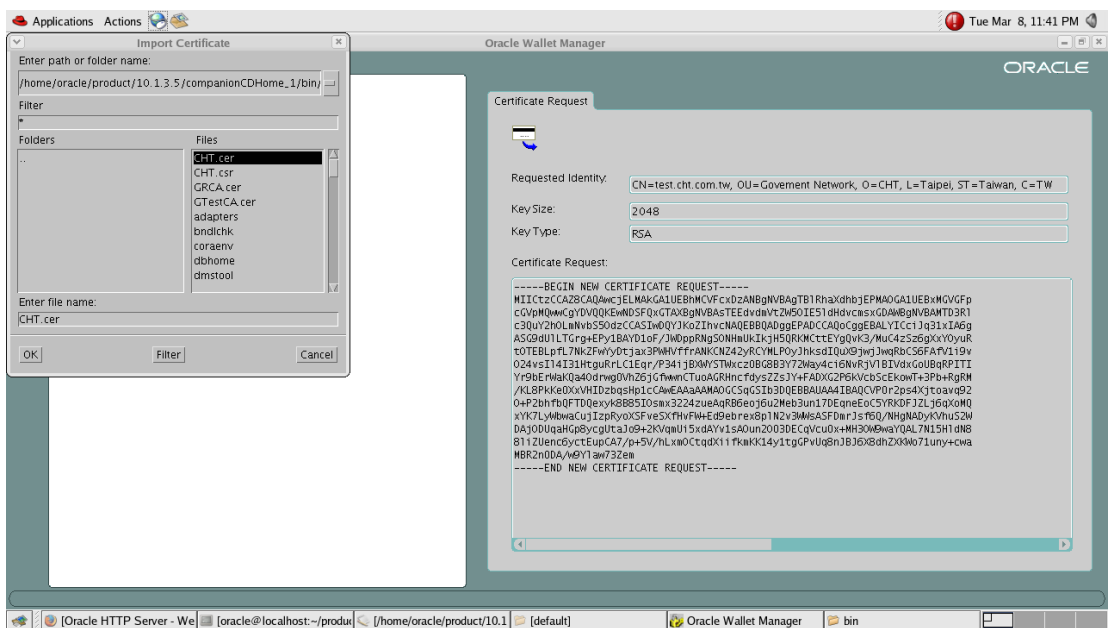
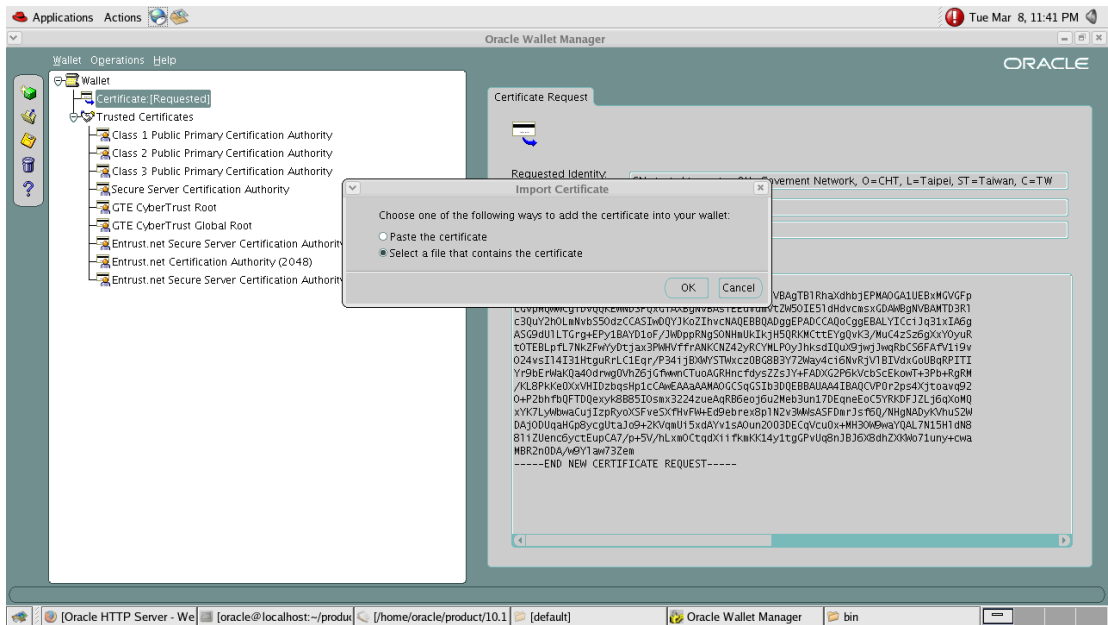
為 PublicCA. cer。





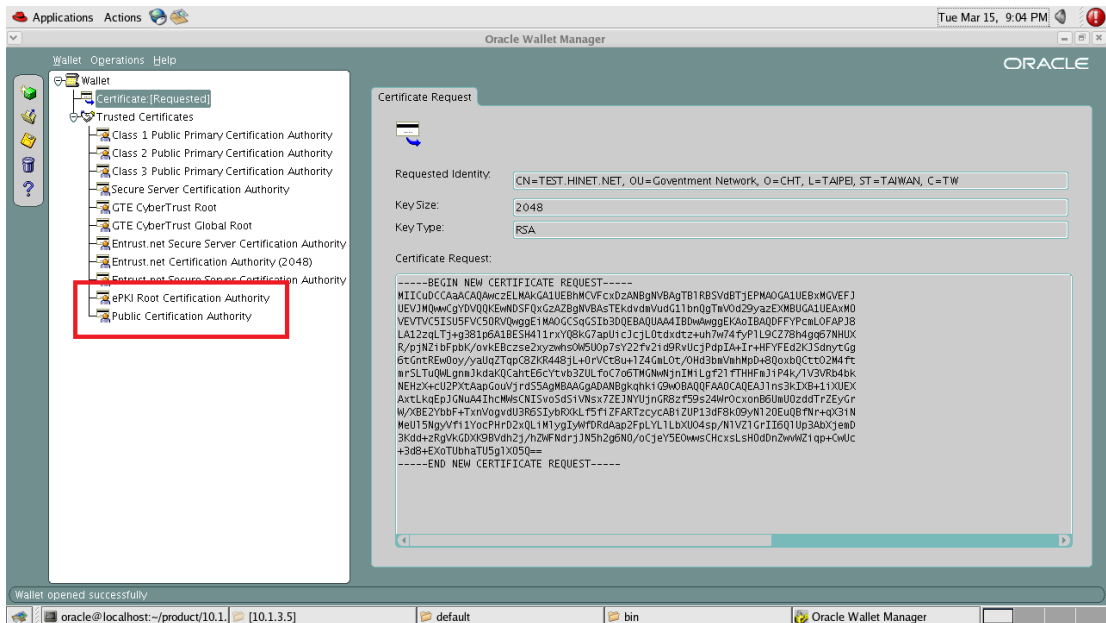
12. 當根憑證與中繼憑證都匯入後，請點選 Operations > Import User Certificate 進行 SSL 憑證的匯入，本操作範例的憑證檔名為 CHT.cer



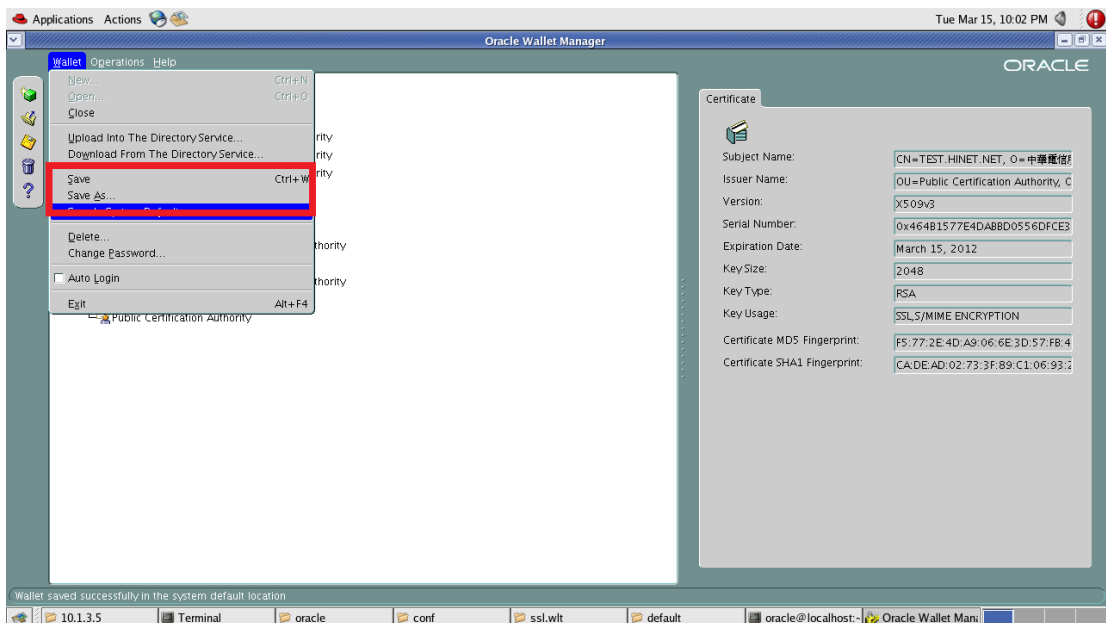


13. 完成後可以看到憑證狀態為 Ready，信任憑證區也多了一個剛剛匯入的根憑證(如下圖顯示為「ePKI Root Certification Authority」)與中繼憑證(如下圖顯示為「Public Certification

## Authority」)

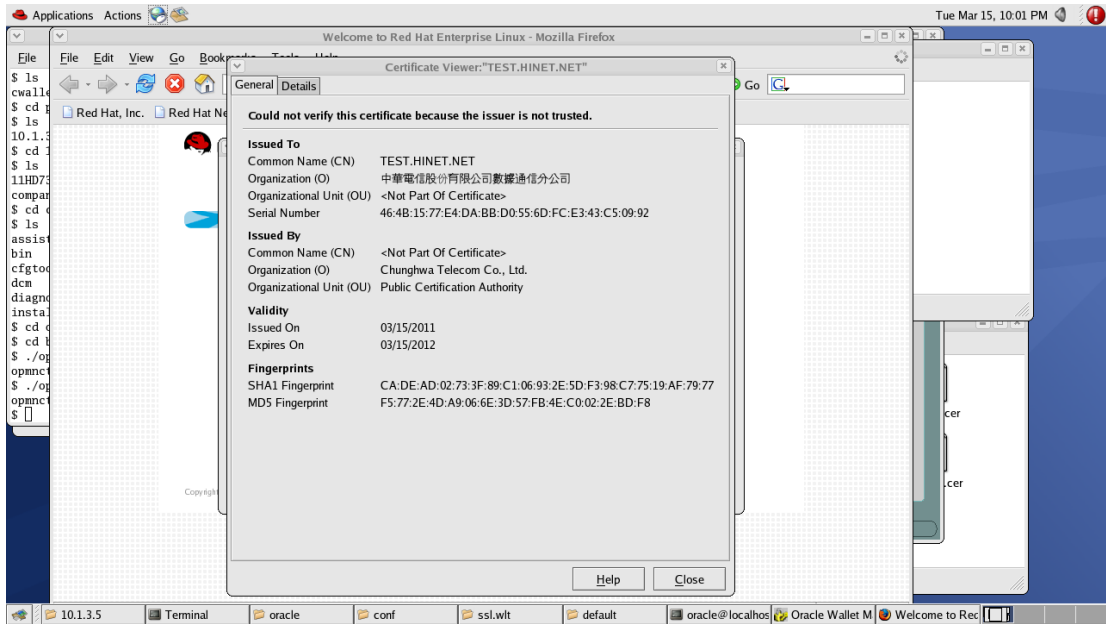


14. 請點選 Wallet > Save，將整個憑證與私密金鑰打包成 PKCS #12 格式的檔案，存到您所設定原本擺放 wallet.p12 的目錄覆蓋之。



15. 將 HTTP Service 重新啟動後，開啟網頁測試。可以看到類似下

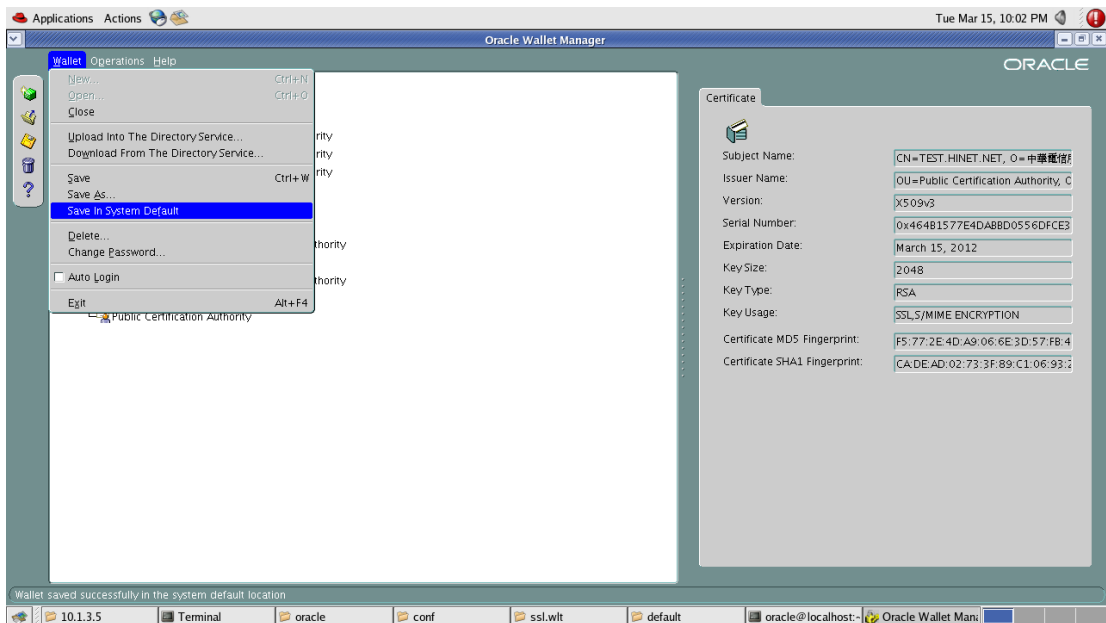
圖的憑證相關資訊，代表 SSL 安全連線 https 成功啟用。



16. 若您查驗發覺依舊為舊有憑證，請再次透過 Oracle Wallet

Manager 開啟剛剛存放 Wallet 的路徑叫出剛剛的憑證包，點選

Wallet > Save in System Default



17. 您會發現有個 `cwallet.sso` 的檔案存放在 Oracle Wallet Manager

的預設路徑(以本範例來說存放於

`/etc/ORACLE/WALLETS/oracle`，將該目錄下的 `cwallet.sso` 與

`ewallet.p12` 複製後存放於您系統設定的 SSL 路徑(以本範例來說

存放於

`/home/oracle/product/10.1.3.5/companionCDHome_1/ohs/conf`

`/ssl.wlt/default`

本範例的 SSL 設定檔位置於

`/home/oracle/product/10.1.3.5/companionCDHome_1/ohs/conf`

`/ssl.conf`