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 | | | | | | | | | | | |
|--|--|--|--|---|---|--|--|--|--|--|--|
| assistants bin cfgtoollogs dcm diagnostics install localhost.loc | install.platform inventory jdbc jdk jlib jre caldomain> cd bin | ldap lib network nls ohs OPatch | opmn oracore oraInst.loc oui owm perl | plsql precomp rdbms relnotes root.sh root.sh.old | slax sqlplus srvm sysman uix xdk | | | | | | |
| | caldomain> ./owm | | localhost.localdomain> ./owm]] | | | | | | | | |



2. 您可以從左邊的 ICON 選擇新增 Wallet 或開啟舊有的 Wallet,

| 📥 Appl | lications Actions 📎 🥸 | | 🜗 Tue Mar 8, 11:23 PM 🔇 |
|--------|------------------------------|--|-------------------------|
| * | | Oracle Wallet Manager | = 8 × |
| | <u>Walet</u> Berge walet | Cracle Wallet Manager New Wallet Aparsword must: * Contain aphabetic characters * Contain aphabetic characters * Contain aphabetic characters * Contain aphabetic characters * Wallet Password: * Wallet Type: * Standard OK Cancel OK Cancel | ORACLE |
| | | | |
| S 🖉 | Uracle HTTP Server - Welcome | I cracie@iocainost:~/product/10.1 🛬 [/home/oracie/product/10.1.3.5/cc] 📁 default 🛛 👔 Oracle Wallet Manag | jer 🕒 |

本手冊以新增一個 New Wallet 說明。

 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。

| | | | T M 15 12-46 AM A |
|---|---|--|--------------------------|
| Applications Actions | | Oracle Wallet Manager | Tue Mar 15, 12:46 AM 🍯 🥌 |
| Wallat Operations Halp | | Oracle wanet manager | |
| Hane operations Help | Please enter the folio Common Name: Organization: Locality/City: State/Province: Country: DN: | Create Certificate Request owing information to create an identity: TEST.HINET.NET Coventment Network CHT TAIVEAN TAIVAN TAIVAN TAIVAN TAIVAN TAIVAN CN=TEST.HINET.NET, OU=Goventment Network Advanced OK Cancel | |
| | | Oracle Wallet Manager(TM) Version 10.1.0.5.0 Production Copyright © 1997, 2005, Oracle All rights reserved. | |
| < 🖉 🧾 [oracle@localhost:~/product/10.1 🔣 Oracle Wallet Ma | inager 📁 📁 or | racle 📁 companionCDHome_1 😂 bin | |

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。

| 📤 Applications Actions 🏹 🍣 | | 🔴 Tue Mar 8, 11:26 PM 🔇 |
|--|---|-------------------------|
| Y | Oracle Wallet Manager | = 6 × |
| Yallet Operations Help | <complex-block></complex-block> | ORACLE |
| | | |
| | Copyright © 1937, 2005, Oracle. All rights reserved. | |
| 🐟 💈 🕑 [Oracle HTTP Server - Welcome 🔳 [oracle@ | localhost:/product/10.1 🤍 [/home/oracle/product/10.1.3.5/cc 😂 default | acle Wallet Manager |

6. 您可以點一下左邊的樹狀圖中 Certficate: [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。

| 🐣 Ap | plications Actions 🥪 জ | | 🕡 Tue Mar 8, |
|----------|---|---|--|
| <u> </u> | | | Oracle Wallet Manager |
| | Wallet Operations Help | | 0 |
| | ⊖ 🔄 Add ⊆ertificate Request | | |
| | Handreit Ber Certificate ⊖C Import Trusted Certificate | | . exclusion of the sec |
| | Remove Certificate Request Remove User Certificate Remove Trusted Certificate | fation Authority ation Authority ation Authority thority | |
| | Export User Certificate Export Certificate Reguest | | |
| | Export Trusted Certificate Export <u>A</u> II Trusted Certificates | tification Authority rity (2048) | |
| | Export Wallet | tification Authority | |
| | | | |
| | | | Oracle Wallet Manager(TM) Version 10.1.0.5.0 Production |
| | | | Copyright © 1997, 2005, Oracle. All rights reserved. |
| (| | | |

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

| Application | | | a 1 m | | | | Tue mai 0, 11.551 m v |
|---------------------------------|--|-----------------------|-------------|--|--|-------------------------|---|
| Y. | Export Certificate Request | | Oracle Wa | allet Manager | | _ | = 0 |
| Enter path o | riolder name. | _ | | | | | ORACLE |
| /nome/oraci | e/product/10.1.3.5/companionCDHome_1/bin/ | | Contifica | to Request | | | |
| Filter | | | Certifica | hin | | - 0 × | |
| Folders | Files | File | Edit View | Places Help | | | |
| - Older 5 | adapters | 23/4 | Tour Tren | Duces Web | ~ | * | |
| | bndichk | | | Q | 00000 | 1 | |
| | coraenv | | La que | | La she | × . | =CHT, L=Taipei, ST=Taiwan, C=TW |
| | dbhome | | adapters | bndichk | coraenv | | |
| | dmstool.tmp | | | | - P | | |
| | echodo | | []: /] | 2- | >- | | |
| | emca | | dhhome | dmstool | dmstool.tmp | | |
| | extjob | | ~ | | ~ | | |
| Enter file nar | me: | | | 0.0 | | | PMADGA1UEBxNGVGFp |
| e/oracle/pro | oduct/10.1.3.5/companionCDHome_1/bin/CHT.csr | | La que | 2- | \Box | | BALYICciJq31xIA6q |
| | | | echodo | emca | extjob | | 8/MuC4zSz6gXxY0yuR |
| Save | Filter Cancel | | \sim | ~ | ~ | * | VIBIVdxGoUBaRPITI |
| |) | bin 🛩 | 61 items, F | ree space: 13.5 GB | | | bScEkowT+3Pb+RgRM |
| | | | 0+P | SPECED STREET STRE | иениканиями осторотного цере у 3224 г. небо RB6 е о 16 и 2Мер 3 и | nt 7DE aneE | CVP0r2ps4Xjtoavq92 oC5YBKDE17L16qXoM0 |
| | | | хYK | 7LyWbwaCujIzpRyoXSFveS | XfHvFW+Ed9ebrex8p1N2v3W | /sASFDmrJs | f6Q/NHgNADyKVhuS2W |
| | | | DAjo 811 |)DUqaHGp8ycgUtaJo9+2KV ZUenc6yctEunC87/n+5V/h | qmUi5xdAYv1sAOun2OO3DECo LymOCtadXiifkmKK14y1taGE | Vcu0x+NH3 Vllo8n1B16 | OW9waYQAL7N15H1dN8 X8db7XKkko71upyacwa |
| | | | MBR | 2n0DA/w9Y1aw73Zem | Exilocoqueri i Rillocomy Logor | 0000000000 | ADUITE ANNOT EURY FEWE |
| | | | | END NEW CERTIFICATE | REQUEST | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | Đ |
| | | | | | | _ | |
| | | | | | | | |
| 121 | | | | | | | |
| 🤹 🖉 🥑 [Ora | acle HTTP Server - We 💷 [oracle@localhost:~/produc | 🔍 [/home/oracle/produ | ct/10.1 📁 d | efault | 没 Oracle Wallet Manager | 📁 bin | |

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。



| Applications | Actions 🌏 🥸 | | Tue Mar 15, 12:33 AM 🔇 [|
|----------------------------------|---|--|--------------------------|
| v | | Oracle Wallet Manager | = = × |
| | Import Trusted Certificate | | |
| Enter path or fo | Ider name: | | |
| /home/oracle/p | product/10.1.3.5/companionCDHome_1/bin/ | | |
| Filter | · | | |
| * | | | |
| Folders | Files | | |
| Enter file name: PublicCA.cer | GF1532CFEB8D686398 | | |
| OK | Filter Cancel | Oracle Wallet Manager(TM) Version 10.1.0.5,0 Production Copyright © 1997, 2005, Oracle. All rights reserved | |
| 🐟 🖇 📁 [default |] [oracle@local | lhost:~/product/10.1.3.5/compar 👸 Oracle Wallet Manager | |

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

| | | Oracle Wallet Manager | |
|--|--|--|--|
| Walkt Operations Help Walkt Operations Help Walkt Import User Certificate. Request Import Turate Certificate Remove Certificate Request Remove Certificate Request Remove User Certificate Report User Certificate Export User Certificate Export User Certificate Request Export Certificate Request Export Certificate Request Export Certificate Request Export Certificate Request Export Certificate Request Export All Trusted Certificate Export Wallet | cation Authority cation Authority cation Authority thority Uffication Authority rity (2048) tification Authority | Oracle Wallet Manager Certificate Request Requested Identity Reguested Identity Key Size: Key Type: Certificate Request Certificate Request: Certificate Request: Certificate Request: Certificate Request: CopMRWwG7VD0QEE C3Uv2A0LIMV5500 C420htTUT7NRZFW1 V79BFW4020AVHIDzb A0420htTUF17NRZFW1 V79BFW4020AVHIDzb A0420htTUF17NRZFW1 C012EBPAC | CN=test.cht.com.tw, OU=Governent Network, O=CHT, L=Taipei, ST=Taiwan, C=TW 2048 RSA NTLFICATE REQUEST RELMAKGALUEBINKUVCF objESDIAS BIT RhaXohb JEPMAOGALUEBINKUVCFp NOSPQCTARS@NJWASTEEdvaWs/SDIESDI Hdv:ns:xGDAMBgWD8AHTD3R1 CCASIMOVI/No2Thv:cHAQEBBAADgEPADCCAQoCgGEBALYICC11331XTA6g BATOLoF, JNoBRASTBACtadVaStaSDIESDI Hdv:ns:xGDAMBgWD8AHTD3R1 CCASIMOVI/No2Thv:cHAQEBBAADgEPADCCAQoCgGEBALYICC11331XTA6g BATOLoF, JNoBRASTBACtadVaStaSDIESDI Hdv:ns:xGDAMBgWD8AHTD3R1 CCASIMOVI/No2Thv:cHAQEBBAADgEPADCCAQoCgGEBALYICC11331XTA6g BATOLoF, JNoBRAMCTSQUSSUBSHKHCTSYQUK;VICAS258gXVTSyUR TJ BAISMAN/TSARCMCESGS/BARKCTSYQUK;VICAS258gXVTSyUR BBS1DGaNAZAAAMAADGC3SGCI BABDRKCTCTSYQUK;VICAS2BXVICAS248gXVD3AHVITSANGC3SGCI BABDRAHTI JNh26JGFMAGT IUBAGBAADAI BADCI VIEDrandbECSYRGAD J2LJGAXONQ DId=AXQHUISXAAVI14SQUAZOBVCKSGEKAAVI1490LJGAAVI1434U120GVVUGADBD/SBdMZXABAZ/JXABAATDIASJA DId=AXQHUISXAAVI14SQUAZOBVCKABABDA/JXABAATDIASJA DId=AXQHUISXAAVI14SQUAZOBVCKABADAATJASAMAATJAALJA12XQBAV/XXBAATJAIABAANAAZADAJAXAAJAADAAAJAAJAAJAADAAATJAAAJAAATJAADAAAATJAAJATIASH IATICAATE REQUEST |
| rtificate request export successful. | | | 22222222 |



| 👄 Applications Actions 😪 🕸 | | 🕕 Tue Mar 8, 11:41 PM 🔇 |
|--|--|---|
| Import Certificate | Oracle Wallet Manager | = 8 × |
| Enter path or folder name: | | |
| /home/oracle/product/10.1.3.5/companionCDHome_1/bin/ | | |
| Filter | Certificate Request | |
| • | _ | |
| Folders Files | | |
| Eff.cor CHT.cor CHT.cor CHT.cor CRCA.cer GRCA.cer adapters bndithk coraenv dbhome dmstool T CHT.cer Cancel | Requested identity. Key Size: Key Type: Certificate Request: COVPINWAGY0000EX: c304720.14750500 c304720.14750500 c304720.14750500 c304720.14750500 c304720.14750500 c304720.14750500 c304720.14750500 c304720.14750500 c3047200000000 c40000000000000000000000000000 | CN-test cht.com tw, OU-Governent Network, O-CHT, L=Taipel, ST=Taiwan, C=TW 2048 BSA NTFICATE REQUEST If HARGAQUEENHCVF cub2AMBglivBAgTB1RhaXchbjEPMADCAQUEBNKOVOFP MOSFQuCTAXBgIVBASTEEdvalutZW901E510HdvcmszC0AMBgNVBAHTD3R1 CCGSSTMQ071ACB/TUCAKQEBBNQDBEFABCCAQGOGEBAUTICs1 aja1.Ta6g 3AMD10F_1Nd0pAMgSOHHULSI;NISQNNCTEVEYgIVK3/MUL4S2580;ArtO109 Ita1200 AMD10F_1Nd0pAMgSOHHULSI;NISQNNCTEVEYgIVK3/MUL4S2580;ArtO119 Ita1200 AMD10F_1Nd0pAMgSOHHULSI;NISQNNCTEVEYgIVK3/MUL4S2580;ArtO129 Ita1200 AMD10F_1Nd0pAMgSOHHULSI;NISQNNCTEVEYgIVK3/MUL4S24 Ita1200 AMD10F_1Nd0pAMgSOHHULSI;NISQNNCTEVEXgIVK3/MUL4S24 Ita1200 AMD10F_1Nd0pAMgSOHHULSI;NISQNNCTEVEXgIVK3/MUL4S24 Ita1200 AMD10F_1Nd0pAMgSOHHULSI;NISQNNCTEVEXgIVK3/MUL4S24 Ita1200 AMD10F_1Nd0pAMgSOHHULSI;NISQNNCTEVEXgIVK3/MUL4S24 Ita1200 AMD10F_1Nd0pAMgSOHHULSI;NISQNNCTEVEXgIVK3/MUL4S24 Ita |
| | |) |
| < 🖉 🕘 [Oracle HTTP Server - We 🧾 [oracle@localhost:~/produ | 🤇 [/home/oracle/product/10.1 📁 [default] | 🤣 Oracle Wallet Manager 🛛 🞾 bin 📃 📃 📃 |

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

Tue Mar 15, 10:02 PM 🔌 🥼 📤 Applications 🛛 Actions 🥪 🥌 Oracle Wallet Manager operations He 6 Certificate Close 4 1 Upload Into The Directory Service.. Download From The Directory Serv CN=TEST.HINET.NET, O=中華電信机 Subject Name 1 Ctrl+ Şave Save <u>A</u>s Issuer Name: OU=Public Certification Authority, C ? Version: X509\/3 Serial Number: 0x464B1577E4DABBD0556DECE3 Expiration Date: March 15, 2012 Change Password Key Size: 2048 Auto Login Кеу Туре RSA E≚it Alt+F4 Public (entrication Authorit Key Usage: SSL S/MIME ENCRYPTION Certificate MD5 Fingerprint: F5:77:2E:4D:A9:06:6E:3D:57:FB:4 Certificate SHA1 Fingerprint: CA:DE:AD:02:73:3F:89:C1:06:93:2 📕 oracle@localhost:^ 没 Oracle Wallet Mani 🐲 📁 10.1.3.5 🔳 Terminal 📁 oracle 📁 conf 📁 ssl.wlt 📁 default

格式的檔案,存到您所設定原本擺放 wallet.pl2 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

| 📥 A | pplications Actions 🎈 | | | | | | | Tue Mar 15, 10:02 PM 🔇 🛛 🕕 |
|---------------------------------------|--|---|---|--------|-------------------|-----------|--|--|
| > // | | | | Orac | le Wallet Manager | | | -B× |
| | Wallet Operations E | elp | Crd+N | | | | | ORACLE |
| 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | Wallet Operations New Open Close Upload Into The D Download From Th Save As Save As Save In System De Delete Change Bassword. Auto Login Egit Egit Public Celt | elp rectory Service e Directory Service ault | Ctrl+N ctrl+O rity rity rity rity thority Alt+F4 | | | Ce | entificate Subject Name: Issuer Name: Version: Expiration Date: Expiration Date: Key Size: Key Type: Key Usage: Certificate MD5 Fingerprint: Certificate SHA1 Fingerprint: | CN=TEST.HINET.NET, 0= 中華賦信 OU=Public Certification Authority, C X509v3 0x464B1577E4DA8BD0556DFCE3 March 15, 2012 2048 RSA SSL_5/MIME ENCRYPTION F5:77:2E:4D:A9:06:6E:3D:57:FB:4 CA:DE:AD:02:73:3F:89:C1:06:93:2 |
| (Walle | t saved successfully in th | ne system default locati | ion | 😤 conf | 😤 ccl wit | 😤 default | aracle@localhost. | Oracle Waltet Max |

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/ORACEL/WALLETS/oracle,將該目錄下的 cwallet.sso 與 ewallet.pl2 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