中華電信通用憑證管理中心(PublicCA)

IBM HTTP Server SSL 憑證請求檔製作與 SSL 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. 產生「憑證請求檔」

「開始」→「程式集」→「IBM HTTP Server V6.1」→「Start Key Management Utility」



2. 啟動 IBM Key Management(IBM Server 的金鑰管理程式)

2-1 建立新的金鑰資料庫 :「金鑰檔案資料庫」→「新建」

🧱 IBM Key Manageme	nt	
金鑰資料庫檔案(F) 建	立(C) 檢視(V) 説明(H)	
■ 新建(N)		
<u>開啓(0)</u>	A AA 25 (10) (10) (10) (10) (10) (10) (10) (10)	
	金獼貨科哩貨訊	
開閉(L)		
另存新檔(S)		
 變更密碼(<u>P</u>)		
貯藏密碼(<u>T</u>)	金編資料庫內容	
結東(<u>X</u>)	▼	接收
		刪除
		4A_27.06±*
		238(1)72.7余雨年町
		匯入
		重建要求
		新建自我簽章的
		取出愿證
如果安督動 ' 請選取	金翔資料理幅茶」功能表來使用金翔資料理	

- 2-2 選擇資料庫型態:『CMS』
- 檔案名稱:key.kdb (預設値) 位置:C:\Program Files\IBM\HTTPServer

IBM Key Management	
論資料庫檔案(F) 建立(C) 檢視(V) 説明(H)	
金論資料庫資訊	
省料庫類型:	
當案名稱:	
2號標籤:	
金論資料庫內容	
個人憑證	▼ 接收
新建	同除
金論資料庫類型 CMS ▼	1後词《编辑
檔案名稱: key.kdb 說覽	匯入
位置: C1Program Files\UBM\HTTPServert	重建要求
確定 取消	
可以依實際存放路極進行修改	新建自我簽章的
	取出憑證

2-3 設定金鑰資料庫密碼

說明: 密碼至少取用 6 個字元,並避免使用一般可以取得的資訊所組成。例如: 生日、 姓名或身分證字號等……

密碼提示				
密碼 :	*****			
確認密碼 =	60 夭皴			
密碼強度:				
確定	重設 取消			

3. 建立新憑證

BM Key Management - [C:Wrogram Files/IBM/HTTPServer/key.kdb]	
金鑰資料庫檔案(P) 建立(C) 檢視(V) 說明(H)	
資料 庫 類 型: CMS 金 論 資料 庫 檔案	
檔案名稱: C:\Program Files\IBM\HTTPServer\key.kdb	
記號標籤:	
金鑰資料庫內容	
簽章者憑證	▼ 新增
Entrust.net Global Secure Server Certification Authority	millitz
Entrust.net Global Client Certification Authority	
Entrust.net Global Client Certification Authority Entrust.net Client Certification Authority	放闹,病毒報
Entrust.net Global Client Certification Authority Entrust.net Client Certification Authority Entrust.net Certification Authority (2048)	
Entrust.net Global Client Certification Authority Entrust.net Client Certification Authority Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority	·····································
Entrust.net Global Client Certification Authority Entrust.net Client Certification Authority Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority VeriSign Class 3 Secure Server CA	
Entrust.net Global Client Certification Authority Entrust.net Client Certification Authority Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority VeriSign Class 3 Secure Server CA VeriSign Class 3 Dublic Primary Certification Authority	
Entrust.net Global Client Certification Authority Entrust.net Client Certification Authority Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority VeriSign Class 3 Secure Server CA VeriSign Class 3 Public Primary Certification Authority VeriSign Class 2 Public Primary Certification Authority VeriSign Class 2 Public Primary Certification Authority	
Entrust.net Global Client Certification Authority Entrust.net Client Certification Authority Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority VeriSign Class 3 Secure Server CA VeriSign Class 3 Public Primary Certification Authority VeriSign Class 4 Public Primary Certification Authority VeriSign Class 1 Public Primary Certification Authority VeriSign Class 1 Public Primary Certification Authority VeriSign Class 4 Public Primary Certification Authority	
Entrust.net Global Client Certification Authority Entrust.net Client Certification Authority Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority VerSign Class 3 Secure Server CA VerSign Class 3 Public Primary Certification Authority VerSign Class 4 Public Primary Certification Authority VerSign Class 4 Public Primary Certification Authority VerSign Class 3 Public Primary Certification Authority VerSign Class 4 Public Primary Certification Authority - G2	
Entrust.net Global Client Certification Authority Entrust.net Client Certification Authority Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority VeriSign Class 3 Secure Server CA VeriSign Class 3 Public Primary Certification Authority VeriSign Class 2 Public Primary Certification Authority VeriSign Class 4 Public Primary Certification Authority VeriSign Class 4 Public Primary Certification Authority VeriSign Class 3 Public Primary Certification Authority - G2 VeriSign Class 3 Public Primary Certification Authority - G2	

- 3-1 輸入憑證相關資訊,輸入完後按→「確定」
- 各欄位說明如下:(建議以下欄位必須使用英文填寫)
- (1)金鑰標籤:可以自行訂定。
- (2)金鑰大小:此處以選擇 『1024』為例。
- (3) 共用名稱:網站名稱 (使用 Domain Name,非 URL)
- (4) 組織:使用憑證之組織 (例如:CHT)
- (5) 部門:使用憑證組織之單位(例如: ValueAdd (加値處))
- (6) 地區: 城市名稱 (例如: Taipei)
- (7) 州/省: 國家全名 (例如: Taiwan)
- (8)請輸入要用來儲存憑證要求的檔案名稱:(例如:C:\Program

Files\IBM\HTTPServer\certreq.arm),此「憑證要求」亦即一般所稱的憑證請求檔(CSR)

			_
金镧大小		1024 💌	
共用名稱		www.test.com.tw]
且織		СНТ]
889	(選用)	ValueAdd]
也區	(選用)	Taipei	
附/省	(選用)	Taiwan	
即远區號	(選用)	100	
國家或地區		TW 💌	
·	灰儲存調	资要求的档案名称:	
	FilecUDM	NHTTPServeringstream	5

3-2 憑證請求檔製作完成,請至中華電信通用憑證管理中心申請憑證。

anagement - [C:\Program Files\IBM\IITPServer\key.kdb] 27.13. 2017;10. 2018;10.0. 2019;10.0.	
金論資料庫資訊 CMS 金编資料庫檔案 C1Program Files\IBM\HTTPServer\key.kdb	
金鑰資料庫內容	
多者育訊 こ こ 日在下列檔案中順利建立新愚證: C.\Program Files\UBM\HTTPServen\certreq.arm + 您必須將檔案傳送給憑證中心,以要求憑證 +	
	K(f) 建立(C) 松桃(M) 副明(H) ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●

4. 新增簽章憑證

4-1 連線至 <u>http://publicca.hinet.net/SSL-07.htm</u> 下載Root CA憑證與中繼憑證(Based 64 編碼)

中華電信通用憲證管理中心 - Windows Internet Explorer	
🕘 🕞 👻 http://publicca.hinet.net/SSL-07.htm	🔽 🗲 🗙 Live Search
當案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(I) 説明(H)	
🕐 🔗 中華電信通用憑證管理中心	
中華電信通用憑證管理 PKI資訊安全產品 снт SSI&邀	里中心 PKI SERVICE 服務 HiPKO網路認證套件包 HiKey随身資安服務 硬體保密器 安全疇纲 儲存庫 問與答 English 首頁
SSL憑證服務	SSL 憑證服務 SSL service 下意識感圖
 SSL服務説明 SSL憑證購買流程 	儲存庫 SSL手冊下载
 SSL 憑證定價 	🧧 中華電信通用憑證管理中心 - 憑證實務作業基準(CPS) 💁
■ SSL 憑證廢止	L ePKI Root CA憑證(eCA自簽憑證)下載 A C (DER編碼)
■ SSL憑證查詢及下載	ePKI Root CA憑證(eCA自簽憑證)下載 [1] (Based 64編碼)
■ 下載專區	□ 補用憑證管理中心中繼憑證(Public CA)下載(DER編碼)
■ 問與答	□ 通用憑證管理中心中繼憑證(Public CA)下載 [] [[Based 64編碼)
1	

4-2 點選「簽章者憑證」

📴 IBM Key Management - [C:\Program Files\IBM\HTTPServer\key.kdb]			
金鑰資料庫檔案(F) 建立(C) 檢視(V) 說明(H)			
金論資料庫資訊 資料庫類型: CMS 金論資料庫檔案			
檔案名稱: C:\Program Files\IBM\HTTPServer\key.kdb			
記號煙籤:			
金鑰資料庫內容			
個人憑證要求 個人憑證要求 個人憑證要求	新建 剛除 檢視 取出		
使用憑證要求向憑證中心 (CA) 要求憑證。			

4-3 安裝 ePKI Root CA 憑證檔案→「新增」

資料型態:Base64 編碼 ASCII 資料

憑證檔案名稱:ROOTeCA_64.cer

位置: D:\TEST_Demo\ → 請依實際存放路徑存檔

BM Key Management - [C. \Program Files\IBM\HTTPServer\key.kdb]			
金鑰資料庫檔案(F) 建立(C) 檢視(V) 説明(H)			
金輪資料庫資訊			
資料庫類型: CMS 金鑰資料庫檔案			
檔案名稱: C12Program FilesVBMHTTPServerikey.kdb			
計號標錄:			
に個糸初后しる意識			
簽章者憑證 資料類型 Base64 編碼 ASCII 資料 ▼		新增	
Entrust.net Global S 憑證檔案名稱: ROOTeCA_64.cer	瀏覽	刪除	
Entrust.net Global C			
Entrust.net Client Ce 位置:D:\TEST_Demo\		檢視/編輯	
Entrust.net Certifica			
Entrust.net Secure State Ray A		取出	
VeriSign Class 3 Dublic Drimary Contification Authority			
VeriSign Class 3 Public Primary Certification Authority			
Verising Class 2 rubits Primary CertarGoton Autority Verising Class 1 Public Primary CertarGoton Autority			
VeriSign Class 4 Public Primary Certification Authority - 62			
VeriSign Class 3 Public Primary Certification Authority - G2			
VeriSign Class 2 Public Primary Certification Authority - G2			
VeriSign Class 1 Public Primary Certification Authority - G2			
VeriSign Class 4 Public Primary Certification Authority - G3	-		

4-3-1 輸入 Root CA 憑證說明文字 → ePKI Root Certificate Authority→「確定 」

🛄 IBM Key M	fanagement - [C:\Program Files\IBM\HTTPServer\key.kdb]	_ D X
金鑰資料庫檔	案(F) 建立(C) 檢視(V) 説明(H)	
🗅 🚄		
	金鑰資料庫資訊	
資料庫類型:	▪ CMS 金编資料庫檔案	
檔案名稱:	C/Program Files\IBM\HTTPServer\key.kdb	
=>\$₽\$₩\$₩\$\$\$\$ ·		
aran dear		
	全論咨判備办交	
繁章者憑證 Entrust.net (Entrust.net (Entrust.net (Entrust.net (Entrust.net S VeriSign Cla VeriSign Cla VeriSign Cla VeriSign Cla VeriSign Cla VeriSign Cla	Global Secure Server Certification Authority Global Client Certification Authority Client Certification Authority Certification Authority (2048) Secure Server Certification Authority ass 3 Secure Server CA ass 3 Public Primary Certification Authority ass 4 Public Primary Certification Authority ass 4 Public Primary Certification Authority 62 ass 3 Public Primary Certification Authority 62 ass 1 Public Primary Certification Authority 63	▼ 新增 ● ● ● ● ● ● ● ● ● ●

4-3-2 Root CA 憑證安裝完成→檢視憑證資訊.參考下圖

🧱 IBM Key Management - [C:\Program Files\]		
金鑰資料庫檔案(F) 建立(C) 檢視(V) 説明(F	[ePKI Roof Certification Authority] 的运输首制	
	ePKI Root Certification Authority	
資料庫類型: CMS 金論資料庫檔案 檔案名稱: C:\Program Files\\BM\\HTTPSer 記號標録:	金鑰大小: 4096 振融內容: 版本 X509 V3 原號: 15 C8 BD 65 47 5C AF B8 97 00 5E E4 06 D2 BC 9D 登録出者: ou=ePKI Root Certification Authority o = Chunghwa Telecom Co., Ltd. c = TW 發出者: ou=ePKI Root Certification Authority ou=ePKI Root Certification Authority	· 新婚… ● ────────────────────────────────────
Entrust.net Global Secure Server Certification Entrust.net Global Client Certification Authori Entrust.net Global Client Certification Authori	o =Chunghwa Telecom Co., Ltd. c =TW	按視為輪
Entrust.net Client Certification Authority Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Author VeriSign Class 3 Secure Server CA VeriSign Class 3 Public Primary Certification VeriSign Class 4 Public Primary Certification VeriSign Class 4 Public Primary Certification VeriSign Class 3 Public Primary Certification VeriSign Class 3 Public Primary Certification VeriSign Class 2 Public Primary Certification VeriSign Class 2 Public Primary Certification	有效期限: 2004年12月20日至 2034年12月20日 指紋(SHA1 摘要): 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0 簽章演算法: SHA1withRSA(1.2.840.113549.1.1.5)	取出

4-4 安裝中繼憑證

資料型態: Base64 編碼 ASCII 資料

憑證檔案名稱:PublicCA_64.cer

位置: D:\TEST_Demo\ → 依實際存放路徑

BM Key Management - [C:\Program Files\IBM\HTTPServer\key.kdb]	- C 🛛
金鑰資料庫檔案(f) 建立(C) 檢視(V) 說明(H)	
金鑰資料庫資訊	
資料庫類型: CMS 金鑰資料庫檔案	
檔案名稱: C1Program Files\IBM1HTTPServer\key.kdb	
記號標籤:	
金鑰資料庫內容	\sim
簽章者憑證	▼ 新增)
ePKI Root Certification Authority Entrust.net Global Secure Server Certification Authority Entrus E	▲

4-4-1 輸入中繼憑證說明文字 → Public Certification Authority→「確定 」

📕 IBM Key M	anagement - [C:\Program Files\IBM\HTTPServer\key.kdb]	_ X
金鑰資料庫檔案	案(F) 建立(C) 檢視(V) 說明(H)	
	金鑰資料庫資訊	
資料庫類型:	CMS 金鑰資料庫檔案	
檔案名稱:	C1Program Files\IBM\HTTPServer\key kdb	
記號標籤:		
	全輪容製庫协究	
該章者憑證 ePKI Root Ce Entrust.net C Entrust.net C Entrust.net C Entrust.net S VeriSign Cla: VeriSign Cla: VeriSign Cla: VeriSign Cla: VeriSign Cla: VeriSign Cla: VeriSign Cla: VeriSign Cla:	ertification Authority Silobal Secure Server Certification Authority Silobal Client Certification Authority Certification Authority Certification Authority Secure Server Certification Authority Sa Secure Server CA Sa Sa Secure Server CA Sa Sa Public Primary Certification Authority Sa Sa Sublic Primary Certification Authority Sa Sa Sublic Primary Certification Authority Sa Sa Sublic Primary Certification Authority Sa Sa S	 ▼ 新培 冊順注 檢測法编辑 取出

4-4-2 中繼憑證安裝完成→檢視憑證資訊.參考下圖

🛄 IBM Key Management - [C:\Program Files\		
金鑰資料庫檔案(E) 建立(C) 檢視(V) 説明([Public Certification Authority] [Pist] [Pist]	
	Public Certification Authority	
<mark>資料庫類型:</mark> CMS 金論資料庫檔案 檔案名稱: C:Program Files\IBM\HTTPSe 記號標籤:	金論大小: 2048 振融内容: 版本 X509 V3 序號: 00 C9 53 FE EE B8 95 E9 18 84 AB B2 2A 68 A4 2A7D 發出至: ou=Public Certification Authority o = Chunghwa Telecom Co., Ltd.	
簽章者憑證	c =TVV	▼ 新增
Public Certification Authority ePkil Root Certification Authority Entrust.net Global Secure Server Certificatin Entrust.net Global Client Certification Author Entrust.net Client Certification Authority Entrust.net Certification Authority (2048) Entrust.net Secure Server CA VeriSign Class 3 Public Primary Certification VeriSign Class 3 Public Primary Certification VeriSign Class 4 Public Primary Certification VeriSign Class 4 Public Primary Certification VeriSign Class 3 Public Primary Certification VeriSign Class 3 Public Primary Certification VeriSign Class 4 Public Primary Certification VeriSign Class 3 Public Primary Certification VeriSign Class 3 Public Primary Certification	陸山者:	FPUIR: FUIR: Constraints Fuire: Constraints Fuire: Fuire:

4-5 安裝個人憑證→點選「個人憑證」

🔛 IBM Key Ma	nagement - [C:\Program Files\IBM\IITTPServer\key.kdb]		
金鑰資料庫檔案(F) 建立(C) 檢視(V) 試明(H)			
	金論資料庫資訊		
資料庫類型:	CMS 金鑰資料庫檔案		
檔案名稱:	C:Program Files\IBM\HTTPServer\key.kdb		
言己發虎想要發班 =			
·	金编資料庫內容		
個人憑證		接收	
* TEST Demo		FRUID\$	
		bb c8 /6523	
		238C #15/2 74/00 %03	
		匯入/匯出	
		重建要求	
		新建自我赞章的	
		田々という時言音	
		-by by by by by by	
個人憑證在資料庫有其相關的私密金鑰。			

4-5-1 安裝個人憑證→「接收」
資料型態: Base64 編碼 ASCII 資料
憑證檔案名稱: www.test.com.tw.cer
位置: D:\TEST_Demo\ → 依實際存放路徑

🧱 IBM Key Ma	agement - [C:\Program Files\IBM\HTTPServer\key.kdb]	_ 🗆 🔀
金鑰資料庫檔案	① 建立(C) 核碱(V) 認明(H)	
Thratist Physics Web	金輪資料庫資訊	
資料庫類型:	CMS 金페資料庫商業	
瘤系名傳:	C:\Program Files\UBM\HTTPServer\key.kdb	
記號標籤:		
	從檔案接收應還	
個人憑證	資料類型 Base64 編碼 ASCII 資料 -	接收
	振設檔案名稱: www.test.com.tw.cer 瀏覽	冊耶律
	位置: DITEST_Demot	也没不是/终局李重
	確定 取消	匯入
		重建要求
		新建自我簽章的
		取出)质證

4-5-2 設定為預設金鑰→ 請選「是」

🚺 IBM Key M	anagement - [C:\Program Files\IB	M\HTTPServer\}	key.kdb]			2
金鑰資料庫檔案	案(F) 建立(C) 檢視(V) 説明(H)					
	🖬 😤 🕵 💶					
3次来》后来来香田山。	CMC 个给孩料商货车		金鑰資料庫資訊			
月科理規学・		Al courted by				
馏茶省柟·	C.IProgram Files(IBMIHTTPServe	пкеу.кар				
記號標籤:						
			金鑰資料庫內容			
個人憑證		直認			-	接收
* TEST Dem	0	?	您要將這個金鑰設定爲資料庫的預設金鑰	馬?		刪除
			(是) 否 取消			檢視/編輯
			\bigcirc			匯入/匯出
						重建要求
						新建自我簽章的
						取出憑證

4-5-3 個人憑證安裝完成→「確定」→檢視憑證資訊.參考下圖

IBM Key Management - [C:\Program Files\I)	TFFT Demol 的会論容明	
金鑰資料庫檔案(f)建立(C)檢視(V) 説明(H	TEST Demo	
資料庫類型: CMS 金論資料庫檔案 檔案名稱: C:\Program Files\IBM\HTTPSen 記號標籤: 個人概識	金輪大小: 1024 振融內容: 版本 X509 V3 序號: 64 9B 2F 38 45 56 5C 14 12 0D 71 C3 62 A6 0B 7C 發出至: cn=www.test.com.tw o=中華電信企業客戶分公司 c=TW	▼ 接收
* TEST Demo	發出者: ou=ePKI Root Certification Authority o =Chunghwa Telecom Co., Ltd. c =TW	冊川除 検·視/法集報
	有效期限: 2010年5月20日 至 2010年6月19日 指紋(SHA1 捷要): 96:24:E3:52:31:24:0E:86:E5:85:98:4C:DB:F6:C5:A3:63:AE:CE:60 發章演算法: SHA1withRSA(1.2.840.113549.1.1.5)	<u>匯入匯出</u> 重建要求
	▶ 按訊明明和	新建自我簽章的 取出憑證

5. 安裝完成