

網域所有權驗證手冊-檔案驗證



臺灣網路認證股份有限公司 TAIWAN-CA. Inc. 台北市 100 延平南路 85 號 10 樓 電話:02-2370-8886 傳真:02-2370-0728 www.twca.com.tw

機密等級:一般 版本:5.0 文件編號:MNT-03-157 生效日期:108 年 12 月 02 日

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變 成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written

permission of TWCA.

網域所有權驗證手冊-檔案驗證

1	目的	. 1
2	範圍	. 2
3	參考資料	. 3
4	定義	. 4
5	作業程序	. 5
6	附件	10

i

- 1 目的
 - 1.1 為符合 SSL 憑證國際審放標準(CA/Browser Forum Baseline Requirements), TWCA 必須驗證 SSL 憑證申請者擁有該網域的所有 權, TWCA 才能進行 SSL 憑證核發。
 - 1.2 說明如何透過檔案驗證方式,完成網域所有權驗證。
 - 1.3 若 SSL 憑證申請者的網域於 Whois(用來查詢網際網路裡網域名稱的 IP 以及所有者等資訊)資料設定為不揭露,TWCA 無法利用網域所有 權方式來驗證 SSL 憑證申請者是否擁有該網域的所有權,將採檔案驗 證方式,來驗證 SSL 憑證申請者推有申請網站的控制權。

2 範圍

2.1 適用範圍

本手冊將針對網域所有權驗證之檔案驗證方式提供操作步驟說 明。

3 參考資料

3.1 CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ,

3.2.2.4. Validation of Domain Authorization or Control

3.2.2.4.6 Agreed-Upon Change to Website

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.5.pdf

4 定義

無

5 作業程序

以下針對市面上三種常用的網頁伺服器, 說明如何設定檔案驗證的操 作步驟。(設定驗證用檔案不會對您的網站造成影響)

5.1 流程圖

無

5.2 控制措施

5.2.1 產生 CSR(憑證請求檔)並至 TWCA 官網上傳。

5.2.2 於上傳步驟中「網域所有權」選項,選擇「網站檔案驗證: (Whois 資料設定為不揭露)」,並填入您欲接收驗證用的檔案的 Email 信 箱,點選繼續完成 CSR 上傳作業。

網域所有權

用试验理者	▲符合SSL墨號國際審放標準,將審驗側域所有權請意選擇以下一種審驗方式。 ● 網域所有權EMAIL機麼:點還確認後,系統將會自動容出驗證信,諸用戶路必至說信翰收信並點擊確認即可。 ● maintain母twca.com.tw (網域註冊資料來源由WHOIS取得) 或諸選擇 ● admin母twca.com.tw ● administrator@twca.com.tw ● webmaster@twca.com.tw ● hostmaster@twca.com.tw ● postmaster@twca.com.tw
	 例站檔案驗證:(Whois資料設定為不提獎) 請您填入接收電子儘管:maintain@twca.com.tw 將郵荷檔案及說明給您。
	諸忽填入接收電子信箱:maintain@twca.com.tw

- 5.2.3 本中心會寄發主旨為「xxx(網站名稱)設定為不揭露 Whois 資訊的網站無法驗證,請協助完成網站驗證」Email,並於 Email 中提供 一個驗證用的附件檔案 dcv.zip
- 5.2.4 解壓縮後目錄與檔案階層為\.well-known\pki-validatio\whois.txt (whois.txt 檔案內容為英文數字亂數值,例如

"f80c1cf0765b6dd2b4a1373f3ece474faaae4c97f23fd2f83f8a7ffb9231a bff") °

5.2.5 IIS 設定方式

- 5.2.5.1 確認網站檔案置放路徑
 - 5.2.5.1.1 開啟 Internet Information Services (IIS) 管理員
 - 5.2.5.1.2 於您的網站名稱上按滑鼠右鍵,選擇「管理網站」,

點選「進階設定」,其中「實體路徑」的設定路徑即為 您的網站檔案置放路徑。

例如:站台"Default Web Site",

"%SystemDrive%\inetpub\wwwroot"即表示您的網站置 放路徑

~	(一般)	
	名稱	Default Web Site
	預先載入已啟用	False
	實體路徑	%SystemDrive%\inetpub\www.rc
	實體路徑認證	
	實體路徑認證登入類型	ClearText
	應用程式集區	DefaultAppPool
	繫結	http:*:80:
	識別碼	1
~	行為	
	已啟用的通訊協定	http
>	限制	
2	28 牧 须	
審	體路徑	

5.2.5.1.3 將步驟 5.2.3 取得並解壓縮後的目錄與檔案,置於您 的網站檔案置放路徑下。

> 例如: 將\.well-known\pki-validatio\whois.txt 置於 %SystemDrive%\inetpub\wwwroot下



5.2.5.1.4 重啟 IIS 服務使設定生效。

- 5.2.5.2 請先參考 5.2.8 章節完成自我驗證,確認設定成功且已生 效。
- 5.2.5.3 通知 TWCA 您已完成檔案驗證設定。

5.2.6 Apache 設定方式

5.2.6.1 確認網站檔案置放路徑

- 5.2.6.1.1 開啟設定檔 httpd.conf
- 5.2.6.1.2 搜尋關鍵字 DocumentRoot,其設定路徑即為您的網站

檔案置放路徑。

例如: 搜尋結果 DocumentRoot "D:/Apache2.2/htdocs"

即表示您的網站置放路徑為 D:/Apache2.2/htdocs # DocumentRoot: The directory out of which you will serve your # documents. By default, all requests are taken from this directory, but # symbolic links and aliases may be used to point to other locations.

DocumentRoot "D:/Apache2.2/htdocs"

5.2.6.1.3 將步驟 5.2.3 取得並解壓縮後的目錄與檔案,置於您

的網站檔案置放路徑下。

例如: 將\.well-known\pki-validatio\whois.txt 置於

D:/Apache2.2/htdocs 下

《 本機磁磁	業(D:) > Apache2.2 > htdocs > .well-known >	pki-validation
^	名稱	修改日期
	whois.txt	2019/9/23 下午 0

5.2.6.1.4 重啟 Apache 服務使設定生效。

5.2.6.2 請先參考 5.2.8 章節完成自我驗證,確認設定成功且已生

效。

5.2.6.3 通知 TWCA 您已完成檔案驗證設定。

5.2.7 Tomcat 設定方式

5.2.7.1 將步驟 5.2.3 取得並解壓縮後的檔案 whois.txt,置於您指定的實體目錄下。

```
例如: 將 whois.txt 置於 D:/Tomcat6.0/temp
```

×	本機磁碟 (D:) >	Tomcat6.0	> temp
	名稱	^	
	whois.txt		

5.2.7.2 於 Tomcat 中增加虛擬目錄

- 5.2.7.2.1 在 apache-tomcat 安裝目錄下的 \conf 底下,編輯 server.xml 檔案。
- 5.2.7.2.2 在 Host 標籤內,新增虛擬目錄節點。
 - 新增設定範例如下:
 - <Context docBase="D:/Tomcat6.0/temp" path="/.well-
 - known/pki-validation" reloadable="true"/>

(docBase 的設定值為您置放 whois.txt 的實體目錄)

- <Host name="localhost" appBase="webapps"
 unpackWARs="true" autoDeploy="true"
 xmlValidation="false" xmlNamespaceAware="false">
- <!-- SingleSignOn valve, share authentication between web applications Documentation at: /docs/config/valve.html -->

- <!-- Access log processes all example. Documentation at: /docs/config/valve.html -->
- ---

ontext docBase="D:/Tomcat6.0/temp" path="/.well-known/pki-validation" reloadable="true"/:

</Host>

5.2.7.2.3 設定完成後儲存 server.xml 檔案。

5.2.7.2.4 重啟 tomcat 服務使設定生效。

5.2.7.3 請先參考 5.2.8 章節完成自我驗證,確認設定成功且已生 效。 5.2.8 自我驗證方式

- 5.2.8.1 使用瀏覽器連至以下網址,確認可正常瀏覽 <u>http://您的網站</u> /.well-known/pki-validation/whois.txt
- 5.2.8.2 以本公司網站為例,設定完成後呈現效果如下

https://www.twca.com.tw/.well-known/pki-validation/whois.txt



5.3 權宜措施

無

5.4 特別注意事項

無

6 附件

無