網站安全傳輸協定(HTTPS)設定說明

112年3月

大綱

1 **HTTPS**安全連線說明

2 網站設置常見錯誤態樣

3 其他注意事項

1.HTTPS安全連線說明

HTTPS安全連線說明

1. 為確保政府網站傳輸之安全性，各政府機關建置、主責之網站應全面導入安全通訊協定(以下稱HTTPS)。HTTPS使用TLS憑證加密封包，降低資料傳輸遭竊取之風險。
2. 數位部建置政府伺服器數位憑證管理中心(GTLSCA，https://gov.tw/iRQ)，專職簽發TLS憑證供各政府機關申請使用，效期為1年，已申請者應於效期前重新申請新憑證。

政府機關申請**TLS**憑證程序

1. 申請網站及說明：https://gov.tw/iNH
2. 申請TLS憑證的兩種方式：
   (1)發文申請。
   (2)使用GCA IC卡線上申請。(核發速度較快)

政府機關安裝**TLS**憑證及憑證串鍊設定

1. 安裝TLS憑證後，須至GTLSCA下載憑證串鍊中其他相關憑證(https://gov.tw/Nur)，並依照各類伺服器軟體安裝手冊說明進行憑證串鍊設定，憑證串鍊中之憑證檔如下：

   - ROOTeCA_64.crt
   - eCA1_to_eCA2-New.crt
   - GTLSCA.crt

政府機關安裝**TLS**憑證及憑證串鍊設定

2. 設定憑證串：
   - 憑證串鍊需完整安裝(不可僅安裝TLS憑證)
   - GTLSCA SSL之憑證串鍊為：eCA → eCA1_to_eCA2-New → GTLSCA →用戶TLS憑證
   - 如憑證串鍊設定錯誤，某些瀏覽器將出現不信任警告。(可使用線上檢測工具SSL Checker確認 https://www.sslshopper.com/ssl-checker.html)
3. 如有申請程序及設定疑義可洽電子化政府客服中心(02-2192-7111)

轉導至**HTTPS**設定及注意事項

如網站已使用HTTPS，仍須檢查是否有同時使用HTTP，建議將 HTTP 關閉或將流量重新導向至HTTPS，設定網站之redirect Port其屬性設定指向正確埠(443)，建議以下兩項設定搭配使用：

(1)**使用301/302轉址**。

(2)**使用HSTS設定(建議設定1年)**。

(1)使用**301/302**轉址

透過設定301/302轉址，讓HTTP網站重新導向至HTTPS。

1. 301轉址(建議)：(永久性轉址)

   將舊網址永久轉導向新網站，並將頁面權重導向新網站。

2. 302轉址：(暫時性轉址)

   僅暫時轉導向新網站，且不移轉頁面權重。

(2)HSTS 設定

1. HSTS說明：
   讓用戶強制使用HTTPS與網站進行連線。
2. 設定方式：
   - 在HTTP header 加入 Strict-Transport-Security 。
   - 參數max-age(瀏覽器記得網站使用HTTPS連線之時間)，建議設定為 1年。

2.網站設置常見錯誤態樣

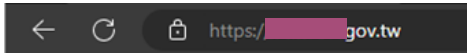
2.常見錯誤態樣

請於設置HTTPS完成後，確認是否有以下錯誤態樣，避免造成設定失效

(1)未關閉HTTP，且未設定轉導。
(2)未立即轉導至HTTPS。
(3)僅有首頁設定轉導。
(4)網頁內嵌HTTP元素。
(5)憑證串鍊中斷。

(1)未關閉**HTTP**，且未設定轉導(案例)

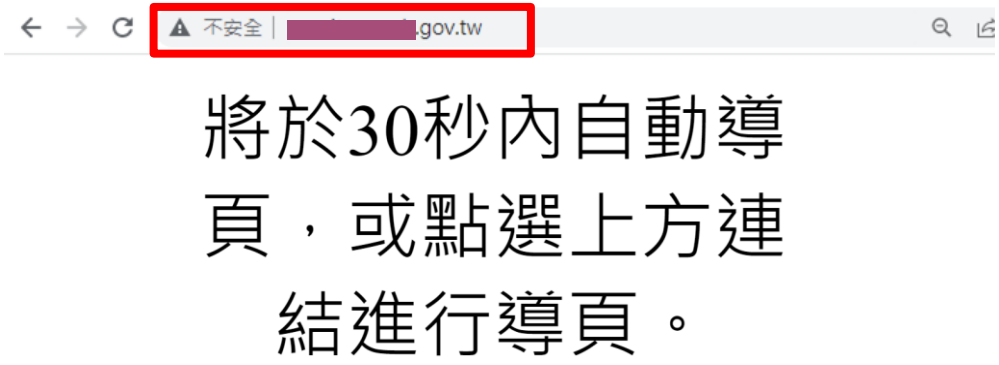
1. 以某網站為例，同時開放(並存)HTTP/HTTPS連線，導致民眾仍有機會連入不安全的網址。
   - HTTP 連線 

   - HTTPS連線 

2. 建議關閉HTTP，或設定轉導至HTTPS。

(2)未立即轉導至HTTPS(案例)

1. 以某平台為例，進入HTTP頁面後，數秒才自動導轉到HTTPS。
2. 請改為立即跳轉，以保持連線安全性，或直接關閉HTTP。



(3)僅首頁設定轉導

1. 僅首頁設置轉導，但網站分頁未設定，如從其他分頁連入網站，將不會自動轉跳至HTTPS安全連線。
2. 請依據建議於站台設定301/302轉導、HSTS ，或關閉HTTP連線。

(4)網頁內嵌HTTP元素

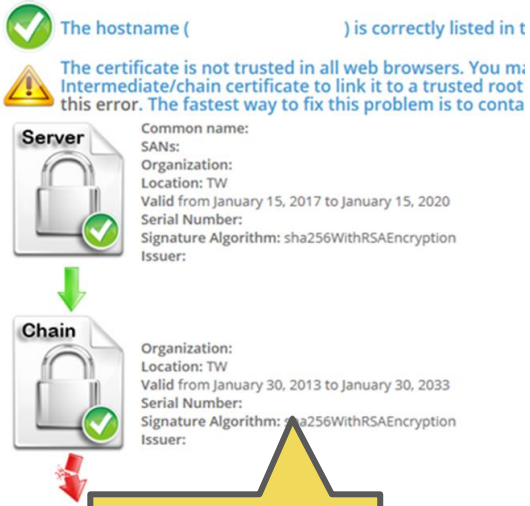
1. 雖已使用HTTPS安全連線，但因網頁內容元素(例如圖檔、影片來源為HTTP站台)，部分瀏覽器會顯示不安全。例如內部網頁內含http圖檔:

2. 請檢查網頁元素，移除所有HTTP元素，改為HTTPS。

(5)憑證串鍊中斷

1. 匯入TLS憑證需注意憑證串鍊完整性，如設定不完整導致憑證串鍊中斷，瀏覽器仍會出現不信任警告。
2. 請洽貴機關網站維護人員重新設定憑證串鍊，並可使用線上工具SSL Checker檢測是否安裝正確。

   https://www.sslshopper.com/ssl-checker.html



憑證串鍊中斷案例
(SSL checker檢測結果)

3.其他注意事項

其他注意事項

1. 請評估網站關閉HTTP之可行性，以全面性提升網站之安全性。
2. 請清查是否有已不再使用的網站(例:特定活動效期之網站、改版後的舊網站)，應將該網站下架且至GSN註銷域名，以避免作為駭客攻擊的跳板。
3. 政府機關TLS憑證效期為1年，請記得於逾期前申請新的憑證。

數位發展部

Ministry of Digital Affairs