

資安宣導

網站為什麼需要導入 HTTPS

網站為什麼需要導入HTTPS

- 一、符合資通安全及個資保護相關法令規範
- 二、依行政院國家資通安全會報第31次委員會議決議、教育部107年3月21日臺教資(五)字第1070041450號函及108年10月24日臺教資(五)字第1080154973號函辦理。
- 三、提高網站資料傳輸的安全性
 - ✓ 保護個資相關資料
 - ✓ 保護業務機敏資料
- 四、瀏覽器逐漸不支援非HTTPS網站
- 五、提升網站的可信任度
- 六、有助提升搜尋引擎排名

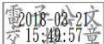
 不安全 | http://.ccu.edu.tw

發文日期：中華民國107年3月21日
發文字號：臺教資(五)字第1070041450號
速別：普通件
密等及解密條件或保密期限：
附件：國發會https簡報(1070041450_Attach1.pdf)

主旨：請依「政府機關導入網站安全傳輸通訊協定」推動目標及範圍(如附件)，依期程於107年6月底前完成所屬對外服務網站導入安全傳輸通訊協定(HTTPS)相關作業，請查照。

說明：依據國家發展委員會106年12月13日發資字第1061503130號函辦理。

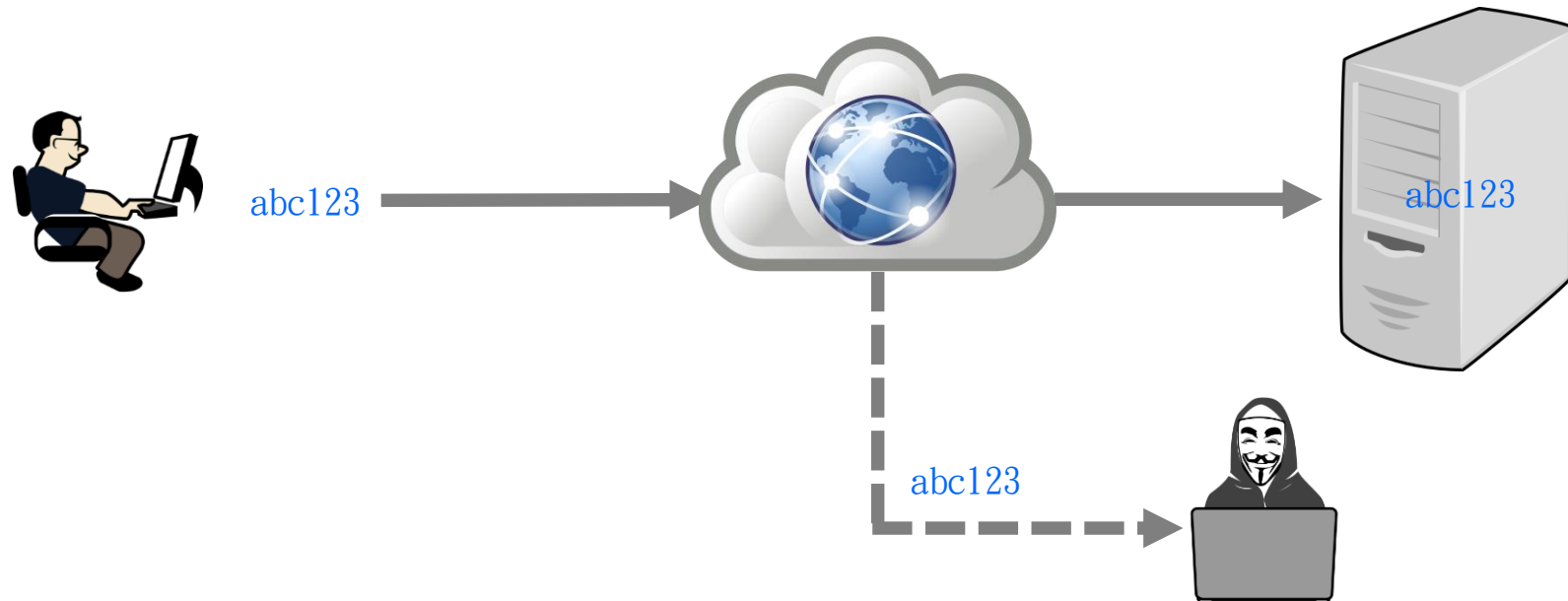
正本：各國立大專校院、各國立大學附設醫院及農林場

副本：

HTTP vs. HTTPS

- HTTP (HyperText Transfer Protocol)

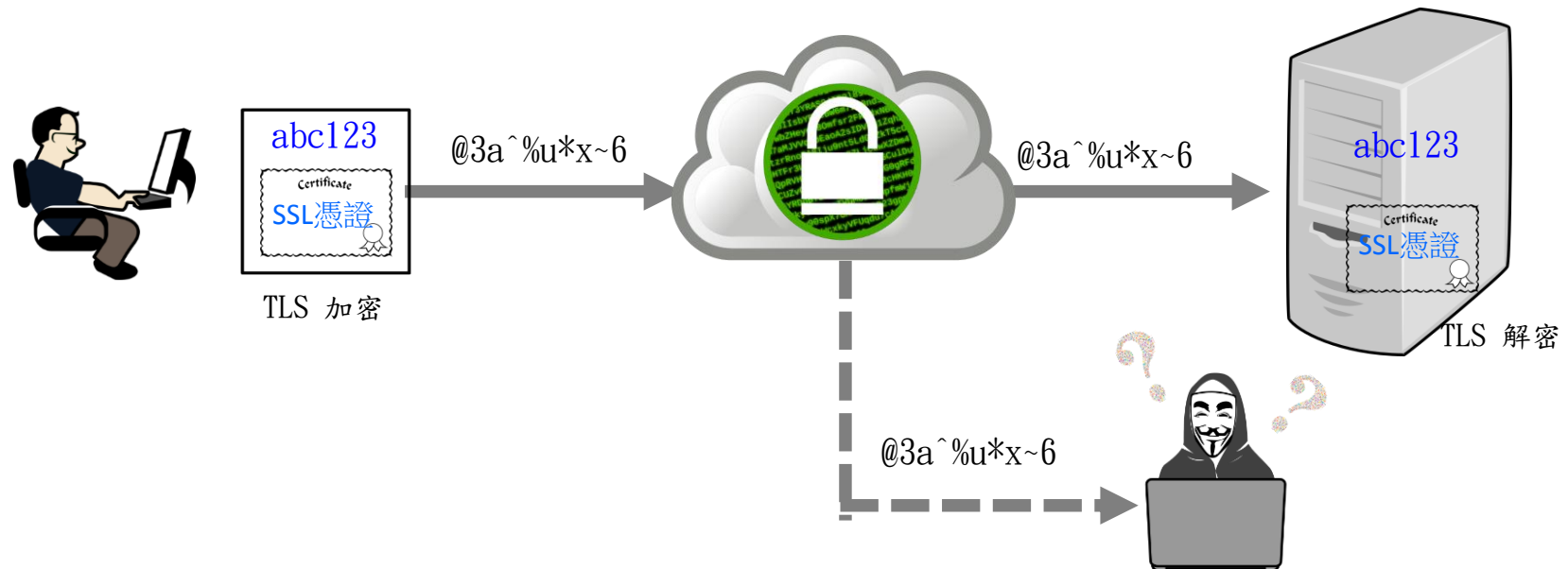
HTTP是瀏覽網站時使用的通訊協定，資料以**未加密的明文**傳送，駭客在中途擷取封包即可以輕易獲知資訊內容，因此是一種**不安全**的通訊協定。



HTTP vs. HTTPS

- HTTPS (HTTP over TLS)

為了防止資料在傳輸途中被駭客攔截竊取，造成個資或業務機敏資料洩漏，瀏覽器和網站之間會建立加密通道，資料經TLS加密成密文後再傳送，即使在途中被駭客竊聽到，也難以得知資訊內容，降低資料外洩的風險，是一種較安全的協定。

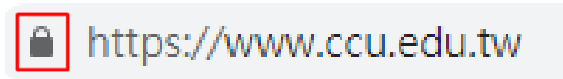


檢視網站是否已經導入HTTPS

- 正確導入HTTPS

(一)以https://... 方式可以正常連線，網址列出現安全鎖。

(二)再以http://... 方式連線，會自動跳轉到https安全連線。



← 點擊安全鎖圖示



← 彈出視窗上出現「憑證(有效)」。

檢視網站是否已經導入HTTPS

• 未導入HTTPS

(一)以http://...方式可正常連線，
網址列出現不安全的圖示。



(二)再以https://...方式連線，
無法連上網站。



✓ 點擊網址列前面的圖示，彈出視窗上沒有出現「憑證」的項目。

檢視網站是否已經導入HTTPS

- 憑證過期



- 不安全的加密協定



TLS (Transport Layer Security) 加密協定

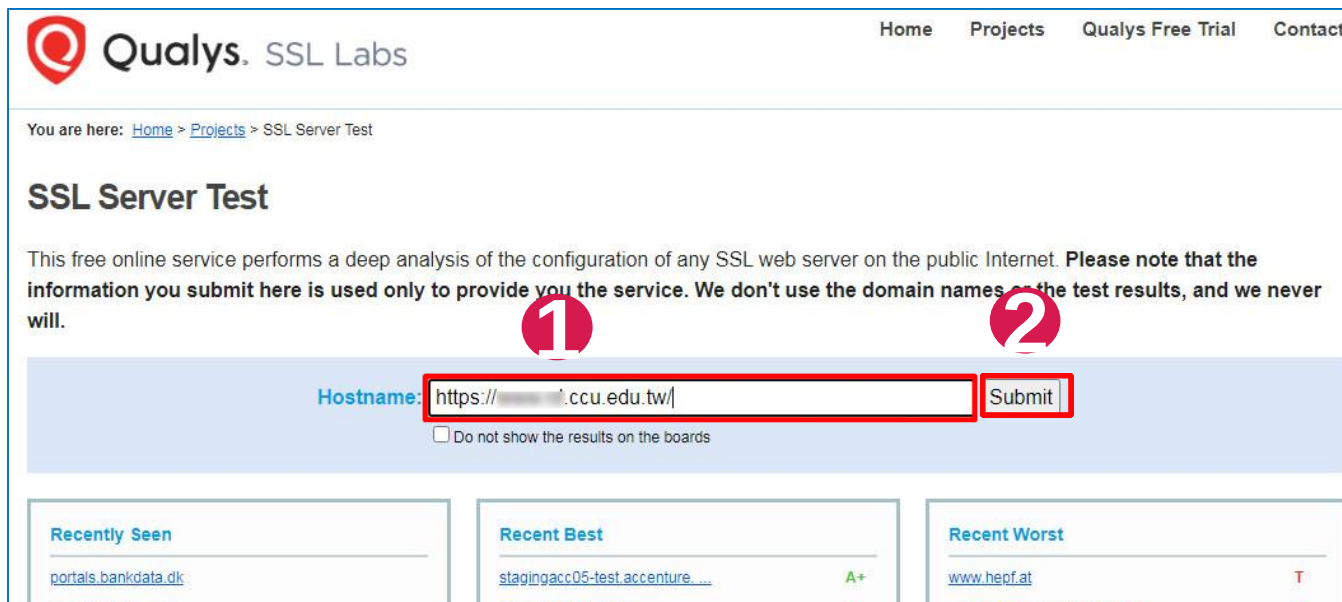
- TLS 的前身稱為 SSL (Secure Sockets Layer)，主要是為網路應用程式提供資料加/解密的服務。

協 定	發布時間	備註
SSL	未公布	網景公司設計，因存在嚴重安全漏洞，從未正式公開
SSLv2	1995 年	2011年棄用， 已不安全, 必須關閉 。
SSLv3	1996 年	2015年棄用， 已不安全, 必須關閉 。
TLS 1.0	1999 年	IETF將SSL標準化並改名為TLS， 已不安全, 必須關閉 。
TLS 1.1	2006 年	瀏覽器大廠在2020年將終止支援TLS1.0 及 TLS 1.1， 具資安風險，必須關閉
TLS 1.2	2008 年	主流地位接近尾聲，逐漸被 TLS 1.3 取代
TLS 1.3	2018 年	新版本瀏覽器逐漸將 TLS 1.3 設為預設值

- 作業系統、瀏覽器**須升級**至較新版本才能支援 TLS1.3

檢查網站 TLS 支援版本

- 如何知道網站支援的TLS版本？
 - ✓ 利用 [Qualys SSL Labs](https://www.ssllabs.com/ssltest/) 線上服務進行測試
 - ✓ 未導入HTTPS之網站或使用IP型式之網址無法測試！



Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names in the test results, and we never will.**

1

2

Hostname:

☐ Do not show the results on the boards

Recently Seen	Recent Best	Recent Worst
portals.bankdata.dk	stagingacc05-test.accenture... A+	www.hepf.at T

網址：<https://www.ssllabs.com/ssltest/>

檢視網站 TLS 支援版本

- ✓ 測試結果相當完整，請將畫面向下捲至Configuration處，即可看到網站 TLS 啟用的狀態：

Configuration		
	Protocols	
	TLS 1.3	Yes
	TLS 1.2	Yes
	TLS 1.1	No
	TLS 1.0	No
	SSL 3	No
	SSL 2	No

- ✓ 請確定 TLS1.1 / TLS1.0 / SSL3 / SSL2 均為 No。

檢視網站 TLS 支援版本

✓ 某單位網站實際案例：



Configuration

Protocols	Status
TLS 1.3	No
TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3	INSECURE Yes
SSL 2	INSECURE Yes

未禁用不安全的加密協定

SSL憑證(SSL Certificate, SSL CA)

- SSL憑證是由受信任的數位憑證認證機構（Certificate Authority, CA）核發，以確認網站的身份
- 網站在導入HTTPS時需先準備好SSL憑證及解密私鑰，以供資料加解密之用。
- SSL憑證有一定的效期，並非永久有效。
- 取得SSL憑證的方式：
 - ✓ 付費：向商業性質的認證機構(例如中華電信、台灣網路認證中心TWCA)申請購買。可依需求決定購買效期。
 - ✓ 免費：可向 Let's Encrypt 申請，最長效期為三個月。

如何申請 SSL 憑證

- 使用 資訊處 提供之 標準環境vm主機 之網站：
 - ✓ 使用單位需配合系統升級至新版環境，之後 SSL憑證之申請及HTTPS之導入，由資訊處協助處理。
 - ✓ 原機升級 (PHP 5 升級至 PHP 7) 可能導致網站無法正常運作，因此必須分兩個階段進行：
 - 申請新版環境測試主機，並自行將網站資料移至測試機進行測試。
 - 待測試無誤後再以測試主機取代原網站vm主機。
 - ✓ 若網站仍為IP形式者，需先申請DNS名稱。
 - ✓ 完成網站環境升級後，由資訊處協助完成HTTPS導入。

如何申請 SSL 憑證

- 非資訊處之標準環境vm主機 (自建主機、委外託管)：
 - ✓ 申請 Let's Encrypt 免費憑證 (以 Ubuntu 20.04 版 Linux 為例)
 - ✓ 使用 dehydrated 套件可非常容易申請 Let's Encrypt 的SSL憑證
 - ✓ 以系統管理員 (root) 身份執行以下命令，即可產生憑證檔

```
# apt update
# apt install dehydrated
# vi /etc/dehydrated/config
WELLKNOW="$[BASEDIR]/acme-challenges
# mkdir /var/lib/dehydrated/acme-challenge
# mkdir /var/www/html/.well-known
# cd /var/www/html/.well-known
# ln -s /var/lib/dehydrated/acme-challenge .
# dehydrated --register --accept-terms
# dehydrated -c -d xxx.ccu.edu.tw
```

//確保取得最新版套件

//安裝 dehydrated 套件

//修改設定檔

將 acme-challenges 的 s 去掉

//以下四行在網站資料夾
底下建立供Let's Encrypt
確認身份用的資料夾

//第一次申請須執行此行

//產生主機 xxx.ccu.edu.tw憑
證及私鑰等必要檔案

如何申請 SSL 憑證

- ✓ 產生之檔案在 </var/lib/dehydrated/cert/xxx.ccu.edu.tw/> 資料夾下，導入HTTPS需要的個檔案：

[fullchain.pem](#)

(主機 xxx.ccu.edu.tw 的SSL憑證檔)

[privkey.pem](#)

(解密資料所需的私鑰)

- ✓ 憑證到期時，執行以下指令即可重新產生憑證檔：

```
# dehydrated -c -d xxx.ccu.edu.tw
```

如何申請 SSL 憑證

- ✓ 如欲申購**付費憑證**，請參考發行憑證機構之相關網頁說明。
委外託管之網站，可洽委辦廠商協助處理。

TWCA：https://www.twca.com.tw/portal/service/ftc_1_6.html

中華電信：<https://publicca.hinet.net/SSL-02.htm>

- ✓ 申購前須先準備**憑證請求檔** (Certificate Signing Request, CSR 檔)
- ✓ openssl 是一套跨平台的套件，可以用來產生憑證請求檔及解密資料用的私鑰。若無法執行，可自行安裝：

```
# apt install openssl
```

- ✓ 執行 openssl 時，系統會要求輸入組織所在地、組織及部門名稱、主機名稱、電子郵件等相關資訊，指令用法如下頁：

如何申請 SSL 憑證

```
# openssl req -new -newkey rsa:2048 -sha256 -nodes -keyout privkey.pem -out  
cert.csr -days 365
```

Country Name (2 letter code) [AU]:	TW
State or Province Name (full name) [Some-State]:	Taiwan
Locality Name (eg, city) []:	Chiayi
Organization Name (eg, company) [Internet Widgits Pty Ltd]:	National Chung Cheng University
Organizational Unit Name (eg, section) []:	Department of Xxx (單位名稱)
Common Name (e.g. server FQDN or YOUR name) []:	xxx.ccu.edu.tw (主機名稱)
Email Address []:	mymail@ccu.edu.tw (主機管理者電子郵件)
A challenge password []:	直接按Enter鍵
An optional company name []:	直接按Enter鍵

註：指令中的365憑證有效天數，可依實際需求更改。

綠字直接照抄無須修改，藍字則依各單位狀況輸入正確資訊。

✓ 執行後會產生 *privkey.pem* 和 *cert.csr* 兩個檔案：

cert.csr (憑證請求檔，上傳至憑證發行機購用)

privkey.pem (日後解密資料用的私鑰，自行保存)

快速總結

- 網站應強制導入HTTPS以提高安全性。
- 作業系統及瀏覽器應升級以支援較新較安全的加密協定。
 - ✓ 網站作業系統 (FreeBSD, Linux, Windows Server, ...) 應升級至最新之穩定版本。
 - ✓ Win7 未支援 TLS 1.3，應升級至 Win10。
- 可用 [Qualys SSL Labs](#) 線上服務檢測網站加密安全性。
 - ✓ 不安全或具資安風險的加密協定，包括：SSL2、SSL3、TLS 1.0 及 TLS 1.1，應全部禁用。
 - ✓ 如無特殊考量，應考慮支援 TLS 1.3。
- 經費困難之單位，可多利用 [Let's Encrypt](#) 免費憑證。

感謝閱讀