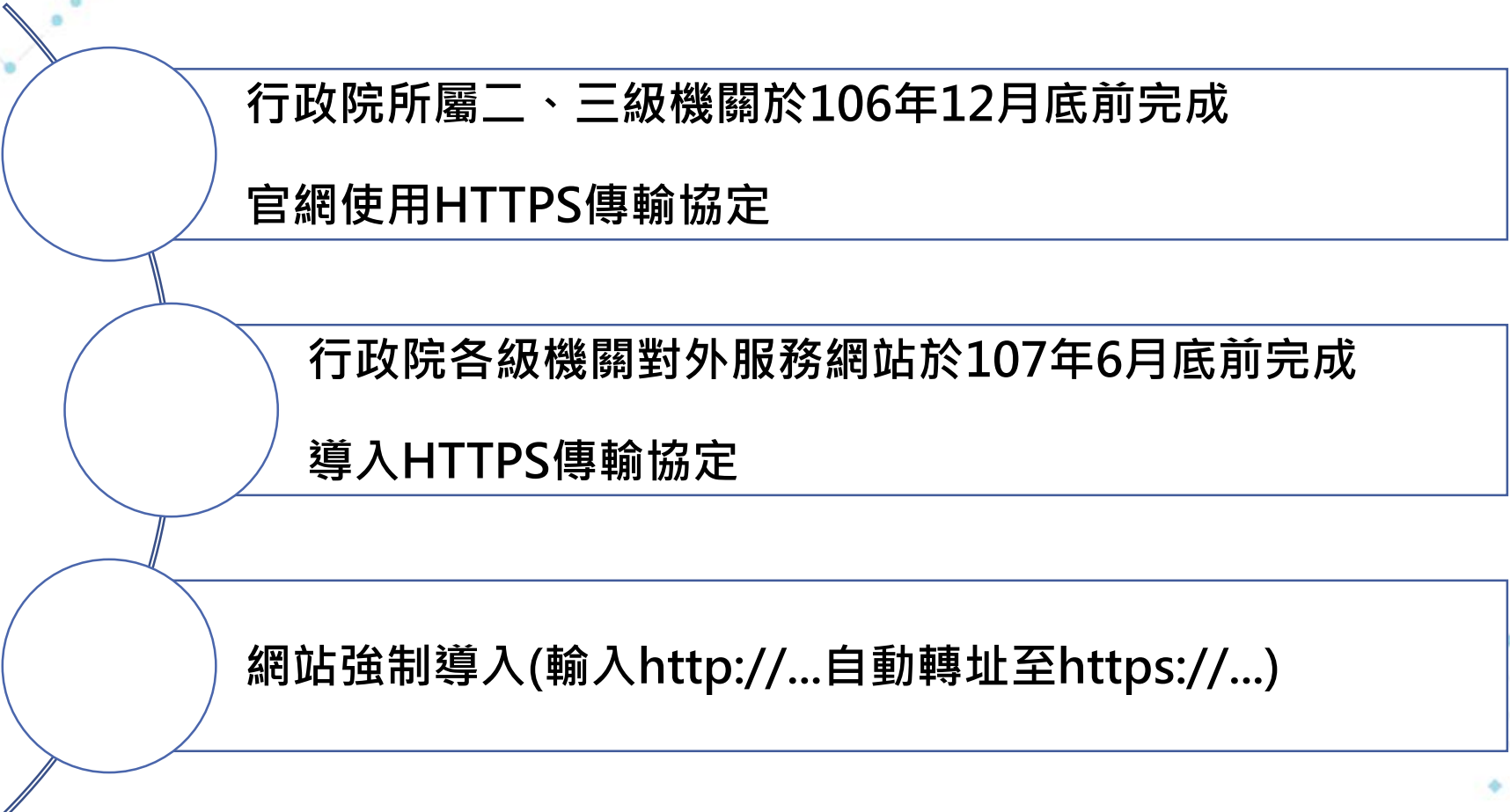




# HTTPS服務導入

國立中山大學圖書與資訊處  
資安組王聖全

# 教育部公文來函導入範圍說明



行政院所屬二、三級機關於106年12月底前完成  
官網使用HTTPS傳輸協定


行政院各級機關對外服務網站於107年6月底前完成  
導入HTTPS傳輸協定

網站強制導入(輸入http://...自動轉址至https://...)


# HTTPS

- HTTP:一個用戶端終端(用戶)和伺服器端(網站)請求和應答的標準
  - <http://www.nsysu.edu.tw>
- HTTPS
  - 加過密的 HTTP，用SSL/TLS來加密封包
  - 在不安全的網路上建立一安全信道，並可在使用適當的加密套件和伺服器憑證可被驗證且可被信任時，對竊聽和中間人攻擊提供合理的防護。

HTTPS 

 安全 | <https://www.google.com.tw>

HTTP 

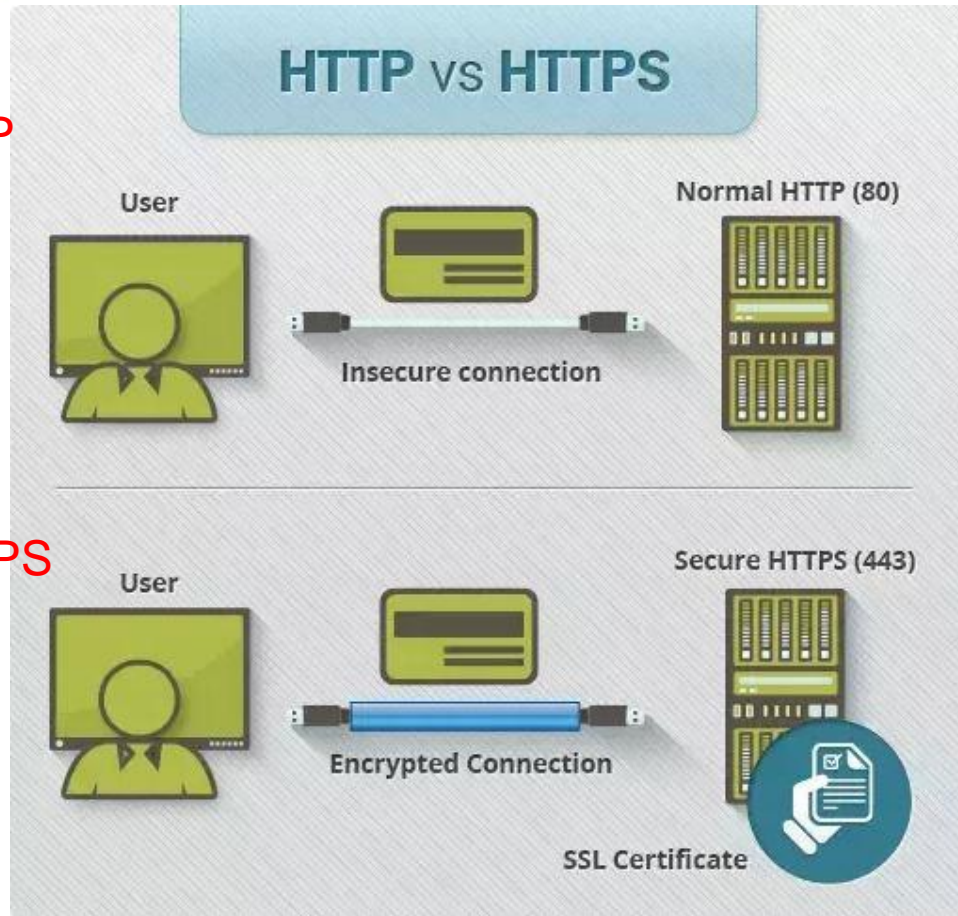
 [www.nsysu.edu.tw/bin/home.php](http://www.nsysu.edu.tw/bin/home.php)



# HTTP v.s. HTTPS

HTTP

HTTPS



HTTP

<http://domain-name.com>

HTTPS

[Secure | https://domain.com](https://domain.com)

# HTTP v.s. HTTPS (cont.)

Transmission Control Protocol, Src Port: 49363 (49363), Dst Port: http (80)  
Source port: 49363 (49363)

Offset	Hex	ASCII
00	00 25 9c 63 e8 65 00 15 c5 82 27 5a 08 00 45 00	..%.c.e... ..'Z..E.
10	04 e4 20 84 40 00 80 06 00 00 c0 a8 01 05 4a 7d	... .@... .....J}
20	57 93 c0 d3 00 50 82 64 11 54 a6 32 9a c6 50 18	w....P.d .T.2..P.
30	40 3d 68 94 00 00 7 15 54 20 2f 73 65 61 72 63	@=h...GE T /searc
40	68 3f 68 6c 3d 65 6 20 3 6f 75 72 63 65 3d 68	h?hl=en& source=h
50	70 26 71 3d 74 65 73 74 26 61 71 3d 66 26 61 71	p&q=test &aq=f&aq
60	69 3d 67 2d 70 33 67 37 26 61 71 6c 3d 26 6f 71	i=g-p3q7 &aql=&oq
70	3d 26 67 73 5f 72 66 61 69 3d 20 48 54 54 50 2f	=&gs_rfa i= HTTP/
80	31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 67	1.1..Host: www.g
90	6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65	oogle.co m..Conne
a0	63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76	ction: k eep-aliv

Transmission Control Protocol, Src Port: 49362 (49362), Dst Port: https (443)  
Source port: 49362 (49362)  
Destination port: https (443)

Offset	Hex	ASCII
0000	00 25 9c 63 e8 65 00 15 c5 82 27 5a 08 00 45 00	..%.c.e... ..'Z..E.
0010	05 1a 21 29 40 00 80 06 00 00 c0 a8 01 05 4a 7d	...!)@... .....J}
0020	57 93 c0 d2 01 bb 9d 85 1c 7a 0f 8b 5f 0f 50 18	w..... .Z...P.
0030	40 3d 68 ca 00 00 7 03 01 04 ed c3 e8 c8 e0 bb	@=h.....
0040	79 2e 7d 7e 82 b6 3 39 6 dc d5 d6 7a 4f 01 35	y.}~... p...zo.5
0050	e1 49 c8 93 60 84 4a 0c b3 fe d7 2b 88 ed 80 c8	.I... .J. ...+....
0060	ea 4e 45 56 df 40 38 07 06 e7 3a 14 07 30 16 50	.NEV.@8. ....0.F
0070	39 bf 49 e1 e4 7d 4f 91 86 47 d3 cd b0 8f f8 99	9.I..}O. .G.....
0080	8e 36 3e 0b ec ba cc 19 d3 66 4b 91 5b ec 65 2b	.6>..... .fK. [.et
0090	d1 ca 92 19 a2 2e c1 57 bd 79 08 91 51 bc 54 91	.....W .y..Q.T.

# SSL憑證

頁面資訊 - https://sso.nsysu.edu.tw/

一般 (G) 媒體 (M) 權限 (P) 安全 (S)

網站身份

網站: sso.nsysu.edu.tw

擁有者: 這個網站沒有提供擁有者資訊。

驗證機構: COMODO CA Limited

到期於: 2019年12月25日

檢視憑證 (V)

隱私及歷史記錄

我以前瀏覽過這個網站嗎? 有, 7 次

此網站有在我的電腦中儲存資訊 (Cookie) 嗎? 是 檢視 Cookie (K)

我有在此網站儲存任何密碼嗎? 是 檢視已存密碼 (W)

技術細節

連線已加密 (TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA、128 位元金鑰、TLS 1.0)

您正在瀏覽的網頁在傳送前有經過加密。

加密功能會讓未授權的使用者很難偷聽兩台電腦間傳輸的資訊, 所以此頁面在網路上傳輸時很難會有人看到內容。

憑證檢視器: 「\*.nsysu.edu.tw」

一般 (G) 詳細資訊 (D)

憑證層級 (H)

- COMODO RSA Certification Authority
  - COMODO RSA Organization Validation Secure Server CA
    - \*.nsysu.edu.tw

憑證欄位 (F)

- \*.nsysu.edu.tw
  - 憑證
    - 版本
    - 序號
    - 憑證簽章演算法
    - 簽發者
  - 有效
    - 不早於

欄位值 (V)

匯出 (O)...

關閉 (C)



# 免費 V.S. 付費

	免費憑證	付費憑證
優點	<ul style="list-style-type: none"><li>• 快速、免費</li><li>• 自動驗證(Domain Validation Only)</li></ul>	<ul style="list-style-type: none"><li>• 使用期限長(1~2年)</li><li>• 安全性較高</li><li>• CA會support</li></ul>
缺點	<ul style="list-style-type: none"><li>• 使用期限短(30~90天)</li><li>• 安全性相對較低</li><li>• No Support</li></ul>	<ul style="list-style-type: none"><li>• 申請時間較長</li><li>• 付費(子網域憑證需分開購置)</li></ul>

# 目前本處已購置之憑證

- 一層
  - \*.nsysu.edu.tw
- 二層
  - \*.lib.nsysu.edu.tw
  - \*.lis.nsysu.edu.tw
  - \*.cloud.nsysu.edu.tw
  - \*.ezproxy.lis.nsysu.edu.tw



# Linux 平台憑證導入

- 啟動Apache SSL module
  - `a2enmod ssl`
- 複製Apache設定檔
  - `cp /etc/apache2/site-available/default-ssl.conf /etc/apache2/site-enabled/ ssl.conf`
- 修改ssl.conf設定檔，更改憑證路徑
  - `SSLCertificateFile /存放路徑/nsysu2014.cer`
  - `SSLCertificateKeyFile /存放路徑/nsysu2014.key`
  - `SSLCertificateChainFile /存放路徑/bundle-sha2.cer`

# Linux 平台憑證導入 (cont.)

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin [REDACTED]
    ServerName [REDACTED]
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
#
# SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
# SSLCertificateKeyFile  /etc/ssl/private/ssl-cert-snakeoil.key
    SSLCertificateFile /etc/apache2/ssl/nsysu2014.cer
    SSLCertificateKeyFile /etc/apache2/ssl/nsysu2014.key
    SSLCertificateChainFile /etc/apache2/ssl/bundle-sha2.cer
    <FilesMatch "\.(cgi|shtml|phtml|php)$">
      SSLOptions +StdEnvVars
    </FilesMatch>
    <Directory /usr/lib/cgi-bin>
      SSLOptions +StdEnvVars
    </Directory>
    <Directory /var/www/>
      Options FollowSymLinks MultiViews
      AllowOverride None
      Order allow,deny
      allow from all
      SSLOptions +StdEnvVars
    </Directory>
  </VirtualHost>
</IfModule>
```

# Linux 平台憑證導入 (cont.)

- 設定檔修改完成後，重新啟動Apache Server
  - `sudo systemctl restart apache2.service`



# 憑證檢查

- SSL Checker

- <https://www.sslshopper.com/ssl-checker.html>
- 確認安裝過程有無問題

## SSL Checker

This **SSL Checker** will help you diagnose problems with your SSL certificate installation. You can verify the SSL certificate on your web server to make sure it is correctly installed, valid, trusted and doesn't give any errors to any of your users. To use the SSL Checker, simply enter your server's hostname (must be public) in the box below and click the Check SSL button. If you need an SSL certificate, check out the [SSL Wizard](#).

[More Information About the SSL Checker](#)

Server Hostname

# 憑證檢查(cont.)

- SSL lab
  - <https://www.ssllabs.com/ssltest/>
  - 確認憑證安全性等級

### 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 or the test results, and we never will.**

Hostname:

Submit

☐ Do not show the results on the boards

#### Recently Seen

<a href="#">analytics.app.wdesk.com</a>	
<a href="#">papexternal.inchcape.com.au</a>	
<a href="#">causatrabalhista.com</a>	
<a href="#">college.com.br</a>	
<a href="#">uatpo4.cbre.com</a>	B
<a href="#">netbank.hwataibank.com.tw</a>	F
<a href="#">uatpo.cbre.com</a>	A
<a href="#">webquote.uat.cbre.eu</a>	A
<a href="#">public.autoins.net.tw</a>	B
<a href="#">www.splprojects.com</a>	B

#### Recent Best

<a href="#">grandest.com</a>	A
<a href="#">game.163.com</a>	A
<a href="#">www.signonday.com.au</a>	A
<a href="#">virageradio.com</a>	A
<a href="#">ylsj.sqianbao.cn</a>	A
<a href="#">www.taishinbank.com.tw</a>	A
<a href="#">analytics.app.wdesk.com</a>	A
<a href="#">youdownload.ctrip.com</a>	A
<a href="#">www.splprojects.com</a>	B
<a href="#">public.autoins.net.tw</a>	B

#### Recent Worst

<a href="#">netbank.hwataibank.com.tw</a>	F
<a href="#">www.hdshowings.com</a>	T
<a href="#">w.couple.net</a>	F
<a href="#">uatecrm.michaelkors-wechat.c...</a>	F
<a href="#">staff.ctc.ca</a>	F
<a href="#">happyemail.co.jp</a>	F
<a href="#">psi.teamexcellencesurveys.co...</a>	F
<a href="#">www.thinkpower.com.tw</a>	F
<a href="#">my.lawsociety.com.au</a>	F
<a href="#">www.corporatebubblesoccer.co...</a>	T