

## Enterprise Linux 實戰講座

### Apache SSL 加密機制

SSL 讓使用者在透過網路傳輸資訊時，用來確保私密性的加密機制。啟用 SSL 的 WWW 伺服器在傳送資料給瀏覽器之前，會先將這些資料加密成密文，使得資料即使在傳送途中遭到截取，第三者也無法讀取資料。瀏覽器收到來自 WWW 伺服器的資料後，會將密文解密以讀取資料。在 WWW 伺服器中使用 SSL，有助於確保 Web 瀏覽器和伺服器之間傳輸的資訊保有私密性，且可讓瀏覽器鑑別伺服器的身分。

# 1 SSL 協定簡介

Secure Sockets Layer (SSL) 通信協定是由 Netscape Communications Corporation 所開發，原先設計的目的是為了確保電子商務以及其他 Web 交易的安全性。SSL 主要是在原網際網路協定架構上加入一個新的 Layer。如圖 1 所示，SSL 插在 HTTP Layer 與 TCP Layer 之間。由於 SSL 是一個新的協定，所以 SSL 通常會要求上下層協定做小幅度的修改，不過其中就 HTTP 應用程式而言，HTTP 應用程式與 SSL 層之間的溝通介面與 HTTP 應用程式直接和 TCP 層之間的溝通介面幾乎相同。除此之外 SSL 協定還有一個非常重要的優點，它可支援 HTTP 以外的應用程式，例如圖 1 所示的 LDAP...

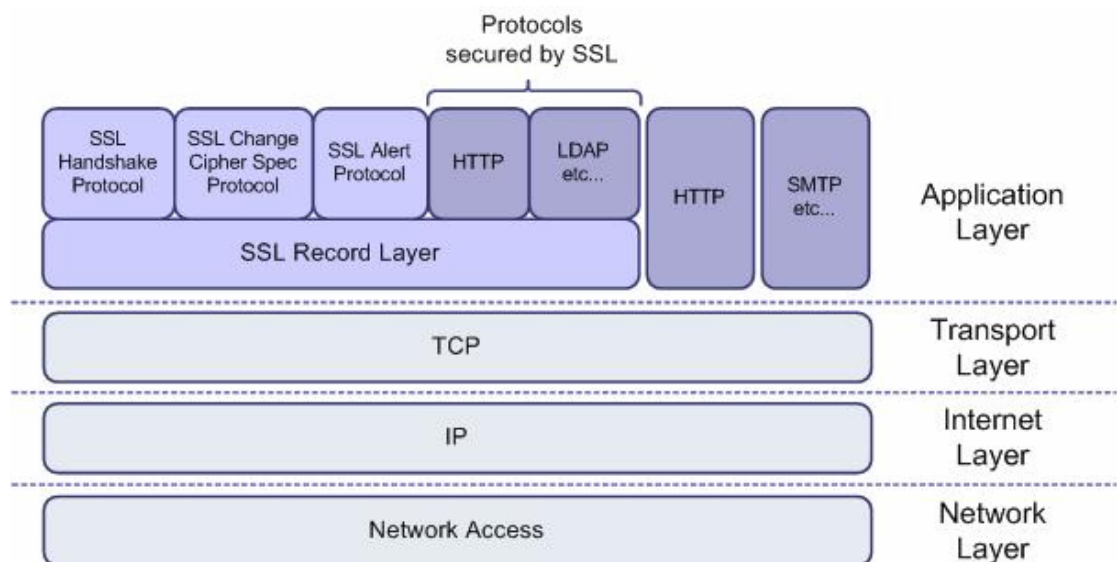


圖 1：SSL 協定架構圖

## 2 SSL 運作流程

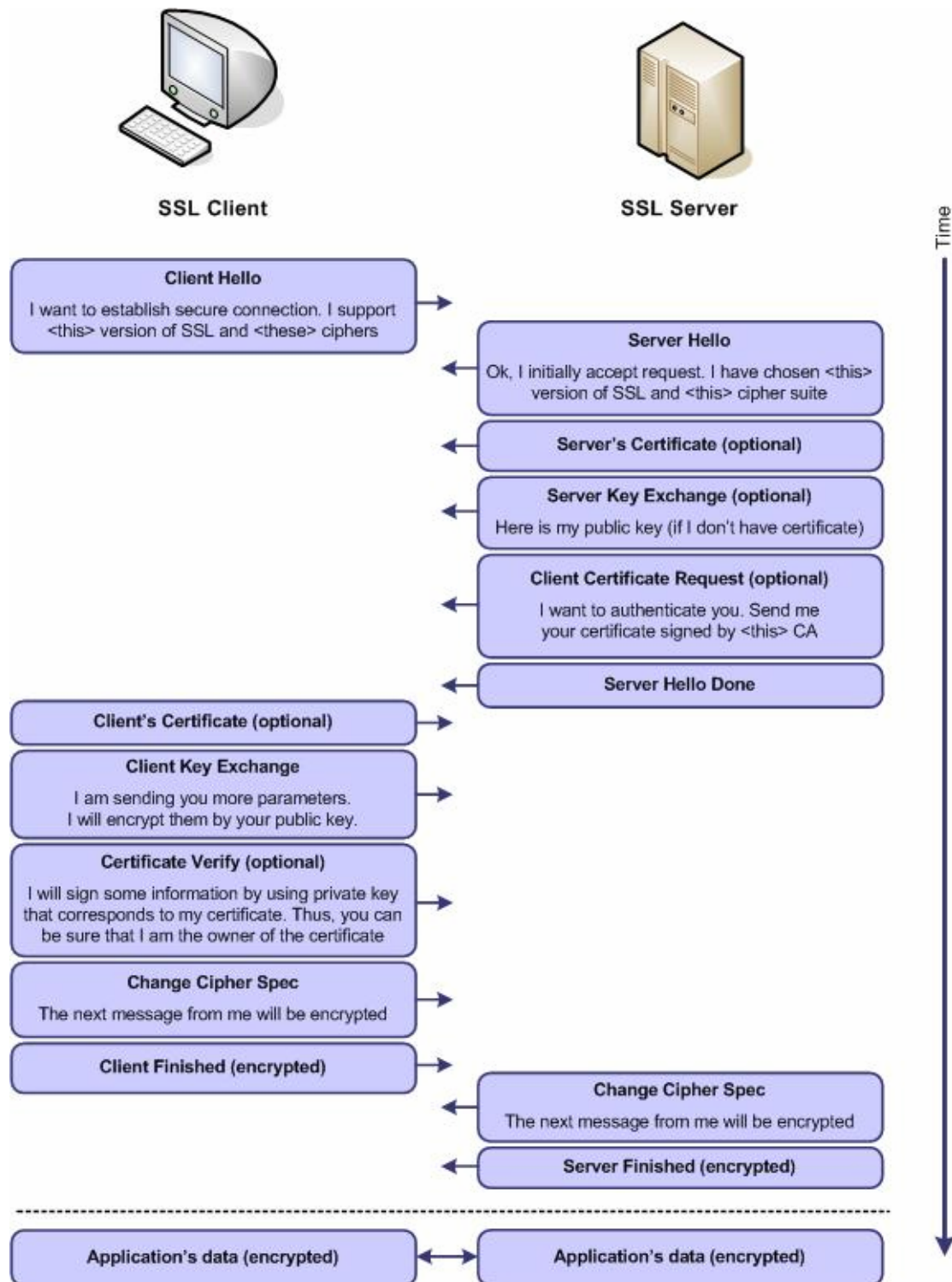


圖 2：SSL 運作流程

圖片來源：<http://www.securityfocus.com/infocus/1818>

- 用戶端傳送 ClientHello 訊息給伺服器端，此資訊包含 SSL 選項清單
- 伺服器端選擇要進行的 SSL 選項，並且利用 ServerHello 訊息將結果回應給用戶端
- 伺服器端利用 ServerKeyExchange 訊息來傳送公開金鑰資訊
- 伺服器利用 ServerHelloDone 訊息來結束部份的協商交談。
- 用戶端利用 ClientKeyExchange 訊息來傳送 session key 資訊，用戶端在傳送 session key 時會先用伺服器端所給的公開金鑰對 session key 進行加密後再進行傳送。
- 用戶端傳送 ChangeCipherSpec 訊息來啟動已達成協議的選項，這些選項跟用戶端將來所傳送的訊息有關。
- 用戶端傳送 Finished 訊息給伺服器端，告知伺服器端可以檢查這些最新啟動的選項。
- 伺服器端傳送 ChangeCipherSpec 訊息來啟動已達成協議的選項，這些選項跟伺服器端將來所傳送的訊息有關。
- 伺服器傳送 Finished 訊息給用戶端，告知用戶端可以檢查這些最新啟動的選項。

### 3 實戰演練：CentOS 4 上的 Apache 2 + SSL

如果要讓 Apache 伺服器和瀏覽器使用 SSL 來進行安全通信，伺服器必須有公開和私密金鑰配對及憑證。伺服器使用其私密金鑰來簽認給瀏覽器的訊息。伺服器會將公開金鑰傳送給瀏覽器，讓瀏覽器能夠確認這些簽章過的訊息是這個伺服器所發出，且瀏覽器可將要傳給伺服器的訊息加密。然後伺服器再使用其私密金鑰解密這些訊息。

如果要傳送公開金鑰給瀏覽器，伺服器需用到憑證管理中心 (CA) 所發的憑證。這個憑證含有伺服器的公開金鑰、伺服器憑證的相關識別名稱、憑證的發出日期或序號，以及憑證的有效期限。

「憑證管理中心」(CA) 是一個負責發出憑證且具公信力的第三方 (或指定的內部憑證中心)。CA 可驗證伺服器的身分，並使用其私密金鑰以數位方式簽認憑證；以及使用其公開金鑰來確定憑證的有效性。已簽章的憑證可讓伺服器身分與一對電子金鑰相連結，藉以加密與簽認數位資訊。憑證管理中心私密金鑰會簽署憑證來驗證伺服器身分。

所以，整個演練流程，大致如下：

- 安裝 mod\_ssl 套件
- 建立私密金鑰 (Private Key) 和憑證申請檔 (Certificate Signing Request)
- 將憑證申請檔 (Certificate Signing Request) 送給 CA 申請憑證
- 載入憑證管理中心所核發的憑證
- 測試網頁及限制只可使用 https 連線

#### 3.1 安裝 mod\_ssl 套件

預設 CentOS 4(由社群人士所開發 RHEL 4 免費相容版本; <http://www.centos.org>) 已安裝實作 https 所需 mod\_ssl 套件，可利用「rpm -qa | grep mod\_ssl」確定是否已安裝 mod\_ssl 套件。

```
[root@www html]# rpm -qa | grep mod_ssl
```

```
mod_ssl-2.0.52-9.ent.centos4.1
```

若是尚未安裝，可以以 root 的身份登入系統，開啟終端視窗，鍵入「system-config-packages」。利用 GUI 套件管理工具「system-config-packages」→「網頁伺服器」（圖 3），點選「詳細資訊」，然後勾選「mod\_ssl」，便會提示放入適當的光碟片，便可完成安裝工作。

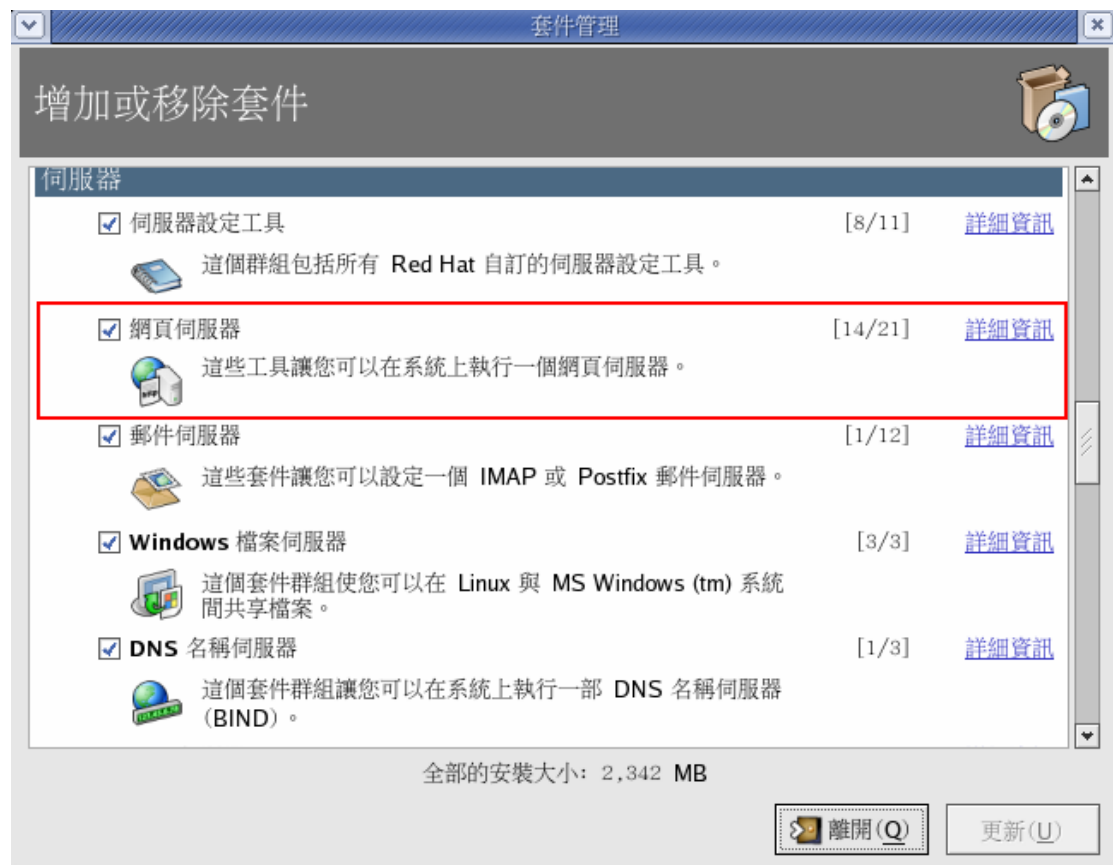


圖 3：增加或移除套件

待安裝 mod\_ssl 套件後，利用「service httpd restart」指令重新啟動 Apache 便可使用 SSL 通訊協定。例如原來是輸入「<http://www.blue-linux.com>」便可改為「<https://www.blue-linux.com>」。接著出現如圖 4 安全性警訊的視窗，是按下「是(Y)」就可利用 https 和此網站溝通。

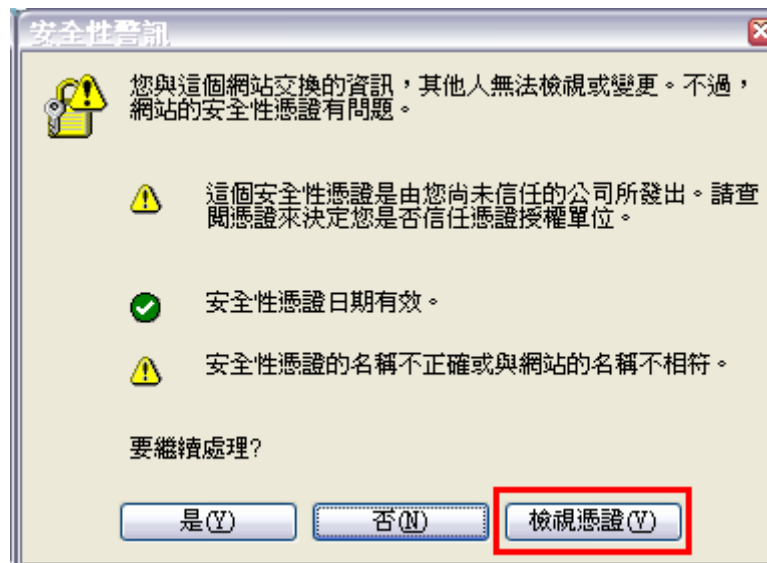


圖 4：https 安全性警訊的視窗

讀者這時候一定很納悶，我們還沒向憑證管理中心申請憑證，怎麼會有憑證呢？其實這張憑證是安裝 mod\_ssl 所產生出來的預設憑證，讀者只要點選圖 4 的「檢視憑證」便可看到憑證的詳細資訊（圖 5）。如果讀者願意使用這個預設的憑證來進行 https 連線，就無需再進行以下步驟，不過一般電子商務網站都會和 CA 憑證中心申請合法的憑證，所以筆者接著介紹完整的憑證申請流程。

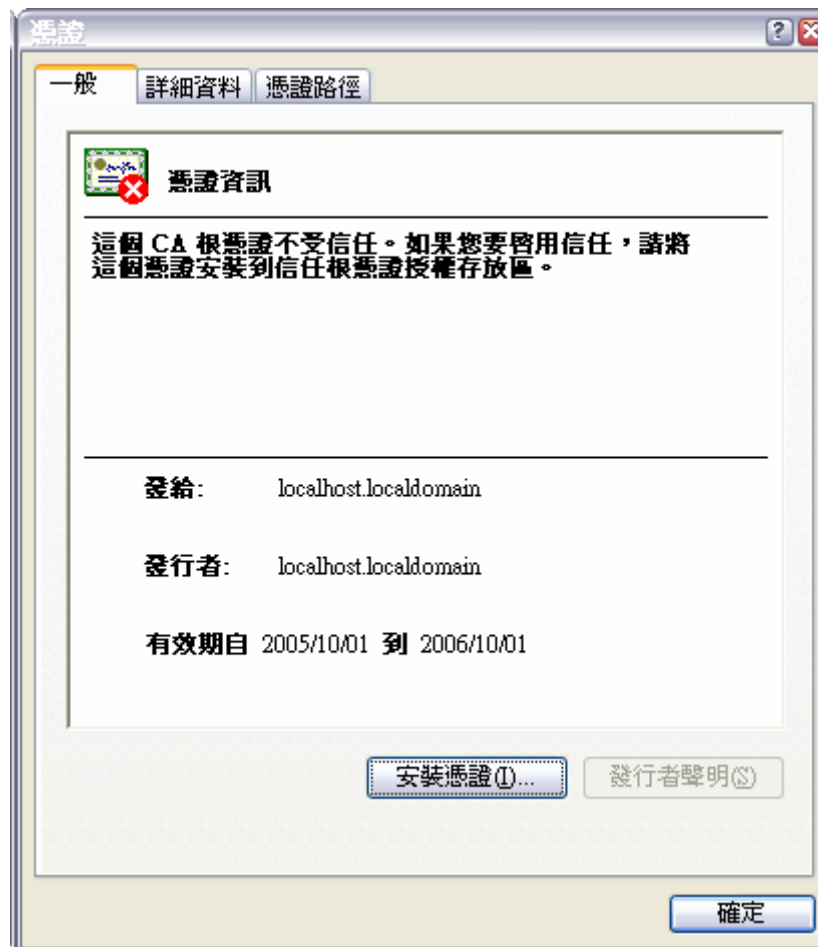


圖 5：預設憑證資訊

### 3.2 建立私密金鑰和憑證申請檔

步驟 1：將原有的私密金鑰（Private Key）和憑證申請檔（Certificate Signing Request）更名備份。

```
[root@www ~]# cd /etc/httpd/conf
[root@www /etc/httpd/conf]# mv ssl.key/server.key ssl.key/server.key.orig
[root@www /etc/httpd/conf]# mv ssl.crt/server.crt ssl.crt/server.crt.orig
```

步驟 2：產生私密金鑰（Private Key）

原有的私密金鑰（Private Key）是存放/etc/httpd/conf/ssl.key 目錄下，所以我們切換至此目錄下，利用「**openssl genrsa 1024 > server.key**」指令建立私密金鑰（Private Key）。



```
[root@www /etc/httpd/conf]# cd ssl.key/
[root@www /etc/httpd/conf/ssl.key]# openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
```

### 步驟 3：產生憑證申請檔 (Certificate Signing Request)

產生憑證申請檔 (Certificate Signing Request) 是為了要 CA 憑證中心申請合法憑證，讀者可以將憑證想成是現實社會中的營業執照。現實社會中若是你想開家公司則必須向政府申請營業執照，營業執照的最主要用處是用來證明你是合法的公司。其實憑證就是用來證明這台 Apache 伺服器是合法登記有案的網頁主機，而申請營業執照必須先向填寫申請表，內容包括公司資訊、負責人、連絡方式...等資訊，然後再送給向政府，等待審查通過，核發營業執照。申請憑證也是如此，必須先產生「憑證申請檔 CSR」（營業執照申請表），然後再送給「CA 憑證中心」（政府）等待審查通過，核發「憑證 CRT」（營業執照）。

切換到/etc/httpd/conf/ssl.csr/目錄（預設憑證申請檔 CSR 存放目錄），利用下列指令產生憑證申請檔：

```
# openssl req -new -key 私密金鑰 -out 憑證申請檔
```

```
#cd /etc/httpd/conf/ssl.csr/
```

```
# openssl req -new -key ../ssl.key/server.key -out server.csr
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
Country Name (2 letter code) [GB]:TW
```

```
State or Province Name (full name) [Berkshire]:Taiwan
```

```
Locality Name (eg, city) [Newbury]:Taipei
```

```
Organization Name (eg, company) [My Company Ltd]:blue-linux
```

Organizational Unit Name (eg, section) []:**Technical Support**

Common Name (eg, your name or your server's hostname)

[]:**www.blue-linux.com**

Email Address []:**alexlin@blue-linux.com**

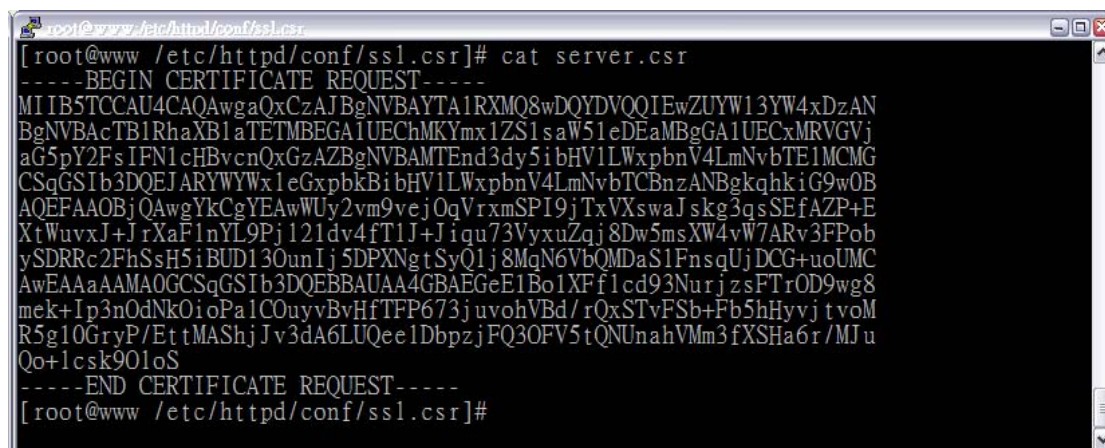
Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []: **←直接按下 Enter 鍵**

An optional company name []:**←直接按下 Enter 鍵**

檢查此目錄下應產生 server.csr 檔案，並利用 cat 指令查看內容，見圖 6。：



```
root@www /etc/httpd/conf/ssl.csr
[root@www /etc/httpd/conf/ssl.csr]# cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIB5TCCAUI4CAQAwgAQCzAJBgNVBAYTA1RlR08wDQYDVQQIEwZUW13YW4xDzAN
BgNVBAcTB1RhaXB1aTETMBEGA1UEChMKYmx1ZS1saW51eDEaMBGGA1UECxMRVGVj
aG5pY2FsIFN1c2F0b3VycnQzAZBgNVBAMTEnd3dy5ibHV1LWxpbmV4LmNvbTEuMCMG
CSqGSIb3DQEJARYWYWxleGxpbnkibHV1LWxpbmV4LmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwYkCgYEAwWUy2vm9vej0qVrxmSPI9jTxVXswaJskg3qsSEfAZP+E
XtWuvxJ+rXaFlnYL9Pj121dv4fT1J+Jiqu73VyXuZqj8Dw5msXW4vW7ARv3FPob
ySDRRc2FhSsH5iBUD13OunIj5DPXngtSyQ1j8MqN6VbQMDaS1FnsqUjDCG+uoUMC
AwEAAaAAMAOGCSqGSIb3DQEBBAAU4GBAEGeE1Bo1XFf1cd93NurjzsFTrOD9wg8
mek+Ip3nOdNkOioPa1COuyvBvHfTFP673juvohVBd/rQxSTvFSb+Fb5hHyvtvoM
R5g10GryP/EtMASHjJv3dA6LUQee1DbpzjFQ30FV5tQNUnahVMm3fXSHa6r/MJu
Qo+1cSk901oS
-----END CERTIFICATE REQUEST-----
[root@www /etc/httpd/conf/ssl.csr]#
```

圖 6：server.csr 檔案內容

### 3.3 申請憑證

一般需要付費才可向憑證中心申請憑證，不過「網際威信」有提供免費憑證測試服務，使用者確定購買時才需付費。所以筆者就跟「網際威信」申請試用的憑證。請連線到以下網址（圖7）：

[http://www.hitrust.com.tw/newsite/ssl\\_c3.asp](http://www.hitrust.com.tw/newsite/ssl_c3.asp)

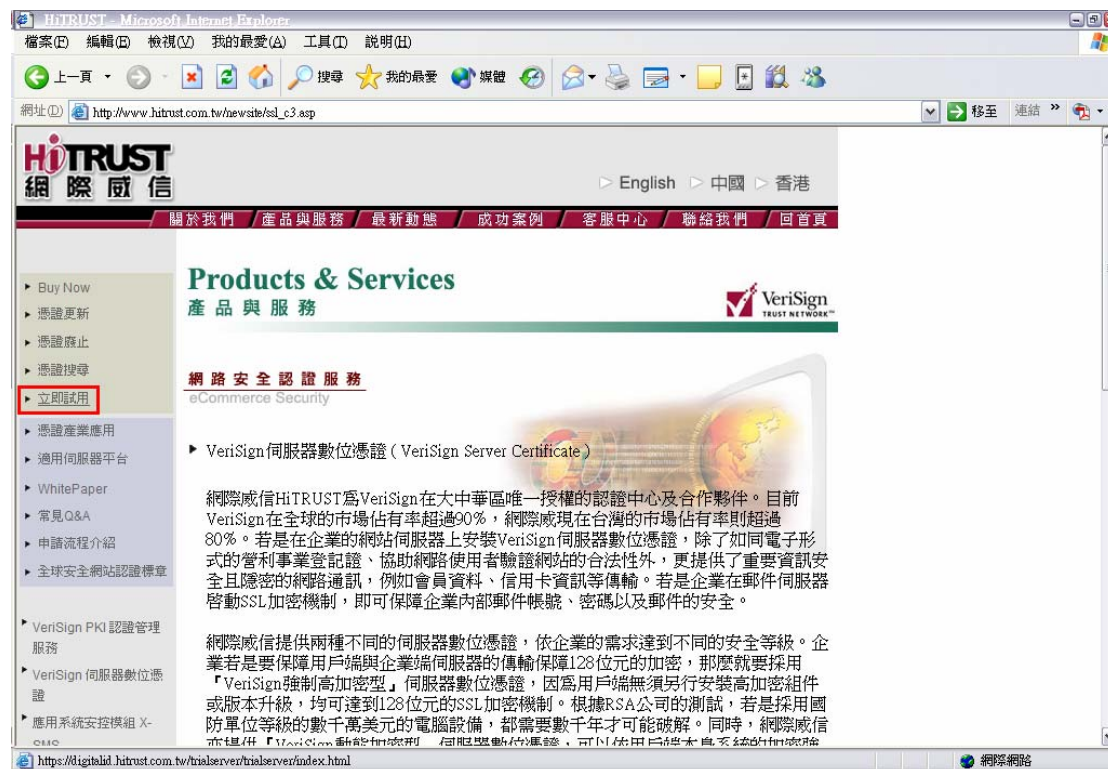


圖 7：網際威信「立即試用」網頁

請點選「立即試用」後，會出現「VeriSign 伺服器數位憑證測試版 (VeriSign Trial Server ID)」網頁，請點選「下一頁」（圖 8）。



圖 8：「VeriSign 伺服器數位憑證測試版 (VeriSign Trial Server ID)」網頁



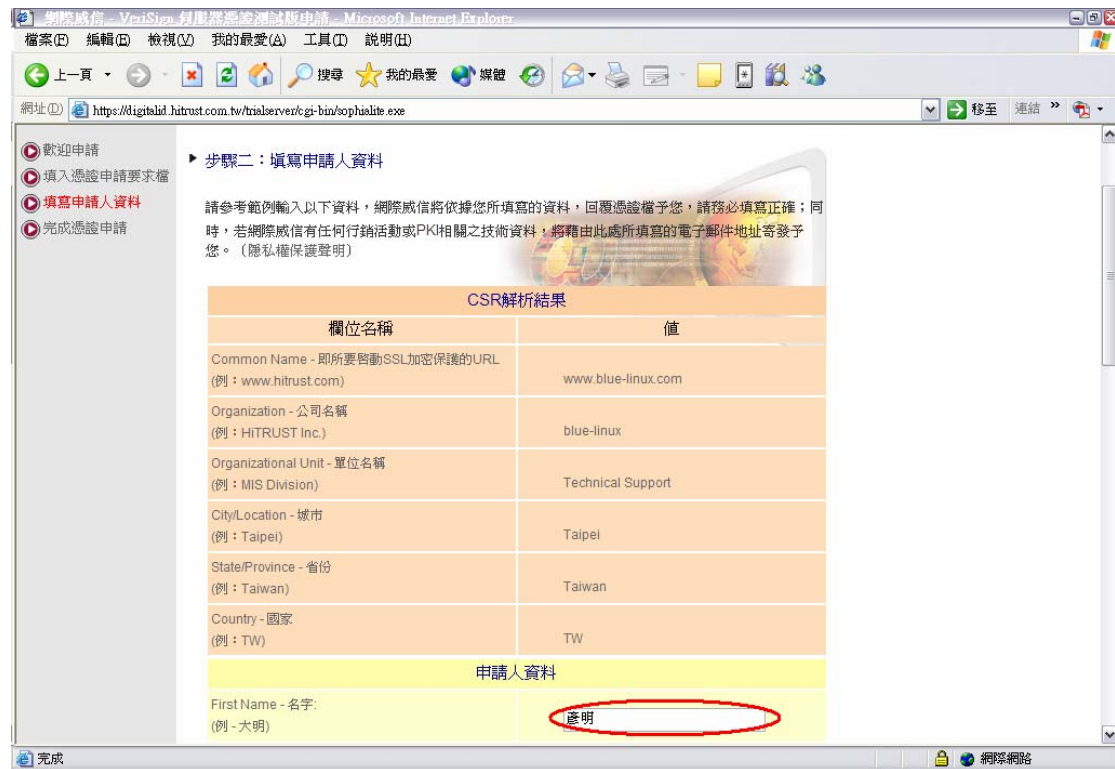


圖 10：填寫申請人資料畫面一

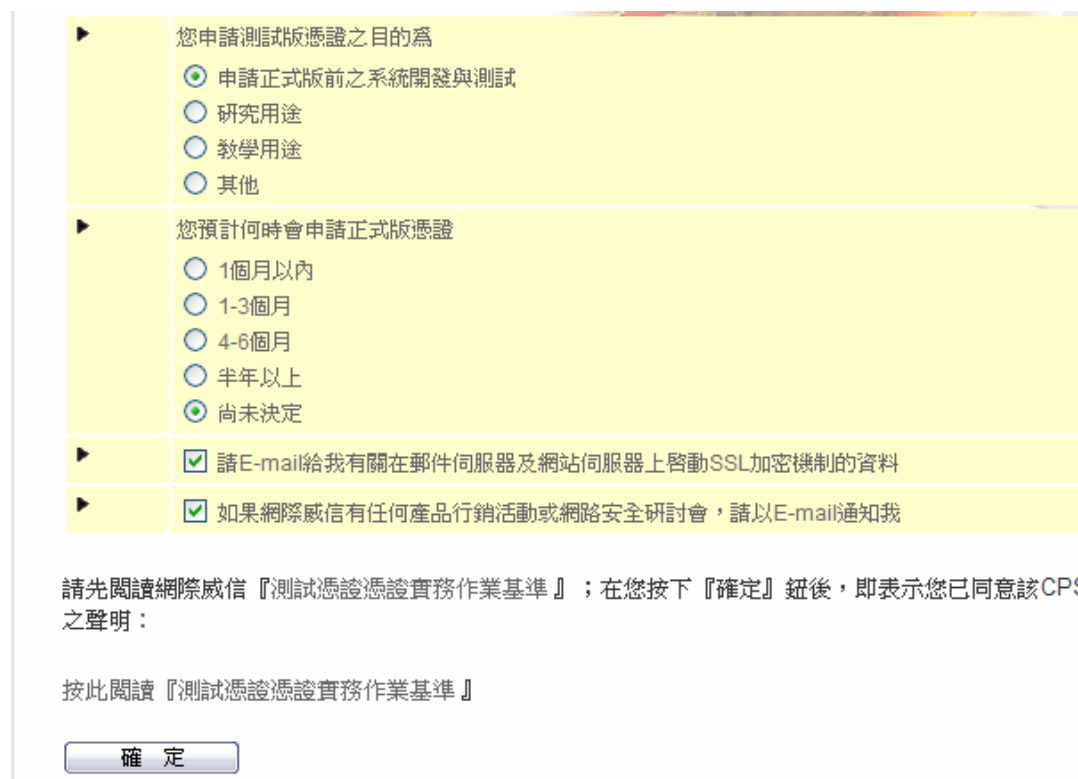


圖 11：填寫申請人資料畫面二



### 3.4 載入憑證

稍候檢查電子郵件地址，應會收到網際威信寄來的試用憑證（圖10），把郵件內文中的「BEGIN」到「END」內容複製並將此段文字另存檔為「/etc/httpd/conf/ssl.crt/server.crt」（圖11），然後重新啟動Apache伺服器。



圖 12：核發 VeriSign 伺服器數位憑證測試版郵件

```
[root@www ~]# vi /etc/httpd/conf/ssl.crt/server.crt
```

```

-----BEGIN CERTIFICATE-----
MIIDyzCCA3WgAwIBAgIQNoVYh9WZ56QH5i1TKTh2EjANBgkqhkiG9w0BAQUFADCB
qTEWMBQGA1UEChMNvVyaVNpZ24sIE1uYzFHMEUGA1UECXM+d3d3LnZ1cm1zaWdu
LmNvbS9yZXBvc210b3J5L1Rlc3RDUFMgSW5jb3JwLjBCEsBSZSWyUExpYWluIEExU
RC4xRjBEBGgNVBAsTPUZvcjBWXzJpU21nbjBhdXRob3JpemVkIHRlc3Rpbmcgb25s
eS4gTm8gYXNzdXJhbmNlcyAoQy1WUzE5OTcwHhcNMDUxMjI2MDAwMDAwWhcNM DYw
MTA5MjM1OTU5WjB9MQswCQYDVQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMQ8wDQYD
VQQHFAZUYW1wZWkxZzARBGgNVBAoUCmJsYWUtdG1udXgxGjAYBgNVBAsUEVR1Y2hu
aWNhbCBTdXBwb3JOMRswGQYDVQQDFBJ3d3cuYmx1ZS1saW51eC5jb20wgZ8wDQYJ
KoZThvcNAQEVBQADgY0AMIGJAoGBAMF1Mtr5vb3ozqla8ZkjyPY08VV7MGibJIN6
rEhHwGT/hF7Vrr8Sfia12hZZ2C/T45dtXb+H05SfiYqru91csbmao/A80ZrF1uL1
uwEb9xT6G8kg0UXNhYUrB+YgVA9dzrpyI+Qz1zYLUskJY/DKje1W0DA2kpRZ7K1I
wwhvrqFDAgMBAAGjggFeMIBWjAJBgNVHRMEAjAAMAsGA1UdDwQEAwIFoDA8BgNV
HR8ENTAzMDGgL6AthitodHRwOi8vY3J5L1Rlc3RDUFMgSW5jb3JwLjBCEsBSZSWyU
ExpYWluIEExUzXJ2ZXIuY3J5SjMIGsBgNVHSAEgaQwgaEwgZ4GC2CGSAGG+EUBBwEBMIGOMCgGCCsG
AQUFBwIBFhxodHRwczovL3d3dy52ZXJpc21nbj5jb20vQ1BTMGIGCCsGAQUFBwIC
MFYwFRYOVmVyaVNpZ24sIE1uYy4wAwIBARo9VmVyaVNpZ24ncyBDUFMgaW5jb3Jw
LjBi eSBYZWZ1cmVUy2UgbG1hYi4gbHRkLiAoYyk5NyBWXzJpU21nbjAdBgNVHSUE
FjAUBgg rBgEFBQCDAQYIKwYBBQUHAwIwNAYIKwYBBQUHAQEEDAmMCOGCCsGAQUF
BzABhhhodHRwOi8vb2NzcC52ZXJpc21nbj5jb20wDQYJKoZThvcNAQEFBQADQQA4
G19FiEkFFVrqpZSoAi17KcSehAPeRGyVPan2Q+7NdzHq6A r tYab0C1Ucggadc3ed
7uHHZ/sH7NY0eTGkHFxc
-----END CERTIFICATE-----
-- 插入 --

```

圖 13：建立/etc/httpd/conf/ssl.crt/server.crt 檔案

```
[root@www ~]# service httpd restart
```

```
停止 httpd: [ 確定 ]
```

```
啟動 httpd: [ 確定 ]
```

### 3.5 測試網頁及限制某目錄只可使用 https 連線

此時，再利用「<https://www.blue-linux.com>」測試，跳出安全性警告視窗時，點選「檢視憑證」，出現如圖14畫面便可看到這張憑證是由「網際威信」所核發給「www.blue-linux.com」主機。

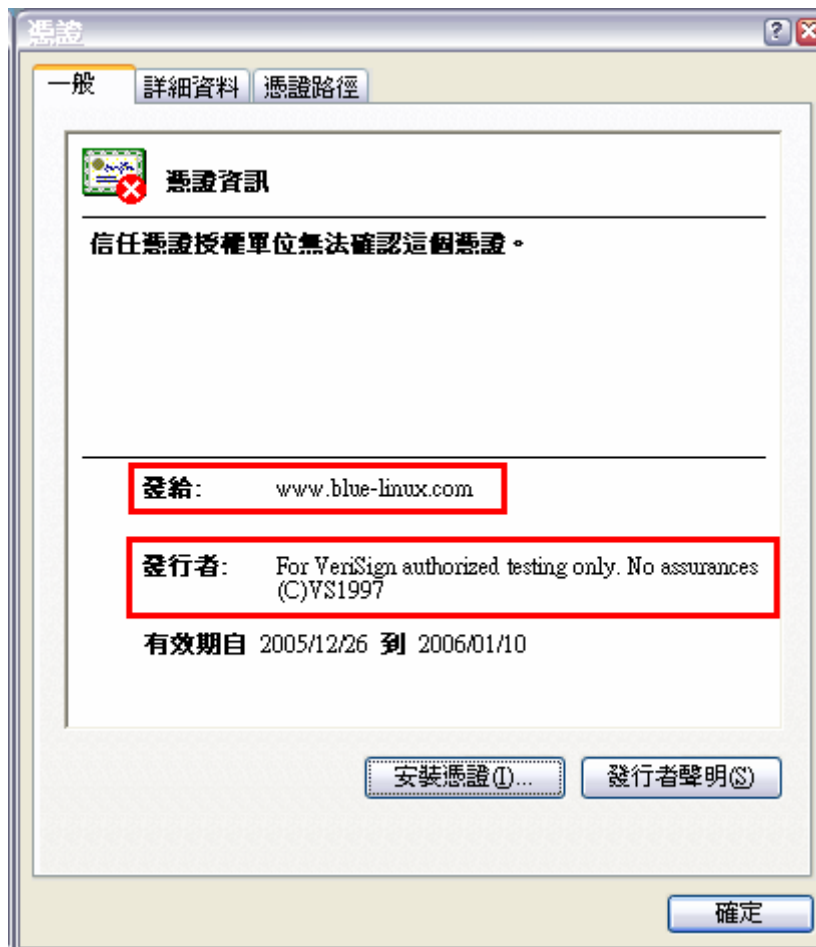


圖 14：「網際威信」核發給「www.blue-linux.com」的憑證

若按下「是」繼續處理，則會用https連線方式顯示網頁（圖15），若是讀者想限制某個目錄只可利用https方式連線，可利用SSLRequiredSSL參數，例如在<Directory /var/www/html> .....</Directory>區段中加入SSLRequiredSSL，然後重新啟動Apache伺服器。

```
[root@www ~]# vi /etc/httpd/conf/httpd.conf
```

```
290 <Directory "/var/www/html"> ←預設的DocumentRoot
```

```
.... SSLRequireSSL
```

```
319 </Directory>
```



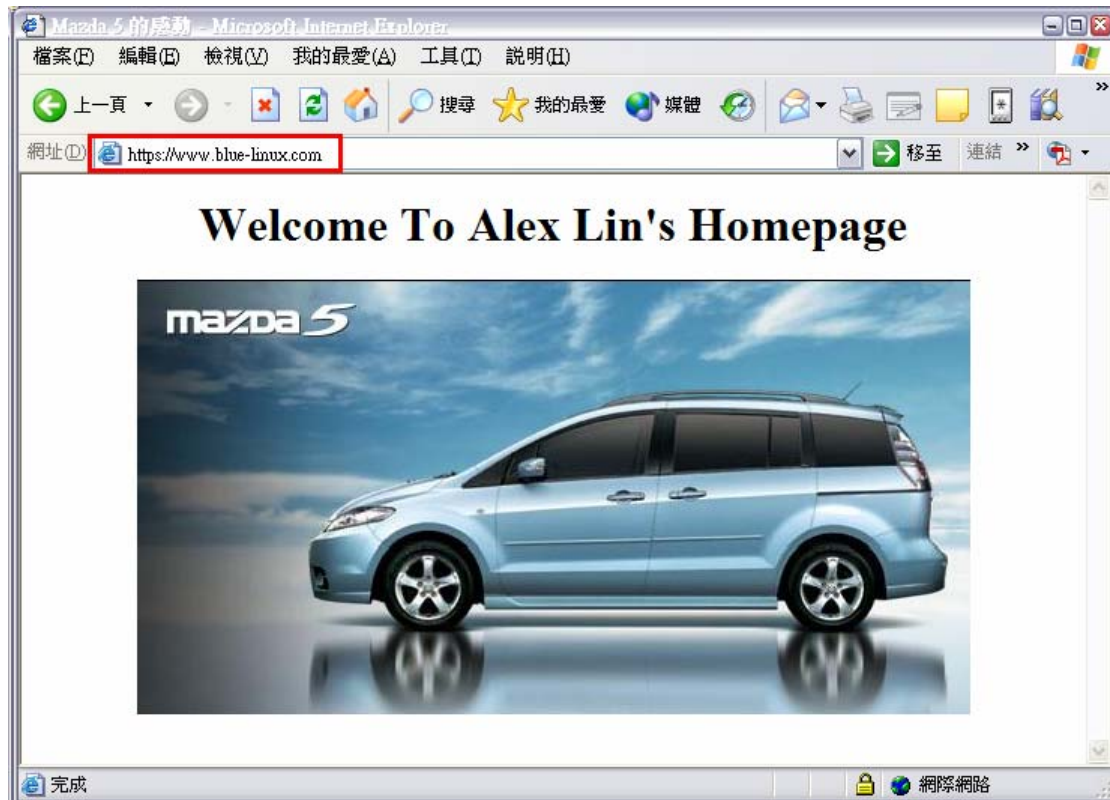


圖 15 : https 測試網頁