# 使用 OpenSSL 簽證中心為 IIS 做伺服器簽證

當您使用 Apache 要做 SSL 憑證時，可以完全使用 OpenSSL 去做完整的設定，這個設定我在 更安全的的連線 Apache + SSL (new window) 有討論其實做，在此就不再贅言，但如果要讓 IIS 也做到有 SSL 的連線，就需要做一點工夫了。

要讓 IIS 做 CA 憑證不難，但是要為該憑證做簽證到是有點麻煩，你可以使用 MS 的憑證中心來做這件事情，但如果你的單位已經有 Linux Based 憑證中心，那麼也可以直接使用。

## 建立專有憑證中心的私有金鑰

你很有可能已經有簽證中心，也有了該簽證中心的簽證檔，如果真的是如此的話，就可以跳過此一步驟，否則請依下所示來建立一個憑證中心的私有金鑰。請注意，你也可以使用 更安全的的連線 Apache + SSL (new window) 中已經生產出金鑰。

```
root # openssl genrsa -des3 -out ca.l-penguin.idv.tw.key 1024
Generating RSA private key, 1024 bit long modulus
.........................................++++++
.............++++++
e is 65537 (0x10001)
Enter pass phrase for ca.l-penguin.idv.tw.key: your_password
Verifying - Enter pass phrase for ca.l-penguin.idv.tw.key: your_password
root # ls
ca.l-penguin.idv.tw.key
root #
```

保護私鑰

做好憑證之後，理應只有 root 或有權限的人可以讀取這個憑證。

```
root # chmod 400 ca.l-penguin.idv.tw.key
```

## 建立憑證中心的簽證檔

請使用剛剛生產的私有金鑰做一個簽證檔。

```
root # openssl req -new -key ca.l-penguin.idv.tw.key -x509 -days 1095 -out ca.l-penguin.idv.tw.crt
Enter pass phrase for ca.l-penguin.idv.tw.key: your_passowrd
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]:Taipei
Locality Name (eg, city) [Newbury]:Taipei
Organization Name (eg, company) [My Company Ltd]:l-penguin Corp.
Organizational Unit Name (eg, section) []:CA
Common Name (eg, your name or your server's hostname) []:ca.l-penguin.idv.tw
Email Address []:steven@l-penguin.idv.tw
```

相同的道理，我們也需要保護這個簽證。

```
root # chmod 400 ca.l-penguin.idv.tw.crt
```

現在我要為 IIS 服務 web.l-penguin.idv.tw 設定一個 SSL 連線。在 IIS 網站內容裡，選擇目錄安全設定頁籤，點選伺服器憑證。請依下順序建立一個 web.l-penguin.idv.tw 的私有金鑰。

- 建立新憑證。
- 準備要求，但稍候傳送。
- 在稱輸入 web.l-penguin.idv.tw。
- 輸入該服務的單位地理資訊。
- 在公用名稱輸入 web.l-penguin.idv.tw（這個非常重要，需與 DNS 配合）。
- 設定私有金鑰的輸出位置及檔名，本例為 web.l-penguin.idv.tw.csr。

設定私鑰之後，請把它上傳到你的認證主機。

接下來使用 ca.l-penguin.idv.tw 去做 web.l-penguin.idv.tw 的簽證。

```
root # openssl x509 -req -days 365 -in web.l-penguin.idv.tw.csr -CA ca.l-
penguin.idv.tw.crt -CAkey ca.l-penguin.idv.tw.key -CAcreateserial -out web.l-
penguin.idv.tw.crt
Signature ok
subject=/CN=web.l-penguin.idv.tw/OU=Web/O=l-penguin
Corp./L=Taipei/ST=Taiwan/C=TW
Getting CA Private Key
Enter pass phrase for ca.l-penguin.idv.tw.key:your_password
root #
```

當你做好簽證之後，請把它保存好。接下來要讓 IIS 使用這個簽證。

- 處理擱置要求及安裝憑證。
- 選擇已簽證過的 crt。
- 確認你的憑證資訊。

現在就可以讓 IIS 以 https 的 SSL 通道做資料傳送。

*For more articles, please visit http://www.l-penguin.idv.tw/*

作者：廖子儀 (Tzu-Yi Liao)

Certified：LPIC Level I、LPIC Level II、RHCE

E-mail：steven@ms.ntcb.edu.tw

Web site：Steven's Linux Note (http://www.l-penguin.idv.tw/)