建立一個可信任的單位根簽證 (Root CA)

小弟在 更安全的的連線 Apache + SSL (new window) 及 使用 OpenSSL 簽證中心為 IIS 做伺服器簽證 (new window) 的文章中，有說明了如何使用 OpenSSL 來為憑證做簽證，你可以使用自己的 CA 做憑證。但是這種情況一遇到大量的的憑證簽章，就會變得無從管理，且自行簽證的憑證也有可能會有假冒的問題。

在這篇文章裡，我會說明如何使用 OpenSSL 建立一個憑證中心的專用憑證，並且匯入到 Windows Client 中，之後若有需要使用到 SSL 簽證的情況之下，只要由憑證中心做簽證，其它的 Windows Client 就會自動信任而不需要次的新增憑證。

建立憑證之前

- 確認憑證中心的主機名稱

  憑證中心的主機名稱非常重要，這有關係著 Client 在做查尋時的主機比對，若是不對不符那麼就無法受到信認。

- 憑證主機的時間

  由於憑證是有時效性的，所以在做憑證簽核時，時間是非常重要的，你可以參考 讓系統更準時 - 使用 NTP 效對時間 (new window) 這篇文章來做時間的調校。 你可使用下列方式得到目前主機時間，查看時間是否正確。

```
root # date
Tue Feb 20 22:26:52 CST 2007
root #
```

- DNS 對應

  當然憑證中心的主機名稱一旦確認，那麼 DNS 就必需有合適的對應才行，否則會找不到主機。你可使用下列方式查看 DNS 是否正確。

```
root # host ca.l-penguin.idv.tw
ca.l-penguin.idv.tw has address 192.168.1.82
root #
```

建立 Root CA

建立一個 Root CA，因為這個 Root CA 是所有憑證的基礎，所以我們需要在建立一個有密碼保護的私有金鑰。

```
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 #
```

使用 Root CA 的私有金鑰做出一個 X.509 的憑證。

```
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_password
```

```
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 County
Organization Name (eg, company) [My Company Ltd]:l-penguin Corp.
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:ca.l-penguin.idv.tw
Email Address []:steven@l-penguin.idv.tw
root #
```

保護金鑰

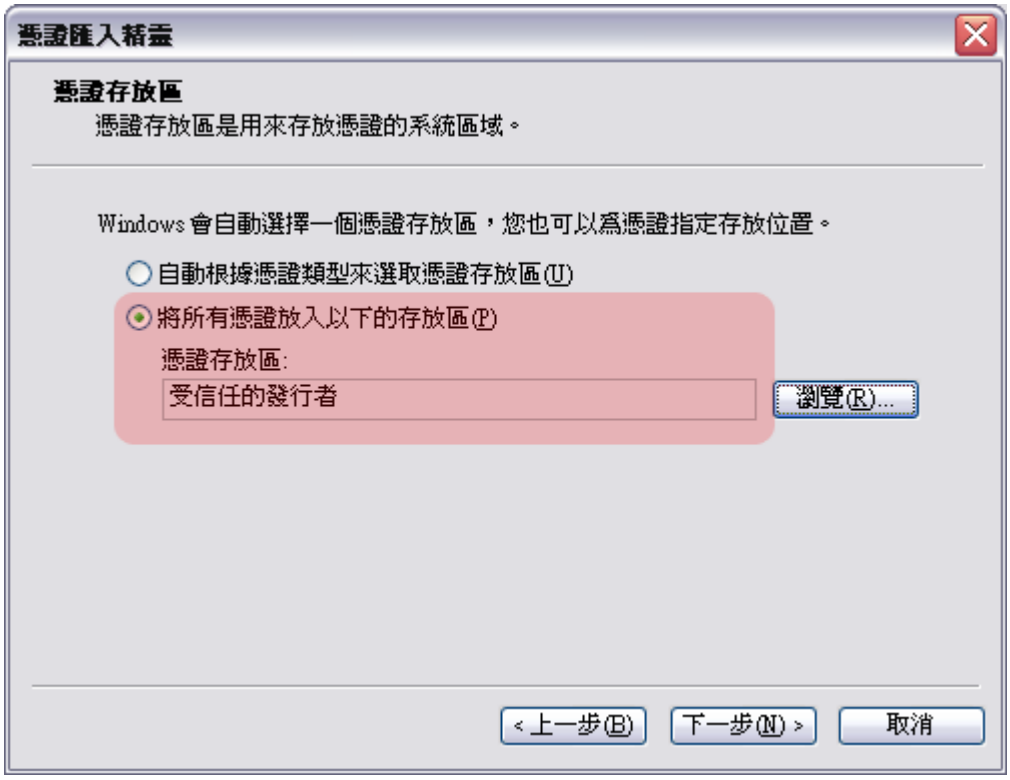
金鑰是 SSL 加密中非常中要的一個資訊演算重點，你應該要保管好這個金鑰並且不要讓他外流，只有相關的使用者可以讀取。

```
root # chmod 600 ca.l-penguin.idv.tw.key
root #
```

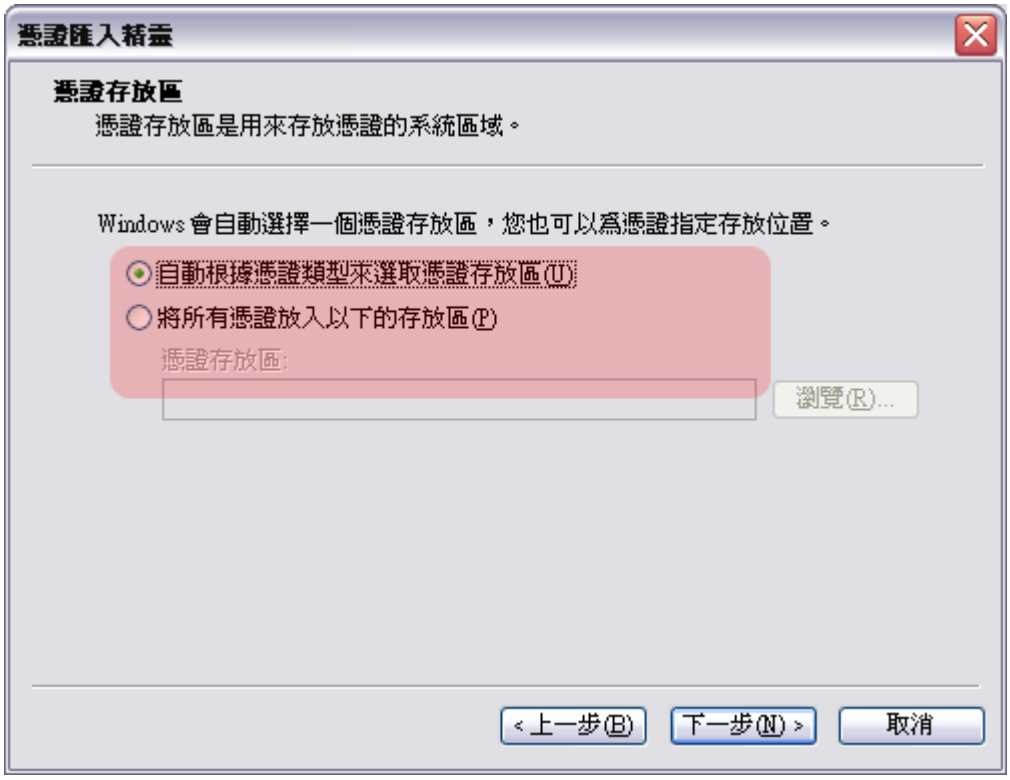
在 Windows 匯入 Root CA

一旦產生出了根信認簽證後，你可以使用 Windows 把這個憑證加入到 Windows 的“受信認的發行者”項目裡，信任任何由 ca.l-penguin.idv.tw 所簽核的憑證。

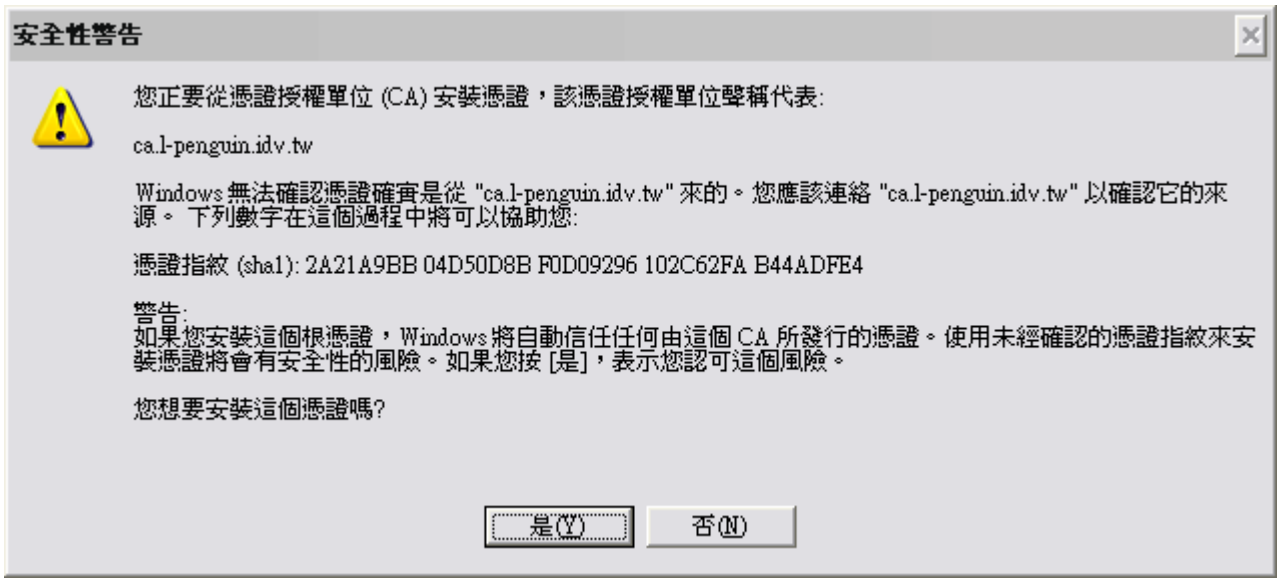
把 ca.l-penguin.idv.tw 匯入到“受信認的發行者”。



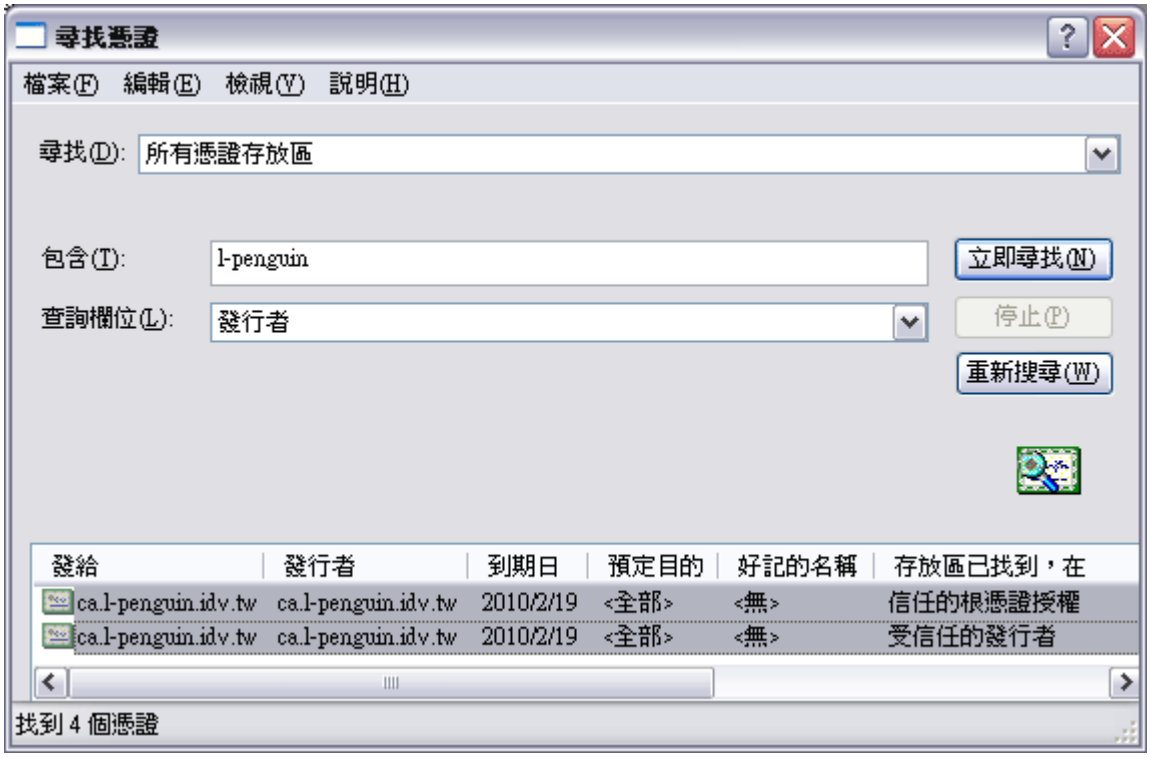
接受 ca.l-penguin.idv.tw.crt 的憑證。



若出現安全性警告的話，請按“是”。

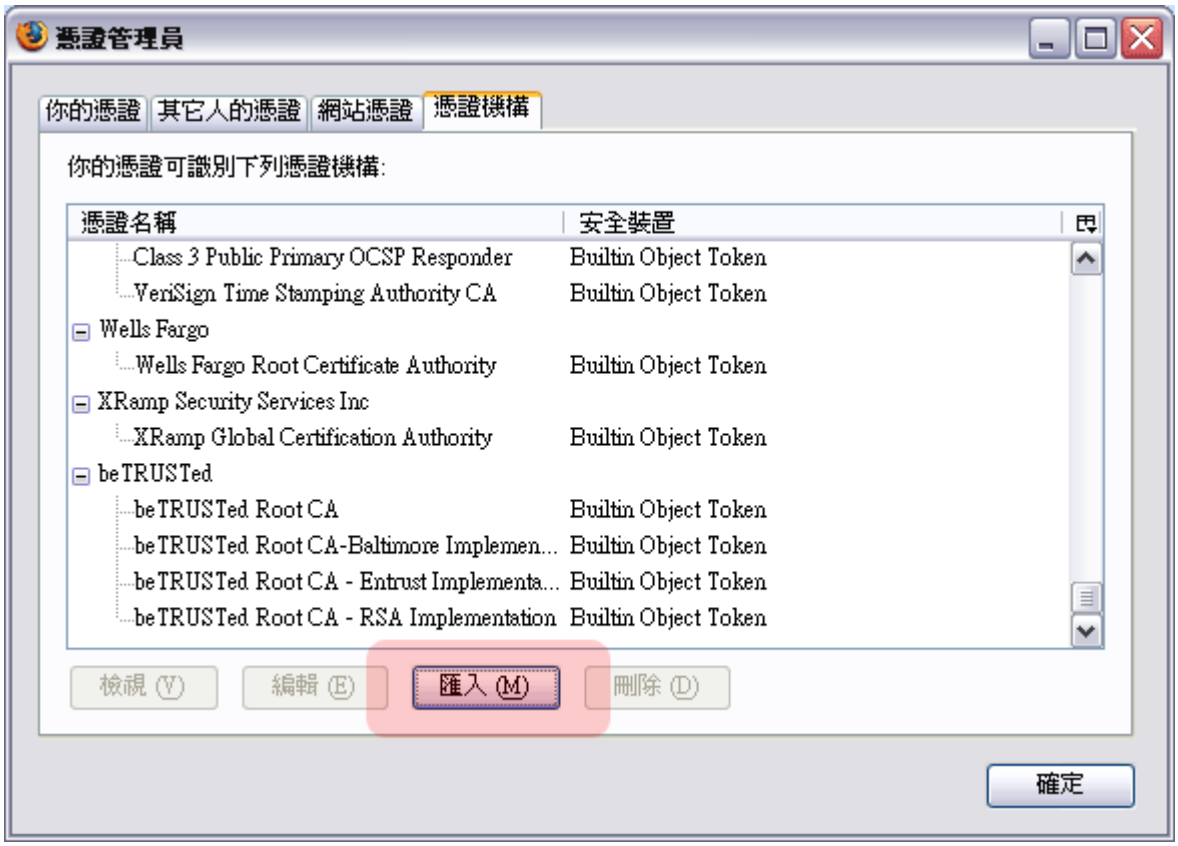


簽查是否已匯入憑證。



將 Root CA 匯入 Firefox

在 Firefox 設定選項中，點選“進階 > 檢視憑證清單”，再選擇憑證所在。



將 Root CA 匯入 Thunderbird

在 Thunderbird 選項中，點選進階，選擇管理憑證。

匯入所信任的憑證檔案。

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/)