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 <u>讓</u> <u>系統更準時-使用 NTP 效對時間</u> (<u>new window</u>) 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。

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.lpenguin.idv.tw.crt Enter pass phrase for ca.l-penguin.idv.tw.key:your password

第1頁/共5頁

2007/02/21

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]:**1-penguin Corp**. Organizational Unit Name (eg, section) []:**IT** Common Name (eg, your name or your server's hostname) []:**ca.1-penguin.idv.tw** Email Address []:**steven@1-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"。

憲證匯入精畫
憲證存放區 憑證存放區是用來存放憑證的系統區域。
₩indows 會自動選擇一個憑證存放區,您也可以為憑證指定存放位置。 ○ 自動根據憑證類型來選取憑證存放區(II)
 ●將所有憑證放入以下的存放區(P) 憑證存放區:
受信任的發行者 瀏覽 (R)
<上一步(B) 下一步(M) > 取消

接受 ca.l-penguin.idv.tw.crt 的憑證。

2007/02/21

憲證匯入精畫 🛛 🔀					
憲證存放區 憑證存放區是用來存放憑證的系統區域。					
Windows 會自動選擇一個憑證存放區,您也可以爲憑證指定存	放位置。				
 ● 自動根據憑證類型來選取憑證存放區(U) ○ 將所有憑證放入以下的存放區(P) 					
源證存放區:	VALUE TO A				
	∋(N)> ■取消				

若出現安全性警告的話,請按"是"。

安全性警	<u>*</u>
	您正要從憑證授權單位 (CA) 安裝憑證,該憑證授權單位聲稱代表:
<u> </u>	ca.l-penguin.idv.tw
	Windows 無法確認憑證確實是從 "ca.l-penguin.idv.tw" 來的。 您應該連絡 "ca.l-penguin.idv.tw" 以確認它的來 源。 下列數字在這個過程中將可以協助您:
	憑證指紋 (sha1): 2A21A9BB 04D50D8B F0D09296 102C62FA B44ADFE4
	警告: 如果您安裝這個根憑證,Windows將自動信任任何由這個 CA 所發行的憑證。使用未經確認的憑證指紋來安 裝憑證將會有安全性的風險。如果您按 [是],表示您認可這個風險。
	您想要安裝這個憑證嗎?

簽查是否已匯入憑證。

2007/02/21

🔲 尋找憑證					? 🔀		
檔案(F) 編輯(E) 檢視(V) 說明(H)							
尋找①: 所有憑證存放區							
包含(I): l-pen	ıguin				立即尋找(N)		
查詢欄位(止): 發行	者				● 停止 @		
					重新搜尋(₩)		
發給	發行者	到期日	預定目的	好記的名稱	存放區已找到,在		
🔛 ca.l-penguin.idv.tw	ca.l-penguin.idv.tw	2010/2/19	<全部>	<撫>	信任的根憑證授權		
🔛 ca.l-penguin.idv.tw	ca.l-penguin.idv.tw	2010/2/19	<全部>	<撫>	受信任的發行者		
<	1111					>	
找到4個憑證							

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。

馬證管理員		
的憑證 其它人的憑證 網站憑證 憑證機構		
你的憑證可識別下列憑證機構:		
憑證名稱	安全裝置	
-Class 3 Public Primary OCSP Responder	Builtin Object Token	~
WeriSign Time Stamping Authority CA	Builtin Object Token	
🖃 Wells Fargo		
-Wells Fargo Root Certificate Authority	Builtin Object Token	
🖃 XRamp Security Services Inc		
-XRamp Global Certification Authority	Builtin Object Token	
🖃 beTRUSTed		
beTRUSTed RootCA	Builtin Object Token	
-beTRUSTed Root CA-Baltimore Implemen	Builtin Object Token	
beTRUSTed Root CA - Entrust Implementa	Builtin Object Token	
beTRUSTed Root CA - RSA Implementation	n Builtin Object Token	~
続親 (𝒴) 匯入 (M)		
		確定

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。

③ 憲證管理員		_ 🗆 🔼
你的憑證 其它人的憑證 網站憑證 認證中心		
你的憑證可識別下列認證中心:		
憑證名稱	安全裝置	E.
-Class 3 Public Primary OCSP Responder	Builtin Object Token	~
VeriSign Time Stamping Authority CA	Builtin Object Token	
🖻 be TRUS Ted		
beTRUSTed Root CAs	Builtin Object Token	
beTRUSTed Root CA-Baltimore Implementation	. Builtin Object Token	
be TRUSTed Root CA - Entrust Implementation	Builtin Object Token	
be TRUSTed Root CA - RSA Implementation	Builtin Object Token	
🖃 l-penguin Corp.		
ⁱ ca.l-penguin.idv.tw	Software Security Device	
検視 編輯 匯入	刪除	
		確定

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

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/)