109550206 陳品劭 Mini report

a. Definition and creation of a certificate for digital signature.

1. Definition

一個用於證明 public key 擁有者的檔案，此檔案包含了公鑰資訊、擁有者身分資訊（主體）、以及數位憑證認證機構 (CA)（簽發者）對這份檔案的數位簽章，以保證這個檔案的整體內容正確無誤。

2. Creation

數位憑證一般由數位憑證認證機構(CA)簽發，簡單的程序如下：

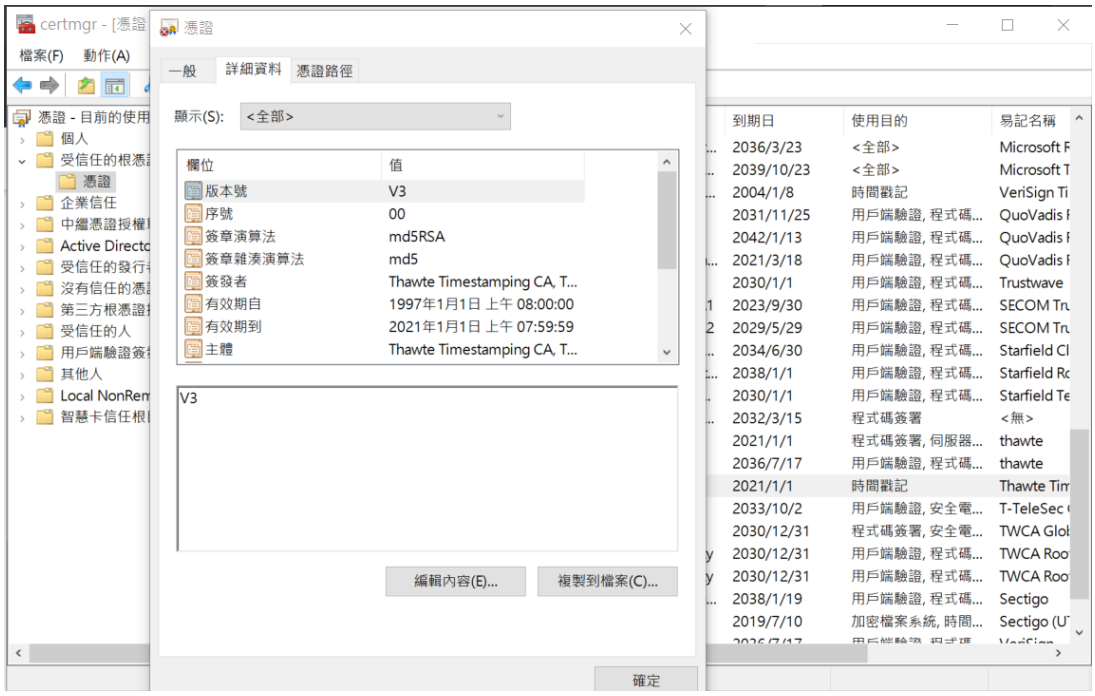
申領

I. User 在自己的機器上產生一對足夠強的密鑰，且 User 的私鑰不會向任何人傳送。
II. User 把他的公鑰，連同主體訊息、使用目的等組成憑證簽署請求，傳送給認證機構 CA。
III. CA（用另外一些管道）核實 User 的身分。
IV. 如果 CA 信任這個請求，他便使用 User 的公鑰和主體訊息，加上憑證有效期、用途等限制條件，組成憑證的基本資料。
V. CA 用自己的私鑰對 User 的公鑰加上數位簽章並生成憑證。
VI. CA 把生成的憑證傳送給 User（CA 也可以透過憑證透明度公佈他簽發了新的憑證）。

使用

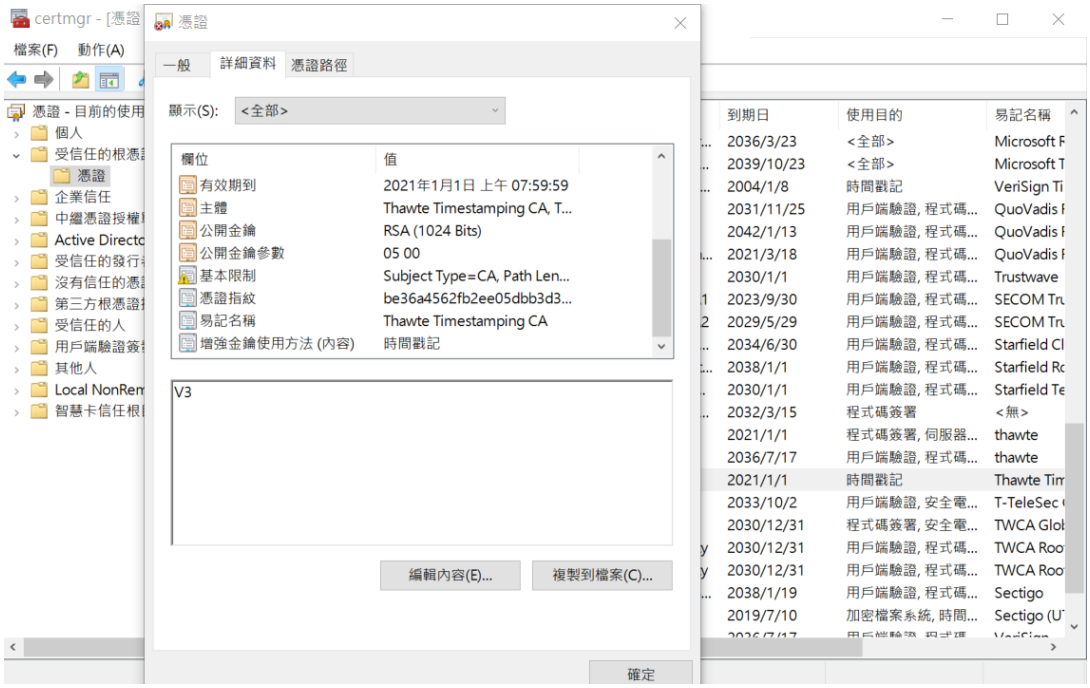
I. User 可以隨便把憑證向外發佈。
II. User 與 Others 事先可能互不認識，但 User 與 Others 都信任 CA，Others 使用 CA 的公鑰驗證數位簽章，如果驗證成功，便可以信任 User 的公鑰是真正屬於 User 的。
III. Others 可以使用憑證上的 User 的公鑰加密明文，得到密文並傳送給 User。
IV. User 可以可以用自己的私鑰把密文解密，得到明文。

b. Find a real certificate of digital signature and explain the fields of the certificate.



1. 版本號：此憑證對應的X.509標準版本號碼。
2. 序號：顯示已安裝憑證的序號，用以辨識每一張憑證，特別在復原憑證的時候有用。
3. 簽章演算法：此憑證使用的簽章演算法。
4. 簽章雜湊演算法：此憑證使用的簽章雜湊演算法。
5. 簽發者：此憑證之簽屬者。

   一般單位(common name ,CN) 、組織單位名稱(organizational Unit name, OU)、組織(organization name ,O) 、地方名稱(locality name ,L) 、州(State or province name, S)、國家(country name ,C)
6. 有效期自：此憑證自何時起有效。
7. 有效期到：此憑證到何時仍有效。



8. 主體：此憑證簽發給誰。

   一般單位(common name ,CN) 、組織單位名稱(organizational Unit name, OU)、組織(organization name ,O) 、地方名稱(locality name ,L) 、州(State or province name, S)、國家(country name ,C)

9. 公開金鑰：此憑證之公開金鑰。

10. 公開金鑰參數：此憑證之公開金鑰之參數。

11. 基本限制：此憑證之限制

12. 憑證指紋：此憑證的指紋碼(Hash值)。

13. 易記名稱：此憑證之較具識別度之名稱

14. 增強金鑰使用方法：Enhanced Key Usage, can be either critical or non-critical.

c. Find an application for certificates and explain how certificates are used for security functions in the application.

HTTPS

主要作用是在不安全的網路上建立一個安全通道，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。

該網頁伺服器需建立一個數位憑證，並交由憑證頒發機構簽章。通常瀏覽器都預裝了憑證頒發機構的憑證，因此可以驗證網站的簽章，便可保證瀏覽其網站的安全。