Mini Report

a. Definition and creation of a certificate for digital signature

Definition:

電子憑證是由 CA(certificate authority)產生，需透過 CSR 文件向 CA 申請憑證，CA 須由具有公信力的第三方擔任(Trusted third party ,TTP)，要同時被傳送者和接收者所信任，每個 user 可以在不同的 CA 底下拿到憑證。憑證用於驗證身分，內容包含所需的驗證資料，以 X.509 為例，X.509 採用 ANS.1 標準，驗證資料包含:版本、序號、憑證簽署演算法 ID、簽發者、有效期限、擁有者、擁有者公鑰資訊、公鑰演算法、公鑰、簽發者唯一識別、擁有者唯一識別、擴充、憑證簽署演算法、憑證簽章值。

Creation:

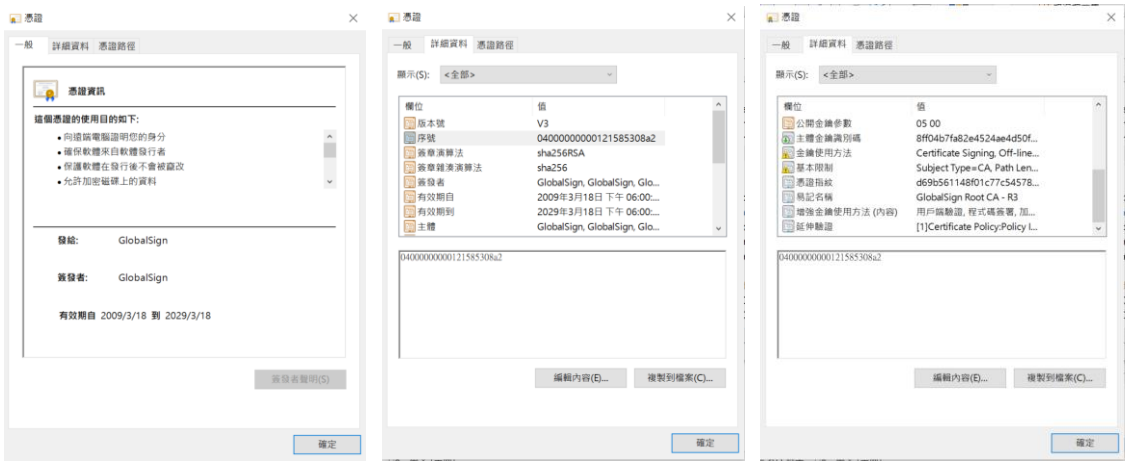
簽章：

使用者透過 Key generation algorithm 產生公鑰，PKI 公鑰基礎建設再透過 CA 將使用者身分和公鑰鏈結，註冊管理中心(Registration authority RA，又稱從屬數字憑證認證機構 Subordinate CA)，然後進行簽章，尚未簽章的憑證內容包含:使用者 ID、使用者公鑰及 CA 的資訊，然後再透過使用的 Haah function 及 CA 的私鑰完成簽章，最後簽章的憑證內容包含:使用者 ID、使用者公鑰、CA 的資訊及簽章。

驗章：

使用尚未簽章的憑證所提供的資料使用 Hash function 算出結果和使用 CA 的公鑰回復簽章為 Hash 之前的值進行比對，若相同，則驗章成功。

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



圖(一)　　圖(二)　　圖(三)

從 certmgr.msc 中我挑選了 GlobalSign 這個電子憑證做討論。

圖(一)為一般資訊，上方欄位可知道此憑證的使用目的包含驗證身分、確保軟體來源、保護軟體不被竄改等等，下方欄位則記載了簽發者、擁有者及有效期限。

圖(二)圖(三)為詳細資訊欄，以下詳細介紹個欄位代表意義:

版本號=>V3 為現行通用版本

序號=>作為辨識每一張憑證的依據，在復原憑證時扮演重要的角色

簽章演算法:SHA256RSA=>使用 SHA256 作為 hash function，使用 RSA 計算數位簽章

簽章雜湊演算法:SHA256=>使用 SHA256 作為 hash function

簽發者=>發行憑證之 CA

有效期限=>包含開始及結束日期

主體: CN=GlobalSign=>Common Name 通用名稱，憑證擁有者的基本名稱

O=GlobalSign=>Organization 組織，憑證擁有者的機構全稱

OU=GlobalSign RootCA-R3=>Organization Unit，憑證擁有者的組織單位名稱

公開金鑰:RSA(2048bits)=>金鑰資訊及金鑰演算法

公開金鑰參數

主體金鑰識別碼

金鑰使用方法

基本限制:Subject Type=CA=>End entity 終端實體

Path Length Constraint=None=>路徑長度限制

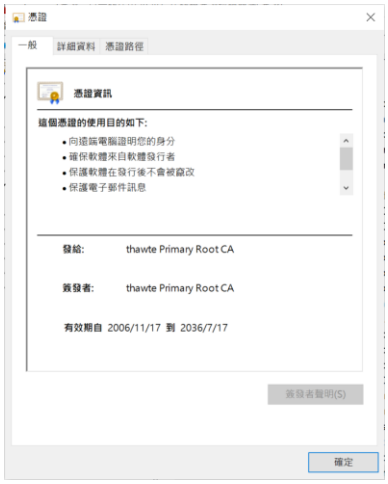
憑證指紋

易記名稱

增強金鑰使用方法(內容)=>簽證用處

延伸驗證

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



圖(一)　　圖(二)

Thawte Primary Root CA 憑證為由 thawte 品牌所發行的 SSL(Secure Socket Layer)憑證，由圖(二)可知，此憑證的用途為:用戶驗證、程式碼簽署、安全電子郵件、伺服器驗證。SSL 憑證用於安全性功能，可為瀏覽器或電腦和伺服器或網路間建立加密連結，保護使用者在使用網站時和網站間所傳遞的資訊不受他人竊取，並以 SSL 技術加密兩個網站間流通的資訊，因此即使資料受到 man-in-middle attack 遭中間者攔截，若沒有解密金鑰，攔截者也只能讀到無法解讀的亂碼。

SSL 憑證所使用的加密機制

(1) 先透過 SSL handshake 機制交換用戶端及伺服器端的加密演算法、密鑰交換演算法或相關規則。

(2) SSL 伺服器端利用憑證將本身公鑰的憑證傳送給用戶端。

(3) 密鑰交換。

(4) 用戶端驗證伺服器端所發送的憑證為合法憑證，用戶端及伺服器端分別利 Handshake 所協商好的加密方法計算交換的 Hash 值，驗證答案是否相同，間接實現用戶端對伺服器端的身分認證。