數位憑證的格式

- **國際標準 - X.509 V3**
  - 電子資料
  - 各種系統間運作 – ASN.1 編碼

版本	憑證格式的版本，如 X.509 Version 3。
序號	用戶的唯一識別序號，同一 CA 所發行的憑證序號不可重複。
演算法識別碼	用來計算此憑證之數位簽章的演算法。
發行者	發行此憑證的 CA 單位。
有效期限	憑證的有效期間。
主體	憑證持有人的相關資料，可能包含有：姓名、郵政地址、E-Mail 地址等等。
公鑰資料	持有人的公開鑰匙、以及其演算法。
數位簽章	CA 的數位簽章，CA 將上述資料經過雜湊演算法計算過後，再經過 CA 的私鑰加密。