

公文使用自然人憑證簽核 Q&A

壹、甚麼是「自然人憑證」？

「自然人憑證」是可以在網路上作資料交換時，如同網路身分證辨識雙方身分，到目前為止，絕大多數政府服務都要求本人帶著身分證，親自到場辦理。隨著科技進步，我們採用了一種叫「憑證」的工具。「憑證」包含了「數位簽章」跟「公開金鑰」由一具公信力之憑證機構(如內政部自然人憑證機構)發行之。這個公開金鑰是智慧型的 IC 卡自己演算出來的一組金鑰對中的一半，另一半稱為「私密金鑰」由使用者妥善保存，則永遠儲存在 IC 晶片當中。經由憑證使用人和憑證管理中心(註 2)約定，日後用這憑證，身分就可以辨認，啟用了加解密的功能，不管你在網路上傳什麼資料，資料都被加密，駭客攔截了資料也無法輕易的解開。

貳、憑證、讀卡機補助？

本校自然人憑證之統一申辦對象，除原編制內教職員工及以校管理費進用之契僱人員外，並擴及擬參加本案試辦之專案工作人員。

參、本校為何使用自然人憑證加簽？

- 簽署內容無遭竄改風險
- 簽署文件具法律效力
- 符合電子簽章法
- 符合檔管局數位歸檔規定
- 符合機關檔案管理資訊化作業要點
- 符合機關檔案管理資訊化要點技術範例手冊
- 憑證私鑰儲存在 IC 卡中，有無法取出或複製之特性，提升安全性。

線上簽核最重要的一個作業環節是須採電子簽章機制，確保簽署檔案的機密性、完整性、不可否認性及法律信證需要。

本校公文線上簽核透過自然人憑證加簽，可以確認公文不可否認性；當完成公文處理，系統要求插入憑證、輸入憑證密碼後，系統即會記錄該簽核人員之憑證，完成電子簽章並存檔，未來如需證明曾經何人、何時簽核過該公文、是否本人簽核公文皆有所依據，並以這樣的方式確保公文在線上傳輸的過程中不會有機會遭到竄改。

公文的簽核對於資訊安全的要求更高於一般系統，因此考慮採用此一憑證機制作為電子公文簽核的認證。

肆、使用自然人憑證是否會洩漏個人隱私資料？

「自然人憑證」就是做為國民在網際網路中確認身分的通行證，因此也被稱之為「網路身證」。每張自然人憑證 IC 卡片都有一個密碼，透過晶片鎖碼設定，可以提供使用者網路認證並確保交易安全，資料經「內政部憑證管理中心」驗證，並且檢驗該憑證是否仍在有效使用期限內，以及是否被列入憑證廢止清單中，如此網路駭客將無法居中假冒，竊取網路上所傳送的資料。

伍、自然人憑證是否可能被偽造？

- 自然人憑證具有防偽設計。
- IC卡具有加解碼設計無法被破解，故不可能被側錄及複製情事。
- 簽發憑證之金鑰儲存於保密器無法複製。
- 若有偽造 IC 卡情形，於應用網路申辦系統時，因有憑證狀態檢查機制，將無法進行交易或查詢個人資料。

陸、獎勵措施

試辦過程中，對於配合度高、使用同意使用自然人憑證比率較高及使用自然人憑證簽核公文較多之前六個單位，本組將簽請校長給予適當獎勵。

參考說明：

註 1. 電子簽章的基本理念

和傳統簽章的用法是一致的。主要的不同是被簽的物體是電子文件而不是紙張。因為電子文件無法蓋上傳統印章，所以不管是不是經過官方印鑑證明的圖章對電子文件一樣沒有作用。所以為了解決證明電子文件的有效性，才產生了一種可以用在電子文件上的簽章方式。因為電子文件不能用傳統的印章去驗證它的有效性，所以國內已制定電子簽章法來規範，加諸於電子文件上的而達到類似傳統簽章的目的。

註 2. 憑證管制中心

憑證管制中心(Certificate Authentication)簡稱 CA，用來核發及驗證電子簽章的印鑑證明。在電子簽章法第二條的名詞解釋所指的憑證機構是指簽發憑證的機構，在政府服務網路(GSN)則是以憑證管制中心這個名詞來說明，二者是相同的。如同傳統的印章，任何人可以刻任何人姓名的印章，但是只有一個印章可以通過區公所的驗證，稱為印鑑章，正式的文書只有這個印鑑章才能說明文件的有效性，所以電子簽章也需要這類機制來查核，發放經過授權的電子簽章。