醫事憑證管理中心醫事人員行動憑證管理服務窗口作業要點

一、本要點之目的

行動憑證管理服務窗口管理及使用醫事人員行動憑證(以下簡稱行動憑證)作業應依本要點辦理。

二、本要點用詞定義

（一）行動裝置：指以 iOS 或 Android 為作業系統，包含但不限於智慧型手機、平板電腦等具通信及連網功能之設備。

（二）行動憑證：指安裝於行動裝置本身或安裝於行動裝置之記憶卡、安全晶片各類載具之醫事憑證管理中心（Healthcare Certification Authority；以下簡稱 HCA）醫事人員憑證。

（三）醫事機構：醫療法第十條第一項所定醫事人員依其專門職業法規規定申請核准開業之機構。

（四）行動憑證管理服務窗口：指醫事機構為醫事人員申辦及管理行動憑證、行動裝置，向 HCA 取得資格者。

（五）行動憑證服務管理系統：指行動憑證管理服務窗口為執行醫事人員行動憑證管理相關業務所建置或管理之軟、硬體。

（六）行動裝置應用程式:指醫事機構安裝於行動裝置內之行動憑證應用軟體，且經行動憑證管理服務窗口驗證認可其安全及應用範圍。

（七）一次性密碼（One Time Password；以下簡稱 OTP)：指運用動態密碼產生器、晶片卡或以其他方式運用 OTP 原理，產生限定一次使用之密碼。

三、行動憑證管理服務窗口資格及權責

（一）醫事機構應依 HCA 網站公告之申請報備方式，取得行動憑證管理服務窗口(以下簡稱服務窗口)資格，並依規定申請醫事機構附卡憑證後，向 HCA 報備本項申請之機構附卡憑證為執行服務窗口作業專屬憑證(以下簡稱專屬憑證)。

（二）服務窗口之建設及權責須由取得服務窗口資格之醫事機構負責，其所需行動憑證服務管理系統之軟硬體設計開發及系統運作環境需求，服務窗口可自行或委託其他單位代為建置或管理。

（三）服務窗口在取得經過醫事人員同意之證明後，可代傳送醫事人員行動憑證申辦或廢止申請訊息至 HCA。服務窗口提出之申請訊息須使用專屬憑證簽章，其內容格式並應符合 HCA 網站公告相關規定。

（四）服務窗口於異常狀況發生時或行動憑證申辦或廢止後，應立即通知行動憑證持有人。

（五）確保行動憑證僅可安裝於本要點定義之各類載具上，以及遵循本要點其他各項要求。

（六）服務窗口應定期清查安裝於各行動裝置設備內之行動憑證狀態，並針對符合廢止條件之行動憑證逕行廢止。

（七）未設立服務窗口之醫事機構得向其他醫事機構之服務窗口取得書面同意後，使用由服務窗口提供之行動憑證服務管理系統與行動裝置應用程式，並由服務窗口代為以數位簽章申辦及管理行動憑證、行動裝置；該醫事機構應於機構內醫事人員變更、離職、停業、歇業、死亡、或醫事機構停業、解散、經主管機關撤銷或廢止許可時立即停止系統帳號使用，並應即時通知服務窗口，相關權責由雙方另行約定。

（八）若經服務窗口申請之行動憑證有安裝於非行動裝置等未遵循本要點之情形，則 HCA 得主動暫停其服務窗口資格。

四、行動裝置設備註冊及管理

（一）服務窗口須註冊待安裝行動憑證之行動裝置資訊，註冊資訊應至少包含裝置之唯一代碼及裝置使用者(含多人使用者)身分資訊。

（二）若行動裝置有新增或異動其共用裝置的使用者時，服務窗口應更新裝置註冊資訊。

五、醫事人員申辦及廢止行動憑證

（一）行動憑證申辦

1. 申請者身分識別方式須採本人持有之醫事人員憑證 IC 卡簽章行動憑證申辦訊息，並由服務窗口驗證申辦訊息簽章，以及憑證有效性、憑證使用效期、憑證鏈等資訊。

2. 服務窗口須確認醫事人員申辦行動憑證時所聲明的憑證使用範圍，是否為服務窗口同意該憑證可使用之應用系統範圍，並且僅可適用於該服務窗口所認可之醫事機構應用。

3. 服務窗口應確認申請使用行動憑證於行動裝置之申請者身分，與該裝置使用者身分相符。

（二）行動憑證廢止

1. 申請者身分識別方式須採本人持有之醫事人員憑證 IC 卡簽章行動憑證廢止訊息，並由服務窗口驗證廢止訊息簽章，以及憑證有效性、憑證使用效期、憑證鏈等資訊。

2. 當以下情形發生時，服務窗口得在尚未徵求醫事人員同意狀況下，代醫事人員主動提出憑證廢止申請：

(1)行動裝置毀損、金鑰遭破解或遭冒用而造成憑證持有人無法使用憑證之情形時。

(2)行動裝置遺失、行動裝置被報廢、人員離職、人員死亡、使用憑證之所有應用系統不再擁有使用權限等原因，而不得再使用憑證之情形時。

(3)若經查行動憑證安裝於非本要點定義可安裝之各類載具之情形時。

六、金鑰對產製及保護

服務窗口使用之系統應確保行動憑證金鑰對產製及保護，採用下列任一款之安全設計。行動憑證金鑰並不得在醫事人員尚未提出憑證申辦需求時預先產生。

（一）由行動裝置應用程式產製金鑰對之設計架構

1. 行動裝置應用程式須設計金鑰安全儲存方式，該應用程式本身並不可提供任何形式備份或匯出私密金鑰之功能(包含不可複製私密金鑰至其他行動裝置)。

2. 行動裝置應用程式須採用軟體保護技術(如白箱加密法)存取及保護金鑰。

（二）由行動裝置安全晶片產製金鑰對之設計架構

1. 安全晶片須符合 NIST 所訂定之 CNS 15135、ISO 19790、FIPS 140-2 Level 2 、其他相同或以上安全強度。

2. 安全晶片須安裝於憑證申辦時所指定之行動裝置，並限制不可提供私密金鑰匯出功能。

（三）由硬體安全模組產製金鑰對之設計架構

1. 硬體安全模組須符合 FIPS 140-2 Level 3、其他相同或以上安全強度認證。

2. 採用硬體安全模組保護主金鑰時，該主金鑰應由非系統開發與維護單位之二個單位（含）以上產製並分持管理其產製之基碼單，另主金鑰得以

加密方式分持匯出至安全載具（如晶片卡）或備份至具存取權限控管之位置，供維護單位緊急使用。

3. 應減少硬體安全模組主金鑰儲存的地點，並允許必要之管理人員存取金鑰，以利管理並降低金鑰外洩之可能性。

4. 當硬體安全模組主金鑰使用期限將屆或有洩漏疑慮時，應進行主金鑰替換。

5. 硬體安全模組須限制，不可提供行動憑證私密金鑰匯出功能，產製之私密金鑰並須限制僅可被憑證申辦時所指定之行動裝置及憑證持有人使用。

6. 行動裝置與硬體安全模組連接之系統間，應具備點對點認證與加密的訊息安全通道保護。

7. 本設計架構僅限應用於醫事機構內部私域網路(含專線、VPN)環境。

七、行動憑證使用管理

服務窗口應確保行動憑證使用方式符合以下要求：

（一）行動憑證僅限安裝於本要點定義可安裝之各類載具上。

（二）行動憑證尚未簽發或憑證過期、憑證被廢止時，不得啟動行動裝置內之醫事人員私密金鑰應用功能。

（三）服務窗口須確保使用行動憑證人員身分與行動裝置使用者身分，以及與申請使用行動憑證於該行動裝置之人員身分皆相符。

（四）行動裝置可多人共用，但行動憑證不可多人共用。行動裝置應用程式應具備能讓憑證持有人設定行動憑證帳號及固定密碼(或 OTP、生物特徵)做為身分識別功能，讓憑證持有人於使用行動裝置時，能正確選擇該持有人於裝置內之行動憑證與私密金鑰進行應用。

（五）服務窗口允許單一醫事人員，可同時持有五張其製發之有效行動憑證。若單一醫事人員有超過五張有效行動憑證之需求，服務窗口應另行向 HCA 提出書面申請。

八、應用程式設計安全

服務窗口使用之系統應確保符合以下要求：

（一）行動憑證服務管理系統設計安全

1. 行動憑證服務管理系統應設計連線控制及網頁逾時中斷機制。使用者超過十分鐘未使用應中斷其連線或採取其他保護措施。

2. 行動憑證服務管理系統接受醫事人員使用醫事人員憑證 IC 卡插卡執行申辦或廢止行動憑證作業時，系統須設計拔插卡檢核機制。

3. 行動憑證服務管理系統應辨識外部連線傳送資訊之訊息來源及資料正確性，以及辨識使用者輸入與系統接收之作業指示一致性。

4. 行動憑證服務管理系統應設計於使用者進行身分確認與申辦或廢止行動憑證機制時，須採用一次性亂數或時間戳記，以防止重送攻擊。

5. 行動憑證服務管理系統應設計個人資料顯示之隱碼機制，以及個人資料檔案、資料庫之存取控制與保護監控措施。

6. 應建立管控機制，限制非授權人員或程式存取行動憑證服務管理系統各項程式功能及內容。

（二）行動裝置應用程式設計安全

1. 行動裝置應用程式應針對所需最小權限進行存取控制。

2. 服務窗口應提供行動憑證應用之行動裝置應用程式名稱、版本與下載位置予醫事人員，確保醫事人員安裝經服務窗口認可且正確之應用程式。

3. 啟動行動裝置應用程式時，應提示使用者注意風險。

4. 於安裝或首次啟動行動裝置應用程式時，得提示建議使用者於行動裝置上安裝防毒軟體。

5. 採用憑證技術進行傳輸加密時，行動裝置應用程式應建立可信任憑證清單並驗證完整憑證鏈及其憑證有效性。

6. 憑證持有人身分識別選擇輸入固定密碼方式時，行動裝置應用程式安全設計應符合以下規定：

(1)密碼不應少於八位。

(2)密碼不應與帳號相同。

(3)密碼超過一年未變更，行動裝置應用程式應有提醒功能。

(4)密碼連續錯誤達五次時應限制使用，須設計有提供憑證持有人重新設定新密碼功能。

(5)密碼由服務窗口發予預設密碼者，於憑證持有人首次登入行動憑證應用程式時，應強制變更預設密碼。

(6)密碼於儲存時應先進行不可逆運算（如雜湊演算法），另為防止透過預先產製雜湊值推測密碼，應進行加密保護或加入不可得知的資料運算。

7. 憑證持有人身分識別選擇輸入 OTP 方式時，行動裝置應用程式安全設計應符合以下規定：

(1)簡訊、Email 或推播 OTP，應設定密碼有效時間以五分鐘內為限，並避免密碼遭竊取或轉發。

(2)密碼連續輸入錯誤達三次時予以鎖定使用，經適當身分認證後才能解除。

(3)憑證持有人使用行動裝置應用程式輸入密碼一旦驗證成功，同一個行動裝置應用程式就不可在驗證成功狀態下,使用同一組密碼進行重複驗證。

(4)密碼應提供予特定行動裝置應用程式做為憑證持有人身分識別使用，不可提供予行動裝置內各任意應用程式取用。

8. 憑證持有人身分識別選擇輸入生物特徵方式時，行動裝置應用程式安全設計應符合以下規定：

(1)憑證持有人身分識別可註冊的生物特徵包含：指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等。

(2)服務窗口應依據其風險承擔能力接受不同生物特徵識別方式，以有效識別憑證持有人身分，必要時應增加多項不同種類生物特徵。

九、本要點有關隱密性及安全性遵循說明

為確保資料之隱密性及安全性，並維持資料傳輸、交換或處理之正確性，HCA 於必要時，得要求服務窗口提高資訊系統資訊安全標準及加強安全控管作業。

本要點未載明之事項，依個人資料保護法、電子簽章法等相關法令辦理。