醫事憑證管理中心

憑證實務作業基準

(Healthcare Certification Authority
Certification Practice Statement)

第 1.6 版

主辦機關：衛生福利部

執行機構:東捷資訊服務股份有限公司

中華民國 107 年 10 月

目錄

1.1 概要 1
1.2 憑證實務作業基準之識別 2
1.3 主要成員及憑證適用範圍 2
1.3.1 醫事憑證管理中心 3
1.3.2 註冊中心 3
1.3.3 註冊窗口 4
1.3.4 卡管中心 4
1.3.5 儲存庫 4
1.3.6 終端個體 5
1.3.7 以委外方式提供認證服務 7
1.3.8 適用範圍 7
1.4 聯絡方式 9
1.4.1 憑證實務作業基準之制訂及管理機關 9
1.4.2 聯絡資料 9
1.4.3 憑證實務作業基準之審定 9
2. 一般條款 10
2.1 職責及義務 10
2.1.1 醫事憑證管理中心之職責 10
2.1.2 註冊中心之職責 10
2.1.3 註冊窗口之職責 11
2.1.4 卡管中心之職責 11
2.1.5 用戶之義務 12
2.1.6 信賴憑證者之義務 14
2.1.7 儲存庫服務之義務 15
2.2 法律責任 15
2.2.1 醫事憑證管理中心之責任 15
2.2.2 註冊中心與註冊窗口之責任 17
2.2.3 卡管中心之責任 18
2.3 財務責任 18
2.4 詮釋及施行 19

2.4.1 適用法律.....19
2.4.2 可分割性、存續、合併、公告通知.....19
2.4.3 紛爭之處理程序.....19
2.5 費用.....19
2.5.1 憑證簽發費用.....19
2.5.2 憑證查詢費用.....20
2.5.3 憑證廢止、狀態查詢費用.....20
2.5.4 憑證更新費用.....20
2.5.5 其他服務之費用.....20
2.5.6 請求退費之規定.....20
2.6 公布及儲存庫.....21
2.6.1 醫事憑證管理中心之資訊公布.....21
2.6.2 公布頻率.....21
2.6.3 存取控制.....22
2.6.4 儲存庫.....22
2.7 稽核方法.....22
2.7.1 稽核之頻率.....22
2.7.2 稽核人員之身分及資格.....22
2.7.3 稽核人員中立性之確保.....23
2.7.4 稽核之範圍.....23
2.7.5 對於稽核結果之因應方式.....23
2.7.6 稽核結果公開之範圍及方法.....23
2.8 資訊保密之範圍.....24
2.8.1 機密之資訊種類.....24
2.8.2 非機密之資訊種類.....24
2.8.3 憑證廢止或暫時停用資訊之公開.....25
2.8.4 應司法機關等要求釋出資訊.....25
2.8.5 應用戶要求釋出資訊.....25
2.8.6 其他資訊釋出之情況.....25
2.8.7 隱私權保護.....25
2.9 權利歸屬.....25
3. 識別和鑑別程序..... 27
3.1 初始註冊.....27

3.1.1 命名種類.....27
3.1.2 命名須有意義.....27
3.1.3 命名形式之解釋規則.....27
3.1.4 命名之獨特性.....27
3.1.5 命名爭議之解決程序.....30
3.1.6 商標之辨識、鑑別及角色.....31
3.1.7 證明擁有私密金鑰之方式.....31
3.1.8 組織身分鑑別程序.....31
3.1.9 個人身分鑑別程序.....33
3.1.10 硬體裝置或伺服軟體鑑別之程序.....34
3.1.11 寫入憑證內之電子郵件驗證.....34
3.1.12 網域名稱擁有者識別程序.....34
3.2 憑證之金鑰更換及展期.....35
3.2.1 憑證之金鑰更換.....35
3.2.2 憑證展期.....35
3.3 憑證被廢止之金鑰更換.....35
3.4 憑證廢止.....36
4. 營運規範..... 36
4.1 申請憑證之程序.....36
4.1.1 憑證申請.....36
4.1.2 憑證內容變更時之憑證申請.....38
4.1.3 憑證遺失時之憑證申請.....38
4.2 簽發憑證及通知憑證已簽發之程序.....39
4.2.1 醫事人員憑證.....39
4.2.2 醫事機構憑證正卡及伺服器應用軟體憑證.....40
4.2.3 醫事機構憑證附卡.....41
4.3 接受憑證及公布憑證之程序.....41
4.4 憑證暫時停用及廢止.....42
4.4.1 廢止憑證之事由.....42
4.4.2 憑證廢止之申請者.....43
4.4.3 憑證廢止之程序.....43
4.4.4 憑證廢止申請之處理期間.....45
4.4.5 暫時停用憑證之事由.....45

4.4.6 暫時停用憑證之申請者 45
4.4.7 暫時停用憑證之程序 46
4.4.8 暫時停用憑證之處理期間及停用期間 48
4.4.9 恢復使用憑證之程序 48
4.4.10 憑證廢止清冊之簽發頻率 48
4.4.11 憑證廢止清冊之查驗規定 48
4.4.12 線上憑證狀態查詢服務 49
4.4.13 線上憑證狀態查詢之規定 49
4.4.14 其他形式廢止公告.....49
4.4.15 其他形式廢止公告之檢查規定 49
4.4.16 金鑰被破解時之其他特殊規定 49
4.5 安全稽核程序 49
4.5.1 被記錄事件種類.....50
4.5.2 紀錄檔處理頻率.....54
4.5.3 稽核紀錄檔保留期限 54
4.5.4 稽核紀錄檔之保護.....54
4.5.5 稽核紀錄檔備份程序 55
4.5.6 安全稽核系統.....55
4.5.7 對引起事件者之告知 55
4.5.8 弱點評估.....55
4.6 紀錄歸檔之方法 56
4.6.1 紀錄事件之類型.....56
4.6.2 歸檔之保留期限.....56
4.6.3 歸檔之保護.....57
4.6.4 歸檔備份程序.....57
4.6.5 時戳紀錄之要求.....57
4.6.6 歸檔資料彙整系統.....57
4.6.7 取得及驗證歸檔資料之程序 57
4.7 金鑰更換.....58
4.8 金鑰遭破解或災變時之復原程序 58
4.8.1 電腦資源、軟體或資料遭破壞之復原程序 58
4.8.2 醫事憑證管理中心之簽章金鑰憑證被廢止之復原程序 58
4.8.3 醫事憑證管理中心之簽章金鑰遭破解之復原程序 59

4.8.4 醫事憑證管理中心安全設施之災後復原工作 59
4.9 醫事憑證管理中心之終止服務 59
5.非技術性安全控管 61
5.1 實體控管.....61
5.1.1 實體所在及結構.....61
5.1.2 實體存取.....61
5.1.3 電力及空調.....62
5.1.4 水災防範及保護.....62
5.1.5 火災防範及保護.....62
5.1.6 媒體儲存.....62
5.1.7 廢料處理.....62
5.1.8 異地備援.....63
5.2 程序控制.....63
5.2.1 信賴角色.....63
5.2.2 角色分派.....65
5.2.3 每個任務所之人數.....65
5.2.4 識別及鑑別每一個角色 66
5.3 人員控制.....67
5.3.1 身家背景、資格、經驗及安全需求 67
5.3.2 身家背景之查驗程序 68
5.3.3 教育訓練需求.....68
5.3.4 人員再教育訓練之需求及頻率 68
5.3.5 工作調換之頻率及順序 69
5.3.6 未授權行動之制裁.....69
5.3.7 聘雇人員之規定.....69
5.3.8 提供之文件資料.....69
6.技術性安全控管 70
6.1 金鑰對之產製及安裝 70
6.1.1 金鑰對之產製.....70
6.1.2 私密金鑰安全傳送給用戶 70
6.1.3 公開金鑰安全傳送給醫事憑證管理中心 70
6.1.4 醫事憑證管理中心公開金鑰安全傳送給信賴憑證者 71
6.1.5 金鑰長度.....71

6.1.6 公鑰參數之產製.....71
6.1.7 金鑰參數品質之檢驗.....71
6.1.8 金鑰經軟體或硬體產製.....72
6.1.9 金鑰之使用目的.....72
6.2 私密金鑰保護.....72
6.2.1 密碼模組標準.....72
6.2.2 金鑰分持之多人控管.....72
6.2.3 私密金鑰託管.....73
6.2.4 私密金鑰備份.....73
6.2.5 私密金鑰歸檔.....73
6.2.6 私密金鑰輸入至密碼模組.....73
6.2.7 私密金鑰之啟動方式.....73
6.2.8 私密金鑰之停用方式.....74
6.2.9 私密金鑰之銷毀方式.....74
6.3 用戶金鑰對管理之其他規定.....74
6.3.1 公開金鑰之歸檔.....74
6.3.2 公開金鑰及私密金鑰之使用期限.....74
6.4 啟動資料之保護.....75
6.4.1 啟動資料之產生.....75
6.4.2 啟動資料之保護.....75
6.4.3 其他啟動資料之規定.....75
6.5 電腦軟硬體安控措施.....76
6.5.1 特定電腦安全技術需求.....76
6.5.2 電腦安全評等.....76
6.6 生命週期技術控管措施.....77
6.6.1 系統研發控管措施.....77
6.6.2 安全管理控管措施.....77
6.6.3 生命週期安全評等.....77
6.7 網路安全控管措施.....77
6.8 密碼模組安全控管措施.....78
7 格式剖繪 78
7.1 憑證之格式剖繪.....78

7.1.1 版本序號.....78
7.1.2 憑證擴充欄位.....78
7.1.3 演算法物件識別碼.....78
7.1.4 命名形式.....79
7.1.5 命名限制.....79
7.1.6 憑證政策物件識別碼.....79
7.1.7 政策限制擴充欄位之使用.....79
7.1.8 政策限定元之語法及語意.....79
7.1.9 關鍵憑證政策擴充欄位之語意處理.....79
7.2 憑證廢止清冊之格式剖繪.....79
7.2.1 版本序號.....79
7.2.2 憑證廢止清冊擴充欄位.....79
8.憑證實務作業基準之維護.....80
8.1 變更程序.....80
8.1.1 變更時不另作通知之變更項目.....80
8.1.2 應通知之變更項目.....80
8.2 公告及通知之規定.....81
8.3 憑證實務作業基準之審定程序.....81

摘要

依電子簽章法授權發布訂定之「憑證實務作業基準應載明事項」規定，醫事憑證管理中心憑證實務作業基準(以下簡稱本作業基準)重要事項說明如下：

1、主管機關核定文號：中華民國 107 年 10 月 16 日經商字第 10702423530 號

2、簽發之憑證：

(1)種類：醫事憑證管理中心(以下簡稱本管理中心)負責簽發及管理醫事領域專業醫事人員、醫事機構及其所屬應用於醫事專門用途的伺服器應用軟體之終端用戶憑證(包括簽章與加解密用的憑證)。

(2)保證等級：本管理中心依據政府機關公開金鑰基礎建設憑證政策(以下簡稱憑證政策)保證等級規範，提供保證等級第 3 級運作，簽發憑證政策所定義保證等級第 3 級的憑證。此等級所簽發之憑證可應用於具風險之醫事專屬通訊網路或網際網路上、傳送敏感之醫療隱私資料，達到身分鑑別、隱私保護、交易完整性與不可否認性之保證。

(3)適用範圍：本管理中心核發之憑證適用於醫事資訊電子化與電子化政府相關應用服務所需的身分認證及資料加解密，業務範圍包括醫事人員之電子證照；醫事人員、醫事機構或應用系統之身分鑑別、隱私資料之完整性保護與醫事資訊交換時之金鑰交換或資料加解密。所稱之醫事資訊，指涵蓋衛生相關之醫療、保健、防疫、藥物及食品等相關資訊。

用戶及信賴憑證者，必須謹慎使用本管理中心所簽發之憑證，並不得違反本作業基準所限制及禁止的憑證適用範圍。

(4)認證服務的第三方稽核：憑證管理中心每年接受兩項的第三方稽核：其一由電子化政府主管機關依政府採購法，委託公正第三方辦理外部稽核作業，就本管理中心的運作進行稽核；其二為主辦機關認可之資訊安全管理系統認證。

3、法律責任重要事項：

本管理中心之憑證機構乃依電子簽章法與醫事資訊電子化相關行政命令規定所設立，適用項目皆為將目前紙本作業流程改為電子化作業流程，故相關應用之法律依據，將以原本作業流程之相關法令規定為準；相關之爭議訴訟與賠償規定亦同。

(1)用戶或信賴憑證者如未依照本作業基準規定之適用範圍使用憑證所引發之後果，本管理中心不負任何法律責任。

(2)用戶或信賴憑證者因使用憑證而發生損害賠償事件時，本管理中心之損害賠償責任以電子簽章法所訂之責任範圍為限，若可歸責於憑證管理中心或其所屬人員未依本作業基準或相關規定辦理用戶註冊、憑證簽發或停用、廢止作業，憑證管理中心依 2.2.1.4 所訂賠償範圍內，賠償用戶或信賴憑證者因憑證作業致受有直接損害為限，但不包括間接損害。

(3)如因不可抗力及其他非可歸責於本管理中心之事由，

所導致之損害事件，本管理中心不負任何法律責任。

(4)註冊中心因執行註冊工作所引發之法律責任除法令另有規定外，由本管理中心負責。

(5)本管理中心所簽發之憑證僅對憑證主體身分做確認，由憑證註冊窗口審驗人員審驗用戶之身分及憑證相關資訊,如因用戶隱瞞事實,提供註冊窗口不正確資訊，導致信賴憑證者遭受損害時，如該損害之造成不可歸責於註冊窗口時，相關法律責任應由用戶自行負責。

(6)用戶之憑證如須暫停使用、恢復使用、廢止或重發，應依照本作業基準相關規定辦理，如發生私密金鑰資料外洩、遺失或遭受冒用、偽造、破解等情形，必須廢止憑證時，應立即通知本管理中心，但用戶仍應承擔本管理中心完成憑證廢止作業程序並公告前所有使用該憑證之法律責任。

(7)本管理中心核發之伺服器應用軟體憑證對應之私密金鑰部份，用戶應採適當的管理機制，對於不當保管與使用此類私密金鑰所造成的損害，本管理中心不負擔任何責任。

4、其他重要事項：

(1)如因本管理中心之系統維護、轉換及擴充等需要，得暫停部分憑證服務，並公告於儲存庫及通知用戶，用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。

(2)用戶在接受本管理中心所簽發之憑證後，即表示已確認憑證內容資訊之正確性，並依照本作業基準相關規

定使用憑證，如憑證內容資訊有誤，用戶應主動通知本管理中心。

(3)用戶及信賴憑證者應慎選安全的電腦環境及可信賴的應用系統，如因電腦環境或應用系統本身因素導致用戶及信賴憑證者權益受損時，應自行承擔責任。

(4)本管理中心如因故無法正常運作時，用戶及信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。如因此致第三人對憑證管理中心為任何主張或請求時，由用戶及信賴憑證者負責對造成憑證管理中心的損害負賠償責任，賠償以憑證管理中心受有之直接損害為限，但不包括間接損害。

(5)信賴憑證者接受使用本管理中心簽發之憑證前，必須確認已了解並同意有關本管理中心法律責任之條款，接受使用時必須依照本作業基準相關規定使用憑證。

1 序論

醫事憑證管理中心憑證實務作業基準(Healthcare Certification Authority Certification Practice Statement，以下簡稱本作業基準)係依據政府機關公開金鑰基礎建設憑證政策(Certificate Policy for Government Public Key Infrastructure，以下簡稱憑證政策)訂定，並遵循電子簽章法及其子法「憑證實務作業基準應載明事項準則」、符合CA/Browser Forum 組織要求等相關規定，說明醫事憑證管理中心(Healthcare Certification Authority, HCA，以下簡稱本管理中心)如何遵照憑證政策保證等級第3級之規定，進行醫事領域專業醫事人員、醫事機構及其所屬應用於醫事專門用途的伺服器應用軟體之終端用戶憑證簽發及管理作業。

1.1 概要

依據憑證政策的規定，本管理中心是政府機關公開金鑰基礎建設(Government Public Key Infrastructure, GPKI，以下簡稱本基礎建設)的第1層下屬憑證機構(Level 1 Subordinate CA)，在本基礎建設中負責簽發及管理醫事領域專業醫事人員、醫事機構及其所屬應用於醫事專門用途的伺服器應用軟體之終端用戶憑證(包括簽章用及加解密用的憑證)，皆為憑證政策保證等級第 3 級之憑證。

本作業基準中，將說明本管理中心的憑證作業實務，以確保本管理中心的憑證簽發及管理作業符合憑證政策訂定之保證等級第3級之規定。本作業基準所載明之實務作業規範僅適用於與本管理中心相關之個體，如本管理中心、註冊中心(Registration Authority)、註冊窗口(Registration Authority Counter)、卡管中心

(Card Management Center)、用戶(Subscribers)、信賴憑證者(Relying Parties)及儲存庫(Repository)等。

衛生福利部(以下簡稱本部)為本管理中心之主管機關，負責本作業基準之訂定及修訂，本作業基準需經電子簽章法主管機關經濟部核可後施行。本作業基準未授權本管理中心以外的憑證機構使用，其他憑證機構因引用本作業基準而引發的任何問題，概由該憑證機構自行負責。

1.2 憑證實務作業基準之識別

本作業基準之名稱為醫事憑證管理中心憑證實務作業基準(Healthcare Certification Authority Certification Practice Statement)，本版本為第 1.5 版，公佈日期為 105 年 5 月 4 日。本作業基準的最新版本可在以下網頁取得(http://hca.nat.gov.tw/download/HCACPSv1.5.pdf)。

本作業基準依據憑證政策訂定，本管理中心之運作遵照憑證政策保證等級第 3 級之規定，其物件識別碼名稱為 id-tw-gpki-certpolicy-class3Assurance，物件識別碼值為{id-tw-gpki-certpolicy 3}。(請參考憑證政策)。

1.3 主要成員及憑證適用範圍

本管理中心提供醫事憑證應用所需之憑證服務。

其相關主要成員包括：

(1)醫事憑證管理中心。

(2)註冊中心。

(3)註冊窗口。

(4)卡管中心。

(5)儲存庫。

(6)憑證用戶。

(7)信賴憑證者。

1.3.1 醫事憑證管理中心

本管理中心是本基礎建設中的第 1 層下屬憑證機構，遵照憑證政策保證等級第 3 級的規定，負責簽發及管理醫事領域專業醫事人員、醫事機構及其所屬應用於醫事專門用途的伺服器應用軟體之終端用戶憑證。

1.3.2 註冊中心

註冊中心負責訂定憑證用戶註冊與身分驗證之詳細程序，收集和驗證用戶的身分及憑證相關資訊之註冊工作，進行憑證用戶之申辦、查詢及廢止等作業，註冊中心將由多個註冊窗口（RA Counter）組成。

註冊中心設置註冊中心伺服器（RA Server），負責驗證註冊窗口審驗人員的身分及管理註冊窗口。註冊中心伺服器由註冊中心管理員（RA Administrator）負責管理，註冊中心管理員於註冊中心伺服器上設定註冊窗口審驗人員之帳號與權限，並製發註冊窗口審驗人員 IC 卡（以下簡稱 RAO IC 卡）。註冊中心伺服器上並裝設註冊中心之私密金鑰，註冊中心伺服器與本管理中心伺服器間的通訊，將由註冊中心之私密金鑰簽章加以保護。

1.3.3 註冊窗口

註冊窗口設有註冊窗口審驗人員（RA Officer, RAO），依其權限負責受理憑證之註冊受理或申請、暫停使用申請、恢復使用申請及廢止申請等業務。

註冊窗口審驗人員依其所屬權限與作業規定進行下列相關業務：

(1) 憑證之註冊申請，在申辦時對申辦用戶(Subject)進行身分識別與申請受理，並對文件進行歸檔保管。

(2) 進行相關文件審核工作，確認身分後始送交申請或廢止憑證之請求至本管理中心，最後將申辦結果回報用戶。

關於註冊中心之作業，將授權全國衛生局所或本管理中心授權之單位擔任註冊窗口，依其權限執行上述註冊中心之相關工作。各註冊窗口之所在地與聯絡電話，將公布於本管理中心網站，憑證用戶依註冊窗口作業規範前往各地衛生局所或授權註冊窗口櫃台辦理相關業務。

1.3.4 卡管中心

本管理中心用戶使用之符記(Token)主要採 IC 卡，本管理中心設置卡管中心，進行 IC 卡製卡及管理作業。IC 卡製卡及管理作業，包括 IC 卡內部產製金鑰對、以亂數設定 IC 卡之初始個人識別碼(以下簡稱 PIN 碼)、將憑證寫入 IC 卡中及印卡、卡片管理與配送管理作業等工作。

1.3.5 儲存庫

儲存庫負責公告由本管理中心所簽發之憑證、憑證廢止清冊

(Certificate Revocation List, CRL)及其他憑證相關資訊。本管理中心除自行建置及維運儲存庫外，將本管理中心所簽發之憑證及憑證廢止清冊轉存至憑證管理中心目錄服務(DirectoryService, DS)中。

儲存庫提供 24 小時全天的服務，網址為(http://hca.nat.gov.tw/)。

1.3.6 終端個體

1.3.6.1 用戶

本管理中心認定之憑證實體用戶包括：

(1) 本部醫事管理系統登記核准之醫事人員。

(2) 本部醫事管理系統登記核准之醫事機構。

(3) 具有應用於醫事專門用途的伺服器應用軟體(醫事用途由部認定之)所有權的醫事機構。

第(1)項醫事人員用戶使用之憑證載具主要為 IC 卡，但用戶也可使用自備之其他安全載具為符記，惟用戶須確保其符記之安全，本管理中心對於用戶不當保管與使用自備符記所造成的損害，亦不負擔任何責任。若以 IC 卡為憑證載具，可同時儲存簽章用及加解密用兩種憑證。每張卡片存有兩對金鑰對，一為簽章用金鑰對，另一為加解密用金鑰對；醫事人員非 IC 卡為憑證載具，則存有一對金鑰對，為簽章用金鑰對。

第(2)項醫事機構用戶使用之符記主要採 IC 卡，但用戶也可使用自備之其他安全載體為符記，惟用戶須確保其載體之安全，本管理中心對於用戶不當保管與使用自備載體所造成的損害，亦不負擔任何責任。每個符記可同時儲存簽章用及加解密用兩種憑證。每個醫事機構只可申請 1 張正卡，但可依應用需要申請多張附卡，每張正卡或附卡皆存有兩對金鑰對，一為簽章用金鑰對，另一為加解密用金鑰對，因

此本管理中心將對每張正卡或附卡簽發簽章用及加解密用兩種憑證。

醫事機構用戶必須依照 3.1 節初始註冊之識別與鑑別程序，申請醫事機構憑證之正卡。如正卡遺失或憑證將到期時，必須依照 3.1 節初始註冊之識別與鑑別程序重新辦理申請。用戶在取得正卡後，可再依照識別與鑑別程序申請附卡，或透過正卡之數位簽章線上申請附卡，並可依應用需要申請多張附卡。

第(3)項伺服器應用軟體憑證之申請，本管理中心接受此類用戶作為憑證用戶之條件，為使用該軟體所屬之單位醫事機構 IC 卡，透過線上驗證機構憑證後直接進行線上申請；或出具公文，並以管理人之名義提出申請。所有因此憑證所產生之法律權責由此管理人承擔。

伺服器應用軟體憑證沒有正附卡之分別，可依應用需要申請多張憑證，憑證中的金鑰用途可為簽章用或加解密用，必要時可同時包含簽章用及加解密用兩種金鑰用途。

1.3.6.2 信賴憑證者

信賴憑證者係指相信憑證主體名稱與公開金鑰之連結關係的個體。

信賴憑證者在使用本管理中心所簽發之憑證前，必須以本管理中心本身的憑證及憑證狀態資訊，檢驗所使用憑證的有效性。在確認憑證的有效性後，才可使用憑證進行以下作業：

(1) 檢驗電子文件之完整性。

(2) 檢驗電子文件產生者的身分。

(3) 與憑證主體間建立安全之通訊管道。

1.3.7 以委外方式提供認證服務

東捷資訊服務股份有限公司接受本部委託，負責本管理中心之建置及系統維運作業。

1.3.8 適用範圍

1.3.8.1 憑證之適用範圍

本管理中心負責簽發及管理醫事領域專業醫事人員、醫事機構及其所屬應用於醫事專門用途的伺服器應用軟體之終端用戶憑證，且包含簽章用及加密用憑證。

本管理中心提供符合憑證政策保證等級第 3 等級之憑證。核發之憑證適用於醫事資訊電子化與電子化政府相關應用服務所需的身分認證及資料加解密，包含醫事人員、醫事機構或應用系統之身分鑑別、隱私資料之完整性保護與醫事資訊交換時之金鑰交換或資料加解密，並假設在網路中有惡意的使用者會去截取或篡改網路資訊，所傳送的資訊可能包含金錢上的交易。

伺服器應用軟體憑證可應用於安全套接層(Secure Socket Layer, SSL)通訊協定及開發專屬的伺服器應用軟體或是提供時戳服務之伺服器應用軟體。

1.3.8.2 憑證之使用限制

本管理中心所核發憑證之使用，有以下幾點限制：

(1) 憑證用戶在使用私密金鑰時，應慎選安全的電腦環境及可信賴的應用系統，以避免私密金鑰被惡意軟體盜取或誤用而引發權益受損。

(2) 信賴本管理中心核發之憑證者在使用憑證前，必須確定依照本作業基準第 2.1.6 節所載之安全方式，取得本管理中心本身的憑證及憑證狀態資訊，檢驗所使用憑證的有效性，在確認憑證之有效性後，始可採信所使用之憑證。

(3) 本管理中心所核發之憑證在其擴充欄位中註記有該憑證對應私密金鑰之用途限制、憑證政策物件識別碼等資訊；信賴該憑證者在驗證其對應私密金鑰所產生之數位簽章時，應確認上述欄位之資訊是否與其用途相符。

(4) 信賴憑證者在使用本管理中心所簽發之憑證前，應確認憑證之類別、正附卡別、保證等級及金鑰用途等是否符合應用需求。

(5) 信賴憑證者應依照 X.509 規範處理憑證中的關鍵性(Critical）與非關鍵性（Non-Critical）憑證擴充欄位(Extensions)。

(6) 用戶及信賴憑證者在使用本管理中心所提供的認證服務前，必須詳讀本作業基準，並遵守本作業基準之規定，同時必須注意本作業基準之修訂。

1.3.8.3 憑證之禁止使用情形

本管理中心所核發之憑證禁止使用於下列應用領域：

(1) 軍令戰情。

(2) 核生化武器管制。

(3) 犯罪。

(4) 依電子簽章法規定明訂排除適用之應用領域。

(5) 其他足以造成損害、死傷以及社會重大環境改變之應用。

1.4 聯絡方式

1.4.1 憑證實務作業基準之制訂及管理機關

本部為本管理中心之主管機關，負責本作業基準之訂定與修訂。本作業基準之制定及修訂在經電子簽章法主管機關經濟部核可後公布施行。

1.4.2 聯絡資料

如對本作業基準有任何建議或用戶報告遺失金鑰等事件，請與本管理中心聯絡，本管理中心之聯絡電話：0800-364422，郵遞地址： 220 新北市板橋區遠東路 1 號研發大樓 4 樓 G 室，電子郵件信箱：hca@mohw.gov.tw，請參閱網址(http://hca.nat.gov.tw/)。

1.4.3 憑證實務作業基準之審定

依據電子簽章法規定，本作業基準必須經該法定主管機關經濟部核定後，始得對外提供簽其發憑證服務。

2 一般條款

2.1 職責及義務

2.1.1 醫事憑證管理中心之職責

本管理中心負責以下工作之職責：

依據憑證政策保證等級第 3 級規定與本作業基準運作。

(1) 簽發及公布憑證。

(2) 廢止、停用及恢復使用憑證。

(3) 簽發及公布憑證廢止清冊。

(4) 執行本管理中心與註冊中心相關人員之識別及鑑別程序。

(5) 安全產製本管理中心之私密金鑰。

(6) 保護本管理中心之私密金鑰。

(7) 支援註冊中心憑證註冊相關作業。

2.1.2 註冊中心之職責

註冊中心負責以下工作之職責：

(1) 負責訂定憑證用戶註冊與身分驗證之詳細程序。

(2) 註冊中心伺服器之維護及安全管理。

(3) 提供憑證申請服務。

(4) 執行憑證申請之識別及鑑別程序。

(5) 將申請資料及用戶公開金鑰透過安全管道(安全管道為使用安全套接層通訊協定 256 位元或其他相同或更高等級之資料加密傳送方式)傳送給本管理中心。

(6) 告知用戶有關本管理中心及註冊中心之義務與責任。

(7) 告知用戶有關接受或使用本管理中心所簽發憑證，必須遵守本作業基準之相關規定。

(8) 執行 RAO 之識別及鑑別程序。

(9) 安全產製註冊中心之私密金鑰。

(10) 保護註冊中心之私密金鑰。

2.1.3 註冊窗口之職責

註冊窗口進行憑證註冊管理工作。依其業務範圍權限負責以下工作之職責：

(1) 接受憑證用戶提出醫事人員憑證申辦受理，進行之身分識別及鑑別、受理資料安全傳輸之工作。

(2) 接受憑證用戶提出醫事機構憑證、醫事機構附卡憑證及伺服器軟體憑證之申請。

(3) 對提出醫事人員憑證、醫事機構憑證及醫事機構附卡憑證申請、廢止等各項憑證申辦作業之申請者進行身分鑑別。

(4) 遵守與本管理中心之憑證機構間之約定事項，嚴格控管其操作安全，並根據既定之處理程序進行業務。

註冊窗口操作人員作業前必須登入系統、依其權限進行用戶識別或資料傳輸等相關作業；本管理中心對任一用戶之申請、識別與審核作業，皆留存有操作稽核紀錄。

2.1.4 卡管中心之職責

(1) 依照 6.1.1.1 節規定，於 IC 卡內部安全產製用戶之金鑰對。

(2) 以亂數設定 IC 卡之初始 PIN 碼。

(3) 統一初始化印卡。

(4) 將憑證寫入 IC 卡及印製。

(5) 卡片內容與卡體列印品質檢驗。

(6) 掛號郵寄用戶之 IC 卡。

(7) 執行 IC 卡配送管理作業。

(8) 執行卡片管理作業。

(9) 提供 IC 卡開卡資料管理作業。

(10) 提供 IC 卡鎖卡管理作業。

2.1.5 用戶之義務

憑證用戶應負擔以下義務：

(1) 詳閱本管理中心公布之本作業基準文件，並應遵守其中所列之相關規定。

(2) 保證提供本管理中心註冊中心正確之用戶之註冊資料，並授權依本作業基準所載之規定之範圍內使用該資料。

(3) 瞭解並遵守本管理中心核發憑證時對金鑰用途之限制，並同意不在設定之用途外不當使用本金鑰。

(4) 本管理中心採用高安全度之 RSA IC 卡做為私密金鑰儲存載具，用戶應妥善保管及使用私密金鑰並設定安全之個人密碼以確認使用權。

(5) 若非由本管理中心代為產製金鑰對之憑證用戶，用戶應自行負責安全產製其金鑰對。

(6) 對本管理中心所簽發之伺服器應用軟體憑證，應有保管人對私密金鑰之使用進行瞭解與監控。伺服器應用軟體應採用安全之金鑰管理機制，防止該金鑰遭不正當之複製導致金鑰非法使用。

(7) 本管理中心所簽發之伺服器應用軟體憑證中所指之憑證主體(Certificate Subject)為各該伺服器應用軟體，並以其所有權人或經授權使用之人為用戶。如各該伺服器應用軟體之所有權或使用權發生移轉時，用戶應廢止原憑證並重新申請憑證。

(8) 如須暫時停用、恢復使用、廢止或重新申請憑證，應依照第 4 章規定辦理，如發生私密金鑰資料外洩、遺失或遭受冒用、偽造、破解等情形，必須廢止憑證時，應立即通知本管理中心。憑證用戶有權提出廢止請求，憑證廢止申請經審核通過後，本管理中心將於 1 個工作天內完成憑證廢止作業，但用戶仍應承擔本管理中心完成憑證廢止作業程序並公告前所有使用該憑證之法律責任。

(9) 在本管理中心核定憑證申請並簽發憑證給用戶後，用戶應依照 4.3 節規定接受憑證。

(10) 用戶接受本管理中心所簽發之憑證，即表示已確認憑證內容資訊之正確性，必須依照 1.3.8 節適用範圍使用憑證，如憑證內容有誤，用戶應主動通知本管理中心。

(11) 應慎選安全的電腦環境及可信賴的應用系統，如因電腦環境或應用系統本身因素導致信賴憑證者權益受損時，應自行承擔責任。

(12) 本管理中心如因故無法正常運作時，用戶應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。如因此致第三人對憑證管理中心為任何主張或請求時，由用戶及信賴憑證者負責對造成憑證管理中心的損害負賠償責任，賠償以憑證管理中心受有之直接損害為限，但不包括間接損害。

2.1.6 信賴憑證者之義務

信賴本管理中心之憑證使用者，在對所採行之憑證信任並確認其有效用途之前，應充分瞭解本管理中心之本作業基準與所實現之政策及相關法律責任條款。此外應承擔以下責任：

(1) 在使用本管理中心所簽發之憑證或查詢儲存庫時，必須遵守本作業基準之相關規定。

(2) 在使用本管理中心所簽發之憑證時，應先檢驗憑證之保證等級以確保權益。

(3) 在使用本管理中心所簽發之憑證時，應確認憑證所記載之正附卡別及金鑰用途。

(4) 依取得憑證內容所規定之演算法驗證本管理中心核發之憑證數位簽章正確性，以確認該憑證或憑證廢止清冊是否正確。

(5) 在使用本管理中心所簽發之憑證時，應先檢驗憑證廢止清冊，以確認該憑證是否有效。

(6) 不可採信任何非在本管理中心授權用途範圍內之應用。

(7) 應慎選安全的電腦環境及可信賴的應用系統，如因電腦環境或應用系統本身因素導致信賴憑證者或其系統用戶權益受損時，應自行承擔責任。

(8) 本管理中心如因故無法正常運作時，信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。如因此致第三人對憑證管理中心為任何主張或請求時，由用戶及信賴憑證者負責對造成憑證管理中心的損害負賠償責任，賠償以憑證管理中心受有之直接損害為限，但不包括間接損害。

(9) 信賴憑證者同時應認知本管理中心之儲存庫為當然且唯一之

憑證與憑證狀態發布單位。

(10) 信賴憑證者如使用本管理中心所簽發之憑證，即表示已了解並同意本作業基準之法律責任相關規定，並依照 1.3.8 節適用範圍使用憑證。

2.1.7 儲存庫服務之義務

儲存庫為本管理中心唯一提供對外公布資料之所在，應負擔以下責任：

(1) 依照 2.6 節規定，定期公布簽發之憑證、憑證廢止清冊及其他憑證相關資訊。

(2) 公布本作業基準的最新資訊。

(3) 儲存庫之存取控制依照 2.6.3 節規定辦理。

(4) 保障儲存庫資訊之可接取狀態及可用性。

2.2 法律責任

2.2.1 醫事憑證管理中心之責任

2.2.1.1 保證範圍及其限制條件

本管理中心依憑證政策保證等級第 3 級運作，並遵守本作業基準規定簽發及管理憑證、簽發及公布憑證廢止清冊以及維持儲存庫之正常運作，保證範圍如下：

(1) 本管理中心處理註冊資料及憑證簽發作業，除未遵照本作業基準之規定辦理，或違反相關法律規章之規定而造成用戶之損失，且可歸責於本管理中心之過失外，本管理中心概不負任何損害賠償責任。

(2) 本管理中心未善盡保管用戶之註冊及憑證相關資料，而造成相關資訊洩漏、被冒用、篡改及任意使用致造成用戶遭受損害時，本管理中心應負擔賠償責任。

(3) 本管理中心應負擔賠償責任如因作業人員惡意或疏失，未遵照本作業基準之規定辦理註冊、憑證之簽發與廢止作業，而造成用戶之損失時，本管理中心應負擔賠償責任。

本作業基準係依據電子簽章法施行細則之規定，送交主管機關經濟部商業司審核通過。檢閱本文之讀者應先確認版本與主管機關核准文號相符。

2.2.1.2 否認聲明及其限制條件

用戶或信賴憑證者如未依照 1.3.8 節適用範圍使用憑證所引發之後果，本管理中心不負任何法律責任。

2.2.1.3 其他除外條款

如因不可抗力及其他非可歸責於本管理中心之事由，所導致之損害事件，本管理中心不負任何法律責任。

如非為本管理中心作業人員惡意或疏失，造成網際網路傳輸之中斷或設備之故障或其他不可抗力之天災事故（例如戰爭或地震等），致所簽發之憑證造成用戶損失時，本管理中心不負任何損害賠償責任。

如因本管理中心之系統維護、轉換及擴充等需要，得暫停部分憑證服務，並公告於儲存庫及通知用戶，用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。

如因 4.4.1 節廢止憑證之事由，用戶應依照 4.4.3 節憑證廢止程序

向本管理中心提出廢止憑證申請，在本管理中心核定廢止憑證申請後1個工作天內完成憑證廢止作業、簽發憑證廢止清冊及公告於儲存庫。用戶於憑證廢止狀態未被公布之前，應採取適當的行動，以減少對信賴憑證者之影響，期間如該用戶憑證被用以進行非法使用，或使用後產生法律糾紛時，本管理中心如依據本作業基準與相關之作業規範執行處理作業時，則不負任何損害賠償責任。

2.2.1.4 賠償責任

憑證管理中心提供用戶於開放網路中的身分識別及資料保護之服務過程，致用戶受有損害，且可歸責於憑證管理中心或其所屬人員未依本作業基準或相關規定辦理用戶註冊、憑證簽發或停用、廢止作業時，負賠償責任，但依據電子簽章法第十四條規定，憑證管理中心能證明行為無過失者，不在此限。

憑證管理中心依前項約定，對於用戶或信賴憑證者所負賠償責任之範圍，均以賠償用戶或信賴憑證者因憑證作業致受有直接損害為限，但不包括間接損害，例如用戶或信賴憑證者因憑證作業致其依通常情形或依已定計畫，預期可取得利益之喪失之情況，不在賠償範圍內。

2.2.2 註冊中心與註冊窗口之責任

2.2.2.1 保證範圍及其限制條件

註冊中心遵守本作業基準規定，收集和驗證用戶的身分及憑證相關資訊之註冊工作，註冊中心將由多個註冊窗口組成，註冊中心與註冊窗口之人員應盡善保管使用者資料，如造成用戶相關資料遭冒用、竄改、或竊取使用於其他不相關應用時，本管理中心應負賠償責任。

註冊中心與註冊窗口之人員因執行註冊工作所引發之法律責任除法令另有規定外，由本管理中心負責。

本管理中心所簽發之憑證僅對憑證主體身分做確認，由憑證註冊

窗口審驗人員審驗用戶之身分及憑證相關資訊，如因用戶隱瞞事實，提供註冊中心不正確資料，導致信賴憑證者遭受損害時，如該損害之造成不可歸責於本管理中心時，相關責任應由用戶負責。

詳細註冊窗口之責任規定於本管理中心註冊窗口作業安全規範內（請參閱 http：//hca.nat.gov.tw/）。

2.2.2.2 否認聲明及其限制條件

用戶或信賴憑證者應依照 1.3.8 節適用範圍使用憑證。

2.2.2.3 其他除外條款

如因不可抗力及其他非可歸責於註冊中心之事由，所導致之損害事件，註冊中心不負任何法律責任。

2.2.3 卡管中心之責任

卡管中心遵守本作業基準規定之程序，負責驅動 IC 卡以產製用戶的金鑰對及相關發卡作業，卡管中心因執行卡片管理作業所引發之法律責任由本管理中心負責。

2.3 財務責任

本管理中心營運所需之經費由本部每年依所編列政府預算提撥，未向保險公司投保，但本部每年均由審計部執行財會稽核。

因本管理中心營運疏失所造成之財務損失與賠償，將循現有行政管理體系流程之訴訟程序與管轄法院規定，進行財務責任之判定與賠償。

2.4 詮釋及施行

2.4.1 適用法律

本管理中心因執行憑證簽發及管理作業需要，所簽署的相關協議之解釋及合法性，依循我國相關法令規定辦理。

2.4.2 可分割性、存續、合併、公告通知

如本作業基準的任何一章節不正確或無效時，其他章節仍然有效，本作業基準的修訂依照第 8 章規定辦理。

2.4.3 紛爭之處理程序

用戶與本管理中心如有爭議時，雙方應本誠信原則，先進行協商，並得依紛爭處理程序(請參閱 http://hca.nat.gov.tw/)，請求本管理中心就本作業基準相關條文提出解釋。

用戶與本管理中心如有爭議時，雙方應本誠信原則，先進行協商。如協商不成，需訴訟時，以臺灣臺北地方法院為第一審管轄法院。

2.5 費用

本管理中心如需向用戶及信賴憑證者收取費用，將配合修訂本作業基準，並訂定相關費用之查詢方法及請求退費之程序。

本部將每 2 年與本管理中心針對相關收費標準進行檢討。

2.5.1 憑證簽發費用

收費方式依本部發布之醫事憑證收費標準辦理。

收費標準將公告於本管理中心網站(http：//hca.nat.gov.tw/)，以供

憑證用戶查詢。

2.5.2 憑證查詢費用

目前沒有收費。

2.5.3 憑證廢止、狀態查詢費用

目前沒有收費。

2.5.4 憑證更新費用

因憑證用戶之私密金鑰使用期限屆滿或憑證所記載之用戶主體名稱變更而需更新憑證時，本管理中心酌收 IC 卡之規費。收費方式依本部發布之醫事憑證收費標準辦理。

收費標準將公告於本管理中心網站(http：//hca.nat.gov.tw/)，以供憑證用戶查詢。

2.5.5 其他服務之費用

收費方式依本部發布之醫事憑證收費標準辦理。

收費標準將公告於本管理中心網站(http：//hca.nat.gov.tw/)，以供憑證用戶查詢。

2.5.6 請求退費之規定

本管理中心目前除因 2.5.4/2.5.5 節所述之情況外，無其他收費機制，因此無請求退費之程序。(請參閱 http：//hca.nat.gov.tw/)

2.6 公布及儲存庫

2.6.1 醫事憑證管理中心之資訊公布

(1) 本作業基準。

(2) 憑證廢止清冊(含憑證廢止及暫時停用資訊)。

(3) 本管理中心本身之憑證(到該憑證相對應之私密金鑰所簽發的所有憑證效期到期為止)。

(4) 線上即時憑證狀態之查詢。

(5) 查詢簽發之憑證。

(6) 隱私權保護政策。

(7) 最近 1 次之稽核結果。

(8) 本管理中心之最新訊息。

(9) 憑證政策。

2.6.2 公布頻率

(1)本作業基準於主管機關核准後發布，本作業基準修訂依照第 8 章規定發布。

(2)本管理中心每天簽發 1 次憑證廢止清冊，公布於儲存庫。

(3)本管理中心本身之憑證，於簽發後 1 個工作天內公布於儲存庫。

(4) 線上即時憑證狀態之查詢，即時公布於儲存庫。

(5)簽發之憑證，於用戶接受時公布於儲存庫。

(6) 最近 1 次之稽核結果於稽核報告出具後 30 日內公布。

(7)本管理中心之最新訊息，不定期修訂。

(8)憑證政策於電子化政府主管機關核准後公布，後續修訂依照憑證政策第 8 章規定發布。

(9)本管理中心隱私權保護政策，每年定期評估是否進行修訂，修訂後經本部核准後 30 日內公布。

2.6.3 存取控制

本管理中心之主機建置於防火牆內部，除本管理中心授權的註冊中心伺服器外，不允許外界直接連線到本管理中心之主機。儲存庫之主機在防火牆系統控管下，連線至本管理中心之資料庫，擷取憑證資訊或下載憑證。

有關 2.6.1 節本管理中心公布的資訊，主要提供用戶或信賴憑證者查詢之用，因此開放閱覽存取，同時為保障儲存庫之安全，將進行存取控制，並維持其可接取狀態及可用性。

2.6.4 儲存庫

儲存庫由本管理中心負責管理，如因故無法正常運作，將於 1 個工作天內恢復正常運作，儲存庫之網址為(http：//hca.nat.gov.tw/)。

2.7 稽核方法

2.7.1 稽核之頻率

本管理中心接受每年 1 次本基礎建設的外部稽核與至少 1 年 1 次的內部稽核，以確認相關運作符合本作業基準規定。

2.7.2 稽核人員之身分及資格

由電子化政府主管機關依政府採購法委外辦理本基礎建設憑證機構之外部稽核作業，委託熟悉本基礎建設相關規定及本管理中心運作之稽核業者，提供公正客觀的稽核服務，本管理中心於稽核時應對

稽核人員進行身分識別。

2.7.3 稽核人員中立性之確保

配合電子化政府主管機關辦理本基礎建設憑證機構之外部稽核作業，將委託稽核業者就本管理中心的運作進行稽核。

2.7.4 稽核之範圍

(1) 本管理中心是否遵照本作業基準運作。

(2) 本作業基準是否符合憑證政策之規定。

(3) 註冊中心是否遵照本作業基準及相關規定運作。

(4) 卡管中心是否遵照本作業基準及相關規定運作。

2.7.5 對於稽核結果之因應方式

如稽核人員發現本管理中心或註冊中心之建置與維運不符合憑證政策及本作業基準等規定時，採取以下行動：

(1) 紀錄不符合情形。

(2) 將不符合情形通知本管理中心。

(3) 對於不符合規定之項目，本管理中心將立即改善，通知原稽核人員進行複核。

(4) 依據不符合情形之種類、嚴重性及修正所需時間，本管理中心將採取暫停營運、廢止簽發給用戶憑證或其他配合行動。

2.7.6 稽核結果公開之範圍及方法

本管理中心將公布最近 1 次的稽核結果於儲存庫，稽核結果除可能導致本管理中心系統被攻擊之資訊外，與信賴憑證者相關資訊均將公布。

2.8 資訊保密之範圍

2.8.1 機密之資訊種類

以下由本管理中心產生、接收或保管之資料，均視為機密資訊。

(1) 用於本管理中心營運的私密金鑰及通行碼。

(2) 本管理中心金鑰分持的保管資料。

(3) 用戶憑證之申請資料與資訊(包括申請單位及連絡人之姓名、電子郵件信箱、通訊地址及電話等)，未經用戶同意或符合法令規定，本管理中心不得公開或提供第 3 人使用。

(4) 申請時填寫於相關申請單（網頁）上的資訊，與身分證明文件（或影印本）上的隱密性資訊。

(5) 本管理中心產生或保管之可供稽核及追蹤之紀錄。

(6) 稽核人員於稽核過程中產生之稽核紀錄及報告，不得被完整公開。

(7) 列為機密等級的營運相關文件。

(8) 本管理中心之現職、離職及退職與人員對於機密資訊均負保密責任。

2.8.2 非機密之資訊種類

(1) 儲存庫公布之簽發憑證、已廢止憑證及憑證廢止清冊不視為機密資訊。

(2) 識別資訊或記載於憑證的資訊，除特別約定外，不視為機密資訊。

(3) 憑證有效性狀態、憑證資訊、憑證政策及憑證實務作業基準等，不視為機密資訊。

2.8.3 憑證廢止或暫時停用資訊之公開

憑證廢止或暫時停用資訊公布於儲存庫。

2.8.4 應司法機關等要求釋出資訊

司法機關、監察機關或治安機關如因調查或蒐集證據需要，必須查詢 2.8.1 節機密資訊，依法定程序辦理，不對用戶另作通知；惟本管理中心保留向申請查詢之機關收取合理費用之權利。

2.8.5 應用戶要求釋出資訊

用戶得以申請之憑證及私密金鑰，線上查詢 2.8.1 節第(3)款本身之憑證申請資料;惟本管理中心保留向申請查詢之用戶收取合理費用之權利。

2.8.6 其他資訊釋出之情況

不提供商業應用，至於其他資訊之釋出依相關規定法令辦理。

2.8.7 隱私權保護

本管理中心依照個人資料保護法處理用戶之申請資料。個人電子郵件位址由用戶自行決定是否要記載於憑證，同時用戶得自行決定是否公布其憑證於本管理中心儲存庫，以保障申請民眾之個人資料隱私。

2.9 權利歸屬

本管理中心的金鑰對與金鑰分持之財產權屬於本部。醫事機構、醫事人員憑證用戶使用之符記須符合 6.2.1 節規範，由本管理中心代為產製金鑰對，該金鑰對之財產權屬於該醫事人員、醫事機構。伺服

器應用軟體憑證及非以 IC 卡為載體之醫事人員及醫事機構憑證之金鑰對由憑證用戶自行產製，該金鑰對之財產權屬於該憑證申請單位。

本管理中心所簽發的憑證及憑證廢止清冊之著作權為本部所有。

本管理中心將儘可能確保用戶名稱的正確性，但不保證用戶名稱之智慧財產權歸屬。用戶名稱如發生註冊商標爭議時，用戶應依法定程序處理，並將處理結果提交本管理中心，以確保權益。

本作業基準之智慧財產權為本部擁有，本作業基準可由儲存庫自由下載，或依著作權法相關規定重製或散布，同時必須保證是完整複製，並註明著作權為本部所擁有。另外，重製或散布本作業基準者，不得向他人收取費用，亦不得拒絕任何人請求取得。本部對於不當使用或散布本作業基準引發之一切結果，不負任何法律責任。

因執行本管理中心之憑證管理作業而產生的資訊及相關文件，如使用手冊、說明文件、簡報資料與產生之資料庫檔案及客製化應用軟體等，其智慧財產權為本部所擁有。

3 識別和鑑別程序

3.1 初始註冊

3.1.1 命名種類

本管理中心所簽發憑證之憑證主體名稱採用X.500唯一識別名稱(Distinguished Name, DN)。

3.1.2 命名須有意義

本管理中心憑證主體名稱必須符合醫事與醫療相關法規資格，登錄核准於本部醫事管理系統資料庫之名稱，作為憑證用戶唯一識別名稱。

伺服器應用軟體憑證之唯一識別名稱包括憑證主體名稱(醫事機構的 X.500 Name)、通用名稱(Common Name)，伺服器應用軟體的名稱(可能是伺服應用軟體之網域名稱、網路位址或其他文字名稱)及序號(Serial Number，本管理中心對伺服應用軟體所編訂的識別代號)。

3.1.3 命名形式之解釋規則

依據本基礎建設憑證及憑證廢止清冊格式剖繪，各式命名形式的解釋規則依 ITU-TX.520 名稱屬性定義。

3.1.4 命名之獨特性

本管理中心的 X.500 唯一識別名稱原為：

C=TW，O=行政院，OU=醫事憑證管理中心。

為便於與國際互通，本管理中心自民國 107 年 8 月 18 日起，新簽發憑證的 X.500 唯一識別名稱使用以下格式：

C=TW，O=行政院，CN=醫事憑證管理中心 – Gn

其中，n=2,3…

為使本管理中心所簽發憑證的憑證主體名稱具備獨特性，本管理中心採用以下名稱格式：

(1) 醫事人員憑證

C=TW

CN=本部醫事管理系統資料庫依照醫事證書登記所儲存的中文姓名

serialNumber=本管理中心自動給定對該用戶的唯一序號

(2) 醫事機構憑證

A.中央政府衛生行政機關/醫務單位，中央政府醫事機構/醫務單位

C=TW

O=機關(構)的法定名稱

OU=附屬機關(構)的法定名稱(選擇性欄位，可以有多層)

B.地方政府衛生行政機關/醫務單位，地方政府醫事機構

C=TW

L=縣市名稱(選擇性欄位，只適用於地方政府)

O=機關(構)的法定名稱

OU=附屬機關(構)的法定名稱(選擇性欄位，可以有多層)

dnQualifier =本管理中心自動給定對該機構的唯一識別碼(選擇性欄位)

C.學校附設醫務單位

C=TW

L=縣市名稱(選擇性欄位，只適用於地區性學校)

L=鄉鎮市區名稱(選擇性欄位，只適用於地區性學校)

O=學校的正式登記名稱

OU=附屬學校的正式登記名稱(選擇性欄位，只適用於附屬學校)

OU=附設醫務單位的正式登記名稱

dnQualifier =本管理中心自動給定對該機構的唯一識別碼(選擇性欄位)

D.學校附設醫事機構

C=TW

O=學校的正式登記名稱

OU=學校單位名稱

OU=醫事機構的正式登記名稱(選擇性欄位)

OU=附設醫事機構的正式登記名稱(選擇性欄位，只適用於醫事機構的附設醫事機構)

E.財團法人附設醫事機構

C=TW

O=財團法人的正式登記名稱

OU=醫事機構的正式登記名稱

OU=附設醫事機構的正式登記名稱(選擇性欄位，可以有多層，只適用於醫事機構的附設醫事機構)

F.醫療財團法人機構

C=TW

O=財團法人的正式登記名稱

OU=醫事機構的正式登記名稱(選擇性欄位，可以有多層，只適用於醫事機構的附設醫事機構)

G.醫療社團法人機構

C=TW

O=社團法人的正式登記名稱

OU=醫事機構的正式登記名稱(選擇性欄位，可以有多層，只適用於醫事機構的附設醫事機構)

H.公司/法人附設醫事機構/醫務單位

C=TW

O=公司的正式登記名稱

OU=醫事機構/醫務單位的正式登記名稱(選擇性欄位，可以有多層)

I.分公司附設醫事機構/醫務單位

C=TW

O=公司的正式登記名稱

OU=分公司的正式登記名稱

OU=醫事機構/醫務單位的正式登記名稱(選擇性欄位，可以有多層)

J.醫事相關自由職業事務所

C=TW

L=縣市名稱

O=自由職業事務所的正式登記名稱

OU=醫事機構的正式登記名稱(選擇性欄位，可以有多層，只適用於醫事/醫事機構的附設機構)

dnQualifier =本管理中心自動給定對該機構的唯一識別碼(選擇性欄位)

(3) 伺服器應用軟體憑證

醫事機構的 X.500 Name

CN=伺服器應用軟體的名稱(可能是伺服應用軟體之網域名稱、網路位址或其他文字名稱)

serialNumber=伺服器應用軟體的識別代號

3.1.5 命名爭議之解決程序

如發生用戶名稱所有權爭議時，一律根據本部所登錄之醫事管理系統資料庫為準，由本部負責解決。

如有名稱重複之情形，本管理中心會以在唯一識別名稱中的序號加以區別，以使用戶的名稱可以保持唯一性。

但是當自動給定的序號發生重複時，本管理中心會以人工給定的方式，而保持序號的唯一，以解決命名爭議的問題。

3.1.6 商標之辨識、鑑別及角色

當憑證主體名稱可能包含商標時，其命名必須符合我國商標法、公平交易法及相關法規之規定，商標之辨識及鑑別非本管理中心管轄範圍，如名稱有爭議，用戶應透過相關法令規定之救濟機制處理。

3.1.7 證明擁有私密金鑰之方式

(1) 醫事人員、醫事機構 IC 卡類憑證

由本管理中心之卡管中心驅動 IC 卡，在 IC 卡內部自行產製金鑰對，簽發憑證時由卡管中心透過安全管道將用戶之公開金鑰傳送至本管理中心，因此用戶在申請憑證時不必證明持有私密金鑰。

(2) 伺服器應用軟體憑證及非IC卡載體之醫事人員及醫事機構憑證由用戶自行產製金鑰對，然後使用金鑰對產生 PKCS#10 憑證申請檔並加以簽章，並於申請憑證時將該憑證申請檔交給註冊中心，註冊中心將使用該用戶的公開金鑰驗證該憑證申請檔的簽章，以證明用戶擁有相對應的私密金鑰。

3.1.8 組織身分鑑別程序

3.1.8.1 醫事機構憑證

醫事機構用戶申請憑證時，必須將憑證申請書(包含機構名稱及

地址等)與機構開業執照影本以正式公文書方式函送註冊中心或至註冊窗口申辦，申請書記載該機構之正式登記名稱及識別代碼等資料，蓋用機構之印鑑章；註冊中心將依據本部醫事系統之資料進行比對確認，並以機構於醫事系統登記時之聯繫資料，進行電話聯繫，確認該機構確實存在與提出憑證之申請，並驗證公文書之真確性；註冊窗口將驗證醫事機構開業證件內容與確認該機構確實存在。

醫事機構憑證用戶申請機構憑證之附卡時，除上述以公文書申請方式外，如用戶已取得正卡，亦可採線上申請方式辦理，註冊中心將檢驗正卡之數位簽章以鑑別用戶之身分。製卡完成後將以機構原開業登記之地址寄送。

3.1.8.2 各項醫事機構憑證線上辦理之管理

本管理中心有3項醫事機構憑證線上辦理作業，其作業的身分鑑別方式分別規範如下：

(1) 線上暫時停用憑證

以用戶所自行選定的用戶代碼來做為身分鑑別的依據。

(2) 緊急暫時停用憑證

以傳真相關機構證明的文件或線上核對資料做為身分鑑別的依據。

(3) 線上恢復使用憑證

以用戶所自行選定的用戶代碼來做為身分鑑別的依據。

3.1.9 個人身分鑑別程序

3.1.9.1 初次申請憑證

申請人初次申請憑證應攜帶附照片之身分證件正本與醫事人員資格證書正本，親臨註冊窗口辦理。

註冊窗口核對身分證件正本與醫事人員資格證書正本是否為本人後，應向本部醫事系統資料庫查驗此身分所記錄的人員是否確實為該申請人。

若申請人無法於註冊窗口辦理，可以用委託書委任代理人行之，然代理人之身分應依前項所述之機制鑑別身分；註冊窗口審驗人員應先核對代理人身分證件正本與委託書，並核對申請人身分證件影本與醫事人員資格證書影本，以本部醫事系統資料庫所記載之申請人聯絡資料，使用電話、書面或其他適當之方式向申請人確認是否委託代理人申請。製卡完成後將以申請人原登記之地址寄送。

3.1.9.2 各項醫事人員憑證線上辦理之管理

本管理中心醫事人員憑證線上辦理作業，其作業的身分鑑別方式分別規範如下：

(1) 線上暫時停用憑證

以用戶所自行選定的用戶代碼來做為身分鑑別的依據。

(2) 緊急暫時停用憑證

以傳真相關身分證明的文件或線上核對資料做為身分鑑別的依據。

(3) 線上恢復使用憑證

以用戶所自行選定的用戶代碼來做為身分鑑別的依據。

(4)行動裝置申請憑證

授權醫事機構單位之行動化裝置，以用戶之正卡做為身分鑑別的依據。

3.1.10 硬體裝置或伺服軟體鑑別之程序

伺服器應用軟體憑證用戶申請須將申請書(包含申請機構/單位、伺服器識別名稱、伺服器IP位址、申請人身分證字號、申請人姓名、電子郵件、聯絡電話、聯絡地址等)以正式公文書方式函送註冊中心，申請書記載該機構之正式登記名稱及識別代碼等資料，並蓋用機構/單位之印鑑章。註冊中心將依據本部醫事系統之資料進行比對確認，並以機構於醫事系統登記時之聯繫資料，進行電話聯繫，確認該機構確實存在與提出憑證之申請，並驗證公文書之真確性，針對伺服器應用軟體憑證(SSL Certificate) 加以確認主機網域名稱確實存在且屬該機構所註冊。如用戶已取得醫事機構正卡，亦可採線上申請方式辦理，註冊中心將檢驗正卡之數位簽章以鑑別用戶之身分。

3.1.11 寫入憑證內之電子郵件驗證

本管理中心所簽發憑證，目前憑證不提供寫入電子郵件信箱資料之服務。

3.1.12 網域名稱擁有者識別程序

用戶申請伺服器應用軟體憑證(SSL Certificate)時，憑證管理中心須依照第 3.1.8 節之「一般申請」程序，鑑別該組織真確性；另應使用以下方式查詢該申請之主機網域名稱確實存在且屬該申請者所註

冊擁有：

- 政府 WHOIS 主機-政府中英文網域名稱註冊系統 (https://rs.gsn.gov.tw)
- TWINC Whois Database (http:// whois. twnic.net.tw)

3.2 憑證之金鑰更換及展期

3.2.1 憑證之金鑰更換

憑證之金鑰更換係指簽發1張與舊憑證具有相同特徵及保證等級的新憑證，而新的憑證除有新的、不同的公開金鑰(對應新的、不同的私密金鑰)及不同的憑證序號外，亦可能被指定不同的有效期限。

如用戶之私密金鑰使用期限屆滿必須更換金鑰時，應可使用有效的私密金鑰簽章進行申請，或依照 3.1 節規定，對於重新申請憑證之用戶進行識別及鑑別。

3.2.2 憑證展期

本管理中心所簽發憑證，有效期限與6.3.2.2節規定之用戶公開金鑰最長使用期限相同，目前不提供展期，展期之相關規定如有變更，將依程序修訂本作業基準送交主管機關經濟部核定後公告辦理。

3.3 憑證被廢止之金鑰更換

如用戶之私密金鑰 因憑證廢止必須更換金鑰時，應重新申請憑證，註冊中心將依照 3.1 節規定，對於重新申請憑證之用戶進行識別及鑑別。

3.4 憑證廢止

廢止憑證請求時之識別及鑑別程序與 3.1 節規定相同。

4.營運規範

4.1 申請憑證之程序

申請人應先閱讀醫事憑證用戶同意書，如同意條款內容再進行憑證申請。

此同意書會記載於在本管理中心的網站(http://hca.nat.gov.tw/)及憑證申請書中。

4.1.1 憑證申請

(1) 醫事人員憑證申請

醫事人員憑證之申請方式有以下兩種：

A.方式一：

- 憑證申請人連線至本管理中心網站(http://hca.nat.gov.tw/)，閱讀醫事憑證用戶同意書，如同意條款內容則填寫及列印憑證申請書，並設定用戶代碼。
- 依照 3.1.9 節的規定，將申請書送至註冊窗口辦理。

B.方式二：

- 申請人或受其委託之代理人直接至註冊窗口填寫申請書辦理。

(2) 醫事機構憑證正卡申請

醫事機構憑證之正卡申請程序如下：

A.醫事機構指派適當人員，代表該機構申請憑證。

B.憑證申請人連線至本管理中心網站(http://hca.nat.gov.tw/)，閱讀醫事憑證用戶同意書，如同意條款內容則填寫憑證申請書，並設定用戶代碼。

C.至註冊窗口申辦或將憑證申請書以公文書方式函送註冊窗口辦理。

(3) 醫事機構憑證附卡申請

醫事機構憑證之附卡申請程序如下：

A. 採用如4.1.1節第(2)項醫事機構憑證正卡的申請程序。

B.採用線上申請方式，使用醫事機構數位簽章，進行身分鑑別，申請程序如下：

(A)憑證申請人連線至本管理中心網站(http://hca.nat.gov.tw/)，閱讀醫事憑證用戶同意書，選擇同意條款內容，進行設定用戶代碼。

(B)以醫事機構憑證之正卡對附卡之憑證申請資料加簽數位簽章後，將相關資料上傳至註冊中心。

(4) 伺服器應用軟體憑證及非IC卡載體之醫事人員與醫事機構憑證申請

A.由申請之醫事機構之所有人或經授權之使用人，代表申請憑證。

B.由憑證申請人自行產製金鑰對，然後使用金鑰對產生PKCS#10憑證申請檔並加以簽章。

C.憑證申請人連線至本管理中心網站(http://hca.nat.gov.tw/)，閱讀醫事憑證用戶同意書，如同意條款內容則填寫憑證申請書及設定用戶代碼，並將PKCS#10憑證申請檔上傳。

D.將憑證申請書以公文書方式函送註冊中心辦理。

E.採用線上申請方式，連線至本管理中心網站(http://hca.nat.gov.tw/)，在同意條款內容，使用伺服器軟體憑證或非IC卡載體醫事人員及醫事機構憑證申請資料加簽數位簽章後，將相關資料上傳至註冊中心。

用戶應提供正確之憑證申請資料，本管理中心及註冊中心將依本作業基準之規定妥善保管用戶相關資料。

4.1.2 憑證內容變更時之憑證申請

憑證用戶如有變更個人的姓名、國民身分證統一編號、醫事機構名稱、醫事機構代碼等資料時，用戶如欲再取得有效的憑證，則需以變更後的資料進行憑證的重新申請。在申請之前，必須依 4.4.3 節的規定先將原憑證做廢止，然後再依 4.1.1 節的規定申請新的憑證。

4.1.3 憑證遺失時之憑證申請

若用戶曾持有憑證，但是因為遺失或損毀而無法使用，可申請新的憑證。在申請之前，必須依 4.4.3 節的規定先將遺失或損毀之憑證做廢止，然後再依 4.1.1 節的規定申請新的憑證。

4.2 簽發憑證及通知憑證已簽發之程序

註冊中心在收到憑證申請資料後，將依本作業基準第 3 章規定，進行以下審核程序，以作為決定是否同意簽發憑證之依據。

4.2.1 醫事人員憑證

由以下的步驟完成憑證的簽發：

1. 用戶使用之符記為 IC 卡:

(1) 註冊窗口確認憑證申請人之身分資料後，便將憑證申請書的資料(含用戶代碼)輸入/轉入註冊窗口系統中。
(2) 註冊窗口系統將相關憑證申請資料透過安全管道傳送至註冊中心。
(3) 註冊中心進行申辦資料覆核後，透過安全管道傳送至本管理中心簽發憑證。
(4) 本管理中心簽發憑證並同時傳送請求檔至卡管中心進行製卡作業，製卡作業包括 IC 卡內部產製金鑰對、以亂碼設定 IC 卡之初始 PIN 碼、將憑證寫入 IC 卡中及印卡等工作。
(5) 製卡完成後，卡管中心將 IC 卡郵寄給用戶。

2. 用戶使用其他符記:

(1) 線上申請軟體憑證，使用機構憑證與人員憑證之數位簽章進行申請者，則由註冊中心以線上驗證之數位簽章方式辦理。

(2)經註冊中心複核或驗證通過之憑證申請資料將透過安全管道傳送給本管理中心，本管理中心在簽發憑證後，將以超文件傳輸協定或電子郵件方式傳送給用戶。

4.2.2 醫事機構憑證正卡及伺服器應用軟體憑證

醫事機構憑證正卡及伺服器應用軟體憑證之簽發審核程序如下：

(1) 註冊窗口審驗人員或註冊中心檢查憑證申請書、申請醫事機構資格(未開業機構不能申請)及公文的真偽。

(2) 註冊窗口審驗人員檢查憑證申請書之資料,如資料正確無誤，將憑證申請書的資料輸入/轉入註冊窗口系統中透過安全管道傳送給註冊中心。

(3) 註冊中心進行申辦資料覆核後，透過安全管道傳送至本管理中心簽發憑證。

(4) 如採線上申請伺服器應用軟體憑證，使用機構憑證之數位簽章進行申請者，則由註冊中心以線上驗證之數位簽章方式辦理。

(5) 因用戶使用之符記不同分成以下兩種程序：

A.如用戶使用之符記為 IC 卡：

本管理中心簽發憑證並同時傳送請求檔至卡管中心進行製卡作業，製卡作業包括 IC 卡內部產製金鑰對、以亂數設定 IC 卡之初始 PIN 碼、將憑證寫入 IC 卡中及印卡等工作。卡管中心將 IC 卡郵寄給用戶。

B.如用戶使用其他符記：

經註冊中心複核或驗證通過之憑證申請資料將透過安全管道傳送給本管理中心，本管理中心在簽發憑證後，將以電子郵件方式傳送給用戶。

4.2.3 醫事機構憑證附卡

憑證附卡之簽發審核方式有以下兩種：

(1) 如採與憑證正卡相同申請程序者，簽發審核程序比照上述憑證正卡之程序。

(2) 如採線上申請方式者，註冊中心將檢驗機構憑證 IC 卡正卡對憑證附卡申請資料所簽之數位簽章方式辦理。

對於未通過以上簽發審核程序之醫事機構，本管理中心將拒絕簽發憑證，同時對於醫事機構不負任何損害賠償責任。

4.3 接受憑證及公布憑證之程序

憑證用戶取得憑證與簽發結果通知後，應查驗下列事項：

(1) 憑證內所載之用戶名稱與註冊申請之內容相符，且同意使用該名稱。

(2) 如使用之符記為 IC 卡，在完成 IC 卡開卡作業後，即表示接受憑證，相關程序如下：

A.連線至本管理中心網站(http://hca.nat.gov.tw/)，進行開卡作業。

B.檢查憑證內容，如資料正確無誤，則輸入申請憑證時所設定之用戶代碼，以執行 IC 卡開卡，在完成開卡後，即表示接受憑證，卡管中心將以亂數設定 IC 卡之初始 PIN 碼。如憑證內容不正確，則應停止開卡作業。

(3) 如使用其他符記，接受憑證之程序如下：

A.連線至本管理中心網站(http://hca.nat.gov.tw/)。

B.檢查憑證內容，如資料正確無誤，則輸入憑證序號及申請憑證時所設定之用戶代碼，以執行憑證接受作業。如憑證內容不正確，則應停止憑證接受作業。

(4) 憑證用戶如有憑證內容變更之需求，需以變更後的資料進行憑證的重新申請，其接受憑證程序與相同。

(5) 完成憑證接受作業之憑證將公布至儲存庫。

(6) 憑證應於簽發後 90 個日曆天內，完成接受憑證。

於憑證簽發後 90 個日曆天內，未能完成接受憑證且無主動告知憑證中心事由,則視為拒絕接受憑證,該憑證將自動被停用，不另行公布。

4.4 憑證暫時停用及廢止

4.4.1 廢止憑證之事由

用戶在以下情形時(但不限)必須向註冊中心提出廢止憑證申請：

(1) 懷疑或證實私密金鑰外洩、遺失或遭受冒用、偽造、破解。

(2) 憑證所記載之內容重大改變，足以影響其信賴度。例如用戶之唯一識別名稱變更，包括用戶的名稱變更：或醫事機構憑證用戶其機構遭撤銷登記、註銷登記、歇業或解散等情形。

(3) 憑證不再需要使用

本管理中心得就下列情形逕行廢止憑證，毋須事先經過用戶同意。

(1) 確認憑證記載之內容不實。

(2) 確認用戶之簽章用私密金鑰外洩、遺失或遭受冒用、偽造、

破解。

(3) 憑證用戶經證實有不法行為或其他危及本管理中心運作之情事時，本管理中心有權廢止憑證用戶之憑證。

(4) 憑證所記載之憑證用戶資訊必須變更時，本管理中心保留考慮廢止該憑證之權力。

(5) 本管理中心依照規定終止服務。

(6) 確認本管理中心之私密金鑰外洩、遺失或遭受冒用、偽造、破解或系統遭受冒用、偽造或破解，足以影響憑證之信賴度。

(7) 確認用戶之憑證未依本作業基準規定之程序簽發。

(8) 確認用戶違反本作業基準或相關法令規定。

(9) 依據司法機關之通知。

(10) 依據用戶之主管機關之通知。

4.4.2 憑證廢止之申請者

(1) 欲廢止憑證之用戶。

(2) 依正式公文辦理的司法機關。

(3) 用戶之主管機關。

4.4.3 憑證廢止之程序

(1) 醫事人員憑證

A. 醫事人員憑證廢止用戶可連線至本管理中心網站(http://hca.nat.gov.tw/)，閱讀用戶約定條款(Subscriber Agreement)，如同意條款內容則填寫憑證廢止申請書。

B. 至註冊窗口辦理，用戶提出被認可身分證明與廢止申請書，註冊窗口在收到憑證申請資料後，將依本作業基準第3 章規定，進行身分鑑別程序，以作為判定是否同意廢止憑證

之依據。

C. 如資料正確無誤，將相關資料上傳至註冊中心

D. 經註冊窗口審驗人員檢查通過之憑證廢止申請資料將由本管理中心廢止憑證。

(2) 醫事機構憑證

A. 由醫事機構指派適當人員申請憑證廢止。

B. 憑證廢止申請人連線至本管理中心網站(http://hca.nat.gov.tw/)，閱讀用戶約定條款，如同意條款內容則填寫憑證廢止申請書。

C. 將憑證廢止申請書以公文書方式函送註冊窗口辦理。

D. 註冊窗口在收到憑證廢止申請公文後，由註冊窗口審驗人員檢查憑證廢止申請公文的真偽。

E. 註冊窗口審驗人員檢查憑證廢止申請書之資料，如資料正確無誤，將相關資料上傳至註冊中心。

F. 經註冊窗口審驗人員檢查通過之憑證廢止申請資料將由本管理中心廢止憑證。

(3) 由於伺服器應用軟體在法律上不具任何行為能力。伺服器應用軟體憑證也僅支援醫事資訊電子化相關應用服務，一旦應用服務變更，重新申請新憑證即可。而舊有應用範圍之憑證即不再有效，不需執行廢止作業。

新廢止之憑證需在每 1 次預定發布廢止清冊時被列入，並在儲存庫上發布，列冊廢止之憑證將保留在每次發布之廢止清冊中。憑證廢止清冊之簽發頻率為每天 1 次，更新後之憑證廢止清冊公布於儲存

庫。

4.4.4 憑證廢止申請之處理期間

本管理中心自註冊窗口受理憑證廢止申請時起，將於 1 個工作天內完成憑證廢止處理程序。

4.4.5 暫時停用憑證之事由

用戶就以下情形得申請憑證之暫時停用：

(1) 儲存憑證相關資料之符記遺失、或懷疑外洩、遭冒用、偽造、破解。

(2) 自行認定必須申請憑證之暫時停用。

本管理中心就以下情形得逕行暫時停用憑證，毋須事先經過用戶同意：

(1)依據司法機關之正式公文通知。

(2)依據用戶主管機關之通知。

4.4.6 暫時停用憑證之申請者

(1)欲暫時停用憑證之用戶。

(2)依正式公文辦理的司法機關。

(3)用戶之主管機關。

4.4.7 暫時停用憑證之程序

用戶申請暫時停用憑證之程序如下：

(1) 醫事人員憑證

A. 連線至本管理中心網站(http://hca.nat.gov.tw/)，填寫IC卡號(使用之符記為IC卡時)或憑證序號(使用其他符記時)及用戶代碼，線上申請暫時停用憑證。

B. 註冊中心在檢驗IC卡之卡號及用戶代碼正確無誤後，上傳至本管理中心。

C. 本管理中心檢驗註冊中心上傳資訊後，進行暫時停用憑證作業。

D. 用戶如忘記用戶代碼，得至註冊窗口辦理暫時停用憑證，提出被認可之用戶身分證明，在註冊窗口依本作業基準第3章規定確認用戶身分後，由註冊窗口代為向本管理中心提出暫時停用憑證申請，得併同辦理重設用戶代碼。

E. 用戶如遺失憑證IC卡，也忘記用戶代碼，因時空限制，而無法利用上述程序之一辦理憑證暫時停用時，則得以緊急暫時停用憑證程序辦理。用戶須以傳真方式辦理緊急暫時停用憑證，檢附含有可鑑別身分之書面資料，並署名緊急聯絡電話與本人簽名。本管理中心收到傳真申請單後會以電話聯絡申請者，洽詢相關問題進行身分鑑別，以作為判定是否同意緊急暫時停用憑證之依據。相關細部程序與表單公布於本管理中心網站(http://hca.nat.gov.tw/)。

(2) 醫事機構憑證

A. 連線至本管理中心網站(http://hca.nat.gov.tw/)，填寫IC卡號(使用之符記為IC卡時)或憑證序號(使用其他符記時)及用戶代碼，線上申請暫時停用憑證。

B. 註冊中心在檢驗 IC 卡之卡號及用戶代碼正確無誤後，加簽數位簽章上傳至本管理中心。

C. 本管理中心檢驗註冊中心之數位簽章後，進行暫時停用憑證作業。

D. 用戶如忘記用戶代碼，得至註冊窗口辦理暫時停用憑證，提出被認可之身分證明，在註冊窗口依本作業基準第 3 章規定確認用戶身分後，由註冊窗口代為向本管理中心提出暫時停用憑證申請，得併同辦理重設用戶代碼。

E. 用戶如遺失憑證IC卡，也忘記用戶代碼，因時空限制而無法利用上述方式辦理憑證暫時停用時，則得以緊急暫時停用憑證程序辦理。用戶須以傳真方式辦理緊急暫時停用憑證，檢附含有可鑑別身分之書面資料。本管理中心收到傳真申請單後會以電話聯絡申請者，洽詢相關問題進行身分鑑別，以作為判定是否同意緊急暫時停用憑證之依據。相關細部程序與表單公布於本管理中心網站(http://hca.nat.gov.tw/)。

對於未通過以上暫時停用憑證申請審核程序者，本管理中心或註冊中心將拒絕暫時停用憑證。

4.4.8 暫時停用憑證之處理期間及停用期間

本管理中心自註冊窗口受理憑證暫時停用申請時起，將於 1 個工作天內完成憑證暫時停用處理程序。

用戶在申請暫時停用憑證時，不需申告預定暫時停用期間，本管理中心允許憑證暫時停用至憑證到期為止。

如用戶取消憑證暫時停用，即恢復使用憑證，則該憑證狀態恢復為有效的(Valid)。

4.4.9 恢復使用憑證之程序

用戶申請憑證恢復使用憑證之程序如下：

(1) 連線至本管理中心網站(http://hca.nat.gov.tw/)，填寫 IC 卡號(使用之符記為 IC 卡時)或憑證序號(使用其他符記時)及用戶代碼，線上申請恢復使用憑證。

(2) 註冊中心在檢驗 IC 卡之卡號及用戶代碼正確無誤後，上傳至本管理中心。

(3) 本管理中心檢驗註冊中心上傳資訊後，進行恢復使用憑證作業。

對於未通過以上恢復使用憑證申請審核程序者，本管理中心或註冊中心將拒絕恢復使用憑證。

4.4.10 憑證廢止清冊之簽發頻率

憑證廢止清冊之簽發頻率為每天 1 次，更新後之憑證廢止清冊公布於儲存庫。

4.4.11 憑證廢止清冊之查驗規定

信賴憑證者在使用本管理中心公布於儲存庫之憑證廢止清冊時，

應先檢驗其數位簽章，以確認該憑證廢止清冊是否正確。有關信賴憑證者查詢儲存庫公布資訊須具備之要件，詳見於 2.6.4 節之說明。

4.4.12 線上憑證狀態查詢服務

本管理中心提供線上憑證狀態(OCSP)查詢服務，相關說明請詳見儲存庫。

4.4.13 線上憑證狀態查詢之規定

如信賴憑證者無法依照 4.4.11 節之規定查詢憑證廢止清冊，則必須使用 4.4.12 節之線上憑證狀態查詢服務，檢驗所使用的憑證是否有效。

4.4.14 其他形式廢止公告

本管理中心不提供其他形式的廢止公告。

4.4.15 其他形式廢止公告之檢查規定

本管理中心不提供其他形式的廢止公告。

4.4.16 金鑰被破解時之其他特殊規定

依照 4.4.1、4.4.2 及 4.4.3 節的規定辦理。

4.5 安全稽核程序

本管理中心之安全相關事件，均具有安全稽核紀錄(Audit Log)。安全稽核紀錄採系統自動產生、工作紀錄本及紙張等方式。所有安全稽核紀錄均妥善保存，且在執行稽核時可立即取得。安全稽核紀錄之維護依照 4.6.2 節歸檔之保留期限規定辦理。

4.5.1 被記錄事件種類

(1) 安全稽核

- 任何重要稽核參數之改變，如稽核頻率、稽核事件型態、新舊參數的內容。
- 任何嘗試刪除或修改稽核紀錄檔。

(2) 識別與鑑別

- 嘗試新角色的設定不論成功或失敗。
- 身分鑑別嘗試的最高容忍次數改變。
- 使用者登入系統時身分鑑別嘗試的失敗次數之最大值。
- 如管理者將已被鎖住的帳號解鎖，而且該帳號是因為多次失敗的身分鑑別嘗試而被鎖住的。
- 管理者改變系統的身分鑑別機制，例如從通行密碼改為生物特徵值。

(3) 金鑰產製

- 本管理中心產製金鑰時(不包括只用在單次或只限 1 次使用的金鑰的產製)。

(4) 私密金鑰之載入和儲存

- 載入私密金鑰到系統元件中。
- 所有為進行金鑰回復的工作，對保存在本管理中心之私密金鑰所做的存取。

(5) 可信賴公開金鑰之新增、刪除及儲存

- 可信賴公開金鑰之改變，包括新增、刪除及儲存。

(6) 私密金鑰之輸出

- 私密金鑰之輸出(不包括只用在單次或只限 1 次使用之金鑰)。

(7) 憑證之註冊

- 憑證之註冊申請過程。

(8) 廢止憑證

- 憑證之廢止申請過程。

(9) 憑證狀態改變之核可

- 核可或拒絕憑證狀態改變之申請。

(10) 本管理中心組態設定

- 本管理中心安全相關之組態設定改變。

(11) 帳號之管理

- 加入或刪除角色和使用者。

- 使用者帳號或角色之存取權限修改。

(12) 憑證格式剖繪之管理

- 憑證格式剖繪之改變。

(13) 憑證廢止清冊格式剖繪之管理

- 憑證廢止清冊格式剖繪之改變。

(14) 其他

- 安裝作業系統。

- 安裝本管理中心系統。
- 安裝硬體密碼模組。
- 移除硬體密碼模組。
- 銷毀硬體密碼模組。
- 啟動系統。
- 嘗試登入本管理中心的憑證管理作業。
- 硬體及軟體之接收。
- 嘗試設定通行密碼。
- 嘗試修改通行密碼。
- 本管理中心之內部資料備份。
- 本管理中心之內部資料回復。
- 檔案操作(例如產生、重新命名及移動等)。
- 傳送任何資訊到儲存庫公布。
- 存取本管理中心之內部資料庫。
- 任何憑證被破解之申告。
- 憑證載入符記。
- 符記之傳遞。
- 符記之零值化。

- 本管理中心之金鑰更換。

(15) 本管理中心之伺服器設定改變

- 硬體。
- 軟體。
- 作業系統。
- 修補程式(Patches)。
- 安全格式剖繪。

(16) 實體存取及場所之安全

- 人員進出本管理中心之機房。
- 存取本管理中心之伺服器。
- 得知或懷疑違反實體安全規定。

(17) 異常

- 軟體錯誤。
- 軟體檢查完整性失敗。
- 接收不合適訊息。
- 非正常路由之訊息。
- 網路攻擊(懷疑或是確定)。
- 設備失效。
- 電力不當。

- 不斷電系統(UPS)失敗。
- 明顯及重大的網路服務或存取失敗。
- 憑證政策之違反。
- 本作業基準之違反。
- 重設系統時鐘。

4.5.2 紀錄檔處理頻率

本管理中心至少每兩個月檢視 1 次稽核紀錄，追蹤調查重大事件。檢視工作包括檢驗稽核紀錄是否被竄改、檢視所有的紀錄項目及檢查任何警示或異常等。檢視稽核紀錄之結果以文件紀錄。

4.5.3 稽核紀錄檔保留期限

稽核資料現場(on site)保留兩個月，並依照 4.5.4、4.5.5、4.5.6 及 4.6 節紀錄保留管理機制等相關規定辦理。

如稽核紀錄檔的保留期限屆滿，在稽核員的監督下，由維運人員負責移除。

4.5.4 稽核紀錄檔之保護

(1) 使用簽章、加密技術保存目前和已歸檔之稽核紀錄，並使用 DVD/VCD-R 或其他無法更改稽核紀錄的媒體儲存。

(2) 簽署事件紀錄的私密金鑰不能再使用於其他用途，嚴禁稽核系統之私密金鑰另作他用，稽核系統不可洩漏私密金鑰。

(3) 手動的稽核紀錄存放於安全場所。

4.5.5 稽核紀錄檔備份程序

電子式稽核紀錄每月至少備份 1 次。

(1) 本管理中心週期性地將事件紀錄備份，稽核系統將稽核軌跡資料以每日、每星期及每月等條件週期性地自動歸檔。

(2) 本管理中心將事件紀錄檔案存放於安全場所。

4.5.6 安全稽核系統

稽核系統內建於本管理中心系統。稽核程序在本管理中心系統啟動時啟用，唯有在本管理中心系統關閉時才停止。

如自動稽核系統無法正常運作，同時保護系統資料之完整性、機密性的安全機制處於高風險狀態時，本管理中心將暫停憑證簽發服務，直到問題解決再行提供服務。

4.5.7 對引起事件者之告知

如因發生事件而被稽核系統紀錄，稽核系統並不需要告知引起該事件的個體其所引發的事件已經被系統記錄。

4.5.8 弱點評估

(1) 作業系統的弱點評估。

(2) 實體設施的弱點評估。

(3) 憑證管理系統的弱點評估。

(4) 網路的弱點評估。

4.6 紀錄歸檔之方法

4.6.1 紀錄事件之類型

(1) 本管理中心被主管機關審查的 (Accreditation)資料。

(2) 憑證實務作業基準。

(3) 重要的契約。

(4) 系統與設備組態設定。

(5) 系統或組態設定修改與更新的內容。

(6) 憑證申請資料。

(7) 廢止申請資料。

(8) 憑證接受的確認紀錄。

(9) 符記啟用的紀錄。

(10) 已簽發或公告的憑證。

(11) 本管理中心金鑰更換的紀錄。

(12) 已簽發或公告的憑證廢止清冊。

(13) 稽核紀錄。

(14) 用來驗證及佐證歸檔內容的其它說明資料或應用程式。

(15) 稽核人員要求的文件。

(16) 依 3.1.8 節規定的組織身分鑑別資料。

(17) 依 3.1.9 節規定的個人身分鑑別資料。

4.6.2 歸檔之保留期限

本管理中心歸檔資料之保留期限為 10 年。用來處理歸檔資料的應用程式也將維護 10 年。

4.6.3 歸檔之保護

(1) 不允許新增、修改或刪除歸檔資料。

(2) 本管理中心可將歸檔資料移到另一個儲存媒體，並儲存於檔管中心，提供適當的保護，保護等級不低於原保護等級。

(3) 歸檔資料存放於安全場所。

4.6.4 歸檔備份程序

歸檔資料備份至異地備援中心(參閱 5.1.8 節)。

4.6.5 時戳紀錄之要求

歸檔之電子式紀錄(例如憑證、憑證廢止清冊及稽核紀錄等)包含日期與時間資訊，而且這些紀錄皆經過適當的數位簽章保護，可用以檢測紀錄中的日期與時間資訊是否遭到篡改。但是，這些電子式紀錄中的日期與時間資訊並非公正第三者所提供之電子式時戳資料，而是電腦作業系統的日期與時間。本管理中心的所有電腦系統都會定期進行校時，以確保電子式紀錄中日期與時間資訊的準確性與可信度。

歸檔的書面紀錄也將記載日期資訊，必要時並將記載時間資訊。書面紀錄的日期與時間紀錄不可任意更改。

4.6.6 歸檔資料彙整系統

本管理中心沒有歸檔資料之彙整系統。

4.6.7 取得及驗證歸檔資料之程序

必須以書面申請獲得正式授權後，才可取得歸檔資料。

由稽核員負責驗證歸檔資料，書面文件必須驗證文件簽署者及日期等之真偽，電子檔則需驗證歸檔資料的數位簽章。

4.7 金鑰更換

本管理中心之私密金鑰依照 6.3.2 節規定定期更換。本管理中心於私密金鑰到期前 2 個月，更換用來簽發憑證的金鑰對。更換金鑰對後，將向政府憑證總管理中心申請新的憑證。

用戶之私密金鑰必須依照 6.3.2 節規定定期更換。如用戶之私密金鑰使用期限屆滿必須更換金鑰時，應依照 4.1 節規定向本管理中心申請新的憑證。

4.8 金鑰遭破解或災變時之復原程序

4.8.1 電腦資源、軟體或資料遭破壞之復原程序

本管理中心訂定電腦資源、軟體及資料遭破壞之復原程序，同時每年進行演練。

如本管理中心的電腦設備遭破壞或無法運作，但本管理中心的簽章金鑰並未被損毀，則優先回復儲存庫之運作，並迅速重建憑證簽發及管理的能力。

4.8.2 醫事憑證管理中心之簽章金鑰憑證被廢止之復原程序

如因災害事件嚴重，致本管理中心本身的憑證必須被廢止時，本管理中心將公告於儲存庫及通知用戶，並依照 4.7 節之程序產生新的金鑰對，將新的憑證公告於儲存庫，供用戶及信賴憑證者下載。

本管理中心訂定簽章金鑰憑證被廢止之復原程序，同時每年進行演練。

4.8.3 醫事憑證管理中心之簽章金鑰遭破解之復原程序

如本管理中心簽章金鑰遭破解時，採取以下復原程序：

(1) 公告於儲存庫，並通知用戶。

(2) 廢止本管理中心簽章金鑰憑證及所簽發之用戶憑證。

依照 4.7 節之程序產生新的金鑰對，將新的憑證公告於儲存庫，供用戶及信賴憑證者下載。

本管理中心訂定簽章金鑰遭破解之復原程序，同時每年進行演練。

4.8.4 醫事憑證管理中心安全設施之災後復原工作

本管理中心訂定災害復原之程序，同時每年進行演練，當發生災害時，將由緊急應變小組啟動災害復原程序，優先回復儲存庫之運作，並迅速重建憑證簽發及管理的能力。

4.9 醫事憑證管理中心之終止服務

本管理中心終止服務時，將依據電子簽章法相關規定辦理。

本管理中心遵守以下事項，以確保終止服務對於用戶與信賴憑證者造成之影響最小：

(1) 本管理中心於預定終止服務 3 個月前，將通知所有未廢止及未過期憑證之用戶（無法通知者，不在此限），並公告於儲存庫。

(2) 憑證管理中心於預定終止服務 3 個月前，應通知電子簽章法主管機關（經濟部）；將終止服務之事實公告於儲存庫。

(3) 憑證管理中心終止服務時將採如下措施：

- 停止簽發新的憑證。
- 終止當時仍具效力之憑證，將於儲存庫繼續提供憑證廢止清冊之服務，直到所有用戶憑證效期到期為止。
- 由政府公開金鑰基礎建設各適當之憑證機構承接各類憑證相關業務，若該類憑證無適當之憑證機構可承接，電子簽章法主管機關得安排其他憑證機構承接。
- 將所有營業期間之紀錄檔案，移交給承接此業務之其他憑證機構。
- 電子簽章法主管機關於必要時，得公告廢止當時仍具效力之憑證。

5.非技術性安全控管

5.1 實體控管

5.1.1 實體所在及結構

本管理中心機房位於衛生福利部機房，符合儲存高重要性及敏感性資訊的機房設施水準，並具備門禁、保全、入侵偵測及監視錄影等實體安全機制，以防止未經授權存取本管理中心之相關設備。

5.1.2 實體存取

本管理中心以保證等級第 3 級的實體控管規定運作。機房共有 4 層門禁，第 1 層和第 2 層分別為衛生福利部全年無休的大門及大樓警衛，第 3 層為機房管理人員執行進出管制，第 4 層為機房人員辨認與門禁密碼磁卡進出系統。

除門禁系統可限制不相干人員接近機房外，機房之監控系統可監控機房之開啟，以防止未經授權存取硬體、軟體和硬體密碼模組等相關設備。

任何可攜式儲存媒體帶進機房，需檢查並確認沒有電腦病毒及任何可能危害本管理中心系統的惡意軟體。

非本管理中心人員進出機房，需填寫進出紀錄，並由本管理中心相關人員全程陪同。

本管理中心相關人員離開機房時，將進行以下之查驗工作並記錄，以防止未授權人員進入機房：

(1) 確認設備是否正常運作。

(2) 確認機箱門是否關閉。

(3) 確認門禁系統是否正常運作。

5.1.3 電力及空調

本管理中心機房的電力系統，除市電外，另設有發電機(滿載油料可連續運轉 4 小時以上，當實際發生市電中斷供應後，指定人員會視情況即時請供應商補充原料，以達持續運作)及不中斷電源系統(UPS)可提供至少 30 分鐘以上備用電力，並具有市電及發電機的電源自動切換功能，供儲存庫備援資料。

本管理中心機房設有恆溫空調系統，以控制環境的溫度及濕度，使機房保持最佳運作環境。

5.1.4 水災防範及保護

本管理中心機房設置在基地墊高的建築物第 3 樓層以上，該建築物並有防水閘門和抽水機，且沒有因為水災造成重大損害紀錄。

5.1.5 火災防範及保護

本管理中心機房具備自動偵測火災預警功能，系統可自動啟動滅火設備，並設置手動開關於各機房主要出入口，以供現場人員於緊急情況時以手動方式啟動。

5.1.6 媒體儲存

稽核紀錄、歸檔和備援資料的儲存媒體於本管理中心機房儲存半年，半年後將移到異地備援場所儲存。

5.1.7 廢料處理

2.8.1 節所述之本管理中心機密資訊，文件資料部分在不需使用時，將經碎紙機處理；磁帶、硬碟、磁碟、磁光碟(MO)及其他形式的記憶體，在報廢前，將經格式化程序清除儲存的資料，光碟將被實

體銷毀。

5.1.8 異地備援

異地備援的地點在台中，與本管理中心機房距離 30 公里以上。備援的內容包括資料與系統程式，全部資料備份 1 個星期至少執行 1 次，異動資料備份於異動當天執行。異地備援系統與本管理中心系統具有相同的安全等級。

5.2 程序控制

本管理中心經由作業程序控管(Procedural Controls)，以規定執行系統相關作業的各種可信賴角色(Trusted Role)、每項工作的人員需求數及每個角色的識別與鑑別，以確保系統作業程序之安全。

5.2.1 信賴角色

本管理中心為使執行系統相關作業的責任，能做適當的區隔，以防止某人惡意使用系統而不被察覺，對於每項系統存取作業，明確規定那些信賴角色才能執行此項作業。

本管理中心共有 5 種不同的信賴角色，分別為管理員(Administrator)、簽發員(Officer)、稽核員(Auditor)、維運員(Operator)和實體安全控管員(Controller)，每種信賴角色將依照 5.3 節規定進行人員控管，以防止可能的內部攻擊。每一種信賴角色可由多人擔任，每種信賴角色設有 1 名主管(Chief Role)，5 種信賴角色的工作內容說明如下：

(1)管理員負責：

- 安裝、設定和維護本管理中心系統。

- 建立和維護本管理中心系統之使用者帳號。
- 設定稽核參數。
- 產製和備份本管理中心之金鑰。

(2)簽發員負責：

- 啟動或停止憑證簽發服務。
- 啟動或停止憑證廢止服務。

(3)稽核員負責：

- 對稽核紀錄的查驗、維護和歸檔。
- 執行或監督內部的稽核，以確認本管理中心運作是否遵照本作業基準的規定。

(4)維運員負責：

- 系統設備的日常運作維護。
- 系統的備援及復原作業。
- 儲存媒體的更新。
- 除本管理中心憑證管理系統外之軟硬體更新。
- 網路及網站的維護：建置系統安全與病毒防護機制及網路安全事件的偵測與通報等。

(5)實體安全控管員負責：

- 系統的實體安全控管(如機房的門禁管理、防火、防水及空

調系統等)。

5.2.2 角色分派

依照 5.2.1 節定義的 5 種信賴角色，本管理中心之角色分派必須符合以下規定：

(1) 管理員、簽發員和稽核員 3 種信賴角色不得同時相互兼任，但可兼任維運員。

(2) 實體安全控管員不得同時兼任其他 4 種角色工作。

(3) 任何 1 種信賴角色均不允許執行自我稽核功能。

5.2.3 每個任務所之人數

依據各種信賴角色的作業安全需求，所需之人數如下：

(1) 管理員：至少 3 位合格人員擔任。

(2) 簽發員：至少 3 位合格人員擔任。

(3) 稽核員：至少 2 位合格人員擔任。

(4) 維運員：至少 2 位合格人員擔任。

(5) 實體安全控管員：至少 2 位合格人員擔任。

每個任務所需之人數說明如下：

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
安裝、設定和維護本管理中心憑證管理系統	2				1
建立和維護本管理中心憑證管理系統之使用者帳號	2				1
設定稽核參數	2				1

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
產製和備份本管理中心之金鑰	2		1		1
啟動或停止憑證簽發服務		2			1
啟動或停止憑證廢止服務		2			1
對稽核紀錄的查驗、維護和歸檔			1		1
系統設備的日常運作維護				1	1
系統的備援及復原作業				1	1
儲存媒體的更新				1	1
除本管理中心憑證管理系統外之軟硬體更新				1	1
網路和網站的維護				1	1
設定系統的實體安全控管					2

5.2.4 識別及鑑別每一個角色

本管理中心利用使用者帳號、密碼和群組之系統帳號管理功能及IC卡，識別及鑑別管理員、簽發員、稽核員及維運員等不同角色，並利用中央門禁系統之權限設定功能，識別及鑑別實體安全控管員。

5.3 人員控制

5.3.1 身家背景、資格、經驗及安全需求

(1) 人員甄選及進用之安全評估

- 個人性格之評估。
- 申請者經歷之評估。
- 學術、專業能力及資格之評估。
- 人員身分之確認。
- 人員操守之評估。

(2) 人員之考核管理

本管理中心之相關人員在進用前先進行資格審查,以確認其資格及工作能力。正式進用後,必須接受適當之教育訓練,並以書面方式簽定應負之責任,同時每年進行資格複查,如無法通過資格複查將調離現職,改派其他符合資格人員擔任。

(3) 人員之任免及遷調管理

如人員之進用、約聘僱條件或契約有所變更,特別是人員離職或聘僱契約終止時,將遵守維護機密責任之約定。

(4) 維護機密責任之約定

本管理中心之相關人員均負維護機密之責任,並署保密切結書,不得以口頭、影印、借閱、交付、文章發表或其他方法洩漏機密。

5.3.2 身家背景之查驗程序

本管理中心對於 5.2.1 節所述之各種信賴角色人員，在進用前予以資格審查，以確認其身分資格相關證明文件是否屬實。

5.3.3 教育訓練需求

信賴角色	教育訓練需求
管理員	1、 本管理中心之安全認證機制。 2、 本管理中心安裝、設定和維護之操作程序。 3、 建立和維護系統之用戶帳號操作程序。 4、 設定稽核參數操作程序。 5、 產製和備份本管理中心之金鑰操作程序。 6、 災後復原及業務永續經營之程序。
簽發員	1、 本管理中心之安全認證機制。 2、 本管理中心系統軟硬體的使用及操作程序。 3、 憑證簽發操作程序。 4、 憑證廢止操作程序。 5、 災後復原及業務永續經營之程序。
稽核員	1、本管理中心之安全認證機制。 2、本管理中心系統軟硬體的使用及操作程序。 3、產製和備份本管理中心金鑰之操作程序。 4、稽核紀錄的查驗、維護和歸檔之程序。 5、災後復原及業務永續經營之程序。
維運員	1、本管理中心之安全認證機制。 2、系統設備日常運作之維護程序。 3、儲存媒體之更新程序。 4、災後復原以及業務永續經營之程序。 5、網路和網站的維護程序。
實體安全控管員	1、設定實體門禁權限程序。 2、災後復原以及業務永續經營之程序。

5.3.4 人員再教育訓練之需求及頻率

在本管理中心之軟硬體升級、工作程序改變、設備更換或相關法規改變時，將安排相關人員再教育訓練並記錄受訓情形，以確實瞭解

相關作業程序及法規之改變。

5.3.5 工作調換之頻率及順序

(1) 管理員調離原職務滿 1 年後，才可轉任簽發員或稽核員。

(2) 簽發員調離原職務滿 1 年後，才可轉任管理員或稽核員。

(3) 稽核員調離原職務滿 1 年後，才可轉任管理員或簽發員。

(4) 擔任維運員滿 2 年，且已接受相關教育訓練及通過審核，才可轉任管理員、簽發員及稽核員。

5.3.6 未授權行動之制裁

本管理中心之相關人員，如違反憑證政策與本作業基準或其他本管理中心公布之程序，將接受適當的管理與懲處，如情節重大而造成損害者，將採取法律行動追究其責任。

5.3.7 聘雇人員之規定

本管理中心聘僱人員之規定與正式人員相同。

5.3.8 提供之文件資料

本管理中心提供本基礎建設憑證政策、技術規範、本作業基準、系統操作手冊及電子簽章法等相關文件給本管理中心之相關人員。

6.技術性安全控管

6.1 金鑰對之產製及安裝

6.1.1 金鑰對之產製

本管理中心依照 6.2.1 節規定，於硬體密碼模組內產製金鑰對，符合 FIPS140-2 亂數產生器及 RSA 金鑰演算法，私密金鑰在硬體密碼模組內產製後一直儲存在其中而不外洩。

本管理中心之金鑰對產製在本部醫事憑證工作小組相關人員與公正第三方代表見證下進行。

用戶使用之符記為 IC 卡，其金鑰對是在卡管中心以安全控管機制驅動 IC 後，在 IC 卡內部自行產製，且金鑰對產製完畢後，其私密金鑰將無法由 IC 卡中匯出。

如用戶使用其他符記時，則由用戶自行產製金鑰對。

6.1.2 私密金鑰安全傳送給用戶

如用戶使用之符記為 IC 卡時，其私密金鑰依照 6.1.1 節規定由本管理中心之卡管中心驅動 IC 卡自行產製，卡管中心將於本管理中心簽發憑證後，將存有私密金鑰的 IC 卡掛號郵寄給用戶。

6.1.3 公開金鑰安全傳送給醫事憑證管理中心

如用戶之金鑰對由本管理中心所信賴的卡管中心代為產製時，則由註冊中心透過安全管道(本節所指的安全管道為使用安全套接層通訊協定 256 位元或其他相同或更高等級之資料加密傳送方式)將用戶之公開金鑰傳送至本管理中心。

如用戶自行產製金鑰對時，則用戶必須以 PKCS#10 憑證申請檔

的格式將公開金鑰送給註冊中心，註冊中心依照 3.1.7 節規定檢驗用戶確實擁有相對應的私密金鑰後，以安全管道將用戶的公開金鑰傳送至本管理中心。

6.1.4 醫事憑證管理中心公開金鑰安全傳送給信賴憑證者

本管理中心本身之公鑰憑證由政府憑證總管理中心簽發，公布在政府憑證總管理中心的儲存庫上，信賴憑證者可直接下載及使用。信賴憑證者在使用本管理中心本身之公鑰憑證前必須依照政府憑證總管理中心憑證實務作業基準規定，由安全管道取得政府憑證總管理中心之公開金鑰或其自簽憑證，然後檢驗政府憑證總管理中心對本管理中心本身之公鑰憑證的簽章，以確保公鑰憑證中之公開金鑰是可信賴的。

6.1.5 金鑰長度

本管理中心使用2048位元的RSA金鑰以及SHA-1、SHA-2雜湊函數演算法簽發憑證，用戶使用1024位元或2048位元的RSA金鑰。

6.1.6 公鑰參數之產製

採用 RSA 演算法之公鑰參數為空的(Null)。

6.1.7 金鑰參數品質之檢驗

本管理中心採用ANSI X9.31演算法產生RSA演算法所需的質數，該法可保證該質數為強質數(Strong Prime)。

用戶金鑰可於IC卡內部或其他軟硬體密碼模組產生RSA演算法中所需的質數，但不保證該質數為強質數。

6.1.8 金鑰經軟體或硬體產製

本管理中心依照6.2.1節規定，使用硬體密碼模組產製亂數、公開金鑰對和對稱金鑰。

卡管中心依照6.2.1節規定，用戶使用通過NIST所訂定之CNS 15135、ISO 19790、FIPS 140-2 Level 2 或安全強度相當之IC卡，並在IC卡內部產製金鑰對。

6.1.9 金鑰之使用目的

本管理中心本身之公鑰憑證由政府憑證總管理中心簽發，其中憑證金鑰用途擴充欄位設定使用的金鑰用途位元為 keyCertSign 與 cRLSign。本管理中心簽章用私密金鑰僅用於簽發憑證及憑證廢止清冊。

用戶憑證包含簽章用及加解密用的兩對金鑰對。

6.2 私密金鑰保護

6.2.1 密碼模組標準

依據憑證政策6.2.1節規定，本管理中心使用通過FIPS 140-2 Level 3 認證安全等級的硬體密碼模組產製亂數及用戶金鑰對，用戶金鑰對之儲存媒體可為IC卡或其他載具。

6.2.2 金鑰分持之多人控管

本管理中心金鑰分持之多人控管，採LaGrange多項式內插法(LaGrange Polynomial Interpolation)的m-out-of-n(以下簡稱m-out-of-n)，它是一種完全隱密(Perfect Secret)的秘密分享(Secret Sharing)方式，可做為私密金鑰分持備份及回復方法。採用此方法可使本管理中心私密

金鑰的多人控管具有最高的安全度，因此也用來做為私密金鑰之啟動方式(參閱6.2.7節)。

本部與本管理中心職務獨立之主管擔任金鑰管理人員，負責保管私密金鑰之相關資訊（例如：IC card）與保護密碼(PIN)，並儲存於具安全管控措施之環境（例如：銀行保險箱）。

6.2.3 私密金鑰託管

本管理中心簽章用私密金鑰不可被託管，本管理中心也不負責保管用戶的簽章用私密金鑰。

6.2.4 私密金鑰備份

依照6.2.2節的金鑰分持之多人控管方法備份私密金鑰，應使用高安全性的IC卡做為秘密分持的儲存媒體，如使用非高全性IC卡之儲存媒體進行，需將其儲存媒體資料刪除。

6.2.5 私密金鑰歸檔

本管理中心簽章用私密金鑰不可被歸檔。本管理中心亦不對用戶簽章用私密金鑰進行歸檔。

6.2.6 私密金鑰輸入至密碼模組

本管理中心只有在進行金鑰備份回復時，才可將私密金鑰輸入至密碼模組中。

6.2.7 私密金鑰之啟動方式

本管理中心之RSA私密金鑰之啟動(Activation)，是以m-out-of-n控

管IC卡組進行控制，不同用途的控管IC卡組分別由管理員及簽發員保管。

6.2.8 私密金鑰之停用方式

本管理中心之RSA私密金鑰之停用，是以多人授權控管的手動方式m-out-of-n控管IC卡組進行控制。

6.2.9 私密金鑰之銷毀方式

為避免本管理中心舊的私密金鑰被盜用，影響簽發憑證之正確性，本管理中心之私密金鑰生命週期屆滿時將加以銷毀，因此，在本管理中心完成金鑰更新及簽發新的憑證後，將會把硬體密碼模組中存放舊的私密金鑰之記憶位址零值化(Zeroize)，以銷毀硬體密碼模組中舊的私密金鑰。同時，舊的私密金鑰之分持也將進行實體銷毀。

6.3 用戶金鑰對管理之其他規定

用戶必須自行管理金鑰對，本管理中心不負責保管用戶的私密金鑰。

6.3.1 公開金鑰之歸檔

本管理中心將進行憑證之歸檔，且依照4.6節規定執行歸檔系統之安全控管，不再另外進行公開金鑰之歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1 本管理中心公開金鑰及私密金鑰之使用期限

本管理中心公開金鑰及私密金鑰之金鑰長度為RSA 2048位元。

公開金鑰憑證之有效期限至多為 20 年，私密金鑰之使用期限至多為 10 年。

6.3.2.2 用戶公開金鑰及私密金鑰之使用期限

用戶公開之公開金鑰及私密金鑰之金鑰長度為RSA 1024位元或RSA 2048位元。當金鑰長度為RSA 1024位元時，公開金鑰憑證之有效期限至多為5年，私密金鑰之使用期限至多為5年；當金鑰長度為RSA 2048位元時，公開金鑰憑證之有效期限至多為10年，私密金鑰之使用期限至多為10年。

6.4 啟動資料之保護

6.4.1 啟動資料之產生

本管理中心之啟動資料由硬體密碼模組產生，再寫入至m-out-of-n控管IC卡組中。IC卡中的啟動資料將由硬體密碼模組內建的讀卡機直接存取。IC卡的PIN碼直接在硬體密碼模組內建的鍵盤上輸入。

6.4.2 啟動資料之保護

本管理中心之啟動資料由m-out-of-n控管IC卡組保護，IC卡的PIN碼由保管人員負責保存，如登入的失敗次數超過3次，則鎖住此IC卡；IC卡移交時，新的保管人員必須重新設定新的PIN碼。

6.4.3 其他啟動資料之規定

沒有規定。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

本管理中心和其相關輔助系統透過作業系統，或結合作業系統、軟體和實體的保護措施提供以下安全控管功能：

(1) 具備身分鑑別的登入。

(2) 提供自行定義(Discretionary)存取控制。

(3) 提供安全稽核能力。

(4) 對於各種憑證服務和信賴角色存取控制的限制。

(5) 具備信賴角色及身分的識別和鑑別。

(6) 以密碼技術確保每次通訊和資料庫之安全。

(7) 具備信賴角色和相關身分識別的安全及可信賴的管道。

(8) 具備程序完整性及安全控管保護。

6.5.2 電腦安全評等

本管理中心採用安全強度與 C2（TCSEC）、E2（ITSEC）或 EAL3（CC,ISO/IEC 15408）等級相當的電腦作業系統。

重要系統至少須具備 B1（TCSEC）、E3（ITSEC） 或 EAL4（CC,ISO/IEC 15408）等級或以上的安全標準。上開所指之重要系統遂依據本部「資訊資產分類分級管理辦法」，評價本管理中心資訊資產數值結果為 4 之資訊系統。

6.6 生命週期技術控管措施

6.6.1 系統研發控管措施

本管理中心的系統研發遵循本部認可的品質管理規範進行品質控管。

本管理中心之硬體和軟體是專用的，僅能使用獲得安全授權的元件，不安裝與運作無關的硬體裝置、網路連接或元件軟體，並且每日自動檢查是否有惡意程式碼。

6.6.2 安全管理控管措施

本管理中心的軟體在首次安裝時，將確認是由供應商提供正確的版本且未被修改。系統安裝後，本管理中心每天自動檢驗軟體的完整性。

本管理中心將紀錄和控管系統的組態及任何修正與功能提升，同時偵測未經許可修改系統之軟體或組態。

6.6.3 生命週期安全評等

每年至少1次評估現行金鑰長度是否有被破解之風險。

6.7 網路安全控管措施

本管理中心之主機和儲存庫透過雙重防火牆和外部網路連接，儲存庫置於防火牆之對外服務區(非軍事區DMZ)，連接到網際網路(Internet)，除必要之維護或備援外，提供不中斷之憑證與憑證廢止清冊查詢服務。

本管理中心之儲存庫資訊(包括憑證與憑證廢止清冊)以數位簽章保護，並自動從核心系統傳送到儲存庫。

本管理中心之儲存庫透過系統修補程式的更新、系統弱點掃描、入侵偵測系統、防火牆系統及過濾路由器（Filtering Router）等加以保護，以防範阻絕服務和入侵等攻擊。

6.8 密碼模組安全控管措施

參照 6.1 及 6.2 節規定辦理。

7 格式剖繪

7.1 憑證之格式剖繪

本管理中心簽發的憑證之格式剖繪依照本基礎建設憑證及憑證廢止清冊格式剖繪相關規定。

7.1.1 版本序號

本管理中心簽發 X.509 v3 版本的憑證。

7.1.2 憑證擴充欄位

本管理中心簽發的憑證之憑證擴充欄位依照本基礎建設憑證及憑證廢止清冊格式剖繪相關規定。

7.1.3 演算法物件識別碼

本管理中心所簽發憑證中的簽章之演算法的物件識別碼：

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

(OID：1.2.840.113549.1.1.5)

本管理中心所簽發憑證中的主體公鑰之演算法的物件識別碼：

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

(OID：1.2.840.113549.1.1.1)

7.1.4 命名形式

憑證之主體及簽發者兩個欄位值，使用 X.500 的唯一識別名稱，此名稱的屬性型態遵循 RFC 3280 相關規定。

7.1.5 命名限制

本管理中心簽發之憑證，不使用命名限制(nameConstraints)。

7.1.6 憑證政策物件識別碼

使用本基礎建設之憑證政策物件識別碼。

7.1.7 政策限制擴充欄位之使用

本管理中心簽發之憑證，不使用政策限制擴充欄位(policyConstraints)。

7.1.8 政策限定元之語法及語意

本管理中心簽發之憑證不含政策限定元(policyQualifiers)。

7.1.9 關鍵憑證政策擴充欄位之語意處理

本管理中心簽發之憑證所含之憑證政策擴充欄位不註記為關鍵擴充欄位。

7.2 憑證廢止清冊之格式剖繪

本管理中心簽發的憑證廢止清冊之格式剖繪依照本基礎建設憑證及憑證廢止清冊格式剖繪相關規定。

7.2.1 版本序號

本管理中心簽發 X.509 v2 版本的憑證廢止清冊。

7.2.2 憑證廢止清冊擴充欄位

本管理中心簽發的憑證廢止清冊擴充欄位依照本基礎建設憑證及憑證廢止清冊格式剖繪相關規定。

8.憑證實務作業基準之維護

8.1 變更程序

本作業基準每年定期評估是否需要修訂，以維持其保證度。修訂方式包括以附加文件方式修訂及直接修訂本作業基準的內容。如憑證政策修訂或物件識別碼變更時，本作業基準將配合修訂。

8.1.1 變更時不另作通知之變更項目

本作業基準重新排版時，不另作通知。

8.1.2 應通知之變更項目

8.1.2.1 變更項目

評估變更項目於儲存庫公告 15 個日曆天，始得修訂。

8.1.2.2 通知機制

所有變更項目將公告於儲存庫。

8.1.2.3 意見之回復期限

對於變更項目有意見者，其回復期限為自公告日起 15 個日曆天內。

8.1.2.4 處理意見機制

對於變更項目有意見者，於意見回復期限截止前，以儲存庫公告之回復方式傳送給本管理中心，本管理中心將考量相關意見，評估變更項目。

8.1.2.5 最後公告期限

本作業基準公告之變更項目依照 8.1.2.2 及 8.1.2.3 節規定進行修訂，公告期限依照 8.1.2.1 節規定至少公告 15 個日曆天，直到本作業基準修訂生效。

8.2 公告及通知之規定

本作業基準修訂後 7 個日曆天內公告於儲存庫，本作業基準之修訂生效日期，除另有規定外，於公告後生效。

8.3 憑證實務作業基準之審定程序

本作業基準經電子簽章法主管機關經濟部核定後，由本管理中心公布。如憑證政策的修訂公告後，本作業基準將配合修訂，並送交電子簽章法主管機關經濟部核定。

本作業基準修訂生效後，除另有規定外，如修訂之本作業基準之內容與原本作業基準有所牴觸時，以修訂之本作業基準之內容為準；如以附加文件方式修訂，而該附加文件之內容與原本作業基準有所牴觸時，以該附加文件之內容為準。