行政院衛生署

95 年度醫療憑證管理中心營運服務案

The operation of Healthcare Certification Authority in 2006

徵求建議書說明文件(RFP)

行政院衛生署資訊中心編撰

中華民國九十四年十一月

目　　錄

壹、簡介

一、背景

邁入以資訊網路科技為核心的新時代裡，行政院衛生署(以下簡稱本署)基於掌管全國衛生醫療業務的主管機關立場，協助醫療院所以先進資訊科技推行各項衛生醫療業務，已成為本署制定及推動衛生醫療政策的重要工作；面對新世紀醫療環境資訊化快速的演進，醫療院所勢必順應潮流將病歷資訊、醫療流程及醫院管理電腦化，以提高醫療品質與效率，並降低醫療管理之成本。

隨著網際網路的誕生及蓬勃發展，民眾對保障自身相關資料的安全性及私密性的意識也逐漸提高，且醫療資訊多涉及個人隱私，攸關個人生命安全，影響至鉅。因此，如何確保資料在網路傳輸過程中的私密與完整性，如何確認網路雙方的身分，及如何避免交易雙方事後否認有收發資料等事實，實為推動醫療資訊電子化應用之首要任務。

本署為加強醫療資訊安全防護措施，並促進醫療資訊電子化應用，於 91 年利用公開金鑰基礎建設(Public Key Infrastructure, PKI)技術，規劃「醫療憑證管理中心(Healthcare Certification Authority, HCA)」，作為推行醫療電子化作業的安全及可信賴的網路環境，並自 92 年 6 月起正式營運 HCA 及簽發醫事人員/醫事機構憑證 IC 卡。

本署「設置及營運醫療憑證管理中心」四年計畫，自 91 年至 94 年期限即將屆滿，基於政策之持續性，本專案將公開徵求廠商營運 HCA，以確保憑證用戶及信賴憑證者之權益，除密切配合本署政策採取適當的營運方式外既有的服務應維持不間斷。

本署針對智慧財產權及所有權歸屬範圍，於 91 年 7 月 31 日第一 期專案執行廠商所簽訂之合約條款界定，說明如下：「乙方依契約所提供之機房、電腦(含作業系統)及通訊設備，其智慧財產權及所有權均為乙方所有，但在契約存續期間甲方擁有其完全使用權，IC 卡應用程式，本署擁有智財權及所有權，IC 卡作業系統之原始碼，本署擁有使用權。另本計畫中除上述部分外，本計畫專屬網站、線上申辦系統設計開發之原始碼及執行碼等，其所有權歸甲方所有，甲方並得依著作權法相關規定修定之。甲方使用乙方提供之系統產生之資料及資料庫檔案等，其所有權歸甲方所有。」（註：甲方為本署，乙方為原承包廠商。）

另 HCA 配合 93 年 4 月 28 日修正公布之醫療法第六十九條規定：「醫療機構以電子文件方式製作及貯存之病歷，得免另以書面方式製作；其

資格條件與製作方式、內容及其他應遵行事項之辦法，由中央主管機關定之。」及配合醫療機構電子病歷製作及管理辦法之規範，於電子病歷上之電子簽章，應憑中央主管機關核發之醫事憑證簽署並經中央主管機關加註時戳規定。

二、徵求建議書說明文件目的

本徵求建議書說明文件之目的，係向投標廠商說明本署 95 年度醫療憑證管理中心營運服務案之需求與期望，俾供投標廠商據以提出符合本專案需求之建議書。

三、徵求建議書說明文件範圍

主要規定投標廠商針對本專案所提出之建議書應包含的內容。

貳、專案概述

一、專案名稱

本專案名稱為「95 年度醫療憑證管理中心營運服務案」(以下簡稱本專案)。

二、專案授權

本專案授權機關為「行政院衛生署」。

三、專案目標

本專案預期達成下列目標：

(一)加強 HCA 營運管理制度，提高營運績效並強化營運作業之安全性。

(二)接受醫事人員／醫事機構憑證申請資料，進行憑證 IC 卡製發卡作業。

(三)加強憑證註冊服務窗口(Registration Authority Operator, RAO)及專屬網站整體服務水準。

(四)技術支援醫事憑證應用於各醫事相關系統專案，以延伸或擴充醫事憑證應用範圍。

(五)完成醫事憑證系統、專屬網站系統、RAO 網站系統、專案管理平台、卡片線上作業管理系統、HCA 安全保密函式庫 (Application Program Interface, API)及時戳服務(Time Stamp Service, TSS)之擴充及更新建置。

(六)執行 HCA 管理及營運作業。

四、專案招標

本專案依政府採購法第 22 條第 1 項第 9 款採限制性招標辦理公開評選，準用最有利標，評選第一名者取得優先議價權，另依採購法第 27 條第 3 項規定得公開預算金額，本專案使用 95 年度預算，預算金額約新台幣 2,480 萬元整。95 年度預算將視本專案公務預算是否經立法院審查通過，若經費遭刪除，則合約自動失效，上述情形得標廠商不得要求任何賠償。

五、專案範圍

(一)提供 HCA 達成下列服務所需之軟硬體及建置

1.基礎服務：提供憑證管理作業、憑證註冊服務作業及訂定 HCA 之憑證實務作業基準(Certification Practice Statement, CPS)。

2.應用服務：含提供應用 API、SSL 安全保密程式介面及 TSS。

3.目錄服務：含更新維護目錄伺服器，提供憑證內容、狀態之查詢與下載功能，並提供目錄服務應用介面函式庫。

4.測試憑證服務：提供測試憑證服務。

(二)提供 IC 卡發卡服務

1.提供本專案所需 IC 智慧卡(以下簡稱 IC 卡)之發放作業。

(1)負責本署提供庫存之IC卡空白卡片(至少 18,000 張)之客製化及發卡服務。

(2)上述庫存之 IC 卡，若有不足之情形，由本署另案辦理採購。

2.提供 IC 卡發卡服務及建立 IC 卡安全控管機制。

3.簽發憑證與製作 IC 卡時，不直接存取本署「醫事管理系統」資料庫，是由本署全國醫療資訊網(Health Information Network, HIN)服務中心(Service Center,SC)定期提供。

(三)提供專屬機房

1.主機房基礎設施：含電源、空調、高架地板、隔間及網路介面之設施。

2.主機房安全設施：含門禁、防盜系統及防災設施。

3.備援機房應與主機房距離 30 公里以上。

(四)提供 HCA 專屬網站：介紹本專案 HCA 之相關訊息。

(五)教育訓練及應用推廣計畫：

1.辦理 RAO 教育訓練，提供講師、教材及場地等。

2.配合本署政策與支援相關應用推廣專案之活動。

(六)提供「醫事憑證線上作業」：提供憑證用戶利用電腦瀏覽器透過本系統之遠程線上申辦方式，辦理憑證開卡、密碼變更、展期、解鎖卡等申請作業。

(七)設置諮詢服務窗口(0800 免付費電話)，至少提供 4 線電話及客服人員。

(八)提供危機應變處理機制。

(九)提供營運管理制度及安全稽核。

六、專案時程

本專案時程自 95 年 1 月 1 日起至 95 年 12 月 31 日並完成 96 年度工作交接為止，工作項目及時程將依第肆章第九節交付產品項目與時程執行。

七、應用服務項目

HCA 係配合國內醫療業務發展情況、時程與策略，採分年分階段實施方式，提供功能應用服務；初期將提供下列應用項目：

(一)讀寫「中華民國國民健保卡」之重大傷病患、過敏藥物、處方箋、器官捐贈同意與否等欄位權限。

(二)提供醫療院所內部各類醫事人員，作為身分確認使用。

(三)提供病歷資料轉診、轉檢之認證使用。

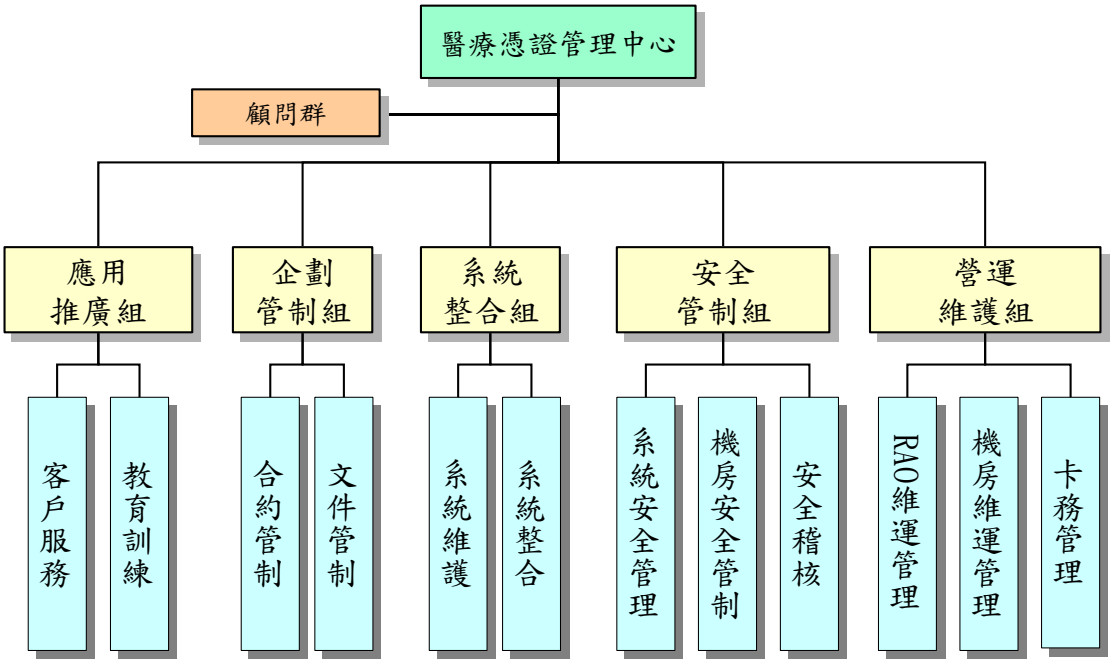
(四)醫療院所發展電子病歷之認證應用：

為鼓勵醫療院所廣為推廣病歷電子化作業，本署將開放醫療院所提出應用 HCA 機制及憑證於各項醫療服務工作之應用計畫，經本署核可後，將免費提供憑證及應用 API，供其使用，醫療院所經本署同意免費使用之 API 不得轉移、重製、更新包裝或使用於商業用途。

參、現有作業說明

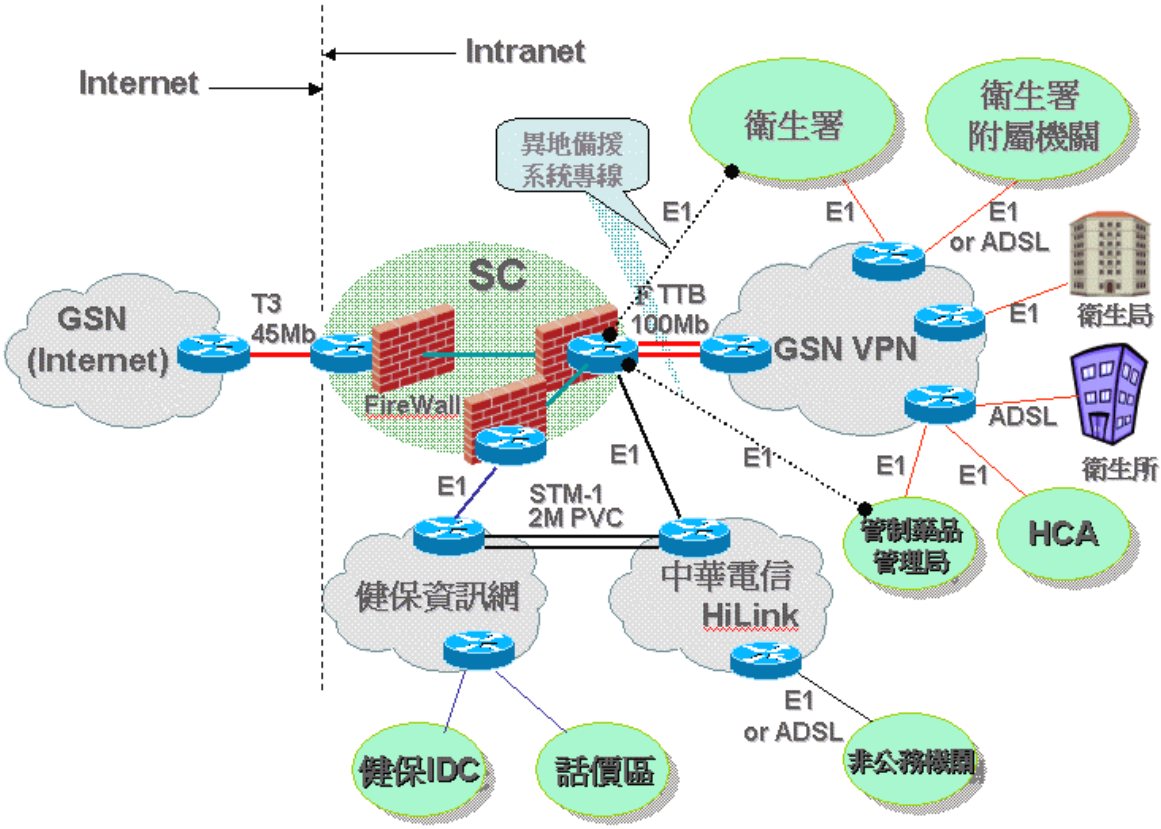
一、醫療憑證管理中心(HCA)營運組織架構圖

醫療憑證管理中心
營運組織架構圖



二、本署全國醫療資訊網

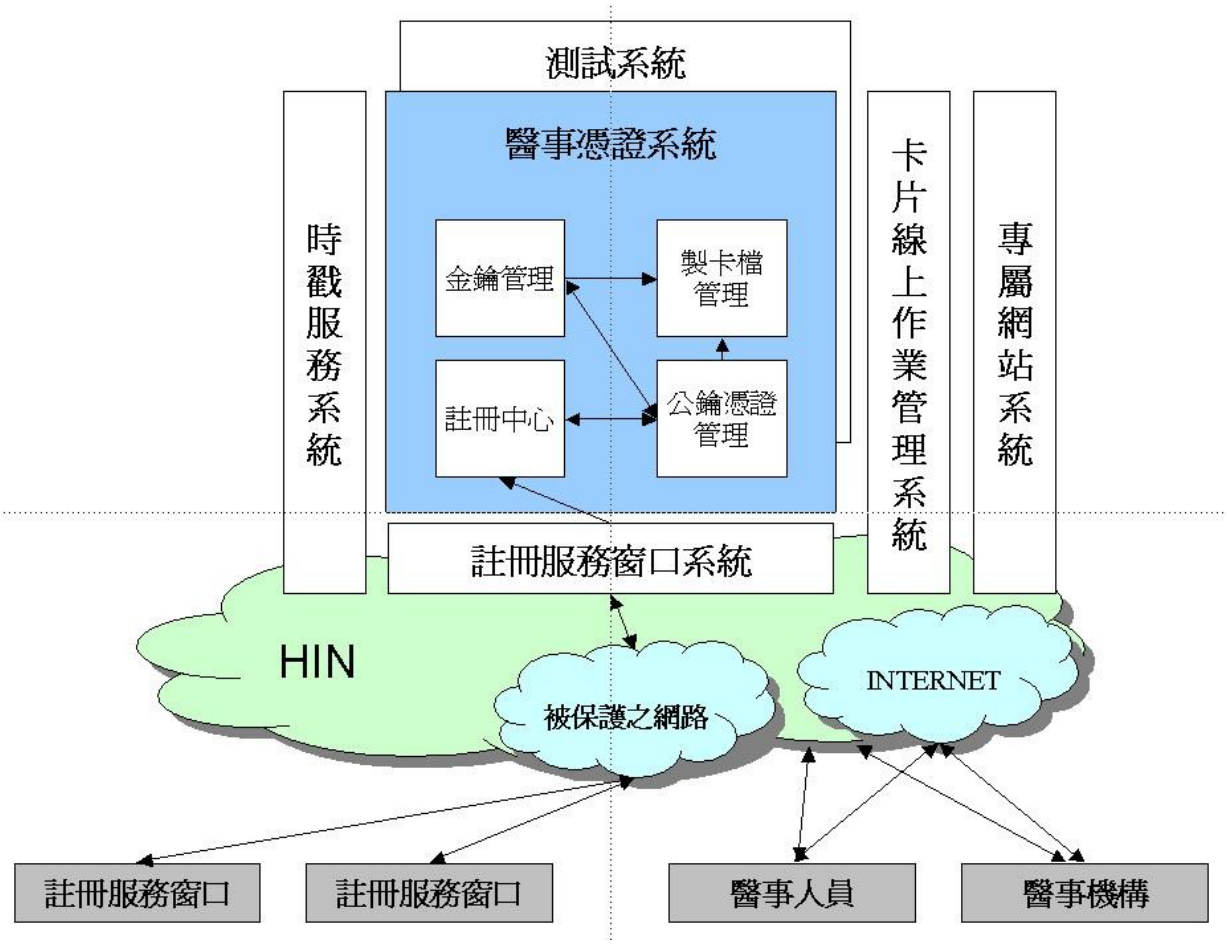
HIN 網路架構圖



三、現行醫療憑證管理中心(HCA)系統架構及功能說明

現行 HCA 系統包含「醫事憑證系統」、「RAO 系統」、「TSS 系統」、「專屬網站系統」、「卡片線上作業管理系統」及「專案管理平台系統」。

以下並針對 HCA 系統做說明。整體系統為一集中式 PKI 建置架構，系統由數個子系統所組成，如下圖：



(一)醫事憑證系統

1.簽發 HCA 各類憑證。憑證系統之所有密碼運算，均在 FIPS-140-1 Level 3 等級之硬體加密模組 (Hardware Security Module,HSM)內完成。同時，CA Server 本身的主基碼 (Local Master Key) 亦將透過此 HSM 保護與備份。

2.提供 RAO 系統註冊管理服務。

3.產生 IC 卡 製發卡流程所需之安控金鑰，及提供系統「金鑰回復」可靠之金鑰保護機制。

4.將憑證 (包括 public certificate 與 attribute certificate) 與憑證廢止清冊 (Certificate Revocation List,CRL) 發行至輕量目錄存取服務 (Lightweight Directory Access Protocol,LDAP) 上。

5.透過 WEB 控制介面與醫事管理系統資料庫定期進行同步作業。

6.醫事憑證 IC 卡製卡檔產製，製卡檔資料包括卡片正反面列印資料 (如照片、卡號、醫事人員或醫療機構中英文名稱、條碼列印、晶片個人

化資料及相關基碼、卡片封裝與郵寄資料和密碼函資料) 。

7.提供現有健保卡所規劃的 HPC Applet 的發卡資料與基碼的準備，包括與現有健保卡的基碼管理系統建立必須的基碼交換作業與基碼管理作業。同時也支援 HCA Applet 的發卡資料與基碼的準備，包括使用 HCA 專案的基碼管理系統建立必須的基碼管理作業、配合註冊管理中心 (Registration Authority,RA) 系統完成憑證申請作業後的其他發卡資料準備。

8.卡片發放作業的回收聯簽回作業及密碼函產製功能。

(二)註冊服務窗口(RAO)系統

透過 SSL 機制提供 RAO 人員 WEB 操作介面，進行 RAO 各項業務服務。登入 WEB 操作介面並需透過 RAO 作業人員 IC 卡簽章驗證後方可認證登入。

(三)時戳服務(TSS)系統

HCA 時戳管理中心(Time Stamp Authority,TSA) Server 分為兩部份：一部份為取得精確且有公信力系統時間之 Time Synchronization client (須符合 Network Time Protocol, NTP, RFC-958)；另一部份為符合 RFC-3161 TSP (Time Stamp Protocol) 之 TSA 。

TSA 所需之簽章服務，透過 HSM 完成。

(四)專屬網站系統

介紹HCA之相關訊息，包括：HCA專案介紹、相關公告訊息及問答集等資訊，加強醫事機構及醫事人員對醫事機構憑證IC卡及醫事人員憑證IC卡之認識。網址：http://hca.doh.gov.tw

(五)卡片線上作業管理系統

提供線上開卡、線上解鎖卡、線上更改密碼、展期作業等功能。可透過專屬網站「開卡作業與卡片工具」鏈結進入。

四、專案原訂原則與規範

(一)執行原則

1.本專案所需之經費由廠商提出價格分析列於建議書內，內容應包含：系統軟硬體、IC 卡客製化(Personalization)成本、安全控管、經營管理、經費運用估算。

2.HCA 架構必須參考 ITU-T X.509 Version 3 及 Version 4 之建議，並符合 ITU-T X.509、RFC 2527、ISO 7816、PKCS…等國際組織訂定之相關標準。

(二)系統建置原則

1.有關系統建置採 Multi-tier 架構、模組化、物件導向設計為原則。

2.系統以操作簡單、易與既有資訊系統整合。

3.相關程式模組須無暗門、木馬等非法程式碼，以確保資訊安全，未來若造成資訊安全損害事件，得標廠商須完全負起賠償及法律責任。

4.本專案建置的相關系統之設計，必須符合「電腦處理個人資料保護法」等相關法律之規定。

5.本專案之醫事憑證 RAO 所使用之相關軟硬體設備等，須包含於本專案中，由得標廠商負責提供；另提供之憑證線上申請作業，個人所需之上網環境由憑證申請使用者自行準備。

(三)營運維護原則

1.參考行政院頒布「行政院及所屬各機關資訊安全管理要點」，以建立一安全可信賴的網路申辦環境為原則。

2.全國各縣市衛生行政機關、醫事機構及醫事人員線上申請作業須能與傳統人工作業方式並行。

肆、需求說明

一、功能需求

(一)系統移轉建置功能需求

1.移轉醫事憑證系統

(1)憑證系統

A.建立憑證簽發機制

- 符合 ITU-X.509/V3 之 PKIX 國際相關標準。
- 應用範圍發放之憑證種類包括：醫事機構憑證(正、副卡憑證)、醫事人員憑證、醫療相關之伺服器應用軟體憑證。
- 憑證之主體名稱(Certificate Subject Name)及所屬機關或單位等資料必須使用中文資訊，並符合國際標準。
- 憑證系統需簽發 HCA 內部使用之憑證，包含 RAO 憑證、註冊服務系統 SSL 憑證、TSS 憑證、專屬網站 SSL 憑證。

B.建立憑證管理機制

- 提供各類憑證申請、展期、廢止之各項簽署功能。
- 提供各類憑證安全管理機制(憑證系統內查詢、刪除、更新機制)。
- 提供各項憑證作業稽查機制。

●提供各項憑證作業資料備份機制。

(2)註冊管理中心 (RA) 系統

A.提供 RAO 上傳之憑證申請者資料核對功能。

B.提供 RAO 憑證簽發審核、更新審核、刪除審核等管理功能。

C.提供伺服器應用軟體憑證簽發審核功能。

D.提供各項註冊作業備份、稽查機制。

(3)金鑰管理系統(KMS)

A.提供產製各類憑證之金鑰對功能。

B.金鑰對之長度必須為 1024 Bits(含)以上，私密金鑰必須存在硬體密碼模組中，硬體密碼模組必須具備金鑰備援管理機制，並符合以下功能：

●實體安全機制之檢測，當實體保護被破壞時，密碼模組必須擁有自動清除秘密參數的功能。

●身分鑑別機制(Identity-Based Authentication)。

●私密金鑰輸入應使用安全(加密處理)之管道，或使用金鑰分持(Key Splitting)技術。

C.得標廠商必須保證移轉具安全性(須通過 FIPS140-1 Leve3 認證或 ITSEC E3)之硬體密碼模組，如有硬體密碼模組被破解，或私密金鑰被非法讀出之情事，得標廠商應負賠償之責任。

D.提供金鑰管理機制，包括金鑰產生、儲存、啟用、停用、更新、銷毀及存放等。

(4)目錄服務管理系統

A.依照 X.500 相關國際標準，移轉建置目錄服務系統，並符合以下需求：

●目錄服務管理系統，並符合 LDAP-V2, V3。

●提供憑證內容資料及憑證狀態等資訊公佈、查詢與下載功能。

B.提供各類憑證廢止清冊之公佈、下載等功能，並具有可設定採即時公佈或每日公佈次數之功能。

●如發現醫事人員或機構已歇業，應主動知會本署醫事處確認後納入憑證廢止清冊內。

C.公佈及下載之憑證需採用 X.509 標準(內含 HCA 憑證機構簽署之數位簽章)。

D.提供各項憑證公佈、下載作業及系統設定作業之記錄功能。

(5)製卡檔案管理系統

A.提供醫事憑證 IC 卡製卡檔案安全產製、刪除、加密、安全匯出及管理功能。

B.得標廠商必須保證每一個醫事憑證 IC 卡製卡檔之唯一性。

C.提供醫事憑證 IC 卡密碼函檔安全產製、加密匯出等功能。

D.提供醫事人員照片掃描匯入功能。

(6)資料更新上傳系統

A.提供醫事系統醫事資料庫手動 FULL UPDATE 至 HCA 資料庫功能。

B.提供醫事系統醫事資料庫 INCREMENTAL xml 資料手動及自動更新至 HCA 資料庫功能。

C.需支援線上接收醫事系統之醫事資料庫資料功能。

D.完整查詢資料線上接收、更新紀錄介面。

E.提供資料異動至 HCA 資料庫錯誤之回復功能。

2.移轉專屬網站系統

(1)網站提供之介面需包含以下：

A.醫事憑證介紹訊息。

B.HCA 各項宣導推廣訊息。

C.HCA 各項最新公告訊息。

D.醫事憑證各類型 Q&A 查詢。

E.醫事憑證 IC 卡卡片工具鏈結網頁。

F.儲存庫資料下載介面，下載資訊並包含以下：

●HCA 各項制度文件下載。

●憑證各項技術規範下載。

●HCA 各項申請表單下載。

●憑證用戶憑證、HCA 憑證及憑證廢止清冊下載。

●憑證狀態之線上查詢介面(On-line Certification Status Protocol, OCSP)。

G.醫事憑證各項醫療應用專案介紹及鏈結。

H.醫事憑證相關法規介紹。

I. 其他相關網站鏈結。

(2)專屬網站應依本署之意見即時新增、刪除、變更網站公告之事項或網站功能。

3.移轉註冊服務窗口(RAO)網站系統

(1)安全登入 RAO 網站系統要求：

A.提供 RSA IC 卡作為 RAO 操作員私密金鑰之儲存媒體登入 RAO 系統使用。

B.提供驗證 RAO 憑證登入系統功能。

(2)RAO 網站需提供以下介面：

A.憑證申辦(醫事機構正、副卡憑證申辦及醫事人員憑證申辦) 。

B.憑證作業處理(廢止、展期、到期重新申請、金鑰回復、卡片解鎖作業)。

C.資料查詢(申請者進度查詢、使用者詳細資料、已審核資料查詢)。

D.稽核紀錄查詢。

E.工具專區(RAO 作業 IC 卡片密碼更改、RAO 作業 IC 卡片憑證內容解析、RAO 教育訓練講義下載、RAO 各類型作業申請書等)。

(3)RAO 網站應依本署之意見即時新增、刪除、變更網站功能。

4.移轉專案管理平台

(1)安全登入專案管理平台網站系統要求：

A.提供帳號、密碼登入機制。

B.依不同權限顯示不同使用功能清單。

(2)專案支援需求

提供本署醫事憑證相關之其他專案廠商使用。並依不同專案性質，可使用不同專案管理項目。

(3)管理平台需提供以下介面：

A.專案管理

●不同專案工作區(個人工作區、待分案事項、完工確認頁面、工作事項查詢、公佈欄、專案成員通訊錄、工作報表)。

●專案設定區(工作事項管理、公佈欄管理、個人資料維護、使用者設定、系統設定)。

B.憑證作業

●憑證申請狀態查詢。

●憑證開卡狀態查詢。

●憑證 IC 卡卡片工具。

●HCA 管理中心憑證簽發統計(HCA 憑證簽發統計、展期數量查詢)。

●憑證狀態服務。

●RAO 稽核紀錄。

C.文件/表單管理介面

●文件/表單儲存庫。

●文件/表單管理(文件/表單目錄管理、文件/表單檔案上傳、文件/表單檔案管理)。

D.客戶服務管理系統(客戶服務問題管理查詢) 。

(4)管理平台應依本署之意見即時新增、刪除、變更網站功能。

5.卡片線上作業管理系統

(1)提供線上讀卡機功能測試介面。

(2)線上自動下載開卡、解鎖卡(含 HPC 及 HCA)、密碼變更(含 HPC 及 HCA)、展期之 OCX 元件或手動下載安裝以上 BATCH SHELL 元件功能。

(3)提供開卡、展期紀錄介面查詢功能。

(4)系統需提供解鎖卡前驗證機構憑證 IC 卡合法性功能。

6.安全保密函式庫(API)

(1)依照國際相關標準，提供開發電子認證應用系統所需之 API。

(2)需透過健保讀卡機呼叫 HCA API。並與健保 Control Software 最新版本整合應用，整合方式以健保 Control Software 與 HCA API 呼叫使用時，不相互佔據健保讀卡機 Com port 為原則。

(3)於 Windows(包括 2000、XP)系統平台，提供以下功能：

A.啟用函式：於系統啟始及結束時使用，並提供 API 所需參數設定函式。

B.加解密函式：對稱式加解密演算法及單向雜湊函數演算法相關函式。

C.數位簽章與數位信封函式：提供確保資料隱密性、完整性及不可否認性相關函式。

D.憑證應用服務函式：提供憑證有效期讀取、驗證憑證及讀取憑證資料相關函式。

E.時戳簽章及驗章函式：提供簽署時戳、時戳內容解析、時戳驗證相關函式。(需配合未來本署時戳服務相關政策，彈性進行函式更新或整合。)

F.其他加值函式。

(4)建立 API 版本控管機制及應用系統審驗功能。

7. 時戳服務(TSS)系統

(1) TSS 功能需求

A. TSA 位於 HCA 內，其相關硬體及服務建置於 HCA 專屬機房中，另需規劃備援機房之服務模式。

B. TSA 提供之 TSS，其可信賴時間需與國內或國外精確且有公信力之時間單位同步，且同步對時方式須符合 NTP (Network Time Protocol) ,RFC-958 規範。

C. TSS 需完全支援 RFC-3161 TSP 標準，可接受來自時戳需求者之時戳請求、傳送時戳請求訊息並驗證回應之時戳訊息。

D. TSS Responder 根據 RFC-2630 及 RFC-2315 規範，傳遞標準時戳回應訊息。

E. TSS 需能透過 ASN.1 DER 編碼格式產生 TST(Time-Stamp Token)，並透過 HSM 簽章，以確保時戳之正確性與不可否認性。

F. 需提供「時戳請求訊息傳送」、「時戳驗證」、「時戳內容解析」之 API，並整合至 HCA API 內。

G. 需能辨識出時戳請求者之身分。

(2) TSA 系統架構需求

A. TSA 系統架構建置及修正需完全配合 HCA 系統架構設計。TSS 伺服器建置於 HCA 機房內，其作業本身需透過 HCA 防火牆保護，重要運算傳輸作業則應保護於內部區域網路內。

B. TSA 系統架構需符合 3-Tier 架構(TSA Client <-> TSA Agent <-> TSA Server)建置，以確保 TSA Server 之安全性。並且需能將 TSA Client 至 TSA Agent 之訊息傳遞換成亂碼模式，提升安全等級。

C. TSS 伺服器需透過 FIPS 140-2 Level 3 認証過之 HSM 進行時戳簽章，得標廠商並應提供保護相關硬體之安全機制。

(3) TSS 安全控制需求

A. TSA 私鑰須由硬體加密模組自行產生，不可匯出。

B. TSA 私鑰須經由其他 KEY(IC 晶片卡或 USB KEY)控管。

C. TSA HSM 可產生 PKCS#10 CSR，並經由 HCA 產生憑證後，匯入 TSS 系統中。

(4) TSS 效能控制需求及擴充需求

A. 得標廠商應確保 TSS 7*24 服務不中斷。

B. 時戳服務器之時間儲存於符合 FIPS 140-2 Level 3 認証之 HSM，無法以人工或程式指令修改時間。

C. TSA 時間源除與上述公正機構同步外，並支援 GPS、IRIG-B 及 1PPS 等以做為標準時間來源之備援。

D. 具備自動校時之功能，未來可由本署時間源設備來控管時戳服務器之校時之功能，例如經由時間憑證(Time Attribute Certificate ,TAC)來證明時戳服務器之時間的有效性與可靠性。

E. 具備處理具公信力時間單位之憑證，以提供任一方之認證與安全之連線、稽核及事後追蹤。

F. 可查詢憑證資訊與狀態、時鐘狀態、時間憑證資訊、日誌(管理

者、機器、使用者、封存)、使用者資料、作業狀態。

G.時間精確度由原 0.1 秒為單位提升為 0.01 秒為單位。

H.將原在不計算網路頻寬影響網路速度之條件下，TSA 需提供同時 100 個 TSS 請求訊息能在 5 秒內回應之效能，提升為每秒至少可執行 120 個時戳運算。

I.得標廠商需隨時評估 TSS 之請求量，並視情況需要提供本署增加設備之建議。

J.投標廠商需說明 TSS 建置之方式及架構(含備援機房)。

(二)營運作業服務移轉建置功能需求

1.醫事憑證 IC 卡發卡作業

醫事憑證自申請至使用，其相關流程說明如下，若流程及方式更動，本署將另行通知。

(1)申請作業

由醫事機構與醫事人員主動提出申請，可向 RAO 或逕向 HCA 提出申請，需核對申請者身分、證件，申請表填寫內容需與「醫事管理系統」資料相符，另人員需繳交符合證件規格之照片。

(2)建檔作業

申請表單應加以掃描建檔，並以機構代碼或身份證號為索引，可迅速查詢瀏覽申請表單影像，必要時可以列印。

(3)憑證簽發

憑證應於申請審核通過 7 日內簽發。

(4)製卡作業

A.憑證申請資料之處理，含資料建檔、掃描、核對與簽發憑證。

B.專業卡廠之卡片個人化作業，含將資料寫入晶片、卡面印刷與封裝。

(5)發卡作業

卡片製作完成，應以掛號方式寄送至申請之醫事機構或醫事人員執業之醫事機構。

(6)接受作業

憑證用戶接到卡片後，應確認卡片印刷內容正確後將回執聯寄回 HCA，以表示接受並確認收到卡片。回執聯應標示郵遞之地址。

(7)寄發密碼

HCA 接到回執聯後，應製作密碼函及以掛號方式寄送密碼函。

(8)卡片管理與採購

本專案未列入採購空白 IC 卡數量，因仍有安全庫存空白卡片

預估約 18,000 張，營運期間，承包廠商應將卡片妥善管理，並供醫事機構、醫事人員之申請、補換發與醫事機構憑證 IC 卡副卡等使用。空白卡片庫存低於 5,000 張，承包廠商應通知本署，IC 卡片數量不足的部分由本署另案編列經費，依照分列的 IC 卡片及個人化的費用報價來向承包廠商購買，每次需超過 20,000 張為單位。計畫工作結束後未使用之 IC 卡應歸本署所有，並於期末驗收請款時扣除個人化費用。

2.機房維運作業

(1)得標廠商需定期確實檢視以下機房系統項目，並繳交檢視紀錄予內(外)部稽核人員當作稽核底稿使用：

A.醫事憑證相關之應用軟體運作狀況。

B.各主機作業系統運作狀況。

C.各系統存取安全性。

D.各系統帳號、群組設定。

E.系統硬體裝置。

F.網路協定及連線狀況。

G.網路存取狀況。

H.備援系統啟動運作狀況。

(2)得標廠商需定期確實檢視以下相關資料庫維運狀況，並繳交檢視紀錄予內(外)部稽核人員當作稽核底稿使用：

A.資料庫備份作業。

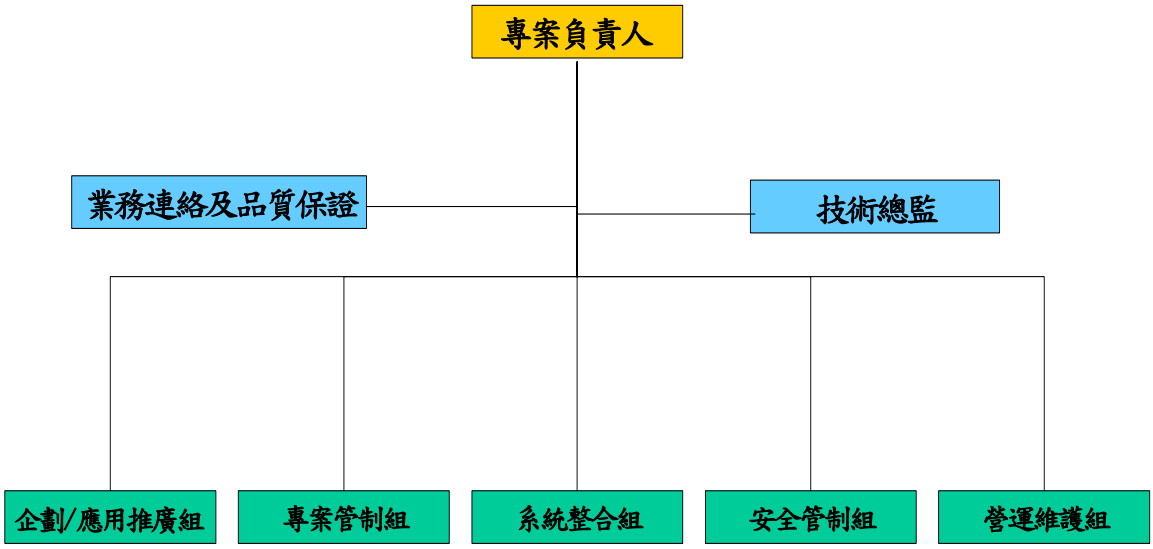
B.資料庫系統各項設定、記憶體、控制檔等狀況。

C.資料庫各項運作紀錄。

3.營運中心管理作業

(1)營運中心管理作業，包含例行的發卡作業、專屬網站的維護與更新、提供諮詢服務的客服專線與電子信箱與作業人員的管理等。

(2)營運中心的組織架構與分工



(3)營運相關文件、紀錄與數據應整合於專案管理平台，以利本署使用管理平台之功能有效管理。

4.主機房及備援機房管理作業

(1)為維持憑證業務活動正常營運及保護 HCA 機房之安全，以確保工作場所及設備不受侵害、干擾或未經授權之存取，得標廠商必須針對 HCA 機房進出、存取、使用授權、監督管制等進行管理及記錄，並建立管理制度文件。

(2)建置 HCA 機房，投標廠商得利用現有機房隔間，但必須具備獨立的門禁，並符合以下需求：

A.基礎設施

(A)電源

必須採獨立電源，供電必須採雙迴路，並設有柴油發電機及不斷電電源系統，提供穩定電源使系統無斷電之虞，保證在市電停電 24 小時內服務不會中斷。

(B)空調

必須提供恆溫、恆濕空調系統，引進新鮮空氣，確保機房之運作環境。

(C)高架地板

必須設置高架地板,每平方公尺可承重 500 公斤(含)以上。

(D)隔間

必須提供堅固可靠之隔間，防止外力破壞入侵。

(E)網路介面

必須提供 Fast Ethernet 或 Packet over SONET(POS)等網路介面。

B.安全設施

(A)門禁

門禁系統至少要有三種管制設施，例如個人密碼、磁卡、IC 卡、影像識別等門鎖，並設有警衛人員管制。

(B)防盜系統

✧監視系統

機房出入口及重要區域，均須設置 24 小時監視系統，並保存錄影紀錄至少 7 天以上。

✧機房(含機箱)入侵偵測及警告系統

對於任何非授權之機房(含機箱)入侵,均能主動偵測並發出警告。

(C)防災設施

✧消防設施

必須設置防火警報，並提供自動滅火設施，至少為 Fire Master 200 System 或同等級(含)以上之系統。

✧防震設施

必須設置防震設施，至少可抵擋六級(含)以下之地震。

✧防電磁干擾設施

必須設置防止電磁波干擾設施，防電磁之干擾。

✧防靜電設施

必須設置防靜電設施，防止靜電之災害。

✧異地備援

備援機房需建置於距離主機房三十公里外之區域，可於主機房遭遇災難而無法正常運作時，於二十分鐘內啟動。備援系統提供之服務需包含 RAO 服務、線上開卡服務、線上展期服務、憑證廢止清冊公佈服務、憑證狀態查詢服務及 TSS 等。

(三)營運內部控制及稽核服務功能需求

1.內部控制制度

(1)制度管理

HCA 前期初步已研擬營運管理制度準則，架構區分依「一般控制作業管制」與「安全制度提昇之規範建立」兩大項，規劃管理文件及制度建構內容。

承包廠商主要工作項目如下：

A.檢討 HCA 既有流程，修訂與檢視研訂之規範文件與實務管理制度達同步一致性，以強化健全制度面及執行面，並研擬 HCA 內部控制之評估要點。

B.遵循「行政院及所屬各機關資訊安全管理規範」為藍本，擬定 HCA 資訊安全管理規範，加強資訊安全管理，建立安全及可信賴之電子化醫療環境，確保資料、系統、設備及網路安全，保障民眾權益。

(2)作業管理

A.對於負責各維運作業之相關工作訂定管理原則與標準作業程序，分散權責，建立人員備援制度，並控制作業是否適當、確實。

B.控制作業應適時自行檢查，各營運作業小組配合稽核單位執行年度內控稽核時，需評估各組之目標及風險，並檢查現有之內控設計可否控制風險及實際執行情形是否依該設計辦理。

C.各營運作業小組需透過表單紀錄方式，確實執行與記錄，以達到整體作業制度流程完整性控管，本署將不定期抽驗作業表單。

2.專案稽核作業

依據目前「HCA 憑證實務作業基準」之規定及本署之要求，承包廠商每年至少需執行外部稽核一次及內部稽核一次。

二、管理需求

(一)專案管理

得標廠商應就專案執行規劃、專案系統移轉建置、專案營運維護等部分，規劃專案管理工作，並據以執行。

1.專案執行規劃：

(1)本專案以整體委外方式辦理，包括規劃、分析、移轉、測試、建置及營運等工作，涉及公權力者仍由本署負責。

(2)本專案應於 95 年 1 月 1 日起即可正常維持營運。

(3)承包廠商應依「專案執行計畫書」之工作進度，執行專案管理各項工作，本署得不定期要求廠商提供進度報告，並召開專案工作會議。

(4)承包廠商應透過現有之專案管理平台，定期將執行進度及執行成果上網、提供發卡狀況（表格由本署另行提供）之即時查詢。

(5)承包廠商應定期對 RAO 作業查核，並於作業異常時提出異常報告及解決方法交由本署複核。

(6)本專案所需之經費由廠商提出價格分析列於建議書內，內容應包含：軟硬體設備、IC 卡客製化(Personalization)成本、安全控管、經營管理、經費運用估算。另須列出本專案各項工作之郵資單價、數量及總價，於期末驗收時，須提報本專案相關實際郵資費用證明(範圍包含本計畫執行過程中衍生之所有郵資費用)，本署將依據實際郵資總費用來給付經費。

(7)HCA 架構必須參考 ITU-T X.509 Version 3 及 Version 4 之建議，並符合 ITU-T X.509、RFC 2527、ISO 7816、PKCS…等國際組織訂定之相關標準。

2.專案系統移轉建置

(1)有關系統開發建置採 Multi-tier 架構、模組化、物件導向設計為原則。

(2)系統以操作簡單、易與既有資訊系統整合為原則。

(3)相關程式模組須無暗門、木馬等非法程式碼，以確保資訊安全，未來若造成資訊安全損害事件，得標廠商需完全負起賠償及法律責任。

(4)應用系統開發，應考慮安全需求，並滿足以下的安全控制事項：

A.應用程式需做好輸入查驗（Input Validation），對於使用者輸入的資料，做適當的過濾與處理，對於輸入資料之長度、型態、特殊字元、特殊指令等，確實的加以檢核過濾。

B.使用者使用 Web 應用系統之各種資源（如服務請求、檔案檢索、資源管理等）， 均需要嚴格的身份管制(Authentication)程序，透過適當的授權程序後（Authorization）， 並保證所有的用戶動作，有明確的責任管制(Accountability）與稽核軌跡。

C.使用者的密碼、交易資料、交易過程產生的敏感資料等，需要適當的保護與管理。

D.主機目錄存取權限，需有妥善的規劃及控管，避免無限制開放使用者存取。

E.需有適當的系統異常或錯誤之管理（Error Handling），以防止系統資訊洩密、阻斷服務、系統癱瘓等狀況發生。

F.需有適當的系統組態設定，以保障系統安全。

(5)本專案建置的相關系統之設計，必須符合「電腦處理個人資料保護法」等相關法律之規定。

(6)本專案之醫事憑證 RAO 所使用之相關軟硬體設備等，須包含於本專案中，由得標廠商負責提供；另提供之憑證線上申請作業，個人所需之上網環境由憑證申請使用者自行準備。

3.專案營運維護

(1)參考行政院頒布「行政院及所屬各機關資訊安全管理要點」，以建立一安全可信賴的網路申辦環境為原則。

(2)全國各縣市衛生行政機關、醫事機構及醫事人員線上申請作業須能與傳統人工作業方式並行。

(3)HCA 之營運須符合「行政院衛生署醫療憑證管理中心憑證實務作業基準(Certification Practice Statement ,CPS) 」之規範。

(4)配合本署於專屬網站公告之收費機制，採取必要之措施與提供協助。

(二)驗收管理

1.得標廠商應依合約所訂之交付項目與時程，依序進行專案工作，本署將依第肆章第二節之專案管理需求的監控原則，即時掌握專案進行情形。

2.測試結果符合招標文件及合約所載需求，並完成所有應交付項目後，始完成驗收程序。

(三)專案人員

1.承包廠商應於「專案執行計畫書」內，依據營運主要工作項目需求詳列組織架構及工作劃分，並將參與本專案工作人員之學經歷背景及證明文件列於「專案執行計畫書」內，作為本專案工作管制及資源分配之管理或監控依據。

2.承包廠商應指定專案負責人，履行各項管理政策及程序，專案負責人需具備五年以上資訊專案管理工作經驗，並全權代表廠商執行各項技術及管理工作。於專案執行期間，除與本署指定聯絡窗口相互保持聯繫及負責協調工作外並定期參與本署召開之專案工作會議，由專案經理率同參與本專案人員 1 至 2 人至本署，進行各項工作計畫及進度之協調提報，以利本署追蹤專案之執行狀況。

三、安全需求

承包廠商對業務上所獲悉之資料，應視同機密文件，並採取必要之保密措施，承包廠商參與本案人員均應依本署規定填具保密契約書及保密切結書(如附錄一、二)，任何因承包廠商人員洩密所致之賠償及刑事責任，概由承包廠商負責，並依本署規定列入本署拒絕往來戶。

四、效能需求

(一)得標廠商應執行下列效能測試：

TSS 系統於離峰時段(上午 9 時前或下午 5 時後)，同時模擬 120 位使用者要求時戳，由得標廠商進行測試，並提出相關紀錄與統計等佐證資料，以證明每秒至少可執行 120 個時戳運算。

(二)得標廠商應自訂服務績效指標 3 項，指標達成情形將列入期末驗收項目。

五、強制性需求

(一)本專案期間，本署可視需要隨時派員至得標廠商處瞭解專案執行情形，並要求得標廠商向本署簡報。

(二)本專案之需求規格經本署確認後，於專案營運階段，仍有不超出整體需求架構 15%功能增修之權利。

(三)作業時如發生錯誤或資料漏失，經確認屬得標廠商責任者，應由得標廠商負責更正；另損及他人權利義務得標廠商亦須負責。

(四)得標廠商未依徵求建議書說明文件及合約規定執行者，經本署要求限期兩週內改善未果者，本署得終止合約。

(五)本專案 95 年度營運結束後若非由原營運廠商得標，原營運廠商應與 96 年度承包廠商辦理交接（含文件、系統操作、架構及最新程式原始碼），交接期間為本署簽定新年度合約當月，並於交接後 1 個月內提供新承包廠商免費諮詢服務以便達到技術移轉之工作，如違反規定則扣除履約保証金。

(六)本合約結束，於次年招標如延誤，廠商需繼續提供服務，有關每個月營運費用依本專案契約價相關工作項目之價格分析計算。

(七)得標廠商須配合本署 HCA 未來營運規劃及方向提供適當之協助。

六、智慧財產權歸屬

(一)本專案得標廠商所有交付本署有關之文件及資訊系統(不含 IC 卡作業

系統)著作權及智慧財產權均屬本署所有，並需放棄著作人格權。

1. 得標廠商依契約所提供之軟體(詳如第肆章需求說明之系統移轉建置功能需求，但不含 IC 卡作業系統)，其智慧財產權及所有權歸本署所有。

2.本專案產生之資料及資料庫檔案等，其所有權歸本署所有。

(二)本專案 TSS 擴充之相關硬體其所有權歸本署所有。

(三)得標廠商交付之本專案相關軟體項目中如包含第三者開發之產品，應切結保證（或提供授權證明文件）軟體使用之合法性（以符合中華民國著作權法規範為準），並提供手冊、磁片或光碟片（若為共享軟體(shareware)則不在此限，惟仍應取得使用授權）。得標廠商如有隱瞞事實或使用未授權軟體之行為，致使本署遭致任何損失或聲譽之損害時，得標廠商應負一切損失與責任，並放棄法律之先訴抗辯權。

(四)得標廠商自行開發之電腦程式應提供系統軟體原始程式碼（若應用程式係由程式開發工具所開發，應將處理程序、鍵值定義及操作步驟等明列說明以代替原始程式碼）光碟片 2 份，經再生測試無誤後，交由本署保管做為系統維護之用，系統相關軟體如有修改時應配合一併更新。系統開發過程本署得指派人員參與，得標廠商應提供必要之指導及訓練，以協助軟體轉移順利進行。

七、客服服務

(一)配合本署之上班時間，設置免付費客服專線提供諮詢服務，應至少 4 線電話與客服人員。

1.回答醫事機構、醫事人員與社會各界對 HCA 之相關問題。

2.回答醫事憑證申請之相關問題。

3.回答 RAO 作業之相關問題。

4.定期接收專屬網站信箱與回覆。

(二)客服專線全部忙線中，應有語音提示。

(三)客服問題應加以記錄，歸納整理後公佈於專屬網站之常見問題集。

(四)回覆電子郵件信箱，一般問題應於一個工作日內回覆，超出授權之問題呈報本署。

八、教育訓練

RAO 教育訓練：

1.RAO 設立於全國各縣市衛生局與台北市、高雄市及台北縣所屬衛生

所。

2.RAO 受理醫事憑證註冊相關作業，包括憑證申請、廢止、展期、金鑰回覆與卡片解鎖卡等。

3.每半年應辦理 RAO 教育訓練，分北、中、南三區共 18 場次，場地、餐點、講師（包括講師費、交通費、食宿）與教材由承包廠商提供，但不包括負擔參訓學員之差旅費。

4.上課現場提供實機操作教學，承包廠商應自備測試環境，使受訓學員可於模擬環境上實際執行各種憑證業務實作。

九、交付產品項目與時程

本專案開發工作項目與相關產品交付及時程如下表：

項次	工作項目	交付產品項目	交付時程	備考
1	專案啟動 (須於 95/1/1 起正常營運 HCA，不得中斷)	專案執行計畫書（含工作項目、時程規劃、交付項目、組織架構與權責、專案監控、系統測試與維護、建構管理、品質保證及風險管理等）	簽約後 2 週內	
2	1.「醫事憑證 IC 卡」製卡、卡片及密碼寄發作業 2.外部稽核(得標廠商需委由具公信力之第三者執行外部稽核) 3.TSS 之擴充及更新建置。	1.營運作業報告書 2.外部稽核報告書 3.交付 TSS 之軟硬體設備	95/3/31 前	
3	HCA 移轉建置(移轉建置內容請參考本文件附錄三、四之說明)	1.營運系統功能確認報告書(需包含各項軟硬體清單) 2.北、中、南 RAO 教育訓練規劃書	95/4/30 前	
4	1.舉辦 RAO 教育訓練 9 場(得標廠商需於教育訓練前提交北、中、南教育訓練規劃) 2.HCA API 功能增修	1.教育訓練成果報告書 2. HCA API 功能增修報告書	95/6/30 前	

5	「醫事憑證 IC 卡」製卡、卡片及密碼寄發作業	年度工作說明書	95/9/30 前	
6	1.舉辦 RAO 教育訓練 2.內部稽核 3.營運內部控制制度檢討 4.交付本專案系統之原始碼及執行碼	1.內部稽核報告書 2.教育訓練成果報告書 3.營運內部控制制度 4.系統原始碼及執行碼	95/12/31 前	
7	HCA 每月整體運作	HCA 每月整體運作報告	每月十日前	內容及格式由本署另訂

(一)本專案所有文件電子檔均需與 Word 2000 中文版套裝軟體相容。

(二)本專案文件產品大綱需經本署同意，文件內容可參考中華民國資訊軟體協會編製之「軟體技術文件指引」(以最新版本為主）製作。

(三)上述各項文件，請交付紙本各一式 3 份及電子檔 1 份，系統之原始碼及執行碼，則交付光碟片 2 套。

(四)上述各項文件，於交付階段期限 1 週前送交本署初稿一式 2 份，本署於收文後，若有修改意見，則承包廠商需於 1 週內修改完畢，再交付定稿之要求數量(含電子檔)，且書面文件採雙面印刷。

伍、付款方式

一、付款原則

本專案費用以新台幣為付款幣別，得標廠商需於規定交付時程（如遇假日則向後延至次一上班日）內，交付本說明文件第肆章第九節所列各項文件，由本署審核當月所有應交付文件，若內容符合本專案要求，得檢附發票請領當月費用（本案合約總金額十二分之一）。

二、履約保證金

得標廠商應於本專案簽約時按不低於合約總金額百分之十為履約保證金，得標廠商完成交付產品項目及時程表之 1、2、3、4、5、6、7 項次工作經本署驗收合格，並協助本署 96 年度之得標廠商移轉作業順

利完成後，履約保證金無息發還。

陸、罰則

一、延遲扣款規定

(一)本專案認定為交付產品項目與時程表之各項次需求建置完成時一次辦理驗收，並由得標廠商正式行文本署為依據，而非分階段性驗收。

(二)本專案交付產品項目與時程表之各項次需求如有超過交貨完工期限，每延遲 1 日(以日曆天計，星期日、國定假日及其它休息日均應計入)，本署得扣除合約總金額千分之一之逾期性違約金，款項可自應付貨款或履約保證金項中扣抵，違約金上限依採購法之採購契約要項第 45 點規定「違約金以契約價金總額之百分之二十為上限」。屆時若違約金達上限時，本署得以書面要求承包廠商於規定期限內完成改善，若廠商於規定期限內仍未完成，本署得終止合約。

(三)本專案期間本署使用者如發現各 RAO 工作站及專案管理平台有問題，通知得標廠商知悉後，得標廠商應於 4 小時內回覆及著手處理，8 小時內恢復作業。另如為 TSS 系統、HCA 專屬網站、RAO 網站系統、線上開卡(含展期、解鎖卡及更改密碼)服務、憑證廢止清冊公佈服務及憑證狀態查詢服務等問題，應於 1 小時內回覆及著手處理，20 分鐘內啟動備援系統之服務，4 小時內恢復作業。若未能依限處理完成，得作成書面報告說明，經本署同意確認才可免罰，否則每逾 1 日(以日曆天計，星期日、國定假日及其他休息日均應計入)，本署得按合約總金額千分之一計算逾期性違約金，並由應付貨款中扣抵，至扣完為止。

(四)本專案之得標廠商須於 95 年 1 月 1 日前與 94 年度之承包廠商辦理交接，並於 95 年 1 月 1 日立即接續營運，若未能正常營運，則每天扣除總金額百分之一，並於達百分之二十時解除合約。

二、例外辦法

若延遲交貨之原因可歸責於本署或其他不可抗力因素時，得標廠商得於事件發生一週內提出事實報告，並經本署同意後免除此延誤之天數與罰金。

三、未如期履約扣款規定

投標廠商應於建議書中詳列作業需求內容之各項工作成果，分析其對應之經費成本、交付時程，如於期末驗收時，經審查發現有不合格之工作項目，本署有權扣除該項工作之款項。

四、損害賠償

投標廠商於得標後須保證履行契約規定，若於合約進行時使本署蒙受損失或有設備系統安全受損害，無法正常運作時，概由得標廠商負責賠償，而本署得自應付價金中扣抵。

五、權利瑕疵擔保

(一)得標廠商應保證本專案交付本署之產品未侵害他人之著作權及其他權利，如有侵害他人合法權益時，應由得標廠商負責處理並承擔一切法律及賠償責任。

(二)得標廠商所提供之產品，因侵害他人著作權或其他權利，以致本署不得繼續使用時，應按下列方式擇一解決，所衍生出之費用概由得標廠商自行負擔：

1.修改侵權部份，使該產品無觸犯他人權利之虞。

2.徵得權利人授權，使本署能繼續使用該產品，如有費用發生，悉由得標廠商承擔支付。

柒、建議書製作規則

一、簡述

投標廠商建議書之製作，應符合本章之規定。

二、裝訂及交付

(一)裝訂

請用 A4 規格雙面印刷，內容以中文橫式由左至右繕打，裝訂成冊(膠裝)且各部分之章節號碼須前後統一，並標註頁碼，軟或硬式封面不可超越 A4 大小。

(二)投遞

1.截止日期及時間：依公告日期為準。

2.投遞地點：行政院衛生署秘書室(台北市愛國東路 100 號 8 樓)。

3.投遞方式：廠商投標文件連同建議書 12 份、電子檔 1 份送達本署。

4.以上如有變更以招標公告為準。

(三)其他規定

1.建議書不得逾期投遞，否則視為棄權。

2.建議書於投遞時間截止後，不得修改或增訂。

三、一般要求

(一)建議書交付後，本署承諾不得交付本署及評選委員以外之第三者參閱。

(二)製作建議書及合約簽訂前所費之成本，由投標廠商自行負擔，得標後建議書之所有權歸本署。

(三)投標廠商對於徵求建議書說明文件內容有疑問時，請於公告截止 7 日前之上班時間以書面或傳真(2321-7561，梁先生收)提出意見或問題，本署不另舉辦說明會。

(四)本署對投標廠商建議書中所提實績經驗有疑問時，得請投標廠商提出證明文件。

(五)投標廠商可於公告截止 7 日前之上班時間至本署資訊中心參閱「營運移轉計畫書」。

四、建議書項目對照表(請附於目錄之後)

行政院衛生署 95 年度醫療憑證管理中心營運服務案

建議書項目對照表

投標廠商：_____ 製表日期：94 年 月 日

建議書重要項目		建議書內容對應		
項目	內容	內容摘要(請針對內容提出概述)	頁數	備 註
目錄	請附上建議書中與評選項目相關之建議重點及頁次	_____	_____	_____
技術建議	(1)解決方案描述（含全案移轉建置之系統規劃、分析、設計等之方法）			
	(2)軟硬體規格建議			
	(3)對本專案移轉環境及工具所具備能力			
	(4)系統安全及備援規劃（含系統備援、回復及系統安全等規劃）			
管理建議	(1)專案組織與管理（含專案工作小組成員及負責之工作項目,與專案管理計畫及相關系統標準、文件、需求變更等之管理,並請註明專案主持人是否曾接受專案管理師之訓練,另若有顧問參與請於附錄附上合作同意書）			
	(2)專案工作項目劃分、時程、交付產品及重要查核點			
	(3)專案監控、驗收及品質保證措施			
	(4)投標廠商之執行能力（包括實績經驗、如期履約能力及過去類似案件履約績效等）			
	(5)效能管理(含績效指標)			
系統導入及維運建議	(1) 維運服務及支援計畫			
	(2) 系統建置整合			
	(3) 系統測試計畫			
	(4) 系統導入策略（包括時程規劃、系統移轉建置、上線等）			
	(5) 教育訓練計畫			
價格分析	價格分析之合理性(含自由回饋)			
附錄	相關證明文件影本			

捌、建議書評選辦法

一、評選項目

行政院衛生署 95 年度醫療憑證管理中心營運服務案
評選評分表

94 年　　月　　日

委員編號：_____	配分	廠商編號				
評選項目		1	2	3	4	5
1.技術建議 (1)解決方案描述（含全案移轉建置之系統規劃、分析、設計等之方法） (2)軟硬體規格建議 (3)對本專案移轉環境及工具所具備能力 (4)系統安全及備援規劃（含系統備援、回復及系統安全等規劃）	25					
2.管理建議 (1)專案組織與管理（含專案工作小組成員及負責之工作項目，與專案管理計畫及相關系統標準、文件、需求變更等之管理，並請註明專案主持人是否曾接受專案管理師之訓練，另若有顧問參與請於附錄附上合作同意書） (2)專案工作項目劃分、時程、交付產品及重要查核點 (3)專案監控、驗收及品質保證措施 (4)投標廠商之執行能力（包括實績經驗、如期履約能力及過去類似案件履約績效等） (5)效能管理(含績效指標)	25					
3.系統導入及維運建議 (1)維運服務及支援計畫 (2)系統建置整合 (3)系統測試計畫 (4)系統導入策略（包括時程規劃、系統移轉建置、上線等） (5)教育訓練計畫	25					
4.價格分析之合理性(含自由回饋)	25					
評分合計	100					
轉換序位						

評選委員意見：	評選委員簽章：

行政院衛生署 95 年度醫療憑證管理中心營運服務案

序位評選總表

94 年　月　日

廠商 / 序位 / 評選委員	廠商一		廠商二		廠商三		廠商四		廠商五	
	分數	序位	分數	序位	分數	序位	分數	序位	分數	序位
A										
B										
C										
D										
E										
F										
G										
序位合計										
平均分數										
優 勝 序 位										

本專案全部評選委員姓名及職業（如公、教）

姓名							
職業							

出席評選委員簽名：

註：以序位合計數最低者，評定為優勝序位第一；次低者為優勝序位第二；其餘類推。由第一序位者取得優先議價權。

二、評選程序

依據政府採購法第 22 條第 1 項第 9 款及「機關委託專業服務廠商評選及計費辦法」採準用最有利標評選方式決標，評選程序如下：

(一)投標廠商資格審查依招標公告，如有任一項不符者，視為資格審查不合格，其建議書不予審查評選，若全無合格廠商，則依規定予以廢標。

(二)資格審查後合格廠商，始可參加建議書評選；並於資格標審查會當場抽籤(資格審查當天廠商未出席者，由本署代為抽籤)，決定評選會議簡報順序。

(三)建議書審查

1.評選方式由本署依據政府採購法第 94 條組成評選委員會並成立工作小組，該小組將依本章第一節「評選項目」就受評廠商資料擬具評比報告，載明處理意見連同廠商資料送委員會決議。

2.評選委員會依據本章第一節「評選項目」進行評選；除對廠商之建議書進行書面審查外，並由本署召開評選會議，由廠商依據建議書做簡報(20 分鐘)，其後並接受評選委員詢問，採統問統答方式，廠商回答以 10 分鐘為原則，專案負責人必須親自出席。評選會議時間及地點，將於資格審查當場宣布或另備文通知。

3.切結辦法：評選會中，廠商對評選委員疑問提出說明，並可對未盡明確部分提出補充，惟所補充之部分不可更改建議書內容，並作成紀錄為合約的一部分。

4.評選準則

(1)本案採序位法評比，價格納入評分，非複數決標。

(2)投標廠商所提之建議書將依本徵求建議書說明文件之「評選項目」進行評選；各出席評選委員對各廠商依配分評比(即個別委員對各廠商之評選項目分別評分後加總，並依加總分數高低轉換為序位)。

(3)本案合格分數為總平均 70 分以上，未達合格標準者，不得列為協商及決標對象。若無任一家廠商評為合格時，則依規定予以廢標。

(4)合格廠商經由各評選委員評定序位，然後加總各評選委員評定之序位，序位合計最低者為第一名，次低者為第二名，依此類推。但若有二家廠商依前述求得之序位總和相同時，則標價低者優勝序位在前。

(5)二家廠商序位總和相同且標價相同時之處理：以抽籤決定優勝序位先後。由廠商抽籤，若廠商不在，則由委員代為抽籤。

(四)決標方式及程序：

1.本專案依據政府採購法第 22 條第 1 項第 9 款「九、委託專業服務、技術服務或資訊服務，經公開客觀評選為優勝者。」之相關規定辦理，準用最有利標，由評選委員評選優勝廠商。

2.評定合格廠商之優勝序位後，依優勝序位及下列方式之一與合格廠商辦理議價：

(1) 合格廠商為一家者，以議價方式辦理。

(2) 合格廠商在二家以上者，依優勝序位，自最優勝者起，依序以議價方式辦理。

玖、附錄

附錄一、資訊安全保密契約書

行政院衛生署保密契約書

行政院衛生署（以下簡稱甲方）及　　（以下簡稱乙方）雙方同意依「95 年度醫療憑證管理中心營運服務案」（以下簡稱本專案）採購契約書（以下簡稱原契約）中之規定訂定本契約，共同遵守，其條款如下：

壹、乙方承諾於原契約本約有效期間內及本約期滿或終止後，對於所得知或持有甲方所必須保有之公務機密，均應以善良管理人之注意妥為保管及確保其機密性。非經甲方事前書面同意，乙方不得為本人或任何第三人之需要而複製、保有、利用該等公務祕密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等公務機密，或對外發表或出售。

貳、乙方因承辦本專案所獲得業務有關資訊，應依電腦處理個人資料保護法及相關法令之規定恪遵保密原則，並應簽署甲方保密切結書，如有違失，由乙方負全部責任，責任說明如后：刑事責任方面，依據刑法、貪污治罪條例及電腦個人處理資料保護法之相關規定，受政府機關委託之電腦廠商人員雖不具公務員身份，但根據貪污治罪條例第 2 條及電腦處理個人資料保護法第 5 條之規定，如廠商人員行為該當法條之構成要件，仍視為公務員而加重處罰；民事責任方面，如可歸因廠商之事由，致使資料外洩，民眾金錢或權利上受到損害，廠商必須完全負損害賠償責任；行政責任方面，政府採購法第 101 條第 1 項第 12 款規定，因可歸責於廠商之事由，致解除或終止契約者，招標單位應將廠商刊登於政府採購公報上，同法第 103 條第 1 項第 2 款規定，經刊登在政府採購公報上之廠商，於刊登次一日開始一年內，將無法參加所有政府採購之招標。

參、乙方應與本專案工作人員訂定工作契約，乙方有義務告知並要求工作人員嚴守工作契約內容、本專案合約內容及甲方業務機密；乙方及其工作人員應切實依據原契約內容執行業務，執行業務過程中若造成第三人權益損失，概由乙方負責。

肆、乙方依原契約提供甲方服務時，所產生、取得或持有甲方之資料，包括文字、影像、圖形、聲音，不論其儲存於印刷、磁性、光學或其他媒體上，皆屬於甲方所有。除非為提供服務所需，或經甲方書面同意，不得複製、揭露或交付第三人。

伍、乙方不得於甲方之原資訊系統或本專案新開發之資訊系統植入木馬程式，或開啟程式後門漏洞，亦不得未經甲方授權刪除或更改原有帳號權限及開立新帳號存取系統資源。

陸、乙方進入甲方資訊資產存放場所作業或維修，有發生意外事件之虞時，乙方應立即採取防範措施。發生意外可歸因於乙方時，乙方應立即採取搶救、復

原、重建措施並對損害負起賠償責任。

柒、乙方作業之檢查與稽核

1、甲方得定期或不定期派員檢查或稽核乙方提供之服務是否符合本契約之規定，乙方應確實配合辦理並提供甲方書面資料，或協助約談相關當事人。上述檢查或稽核得以不預告之方式進行之，乙方不得拒絕，有關稽核缺失乙方應限期改善不得推諉，如無正當理由未依限改善，以違約論。

2、甲乙雙方得協議委由專業之第三人稽核乙方提供之服務，費用由甲方負擔。

立契約人

甲　方：行政院衛生署

代表人：

地　址：

電　話：

乙　方：

代表人：

地　址：

電　話：

中華民國　　年　　月　　日

附錄二、資訊安全保密切結書

_____公司資訊安全保密切結書（公司）

行政院衛生署（以下簡稱甲方）委託 XXX 公司（以下簡稱乙方）辦理「95年度醫療憑證管理中心營運服務案」（以下簡稱本專案），乙方因執行本專案接觸之公務（機密）資料，具結依下列規定保密並履行責任：

一、乙方於本專案進行期間因進行調查、搜集依合約所產生或所接觸之公務（機密）資料，非經甲方同意或授權，不得以任何形式洩漏或將上開資料再使用或交付第三者。對所獲得或知悉之上述公務（機密）資料，乙方須負保密責任。

二、公務（機密）資料保密期限，不受本專案工作完成（結案）及乙方不同工作地點及時間之限制。乙方持有或獲知公務（機密）資料，不得洩漏或轉讓於第三者。

三、乙方違反本資訊安全保密切結書之規定，致造成甲方或第三者之損害或賠償，乙方同意無條件負擔全部責任，包括因此所致甲方或第三人涉訟，所須支付之一切費用及賠償。於第三人對甲方提出請求、訴訟，經甲方以書面通知乙方提供相關資料，乙方應合作提供，絕無異議。

此致

行政院衛生署

立切結書人

乙　　方（關防）：

負 責 人：

統一編號：

公司地址：

中華民國　　年　　月　　日

＿＿＿＿＿＿＿＿公司資訊安全保密切結書（個人）

立切結書人　　（以下簡稱乙方）參與＿＿＿＿＿＿＿＿**公司**（以下簡稱甲方）辦理「95 年度醫療憑證管理中心營運服務案」（以下簡稱本專案），工作期間因業務需要接觸之公務（機密）資料，乙方願意依下列規定辦理：

一、乙方於專案進行期間因進行調查、搜集依合約所產生或所接觸之公務（機密）資料，非經甲方同意或授權，不得以任何形式洩漏或將上開資料再使用或交付第三者。對所獲得或知悉之上述公務（機密）資料，乙方須負保密責任。

二、公務（機密）資料保密期限，不受專案工作完成（結案）及乙方不同工作地點及時間之限制。乙方持有或獲知公務（機密）資料，不得洩漏或轉讓於第三者。

三、乙方違反本資訊安全保密切結書之規定，致造成甲方或第三者之損害或賠償，乙方同意無條件負擔全部責任，包括因此所致甲方或第三人涉訟，所須支付之一切費用及賠償。於第三人對甲方提出請求、訴訟，經甲方以書面通知乙方提供相關資料，乙方應合作提供，絕無異議。

此致

＿＿＿＿＿＿＿＿**公司**

立切結書人

姓　　名：

身份證字號：

戶 籍 地 址：

中華民國　　年　　月　　日

附錄三、醫療憑證管理中心(HCA)移轉建置規格及需求說明

1. 移轉建置明細

以下移轉內容為前承接本專案廠商之程式移轉明細，得標廠商須沿用移轉之程式執行專案。

(1)HCA 憑證機房軟體明細

NO	建構項目名稱	產品型號／規格	數量	作業系統
1	憑證系統	CA 硬體加密模組驅動程式及金鑰管理工具	1	WIN 2K Server
		CA 端 IC 智慧卡讀卡機驅動程式		
		CA 憑證中心主系統		
		CA 憑證中心控制台		
2	註冊系統	RA 硬體加密模組驅動程式及金鑰管理工具	2	Solaris 8
		RA 註冊管理中心主系統		
		RA 註冊管理中心設定工具		
		TSA 時戳服務系統		
		OCSP 憑證線上即時狀態查詢系統		
		Agent 代理程式		
3	目錄服務管理系統&時戳服務系統	Directory Server 作業系統	2	Solaris 8
		iPlanet 目錄服務器		
		OCSP Responder 服務器		
		TSA Agent 時戳服務代理程式		
4	金鑰管理系統	KMS 硬體加密模組驅動程式及金鑰管理工具	1	WIN 2K Server
		KMS 資料庫		
		KMS 端 IC 智慧卡 讀卡機驅動程式		
		金鑰管理主系統		
		金鑰管理子系統		
		金鑰伺服子系統		
5	DB	Database Server 作業系統	1	Oracle 8.1.7
		資料庫軟體		
6	製卡檔案管理系統	CMS 憑證管理主控台	1	WIN 2K Server
		CMS 訂單派送程式		
7	資料更新上傳系統	Xml 資料更新程式	1	WIN 2K Server
8	卡片線上作業管理系統	HCA applet 開卡程式	1	WIN 2K Server
		HCA、HPC 解鎖卡程式		
		HCA、HPC 更改密碼程式		
		展期程式		

(2)HCA 專屬網站軟體明細

NO	建構項目名稱	產品型號／規格	數量	備註

NO	建構項目名稱	產品型號／規格	數量	備註
1	WEB Server	Web Server 硬體加密模組驅動程式 及金鑰管理工具	2	Linux 7.3
		網頁伺服器系統		

(3)醫事憑證 IC 卡應用程式

NO	**名 稱**	**主要規格說明**
1	HCA 醫事人員憑證 applet	醫事憑證 IC 卡內之 HCA 醫事人員程式
2	HCA 醫事機構憑證 applet	醫事憑證 IC 卡內之 HCA 醫事機構程式

2. 硬體建置規格建議

以下規格為現行 HCA 使用之硬體明細，得標廠商需使用同等規格或更高等級之硬體建構專案應用系統。

NO	建構項目名稱	產品型號／規格		數量	硬體所在點
1	憑證系統主機	Compaq Proliant DL380	PIII 1.4G 512MB Ram 256K Cache Ultra 160 SCSI 36G IDE x 2 (Hard-Mirrors) Ethernet 100m	1	HCA 主機房
2	註冊系統主機	Sun E420R	450Mhz CPU x 1 2G RAM 18.2G HD x2 360WPS Ethernet 100m*2	1	HCA 主機房
3	目錄服務管理系統及 RAO 網站 主機	Sun E420R	450 Mhz CPU x 1 2G RAM 18.2G HD x2 360WPS iPlant Directory Software	2	HCA 主機房
4	金鑰管理系統 主機	IBM X300	Intel P4 2.0GMhz /256K cache CPU *1 18GB SCSI HDD x1 24X CD ROM, 1.44FDD Dual Intel 10/100Ethernet *1 512MB RAM	1	HCA 主機房

NO	建構項目名稱	產品型號／規格		數量	硬體所在點
5	資料庫 主機	Sun E420R	450Mhz CPU x 1 2G RAM 18.2G HD x2 360WPS 20/40G DDS4 DAT drive(內接) Ethernet 100m*2 Oracle 8i	1	HCA 主機房
6		Diskarray Proware Technology Corp OT-6604	RAID5, SCSI 36GB x5 含 Y Cable	1	HCA 主機房
7	專屬網站主機	Compaq Proliant DL380	PIII 1.4G 512M RAM 256K Cache Ultra3 W/SCSI interface 18G Ultra3 W/SCSI Ethernet 100M	2	HCA 主機房
8	憑證系統 硬體加密模組	nCipher	SCSI 介面 CASE	1	HCA 主機房
9	時戳服務 硬體加密模組	Rainbow	PCI 介面	2	HCA 主機房
10	金鑰管理系統 硬體加密模組	WebSentry	SCSI 介面 CASE	1	HCA 主機房
11		網路集線器 10/100 Switch HUB	24port	1	HCA 主機房
12		防火牆 -Firewall		1	HCA 主機房
13	製卡檔案管理 系統主機	Compaq ML330	P3 1.G 1024MB RAM 18G x 1 HD Dual Intel 10/100Ethernet *1	1	HCA 主機房
14	資料更新 上傳系統主機		P4 1.8G / 512MB 20G x 1 HD ASUS / Broadcom 440x Ethernet *1	1	HCA 主機房
15	卡片線上作業 管理系統主機	PC Server		1	HCA 主機房
16	RAO 設備	神通電腦	P4 1.7G 256MB RAM 40GB HD 15"MON Ethernet 10/100M *1 IC 卡暨讀卡機*2	43	RAO

NO	建構項目名稱	產品型號／規格		數量	硬體所在點
17		IBM A50P PC	P4 2.4G 256MB RAM 40GB HD BENQ 15" TFT LCD Ethernet 10/100M *1 IC 卡暨讀卡機*2	30	RAO
18	SP-55 印卡機		中文罕字印卡使用	1	HCA 營運中心
19	憑證系統 備援主機	PC Server	P4 3.0G 512M RAM *2 80G HD	1	HCA 備援機房
20	註冊系統 備援主機	SUN E220R	450M CPU *1 2G RAM 18.2G HD *2	1	HCA 備援機房
21	RAO 網站備援 主機	SUN E420R	450M CPU *1 2G RAM 18.2G HD *2	1	HCA 備援機房
22	DB 備援主機	PC Server	P4 3.0G 512M RAM *4 160G *2 Raid1(SATA)	1	HCA 備援機房
23	金鑰管理系統/ 製卡檔案管理 系統備援主機	PC Server	P4 3.0G 512M RAM *2 80G HD	1	HCA 備援機房
24	資料更新上傳 系統/卡片線上 作業管理系統 備援主機	PC Server	P4 2.6G 512M RAM *1 80G HD	1	HCA 備援機房
25	憑證系統備援 硬體加密模組	nCipher	SCSI 介面 CASE	1	HCA 備援機房
26	時戳服務備援 硬體加密模組	Rainbow	PCI 介面	1	HCA 備援機房
27	金鑰管理系統 備援硬體 加密模組	WebSentry	PCI 介面	1	HCA 備援機房

3. 移轉建置規格需求

得標廠商需配合本署規劃之營運移轉計畫，執行與前期承接專案廠商之移轉作業，並進行建置 HCA 各軟硬體系統。以下針對 HCA 規格需求做說明：

(1)建置架構及說明

包括 HCA 軟硬體設備建置，專屬機房建置，作業環境之建置，專屬網站之建置，IC 卡客製化及發卡作業等。本項作業係建立一套憑證管理機制，並建置憑證管理系統、註冊伺服系統等相關資訊系統，對 HCA 及各衛生行政機關、醫事機構、醫事人員所進行的憑證作業流程執行嚴密的監控管理。

得標廠商依照所設計之作業流程及時程，進行憑證管理中心之建置，並遵循下列原則：

A.採集中式憑證管理中心之建置，將醫事憑證系統、RAO 網站系統、卡片線上作業管理系統及專屬網站系統，置於同一機房內管理。專案管理平台則建置於外；本署醫事處、全國各縣市衛生局與台北市、高雄市及台北縣所屬衛生所至少計 72 個地點建置為 RAO，各項憑證管理所需軟硬體設備並與本署 HIN 網路連接。

B.由得標廠商負責提供本專案專屬機房，並須具備獨立的基礎設施(含電源、空調、網路…等)、門禁設施、安全及防災設施等，並經本署同意後辦理。

C.卡片及憑證發放種類說明如下：

(A)醫事人員憑證 IC 卡

包含全國所有經考試合格或領有醫療相關專業執照、證書之醫事人員。

(B)醫事機構憑證 IC 卡正卡

包含全國所有經申請合格且執業狀態為執業，而由本署醫事處認定之醫事機構。

(C)醫事機構憑證 IC 卡副卡

領有醫事機構憑證 IC 卡正卡之醫事機構可申請副卡。

(D)伺服器應用軟體憑證

發放予醫療應用之伺服器應用軟體。

(E)醫師備用卡

僅提供健保第二階段上線功能使用。

D.本專案憑證服務之儲存媒體全面採用 IC 卡。所採購 IC 卡及得標廠商所設計之機制必須與中央健保局之健保 IC 卡、安全模組(SAM)相容，所需之相關資料則由本署負責協調健保局提供。本專案使用之卡片數量由本署規劃安全庫存量於 95 年底前使用。若卡片數量不夠，本署將透過卡片採購議價之方式添購辦理。

E.本專案之網路規劃，得標廠商應提供規劃建議並交由本署審核同意後，由本署統籌調整建置於 HIN 之中。另本專案中設置 HCA 機房與 HIN 連結所需之數據專線、頻寬需求、線路申裝等，須由得標廠商提供規劃建議，並俟本署審查同意後由本署統一辦理，數據專線之相關費用由本署支付。惟在本專案期程內，本署將進行 HIN 電路流量監控，若平均月通訊流量超過百分之四十，或連續三天每日有連續三小時尖峰通訊流量超過百分之八十，本署將主動提升速率或調整網路架構並告知得標廠商，得標廠商需配合免費提供本專案所提專屬機房之網路設備或更新設備模組，並符合本署整體規劃要求。

F.本專案採用之密碼系統及硬體密碼模組，不論國內外產品，均必須由原廠出具切結文件，保證無金鑰代管之事實。

(2)業務需求

A.細部作業設計，應含：

(A)HCA 及 RAO 之設立及運作方式。

(B)HCA 營運作業建置(包含 IC 卡片發放控管、憑證用戶憑證狀態控管、客服服務 0800 四線專線管理)。

(C)機房管理。

(D)相關憑證之功能及所需配合事項。

(E)IC 卡之空間、存放資料及相關標準、介面之延續。

(F)相關安全機制。

(G)時戳服務機制。

(H)整體時程、檢核點規劃。

(I)軟硬體需求與數量。

B.IC 卡片製作、圖樣底稿需沿用現行 IC 卡片製作之方式及樣板。

C.軟硬體系統之建置

依照細部作業規劃之內容，進行相關軟硬體資訊系統之建置，例如相關發卡作業及 HCA、醫事憑證 RA 之建置、安全管理稽核建置措施等。

D.系統運作

於整體系統建置完成後，由得標廠商依計畫作業項目，進行系統之運作，例如相關發卡及 HCA、醫事憑證 RA 之運作等。

E.軟硬體維護

於本專案期程內，由廠商進行相關軟硬體設備之維護工作。

F.軟硬體更新

於本專案期程內，若有新技術或新設備推出，由得標廠商徵得本署同意後，在不影響相關作業下，進行相關軟硬體之更新工作。

G.建立作業程序標準及完整系統文件。

(3)技術需求與規格

A.公鑰憑證服務

本專案之公鑰憑證服務，至少包含下列之作業及技術需求：

(A)憑證作業

投標廠商至少須提供下列憑證作業，並於建議書中詳細說明其作業方式：

a. 憑證申請

b. 憑證展期

c. 憑證廢止

d. 憑證廢止清冊管理

e.安全保密函式庫(API)

(B)技術需求

a. IC 卡功能需求

(a).卡片內至少應存放一份專為醫事機構或醫事人員使用的電子憑證金鑰對。

(b).卡片除提供電子簽章的功能外，並需提供電子憑證驗證(verification)功能。

(c).卡片須提供資料加解密(encryption/decryption)功能。

(d).卡片須提供私密金鑰自行產生(key generator)功能，也可由外界產生再寫入，但私密金鑰是不允許被讀出的。

b. IC 卡防偽變造設計

投標廠商須於建議書中提供 IC 卡防偽變造設計及實作方式，且等於或優於下述規格。

(a).扭索狀及彩虹紋印刷(Guilloche and Rainbow Printing)

(b).細微字印刷(Microline Printing)

(c).彩虹印刷效果(Rainbow Printing effect/Mimic half-tone printing)

(d).光學變色油墨印刷(Optical Variable Ink(OVI) Printing)

(e).紫外線隱形墨水印刷(Ultraviolet Fluorescent Ink (UV) Printing)

(f).照片背景淡化處理功能(Softened Photo Back- Ground)

c. 得標廠商於契約生效日起對 IC 卡存放資料內容，應配合本署健保局之需求作必要之修正。

B.憑證管理中心技術規範

(A)憑證格式：符合 CPS 之 ITU-T Recommendation X.509 V3(1997)(含)以上及 PKIX Certificate and CRL Profile (IETF RFC 2459 或更新版)。

(B)憑證廢止清冊：符合 CPS 之 ITU-T Recommendation X.509 V2(1997)(含)以上及 PKIX Certificate and CRL Profile (IETF RFC 2459 或更新版)。

(C)線上憑證狀態查詢服務：支援憑證狀態之線上查詢介面(OCSP)。

(D)非對稱金鑰數位簽章演算法：演算法必須符合 RSA 或 El Gamal 或 Elliptic-curve，金鑰長度 1024 bits(含)以上，加解密格式符合 PKCS#1 (V1.5/V2.1)。

(E)非對稱金鑰數位簽章演算法：演算法必須符合 RSA with SHA-1，金鑰長度 1024 bits(含)以上，簽章格式符合 PKCS #1(V1.5/V2.1)。

(F)對稱金鑰加解密演算法：符合 Triple-DES、金鑰長度 128 bits(含)以上，或符合 AES、金鑰長度 128 bits(含)以上。

(G)私密金鑰語法及保護方式：符合 PKCS #12 V1.0 或使用 RSA IC 卡。

(H)雜湊函數演算法：至少應提供 SHA-1 的演算方法標準。

(I)建立「金鑰回復機制」 (Key Recovery)：提供醫事機構憑證申請者加解密私密金鑰回復功能，以確保私鑰擁有者不慎遺失或遭不當使用時之回復作業。

(J)數位信封標準: 語法符合Cryptographic Message Syntax Standard (PKCS #7 V1.5 或更新版)或 Cryptographic Message Syntax (CMS)(IETF RFC 2630 或更新版)。

(K)憑證管理訊息格式與協定：符合 Certificate Management

Protocol(CMP)(IETF RFC 2510 或更新版)或 Certificate Management Messages over CMS(CMC)(IETF RFC 2797 或更新版)。

(L)憑證簽發要求格式:符合Certificate Request Message Format (CRMF)(IETF RFC 2511 或更新版)或 Certification Request Syntax Standard(PKCS #10 V1.7 或更新版)。

(M)憑證申辦審核格式：符合 PKIX 標準語法及通訊協定。

(N)ASN.1 語法及編號：符合 ITU-T X.208(1988)、X.209(1988)及 X.680(1997)、X.681(1997)、X.682(1997)、X.690(1997)、X.691(1997)(含)以上。

(O)授權管理基礎建設(Privilege Management Infrastructure, PMI)：符合 ITU-T X.509 4th Edition Draft V8(含)以上。

(P)時戳服務：符合 PKIX Time Stamp Protocol Draft 15(含)以上。

(Q)支援 Secure Socket Layer(SSL)安全協定。

(R)支援 Secure/Multipurpose Mail Extensions(S/M/ME)。

(S)提供標準圖形化 IC 卡登入介面。

(T)提供標準憑證儲存模式以利各式應用程式使用

(U)安全等級：

認證中心金鑰之產製、儲存及運算均在獨立之密碼伺服器中 HSM 電路執行完成，其過程完全不使金鑰在作業系統使用的記憶體出現。密碼伺服器需具備防暴侵入(Tamper Resistance)、IC 卡開機控制、IC 卡金鑰分持備份。憑證管理中心之加密模組至少應通過 FIPS140-1 Level 3 (含) 以上或 ITSEC Level 3 (含)或同等級產品之認證 (應提供證明)，需具備金鑰回復功能(KEY RECOVERY) (應提供證明)，以確保金鑰管理之安全無虞，或被不當使用時進行回復作業。同時憑證之核發必須經過面對面確認或本署所認證開發之醫事憑證線上申辦系統核可。

(V)憑證政策及憑證實務作業基準：

符合 PKIX Certificate Policy and Certification Practices Framework(IETF RFC 2527 或更新版)。

附錄四、醫療憑證管理中心(HCA)現行資料庫架構(參考)

CA 系統資料庫

Table	Name
→	BUSINESSDOMAIN
→	CAAUDIT
→	CACERT
→	CADETAIL
→	CAKEY
→	CANEXTKEY
→	CAOP
→	CONSOLEAUDIT
→	KEYSTORE
→	RACERT
→	RADETAIL
→	RAOP
→	SYSLMK
→	USERCERT

Table(s) of "BUSINESSDOMAIN" Entity

Name	Comment	Column
BUSINESSDOMAIN	業務識別資料	→

Column(s) of "BUSINESSDOMAIN" Table

Name	Datatype	Comment	Is PK
DOMAINID	VARCHAR2(50)	業務識別名稱	Yes
RAID	VARCHAR2(2)	RA 識別號	No
O	VARCHAR2(50)	組織名稱	No
OU	VARCHAR2(50)	單位名稱	No
CN	VARCHAR2(50)	識別名稱	No
OTHERQUALIFIER	VARCHAR2(50)	保留欄位	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "CAAUDIT" Entity

Name	Comment	Column
CAAUDIT	CA 伺服器稽核紀錄	→

Column(s) of "CAAUDIT" Table

Name	Datatype	Comment	Is PK
SN	NUMBER(20)	流水號	Yes
CAOPID	VARCHAR2(50)	操作人員	No
AUDITTIME	DATE	稽核時間	No
AUDITEVENT	VARCHAR2(100)	稽核事件	No
AUDITRESULT	VARCHAR2(100)	稽核結果	No
AUDITSOURCE	NUMBER(2)	稽核來源 1.Console 2.CA / RA Process 3.Database 4.Token 5.CryptoOthers	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "CACERT" Entity

Name	Comment	Column
CACERT	CA 憑證資料	→

Column(s) of "CACERT" Table

Name	Datatype	Comment	Is PK
CAID	VARCHAR2(2)	CA 識別號	Yes
B64CERT1	VARCHAR2(255)	CA 憑證資料 1	No
B64CERT2	VARCHAR2(255)	CA 憑證資料 2	No
B64CERT3	VARCHAR2(255)	CA 憑證資料 3	No
B64CERT4	VARCHAR2(255)	CA 憑證資料 4	No
B64CERT5	VARCHAR2(255)	CA 憑證資料 5	No
B64CERT6	VARCHAR2(255)	CA 憑證資料 6	No
CERTPATH	VARCHAR2(100)	保留欄位	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "CADETAIL" Entity

Name	Comment	Column
CADETAIL	CA 伺服器資料	→

Column(s) of "CADETAIL" Table

Name	Datatype	Comment	Is PK
CAID	VARCHAR2(2)	CA 識別號	Yes
SYSID	VARCHAR2(2)	系統識別號	No
C	VARCHAR2(2)	國家代碼	No
O	VARCHAR2(50)	組織名稱	No
OU	VARCHAR2(50)	單位名稱	No
CN	VARCHAR2(50)	識別名稱	No
E	VARCHAR2(50)	電子郵件	No
ADDR	VARCHAR2(100)	地址	No
TELNO	VARCHAR2(20)	電話號碼	No
FAXNO	VARCHAR2(20)	傳真號碼	No
HASHALG	NUMBER(2)	憑證演算法 1: MD52: Sha1	No
CAKEYLENGTH	NUMBER(8)	CA 金鑰長度 1024 / 2048 / 409	No
USERDKEYLENGTH	NUMBER(8)	使用者金鑰長度 1024 / 2048	No
LASTCRLPUBLISHING	DATE	最後一次 CRL 公佈時間	No
CRLPERIOD	NUMBER(4)	CRL 公佈週期	No
CRLLOCATION	VARCHAR2(100)	匯出 CRL 目的地	No
CURRENTCERTID	VARCHAR2(18)	目前憑證序號	No
B64EMACKEY	VARCHAR2(30)	押碼金鑰	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "CAKEY" Entity

Name	Comment	Column
CAKEY	CA 伺服器金鑰檔	→

Column(s) of "CAKEY" Table

Name	Datatype	Comment	Is PK
CAID	VARCHAR2(2)	CA 識別號	Yes
B64PRIKEY1	VARCHAR2(255)	加密之 CA 私密金鑰 1	No
B64PRIKEY2	VARCHAR2(255)	加密之 CA 私密金鑰 2	No

B64PRIKEY3	VARCHAR2(255)	加密之 CA 私密金鑰 3	No
B64PRIKEY4	VARCHAR2(255)	加密之 CA 私密金鑰 4	No
B64PRIKEY5	VARCHAR2(255)	加密之 CA 私密金鑰 5	No
B64PRIKEY6	VARCHAR2(255)	加密之 CA 私密金鑰 6	No
B64PRIKEY7	VARCHAR2(255)	加密之 CA 私密金鑰 7	No
B64PRIKEY8	VARCHAR2(255)	加密之 CA 私密金鑰 8	No
B64PRIKEY9	VARCHAR2(255)	加密之 CA 私密金鑰 9	No
B64PRIKEY10	VARCHAR2(255)	加密之 CA 私密金鑰 10	No
B64PRIKEY11	VARCHAR2(255)	加密之CA私密金鑰 11	No
B64PRIKEY12	VARCHAR2(255)	加密之 CA 私密金鑰 12	No
B64PRIKEY13	VARCHAR2(255)	加密之 CA 私密金鑰 13	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "CANEXTKEY" Entity

Name	Comment	Column
CANEXTKEY	CA 伺服器金鑰檔	→

Column(s) of "CANEXTKEY" Table

Name	Datatype	Comment	Is PK
CAID	VARCHAR2(2)	CA 識別號	Yes
NEXTB64PRIKEY1	VARCHAR2(255)	加密之 CA 備用私密金鑰 1	No
NEXTB64PRIKEY2	VARCHAR2(255)	加密之 CA 備用私密金鑰 2	No
NEXTB64PRIKEY3	VARCHAR2(255)	加密之 CA 備用私密金鑰 3	No
NEXTB64PRIKEY4	VARCHAR2(255)	加密之 CA 備用私密金鑰 4	No
NEXTB64PRIKEY5	VARCHAR2(255)	加密之 CA 備用私密金鑰 5	No
NEXTB64PRIKEY6	VARCHAR2(255)	加密之 CA 備用私密金鑰 6	No
NEXTB64PRIKEY7	VARCHAR2(255)	加密之 CA 備用私密金鑰 7	No
NEXTB64PRIKEY8	VARCHAR2(255)	加密之 CA 備用私密金鑰 8	No
NEXTB64PRIKEY9	VARCHAR2(255)	加密之 CA 備用私密金鑰 9	No
NEXTB64PRIKEY10	VARCHAR2(255)	加密之 CA 備用私密	No

		金鑰 10	
NEXTB64PRIKEY11	VARCHAR2(255)	加密之 CA 備用私密金鑰 11	No
NEXTB64PRIKEY12	VARCHAR2(255)	加密之 CA 備用私密金鑰 12	No
NEXTB64PRIKEY13	VARCHAR2(255)	加密之 CA 備用私密金鑰 13	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "CAOP" Entity

Name	Comment	Column
CAOP	Console 操作人員資料檔	→

Column(s) of "CAOP" Table

Name	Datatype	Comment	Is PK
CAOPID	VARCHAR2(50)	Console 登入帳號	Yes
CAID	VARCHAR2(2)	CA 識別號	No
OPAUTHCODE	VARCHAR2(30)	資料壓碼	No
OPLEVEL	NUMBER(2)	授權層級 1: Administrator2: Authorizer3: Operator	No
AUTHTYPE	NUMBER(2)	身份驗證方式 1: 密碼 2: IC 智慧卡	No
FULLNAME	VARCHAR2(50)	完整名稱	No
INITFLAG	NUMBER(2)	初始旗標 0: 帳號未曾登入 1: 帳號已登入	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "CONSOLEAUDIT" Entity

Name	Comment	Column
CONSOLEAUDIT	Console 稽核紀錄	→

Column(s) of "CONSOLEAUDIT" Table

Name	Datatype	Comment	Is PK
SN	NUMBER(20)	流水號	Yes
CAOPID	VARCHAR2(50)	操作員代碼	No
AUDITTIME	DATE	稽核時間	No
AUDITEVENT	VARCHAR2(100)	稽核事件	No
AUDITRESULT	VARCHAR2(100)	稽核結果	No
AUDITSOURCE	NUMBER(2)	稽核來源	No

B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "KEYSTORE" Entity

Name	Comment	Column
KEYSTORE	其他金鑰資料	→

Column(s) of "KEYSTORE" Table

Name	Datatype	Comment	Is PK
KEYTYPE	NUMBER(4)	金鑰型別	No
KEYLABEL	VARCHAR2(128)	金鑰標籤名稱	No
B64EKEY	VARCHAR2(2048)	加密後的金鑰	No
MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "RACERT" Entity

Name	Comment	Column
RACERT	RAOP 人員憑證資料	→

Column(s) of "RACERT" Table

Name	Datatype	Comment	Is PK
CERTID	VARCHAR2(20)	憑證序號	Yes
RAOPID	VARCHAR2(50)	RAOP 人員識別號	No
B64CERT1	VARCHAR2(255)	RAOP 人員憑證 1	No
B64CERT2	VARCHAR2(255)	RAOP 人員憑證 2	No
B64CERT3	VARCHAR2(255)	RAOP 人員憑證 3	No
B64CERT4	VARCHAR2(255)	RAOP 人員憑證 4	No
B64CERT5	VARCHAR2(255)	RAOP 人員憑證 5	No
B64CERT6	VARCHAR2(255)	RAOP 人員憑證 6	No
ISSUEDATE	DATE	憑證取得時間	No
EXPIREDATE	DATE	憑證到期時間	No
CERTSTATUS	NUMBER(2)	憑證狀態 1: 憑證啟用中 2: 憑證暫停 3: 憑證已中止 4: 憑證已到期	No
CAOPID	VARCHAR2(50)	審核憑證人員代碼	No
CERTSTATUSUPDATEDATE	DATE	憑證狀態異動時間	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "RADETAIL" Entity

Name	Comment	Column
RADETAIL	RA 伺服器資料	→

Column(s) of "RADETAIL" Table

Name	Datatype	Comment	Is PK
RAID	VARCHAR2(2)	RA 識別號	Yes
CAID	VARCHAR2(2)	CA 識別號	No
O	VARCHAR2(50)	組織名稱	No
B64EMACKEY	VARCHAR2(30)	押碼金鑰	No
CURRENTUUID	VARCHAR2(18)	最後取得之使用者識別號	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "RAOP" Entity

Name	Comment	Column
RAOP	RAOP 人員資料	→

Column(s) of "RAOP" Table

Name	Datatype	Comment	Is PK
RAOPID	VARCHAR2(50)	RAOP 人員識別號	Yes
RAID	VARCHAR2(2)	RA 識別號	No
C	VARCHAR2(2)	國家代碼	No
O	VARCHAR2(50)	組織名稱	No
OU	VARCHAR2(50)	單位名稱	No
CN	VARCHAR2(50)	識別名稱	No
E	VARCHAR2(50)	email	No
ADDR	VARCHAR2(100)	地址	No
TELNO	VARCHAR2(20)	電話	No
CAOPID	VARCHAR2(50)	審核憑證人員代碼	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "SYSLMK" Entity

Name	Comment	Column
SYSLMK	系統押碼資料	→

Column(s) of "SYSLMK" Table

Name	Datatype	Comment	Is PK
SYSID	VARCHAR2(2)	系統代號	Yes
B64HLMK	VARCHAR2(30)	保密基碼特徵值(hash)	No
B64EKEK	VARCHAR2(30)	加密之 Key Encrypt Key	No
INITFLAG	NUMBER(2)	初始旗標 0: 系統未初始化 1: 系統已初始化完成	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "USERCERT" Entity

Name	Comment	Column
USERCERT	使用者憑證資料	→

Column(s) of "USERCERT" Table

Name	Datatype	Comment	Is PK
CERTID	VARCHAR2(20)	憑證序號	Yes
UUID	VARCHAR2(20)	使用者識別號	No
USERID	VARCHAR2(20)	機構代碼或人員證號	No
B64CERT1	VARCHAR2(255)	憑證內容 1	No
B64CERT2	VARCHAR2(255)	憑證內容 2	No
B64CERT3	VARCHAR2(255)	憑證內容 3	No
B64CERT4	VARCHAR2(255)	憑證內容 4	No
B64CERT5	VARCHAR2(255)	憑證內容 5	No
B64CERT6	VARCHAR2(2048)	憑證內容 6	No
ISSUEDATE	DATE	憑證啟用時間	No
EXPIREDATE	DATE	憑證到期時間	No
CERTSTATUS	NUMBER(2)	憑證狀態	No
CAOPID	VARCHAR2(50)	審核憑證人員代碼	No
CERTSTATUSUPDATEDATE	DATE	憑證狀態異動時間	No
RENEWFLAG	NUMBER(2)	保留欄位	No
DOWNLOADFLAG	NUMBER(2)	下載憑證旗標 0: 已下載完成 1-5：已通知下載次數	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

註冊系統資料庫

Table	Name
→	ENROLLMENT
→	SIAUDIT

Table(s) of "ENROLLMENT" Entity

Name	Comment	Column
ENROLLMENT	憑證申請資料	→

Column(s) of "ENROLLMENT" Table

Name	Datatype	Comment	Is PK
APPLYID	NUMBER(20)	流水號	Yes
USERID	VARCHAR2(20)	機構代碼或人員證號	No
OWNERID	VARCHAR2(20)	負責人身份證字號	No
APPLYTIME	DATE	申請時間	No
C	VARCHAR2(50)	國家代碼	No
O	VARCHAR2(128)	組織名稱	No
OU	VARCHAR2(128)	單位名稱	No
CN	VARCHAR2(128)	識別名稱	No
E	VARCHAR2(128)	電子郵件	No
OWNERNAME	VARCHAR2(128)	負責人姓名	No
APPLIANTID	VARCHAR2(128)	申請人身分字號	No
APPLIANTNAME	VARCHAR2(50)	申請人姓名	No
ALTEMAIL1	VARCHAR2(128)	備用電子郵件 1	No
ALTEMAIL2	VARCHAR2(128)	備用電子郵件 2	No
ADDRCITY	VARCHAR2(20)	地址(城市)	No
ADDRZIPCD	VARCHAR2(20)	地址(郵遞區號)	No
ADDR	VARCHAR2(255)	地址	No
CONTADDRCITY	VARCHAR2(20)	聯絡地址(城市)	No
CONTADDRZIPCD	VARCHAR2(20)	聯絡地址(郵遞區號)	No
CONTACTADDR	VARCHAR2(255)	聯絡地址	No
TELNO	VARCHAR2(20)	電話號碼	No
FAXNO	VARCHAR2(20)	傳真號碼	No
REFID1	VARCHAR2(20)	備用 ID1	No
REFID2	VARCHAR2(20)	備用 ID2	No
USERTYPE	NUMBER(4)	用戶型別: 1. 機構 2. 人員	No

APPLYSTATUS	NUMBER(2)	申請狀態: 1. ok 2. 拒絕 3. 金鑰回復	No
MEMO	VARCHAR2(255)	備註	No
SOURCE	VARCHAR2(20)	資料來源(RAOID)	No
DELIVERMETHOD	NUMBER(2)	領卡方式: 0.親臨櫃檯 1.郵寄	No
LICSTATUS	NUMBER(2)	證書狀態: 0. 初始化 1. ok	No
LICUPDID	VARCHAR2(20)		No
LICUPDTIME	DATE		No
PICSTATUS	NUMBER(2)	照片狀態: 0. 初始化 1. ok	No
PICUPDID	VARCHAR2(20)		No
PICUPDTIME	DATE		No
FEESTATUS	NUMBER(2)	繳費狀態: 0. 初始化 1. ok	No
FEEUPDID	VARCHAR2(20)		No
FEEUPDTIME	DATE		No
DOMAINID	VARCHAR2(128)	業務範圍	No
B64MAC	VARCHAR2(40)	資料庫押碼	No
CERTIFYSTATUS	NUMBER(4)	憑證狀態: 0. 初始化 1. ok 2. 暫停 3. 廢止 4. 過期	No
UUID	VARCHAR2(20)	使用者識別號	No
FTB64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "SIAUDIT" Entity

Name	Comment	Column
SIAUDIT	RA 稽核紀錄	→

Column(s) of "SIAUDIT" Table

Name	Datatype	Comment	Is PK
LOGID	NUMBER(20)	流水號	No
APPLYID	NUMBER(20)	申請資料項的序號	No

OPID	VARCHAR2(50)	RAO 執行人員識別號	No
AUDITTIME	DATE	稽核時間	No
AUDITEVENT	VARCHAR2(100)	稽核事件	No
AUDITRESULT	VARCHAR2(100)	稽核結果	No
AUDITSOURCE	NUMBER(4)	稽核來源	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

RA 系統資料庫

Table	Name
→	BUSINESSDOMAIN
→	RAAUDIT
→	RADETAIL
→	USERDN
→	USERINFO

Table(s) of "BUSINESSDOMAIN" Entity

Name	Comment	Column
BUSINESSDOMAIN	業務範圍	→

Column(s) of "BUSINESSDOMAIN" Table

Name	Datatype	Comment	Is PK
DOMAINID	VARCHAR2(50)	業務識別名稱	Yes
RAID	VARCHAR2(2)	RA 識別號	No
O	VARCHAR2(50)	組織名稱	No
OU	VARCHAR2(50)	單位名稱	No
CN	VARCHAR2(50)	識別名	No
OTHERQUALIFIER	VARCHAR2(50)	保留欄位	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "RAAUDIT" Entity

Name	Comment	Column
RAAUDIT	RA 伺服器稽核紀錄	→

Column(s) of "RAAUDIT" Table

Name	Datatype	Comment	Is PK
SN	NUMBER(20)	流水號	Yes
AUDITTIME	DATE	稽核時間	No
AUDITEVENT	VARCHAR2(100)	稽核事件	No
AUDITRESULT	VARCHAR2(100)	稽核結果	No
AUDITSOURCE	NUMBER(2)	稽核來源	No
RAOPID	VARCHAR2(50)	執行者	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "RADETAIL" Entity

Name	Comment	Column
RADETAIL	RA 伺服器資料檔	→

Column(s) of "RADETAIL" Table

Name	Datatype	Comment	Is PK
RAID	VARCHAR2(2)	RA 識別號	Yes
CAID	VARCHAR2(2)	CA 識別號	No
O	VARCHAR2(50)	組織名稱	No
B64EMACKEY	VARCHAR2(30)	資料庫押碼金鑰	No
CURRENTUUID	VARCHAR2(18)	最後取得的使用者識別號	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "USERDN" Entity

Name	Comment	Column
USERDN	憑證持有者識別資料	→

Column(s) of "USERDN" Table

Name	Datatype	Comment	Is PK
UUID	VARCHAR2(20)	使用者識別號	Yes
USERID	VARCHAR2(20)	機構代碼或人員證號	No
DOMAINID	VARCHAR2(50)	業務識別名稱	No
C	VARCHAR2(2)	國家代碼	No
O	VARCHAR2(50)	組織名稱	No
OU	VARCHAR2(50)	單位名稱	No
CN	VARCHAR2(50)	識別名稱	No
E	VARCHAR2(50)	電子郵件	No

RAOPID	VARCHAR2(50)	RAO 執行人員	No
CARDACCESSKEY	VARCHAR2(30)	卡片存取密碼	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

Table(s) of "USERINFO" Entity

Name	Comment	Column
USERINFO	憑證持有者基本資料檔	

Column(s) of "USERINFO" Table

Name	Datatype	Comment	Is PK
UUID	VARCHAR2(20)	使用者識別號	Yes
USERID	VARCHAR2(20)	機構代碼或人員證號	No
OWNERID	VARCHAR2(20)	負責人身份證字號	No
OWNERNAME	VARCHAR2(50)	負責人姓名	No
APPLIANTID	VARCHAR2(20)	申請人身份證字號	No
APPLIANTNAME	VARCHAR2(50)	申請人姓名	No
ALTEMAIL1	VARCHAR2(50)	備用電子郵件 1	No
ALTEMAIL2	VARCHAR2(50)	備用電子郵件 2	No
KEYUSERID	VARCHAR2(20)	金鑰保管人代號	No
ADDR	VARCHAR2(100)	地址	No
CONTACTADDR	VARCHAR2(100)	聯絡地址	No
TELNO	VARCHAR2(20)	電話號碼	No
FAXNO	VARCHAR2(20)	傳真號碼	No
REFID1	VARCHAR2(20)	備用 ID1	No
REFID2	VARCHAR2(20)	備用 ID2	No
B64HPW	VARCHAR2(30)	使用者申請憑證密碼特徵值	No
USERTYPE	NUMBER(4)	使用者型別: 1. 機構 2. 人員 3. 伺服器	No
B64MAC	VARCHAR2(40)	資料庫押碼	No

CMS 系統資料庫

Table	Name
→	CMS_PERSO_INFO
→	CMS_RA_REQUEST

Table(s) of "ENROLLMENT" Entity

Name	Comment	Column
CMS_PERSO_INFO	存放製卡個人化資料	→

Column(s) of "CMS_PERSO_INFO" Table

Name	Datatype	Comment	Is PK
IDX	NUMBER(10)	索引	Yes
PERSO_PROFILE	VARCHAR2(255)	製卡設定檔	No
PERSO_CREATE_DATE	DATE	建立日期	No
PERSO_HBUREAU_ID	VARCHAR2(255)	衛生局所代碼	No
PERSO_HOSPITAL_ID	VARCHAR2(255)	醫療機構代碼	No
PERSO_UUID	VARCHAR2(255)	RA 憑證 UUID	No
PERSO_MODE	NUMBER(10)	申請類別 首次/例發/補換	No
PERSO_CARD_TYPE	NUMBER(10)	卡別 機構卡/醫師卡	No
PERSO_APPLY_DATE	DATE	申請日期	No
PERSO_USER_ID	VARCHAR2(255)	機構代號/醫師身分證字號	No
PERSO_CA_CERT	VARCHAR2(4000)	CA 憑證	No
PERSO_USER_CERT1	VARCHAR2(4000)	使用者憑證 1	No
PERSO_USER_PVK1	VARCHAR2(4000)	使用者私鑰 1	No
PERSO_USER_CERT2	VARCHAR2(4000)	使用者憑證 2	No
PERSO_USER_PVK2	VARCHAR2(4000)	使用者私鑰 2	No
PERSO_PIN_BLOCK	VARCHAR2(4000)	PIN BLOCK	No
PERSO_ISSUE_DATE	DATE	發卡日期	No

PERSO_VALID_DATE	DATE	有效日期	No
PERSO_MAIL_ADDRESS	VARCHAR2(255)	郵寄地址	No
PERSO_PUK	VARCHAR2(255)	PUK	No
PERSO_ORDER_IDX	NUMBER(10)	派工單索引	No
PERSO_ICCSN	VARCHAR2(255)	卡片序號	No
PERSO_DELIVER_DATE	DATE	卡片寄發日期	No
PERSO_STATUS	NUMBER(10)	卡片狀態 (1) 新增 (2) 產生製卡檔成功 (3) 產生製卡檔失敗 (4) 製卡成功 (5) 製卡失敗 (6) 簽回 (7) 製作密碼函新增 (8) 製作密碼函成功 (9) 製作密碼函失敗 (10) 終止	No
PERSO_UPDATE_HISTORY	VARCHAR2(4000)	狀態更新歷史紀錄	No
PERSO_GENIMG_ERR_REASON	VARCHAR2(255)	產生製卡檔錯誤原因	No
PERSO_ISSUE_ERR_REASON	VARCHAR2(255)	製卡失敗原因	No
PERSO_PIN_MAILER_IDX	NUMBER(10)	PIN 派工單索引	No
PERSO_MAIL_ZIP	VARCHAR2(255)	郵寄地址(ZIP CODE)	No
PERSO_MAIL_CITY	VARCHAR2(255)	郵寄地址(CITY)	No
PERSO_MAIL_ERR_REASON	VARCHAR2(255)	產生 PIN 製卡檔錯誤原因	No

Table(s) of "ENROLLMENT" Entity

Name	Comment	Column
CMS_RA_REQUEST	CMS 製卡需求資料	→

Column(s) of "CMS_RA_REQUEST" Table

Name	Datatype	Comment	Is PK

RA_UUID	VARCHAR2(255)	RA 憑證 UUID	No
RA_MODE	NUMBER(10)		No
RA_CARD_TYPE	NUMBER(10)	卡片型態	No
RA_APPLY_DATE	DATE	申請日期	No
RA_USER_ID	VARCHAR2(255)	機構代號/醫師身分證字號	No
RA_CA_CERT	VARCHAR2(4000)	CA 憑證	No
RA_USER_CERT1	VARCHAR2(4000)	使用者憑證 1	No
RA_USER_PVK1	VARCHAR2(4000)	使用者私鑰 1	No
RA_USER_CERT2	VARCHAR2(4000)	使用者憑證 2	No
RA_USER_PVK2	VARCHAR2(4000)	使用者私鑰 2	No
RA_PIN_BLOCK	VARCHAR2(4000)	PIN BLOCK	No
RA_ISSUE_DATE	DATE	發卡日期	No
RA_VAILD_DATE	DATE	有效日期	No
RA_MAIL_ADDRESS	VARCHAR2(255)	郵寄地址	No
RA_MAC	VARCHAR2(255)	資料庫押碼	No
RA_MAIL_ZIP	VARCHAR2(255)	郵寄地址(ZIP CODE)	No
RA_MAIL_CITY	VARCHAR2(255)	郵寄地址(CITY)	No