行政院衛生署

99 年度醫事憑證管理中心營運案

The operation project of Healthcare Certification Authority in 2010

徵求企劃書說明文件

投標廠商（蓋章）	負責人（蓋章）

行政院衛生署資訊中心

中華民國 98 年 11 月

目　　錄

壹、簡介

一、背景

為建立衛生醫療電子文件認證機制，提供安全及可信賴的網路環境，確保電子資料傳輸的完整性、機密性、資料來源的身分認證及不可否認性，行政院衛生署(以下簡稱本署)於 92 年 6 月起正式營運醫療憑證管理中心（以下簡稱 HCA1.0），簽發醫事人員及醫事機構憑證 IC 卡，提供電子簽章及加密服務，有效期限為 5 年。為銜接 5 年到期之憑證 IC 卡，及符合政府公開金鑰基礎建設(Government Public Key Infrastructure, GPKI)憑證機制，本署於 97 年建置第二代醫事憑證管理中心(以下簡稱 HCA2.0)，並於同 (97) 年 8 月 13 日獲經濟部核定憑證實務作業基準(Certification Practice Statement , CPS)，及於同年 8 月 19 日正式納入政府憑證總管理中心(Government Root Certification Authority, GRCA)轄下，同年 8 月 21 日起開始簽發第二代醫事憑證 IC 卡，以利憑證服務之持續。截至今(98)年 9 月底止，第一代醫事憑證共發放 157,992 張，第二代則為 68,195 張，合計共 226,187 張。HCA1.0 及 HCA2.0 統稱為 HCA(Healthcare Certification Authority)。

依據 GPKI 憑證政策(Certificate Policy, CP)及 HCA CPS 規定，HCA2.0 憑證用戶首次申請憑證，須臨櫃辦理。本署 HCA 於全國各縣市衛生局、高雄市及台北縣衛生局所轄衛生所、台北市衛生局所轄聯合稽查分隊等共計 71 個地點，設立註冊窗口（Registration Authority Officer, RAO），受理醫事人員、醫事機構或其委託人，臨櫃申請醫事人員、醫事機構憑證 IC 卡及其相關作業。另為提供醫事人員另一個臨櫃申請憑證之管道，HCA 授權醫院設立初審註冊窗口(以下簡稱初審 RAO)，受理該院醫事人員之憑證申請作業。

另依據 GPKI CP 規定，GRCA 轄下各 CA 應配合於 99 年 12 月 31 日停止簽發用戶金鑰長度 RSA 1024 位元之憑證，並改簽發 RSA 2048 位元之憑證，但於此之前所簽發之憑證，仍可使用到效期到期日為止。

「98 年度醫事憑證管理中心營運案」執行期限即將屆滿，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，除密切依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。

二、本文件目的及範圍

為使投標廠商瞭解本專案需求，故製作「99 年度醫事憑證管理中心營運案」徵求企劃書說明文件，向投標廠商說明本署之需求與期望，俾供投標廠商據以提出符合本專案需求之企劃書，並規定投標廠商針對本專案所提出之企劃書應包含的內容。

貳、專案概述

一、專案名稱

本專案名稱為「99 年度醫事憑證管理中心營運案」(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

本專案目標為加強醫療資訊安全防護措施，促進醫療資訊電子化應用，持續營運 HCA 及簽發醫事人員、醫事機構憑證 IC 卡，作為推行醫療電子化作業的安全及可信賴的網路環境。並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，現有作業說明，請參閱附錄一。

四、招標依據

(一)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，評選第 1 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，本專案所需總經費為新台幣 4,226 萬元，其中包含覈實支付部分 1,036,200 元(郵遞相關費用)，由本署 99 年度預算支應。

(二)本專案 99 年度經費將依該年度相關公務預算是否經立法院審查通過，若經費遭刪除，則契約自動失效，若經費遭刪減，將重新與承包廠商進行議約，若議約不成將終止契約，本專案則重新辦理。上述情形承包廠商不得要求任何賠償。

(三)覈實支付費用部分採固定金額給付，列入本案議價(約)範圍。惟決標無須調整各項單價。

(四)投標廠商報價不得逾預算金額，投標廠商報價超過預算金額者，依政府採購法第 50 條第 1 項第 2 款暨行政院公共工程委員會 96 年 10 月 2 日工程企字第 09600396110 號函規定，列為不合格標，不予減價機會。

五、專案範圍

本專案之工作範圍，主要包括下列事項，惟投標廠商可依專案目標、國內實際運作流程及環境、或國際上足以提供參考之實務經驗，建議增加專案工作項目，若建議內容經評選確實對本專案有實質效益，將可於評選作業獲得適當加分：

(一)營運專屬機房

(二)提供 HCA 營運辦公室

(三)營運 HCA2.0 及提供所需相關系統之維運服務

(四)提供 HCA2.0 IC 卡發卡服務

(五)維護 HCA 專屬網站與專案管理平台

(六)維護 HCA 營運中心管理資訊系統

(七)提供營運管理制度及配合外部安全稽核

(八)提供符合 GPKI 規範要求

(九)設置諮詢服務窗口，並提供客戶服務品質管理機制

(十)提供系統危機應變處理機制、災害演習作業及營運移轉規劃

(十一)提供 HCA1.0 對外目錄服務、黑名單公告、儲存庫等相關服務

(十二)完成 TSS 功能增修及設備購置

(十三)完成用戶憑證金鑰長度由 1024 提升為 2048 位元

(十四)提供已開發系統所需之 2048 位元金鑰長度 API 並提供諮詢服務

(十五)辦理教育訓練及說明會

(十六)其它

六、專案時程

本專案時程自 99 年 1 月 1 日(如決標日為 99 年 1 月 1 日以後，則自決標日起)起至 99 年 12 月 31 日止，工作項目及時程將依第參章第八節交付產品項目與時程執行。

參、需求說明

一、HCA2.0 作業需求

(一)營運專屬機房

1.主機房至少有 15 坪(含)以上大小之專屬獨立維運空間，並已通過 ISO27001：2005 之認證。

2.為維持憑證業務活動正常營運及保護 HCA 主機房之安全,以確保工作場所及設備不受侵害、干擾或未經授權之存取，承包廠商必須針對 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。

3.承包廠商應提供足以存放 9 萬張空白卡片及耗材之安全空間。

4.承包廠商採用之 HCA 主機房地點得使用現有機房營運空間,主機房與 GSN VPN 之 E1 網路專線費用由本署另案支付，機房須具備獨立門禁，並符合以下需求：

(1) 基礎設施

A.電源

(A)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，且保證在市電停電 24 小時內服務不會中斷。

(B)提供完整大型不斷電系統且為雙主機備援，確保緊急供電，並提供雙迴路設計。

B.空調

必須有下吹式送風設計、恆溫恆濕示警功能、多主機輪流運轉，以及迴風設計。

C.高架地板

必須為 50 公分(含)以上高架地板，每平方公尺可承重 500 公斤(含)以上。

D.隔間

必須為堅固可靠之隔間，可防止外力破壞入侵。

E.網路介面

必須有 Fast Ethernet(含)以上網路介面。

(2) 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

(A)監視系統

機房出入口及重要區域，均須有 24 小時監視系統，並保存錄影紀錄至少 14 天以上。

(B)機房(含機箱)入侵偵測及警告系統

人員進出機房要有門禁卡，對於任何非經授權之人員強制進入機房(含機箱)，均能主動偵測並發出警告。

C.防災設施

(A)消防設施

必須有防火警報，並有自動滅火設施，至少為 Fire Master 200 System 或同等級(含)以上之系統。

(B)防震設施

必須有防震設施，至少可抵擋五級之地震。

(C)防電磁干擾設施

必須有防止電磁波干擾設施，防電磁之干擾。

(D)防靜電設施

必須有防靜電設施，防止靜電之災害。

D.異地備援

(A)備援機房需建置於距離主機房 30 公里外之區域，於主機房遭遇災難而無法正常運作時，並確認需啟動備援機制後，完成啟動作業，以確保 HCA 之營運，未依規定辦理，將依第伍章第一節第(六)點之罰則說明辦理。備援機房須遵循 ISO27001：2005 之機制營運。

(B)支援備援機制之一般例行性作業並包含透過主、備援機房網路及 SAN 架構進行資料備援。

a.依照 HCA 現行機制，透過點對點光纖線路進行主機房資料庫資料即時備份至備援機房作業。

b.備援機房內之憑證系統主機、註冊系統主機、資料庫主機、備份主機皆需與磁碟陣列共同納入 SAN 架構中。

c.備援機房磁碟陣列遵循現行 Raid 5 架構進行運作。

d.主、備援機房之網路相關費用由本專案支付，頻寬至少為 8 mbps。

e.備援機房與 GSN VPN 之網路相關費用由本專案支付，頻寬至

少為 2 mbps 。

(C)如憑證管理中心發生重大災害，無法運作時，異地備援中心應提供憑證管理中心對外服務功能，直至憑證管理中心恢復正常運作為止。對外服務包含以下：

a.CA 系統簽發憑證、簽發 CRL 服務。

b.RA 系統註冊管理服務。

c.目錄服務管理系統憑證公告、儲存庫管理服務。

d.卡片作業管理及統計作業系統之線上卡片作業服務。

e.專屬網站對外網頁服務。

(二)提供 HCA 營運辦公室

1.承包廠商採用之 HCA 營運辦公室地點得使用現有營運辦公室空間，營運辦公室為專案人員執行營運 HCA 業務之舒適營運辦公環境，至少可同時容納 12 人之座位空間，且至少有 22 坪(含)以上大小之專屬獨立空間，並足以放置現行營運作業文件之收納空間及製卡工作區之空間。

2.卡片個人化作業於營運辦公室執行，同時，卡片個人化作業有關之硬軟體設備應設置於營運辦公室內，且須依製卡作業及日常營運作業需求，適時整合機房與營運辦公室之網路環境，以順利執行卡片個人化作業。

3.承包廠商至少須派駐執行本專案一般營運作業人員至營運辦公室上班，執行一般營運作業之人員至少包含：8 位客服人員、1 位製卡作業人員、1 位一般作業人員，及 1 位營運作業主管(其他軟體技術工程師、硬體維護工程師、系統管理工程師、資料庫管理師等技術人員則不計算在一般營運作業人員範疇內，可不用全年派駐至營運辦公室上班，但須視需求隨時駐點至機房或營運辦公室進行支援)。

(三)營運 HCA2.0 及提供所需相關系統之維運服務

1.承包廠商需負責依現有 HCA2.0 之各項制度規定來營運 HCA2.0，並維持下列各項系統之正常運作，現有作業說明，請參閱附錄一。

(1)憑證管理系統

(2)註冊管理中心系統

(3)金鑰管理系統

(4)個人化製卡管理系統

(5)醫事資料同步交換系統

(6)目錄服務管理系統

(7)卡片作業管理及統計作業系統

(8)營運中心表單影像管理系統

(9)時戳服務系統

(10)API 維護

2.為加強服務品質，請優化現行 HCA2.0 應用系統，其工作內容至少包含以下：

(1)將開卡、解鎖卡等對外存取較頻繁之服務與原 HCA2.0 專屬網站切割，並提供負載平衡設計，以提高使用者存取服務之品質。

(2)將程式開發人員專屬網站獨立於 HCA2.0 專屬網站外，以提供技術開發人員做為 HCA 知識庫專用。此網站內應公告各醫院與 HCA2.0 有關之最新應用進度、最新版本 API、範例程式與技術問答結果等資訊。

(3)使用專屬伺服器運算並提供各醫院自行下載其所屬之憑證到期、廢止清單等資料檔案，以減低使用者要自行解析 CRL 之負擔。

(4)因應醫療院所應用需求，調整、優化或重新設計及建置 HCA2.0 相關應用系統。

(5)承包廠商應提出上述各項 HCA 應用系統優化工作，其整體硬體調配原則。

3.為配合電子病歷及其他醫事應用之推廣，醫療院所或醫療資訊廠商詢問 API 相關問題（含 2048 位元金鑰長度之升級問題），如於線上無法解決者，承包廠商需適時提供到點人力技術服務(全年度至少 24 次到點服務)，以協助醫療院所順利導入醫事憑證之應用，上述到點支援狀況，請於每月營運報告中詳述。

(四)提供 HCA2.0 IC 卡發卡服務

1.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)通知用戶申請

卡片到期通知應每月寄發予隔月卡片將到期之使用者，並於通知內註明使用者應於卡片到期前至 RAO(或初審 RAO)進行卡片換發申請作業。

(2)用戶申請作業

A.醫事人員可線上進行預約申請，再至 RAO(或初審 RAO)進行臨櫃

申辦，或直接透過 RAO(或初審 RAO)進行臨櫃申辦。相關作業產出之紙本資料並由 RAO(或初審 RAO)自行歸檔。

B.本署附屬機關、醫事機構或醫事相關公學協會亦可扮演初審 RAO 角色，初審 RAO 可提供單筆及批次醫事人員申辦作業。承包廠商須輔導建置有意願承接初審註冊業務之初審 RAO，並明訂其相關權責義務等規範。

C.醫事機構正卡之憑證必須透過公文書向本署進行申辦，附卡及非 IC 卡載具之憑證則可透過線上安全驗證程序，進行線上申辦。

D.伺服器應用軟體憑證申請者若為醫事機構，其申請程序與醫事機構附卡申請程序相同。申請者若非為醫事機構，其申請程序與醫事機構正卡申請程序相同。

(3)用戶身分驗證

醫事人員憑證 IC 卡須進行臨櫃申辦，透過身分驗證無誤後，方可進行申辦作業，申辦之過程中應由用戶自行設定用戶代碼。HCA2.0 首張醫事機構憑證 IC 卡則必須透過公文書進行核對或透過臨櫃驗證後，方能申辦，非首張之醫事機構附卡或非以 IC 卡為載具之各類憑證可透過已申辦過之醫事機構憑證 IC 卡驗證後進行申辦。

(4)卡片個人化、製發卡及卡片遞送程序

A.卡片製作應包含卡體防偽印刷、卡片顯性資料印刷、卡片隱性資料個人化、卡衣及郵寄信封製作等程序。

B.用戶申請憑證核可後，承包廠商應透過製發卡管理系統協助產製相關憑證 IC 卡。製發卡管理系統應透過安全之管道取得並妥善管理卡片個人化資料(包括製卡檔、卡片金鑰對等)。取得資料後尚應通過授權金鑰(金鑰應保存於本專案提供之硬體保密模組)之許可才可進行卡片個人化作業。個人化程序應產生相關之製卡回復檔，並記錄存查。

C.卡片遞送方式則需透過專人或掛號郵寄方式進行遞送，用戶申請憑證 IC 卡時，可選擇 HCA2.0 提供之領卡地點進行領卡。

(5)卡片寄發簽收程序

提供各領卡承辦人員(包含用戶自行領卡)線上進行卡片簽收作業程序。

(6)用戶接受、啟動卡片程序

用戶透過線上機制，以用戶代碼認證後進行用戶權利同意書確

認並取得 PIN 碼，透過 PIN 碼以線上開卡方式接受憑證並啟動卡片。用戶接受憑證後，HCA2.0 方可公布用戶憑證於儲存庫中。

(7)卡片停復用、廢止程序

需提供臨櫃、線上及 0800 電話申請等多重管道，卡片廢止作業僅可採臨櫃申辦方式申請。

2.卡片管理與採購

A.本專案使用之空白 IC 卡及製卡作業之耗材由本署提供，營運期間，承包廠商應將卡片及耗材妥善保管與管理。

B.上述卡片僅供本專案醫事機構憑證 IC 卡(含附卡)、醫事人員憑證 IC 卡、測試卡、備用卡及全民健康保險特約藥局專用卡(簡稱藥局專用卡)等使用。

C.空白卡片庫存低於 10,000 張時，承包廠商應通知本署，IC 卡片數量及製卡機耗材不足的部分由本署另案編列經費。

D.發放之 IC 卡若於客製化過程中發現卡片為壞卡無法製發時，承包廠商須通知本署對提供卡片之廠商進行卡片一對一汰換。

3.簽發憑證與製作 IC 卡之過程中，若需取得本署醫事管理系統資料庫之資料，則需配合使用本署醫事管理系統提供之應用程式介面或資料介接協定，進行資料庫異動資料同步作業。

(五)維護 HCA 專屬網站與專案管理平台

1.HCA 對外營運之網站系統

HCA 對外營運之專屬網站(http://hca.nat.gov.tw)，內容包含 HCA 各項訊息、公告及文件下載、鏈結儲存庫、目錄服務、卡片作業工具等後端系統，提供前端網頁介面供使用者存取後端各項作業服務。網站內容並須經本署同意後，方可進行網站改版。

2.HCA 提供 RAO(含初審 RAO)申辦作業之網站

HCA 提供 RAO(含初審 RAO)所需申辦作業之網站(https://rao.doh.gov.tw)，內容包含憑證申辦各項作業、各項訊息提供，以利進行相關憑證之申辦作業。網站內容並須經本署同意後，方可進行網站改版。

3.專案管理平台系統

(1) 提供帳號、密碼登入機制及依不同權限顯示不同使用功能清單功能。

(2) 提供專案管理功能，包含以下：

A.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、公布欄、專案成員通訊錄、工作報表)。

B.專案設定區(工作事項管理、公布欄管理、個人資料維護、使用者設定、系統設定)。

C.文件、表單管理介面。

(六)維護 HCA 營運中心管理資訊系統

1.營運維護 ISO 27001：2005 之文件檔案管理機制。

2.文件之管理作業須依照文件等級、屬性及文件所屬組別進行分類，各組別人員並依照系統賦予之不同權限可對不同之文件有存取修改之能力。

(七)提供營運管理制度及配合外部安全稽核

廠商應於企劃書中提出 HCA 之資訊安全管理規劃及執行，並應符合下列規範：

1.行政院及所屬各機關資訊安全管理要點。

2.行政院及所屬各機關資訊安全管理規範。

3.ISO 27001：2005。

4.配合行政院研考會 GPKI 外部稽核作業要求，協助提供稽核所需之各項資料，並配合改善相關缺失。

5.配合本署另案辦理之 ISO 27001：2005 認證案，本專案承包廠商需配合該案，以利 HCA 通過驗證或複驗，維持資訊安全認證持續有效。其有關之輔導及缺失改善作業，由本專案承包廠商辦理。

(八)提供符合 GPKI 規範要求

1.必須遵循 GRCA 之相關規定，包含 GPKI CP、GPKI 技術規範、GPKI 憑證與憑證廢止清冊格式剖繪…等，請至網站 http://grca.nat.gov.tw/儲存庫項下查詢。

2.依照 RFC 2527 之架構與定義及國內相關法規與主管機關之規定，協助維護本署 HCA 之 CPS，並協助送經濟部審查修正通過。

3.HCA 之營運須符合 CPS 之規範。

(九)設置諮詢服務窗口，並提供客戶服務品質管理機制

1.設置諮詢服務窗口(需沿用 HCA 0800-364-422 服務電話號碼)，並提供客戶服務品質管理機制。

A.每週一至週五 8:30 至 17:30(例假日除外)，提供 8 位客服人員及 8 線電話。如當週之 8 位客服人員輪值週六值班，則該員可於輪值後 1

週內休假 1 天，惟當天之休假人數不得高於 1 人，以確保每天至少有 7 位服務人員執勤。

B.每週六 8:30 至 12:30(例假日除外)，至少提供 2 位客服人員輪值。輪值人員可於週一至週五休假 1 天，惟當天之休假人數至多 1 人，以確保至少有 7 位服務人員執勤。

C.除上述之時間之外，非上班時間亦請提供 1 線電話之諮詢服務，若該線諮詢電話有增多之趨勢或情形，應提出改善措施，並確實執行。

D.本署將參考諮詢電話數量之多寡，要求承商做必要之人力輪班調配。

2.客服專線全部忙線中，應有語音提示。

3.提供 E-Mail、FAQ、網路電話及線上留言板等。

4.使用客戶服務系統，進行服務資料統計分析，並定期提供統計分析資料予本署參考，所分析之資料應包含聯絡時間、機構名稱、聯絡電話、客服人員姓名、問題描述、回覆情形、結案時間、問題分類等。

(十)提供系統危機應變處理機制、災害演習作業及營運移轉規劃

1.危機應變處理範圍包含 CA 金鑰遭破解或 Server、AP、DB 等軟硬體系統遭受不當使用之資訊安全事件。

2.針對可能發生之危機事件，訂定危機應變處理機制，並實際於 99 年 7 月 31 日前進行災害演習作業至少 1 次，以採取預防、應變及善後處理三層級措施，以期防範及降低各類危機事件可能造成之損害。

3.提供本專案之營運移轉規劃，以利本專案永續經營。

(十一)完成 TSS 功能增修及設備購置

1.為配合各醫療院所實施電子病歷索取時戳服務，本專案請新購一台時戳管理系統主機，建置於主機房中，說明如下：

(1)配合政策，規劃前端可接受本署 HIN 網路或健保 VPN 網路之需求，並與原主機房內之時戳管理系統主機共同提供負載平衡服務，以擴充時戳服務品質，承包廠商得申請健保 VPN 網路，網路申請費用由本專案支付。

(2)本專案所購置之時戳管理系統主機，應與 HCA2.0 現有時戳管理系統主機相容。

(3)承包廠商需監控時戳服務流量，每月定期提供本署參考。

2.配合營運需要，調整 HCA 網路架構，說明如下：

(1) 調整 HCA 所有硬體設備至同一個防火牆架構內，撤除原 HCA1.0

軟體防火牆，並替換原路由器設備。新購路由器設備要能夠轉接本署 HIN 網路及健保 VPN 網路，另外在 HCA 防火牆上新增設定可連接健保局 VPN 網路。原 HCA 應用系統並應全面檢視調整，以符合最新之網路架構。

(2) 採用新購之網路交換器取代原 HCA1.0 交換器，並設定符合整體應用架構之 VLAN 網段，同時新購之網路交換器需與 HCA 防火牆連接。

(3) 新購之時戳管理系統主機架構於非軍事區 DMZ 網段內，其負載平衡機制需配合現行負載平衡交換器進行設定。

(4) 配合優化 HCA 應用系統架構工作，部份系統軟體需拆解後重新配置至不同伺服器設備以執行其功能。網路架構及相關路由、防火牆等設定則需配合調整因應，調整之內容，需經本署同意後，方可執行。

(5) 本專案增購之網路路由器及網路交換器，廠商報價不得高於公共工程委員會共同供應契約同等級網路設備之報價，規格請參考共同供應契約電腦週邊設備(第 4 組) 路由器及交換器網路設備，其等級至少如下所述：

A.項次65.02 路由器設備封包轉送率150Kpps 網路路由器。

B.項次25.04 有網管功能之超高速乙太網路交換器24 埠 10/100/1000Base-T (具10GBase-X)。

(十二)完成用戶憑證金鑰長度由 1024 提升為 2048 位元

因應網路環境電腦硬體效能提昇，防範憑證應用各類演算法破解，本專案將依據政府機關公開金鑰基礎建設憑證政策第 1.4 版之 6.3.2.2 節「用戶公開金鑰及私密金鑰之使用期限：基於金鑰安全強度的需求，憑證機構至遲必須於民國 99 年 12 月 31 日停止簽發與 RSA 1024 位元安全強度相當的憑證，但在此之前簽發的憑證，仍可使用到效期到期日為止」辦理憑證用戶升級 2048 位元金鑰。預計於民國 100 年 1 月 1 日前簽發 2048 位元之用戶憑證。需針對相關應用程式介面進行改版，提供可支援 1024 位元 PKI-enabled 應用系統並相容於 2048 位元憑證 IC 卡，包含下列工作事項。

1.HCA 應用系統調整

承包廠商需完成在現行硬體架構上升級 2048 位元金鑰長度之調整，同時保留原 1024 位元金鑰長度之各項建設，必要時能雙軌並行或切換回現行金鑰長度為 1024 位元之相關服務。

本專案系統因應 2048 位元金鑰長度升級工作，最少應包含以下系統調整，承包廠商應在本署規定時程內，完成各系統調整工作：

(1)憑證系統、註冊系統等相關系統調整。

(2)個人化製卡管理系統調整。

(3)卡片作業管理及統計作業系統調整。

(4)資料庫流程新增並相容原發卡作業資料。

(5)系統功能測試及整合性測試。

2.卡片程式改版

改版現行醫事人員卡及醫事機構卡內之卡片程式 Applet，以符合 2048 位元金鑰長度應用之要求，同時保留原 1024 位元金鑰長度存放空間，必要時亦能依現行作業方式，發放金鑰長度為 1024 位元之醫事人員及醫事機構卡片。

3.發放醫事憑證測試卡片

於本專案 2048 位元金鑰長度升級使用者平行作業測試期間、使用者上線作業期間，提供發放新版 2048 位元金鑰長度之醫事憑證測試卡片。

(十三)提供已開發系統所需之 2048 位元金鑰長度 API 並提供諮詢服務

1.2048 位元金鑰長度 API

(1)因應新版用戶憑證 2048 位元金鑰長度改版作業，承包廠商需升級改版 HCA API 並相容現行用戶憑證。

(2)HCA API 改版項目包含以下：

A.HCA 應用於一般讀卡機 API(HCACSAPI)改版。

B.HCA 應用於健保讀卡機 API(HCAAPI)改版。

C.PKCS#11 改版。

D.CSP 改版。

(3)新版 HCA API 改版需包含以下相容性：

A.相容現行用戶憑證 1024 位元金鑰長度之 HCA 醫事憑證 IC 卡。

B.配合及相容最新健保控制軟體(Control Software)。

C.符合 GPKI 規範。

D.相容新版用戶憑證 2048 位元金鑰長度之醫事憑證 IC 卡。

(4)HCA API(包含 HCACSAPI、HCAAPI)需提供以下功能：

A.密碼模組函式：單向雜湊函數演算法、對稱式金鑰之加密函式、對稱式金鑰之解密函式、非對稱式金鑰之加密函式、卡

片非對稱式金鑰之解密演算法、卡片產生數位簽章及檢驗簽章等相關函式。

B.憑證應用服務函式：提供驗證 HCA 對憑證之簽章與讀取憑證各資料欄位的相關函式以及時戳應用相關函式。

C.憑證狀況查詢函式：提供驗證 HCA 對 CRL 之簽章、讀取 CRL 各資料欄位、查詢憑證是否列於 CRL 中及查詢該憑證在 CRL 中所記載之憑證廢止日期及理由等相關函式，並提供 OCSP 服務函式。

D.卡片欄位應用函式：提供卡片內各項醫事資料讀取及寫入函式。

E.提供目錄服務應用介面 API。

2.提供使用 HCA API(含 HCACSAPI、HCAAPI)之範例程式

(1)提供 DOT NET、VB、VC、JAVA、COBOL、HTML ActiveX、Delphi 等程式語言之 HCA API 範例程式。

(2)以上範例程式皆需設計含 UI 操作使用者介面。

(3)範例程式需能夠使用於現行用戶憑證 1024 位元金鑰長度之 HCA 醫事憑證 IC 卡，以及新版用戶憑證 2048 位元金鑰長度之醫事憑證 IC 卡。

(4)範例程式原始碼內需註明各應用作業詳細註解說明。

3.2048 位元金鑰長度 HCA API 庫諮詢服務

(1)於技術人員專屬網站提供 API 測試程式原始碼及測試介面，其內容需至少包含以下：

A.各種版本 API 與說明文件之下載。

B.各種作業系統或平台之範例程式分享。

C.開發人員之經驗分享。

D.開發環境(包括讀卡機)與 IC 卡正常性之檢測。

(2)因應醫院或醫療資訊廠商環境特殊之問題排除與程式修正。

(3)由醫院或醫療資訊廠商自行提供所屬 Linux、Solaris 或其他 Unix-like 版本之作業系統環境予營運中心，承包廠商須將 API 與作業系統核心進行編譯後回覆醫院或醫療資訊廠商。

(4)嚴格控管 API 之發布與差異說明，差異說明需註明於公告之 API 或範例程式下載區中。

(5)提供 API 使用單位直接之技術客服專線，加速問題排解之效率並減少醫院或醫療資訊廠商客訴問題。

4.HCA 應用作業諮詢服務

(1)提供本署電子病歷技術事項或其他 HCA PKI 應用之憑證實務應用諮詢。

(2)承包廠商應支援醫院或醫療資訊廠商實務應用 HCA 於醫療系統之相關技術諮詢服務,並定期於 HCA 專屬網站或技術人員專屬網站提供各類應用 HCA 之指標性論壇文章,如文章內容涉及智慧財產權或專利等，需經過醫院或醫療資訊廠商同意後始得刊載於 HCA 專屬網站。

(3)承包廠商需提供跨現行用戶憑證 1024 位元金鑰長度之醫事憑證，以及新版 2048 位元之系統應用修改建議說明，必要時，得提供原始碼。

(4)承項次(3)，所提供之說明，應包含已使用過 HCA 之醫療院所或醫療資訊廠商如何進行程式系統升級之建議，以及從未使用過 HCA 之醫療院所或醫療資訊廠商如何導入 HCA 應用架構。

(十四)辦理教育訓練及說明會

因應本專案之執行，需配合辦理相關教育訓練及說明會等，所需之場地、布置、茶水餐點、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。上課地點應靠近當地火車站、高鐵站或捷運站。承包場商可視需要，增加辦理之場次。

1.RAO 教育訓練

(1)辦理 RAO 教育訓練至少 9 小時，每場至少 3 小時，分北、中、南 3 區至少各 1 場次。

(2)上課現場講師需進行操作教學，承包廠商並須建立模擬環境，供受訓學員課後可於模擬環境上實際執行各種憑證業務操作。

2.初審 RAO 教育訓練

(1)辦理初審 RAO 教育訓練至少 9 小時，每場至少 3 小時，分北、中、南 3 區至少各 1 場次。

(2)上課現場講師需進行操作教學，承包廠商並須建立模擬環境，供受訓學員課後可於模擬環境實際執行各種憑證業務操作。

3.HCA API 改版說明會

(1)辦理 HCA API 改版說明會至少 24 小時，每場至少 3 小時，分北、中、南、東區至少各 2 場次。

(2)上課現場講師需進行程式寫作實機教學。

4.HCA API 應用說明會

(1)辦理 HCA API 應用說明會至少 24 小時，每場至少 3 小時，分北、中、南、東區至少各 2 場次。

(2)上課現場講師需進行程式寫作實機教學。

(十五)其它

配合本署業務需求，提供與本專案有關 HCA2.0 之必要協助。

二、HCA1.0 作業需求

(一)提供 HCA1.0 對外目錄服務、黑名單公告、儲存庫等相關服務

1.醫事憑證業務作業服務

(1)維護 HCA1.0 目錄服務之資料內容及整合目錄樹結構。

(2)提供 HCA1.0 CRL 持續發行至 LDAP 上之功能。

(3)提供 HCA1.0 儲存庫管理服務。

2.RAO 服務

由營運中心作業人員執行 HCA1.0 RAO 作業，並透過 SSL 機制使用 WEB 操作介面進行各項之業務服務。

3.專屬網站系統

營運及維護 HCA1.0 專屬網站系統，且網站內容須經本署同意後，方可進行網站改版。

4.卡片線上作業服務

持續提供 HCA1.0 醫事憑證 IC 卡之線上開卡、線上解鎖卡、線上更改密碼作業等卡片線上作業服務。

(二)其它

配合本署業務需求，提供與本專案有關 HCA1.0 之必要協助。

三、管理需求

(一)專案管理

1.承包廠商於專案啟動時應提出專案執行計畫書，並依據本章第八節所訂之工作項目及交付時程，詳列工作查核點及分階段交付項目，以有效控制進度。

2.承包廠商應提出專案監控之規劃說明及專案管理工具，以針對專案

之進行隨時掌握其狀況，並對狀況能提出解決方案或作相關的調變。

3.本署將視需要召開專案工作會議，承包廠商須由專案經理率參與本專案主要工作人員至本署報告專案工作進度並答復本署提出之問題，並依本署建議事項及時程進行改善。

4.專案執行期間，廠商應於每週五中午前提出當週工作報告，每月 10 日前提交上月之營運作業報告，內容應包括該月份之重要工作項目、完成工作項目、執行人員、進度檢討、下月份預定工作及問題與建議等項目。

(二)專案小組組成

1.承包廠商應成立專案工作小組，負責本專案之各項需求規劃、協調、執行及諮詢等工作。投標廠商須提供專案小組成員之學經歷背景(包含曾經參與專案之規模、所負責之工作項目、投入人日之估算、使用工具等)、專長(是否具有證照)、負責本專案之工作項目及工作內容(註明是否專職投入本專案或其投入之工時比例)，並說明是否包含系統架構師、本專案應用技術架構之各項專業人員，具軟、硬體、網路平台知識及相關技術、知識經驗，足以規劃與設計本專案資訊架構，以作為廠商評選之參考。

2.承包廠商須指派積極且具良好溝通、統籌協調及行政規劃能力，並具有本專案應用之各項技術基本知能之專職專案經理，擔任本專案聯絡窗口，以彙總及追蹤本專案工作項目執行情形，並即時傳達及回復本署相關交辦工作事項處理結果。

3.參與本專案工作人員(須與企劃書名單一致)之學經歷背景及證明文件於專案啓動階段先送本署備查，專案過程中非經本署函文同意不得更換，惟可增加人員（人員異動時仍應檢附學經歷、專長、證明文件、到職日期、健保卡正面影本及在本專案擔任工作等），人員更換交接工作期至少 2 週，並於交接之起、迄日至本署報告，以上若為人員不適任經本署要求更換者亦同。

(三)驗收管理

1.承包廠商應依本說明文件所訂之交付項目與時程，依序進行專案工作。本署得不定期要求承包廠商提供進度報告。

2.為確保承包廠商之交付項目能滿足本專案需求，故針對本專案各項工作項目之執行成效應以量化及書面資料展示，以作為驗收依據。

四、安全需求

(一)承包廠商對業務上所接觸之資料，應視同機密文件採必要之保密措施，並應依本署規定填具資訊安全保密切結書(如附錄三)，且承包廠商應與其在本專案之工作人員訂定工作契約，告知並要求其工作人員嚴守工作契約內容、本專案契約內容及業務機密。任何因承包廠商或其工作人員洩密所致之賠償及刑事責任，概由承包廠商負責，並提報行政院公共工程委員會列為不良廠商。

(二)本署將依需要進行實地現場訪視承包廠商專案相關工作之執行及資料之處理。

(三)承包廠商應確保開發之程式絕無留有任何形式之後門或弱點，以免危害本專案內系統及資訊安全。如發現安全漏洞時，承包廠商必須於接獲本署通知 3 日內,提出改善措施且依本署規定時程(原則上為一週內)無條件進行修補。

(四)系統安全機制須整體考慮實體安全、軟體安全及資料安全。各流程須考量資料安全及交易正確，於各種不同使用者溝通管道上，規劃適當之安全協定，以完整地保護各項交易不被盜取、竄改，並杜絕發生系統被入侵之行為。

(五)承包廠商對所設計程式應做好輸入查驗（Input Validation）工作，並對使用者輸入資料之長度、型態、特殊字元及特殊指令等，確實加以過濾與處理。

(六)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），均須進行嚴格的身分管制（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。

(七)對於使用者的密碼、交易資料、交易過程產生之敏感資料等，進行適當的保護與管理。

(八)伺服器主機目錄存取權限，須有妥善的規劃及控管，避免無限制開放使用者存取。

(九)須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。

(十)須有適當的系統組態設定，以保障系統安全。

(十一)本專案系統之 error log 及 access log 機制，承包廠商應維持正常運作。

(十二)處理交易安全控制需求。保持系統各項交易之完整性，若在異動資料過程中失敗，能終止此異動，並復原成異動前狀態，且顯示適當之訊息。

(十三)承包廠商攜入可攜式運算及儲存設備，暨無線通訊設備，須經本署許可，並經資訊安全檢測後，方可使用。

(十四)每次程式上線前及異動後，承包廠商均應進行資訊安全檢測，並檢附系統異動之相關文件及資訊安全檢測報告(報告中至少應含自我檢測及以本署所提供工具檢測之結果)。

(十五)除上述需求外，本專案各項作業均應符合本署資訊安全作業之要求。

五、強制性需求

(一)由投標廠商以正式機關章蓋妥投標文件向本署提出申請，由個人名義申請者概不受理。

(二)執行本專案時如發生錯誤或資料漏失，經確認屬於承包廠商責任者，應由承包廠商負責更正；另損及他人權利義務時，承包廠商亦須負責。

(三)承包廠商未依本說明文件及本專案契約執行者，經本署書面通知仍未改正，本署得終止全部或部分契約，已支付之款項予以追回，承包廠商不得要求任何賠償。

(四)本專案期間，本署可視需要隨時派員至承包廠商處瞭解專案執行情形，並要求承包廠商向本署簡報。

(五)如有 HSM 被破解，或私密金鑰被非法讀出之情事，承包廠商應負賠償之責任。

(六)本專案 99 年度營運結束後若非由原營運廠商得標，原營運廠商應與 100 年度承包廠商或本署辦理交接（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契約當月，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及系統正確運作，如違反規定則扣除履約保証金（投標廠商應於企劃書中預估交接之成本)。

(七)本契約結束，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。

(八)若承包廠商於本專案中有協力廠商，需於投標企劃書中敘明，並附合作同意書。

六、智慧財產權歸屬

(一)承包廠商應與其受僱人或其他合作人員，就本契約應完成之電腦程式，約定以承包廠商為著作人。

(二)承包廠商因履行契約所完成之著作（授權軟體除外），其著作財產權之全部（包含程式原始碼使用、複製、修改之權利）於著作完成之同時讓與本署，承包廠商並承諾不對本署及本署所同意利用該電腦程式之人行使著作人格權。

(三)承包廠商為開發本專案所利用之技術或技術資料，其智慧財產權仍屬原權利人所有，不受影響。承包廠商於本專案所交付之套裝軟體之智慧財產權皆歸屬於原軟體廠商，使用單位僅擁有軟體使用權，若專案內容涉及其他相關智慧財產權，承包廠商應先獲得授權同意。本署使用承包廠商提供之系統產生之資料及資料庫檔案等，其所有權歸本署所有。

(四)承包廠商交付之本專案相關軟體項目中如包含第三人開發之產品，應切結保證並提供授權證明文件，以證明軟體使用之合法性（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，若發生侵害第三人合法權益時，由承包廠商負責處理，並承擔一切法律責任。承包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，承包廠商應負一切損失賠償與責任，並放棄法律之先訴抗辯權，且維持本系統之正常運作。

(五)承包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，承包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、維護保固

本專案使用之軟硬體設備需於本專案執行期間（99 年 1 月 1 日至 99 年 12 月 31 日）提供維護保固。維護期間如設備有故障時，須於營運不中斷之原則下，排除故障或暫時更換不低於原標的物性能之同級備品，供本署系統能繼續運作至標的物修復完成；非人為因素，若有損壞、更換不良品或改善施工不良處之各項設備（零件）均由廠商無償完全修復。

八、交付產品項目與時程

本專案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99/1/1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）	99/1/31 前	
2	舉辦HCA API改版說明會	HCA API 改版說明會成果報告書	99/4/30 前	
3	1.時戳管理系統主機之擴充建置 2.HCA 網路架構調整 3.醫事憑證用戶金鑰升級2048位元系統改版及建置(含憑證相關系統改版、API改版、卡片 Applet 改版) 4.發放新版測試卡、HCA API 5.提供應用系統配合用戶金鑰長度升級至2048 位元作法之建議說明	1.交付時戳管理系統主機之軟硬體設備 2.交付網路硬體設備 3.醫事憑證用戶金鑰升級2048位元系統改版報告書 4.申請新版測試卡、新版安全保密函式庫成果報告書 5.應用系統配合用戶金鑰長度升級至 2048 位元作法之建議說明書	99/5/31 前	
4	1.舉辦RAO教育訓練 2.舉辦初審RAO教育訓練	RAO 與初審 RAO 教育訓練成果報告書	99/6/30 前	需提供人員簽到單。

項次	工作項目	交付產品項目	交付時程	備考
5	1.因應金鑰長度升級2048位元系統改版正式切換上線 2.舉辦HCA API應用說明會	1.開始發放2048位元金鑰長度卡片 2.HCA API 應用說明會報告書	99/8/31前	1.正式對外提供申請之時間，由本署另訂。 2.需提供人員簽到單。
6	1.危機應變處理機制及災害演習作業 2.營運移轉規劃	1.危機應變處理機制及災害演習報告書 2.營運移轉規劃書	99/10/31前	
7	1.醫事憑證IC卡製卡、卡片寄發作業 2.交付本專案系統之原始碼及執行碼 3. HCA應用系統優化	1.年度工作成果說明書 2.系統原始碼及執行碼 3.HCA應用系統優化報告書	99/12/20前	
8	99年度HCA每月營運作業	HCA每月營運作業報告	99年度1月至11月份報告分別於次月10日前交付 12月份報告於12月31日前交付	內容及格式由本署另訂

(一)投標廠商須於企劃書中依所規劃之執行期程自訂各項文件產出之交付查核點，並可另依執行需要，自訂其他必要之交付項目及其查核點，於查核點前交付本署審核，自訂查核點及自訂交付項目應審慎合理可行，並列入評選項目。承包廠商若未依上表及自訂之交付項目及時程執行，將依本文件之延遲扣款規定計算違約金。

(二)本專案各項文件應於交付階段期限2週前（項次1除外）免備文送交本署初稿2份（須採A4紙雙面印刷）及電子檔（須與本署辦公室文件處理軟體版本相容，且遵循本署規範之檔案命名原則，以下同），本署若有修改意見，則承包廠商須於1週內修改完畢。

(三)本專案各項文件應於交付階段期限前備文送交本署書面文件及電子檔各 1 份，本署若有修改意見，承包廠商仍須於 1 週內修改完畢備文重新提交，俟本署同意備查後，再交付需求數量之書面文件（採 A4 紙雙面列印、膠裝，並於文件封面及書脊註明案名、文件名稱、版本及文件產生日期），且所有文件電子檔併同原始碼及執行碼以光碟片備份 2 套提交。

(四)專案會議或審查會議：由承包廠商準備開會資料及提供審查文件，不限於上表所訂之文件項目及份數。

九、後續擴充需求

無。

肆、付款方式

一、付款原則

(一)本專案費用以新台幣為付款幣別，並依下列方式分期付款：

1.第 1 部分：契約總價款之 10%

完成簽約及第參章第八節項次 1 並經本署查驗認可後，支付契約總價款 10%。

2.第 2 部分：契約總價款之 30%

完成第參章第八節項次 3，由承包廠商正式行文本署通知完工，於本署辦理驗收無誤後，支付契約總價款 30%。

3.第 3 部分（營運作業）：契約總價款之 60%

共分第 1 至 12 期：承包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，交付本說明文件第參章第八節所列各項文件（項次 1 至 8），由本署查驗認可當月所有應交付產品項目及文件，若內容符合本專案要求，得檢附發票請領當月營運費用，即第 3 部分（契約總價款之 60%）營運費用總金額十二分之一。(最後一期採書面驗收辦理，其中 1,036,200 元之覈實支付部份，如未支付，將於本期經費中予以扣除。)

(二)因會計年度結束需依規定辦理保留該款項時，本署得視保留核定情形再行支付，並不負延遲責任。年度預算將視立法院審議核定後撥付，經費如遭凍結，不能如期支付，本署得延期辦理支付。

(三)本專案所需之經費由廠商提出價格分析列於企劃書內，內容應包含：軟硬體設備建置與維護、安全控管、經營管理、機房管理、營運辦公室及所有相關營運費用等之估算。另須列出本專案各項工作之郵資單價、信封數量及總價，於期末驗收時，須提報本專案相關實際郵資、紙張印刷及信封費用證明(範圍包含本計畫執行過程中衍生之所有郵資費用)，本署將覈實支付費用，最高以 1,036,200 元為限。

(四)本專案決標後，本署得以合理性為前提，將機房、辦公室等租金與管理費用，與承包廠商協議調整單價分析，調整原則得不受依決標金額按比例分配之限制。另本專案之覈實支付部份，亦得不受依決標金額

按比例分配之限制。

二、履約保證金

承包廠商應於本專案簽約時按不低於契約總金額百分之五為履約保證金，承包廠商完成交付產品項目及時程表之各項次工作經本署審核或驗收合格，並協助本署 100 年度之承包廠商移轉作業順利完成後，履約保證金無息發還。

三、其他

本案經議價決標後，得標廠商應於決標日起 3 日內，依下列規定，調整決標單價分析表經費：

(一)人事費：若決標日在 99 年 1 月 1 日前，則自 99 年 1 月 1 日起算調整。若決標日在 99 年 1 月 1 日之後，則自決標日起算調整。

(二)業務費：扣除調整後之人事費後，除第肆章第一節第(四)點說明外，其餘按決標金額比率逐項調整（不得僅單純調整某項）。

(三)調整後之各項單價，不得高於原報各項單價金額，另調整後之總價金額應與決標價相同。

(四)調整後之單價分析表，應經請購單位人員審查確認無誤，始得辦理後續契約書印製事宜。

伍、罰則

一、遲延履約罰則規定

(一)本專案認定交付產品時程以承包廠商正式行文本署，並以本署收文日期為依據。

(二)本專案廠商各項交付項目如有超過交付期限，每延遲 1 日（以日曆天計，星期日、國定假日、及其他休息日均應計入），應按逾期日數，每日依當期應付契約價金之千分之一計算逾期違約金。

(三)逾期違約金之支付，本署得自應付價金中扣抵；其有不足者，得通知廠商繳納或自履約保證金扣抵。

(四)逾期違約金之總額（含逾期未改正之違約金）以契約價金總額之 20％為上限。

(五)如因可歸責於廠商之事由，致履約進度落後達 20％以上，且日數達 10 以上者，屬延誤履約情節重大，本署得以書面通知承包廠商終止或解除契約之部分或全部，且不補償承包廠商所受之損失，並得依採購第 101 條規定辦理。

(六)99 年度本署或使用者如發現各 RAO 業務作業及專案管理平台有問題，通知承包廠商知悉後，承包廠商應於 4 小時內回復及著手處理，8 小時內恢復作業。另如為 TSS 系統、HCA 專屬網站、RA 網站系統、線上開卡(含展期、解鎖卡及更改密碼)服務、憑證廢止清冊公布服務及憑證狀態查詢服務等問題，應於通報問題後 1 小時內回復並著手處理，及 4 小時內恢復作業，若研判未能於 4 小時內恢復作業，應立即啟動備援系統之服務，於通報問題後 4 小時內完成備源系統之啟動，並於 8 小時內恢復主機房之作業。上述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)，本署得按契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。

(七)本專案之承包廠商須於 99 年 1 月 1 日立即接續營運 HCA，如決標日為 99 年 1 月 1 日以後，廠商應於決標日起 1 日內完成，若未能正常營運，則每天扣除總金額千分之五，並於達百分之二十時解除契約。

二、其他罰則規定

(一)承包廠商應於議價後成本分析中，詳列各項工作項目成本，如於驗收

時，經審查發現有不合格之工作項目，廠商應依期限予以改正。如未改正，本署有權扣除該項工作之款項。

(二)承包廠商應將文件品質保證納入專案品質保證項目，嚴謹製作本專案各項文件，包含版面及內容皆須嚴格要求一致性及正確性。交付本署之文件經本署審閱時，所發現錯漏處達 3 處以上，或業經本署要求修訂仍未修訂，本署得按每字新台幣 500 元計算懲罰性違約金，並得自應付價金中扣抵；其有不足者，得通知廠商繳納或自履約保證金扣抵。

(三)承包廠商指派之專案負責人及工作成員，未經本署同意，不得更換，如有未經本署同意即自行更換時，每更換乙次得依契約總價千分之一計算懲罰性違約金。

三、例外辦法

若延遲交付之原因可歸責於本署或其他不可抗力因素時，承包廠商可提出事實報告經本署同意後免除此延誤之天數與罰金。

四、損害賠償

承包廠商於本專案進行中因故致使本署蒙受之損失，經確認確屬承包廠商應負責任，應由承包廠商負責賠償，若無法精算損害額度，得以履約保證金之百分之二十作為損害賠償金額，而本署並得自應付價金中扣抵。

五、權利瑕疵擔保

(一)承包廠商應保證本專案交付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，應由承包廠商負責處理並承擔一切法律及賠償責任。

(二)承包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承包廠商自行負擔：

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。

陸、投標廠商基本資格及應檢附之資格證明文件

一、投標廠商基本資格(具下列■資格之一者)及應檢附之資格證明文件(廠商需提出資格文件影本繳驗，必要時本署並得通知廠商提供正本供查驗)：

■ 財（社）團法人團體、公、協、學會
■ 公（私）立大專院校
■ 公立學術研究機構
■ 政府機關及其附屬之研究機構
■ 經政府合法登記與本採購案有關之公司、機構

二、應檢附之資格證明文件：

■ 與本採購案有關之登記或設立證明影本（如：公司登記或商業登記證明文件、**非屬營利事業之法人、機構或團體依法須辦理設立登記證明之文件**、工廠登記證、**許可登記證明文件**、執業執照、開業證明、立案證明或其他由政府機關或其授權機構核發之合法登記或設立證明文件）。

上開證明，廠商得以列印公開於目的事業主管機關網站之資料代之。

【注意：依經濟部 98 年 4 月 2 日經商字第 09802406680 號公告：「直轄市政府及縣（市）政府依營利事業統一發證辦法所核發之營利事業登記證，自 98 年 4 月 13 日起停止使用，不再作為證明文件。」準此，投標廠商如以營利事業登記證作為資格證明文件，而無其他足資證明之文件者，視為資格不符】

■ 最近一期營業稅納稅證明影本，不及提出最近一期證明者，得以前一期之納稅證明代之。新設立且未屆第一期營業稅繳納期限者，得以營業稅主管稽徵機關核發之核准設立登記公函及申領統一發票購票證明等相關文件代之。

依法免稅者，應提供相關申報證明文件。

□ 廠商依工業團體法或商業團體法加入工業或商業團體之證明影本（如：會員證）。

■ 前述相關證明，下列單位得以組織條例、規程之影本或准予投標之公函正本(附於投標文件內)代之：**（撰寫說明：倘無勾選該類廠商資格，則本條請刪除）**

1. 公（私）立大專院校
2. 公立學術研究機構
3. 政府機關及其附屬之研究機構

柒、企劃書製作規則

一、簡述

投標廠商企劃書製作，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，文件封面及書脊註明案名、文件名稱及投標日期，內容以中文直式橫書由左至右繕打，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(台北市大同區塔城街 36 號 2 樓)。

3.投遞方式：廠商投標文件連同企劃書 14 份，及電子檔一併送交。報價應以密封方式並加蓋廠商戳(即標單)連同企劃書投遞。

4.以上如有變更以招標公告為準。

(三)其他規定

1.企劃書不得逾期投遞，否則視為無效標。

2.企劃書於投標後，不得修改或增訂。

3.企劃書及附件資料，決標後本署不予寄還。

三、一般要求

(一)企劃書交付後，本署承諾不得交付本署及評選委員以外之第三人參閱。

(二)製作企劃書及契約簽訂前所費之成本，由投標廠商自行負擔，承包廠商之企劃書所有權歸本署。

(三)投標廠商對於本徵求企劃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(02-8590-6031，林先生收)提出意見或問題。

(四)投標廠商得於本專案公告期間之上班時間至本署資訊中心參閱「營運

移轉規劃書」，惟不得抄寫、複印或攝影（洽詢電話：02-8590-6324，林先生）。

(五)本署對投標廠商企劃書中所提實績經驗有疑問時，得請投標廠商提出證明文件。

四、企劃書內容

投標廠商所提企劃書應力求詳盡完整，相關章節須參閱附錄四所規範順序撰寫，惟若有補充可於適當處另闢章節段落說明。

捌、招標、決標、評選方式及原則

一、招標方式

(一)限制性招標。

(二)依政府採購法第 22 條第 1 項第 9 款規定委託資訊服務辦理。

二、決標原則

(一)本專案依政府採購法與機關委託資訊服務廠商評選及計費辦法規定辦理。

(二)本專案訂有底價，採取總包價法及以準用最有利標決標。

三、評選方式及評選原則

(一)投標廠商資格審查依招標公告，資格審查不合格者，其企劃書不予審查評選，若全無合格廠商，則停止辦理，所送企劃書廠商得領回，並另行辦理。

(二)資格審查後合格廠商，始可參加企劃書評選；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)本專案採序位法－評分轉序位評比，並將價格納入評比。

(四)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，該小組將依據本章之評選項目，就受評廠商資料擬具初審意見，載明下列事項，連同廠商資料送委員會供評選參考：(1)採購案名稱(2)工作小組人員姓名、職稱及專長(3)受評廠商於各評選項目所報內容是否符合招標文件規定(4)受評廠商於各評選項目之差異性。

(五)由本署依法組成採購評選委員會辦理評選，並由各評選委員依據各投標廠商所提企劃書及簡報內容，按本專案所列評選項目及配分，評定各廠商得分。

(六)全部評選項目之合計總分數（滿分）為 100 分，由各評選委員就評選項目及配分，填寫評選評分表（含序位）乙份，交由工作人員計算總平均分數及序位總和。

(七)評選委員會出席委員評分結果，總平均分數達 70 分（含）以上者為合格廠商；總平均分數未達 70 分者為不合格廠商。經評定為不合格者，不得作為優勝廠商。

(八)評選委員對於廠商價格項目之給分，將考量該價格相對於所提供服務標的之合理性，以決定其給分，而非僅與其他廠商之價格高低相較而決定其得分。

(九)評選委員會之評選作業，以「記名方式秘密為之」為原則。會議中除

評選委員就投標廠商所提資料、簡報有關內容提出發問外，其他列席人員均不得發問。

(十)優勝廠商評定方式：經計算各投標廠商之序位數總和結果，以總序位合計數最低且經評選委員會出席委員過半數決定者為第一優勝序位廠商，次低者為第二優勝序位廠商，依此類推。

(十一) 評定優勝廠商之優勝序位後，依優勝序位及下列方式與優勝廠商辦理議價（議約）：

1.優勝廠商為 1 家者，以議價方式辦理。

2.優勝廠商在 2 家以上者，依優勝序位，自最優勝者起，依序以議價方式辦理。但有 2 家以上廠商為同一優勝序位者，以標價低者優先議價。

(十二) 序位第一之廠商有 2 家以上且標價相同時，擇獲得評選委員評定序位第一較多者為第一優勝序位廠商，仍相同者，抽籤決定之。次一優勝序位如有相同情形時，比照上述方式辦理。

(十三) 本案依優勝序位最多選出 3 名優勝廠商，並依序辦理議價，第一優勝序位廠商議價不成，則由第二優勝序位廠商遞補，依此類推。

(十四) 評選評分表(含評選項目標準及配分)及評選評比總表，詳見附錄六及附錄七。

(十五) 簡報及答詢

1.投標廠商應由本專案之專案經理或專案主持人出席評選委員會議簡報，所有參與人員請攜帶身分證件備查。

2.簡報之順序，將於本署完成資格審查後，當場由資格審查合格廠商抽籤決定。廠商簡報時，其他廠商應退出場外。

3.簡報時間及地點，由本署另行通知合格廠商。簡報型態由廠商自行決定，除會議室現有播放硬體設備外，其他必要設備由投標廠商自行攜帶準備。

4.資格審查合格廠商於本專案之專案經理或專案主持人應就所提企劃書內容對本專案採購評選委員進行口頭簡報（20 分鐘，簡報前請介紹廠商與會人員於本專案所擔任之角色），其後並接受評選委員詢問，採統問統答方式，回答時間以 15 分鐘為原則。簡報結束前 3 分鐘按鈴聲一短聲，簡報時間到按鈴聲－長音，廠商即應停止簡報。

5.簡報時廠商若經本署唱名三次未到者視同放棄「簡報及答詢」機會，評選委員得逕依企劃書內容進行評分。

6.簡報資料以企劃書原有方案內容表達為主，現場不接受廠商補充資料，且簡報內容不得更改投標文件內容。廠商另外提出變更或補充資料者，該資料不納入評選。

7.所有參與評選廠商，均不給予任何經費補助。

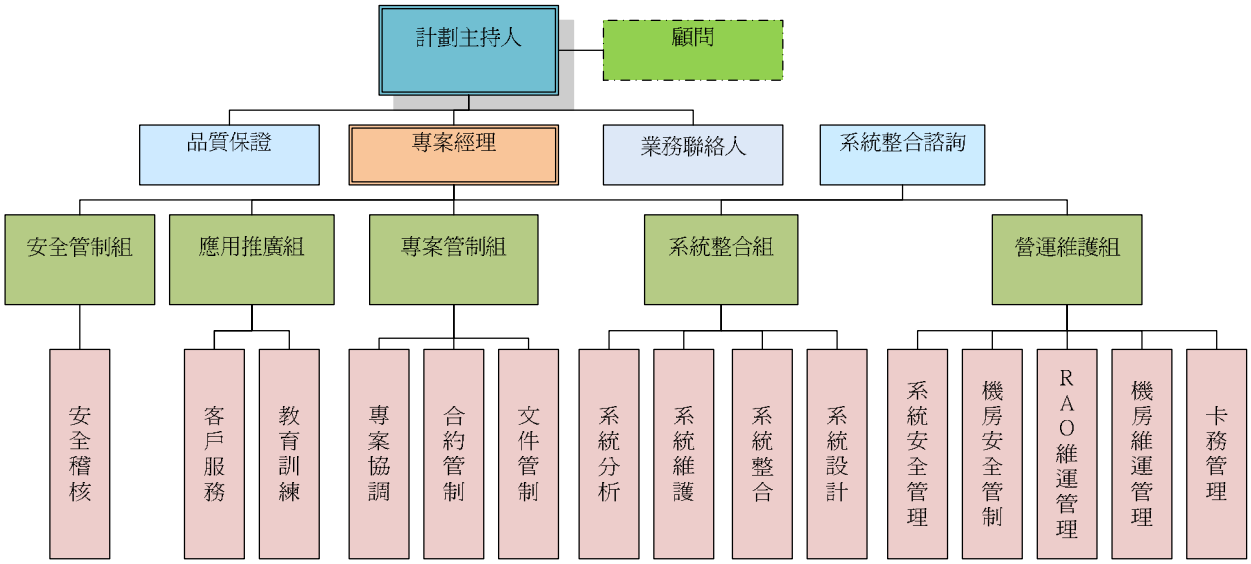
8.評選優勝者，如發現有資料提列不實或抄襲之情事者，由廠商自負相關責任，且本署得立即取消其議價資格。

(十六) 本專案評選結果，經奉機關首長（或其授權人員）核定後，始得公布。

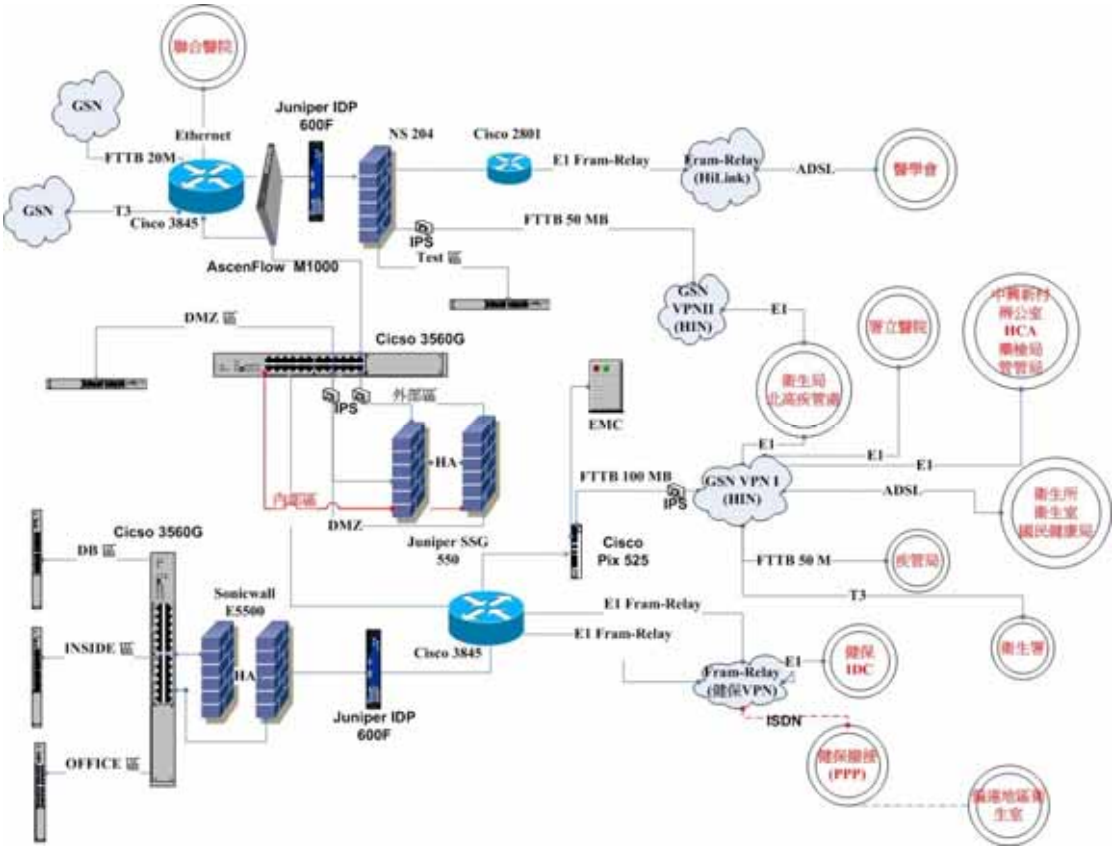
玖、附錄

附錄一、現有作業說明

一、HCA 營運組織架構圖

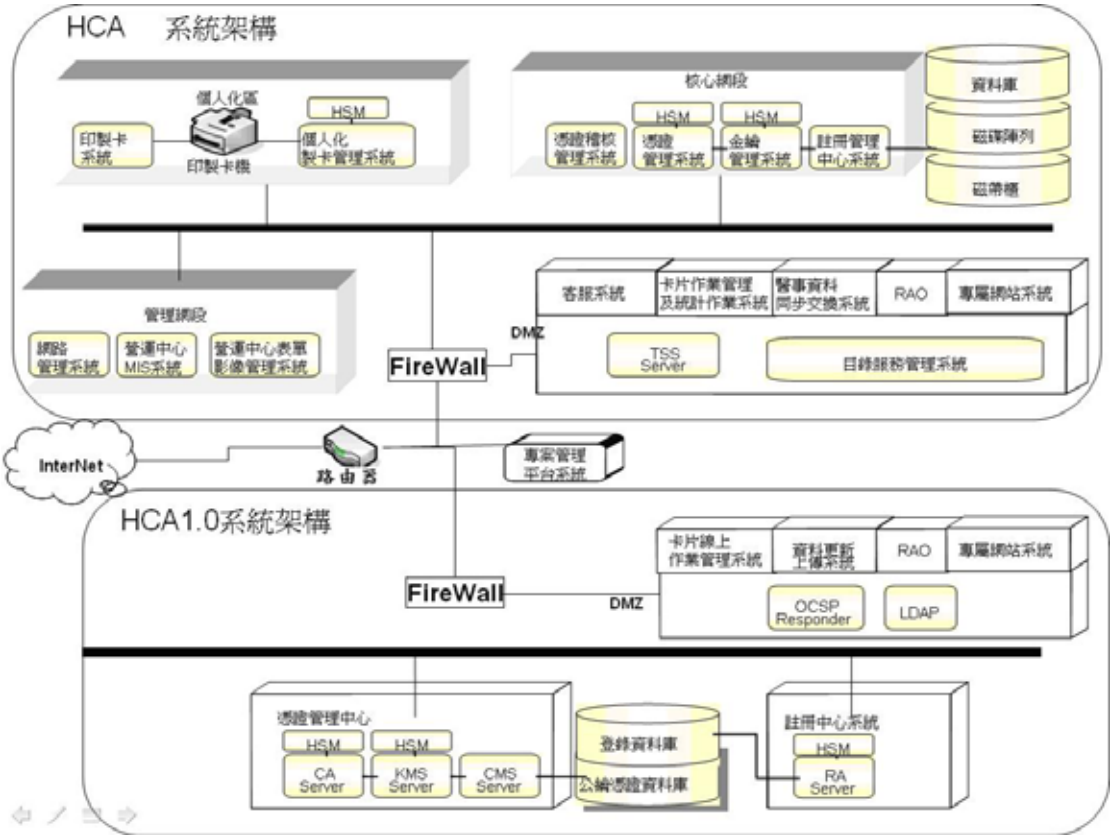


二、本署全國醫療資訊網與 HCA 機房網路架構



三、現行 HCA 系統架構及功能說明

(一)詳細軟硬體設備清單如附錄二，系統架構圖參考如下：



(二)HCA1.0 應用系統說明

1.憑證系統

(1)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 HCA1.0 憑證廢止簽署功能。

(3)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)。

(4)提供各項憑證作業稽查機制。

(5)提供各項憑證作業資料備份機制。

(6)將憑證廢止清冊(Certificate Revocation List, CRL)發行至輕量目錄存取服務(Lightweight Directory Access Protocol, LDAP)上。

2.註冊管理中心(Registration Authority, RA)系統

(1)提供上傳之憑證廢止者資料核對功能。

(2)提供憑證刪除審核等管理功能。

(3)提供各項註冊作業備份、稽查機制。

3.金鑰管理系統(Key Managerment System, KMS)

提供 HCA1.0 系統各類金鑰保護功能。

4.目錄服務管理系統

(1)依照 X.500 相關國際標準並符合 LDAP-V2, V3。

(2)提供憑證內容資料及憑證狀態等資訊公布、查詢與下載功能。

(3)提供各類憑證廢止清冊之公布、下載等功能，並可設定即時公布或每日公布次數之功能(如發現醫事人員或機構已歇業，應主動納入憑證廢止清冊內)。

(4)公布及下載之憑證採用 X.509 標準(內含 HCA1.0 憑證機構簽署之數位簽章)。

(5)提供各項憑證公布、下載作業及系統設定作業之記錄功能。

5.資料更新上傳系統

(1)提供現行醫事系統醫事資料庫 UPDATE 至 HCA 資料庫功能。

(2)提供資料異動至 HCA 資料庫錯誤之回復功能。

6.RAO 網站系統

透過 SSL(Secure Socket Layer)機制提供 WEB 操作介面，進行憑證廢止業務服務。登入 WEB 操作介面並需透過 HCA1.0 RAO 作業人員 IC 卡驗證後，方可登入。

7.HCA1.0 專屬網站系統

(1)公布 HCA1.0 之相關訊息，包括：HCA1.0 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 HCA1.0 醫事憑證 IC 卡之認識。網址：http://hca1.doh.gov.tw。

(2)專屬網站視需要不定期進行新增、刪除、修改內容及功能。

8.卡片線上作業管理系統

(1)提供 HCA1.0 卡片線上開卡、線上解鎖卡、線上更改密碼等功能。

(2)卡片線上作業管理系統介面及元件

A.維護線上讀卡機功能測試介面。

B.維護線上自動下載 HCA1.0 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。

C.維護開卡介面查詢功能。

(三)HCA2.0 應用系統說明

1.憑證管理系統

(1) 提供 HCA2.0 憑證註冊、簽發、公布、暫時停用、恢復使用、廢止、

憑證查詢等功能。

(2) 憑證採用 ITU-T X.509 V3 格式，並符合 IETF PKIX Certificate and CRL Profiles 標準。

(3) 能夠簽發並公布 HCA2.0 完整憑證廢止清冊（Complete CRL）及異動憑證廢止清冊（Delta CRL），公布週期每天至少一次。

(4) 提供符合 RFC2560 之 HCA2.0 憑證狀態線上查詢(On-line Certificate Status Protocol, OCSP）服務。

(5) CA 伺服器使用通過 NIST FIPS140 Level3 以上驗證的 HSM 來產製及儲存其所有金鑰對，包括用於簽署 HCA 憑證及憑證廢止清冊的金鑰對、用於簽署稽核紀錄的金鑰對、及用於與 RA 伺服器通訊時簽章或金鑰交換的金鑰對。

(6) 憑證發放類別：

A.醫事機構憑證

B.醫事人員憑證

C.醫事用途之伺服器應用軟體：由公家機關或醫事機構建置，用於醫療、健保或公共衛生等相關醫事服務用途之時戳伺服器應用軟體、SSL 伺服器應用軟體或其他通訊協定之醫事專門用途的伺服器應用軟體。

(7) 醫事機構及醫事用途之伺服器應用軟體得使用 IC 卡、HSM 或軟體密碼模組做為憑證及金鑰載具，醫事人員則一律使用 IC 卡做為憑證及金鑰載具。當使用 IC 卡為載具時，本專案系統透過卡管系統將憑證寫入 IC 卡中。

(8) 醫事機構之 IC 卡區分為正卡及附卡，除卡片到期前之新舊卡交接期之外，在任何時間，系統必須確保同一醫事機構僅能存在一張有效之正卡，附卡則依應用情形可不限申請之張數。

(9) 憑證格式的設計仿照 GPKI 憑證及憑證廢止清冊格式剖繪（Certificate and CRL Profiles for the Government Public Key Infrastructure）現有的憑證格式，即憑證基本欄位包含 version、serialNumber、signature、issuer、validity、subject、subjectPublicKeyInfo 等欄位，但不使用 issuerUniqueIdentifier 及 subjectUniqueIdentifier 欄位；憑證的擴充欄位（Extensions）支援 authorityKeyIdentifier、subjectKeyIdentifier、keyUsage、certificatePolicies、subjectAltName、subjectDirectoryAttributes 、 extKeyUsage 、 cRLDistributionPoints 、 authorityInfoAccess 等欄位。

(10)憑證的 issuer 及 subject 欄位採用 X.500 Distinguished Name (DN)，並且能夠記載我國官方正式登記的中文名稱；當名稱屬性資料中含有中文時，並支援 CNS 11643 完整中文字集，且使用符合 Unicode 4.0 版（或更新版本）之 UTF-8 編碼方式記載於憑證中。Subject 欄位之 DN 資訊透過醫事系統提供。

(11)仿照 GPKI 憑證及憑證廢止清冊格式剖繪現有的憑證格式，於 subjectDirectoryAttributes 欄位記載發證對象特有的屬性資料。

(12)憑證廢止清冊需採用 ITU-T X.509 V2 格式，並符合 IETF PKIX Certificate and CRL Profiles 標準（RFC 3280 或更新的版本）。

(13)憑證廢止清冊格式的設計，仿照 GPKI 憑證及憑證廢止清冊格式剖繪現有的憑證廢止清冊格式，即憑證廢止清冊基本欄位應包含 version、signature、issuer、thisUpdate、nextUpdate、revokedCertificates 等欄位；兩種憑證廢止清冊中之 revokedCertificate 欄位，每一個 Entry 所使用的 CRL Entry 擴充欄位 (CRL Entry Extensions) 支援 reasonCode 欄位；憑證廢止清冊的擴充欄位（CRL Extensions）支援 authorityKeyIdentifier、cRLNumber、deltaCRLIndicator（適用於 Delta CRL）、freshestCRL（適用於 Complete CRL）等欄位。

(14)發現醫事人員或機構已歇業，則主動納入憑證廢止清冊內。

(15)CA 伺服器簽發憑證及憑證廢止清冊時，採用長度 2048 位元（含）以上之 RSA 金鑰，並使用 sha1WithRSA 簽章演算法（OID = 1.2.840.113549.1.1.5）。

(16)CA 伺服器簽署稽核紀錄時，採用長度 1024 位元（含）以上之 RSA 金鑰。

(17)CA 伺服器對 RA 伺服器進行通訊時之簽章或金鑰交換，採用長度 1024 位元（含）以上之 RSA 金鑰。

(18)系統對於人員角色的分工，符合 GPKI CP 之保證等級第三級以上的規定，且對於各類人員角色必須能夠強制權限分散(Separation of Duties)，也就是說各類人員角色操作系統時，強制採用 n 取 m（m-out-of-n）多人控制（multi-person control）的機制。

(19)系統所自動記錄的稽核記錄種類符合 AICPA/CICA WebTrust Program for Certification Authorities 之規定，並符合 GPKI CP 之保證等級第三級以上的規定。

2.註冊管理中心系統

(1) 註冊管理中心系統提供對 RAO 之網頁服務，並透過 Web Base 完整

之操作介面供 RAO 使用，並可與營運作業等系統介接必要之各類申辦與審核資訊。

(2) 註冊管理中心之 Web Base 系統操作介面，提供 HCA 憑證申辦、憑證廢止、憑證IC 卡解鎖卡、卡片簽收註記、各類申辦作業進度查詢、各項作業紀錄稽核等業務作業功能。

(3) RAO 必須使用 IC 卡登入 RA 伺服器，並使用 IC 卡對於審理的案件內容簽署數位簽章，同時對憑證註冊相關資訊加以記錄。所使用的 IC 卡通過 NIST FIPS140 Level2 以上的驗證，並為長度 1024 位元（含）以上之 RSA 金鑰。

(4) 註冊管理中心系統提供 RAO、初審 RAO、營運中心操作人員、系統管理員等各類系統使用者不同角色權限使用者之系統操作應用功能。

(5) 提供 IC 卡（含 PC/SC 讀卡機）作為 RAO 私密金鑰之儲存媒體。

(6) 註冊管理中心系統提供與伺服器應用軟體憑證申辦服務、憑證申辦作業預約服務介接功能。

(7) RA 伺服器對 CA 伺服器進行通訊時之簽章或金鑰交換，採用長度 1024 位元（含）以上之 RSA 金鑰。

(8) 註冊管理中心系統與 RAO 於作業過程中，在取得本署醫事管理系統資料庫之資料時，需配合本署醫事管理系統提供之應用程式介面或資料介接協定，進行資料驗證比對處理，於審驗資料之過程中如發現資料有錯誤時，並主動透過醫事管理系統提供之介面回復資料需修正的訊息。

3.金鑰管理系統

(1) 提供專屬機房內各系統及跨機房各單位之間，傳輸機密資料時所使用的加解密金鑰及資料加解密作業。

(2) 提供產生、儲存、啟用、停用、更新、銷毀及存放金鑰的完整管理機制。

(3) 提供健保 HPC Key 安全匯入金鑰管理系統之功能，並提供符合健保 HPC Key 安全管控要求之金鑰代管功能。

(4) 金鑰管理系統使用通過FIPS140-2 Level3 以上驗證的HSM 來產製及儲存其所有金鑰對。

(5) 配合 HCA 的系統需求，提供金鑰遠端伺服的功能，使 RAO 網站系統可在安全的網路連線作業下，達到高品質 RSA 金鑰對及對稱式金鑰產生、PIN Hash 和 IC Card 製卡資料檔加密保護 (IC Card

Personalization Block) 的金鑰服務功能。

(6) 系統提供健保 HPC Key 安全匯入金鑰管理系統之功能，並符合健保 HPC Key 安全管控要求。

4.個人化製卡管理系統

(1) 個人化製卡管理系統功能為印製醫事人員憑證 IC 卡、醫事機構憑證 IC 卡與 RAO 作業 IC 卡，其範圍包括顯性資料姓名、ID、卡號之印刷、隱性資料寫入 IC 卡晶片與相關防偽印刷之處理。

(2) 本專案印製卡系統處理個人化資料之傳遞與保存，均以本地端金鑰加密。

(3) 本系統搭配 HSM，保護相關個人化所需金鑰及主機端管理金鑰。

(4) 製卡機與本系統作業連接，以進行卡片個人化作業。

(5) 製發醫事人員憑證 IC 卡、醫事機構憑證 IC 卡(含附卡)、測試卡、備用卡及藥局專用卡。備用卡及藥局專用卡僅提供健保應用功能，即卡內需載入健保 HPC Key Set，但不可載入憑證。

(6) 製卡管理應包含製卡檔匯入製卡流程操作介面、製卡結果回復檢視介面(需相容本專案印製卡機操作軟體)、製卡紀錄歷史查詢、製卡狀態與廢卡查詢等功能，製卡狀態應提供日、月、年報表檔。

(7) 作業方式為每一張卡片憑證簽發完畢後,可立即進行卡片製作工作。

5.醫事資料同步交換系統

(1) 執行醫事資料庫完整更新及差異更新至 HCA2.0 資料庫作業。

(2) 提供醫事資料同步作業之完整稽核紀錄查詢介面。

(3) 結合 RAO 憑證作業申請者身分驗證需求,透過本署醫事管理系統提供之介面，即時與醫事管理系統資料庫進行資料比對，及傳遞申請者資料需修正之通知至醫事管理系統。

(4) 提供即時與定期接收醫事管理系統之醫事機構或醫事人員 DN 資訊功能。

(5) 提供資料異動至 HCA2.0 資料庫錯誤之回復功能。

6.目錄服務管理系統

(1) 依照 X.500 相關國際標準並符合 LDAP-V2、V3。

(2) 提供憑證內容資料及憑證狀態等資訊公布、查詢與下載功能。

(3) 提供各類憑證廢止清冊之公布、下載等功能，並可設定即時公布或每日公布次數之功能。

(4) 公布及下載之憑證採用 X.509 標準(內含 HCA2.0 憑證機構簽署之數位簽章)。

(5) 提供各項憑證公布、下載作業及系統設定作業之記錄功能。

(6) 提供中文化之憑證查詢網頁，所查詢的憑證中如含有中文，則在網頁上必能夠完整顯示 CNS11643 中文字集所有的中文字。

(7) OCSP 伺服器應使用通過 NIST FIPS140 Level3 以上驗證的 HSM 來產製及儲存其簽署 OCSP Response 訊息之金鑰對。

(8) OCSP 伺服器簽署 OCSP Response 訊息時，採用長度 2048 位元(含)以上之 RSA 金鑰，並使用 sha1WithRSA 簽章演算法（OID = 1.2.840.113549.1.1.5）。

7.卡片作業管理及統計作業系統

(1) 提供線上讀卡機功能測試介面。

(2) 提供線上 HCA2.0 卡片內容解析介面。

(3) 線上自動下載 HCA2.0 卡片開卡、解鎖卡、密碼變更之 OCX 元件或手動下載安裝以上 BATCH SHELL 元件功能。

(4) 提供開卡統計、卡片點收介面及查詢功能。

(5) 提供營運整體流程內各項作業績效狀況統計及查詢功能。

(6) 透過 SSL 安全通道及驗證用戶代碼進行 PIN 碼設定及解鎖卡。

(7) 提供營運整體流程內各項作業績效狀況統計及查詢功能。

(8) 因應營運作業需求及配合醫療院所環境之作業彈性，提供線上與卡片作業有關之各類 ActiveX 元件。各類元件需視不同需求支援健保讀卡機或 PC/SC 讀卡機應用。

8.營運中心表單影像管理系統

配合本專案需求，掃描使用者填寫內含罕見字之紙本申請單，並於製卡作業時進行影像調閱比對使用。

9.時戳服務系統(Time Stamp Service, TSS)

(1) TSS 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。

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

(3) TSS 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。

(4) TSS 伺服器透過 FIPS 140-2 Level 3 認証過之 HSM 進行時戳簽章。

(5) TSA 私鑰由硬體加密模組自行產生，不可匯出。

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

(7) 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。

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

(9) 具備自動校時之功能。

(10)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。

(11)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。

(12)時間精確度以 0.01 秒為單位。

(13)時戳服務之對外 IP 或 URL 若有調整之需求，須經本署同意後才可進行調整。

10.安全保密函式庫(Application Program Interface, API)維護

(1) 維持營運電子認證應用系統所需之 API，包含 PKCS#11、CSP、HCACSAPI、HCA API。

(2) 維持營運 API 測試程式原始碼及測試介面。

附錄二、軟硬體設備清單

1.HCA1.0 軟體明細

(1)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)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
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

NO	建構項目名稱	產品型號／規格	數量	備註
		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. HCA1.0 硬體規格

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	1	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	憑證系統 備援主機	PC Server	P4 3.0G 512M RAM *2 80G HD	1	HCA 備援機房
17	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
18	RAO 網站備援主機	SUN E420R	450M CPU *1 2G RAM 18.2G HD *2	1	HCA 備援機房

NO	建構項目名稱	產品型號／規格		數量	硬體所在點
19	DB 備援主機	PC Server	P4 3.0G 512M RAM *4 160G *2 Raid1(SATA)	1	HCA 備援機房
20	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
21	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
22	憑證系統備援硬體加密模組	nCipher	SCSI 介面 CASE	1	HCA 備援機房
23	時戳服務備援硬體加密模組	Rainbow	PCI 介面	1	HCA 備援機房
24	金鑰管理系統備援硬體加密模組	WebSentry	PCI 介面	1	HCA 備援機房
25	時戳硬體伺服器	nCipher	DSE 200	1	HCA 主機房

3.HCA2.0 軟體明細

NO	建構項目名稱	功能說明	作業系統
1	憑證管理	發放醫事人員、醫事機構憑證 IC 卡及醫事用途之伺服器應用軟體憑證	Solaris 9
		稽核紀錄管理	Windows 2003
2	註冊管理中心	憑證作業申辦格式及內容檢核	Solaris 9
		註冊服務窗口網頁系統	Windows 2003
3	金鑰管理	3DES Session Key 及系統 RSA Key Pair 產製、使用	AIX 5L
		HPC Key Set 保存及使用	Windows 2003
4	個人化製卡管理	製發醫事人員卡、醫事機構(正、附)卡、測試卡、備用卡及藥局專用卡	Windows 2003
5	醫事資料同步交換	即時與定期接收醫事管理系統之醫事機構或醫事人員 DN 資訊功能	AIX 5L
6	目錄服務管理	憑證內容資料及憑證狀態等資訊公布、查詢、下載與刪除功能	Linux on Power
		OCSP 服務	Linux Red Hat
7	卡片作業管理及統計	線上與卡片作業有關之各類 ActiveX 元件	Windows 2003
		作業績效狀況統計及查詢	
8	專屬網站	HCA2.0 各項訊息、公告及文件下載	AIX 5L

NO	建構項目名稱	功能說明	作業系統
9	客服系統	FAQ、線上技術問題資料庫	AIX 5L
10	營運中心表單影像管理	製卡作業時進行影像調閱比對使用	Windows 2003
11	營運中心管理資訊	ISO 27001：2005 之文件檔案管理機制	Windows 2003
12	時戳服務	nCipher DSE 200	HSM
13	DB	HCA 營運資料庫	Oracle 10g

4.HCA2.0 硬體規格

項次	品　　名	交付數量		廠牌及型號
		主機房	備援機房	
1	專屬網站主機	2	1	IBM System P5 510(P51A)
2	客服系統主機	2	0	IBM System P5 510(P51A)
3	目錄服務管理系統主機	2	1	IBM System P5 510(P51A)
4	醫事同步交換系統主機	2	0	IBM System P5 510(P51A)
5	金鑰管理系統主機(KMS)	1	1	IBM System P5 510(P51A)
6	備份主機	1	1	IBM System P5 510(P51A)
7	資料庫主機	2	1	IBM System P5 550(P55A)
8	卡片作業管理及統計作業系統主機	2	0	IBM System X3650
9	憑證稽核管理系統主機	1	1	IBM System X3650
10	註冊管理中心系統主機(RA)	2	1	IBM System X3650
11	網路管理主機	1	0	IBM System x3500
12	營運中心 MIS 主機	1	0	IBM System x3500
13	營運中心表單影像管理系統主機	1	0	IBM System x3500
14	個人化製卡管理系統主機(1)	2	0	IBM System x3500
15	個人化製卡管理系統主機(2)	2	0	DELL OPTIPLEX
16	備份主機 FOR TSM	1	1	IBM System x3500
17	憑證管理系統主機	2	1	Sun Fire V245

項次	品　　名	交付數量		廠牌及型號
		主機房	備援機房	
18	光纖磁碟陣列儲存系統	1	1	IBM System Storage DS4700
19	磁帶櫃	1	1	IBM System Storage TS3200 Tape Library
20	資料備份軟體	一式	一式	IBM Tivoli Storage Manager
21	網路光纖交換器 A	2	0	IBM System Storage SAN32B
22	網路光纖交換器 B	0	1	IBM System Storage SAN32B
23	網路負載平衡交換器	2	0	Juniper DX3280
24	網路交換器	6	1	DLINK DGS-3100
25	核心防火牆	2	1	Juniper ISG1000
26	乙級防火牆	1	0	Nokia IP290
27	硬體密碼模組	2	0	nCipher NetHSM500
28	時戳管理系統主機	0	1	nCipher TSS200
29	印製卡機	2	0	Datacard SP75
30	多功能事務機	1	0	HP CM1015

附錄三、資訊安全保密切結書

資訊安全保密切結書

公司（以下簡稱乙方）受行政院衛生署（以下簡稱甲方）委託辦理「99 年度醫事憑證管理中心營運案」(以下簡稱本專案)，依本專案契約規定乙方應與甲方簽署保密切結書。乙方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、蒐集依契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人。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人。

三、乙方違反本資訊安全保密切結書之規定，致造成甲方或第三人之損害或賠償，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

附錄四、企劃書大綱

目錄：目錄後請附上企劃書中與評選項目相關之建議重點、頁次對照彙總表

企劃書項目對照表(詳附錄五)

壹、緣起：背景說明、未來環境預測、問題評析及醫事憑證問題之瞭解。

貳、專案概述

一、專案名稱

二、專案目標

三、專案範圍

四、專案時程

參、規劃建議

一、整體計畫架構

二、實施策略與方法：詳述本計畫各工作項目之實施策略及方法

(一)營運專屬機房

(二)提供 HCA 營運辦公室

(三)營運 HCA2.0 及提供所需相關系統之維運服務

(四)提供 HCA2.0 IC 卡發卡服務

(五)維護 HCA 專屬網站與專案管理平台

(六)維護 HCA 營運中心管理資訊系統

(七)提供營運管理制度及配合外部安全稽核

(八)提供符合 GPKI 規範要求

(九)設置諮詢服務窗口，並提供客戶服務品質管理機制

(十)提供系統危機應變處理機制、災害演習作業及營運移轉規劃

(十一)提供 HCA1.0 對外目錄服務、黑名單公告、儲存庫等相關服務

(十二)完成 TSS 功能增修及設備購置

(十三)完成用戶憑證金鑰長度由 1024 提升為 2048 位元

(十四)提供已開發系統所需之 2048 位元金鑰長度 API 並提供諮詢服務

(十五)辦理教育訓練及說明會

(十六)其它

肆、管理建議

一、專案組織與管理

(一)專案成員及分工

(二)專案管理相關文件標準及工具(註明是否建置專案管理網站，並

說明其功能)

二、專案管理

(一)專案工作項目劃分、時程及重要查核點(含自訂交付產品項目及查核點)

(二)專案監控(含專案執行、問題處理...等)、品質保證措施及方法、風險管理、需求變更管理

(三)投標廠商之執行能力(包括實績經驗、如期履約能力、過去類似案件履約績效、是否包含各相關專業成員...等)

伍、預期成果效益及自訂服務水準指標項目

陸、特色項目

一、凡有助於本專案之創新性、完整性及具體可行之建議

二、與本專案有關之優規建議或服務

柒、價格分析：投標廠商應針對本專案各項需求作業，詳細分析其對應價格及佔全案比率。並詳細預估交接之成本。

捌、附錄(相關證明文件影本)

附錄五、評選項目與企劃書內容對照表

99 年度醫事憑證管理中心營運案

「　　公司」企劃書項目對照表

日期：　年　月　日

評選項目		企劃書內容對照			
項目	內容	內容摘要 (請針對內容提出概述)	章節	頁次	備註
一、計畫內容	(一)對本專案需求瞭解程度、配合度				
	(二)對本專案整體解決方案規劃之可行性、完整性				
	(三)對本專案人力之調配及教育訓練規劃及執行方法之可行性、適切性				
	(四)系統安全及備援規劃（含系統備援、回復及系統安全等規劃）				
	(五)交接、營運移轉規劃				
二、廠商專案經驗及專案管理能力	(一)團隊組織之成員專業背景、經驗、具體實績及執行能力				
	(二)團隊之分工及合作機制之適切性				
	(三)專案工作項目劃分、時程及重要查核點				
	(四)自訂查核點及交付項目之完整性、合理性				
	(五)專案監控（含專案執行、問題處理...等）、品質保證措施及方法				
三、特色	(一)凡有助於本專案之創新性、完整性及具體可行之建議				

評選項目		企劃書內容對照			
項目	內容	內容摘要 (請針對內容提出概述)	章節	頁次	備註
項目	(二)與本專案有關之優規建議				
四、價格分析及經費編列之合理性及完整性（應針對本專案各項需求作業，詳細分析其對應價格及佔全案比率）					
五、附錄：相關證明文件(含實績證明)影本					

附錄六、評選評分表

99 年度醫事憑證管理中心營運案評選評分表

委員編號：	配	廠商編號				
評選項目	分	1	2	3	4	5
1.計畫內容 (1) 對本專案需求瞭解程度、配合度 (2) 對本專案整體解決方案規劃之可行性、完整性 (3) 對本專案人力之調配及教育訓練規劃及執行之可行性、適切性 (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） (5) 交接、營運移轉規劃	40					
2.廠商專案經驗及專案管理能力 (1) 團隊組織之成員專業背景、經驗、具體實績及執行能力 (2) 團隊之分工及合作機制之適切性 (3) 專案工作項目劃分、時程及重要查核點 (4) 自訂查核點及交付項目之完整性、合理性 (5) 專案監控（含專案執行、問題處理…等）、品質保證措施及方法	30					
3. 特色項目 (1) 凡有助於本專案之創新性、完整性及具體可行之建議 (2) 與本專案有關之優規建議	10					
4.價格分析及經費編列之合理性及完整性	20					
評分合計	100					
轉換序位						

評選委員意見：

委員簽章：

註：受評廠商之總評分平均分數未達合格分數 70 分者，不得為最有利標或優勝廠商。

附錄七、評選評比總表

行政院衛生署

廠商評選評比總表(序位法-評分轉序位法)

採購案名稱：99 年度醫事憑證管理中心營運案 日期：年 月 日

<table>
<tr><td colspan="3">廠商名稱
序位
標價</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="3">出席評選委員</td><td>評分</td><td>序位</td><td>評分</td><td>序位</td><td>評分</td><td>序位</td><td>評分</td><td>序位</td><td>評分</td><td>序位</td></tr>
<tr><td colspan="3">A 委員</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">B 委員</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">C 委員</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">D 委員</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">E 委員</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">F 委員</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">G 委員</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">H 委員</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">序位合計數</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="3">總分合計</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="3">總平均分數</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="3">合格廠商優勝序位(準用最有利標)(出席評選委員綜合考量及過半數決議)</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td rowspan="4">出席委員(簽名)</td><td>姓名</td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>職業</td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>姓名</td><td></td><td colspan="2"></td><td rowspan="2">請假委員</td><td>姓名</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>職業</td><td></td><td colspan="2"></td><td>職業</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
</table>

註：受評廠商之總評分平均分數未達合格分數 70 分者，不得為最有利標或優勝廠商。