行政院衛生署

95 年度醫事憑證應用推廣案

醫事憑證系統導入指引

台灣醫院協會　謹提

中華民國 95 年 12 月 20 日

衛生署資訊中心審查委員意見回覆對照表

編號	審查意見事項	意見回覆內容	修改頁碼
1	建議醫院考慮向醫療憑證管理中心申請伺服器應用軟體憑證進行簽章應用，此建議是否符合現行法令。	行政院衛生署「醫療憑證管理中心」為中央主管機關於醫療領域建立電子認證及安全制度而設立之合法憑證管理中心，其簽發之憑證具有合法之效力，可代表申請機構之身分，應用於電子化政府的各項應用(如電子公文等)。惟醫療機構電子文件以「應用伺服器應用軟體憑證」進行簽章外，仍需加上製作人之醫事人員憑證簽章並經中央主管機關加註時戳，始為合法之電子病歷。	P18
2	內容有多處重複。	已經過本會健康管理資訊委員 (雷欽隆、范仲玫、張顯洋、黃援傑、劉德明、陳建志、吳東泰、李中原、許世欣、筆恆泰、楊新偉、傅仲蓉等)提供意見，其成員多為各醫療院所之 CIO，承署內委員意見與本會健康管理資訊委員意見有類似之處，本會依據檢討指引文件，進行大幅修改。	整份文件
3	本文件之使用對象應包含台灣任何醫療院所在考慮導入醫事憑證應用之「可行性參考」；建議將本計畫在三個醫療院所導入過程中之各個環節所考慮因素、環境、決策情境，以及與既有系統整合考量等寶貴經驗詳實記錄、整理與分析清楚。	承委員建議，本會已補充三個醫療院所導入過程中之各個環節所考慮因素、環境、決策情境，以及與既有系統整合考量。 本指引以參考醫療界在感控、病安、大量傷患等指引為基礎，完成後並交付本會衛生資訊委員會修訂。本會衛生資訊委員會之成員皆為國內具代表性之醫院資訊高階主管，藉從醫療界慣例與專家意見來產出有助醫院導入醫事憑證之文件。 本會已根據委員建議增加「可行性參考」為指引之第伍章節中。	P6~P8 P9~P11
4	應朝向如何解決醫院所考慮的問題，提供更明確之指引。	已經過本會健康管理資訊委員(雷欽隆、范仲玫、張顯洋、黃援傑、劉德明、陳建志、吳東泰、李中原、許世欣、筆恆泰、楊新偉、傅仲蓉等)提供意見，其成員多為各醫療院所之 CIO，承署內委員意見與本會健康管理資	P11~P19

編號	審查意見事項	意見回覆內容	修改頁碼
		訊委員意見有類似之處，本會依據檢討指引文件，針對醫療院所導入醫事憑證應用考慮之問題進行補充，提供更明確之方向，供醫療院所參考。	

目　　錄

壹、前言

醫療憑證係行政院衛生署「網路健康服務推動計畫」之子計畫之一，為了配合行政院「挑戰 2008-國家發展重點計畫」，規劃以公開金鑰(Public Key Infrastructure, PKI)為基礎建設，設置及營運「醫療憑證管理中心」(Healthcare Certification Authority, HCA)，於 92 年 6 月正式對外提供醫療電子認證服務及電子簽章機制，並在醫療體系內形成安全可信賴的醫療資訊交換環境。

84 年「電腦個人資料保護法」通過，91 年 11 月「電子簽章法」通過，93 年 3 月公佈「醫療機構實施電子病歷作業要點」，其第三條明文規定電子病歷之製作方式為「應經由行政院衛生署醫療憑證管理中心簽發憑證之醫事人員卡或醫事機構卡製作」，以及 93 年 4 月醫療法新修訂「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」。行政院衛生署於 94 年 11 月 24 日公告「醫療機構電子病歷製作及管理辦法」，該辦法第五條規定「電子病歷之簽章，應憑中央主管機關核發之醫事憑證為之，並經中央主管機關加註時戳」。因醫療資訊多涉及個人隱私、個人生命安全，考量採醫事憑證、電子簽章及時戳等方式，這些條文的修訂通過，成就醫療資訊電子文件化的環境，資訊、資料電子化已是當前的潮流趨勢，未來醫療機構勢必漸漸朝向無紙化、無片化的電子文件方式發展，因此，醫院如何配合法規政策提昇醫事憑證之整合應用，乃是目前所需面臨的重要課題。

行政院衛生署「醫療憑證管理中心」已於 92 年 6 月正式設置並啟動，運用醫事憑證機制，除可運用在水平層級醫療院所間的醫療資訊傳遞交換，如醫院與醫院之醫療影像瀏覽查詢，亦可運用在垂直層級醫療院所間的醫療資訊瀏覽查詢，如醫院開放檢驗檢查報告與放射影像讓合作診所查詢，這樣不但可以增加醫療照護網的診療效率，也可避免不必要的重複檢驗檢查，進而減少醫療資源的浪費。

行政院衛生署有鑑於將資訊科技應用於醫療產業將是未來醫院管理必然的趨勢，經公開徵選企劃案後，特委由台灣醫院協會承辦 94 與 95 年度醫事憑證應用推廣計畫。為順利引導及輔助醫療院所相關醫事憑證應用，並且對醫事憑證有更深層的瞭解，台灣醫院協會於計畫成果中摘要出本「醫事憑證系統導入指引」，希透過成果研討與網站下載的方式宣導醫事憑證正確的使用觀念與應用實務，強化醫事機構與人員對於醫事憑證的瞭解，並期望將醫療資訊系統導入醫事憑證應用之實施經驗傳達至各醫事服務機構。

為確保本作業指引於實務上之運作無虞，95 年度醫事憑證應用推廣計畫徵求三家區域級以上示範醫院實際採用本作業指引草案試辦醫事憑證應用系統導入，並依據實際試辦經驗再次修正本作業指引草案，特於草案完成之際，鑒請本會醫療資訊委員會雷欽隆副召集人針對本指引召開座談會議，並針對委員所提出之意見做進一步的修改，始完成本作業指引，本協會期能藉由此作業指引之製訂，促使全國醫院重視並強化導入醫事憑證應用，若本作業指引仍有為未盡完善事宜或任何建議，皆歡迎提供意見予本會，使本作業指引之訂定更臻完

善。

貳、通則

一、合法性原則

本指引完全以相關法律之合法性考量之。

二、彈性原則

本指引是由醫事憑證應用之共同作業與考量之角度方面著手,為多樣化醫療應用系統根據機密性需求、身分鑑別需求、完整性需求、不可否認性需求而異中求同，本指引可視為醫事憑證作業之指引，而非特定醫療應用系統流程之規範指引。

三、經濟性原則

資通安全品質是正比與金錢及各項資源的投入，本指引之建議採行最適效益原則，而非最佳效益原則，醫院可視本身投入預算與決心在合法的前提下，自行決定採最佳效益原則。

四、實用性原則

由於本指引係以「醫事憑證應用」為目標，經過審慎評估後，本作業指引著重於醫事憑證基本實務作業面，無關乎醫院層級及規模皆能一體適用，因而未加以區分版本。

參、範圍

本指引針對國內醫療院所應用公開金鑰基礎建設之唯一合法單位「衛生署醫療憑證管理中心」為作業對象。

本指引以國內醫療院所在現行或新建資訊系統中，規劃應用醫療憑證之 PKI 公開金鑰基礎建設來保障醫療資訊之機密性、身分鑑別、完整性、不可否認性之相關衍生作業之建議，提供醫療院所在院內政策、流程制定、系統建置過程中之資源。

本指引另檢附衛生署醫療憑證應用之示範功能原始碼，針對電子簽驗章、時戳、TMT 標準之簽章應用提供國內醫療院所在系統建置期間之參考。

肆、使用方式

一、用以建立適當的醫事憑證應用流程

以符合衛生署醫事處現有法令依據為標準,並考慮醫療院所相關的院內衍生作業供醫療院所建立醫事憑證應用流程。

二、衡量醫事憑證應用系統營運所需的資源多寡

以此作為醫療院所評量營運醫事憑證應用系統時的資源需求。本指引所提出的作業項目,醫療院所可以依據作業項目度量營運醫事憑證應用系統的人力與效益,可有效度量經費分配與資源需求。

三、評量廠商能力與產品適用性的標竿

以此作為醫療院所評量醫事憑證應用系統廠商能力與產品功能的指引。市場上有許多運用在醫療院所 PKI 的系統,醫療院所可以本指引所提出的作業項目做一衡量參考,審慎選擇。

伍、醫事憑證系統導入可行性作業

一、評估與導入階段建議考量因素

(一) 院內自我環境評估

每家醫療院所的規模，作業流程各不相同，雖然很難統一給予建議，但基本之評估準則建議醫療院所根據自身的規模、層級、作業流程需求、安全等級要求來思考，以下針對特別幾項要提醒院所在導入醫事憑證應用時之評估事項。

1. 法規的符合度

若院所已有想要導入醫事憑證應用之標的系統，應審慎了解電子簽章法、醫療法、醫療機構電子病歷製作及管理辦法之內涵，評估應用系統事憑證應用之標的系統在醫療資訊製作、管理、儲存、傳遞各層面是否符合法規之要求。

2. 要導入的應用範圍

若院所已有想要導入醫事憑證應用之標的系統，應審慎評估本身要導入之應用，是單純院內應用，還是會與院外交換，需要接受他院的病歷資訊嗎? 本身此應用有無法律規範，系統每日、每分之平均應用交易量可能為多少，需要存證嗎? 確定範圍後才能仔細的檢視這些問題。

3. 穩定持續運轉的風險評估

若院所已有想要導入醫事憑證應用之標的系統，應審慎評估能否如法規所規範的持續不中斷運轉，例如人員簽章的速度是否能夠接受，目前健保讀卡機簽章速度平均為兩秒，時戳是否能持續取得?院內的網路備援如何?最近三年的網路斷線率如何?

4. 使用者的共識

院所導入醫事憑證應用應該要了解使用者之舊有使用習慣，尤其醫師，簽章對醫師是一種責任的賦予，在使用者教育與系統使用的友善度上，需要與使用者有一定程度之共識。

5. 導入之效益

院所應了解導入醫事憑證之效益， 因為醫事憑證導入應用具多樣化性，了解本身應

用之效益所在才能成功的改變作業流程，使院內使用者有動機配合，以下就 衛生署 95 度醫事憑證應用推廣計畫之示範醫院的導入效益舉例供作參考之。

(1) 三軍總醫院

- 提升他院對三總放射影像的信任度。
- 踏出放射影像交換安全環境營造的第一步。

(2) 行政院衛生署新竹醫院

- 解決無片化合法性的隱憂。
- 強化兵役體檢的放射影像證據力。

(3) 臺北醫學大學附設醫院

- 提早因應電子病歷趨勢，賦予電子醫令證據力。

(二)作業大環境了解評估

1. HCA 的相關作業了解

雖然目前醫院都有配合醫師卡開卡與展期作業，但若實際導入應用，可能會衍生其他即時的線上作業，例如即時需要解鎖卡，因此建議醫療院所在導入前先針對 HCA 相關的作業可能需要在院內處理的，先做好準備，要了解衛生署醫事憑證管理中心之作業可透過客服專線(0800-364-422)尋求協助。

2. 衛生署計畫示範醫院的應用方式參考

衛生署於 95 年度之醫事憑證應用推廣計畫，已在三軍總醫院、行政院衛生署新竹醫院導入「PACS 醫事憑證應用系統」，台北醫學大學附設醫院導入合「門診醫令醫事憑證應用系統」，院所在導入前可聯絡並參考三家醫院之導入方式。

二、維運階段建議考量因素

(一)院內新作業流程

1. 醫師卡解鎖卡作業

院所應考慮，醫師卡解鎖卡作業、憑證管理作業等新線上服務作業流程。

2. 其他抱怨與處理服務

包括卡片故障、忘記密碼、卡片遺失等等，由於簽章需要即時作業，因此這些有關卡片的處理將會嚴重影響線上作業，建議依針對相關作業評估新可行流程。

(二) 系統維運考量因素

1. 簽章存證的管理

電子病歷之儲存，可取代紙本，因此電子資料儲存的可靠度需要良好的持續管理，包含儲存容量、儲存速度，備援方式都需要評估維運環節。

2. 時戳索取的備援方案

目前時戳依法須向 HCA 取得，但台灣網路環境之穩定性尚仍無法維持 24X7 等級之運作，因此醫療院所若導入電子病歷應用醫事憑證時，建議除 VPN 外，院內應至少有實體分開之備援網路兩條，同時需持續監測院內與 HCA 時戳服務間之效能測試，異常時需即時作出反應，以免電子病歷在斷線的時間點間無法取得時戳。

陸、醫事憑證系統導入作業

一、導入評估

(一) 導入目標

醫療院所在評估導入醫事憑證可達成的目標與方式時，建議以欲達成醫療資訊儲存、傳遞之機密性、完整性、身分鑑別、不可否認性來思考。

1. 機密性

應用系統在醫療資訊儲存、傳遞中，是否只容許已授權的人存取資料，例如轉診轉檢資料傳遞時，為了避免病人的隱私資訊被取得即是一例，此例中可運用醫事機構憑證加解密機制來加密診所與醫院之間透過網際網路所傳遞的訊息，使第三者無法透過網路竊聽或其他方式得知病人的隱私資訊。

2. 完整性

應用系統在醫療資訊儲存、傳遞中，是否送出的資料不容許被竄改，例如院外放射影像的光碟讀取，希望能確認此光碟中的 DICOM 影像的確在攜出原來的造影醫院後，並沒有被修改過，此例中可運用醫事人員/機構憑證簽驗章機制，來驗證確保 DICOM 影像的完整性。

3. 身分鑑別

使用者在使用應用系統時，是否需要比密碼還更高等級的方法來確認是誰，若需要可採用醫事人員 IC 卡的機制，在應用系統做身分簽入時除了輸入密碼外，還需要讀取 IC 卡來驗證。

4. 不可否認性

應用系統在醫療資訊儲存、傳遞中，是否使用者不可對其所作的行為否認，例如門診醫令補正，則可以使用醫事人員憑證簽驗章來儲存每次修正的版本，如同紙本病歷一樣保留累加來作為強化病歷製作與管理的機制。

(二) 適法性分析

1. 電子簽章法 (91.4.1 公布)

第 6 條：文書依法令之規定應以書面保存者，如其內容可完整呈現，並可於日後取出供查驗者，得以電子文件為之。

第 9 條：依法令規定應簽名或蓋章者，經相對人同意，得以電子簽章為之。

2. 醫療法 (93.4.28 修正)

第 68 條：醫療機構應督導其所屬醫事人員於執行業務時，親自記載病歷或製作紀錄，並簽名或蓋章及加註執行年、月、日。前項病歷或紀錄如有增刪，應於增刪處簽名或蓋章及註明年、月、日；刪 改部分，應以畫線去除，不得塗燬。 醫囑應於病歷載明或以書面為之。但情況急迫時，得先以口頭方式為之， 並於二十四小時內完成書面紀錄。

第 69 條：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。

3. 醫療機構電子病歷製作及管理辦法(94.11.24 公布)

第 1 條：本辦法依醫療法(以下簡稱本法)第六十九條規定訂定之。

第 2 條：醫療機構以電子文件方式製作及貯存之病歷(以下簡稱電子病歷)，符合本辦法之規定者，得免另以書面方式製作。

第 5 條：電子病歷之簽章，應憑中央主管機關核發之醫事憑證為之，並經中央主管機關加註時戳。

二、 導入週期

國內醫療院所建議採用下列步驟來建立醫事憑證之應用，首先考量整體院內的相關流程，包含發卡、簽章時機、驗章時機、卡片異常處理等流程設計規劃，詳細確認本身的應用流程之後，就可以根據流程與導入目標需求，來決定要用哪一類的醫事憑證來應用，接著才是資訊部門需要建置實際的醫事憑證機制，醫事憑證實務上是需要跟國內的醫療資訊標準來整合的，最後方是教育訓練的規劃。

醫事憑證的導入是需要相當之使用者共識方可進行,因此使用者運用醫事憑證的好處應跟醫療院所導入的效益一併考量，方能增加醫事憑證系統導入成功之機率。下表「導入評估表」是以「行政院衛生署 95 年度醫事憑證應用推廣計畫」示範醫院導入醫事憑證應用之經驗整理而成，可協助導入醫事憑證應用之評估。

※以示範醫院導入門診醫令作業及醫療影像作業為例

導入評估表					
評估項目	法律依據	導入目標	資源需求	資料量	醫療需求
應用流程設計	● 醫療法 68 條 ● 醫療機構電子病歷製作及管理辦法第五條	● 機密性完整性 ● 身分鑑別 ● 不可否認性	● 醫師 ● 放射師 ● 醫技師	● ？筆/日 ● ？筆/月	●
醫事憑證的選擇使用	● 醫療機構電子病歷製作及管理辦法第五條	…	● 醫事機構憑證 ● 醫事人員憑證	● 簽章時間 ● 時戳時間	●
應用系統建置/擴充	● 醫療機構電子病歷製作及管理辦法第五條	…	● 外包 ● 自行開發	● ？筆/日 ● ？筆/月	● 電子簽章 ● 資料加解密 ● 身分鑑別 ● 時戳
教育訓練的方式與對象		…	● 教育訓練師資	●	● 實例說明

三、 導入方式

(一) 導入步驟

建議醫療院所採下列步驟導入醫事憑證應用：

1. 了解醫事憑證之憑證種類。
2. 了解醫事憑證之相關法律規定。
3. 建立醫事憑證院內即時處理作業流程。
4. 完整規劃醫事憑證整合現有系統之作法。
5. 規劃應用系統之簽章時機方式、驗章時機方式、取時戳方式、簽體與資料保存方式。
6. 設計教育訓練計劃並執行。
7. 檢視醫事憑證導入效益。

(二) 導入指引

1. 總則

1.1 目的

本指引冀能藉由醫療與資訊產業的專家學者群不斷的集思廣益，精益求精，來達成下列目標：

- 滿足全國醫療院所需快速、正確、便利、穩定導入醫事憑證應用之需求。
- 滿足跨院所機構間資訊流通之需求。
- 協助醫療院所有效運用醫事憑證、TMT 電子病歷內容基本格式與政府機關推動之相關標準。

1.2 適用範圍

1.2.1 規範適用子領域範圍

本指引之主要適用範圍為：醫療電子化文件之醫事憑證應用指引。

1.2.2 適用對象範圍

本規範書的使用對象主要有下列三類：

- 要建置醫事憑證應用系統的醫療院所或機構。
- 要提供醫療電子化文件作跨機構資料交換的醫療院所或機構。
- 提供醫療院所醫事憑證應用系統整合服務及中介軟體服務的資訊服務廠商。

2. 醫療憑證管理中心

2.1 醫療憑證管理中心的設置

行政院衛生署為加強醫療資訊安全及隱私權的保障，並促進醫療資訊電子化應用，採用以「公開金鑰系統」(Public Key System)為基礎之醫療資訊電子認證機制，並設置及營運「醫療憑證管理中心」(Healthcare Certification Authority, 簡稱 HCA)。

2.2 醫療憑證管理中心的角色及功能

「醫療憑證管理中心」負責憑證之簽發與管理作業，為目前醫療憑證信任之「最上層 CA」，其簽發之憑證有醫事人員憑證、醫事機構憑證、醫事機構副卡憑證及醫療資訊相關之伺服器應用軟體憑證（以下簡稱「伺服器應用軟體憑證」)。

3. 醫事憑證

目前國內用以証明在網路上具備醫事人員資格及醫事機構資格的身分,政府可以依據這個醫事憑證來確認身分及資格，提供網路上方便的服務及確保資料傳輸的安全。

3.1 醫事憑證的種類(原 2.3.2 及 2.1)

憑證的種類可依據憑證實體用戶來區分，分類如下：

項次	憑証實體用戶	憑證總類
1.	合於本署規定、登錄有案之醫事人員	醫事人員憑證
2.	醫事機構	醫事機構憑證
3.	醫療資訊相關之伺服器應用軟體	伺服器應用軟體憑證

第 3 項伺服器應用軟體憑証的憑證實體用戶非為法律上之行為人,故申請方式為該軟體所屬之單位(醫事機構)出具公文，並以管理人之名義提出申請，其所有因此憑證所產生之法律權責則由此管理人承擔。

3.2 醫事憑證的效期及儲存媒體、規格(原 1.2, 2.1, 2.3.5, 3.3.3，加伺服器應用軟體)

醫事憑證有效期限為憑證產生之日期起算，為期 5 年，且期滿後需重新申請新憑證。

醫事憑證的儲存媒體為醫事憑證 IC 卡，主要提供電子簽章功能、加解密功能及儲存憑證功能，其晶片主要規格如下：

- 具密碼運算模組之 32K Java Card。
- 可以處理 1024 bits RSA 非對稱加解密。
- 可運算 10 萬次以上。

醫事憑證 IC 卡共有兩種類型，說明如下：

1. 醫事人員憑證 IC 卡，其儲存內容如下：
   - HPC Applet。
   - HCA Applet。
   - 金鑰對一組。

2. 醫事機構憑證 IC 卡，其儲存內容如下：

- HPC Applet。
- HCA Applet。
- 金鑰對兩組(支援加密功能)

3.3 收費依據

依據行政院衛生署公告之「醫事憑證收費標準」。

3.4 醫事憑證的內容

憑證內容含有憑證格式版本、憑證序號、憑證簽署採用演算法、發證單位名稱、憑證效期、憑證用戶名稱、憑證對應之公鑰、憑證擴充欄位、HCA 簽署憑證之簽章內容。

3.5 醫事憑證的核發作業

3.5.1 憑證申請

憑證申請須臨櫃辦理,醫院可由專人負責或醫事人員本身備妥相關文件至各縣市衛生局「註冊服務窗口(RAO)」辦理憑證申請，其相關申請文件可由「醫療憑證管理中心」HCA 專屬網站(http://hca.doh.gov.tw)上下載。

3.5.2 憑證領取

醫事憑證 IC 製作完成後,「醫療憑證管理中心」將以掛號方式郵寄憑證用戶。

3.5.3 憑證使用

3. 醫事機構憑證 IC 卡，代表醫事機構法人於醫療資訊電子化環境之法人行為—機構關防。可應用於加密、簽章：如電子公文、網路出生通報系統等。
4. 醫事人員憑證 IC 卡，代表醫事人員於醫療資訊電子化環境之個人行為—印鑑證明，可應用於權限控管：健保第二階段存放內容讀取權限憑證(限醫師卡)、簽章：如電子病歷。

3.6 醫事憑證的更換及廢止

醫事憑證的更換或廢止，應依照 CPS 5.2 節規定辦理，如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，須立即通知 HCA 辦理廢止，其相關申請文件可由「醫療憑證管理中心」HCA 專屬網站(http://hca.doh.gov.tw)上下載。

4. 醫事憑證的應用

4.1 用詞定義如下

4.1.1 電子簽章

「電子簽章」是指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分，資格及電子文件真偽者。電子簽章可達到電子環境中「鑑別雙方身份」及「不可否認性」之安全要件。

4.1.2 驗章

「驗章」是指對「電子簽章」進行鑑別，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。驗章可達到電子環境中「鑑別身份」及「不可否認性」之安全要件。

4.1.3 時戳

電子時戳可以為任何電子文件或網上交易提供準確的時間證明，並且驗出文件或交易的內容自蓋上時戳後是否曾被人修改過。

4.2 簽章及驗章時機

簽章時機之基本原則為當資料產製完成時立刻進行電子簽章，若產製完成之時點進行電子簽章有困難性，則可考慮順延至資料下一儲存之時點，然需考量產製完成至資料下一儲存之間隔時間是否太長。

驗章時機之基本原則為當調閱簽署過之資料時皆應進行驗章程序，並顯示驗章結果供使用者瞭解。若醫事憑證應用機構應對驗章有其基本之政策，則簽署憑證有效性之認定可考量視應用之不同而有所調整。

4.3 時戳應用與限制

醫事憑證管理中心之電子時戳可以為醫療應用的電子文件或網路交易提供準確的時間證明，並可於事後加以檢驗與認證，實務上當電子簽章產生簽體後，需使用醫事憑證管理中心電子時戳服務，透過網際網路送出簽體取得電子時戳。

應用系統可檢核電子簽章簽體與電子時戳是否符合，電子時戳可確保此時戳與電子簽章簽體之唯一關聯性。

醫事憑證管理中心電子時戳服務產生之時戳可以解譯出下列資訊。

- Policy ID。
- 蓋時戳資料之數位指紋。
- 時戳序號。
- 時戳時間。

電子病歷管理及製作辦法規定應用系統製作電子病歷必須向醫事憑證管理中心電子時戳服務取得電子時戳。醫療院所在考量向醫事憑證管理中心電子時戳服務，取得電子時戳需對網路離線與網路效率先進行評估，以免影響現行應用系統作業。

4.4 簽體儲存

4.4.1 格式標準

簽體之儲存格式可採 128 bytes 之原始簽體或採 PKCS#7 國際標準儲存，原始簽體之優點為檔案小，PKCS#7 國際標準之優點為內含簽署憑證做嚴謹驗章不需另外儲存簽署憑證。

4.4.2 內嵌式與外存式

簽體之儲存位置可放置於簽署過的資料之中(如 TMT，DICOM)、或另外存檔。其差別在於內嵌式需要注意取出簽體時，不可影響簽署資料 byte 數。

4.5 醫療資訊相關數位憑證應用

4.5.1 數位憑證應用系統

數位憑證應用系統為可受理申請、發行、證明一電子憑證的應用系統。此系統可產生、辨識數位憑證的內容、資料、效期及使用範圍，在電子化環境(網路)下辨識憑證所代表之人、物的身分，而憑證持有者可信任此系統及遵循相關之使用規定。數位憑證產生時，申請人須提供所需之資料寫入數位憑證內，例如申請人姓名等。

此系統可明確辨識數位憑證內容及使用內容的應用系統，其中須包含：

- 系統管理方式符合醫事憑證管理中心之安全規範及要求。
- 系統可自行產生金鑰對，並經過醫事憑證管理中心簽署。
- 數位憑證的使用，具有效之法律效力。

4.5.2 數位憑證應用系統建立模式

依照符合醫事憑證管理中心之規範產生數位憑證，備有相關安全機制之管理，例如申請使用對象、使用效期及安全的儲存管理方式。

5. 電子病歷基本格式的遵循

此章節將針對醫事憑證應用實務進行說明。

5.1 醫事憑證整合議題

醫療院所在應用醫事憑證時，建議先考量下列議題。

5.5.1 簽章速度

簽章的速度是目前醫事憑證 IC 卡一個重要的議題，一般簽章時間約需 2 秒鐘，若簽章速度對醫事憑證應用極為重要時,建議可考慮向醫事憑證管理中心申請伺服器應用軟體憑證來進行簽章。

5.5.2 簽體存放方式

簽體之儲存位置可放置於簽署過的資料之中(如 TMT，DICOM)、或另外存檔。其差別在於內嵌式需要注意取出簽體時，不可影響簽署資料 byte 數。

5.5.3 簽章時機

簽章時機之基本原則為當資料產製完成時立刻進行電子簽章,若產製完成之時點進行電子簽章有困難性,則可考慮順延至資料下一儲存之時點，然需考量產製完成至資料下一儲存之間隔時間是否太長。

5.2 DICOM

應用醫事憑證簽署 DICOM 檔案時，建議先考量下列議題：

- 簽章速度，建議可考慮向醫事憑證管理中心申請伺服器應用軟體憑證來進行簽章，但電子病歷需使用醫事人員 IC 卡簽署才合法。
- 是否會儲存多份簽章在一份 DICOM 之中，若需則要注意驗章次序。

5.3 臺灣電子病歷基本格式 TMT

應用醫事憑證簽署臺灣電子病歷基本格式 TMT 檔案時，建議先考量下列議題：

- 臺灣電子病歷基本格式尚未定義醫事機構簽體的儲存模組，須另存檔案保存之並保留其關連性。
- 臺灣電子病歷基本格式 TMT 以 XML 檔案為單位,儲存方式可採每次修正都存一版本，或採只保留最後版本，不論合種方式儲存，每次補正皆須重新以醫事人員 IC 卡簽章才合法。

6. 其他事項

6.1 相關法令問題

6.1.1 伺服器應用軟體憑證簽章應用適法性

行政院衛生署「醫療憑證管理中心」為中央主管機關於醫療領域建立電子認證及安全制度而設立之合法憑證管理中心，其簽發之憑證具有合法之效力，可代表申請機構之身分，應用於電子化政府的各項應用(如電子公文等)。

醫療機構電子文件以「應用伺服器應用軟體憑證」進行簽章仍未成為合法之電子病歷，依照「醫療機構實施電子病歷作業要點」第三條，電子病歷之製作方式為『應經由行政院衛生署醫療憑證管理中心簽發憑證之醫事人員卡或醫事機構卡製作』;「醫療法」新修訂『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』; 以及「醫療機構電子病歷製作及管理辦法」，第五條，『電子病歷之簽章，應憑中央主管機關核發之醫事憑證為之，並經中央主管機關加註時戳』等規定，醫療機構電子文件需加上製作人之醫事人員憑證簽章並經中央主管機關加註時戳,始為合法之電子病歷。

6.2 常見問題處理

6.2.1 遺失 IC 卡

遺失 IC 卡時，需至各縣市衛生局「註冊服務窗口(RAO)」申請憑証廢止，並重新申請新憑證。

6.2.2 忘記 PIN 碼

忘記 PIN 碼時，可至各縣市衛生局「註冊服務窗口(RAO)」進行身份確認後，重新設定 PIN 碼，建議由醫院統一保管醫事人員 PIN 碼，應用程式提供設 PIN 碼與解鎖卡功能，做到即時進行處理。

6.2.3 鎖卡

鎖卡時，可透過「醫療憑證管理中心」HCA 專屬網站(http://hca.doh.gov.tw)上，憑證作業/醫事人員卡解鎖卡作業網頁中進行解鎖卡，或至各縣市衛生局「註冊服務窗口(RAO)」辦理解鎖卡作業，建議由醫院統一保管醫事人員 PIN 碼，應用程式提供設 PIN 碼與解鎖卡功能，做到即時進行處理。

6.2.4 卡片故障

卡片故障時，可將卡片郵寄回憑證管理中心(地址：台北市內湖區瑞光路 192 號 5 樓)進行卡片重製，或透過各縣市衛生局「註冊服務窗口(RAO)」處理。

6.2.5 憑證展期

「醫療憑證管理中心」自 CPS V1.1 修訂通過後起，所簽發之憑證效期調整為 5 年，但本修訂通過前所簽發之憑證效期（原為 2 年），為使一致，將於該效期屆滿後將其展期為三年(合計共 5 年)。此類憑證之憑證用戶應於憑證使用期限屆滿前二個月內，至各縣市衛生局「註冊服務窗口(RAO)」申請憑證展期。

6.2.6 其他問題處理

可透過客服專線(0800-364-422)尋求協助。

柒、示範原始碼

為加強醫院醫事憑證應用系統建置所需之技術示範與減少實際實施醫事憑證應用時遭遇之困難為目標，開發此示範程式，並以開放原始碼方式釋出，希望能落實醫事憑證應用發展之宣導，主要提供醫療院所三種院內應用醫事憑證的方式，讓醫療院所根據自身的規模、層級、作業流程需求、安全等級要求來選擇適用的導入方式。此開放原始碼方式的取得方式，可由台灣醫院協會網站「醫事憑證計畫專區」取得。

一、功能介紹

(一) 簽驗章模組

透過醫事人員卡，對單一檔案，進行簽章與驗章的功能。

(二) 時戳模組

將已簽章的檔，連線至 HCA 伺服器，取得時戳戳記。

(三) TMT 模組

先對 TMT 格式的 XML 進行簽章、取得時戳戳記，將簽章資料、時戳戳記與憑證一併寫成 TMT 格式，另儲存成一個 TMT 格式的 XML。

二、函式介紹

(一) 簽驗章模組

1. getFileData：將欲簽章的檔案內容讀入

   getFileData(ByRef bArr() As Byte, ByRef fLen As Integer)

   - 回傳值- Boolean 型態：True 表示讀檔成功，false 表示讀檔失敗
   - bArr -存放檔案的陣列
   - fLen -檔案長度

2. getSignData：將簽章檔讀入

   getSignData(ByRef signArr() As Byte)

   - 回傳值- Boolean 型態：True 表示讀檔成功，false 表示讀檔失敗
   - signArr-存放簽章檔的陣列

3. signData：簽章

   HCA_GNFuncCallEx2(HCA_F_SignMessage, bArr(0), signArr(0), fLen, 128,0,0,0)

   - 回傳值- long 型態：執行成功回傳值為 HCA_E_SUCCESS，否則是錯誤碼
   - bArr-欲簽章的檔案存放位址
   - signArr-簽章檔的存放位址
   - fLen-欲簽章檔案的儲放記憶體長度

4. verifySign：驗章

   HCA_GNFuncCallEx2(HCA_F_VerifySignMessage, bArr(0), signArr(0), fLen, 128, 0, 0, 0)

   - 回傳值- long 型態：執行成功回傳值為 HCA_E_SUCCESS，否則是錯誤碼
   - bArr-簽章的檔案存放位址
   - signArr-簽章檔的存放位址
   - fLen-欲簽章檔案的儲放記憶體長度

(二) 時戳模組

1. getTimeStamp：取得時戳

   getTimeStamp(ByRef signArrTSP() As Byte)

   - 回傳值-Boolean 型態：True 表示取時戳成功，false 表示取時戳失敗
   - signArrTSP -簽章檔存放位址

(三) TMT 模組

1. setXmlNodeValue：XML 存取設定

   setXmlNodeValue(ByRef strTMTFile As String, ByRef strXmlNodePath As String, ByRef strXmlNodeValue As String)

   - 回傳值- Boolean 型態：True 表示存取設定成功，false 表示存取設定失敗
   - strTMTFile-使用者選取 TMT 格式的 XML 檔存放位址
   - strXmlNodePath-欲存取 XML 的欄位
   - strXmlNodeValue-欲存取 XML 的值

2. writeTMT：寫入 TMT

   將指定的值寫入指定的欄位到 XML 內

3. getTimeStamp：取得時戳

   getTimeStamp()

   - 回傳值-string 型態：表示得到的時戳戳記，以 Base64 格式輸出

4. getSignData：簽章

   getSignData()

   - 回傳值-string 型態：表示得到的簽章值，以 Base64 格式輸出

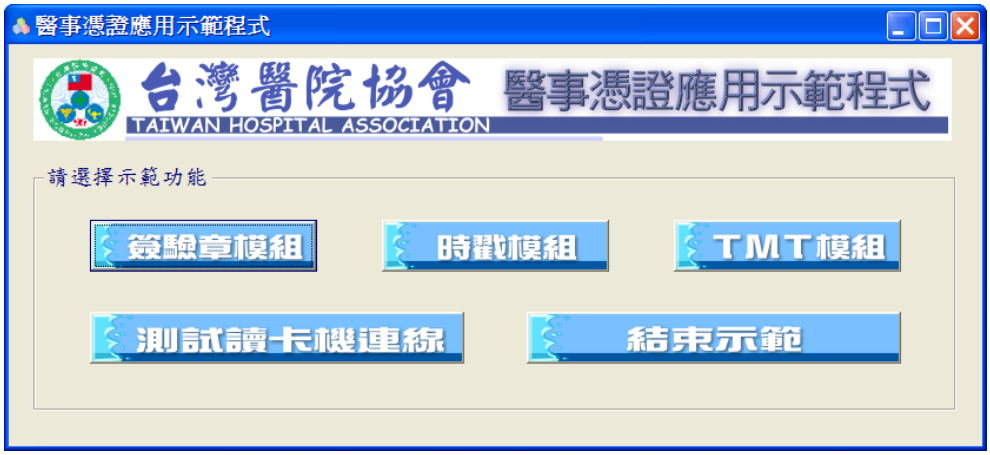
5. getUserCert：取公開鑰匙

   getUserCert()

   - 回傳值-string 型態：表示得到的公開鑰匙，以 Base64 格式輸出

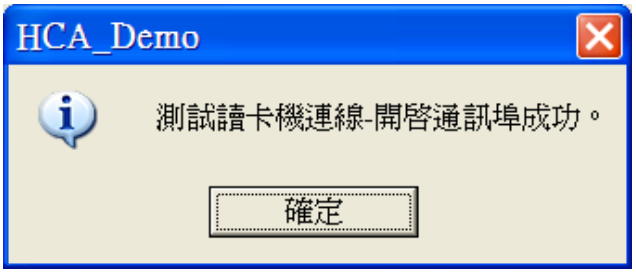
三、使用說明

(一) 程式主畫面

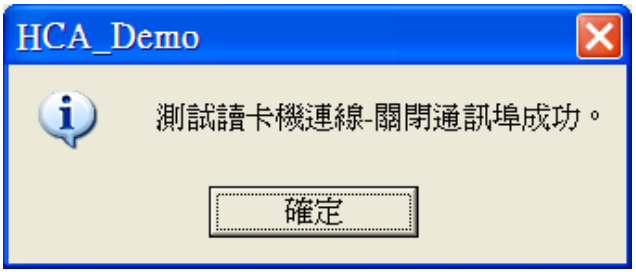


(二) 測試讀卡機連線

1. 開啟通訊埠成功

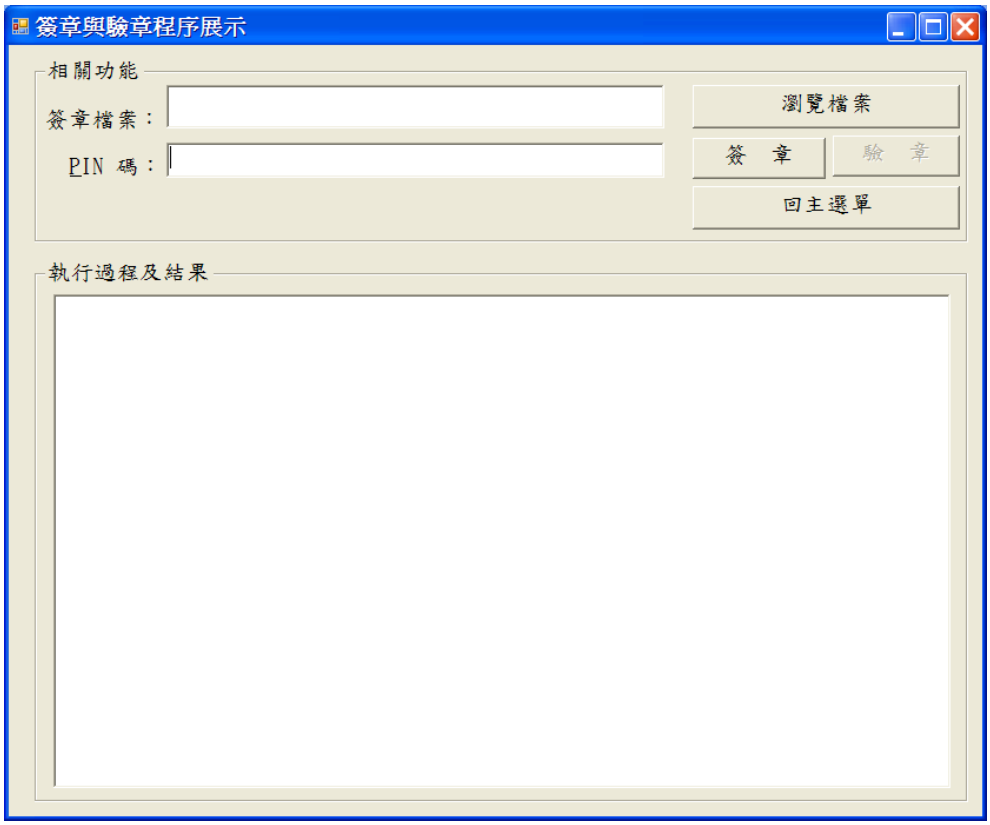


2. 關閉通訊埠成功

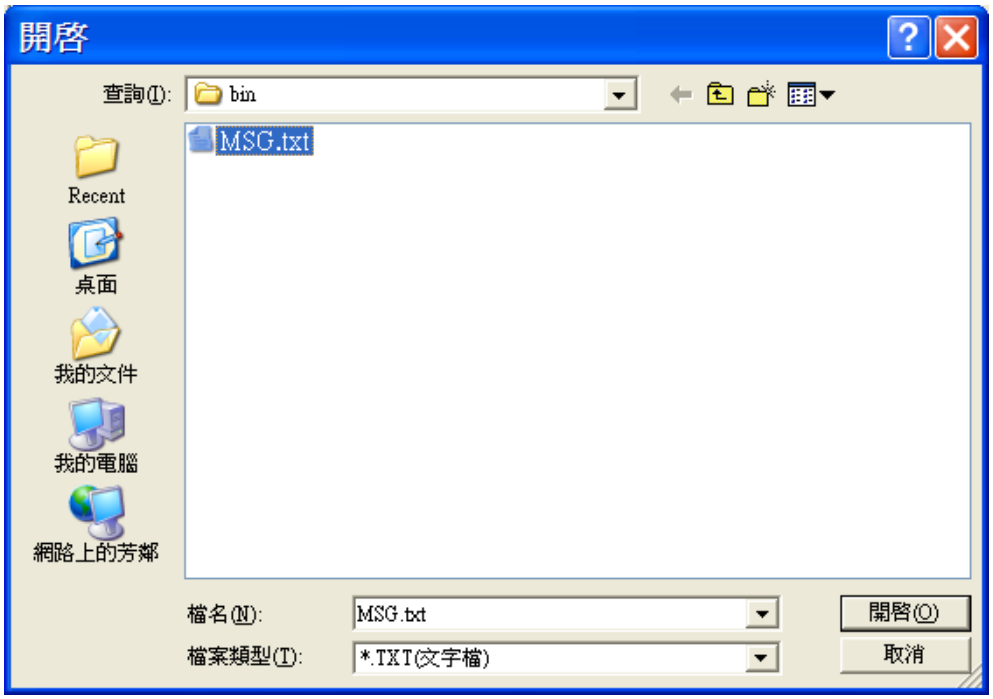


(三) 簽驗章模組

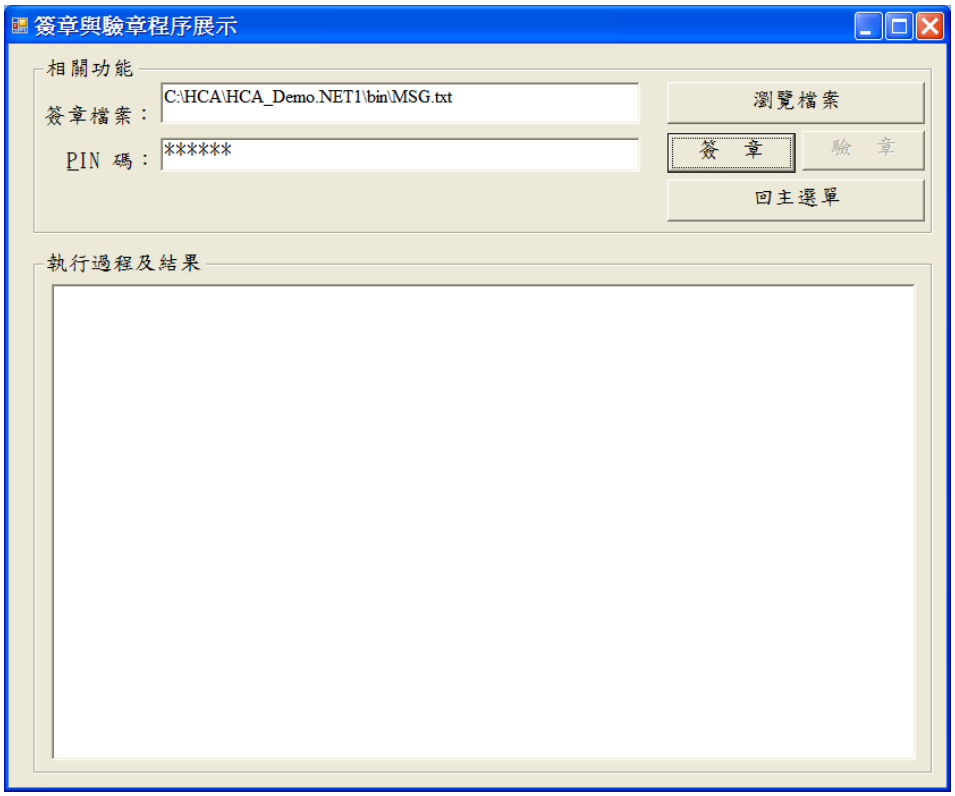
1. 主畫面



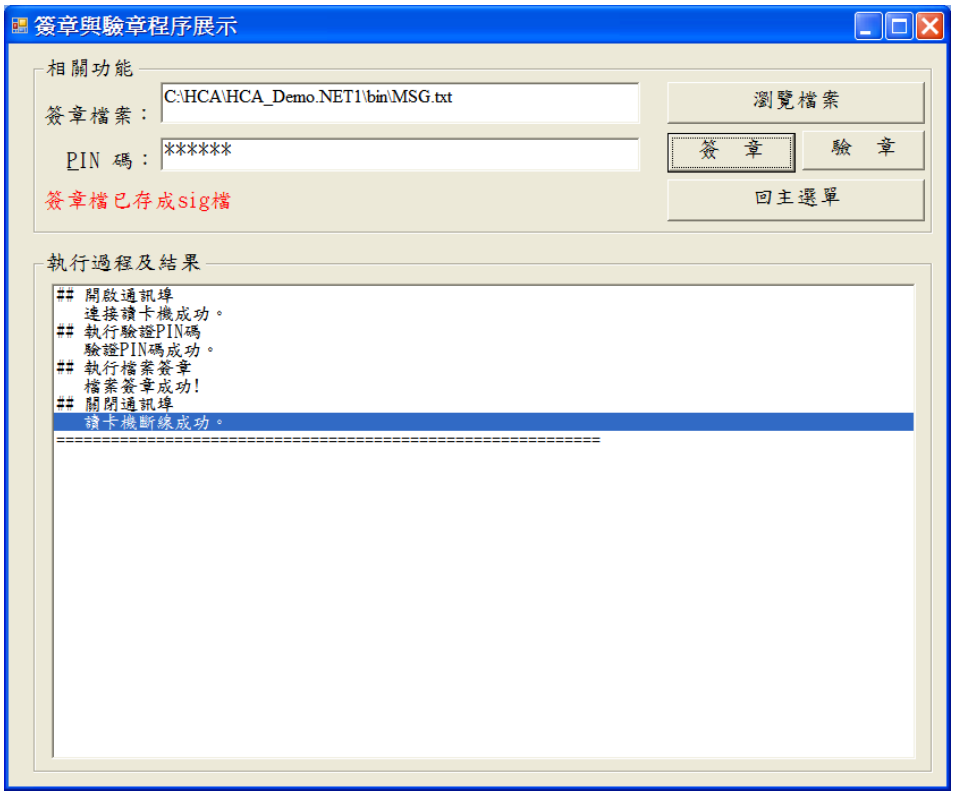
2. 瀏覽檔案



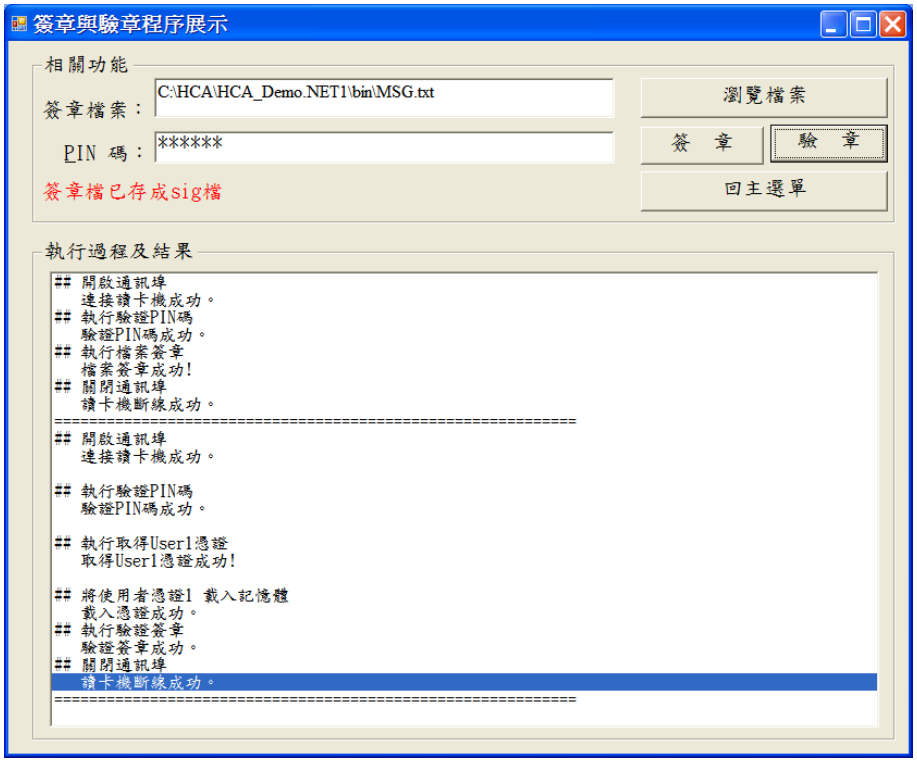
3. 輸入 PIN 碼


簽章與驗章程序展示
相關功能
簽章檔案：
C:\HCA\HCA_Demo.NET1\bin\MSG.txt
PIN 碼：
******
瀏覽檔案
簽 章
驗 章
回主選單
執行過程及結果

4. 簽章

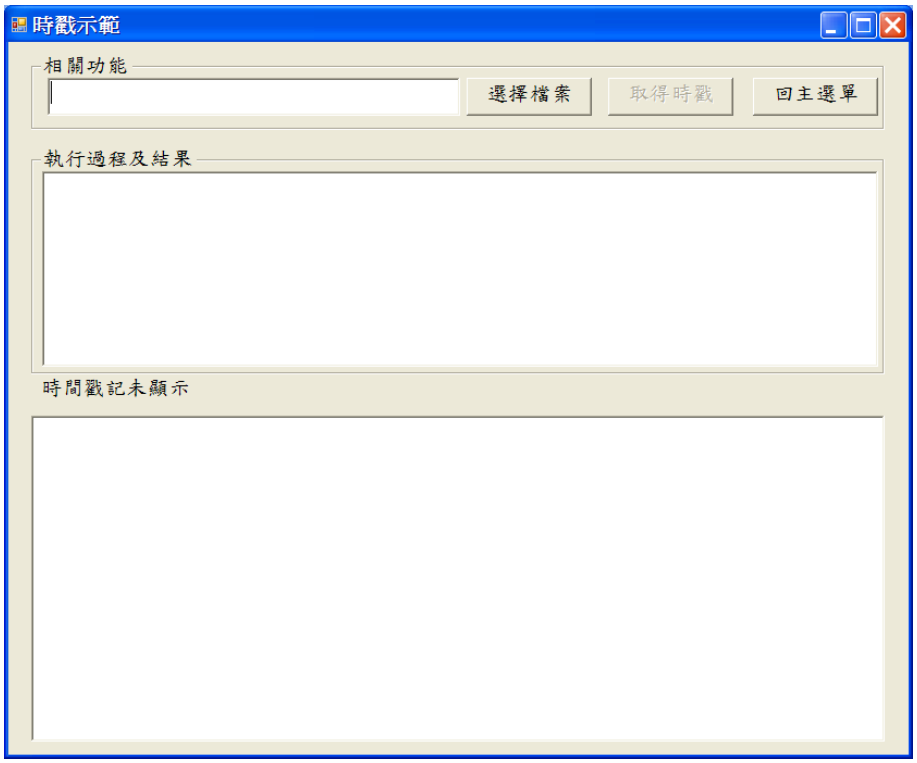

簽章與驗章程序展示
相關功能
簽章檔案：
C:\HCA\HCA_Demo.NET1\bin\MSG.txt
PIN 碼：
******
瀏覽檔案
簽 章
驗 章
回主選單
簽章檔已存成sig檔
執行過程及結果
開啟通訊埠
連接讀卡機成功。
執行驗證PIN碼
驗證PIN碼成功。
執行檔案簽章
檔案簽章成功!
關閉通訊埠
讀卡機斷線成功。

5. 驗章

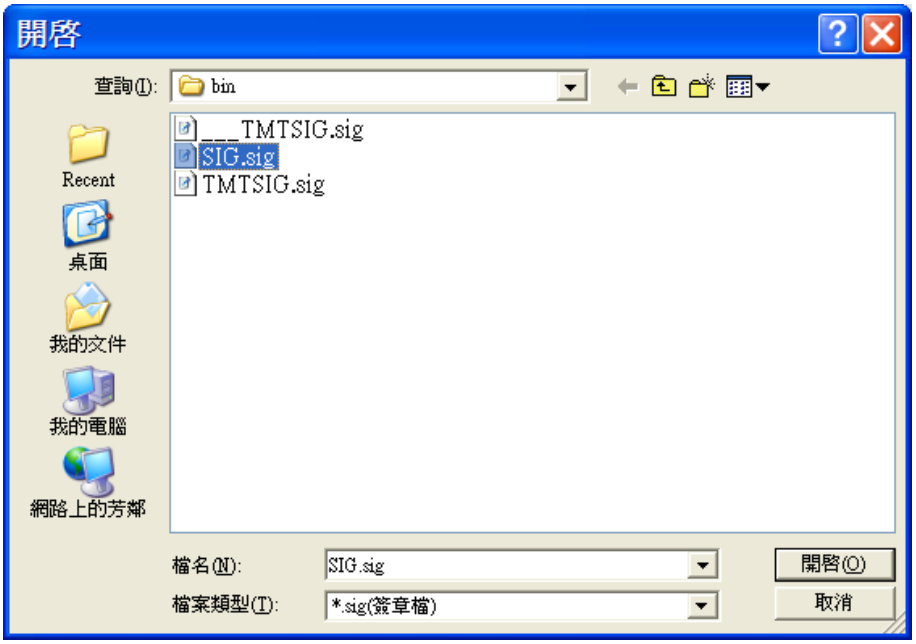


(四) 時戳模組

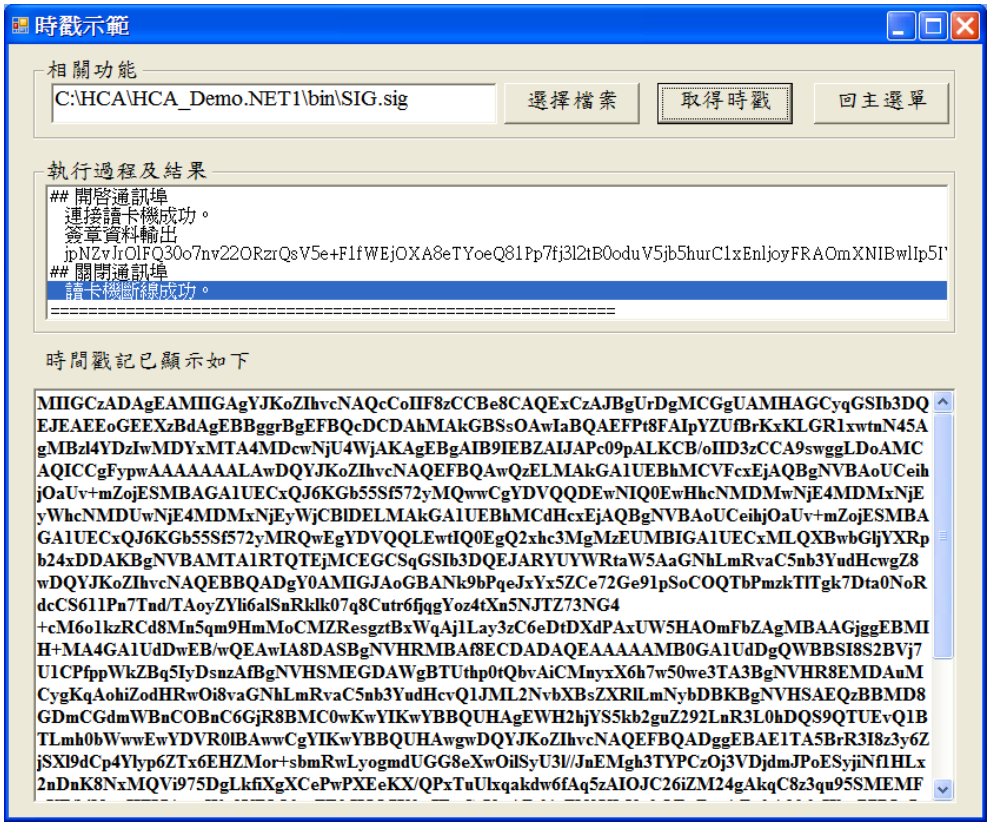
1. 主畫面



2. 選擇檔案

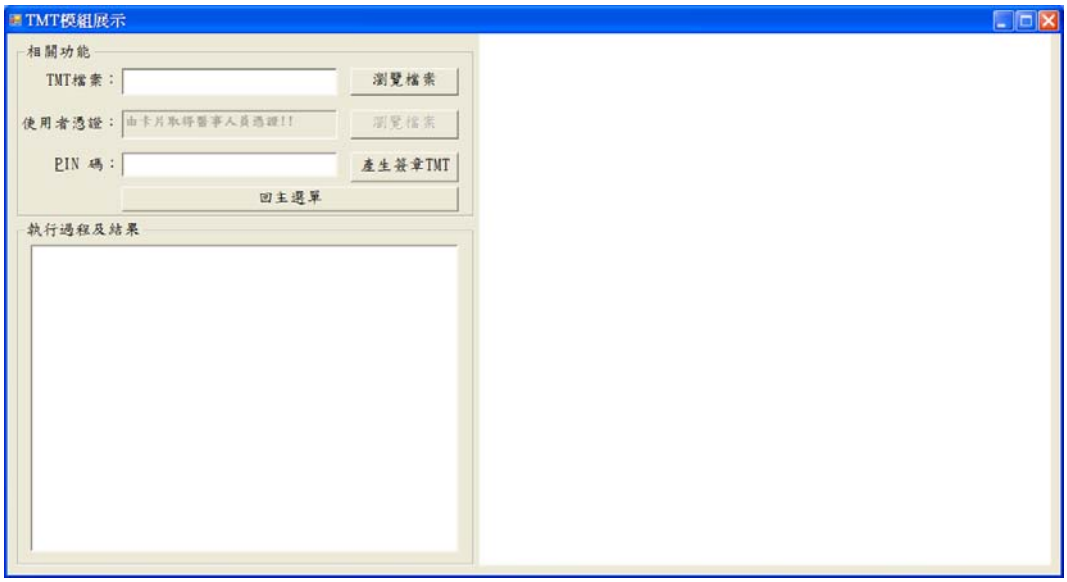

開啓
查詢(I):
bin
___TMTSIG.sig
SIG.sig
TMTSIG.sig
Recent
桌面
我的文件
我的電腦
網路上的芳鄰
檔名(N):
SIG.sig
開啓(O)
檔案類型(T):
*.sig(簽章檔)
取消

3. 取得時戳

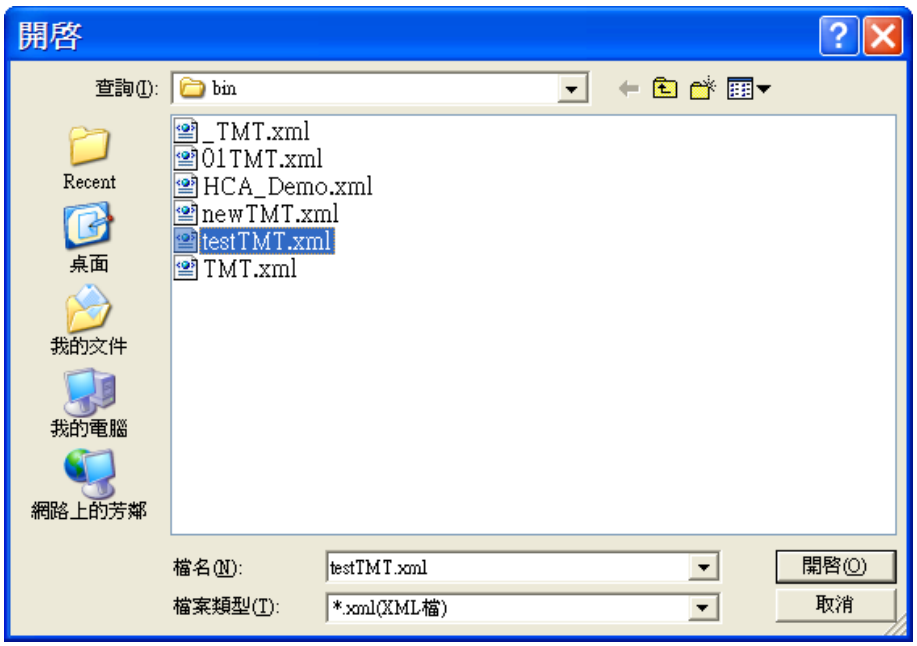

時戳示範
相關功能
C:\HCA\HCA_Demo.NET1\bin\SIG.sig
選擇檔案
取得時戳
回主選單
執行過程及結果
開啓通訊埠
連接讀卡機成功。
簽章資料輸出
jpNZvJrOlFQ30o7nv22ORzrQsV5e+F1fWEjOXA8eTYoeQ81Pp7fj3l2tB0oduV5jb5hurC1xEnljoyFRAOmXNIBwlIp5I'
關閉通訊埠
讀卡機斷線成功。
時間戳記已顯示如下
MIIGCzADAgEAMIIGAgYJKoZIhvcNAQcCoIIF8zCCBe8CAQExCzAJBgUrDgMCGgUAMHAGCyqGSIb3DQ
EJEAEEoGEEXzBdAgEBBggrBgEFBQcDCDAhMAkGBSsOAwIaBQAEFPt8FAIpYZUfBrKxKLGR1xwtnN45A
gMBzl4YDzIwMDYxMTA4MDcwNjU4WjAKAgEBgAIB9IEBZAIJAPc09pALKCB/oIID3zCCA9swggLDoAMC
AQICCgFypwAAAAAALAwDQYJKoZIhvcNAQEFBQAwQzELMAkGA1UEBhMCVFcxEjAQBgNVBAoUCeih
jOaUv+mZojESMBAGA1UECxQJ6KGb55Sf572yMQwwCgYDVQQDEwNIQ0EwHhcNMDMwNjE4MDMxNjE
yWhcNMDUwNjE4MDMxNjEyWjCBlDELMAkGA1UEBhMCdHcxEjAQBgNVBAoUCeihjOaUv+mZojESMBA
GA1UECxQJ6KGb55Sf572yMRQwEgYDVQQLEwtIQ0EgQ2xhc3MgMzEUMBIGA1UECxMLQXBwbGljYXRp
b24xDDAKBgNVBAMTA1RTQTEjMCEGCSqGSIb3DQEJARYUYWRtaW5AaGNhLmRvaC5nb3YudHcwgZ8
wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANk9bPqeJxYx5ZCe72Ge91pSoCOQTbPmzkTlTgk7Dta0NoR
dcCS611Pn7Tnd/TAoyZYli6alSnRklk07q8Cutr6fjqgYoz4tXn5NJTZ73NG4
+cM6o1kzRCd8Mn5qm9HmMoCMZResgztBxWqAj1Lay3zC6eDtDXdPAxUW5HAOmFbZAgMBAAGjggEBMI
H+MA4GA1UdDwEB/wQEAwIA8DASBgNVHRMBAf8ECDADAQEAAAAAMB0GA1UdDgQWBBSI8S2BVj7
U1CPfppWkZBq5IyDsnzAfBgNVHSMEGDAWgBTUthp0tQbvAiCMnyxX6h7w50we3TA3BgNVHR8EMDAuM
CygKqAohiZodHRwOi8vaGNhLmRvaC5nb3YudHcvQ1JML2NvbXBsZXRlLmNybDBKBgNVHSAEQzBBMD8
GDmCGdmWBnCOBnC6GjR8BMC0wKwYIKwYBBQUHAgEWH2hjYS5kb2guZ292LnR3L0hDQS9QTUEvQ1B
TLmh0bWwwEwYDVR0lBAwwCgYIKwYBBQUHAwgwDQYJKoZIhvcNAQEFBQADggEBAE1TA5BrR3I8z3y6Z
jSXl9dCp4Ylyp6ZTx6EHZMor+sbmRwLyogmdUGG8eXwOilSyU3l//JnEMgh3TYPCzOj3VDjdmJPoESyjiNf1HLx
2nDnK8NxMQVi975DgLkfiXgXCePwPXEeKX/QPxTuUlxqakdw6fAq5zAIOJC26iZM24gAkqC8z3qu95SMEMF

(五) TMT 模組

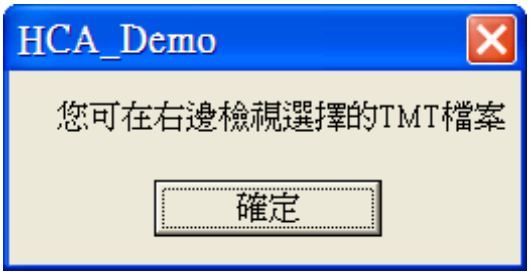
1. 主畫面



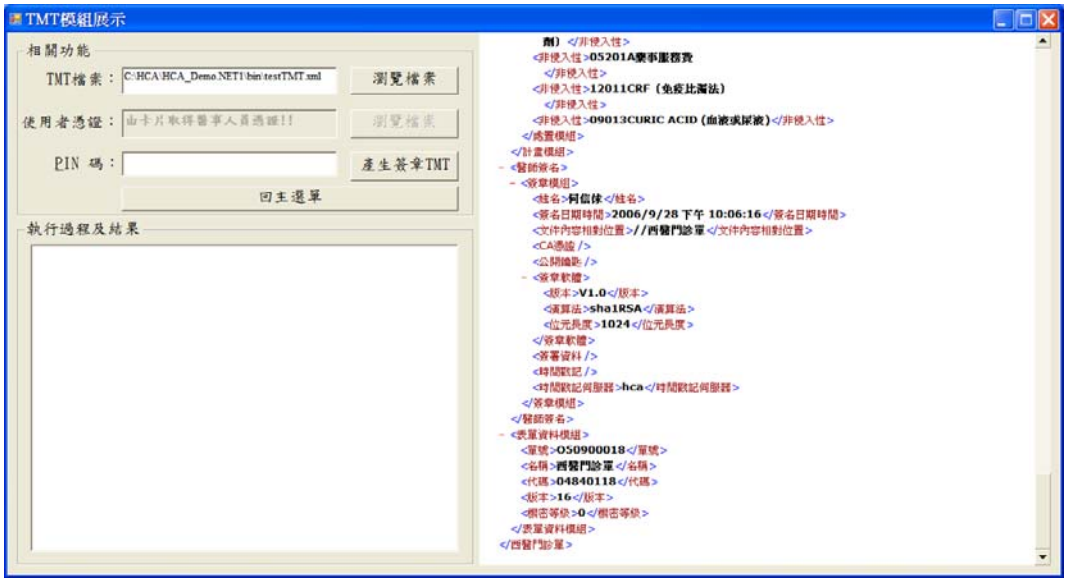
2. 瀏覽檔案



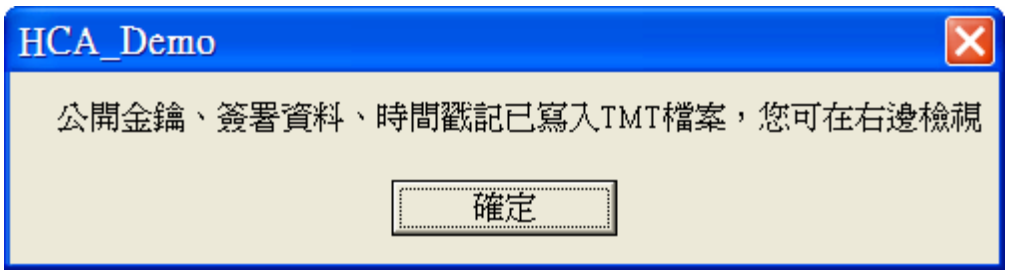
3. 提醒訊息



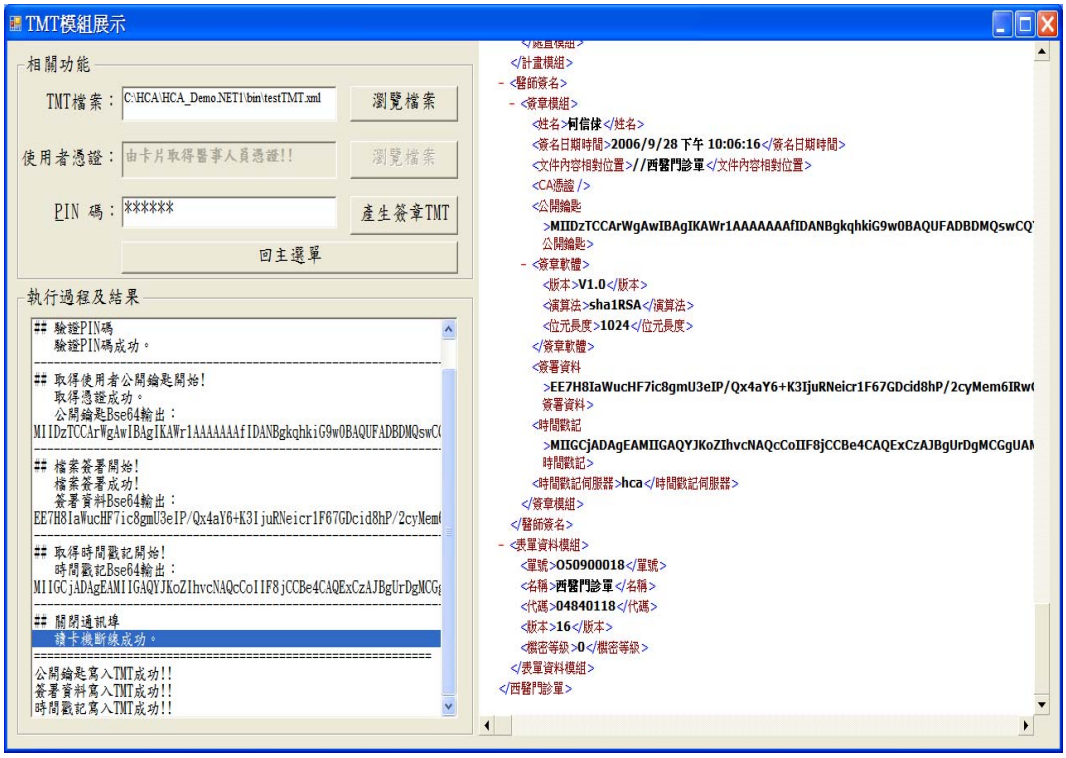
4. 檢視 TMT 檔



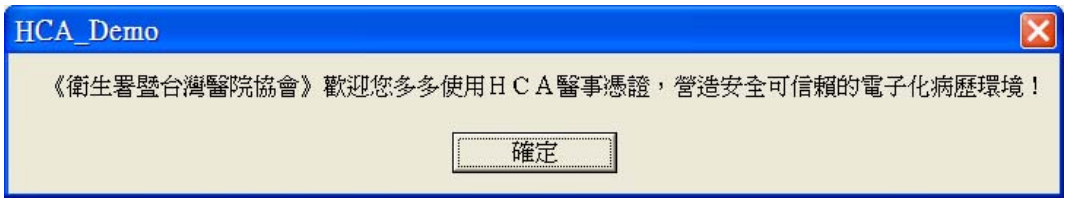
5. 輸入 PIN 碼，產生簽章 TMT



6. 檢視新的 TMT 檔，可看到公開金耀、簽署資料、時戳戳記已寫入



(六)結束-感謝畫面



四、錯誤碼列表

錯 誤 名 稱	代 碼	說 明
HCA_E_SUCCESS	0	成功
HCA_E_UNSUPPORT_FUNC	30001	該函式尚未支援
HCA_E_UNSUPPORT_HPC_PRIVATE_DECRYPT	30002	未支援醫事人員卡私鑰解密
HCA_E_INVALID_COM_HANDLE	30003	不合法的 COM port Handle
HCA_E_INVALID_FUNC_ID	30004	不合法的函式識別碼
HCA_E_INVALID_PARAMETER	30005	不合法的參數
HCA_E_LICENSE_IS_EXPIRE	30006	權限已過期
HCA_E_PIN_IS_NOT_VERIFICATION	30007	卡片 PIN 碼未驗證
HCA_E_FAIL_TO_GET_UUID	30010	取卡片 UUID 碼失敗
HCA_E_NOT_RUN	30011	未執行動作
HCA_E_FAIL_TO_LOGIN_HPC	30012	登入卡片失敗
HCA_E_FAIL_TO_GET_CARD_TYPE	30013	取卡別失敗
HCA_E_FAIL_TO_GET_CARD_SN	30014	取卡片序號(卡號)失敗
HCA_E_FAIL_TO_GET_PRIVATE_KEY	30015	取卡片金鑰失敗
HCA_E_FAIL_TO_GET_PUBLIC_KEY	30016	取卡片公鑰失敗
HCA_E_FAIL_TO_GET_BASIC_DATA	30017	取卡片基本資料失敗
HCA_E_FAIL_TO_GET_CARD_INFO	30018	取卡片資訊失敗
HCA_E_FAIL_TO_GET_CERT	30019	自卡片取憑證失敗
HCA_E_FAIL_TO_SIGN_MESSAGE	30020	簽章失敗
HCA_E_FAIL_TO_VERIFY_SIGNMESSAGE	30021	驗章失敗
HCA_E_FAIL_TO_VERIFY_PIN	30022	驗卡片 PIN 碼失敗
HCA_E_FAIL_TO_HASH_MESSAGE	30023	hash 動作失敗
HCA_E_FAIL_TO_PUBLIC_ENTRYPT	30024	公鑰加密失敗
HCA_E_FAIL_TO_PRIVATE_DECRYPT	30025	金鑰解密失敗
HCA_E_FAIL_TO_RESET_APPLET	30026	重設 HPC 卡片狀態失敗
HCA_E_FAIL_TO_SET_PIN	30027	重設卡片 PIN 碼失敗
HCA_E_FAIL_TO_LOAD_CERT	30028	載入憑證至記憶體失敗
HCA_E_FAIL_TO_TS_Query	30029	TS Query 失敗
HCA_E_FAIL_TO_TS_Verify	30030	TS Verify 失敗

錯 誤 名 稱	代 碼	說 明
HCA_E_FAIL_TO_Find_Reader	30031	AppAPI 1.72 initial 失敗，請安裝讀卡機
HCA_E_FAIL_TO_Init_Function	30032	AppAPI 1.72 initial 失敗，請正確安裝讀卡機並插入醫事憑證之卡片
HCA_E_FAIL_TO_GetCertAttrib	30033	Get Cert Attrib 失敗
HCA_E_FAIL_TO_GetTSInfo	30034	取得 TS Info 失敗
HCA_E_FAIL_TO_GetHash	30035	取得 Hash 失敗
HCA_E_FAIL_TO_CertValidate	30036	憑證驗證失敗
HCA_E_FAIL_TO_CheckCard	30037	檢查卡片是否插入