

共同的電子簽章

Mutual Electronic Signatures

吳志成

Chih-cheng Wu

財團法人佛教慈濟綜合醫院
資訊室

chihcheng@tzuchi.com.tw

蔡欣晏

Shin-Yann Tsai

慈濟技術學院
護理系

yann@tccn.edu.tw

摘要

近幾年來，如何將醫療資訊系統導入電子簽章使其成為真正擁有合法地位、可以取代病歷紙本的電子病歷，一直都是醫療資訊領域的熱門話題。它帶來極大的經濟效益，舉凡大幅降低醫院管理紙本病歷的成本及其貯存的空間、並且是未來院際間線上即時資料交換的基礎，可以免去病人重覆作檢查的痛苦，節省大量的醫療資源、對於搶救生命及地球的環保都大有助益[2]。

以現在的資訊技術而言要將醫療資訊系統導入電子簽章並沒有窒礙難行之處，反倒是因為醫療資訊系統要導入電子簽章，醫院內部的作業流程需要重新討論及訂定才是比較棘手的工作。

然而，當兩位以上的醫師聯合看診，他們「共同的電子簽章」該如何產生，是一個值得探討的議題，同樣的「共同的電子簽章」的機制也適用在商業契約的訂定上。

「共同的電子簽章」代表兩造以上的雙（多）方對同一份文件或契約有著共同的共識及承諾。

Abstract

It has been increasingly discussed that how to enable electronic signatures to carry legal weight in place of written signatures in recent years. The practice of electronic signatures has

demonstrated its advantages, such as cost savings on the management of consumption of paper and the storage space. Furthermore, it provides the data interchange links among medical units so they can share the necessary medical records for the interests of the patients. By employing the electronic signatures, it surely will be a great benefit to medical resources and the highly concerned environmental problems.

With current modern information technology, the main tasks should not focus on the employment of the electronic signatures, but on the re-arrangement of operation processes inside the hospitals instead.

However, when joint-clinic occurs, how to generate a “mutual electronic signatures” is an issue. The “mutual electronic signatures” also can be used for the establishment of commercial contracts.

The “mutual electronic signatures” represents the consensuses and commitments towards a document/contract among parties.

研究動機

在衛生署所有電子簽章的規範中，對於多科醫師聯合看診的行為並沒有任何的規定及描述，在醫療院所要將資訊系統導入電子簽章的過程中這是一塊還沒有解答的空白區域，屆時

也會讓導入電子簽章的醫療院所無所適從。環顧現今群體簽章的研究，並無法有效解決此一問題，因為要使用群體簽章的機制，兩造以上的雙（多）方必須先行加入該群體，群體中的成員與成員間，才能使用、啟動群體簽章的機制[4]。對要舉行聯合看診的醫師們來說會有時間上的延宕、及程序上的困擾。

研究目的

我們希望能設計一個簡易的機制及架構，使得任意的雙(多)方要簽署「共同的電子簽章」，在任何時間、任何地點都是可行的，並且沒有時間上的延宕、及複雜的程序，而且也必須能防止有任一方有企圖隱瞞、欺騙另一方的意圖。事後任意持有該簽署文件的第三者，都可以對該文件所有的簽署者進行驗證以確定他們的 Authentication。以期能有效、安全的保障所有簽署者及病患的權益。

同時此一「共同的電子簽章」的機制也適用在商業契約的訂定上

相關文獻

「數位簽章」(Digital Signature) 為目前所有電子簽章技術中發展最快速且最為成熟的一種。數位簽章的定義為：「將電子文件以數學演算法或其他方式運算為一定長度之數位資料，再以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者」。換言之，數位簽章技術是將任何長度之文件先利用數學函數或其他方式計算成固定長度的摘要值後，簽署人以其私密金鑰對運算出之摘要值進行「加密」製成簽體（數位簽字）[3]。

所謂「加密」係指：「利用數位演算或其他方法將電子文件以亂碼處理」，使該數位簽字類似於實體世界中之「簽名或蓋章」，惟其不同於實體簽名或蓋章之處，在於實體簽名蓋章多能呈現大致相同式樣，但以同一私密金鑰對不同的文件簽署時，所得出的乃為不同之簽體[3]。

數位簽章中的金鑰對，即公開金鑰及私密金

鑰，為具配對關係之數位資料，其中由簽署人保有者稱之為私密金鑰 (Private Key)，供簽署人作為「製作」數位簽章之用；公開金鑰 (Public Key) 顧名思義其係對外公開，交由驗證者作為「驗證」數位簽章之用。具配對關係之公開金鑰及私密金鑰間，具有唯一的對應性，因而只有與之配對的公開金鑰能夠解開經由該私密金鑰加密之文件，並呈現其原文。另外，配對之數位資料（金鑰對）雖具有唯一的對應性，但持有具配對關係之金鑰對中公開金鑰者，並不能夠推算出與之配對之私密金鑰，反之亦同。

雜湊(赫序)函數 (hash function) 的作用是，對任意長度的明文，經由赫序函數的運算，可產生固定長度的赫序值，長度通常在 128 至 256 bit 之間，是一個巨大的數字，這數字有時亦稱為訊息摘要，赫序函數值可以說是對明文的一種「指紋」 (Fingerprint) 或是「摘要」 (Digest)。所以對赫序函數值的數位簽名，就可以視為對此明文的數位簽名，可以提高簽名的效率[1]。

赫序函數必須滿足以下的幾個要素：

- 1.能夠應用在任意大小的明文檔案。
- 2.可以產生固定長度的赫序值。
- 3.可以經由硬體或軟體的機制，容易的達成。
- 4.對於任一個 Hash value h ，要找到一個值 x ，使得 $H(x)=h$ ，在計算上是不可能的，這是 Hash function 的 One-way 特性。
- 5.對任何的值 x ，不可能找到，一個 $y \neq x$ ，但 $H(x)=H(y)$ 。

目前的應用上，有三個比較重要的 Hash functions 為：MD5(Message Digest 5)，SHA-1(Secure Hash Algorithm-1)，and RIPEMD-160，輸出分別為 128-bit，160-bit，160-bit[1][6]。

公開金鑰基礎建設 (PKI, Public Key Infrastructure)為非對稱密碼系統的應用，一組金鑰對包含，公開金鑰及私密金鑰，公開金鑰

可廣為散佈，私密金鑰為擁有者唯一擁有，成對的公開金鑰及私密金鑰具有互相可作加解密的關係，但並沒有取代彼此的功能。PKI 電子認證機制必須達成以下四項重要的安全保障[5]

1. 來源鑑別(Authentication) — 確認資料的來源。
2. 資料的完整性(Integrity) — 防止他人竄改資料內容。
3. 不可否認性(Non-repudiation) — 資料發送方無法否認曾經發送資料。
4. 資料保密性(Confidentiality) — 防止他人窺探資料內容。

研究方法

不論是多位醫師的聯合看診、或是在商業上兩造以上雙方要訂定契約，每一位參與的成員手中必定有一份要簽署文件的原文，而且它們的內容必定是相同一致的。

在整個「共同的電子簽章」的過程中，必須保證每一位成員都是對此一文件作簽署的，而且必須防止任一成員有企圖隱瞞、欺騙群組成員意圖的機會。

只有在擁有以上機制下所產生的「共同的電子簽章」才會是一份共同意志力及承諾表現的文件。我們以 RSA 演算法為基礎，提出兩個解決的方法，以下分別以二個章節來加以說明。

研究方法一：

(Cosigned Signatures, 共同連署的簽章)

要產生某一組成員「共同的電子簽章」最簡單有效的方法，是使用群組中每一成員的私密金鑰，對由原文所產生的雜湊值 $H(M)$ 施以單一連續的加密，即可得到最後期望的簽章值。

驗證時僅需利用每一成員的公開金鑰對簽章值施予單一連續反向的解密，即可反推得到文件製作當時所產生的雜湊值 $H(M)$ 。驗證者可再次對原文(M)作一次雜湊，比對兩個雜湊值是否相同，即可判定簽章值的真偽；相同為真，不相同為偽。

以下我們以三個成員 A、B、C 要對原文(M) 產生「共同的電子簽章」為例，首先將雜湊值 $H(M)$ 以 A 的私密金鑰對其加密，也就是將雜湊值 $H(M)$ 取 D_a 指數的乘方後，再以 n_A 取其模數($\{D_a, n_A\}$ 為 A 的私密金鑰)，即可得到 A 對 $H(M)$ 的簽章值 S_1 。之後，A 再將 S_1 傳給 B，同樣的 B 亦以其私密金鑰 $\{D_b, n_B\}$ 對 S_1 加密後得到簽章值 S_2 ，B 再將 S_2 傳給 C，C 再以其私密金鑰 $\{D_c, n_C\}$ 對 S_2 加密後得到簽章值 S_3 即為最後所求。其相關數學式子如下所示：

簽章方法

$$\begin{aligned} S_1 &= H(M)^{D_a} \bmod n_A \\ S_2 &= S_1^{D_b} \bmod n_B \\ S_3 &= S_2^{D_c} \bmod n_C \end{aligned}$$

驗證時要依原來簽章相反的順序 C、B、A 為之，C 先以他的公開金鑰 $\{E_c, n_C\}$ 對簽章值 S_3 作解密可反推得到 S_2 。

同樣的 B 及 A 亦分別以其公開金鑰對簽章值 S_2 及 S_1 作解密，最後可反推得到最原始的簽章值 $H(M)$ 。依此簽章值 $H(M)$ 我們便可據以判斷簽章值 S_3 的有效性。其相關數學式子如下所示：

驗證方法

$$\begin{aligned} H(M) &= S_1^{E_a} \bmod n_A \\ S_1 &= S_2^{E_b} \bmod n_B \\ S_2 &= S_3^{E_c} \bmod n_C \end{aligned}$$

雖然上述的方法在理論上是可行的，但在簽章的過程當中，成員 B 在收到 A 傳來的簽章值 S_1 時，B 如何能夠相信 A 是以雙（多）方約定的原文 M 為範本產生的呢？或是 A 基於其它的因素蓄意或非故意的使 B 簽署非約定的文件呢？同樣的 C 在收到 B 傳來的簽章值時，也有相同的疑慮。另外，在傳送的過程中簽章值也有可能遭受到惡意第三者的竄改。

因此我們必須設立一個機制讓每一位成員在簽署文件時，都能很清楚的知道自己所要簽署的是不是自己承諾的那一份文件，先前又有那些人已經簽署過了。

剛開始時，由於成員 A 為首位的簽署人員，因此他直接將原文作 Hash 後，再以他的私密金鑰對 Hash value ($H(M)$) 作加密得到簽章值 1，他再將簽章值 1 及他本身的憑證 a 傳送給成員 B。

成員 B 在收到 A 送來的資料後，首先以 CA (Certification Authority, 憑證管理中心) 的公開金鑰來驗證憑證 a 的有效性，在驗證無誤後，取出憑證 a 中的公鑰對簽章值 1 進行解密可以反推得到由 A 所產生的 $H(M)$ ；接著 B 可將手中的原文作 Hash 產生另一新的 $H(M)$ ，兩相比對，如果是相同的，則 B 就可以相信 A 所傳來的簽章值 1 是以所約定的原文，而且是以 A 的私鑰所產生的，並且也驗證了憑證 a 的有效性。接著 B 以其私密金鑰對簽章值 1 加密產生簽章值 2，B 再將簽章值 2、憑證 a、以及憑證 b 一起傳給成員 C。

成員 C 在收到 B 送來的資料後，同樣的先驗證憑證 a、及憑證 b 的有效性後，再分別、連續、反向 (b 在前 a 在後) 的對簽章值 2 解密可反推得到原始的 $H(M)$ ，再與 C 自行產生的 $H(M)$ 比較無誤後，即可相信 B 所送來的資料。接著 C 再以其私鑰對簽章值 2 加密，可產生簽章值 3，因其為最末位的簽署人，故簽章值 3 即為我們最後所求的 Cosigned Signatures。

由以上可清楚的知道，第 N 位的簽署者，必定會收到簽章值 N-1，以及憑證 1、憑證 2...、憑證 N-1 (如 Figure 1)，借由這 N-1 個憑證可以得知他所要簽署的文件內容，是否與他所承諾的文件內容是否相同，以及此份文件已經由那些人簽署過了，並可以確認他們的身份，因此他可以很放心的去從事簽署的行為，而不必有所疑慮。同樣的他必須將他所產生的簽章值 N，以及憑證 1、憑證 2...、憑證 N-1，再串接加上自己的憑證 N 送給下一位的簽署人員。

Figure 2 為 Figure 1 的細部流程。

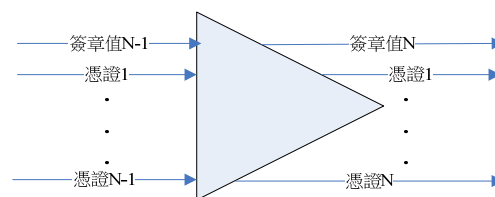


Figure 1: 成員N需接收的參數，以及需傳出的引數。

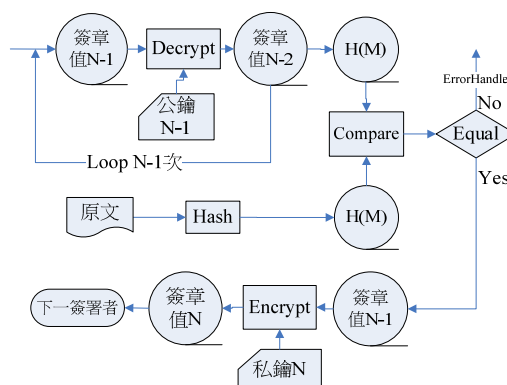


Figure 2: 成員N需要經過N-1個解密過程，才可反推得到 $H(M)$ ，確認文件來源。並再加簽後送給下一位簽署者。

研究方法二：

(Cosigned Certifications, 共同連署的憑證)

對於要連署的成員來說，方法二要簡單許多，各成員只需要各自產生自己的簽值值，傳送給 CA，由 CA 負起驗證的工作，如果一切正確無誤由 CA 發出一個憑證用以證明該群組的成員在某一特定的時間曾對某一份文件進行共同簽署的行為。

在 Figure 3 中，是我們 Cosigned Certifications (共同連署的憑證，以下簡稱 CSCR) 的 Flowchart，我們以此為藍圖對系統進行說明：

1. 首先要簽署共同文件的雙方 Alice 與 Bobs，可以先經由 RSA、DIFFIE-HELLMAN 或其他方式對要簽署的文件進行溝通、確認 (此方法在現在的技術上是可行的，不在我們研究論文的範疇中，故其說明予以省略) [6]。
2. Alice 與 Bobs 各自對已達成協議的文件進行簽章，並同時以此簽章向 CA 進行 CSCR 的請求。

3. CA 收到 Alice 與 Bobs 的請求後，比對雙方的 $H(M)$ ，如果相同可以確認雙方對要簽

署的文件有著共同的認知、及承諾。此時 CA 以它的私鑰 KR_{ca} 對 {文件的雜湊值($H(M)$)、Alice 的 id、Bobs 的 id、以及當時取得的時戳 T_s } 作簽章，產生一個簽章值 S 。

我們將上述的 5 個 Elements 的集合，合稱為 CoSigned Certifications (共同連署的憑證，簡稱 CSCR)。此由 CA 發出的憑證足以說明 Alice 及 Bobs 為此文件的聯合簽署者。

4. CA 要將 CSCR、Alice 的簽章值、以及 Bobs 的簽章值儲存在公開的 CSCR 伺服器中。

5. CA 分別將 CSCR 送回給 Alice 及 Bobs。

6. Alice 及 Bobs 必須將明文 (M) 與 CSCR 成對的進行儲存也可以將它傳送給其他的第三者。藉由 CSCR 用以宣稱 (表示) Alice 與 Bobs 雙方對此文件有共同簽署的行為 (事實)。

7. 收到 CSCR 的第三者只要經由 CA 公鑰的驗證即可相信此 CSCR 憑證，確實是由 CA 所發出。就可以相信 CSCR 上的記載：Alice 及 Bobs 在 T_s 的時間曾經對文件 $H(M)$ 作過共同的簽署，此為第一層的驗證。

一般而言，只需作第一層的驗證即可確定雙方聯合簽署的事實。如仍有疑慮，可以進行第二層的驗證：取出 CSCR 中的簽章值 S (SCSR Value) 傳送給 CA，藉以取得 Alice 與 Bobs 原始的簽章值，再分別以 Alice 與 Bobs 的公鑰加以解密並與 $H(M)$ 比較就可以知道真偽。如果仍有疑慮，仍可向 CA 請求爭議的評斷。

根據我們的系統流程，可以看出我們付予 CA 一個新的任務：就是核發 CSCR 的憑證、以及回應使用者對於爭議評斷的請求。

就醫療環境而言，醫院本身可以被視為公正的第三者，因此由各醫院自行設置 CSCR 伺服器，且由各醫院擔任仲裁者，以該醫院的醫事機構卡對 {文件的雜湊值($H(M)$)、Alice 的 id、Bobs 的 id、以及當時取得的時戳 T_s } 作簽章，產生並發出 CSCR 憑證，也是相當可行的方式，其餘系統流程與 Figure 3 相同。

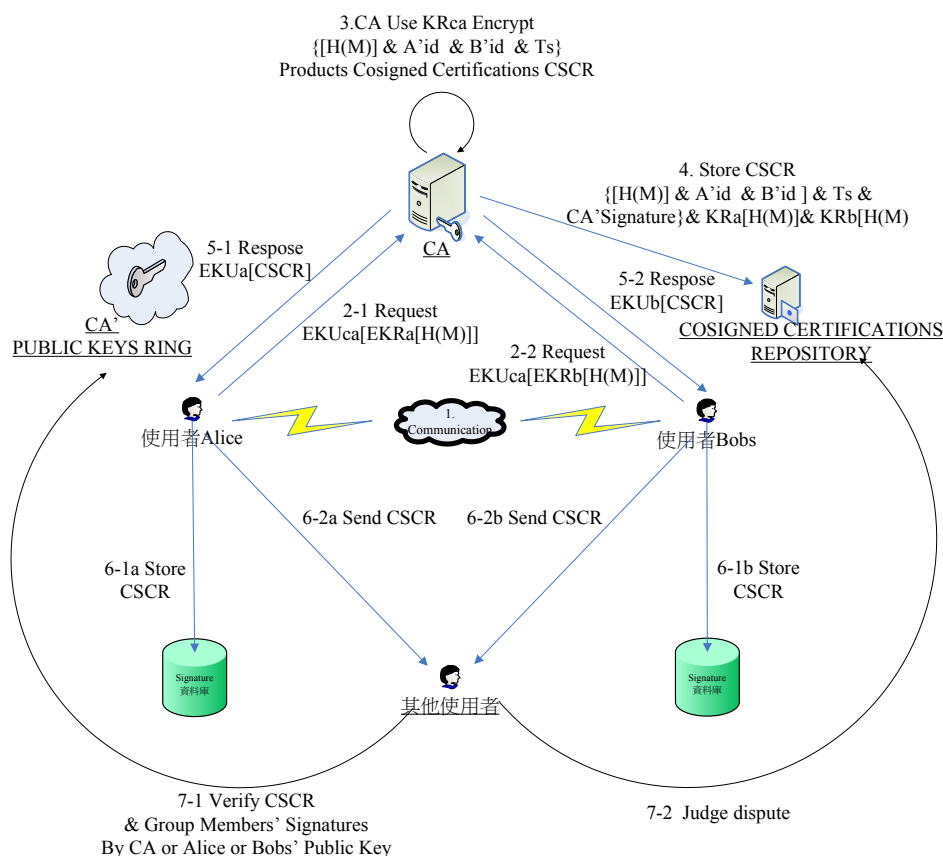


Figure 3
 Cosigned Certifications Flowchart

Table 1: Figure 3 使用符號的說明

M: 明文	H(M): 使用 SHA-1 對明文運算產生的 雜湊值
Private Key: 私密金鑰	Public Key: 公開金 鑰
KRa: a 的私密金鑰	KUa: a 的公開金鑰
KRb: b 的私密金鑰	KUb: b 的公開金鑰
KRca: CA 的私密金鑰	KUca: CA 的公開金 鑰
E: 加密	D: 解密
CA: Certification Authority 憑證管理中心	Ts: TimeStamp 時戳
EKRa[H(M)]: 以 a 的私密金鑰對 HASH VALUE 進行加密(簽章)	
CSCR: 此憑證由 CA 所發出, 其內容說明了 a & b 在 Ts 的時間曾為此文件進行聯合簽署的事 實	

結論及未來展望

不論是在醫療或是其他商業的領域上, 有許多需要兩造以上的雙(多)方所共同簽署的文件。在我們的研究中我們分別提出了二個方法(Cosigned Signatures, 共同連署的簽章)及(Cosigned Certifications, 共同連署的憑證)來達成上述製作「共同電子簽章」的目的。

Cosigned Signatures 的優點是製作容易, 學理上的流程簡單, 缺點則是每一位連署人員都需要將連署人員的憑證 cascade 的串接起來送出及驗證, 適合在連署人員較少時使用。

Cosigned Certifications 的優點是每一位連署人員只需將自己產生的簽章送給 CA, 驗證的工作則交由 CA 來執行, 由收到 CA 的「共同連署的憑證」CSCR 來加以證明眾人曾在 Ts 時間連署的事實, 缺點則是需要經由 CA (或其他公正仲裁者) 的支援。

在衛生署及 HCA (醫療憑證管理中心) 相關的規

範中，對於醫師聯合看診所需要的「共同的電子簽章」，並沒有任何的描述，經由我們的研究已經為此缺陷找到了解決方法。

雖然就資訊技術而言要將醫療資訊系統導入電子簽章並沒有窒礙難行的地方，然而在其過程中，仍然有許多可以再加強改良的空間，諸如如何提昇醫療影像作雜湊的速度，如何設計一個完善的簽章資料庫，使系統運作能更為順暢等等，都是可以再努力的方向。

希望藉由眾人的努力能早日看到醫療資訊領域 Paperless 及院際間醫療資訊線上即時交換的來臨及實現。

參考文獻

- [1] 王大為 劉敦仁 陳怡璋，“電子病歷認證機制研究”，The Journal of China Association for Medical Informatics No 10, December 1999, pp 71-84. Copyright© CAMI, 1999
- [2] 吳志成，“醫療資訊系統導入電子簽章之參考架構與整體解決方案 A Reference Architecture and Solution Plan For The Employment of Digital Signature in Medical Information System”，東華大學資訊工程學系碩士論文(民 93)
- [3] “經濟部商業司電子簽章”，http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm
- [4] 劉俊茂，“簡易的群體簽章方案 Very Simple Schemes for Group Signatures”，中原大學電機工程學系碩士論文(民 92)
- [5] 賴溪松，“近代密碼學及其應用 Contemporary Cryptography and It's Applications”，旗標出版股份有限公司，中華民國 92 年 8 月出版
- [6] William Stallings. “Cryptography and Network Security. Principles and Practice.”. Third Edition, Prentice Hall, 2003.