一個支援長期檢驗電子健康記錄管理之身份識別與授權機制

吳佳怡[1]、羅乃維[2]、莊祐軒[3]、陳世仁[4]、許明淵[5]
台灣科技大學資訊管理系[1,2,3]
財團法人資訊工業策進會資安科技研究所[4,5]
M10209118@mail.ntust.edu.tw[1]、nwlo@cs.ntust.edu.tw[2]、D10009103@ mail.ntust.edu.tw[3]、
sjchen@iii.org.tw[4]、wayne@iii.org.tw[5]

摘要

現今，因醫療普及人們普遍壽命延長，我們需要長期保存並存取一生中健康資料，以讓該資料可於未來與醫院、健康組織、醫療人員共享，因此歷史健康資料的保存是重要的。我們的目的是維持與管理人們的歷史健康記錄，並避免電子健康記錄遺失。

為了讓歷史健康記錄可以長期保存至人的一生，我們提出一個身份識別與授權機制來保存與管理長期電子健康記錄，使用者可自行將其醫院或健康組織內的健康記錄轉移至特定的組織。機制是採用累積簽章機制將在轉移前擁有資料的組織的信任程度轉移至新組織，並以第三方可信任機關作為身份提供商身份識別所有組織，最後由授權機制確保使用者授權該機構共享資料，並可以達到長期電子健康記錄的完整性、可用性與記錄授權的不可否認性。

關鍵詞：電子健康紀錄、長期管理電子資料、累積公證簽章、身份辨識、授權

An Authentication and Authorization Mechanism for Long-term Electronic Health Records Management

Chia-Yi Wu[1], Nai-Wei Lo[2], Yo-Hsuan Chuang[3], Shih-Jen Chen[4] and Ming-Yuan Hsu[5]
Department of Information Management, National Taiwan University of Science and Technology[1,2,3]
CyberTrust Technology Institute, Institute for Information Industry[4,5]
M10209118@mail.ntust.edu.tw[1], nwlo@cs.ntust.edu.tw[2], D10009103@ mail.ntust.edu.tw[3],
sjchen@iii.org.tw[4], wayne@iii.org.tw[5]

Abstract

Due to the medicine knowledge widespread, the human life expectancy is extending. People have to keep personal health records during their lifetime to share and discuss with medical professionals. Therefore, the issue of maintaining the historical personal health records becomes more significant. Our aim is to keep and manage the long-term historical

electronic health records to avoid the records lost.

In this paper, we proposed an authentication and authorization protocol for the long-term historical electronic health records to manage more than the human life lifetime. User can request its records to migrate to a specific organization, and then authorize the organization. The proposed protocol is referring the cumulatively notarized signature to transfer the trustworthiness to a specific organization, and the trust third notary as an identity provider to authenticate the user, specific organizations. Finally, the trust third notary requests the authorization to user to share their historical records with the organization. And the proposed protocol achieves data integrity, non-repudiation for data authorization and availability of EHR.

Keywords: Electronic health records, Long-term electronic records management, Cumulatively notarized signature, Authentication, Authorization

壹、前言

醫院、診所等機構以及醫療衛生系統的趨勢在最近幾年有所改變。由於無線人體區域網路[10]的出現，讓醫療產業有了重大的突破。近年來，舊有的診所及醫療資訊逐漸電子化轉變成電子記錄，並儲存在電子病歷(EMR)[2]或電子健康記錄(EHR)裡。人們不只從醫院看病得到自己的健康相關資料，還可以透過像是健康手環之類的健康裝置來得知自己的身體資訊。此外，健康相關記錄的歷史資料是一項重要的資產，可以用在未來改善病患的照護。而這些歷史病歷相關資料通常會存放於相關的醫療衛生組織中，且都需要有相當程度的安全需求[1][17]，像是記錄的隱私性、機密性、可驗證性、授權以及長期保存等。

健康相關記錄具有高度敏感性及機密性，故在傳輸時需要加密，即便是在線下存取也相同[1]。隨著 Personal Data Protection Act 在各國的釋出，個人資料的隱私[14][18][19]變得至關重要。健康記錄的擁有者或保存者須確保身份認證的正確性，以避免受到任何的攻擊及資料的竄改，導致任何違法的事情發生。根據文獻[11]，在遠距照護上，資料交換是一個重要的議題，其驗證機制必須可以建立一個安全通道，讓 EMR 或 HER 能有效且安全地交換。此外，授權機制[3][4][9][24]也是另一個議題，而電子健康記錄及電子病歷的擁有權在近期也受到許多討論。這些記錄由專業的醫療或照護人員所產生出來，而這些記錄都跟病患本身息息相關，所以如何與其他人分享記錄變成了一個議題。在文獻[24]中，作者們提出了一套病患自我控制多階級隱私保留合作授權機制(patient self-controllable multi-level privacy-preserving cooperative authentication scheme，PSMPA)，

可達到健康資訊的機密性並保有病患的隱私。這套機制將存取病患健康資訊的人分成三個等級，包含了直接授權醫事人員(directly authorized physicians)、間接授權醫事人員(indirectly authorized physicians)及無授權人員(unauthorized persons)。直接授權醫事人員是被病患直接授權，醫事人員可以得知病患所有的健康資訊；間接授權醫事人員可能為學術研究員、醫療顧問等，他們只能得知病患的健康資訊，但不知道病患身份；無授權人員則無法存取及分享任何健康資訊。

健康記錄的長期保存[8][12][13][20][22]相對於其他需求而言是更為重要的，這些記錄往往需要存放比人類壽命還久的時間。每個人幾乎都會在醫院、診所、提供物聯網服務的公司及健康照護中心等地方留有記錄，而這些機構所有的健康相關歷史記錄對於病患的治療以及醫學上的研究都極有幫助。在文獻[23]中，將數位文件的保存方式大略分為四種方法：硬體與程式(hardware and programs)、模擬器(emulators)、將數位文件編碼(transcode the digital documents)、標準格式(standard formats)。然而，這些方法都無法完整地管理這些長期保存的文件。

在台灣，因地小人稠，住家與工作地點附近均容易找到醫院，較容易得到醫療資訊，而且衛福部健保署會強制管理人民的醫療記錄，很少有醫療記錄遺失的情況發生。但在某些大國家，像是美國、英國等，醫院的電子病歷結構並沒有像是台灣健保署這樣集中化強制管理的政府機構，人們可能會因工作、結婚等原因而改變自己的住所，人們轉換醫療院所後，轉換前的資料難以取得。若因為醫院的合併、倒閉更有可能讓重要資訊遺失。因此，健康記錄的長存保存是一件非常重要的課題。

另一方面，現今穿戴式裝置盛行，每個人身上配戴的穿戴式裝置以及在每一個人生階段的就診紀錄、健康檢查等，均為人們的重要資產。特別是因網際網路的發達，使偏遠地區的人們可以透過穿戴式裝置，遠距離透過網路即時得到人們的身體資訊(身體健康狀況)。甚至未來，人們可以與醫生即時討論自己的身體資訊，而非只聽從醫生指示，但這些資訊目前大多為科技公司所管理，更無法強制管理每個人的身體健康資訊等重要資產。

基於上述理由，我們針對 EMR 及 EHR 兩種型式的記錄提出一個機制。EMR 是由醫院、急診等所產生的個人記錄，內容包含了醫療諮詢記錄、照護計畫、生命徵象記錄、醫療實驗記錄及報告、藥物使用記錄、過往診斷記錄、家族病史等。而 EHR 則是含蓋了 EMR，包含健康相關記錄、身體健康記錄、診療、人口統計學、保險資料以及其他非醫療相關的管理資訊。我們提出一個身份識別與授權機制來保存與管理長期電子健康記錄，使用者可自行將其醫院或健康組織內的健康記錄轉移至特定的組織。機制是採用累積簽章機制[12][13]將在轉移前擁有資料的組織的信任程度轉移至新組織，並以第三方可信任機關[15]作為身份提供商身份識別所有組織，最後由授權機制確保使用者授權該機構共享資料，並可以達到長期電子健康記錄的完整性、可用性與記錄授權的不可否認性。其主要貢獻如下：

1. 使用第三方可信任機關及 PKI 加密系統來確保健康資料長期的安全。
2. 可保有電子健康記錄的完整性、授權的不可否認性以及可用性。
3. 可以簡易的根據使用者的意願轉移其資料。

貳、文獻探討

一、長期記錄保存(Long-term Records Preservation)

隨著電子資料的廣為流傳，我們必須維持其可用性、完整性、機密性、可靠性及不可否認性。有些政府已經建立規範來確保病患記錄的安全，像是美國健康保險便利和責任法案(HIPAA)[7]。但對於數位文件的長期保護仍存在某些問題，例如：產生金鑰的演算法會被攻破、憑證會失效以及第三方公正單位不再被信任等。

我們研讀了一些有關長期資料保護方法的文獻。在文獻[23]中，作者們研究長期保護數位資料的方法，像是：ERS[5][8][22]、ETSI 標準[25][26]、內容完整性服務(content integrity service，CIS)、最佳化憑證等。ERS 是基於 Merkle 樹 PKIX 時間戳而成的方法，可以用來確保完整性及證明長期資料的存在。而 ETSI 標準則是基於數位簽章及 PKIX 時間戳而成的方法，該標準可延長簽章的可信任時間及確保長期資料的真實性。在文獻[20]中，Carmela 等人提出一套安全的長期檔案系統(Secure Long-Term Archival System，SLTAS)，以 client-server 為架構，可以驗證簽章的真實性以保護資料。在簽章階段，作者認為時間戳無法完全證明該簽章是多早之前所簽署的，所以 client 會要求兩個時間戳，包含簽章前以及簽章後的時間。此外，為了增強可靠性，該系統使用洋蔥式的 re-timestamp 並適用於目前的時間戳演算法。當 client 需要取回資料時，該系統會驗證最後一次的洋蔥式時間戳或是最後一次時間戳後的所有時間戳。在文獻[22]提到最常使用在長期記錄保存的方法通常會採用時間戳權力(timestamp authority，TSA)來保存文件。短時間內，委託人會信任受託人，但 TSA 會把時間拉長，而在此情況下，會降低對受託人的信任，一旦信任程度下降，委託人可能就不會再信任任何的委託人。故它使用信譽來評估及分析該信任程度。

電子健康記錄可以改善醫療照護的品質、病患的身心安全以及減少醫療疏失。而這些資訊往往來自醫院、診所、家裡以及任何醫療照護中心，像是目前的藥物治療、患者病情、家族病史、體重、血壓、病人的保險、財務資料及護理資料等。由於患者的資訊可能會被用在學術研究上或是分享給醫療專家，故這些記錄都必須能被長期的保存著。現今已有些研究在探討電子病歷及電子健康記錄的長期保存方法。文獻[16]提到創建一個可信賴的公正檔案(trust notary archive，TNA)來儲存來自於不同 EHR 系統的記錄，並且可達到不可否認性及完整性。在文獻[13]中，作者主要探討長期記錄保存的 EHR 系統

其可靠性。它使用公證人及採用累積式的公證簽章來簽署 EHR，藉此延長簽章的時間性且讓該時間大於一般人的壽命。

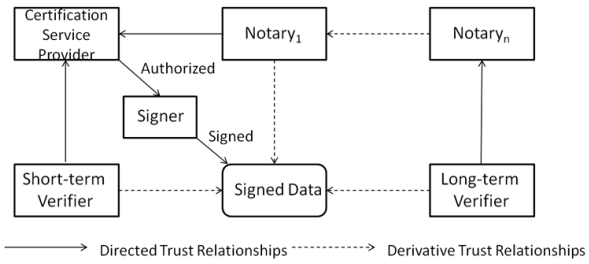
二、累積公證簽章(Cumulatively Notarized Signature)

針對長期保存電子記錄的方法，我們使用數位簽章來驗證資訊的可靠性。而數位簽章的生命週期會因為金鑰及憑證而有所限制，為了延長數位簽章的時效性，便有些方法被提出，像是實作一個 PKI 非對稱金鑰結構。即便如此，依然有些限制，在資料傳送到可信賴的公正第三方機構之前，我們必須先將該資料簽章，此簽章包含時間戳及公證(notarization)。該簽章的時效性仍短，時間戳及公正第三方機構僅能解決部分問題。

在文獻[12]中，作者們提出使用累積式簽章(accumulating notary)，主要概念是在資訊到達新的機構之前，消除任何被淘汰的資料或技術之間的信任關係，來達到連續性移轉的信任、資訊及技術。主要角色有簽章者(signer)、憑證服務提供者(certification service provider，CSP)、公證者(notary)、驗證者(verifer)。簽章者負責產生簽章；憑證服務提供者負責發送憑證及經由認證者簽章的授權；公證者負責授權給簽章者及認證者；驗證者負責驗證簽章的正確性。採用信任移轉的特性，若 A 信任 B 且 B 信任 C，則 A 也會信任 C。假設驗證者信任公證者，則驗證者則也會信任公證者所信任的機構。圖一為信任關係模型，短期驗證者信任憑證服務提供者、憑證服務提供者授權給簽章者、第一個公證者信任憑證服務提供者以及長期驗證者信任第 N 個公證者，故長期驗證者也會信任擁有簽章的資料(Signed data)。

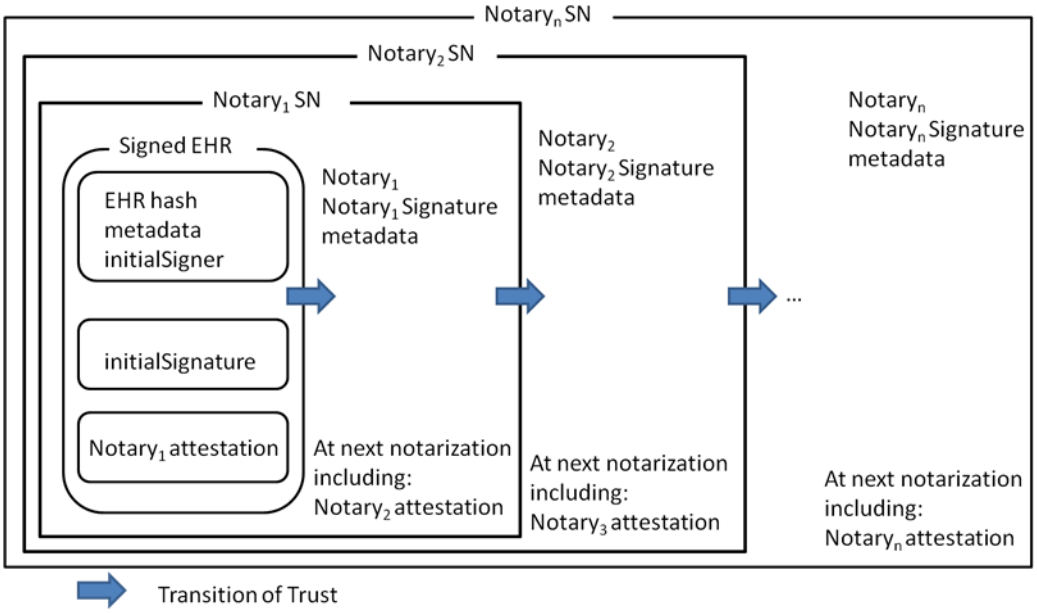
由於病例的生命週期非常重要，所以 D. Lekkas 等學者[13]提出累積洋蔥式簽章(cumulatively notarized signature)，讓電子病歷能夠長期且安全地被保存著，保存期限遠大於數位簽章，也保證至少會等同於病患的壽命時間。

圖二為累積公證式簽章的連續封裝示意圖[13]，作者假設公證者被憑證服務者所信任且憑證是有效的。該機制將 EHR 資料、metadata、初始簽章者 id 以及經過第一個公證者認證過之初始簽章者的簽章打包在一起，封裝後傳送至新的公證者單位，如此一來便能達到長期且連續的保存。$Notary_1$ SN 包含了簽章過的 EHR 資料、$Notary_1$ 簽章、簽章



圖一：信任關係模型

的 metadata 及 $Notary_1$ 的 id；$Notary_2$ SN 則包含了 $Notary_1$ SN 簽章、簽章的 metadata、$Notary_2$ 的 id，就這樣經由各個公證者連續地封裝下去。



圖二：累積公證簽章

三、其他

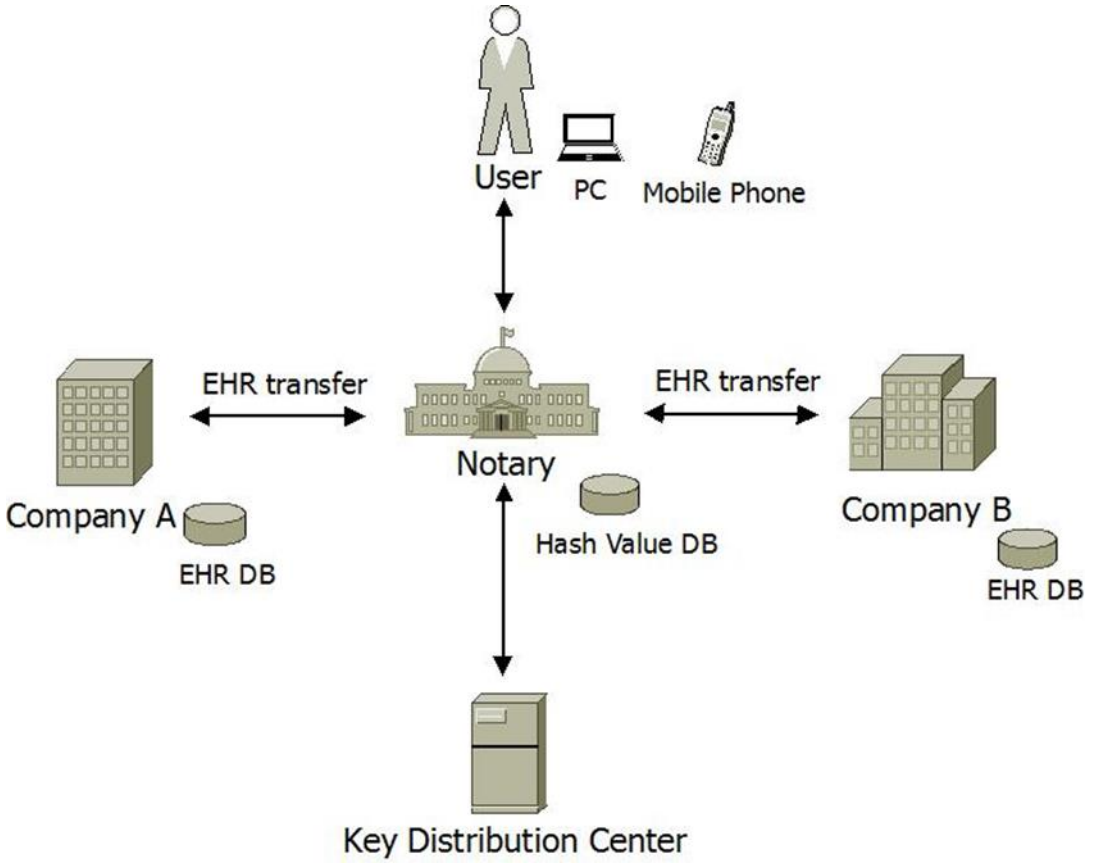
I、公開金鑰加密系統(Public Key Cryptosystem)

公開金鑰加密系統[15]基於非對稱式金鑰演算法，有兩把金鑰，一把為公開金鑰，另一把為私人金鑰。將某使用者的公開金鑰加密後之訊息，只有該使用者的私人金鑰才能解密，且無法利用公開的金鑰計算出私人的金鑰為何，其負責度極高，為 NP-completed 問題。

II、對手模式(Adversary Model)

假設對手遵守 honest-but-curious 原則且具有有限的計算能力，並遵循機制及拿到所有的傳輸交換訊息。若對手擁有公開金鑰，也無法計算出對應的私鑰。惡意的對手可以擷取、竊聽並替換原本的即時訊息。此外，對手從收到的訊息封包學習並隨心所欲地注入有害的東西。當對手知道其加解密演算法及雜湊含數，便可以得到使用者的 id，但也無法拿到使用者的 EHR 記錄，即便對手替換了變數並送出部分的加密訊息並回傳給使用者。總結來說，竊聽攻擊、替換攻擊、中間人攻擊及偽造攻擊都可能發生。

參、一個支援長期檢驗電子健康記錄管理之身份識別與授權機制



圖三：一個支援長期檢驗電子健康記錄管理之身份識別與授權機制架構示意圖

一、簡介

這小節將會介紹我們的機制，而在此機制當中，我們以公司替代醫院、診所及醫療照護中心等機構。圖三中，有五個主要的單位分別為公司 A、公司 B、使用者、公證者及金鑰發布中心，以下針對每個單位作描述：

- 公司 A：擁有使用者的 EHR 記錄。公司 A 可能會被併購或倒閉使其所有 EHR 記錄轉移至其他公司。換句話說，使用者可以授權轉移 EHR 記錄給新公司。
- 公司 B：公司 B 可能會收購或接管公司 A，但不一定可以取得使用者的 EHR 記錄，須經由使用者同意。故公司 B 的最大目標則是從公司 A 手中接管所有的使用者 EHR 記錄。首先，使用者必須同意將記錄交給公司 B，接著公司 B 才能發送請求至公證者以達到轉換使用者 EHR 記錄之目的。
- 使用者：使用者在公司 A 裡存有自己的 EHR 記錄，當使用者想移轉記錄時，可以使用電腦、手機經由無線網路來完成移轉程序。使用者也可自行決定要將自己的 EHR 記錄授權給哪家公司。

- 公證者(Notary，NOR)：NOR 是一個永久且可信任的醫療單位，此單位建議為政府機構，相對於私人企業會來得穩定許多。所有公司跟使用者都必須向 NOR 註冊登記。NOR 最大的任務就是確認公司在接管或被接管的過程中，所有被移轉的使用者資料都是合法的。舉例來說，公司 A 持有的 EHR 記錄要被移轉至公司 B 並且再移轉至公司 C，若使用者沒有授權給公司 A 及公司 B，NOR 則會保存公司 A 及公司 B 的所有 EHR 記錄。
- 金鑰發布中心(Key Distribution Center，KDC)：KDC 負責處理所有單位的公開金鑰、私人金鑰以及憑證。KDC 會在使用者授權給新公司時更新其金鑰。

我們的協定採用了數位簽章、驗證及授權機制，其中簽章機制是參考累積公證簽章[12][13]；而驗證及授權機制則是參考 PKI[15]機制。而本機制中所使用的符號意義如表一所示。

表一：符號意義表

符號	描述
U_i	使用者 i
C_j	公司 j
NOR	公證者；一個永久且可信任的公正第三方
KDC	金鑰發布中心
UID_i	U_i 的 ID
CID_j	C_j 的 ID
NID_n	$NOR\ n$ 的 ID
KID_k	$KDC\ k$ 的 ID
s_i^u	U_i 與 NOR 的秘密值
s_j^c	C_j 與 NOR 的秘密值
D_i	U_i 的健康記錄
K_i^p	U_i 的公鑰
K_i^s	U_i 的私鑰
K_j^p	C_j 的公鑰
K_j^s	C_j 的私鑰
K_n^p	$NOR\ n$ 的公鑰
K_n^s	$NOR\ n$ 的私鑰
K_k^p	$KDC\ k$ 的公鑰
K_k^s	$KDC\ k$ 的私鑰
$Sig_x(\cdot)$	以金鑰 x 簽章
$E_x(\cdot)$	以金鑰 x 加密
$D_x(\cdot)$	以金鑰 x 解密
$H(\cdot)$	抗碰撞單向雜湊函數
T_s	時間戳

二、本機制流程

我們的機制採用了信任移轉及連續授權的特性。信任移轉指的是若 A 信任 B 且 B 信任 C，則 A 信任 C；連續授權是指，若U_i 將從C_a 移轉D_i 至C_b ，並繼續移轉至C_c ，當U_i 授權給C_c 時，C_c 可以解密所以從C_a 移轉給C_b 再移轉給C_c 的資料。

我們的機制有三個階段。第一階段為初始階段，首先C_j 和U_i 都會向 NOR 註冊，然後 KDC 會產生公鑰及私鑰並傳送給所有單位；第二階段為驗證階段，U_i 將D_i 從C_a 移轉至C_b ，而U_i 可以在任何時間取存放置在C_b 裡的D_i ；第三階段為授權階段，U_i 經由 NOR 送出授權給C_b ，此時C_a 會將D_i 簽章並加密後移轉至C_b ，C_b 便可解密並驗證D_i 。最終，NOR 會刪除相關的雜湊值並要求 KDC 更新使用者的金鑰。

I、初始階段(Initialization Phase)

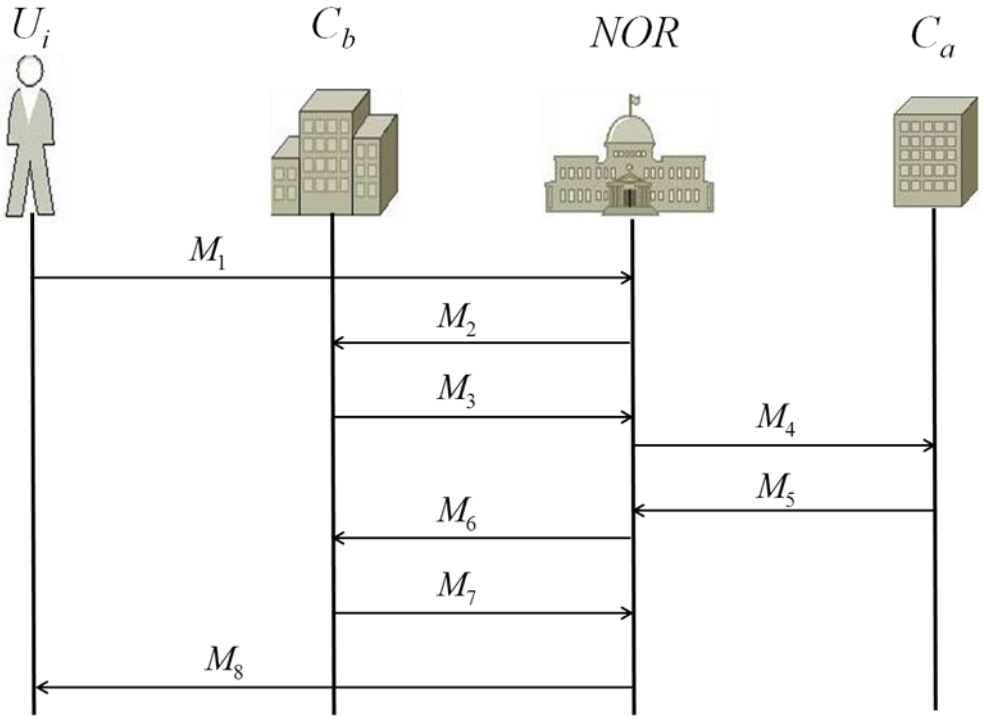
首先，C_j 和U_i 都必須向 NOR 註冊。NOR 和C_j 有共同的祕密值S_j^c ，NOR 和U_i 也有共同的秘密值S_i^u 。若C_j 和U_i 遺失了秘密值，則 NOR 會讓原有的秘密值失效並重新產生新的秘密值。KDC 會產生所有單位的公私鑰包含U_i 的(K_i^p, K_i^s)、C_j 的(K_j^p, K_j^s)、NOR 的(K_n^p, K_n^s)以及 KDC 的(K_k^p, K_k^s)。然後，KDC 會處理其憑證並傳送金鑰對給所有單位，而每個單位所儲存的參數如表二所示。

表二: 參數表

單位	儲存參數
U_i	$(UID_i, K_i^p, K_i^s, s_i^u, CID_j, NID_n, KID_k, K_k^p, K_n^p)$
NOR	$(NID_n, K_n^p, K_n^s, s_i^u, s_j^c, UID_i, CID_j, KID_k, K_i^p, K_j^p, K_k^p)$
KDC	$(KID_k, K_k^p, K_k^s, UID_i, NID_n, K_i^p, K_n^p)$
C_j	$(CID_j, K_j^p, K_j^s, s_j^c, UID_i, NID_n, K_i^p, K_n^p)$

II、使用者資料移轉驗證階段(User Data Transfer Authentication Phase)

圖四為使用者資料移轉的驗證階段，我們假設D_i 從C_a 移轉至C_b ，其步驟如下：



圖四：使用者資料移轉驗證流程

1、$U_i \rightarrow NOR$：

當U_i 想要從C_a 轉移D_i ，U_i 必須告知 NOR 其UID_i 、CID_a 及CID_b 。首先，U_i 先將CID_a 、CID_b 、秘密值s_i^u 及時間戳作雜湊，再將此雜湊值與UID_i 、CID_a 、CID_b 及時間戳包在一起傳送訊息 $M_1 = \{UID_i, CID_a, CID_b, H(CID_a, CID_b, s_i^u \oplus T_s), T_s\}$ 至 NOR。

NOR：

當 NOR 接到訊息M_1 ，會依照接收到的UID_i 檢查相對應的秘密值s_i^u ，然後 NOR 使用CID_a 、CID_b 、s_i^u 計算出雜湊值並與$H(CID_a, CID_b, s_i^u \oplus T_s)$ 比較數值是否相同。

2、$NOR \rightarrow C_b$ ：

當 NOR 確認後，NOR 會要求C_b 接收D_i 。首先，U_i 計算UID_i 、s_b^c 及時間戳之雜湊值後產生$H(UID_i, s_b^c \oplus T_s)$ ，NOR 再將此雜湊值、UID_i 、NID_n 及時間戳打包成訊息 $M_2 = \{UID_i, NID_n, H(UID_i, s_b^c \oplus T_s), T_s\}$ 給C_b 。

C_b ：

當C_b 接收到訊息M_2 後，會使用秘密值s_b^c 及接收到的UID_i 來驗證$H(UID_i, s_b^c \oplus T_s)$ 是否正確。接著，C_b 便可以確認U_i 的 ID。

3、$C_b \rightarrow NOR$：

當C_b確認可以從C_a移轉D_i時，便會告知NOR。C_b會先計算s_b^c及時間戳之雜湊值取得$H(s_b^c \oplus T_s)$，接著將此雜湊值與UID_i用K_n^p加密得到$E_{K_n^p}(UID_i, H(s_b^c \oplus T_s))$，最終$C_b$會傳送訊息至$M_3 = \{CID_b, E_{K_n^p}(UID_i, H(s_b^c \oplus T_s)), T_s\}$NOR。

NOR：

NOR 接受到M_3後會將解密$E_{K_n^p}(UID_i, H(s_b^c \oplus T_s))$，並比對$H(s_b^c \oplus T_s)$是否正確，接著$C_b$便能開始接管$D_i$。

4、$NOR \rightarrow C_a$：

當NOR確認C_b可以接管D_i時，便會要求C_a提供D_i。首先，NOR會計算UID_i、s_b^c與時間戳之雜湊值得到$H(UID_i, s_a^c \oplus T_s)$，再將此雜湊值與$UID_i$、$NID_n$及時間戳打包成訊息$M_4 = \{UID_i, NID_n, H(UID_i, s_a^c \oplus T_s), T_s\}$傳送至$C_a$。

C_a：

當C_a接收到訊息M_4，會驗證$H(UID_i, s_a^c \oplus T_s)$是否正確。

5、$C_a \rightarrow NOR$：

在C_a移轉D_i之前，會先將D_i簽章後，並與D_i、K_a^p作加密得到$E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p)$，接著將此加密訊息簽章後得到$Sig_{K_a^s}(E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p))$。接著$C_a$會計算$s_a^c$與時間戳的雜湊值$H(s_a^c \oplus T_s)$。之後將上述三個訊息用$K_n^p$與$UID_i$作加密。最後再與$CID_a$及時間戳打包成訊息

$M_5 = \{CID_a, E_{K_n^p}(UID_i, E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p),$

$Sig_{K_a^s}(E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p)), H(s_a^c \oplus T_s)), T_s\}$傳送回NOR。

NOR：

當NOR接收到M_5後，會驗證$Sig_{K_a^s}(E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p))$與$H(s_a^c \oplus T_s)$之正確性。接著，將$E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p)$作雜湊後儲存起來以便日後驗證。

6、$NOR \rightarrow C_b$：

當NOR獲得D_i後，會將D_i送至C_b。NOR會計算出$H(s_b^c \oplus T_s)$，接著與$E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p)$用$K_b^p$加密。最後NOR會傳送訊息$M_6 = \{UID_i, NID_n, E_{K_b^p}(E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p), H(s_b^c \oplus T_s)), T_s\}$至$C_b$。

C_b：

當C_b收到M_6後，會驗證$H(s_b^c \oplus T_s)$是否正確。

7、$C_b \rightarrow NOR$：

在 C_b 收到 D_i 後，會告知 NOR。C_b 會先計算 $H(s_b^c \oplus T_s)$，接著傳送訊息 $M_7 = \{UID_i, CID_b, H(s_b^c \oplus T_s), T_s\}$ 給 NOR。

NOR：

當 NOR 收到 M_7 後，會驗證 $H(s_b^c \oplus T_s)$ 是否正確，若正確，則 NOR 確認此移轉成功。

8、$NOR \rightarrow U_i$：

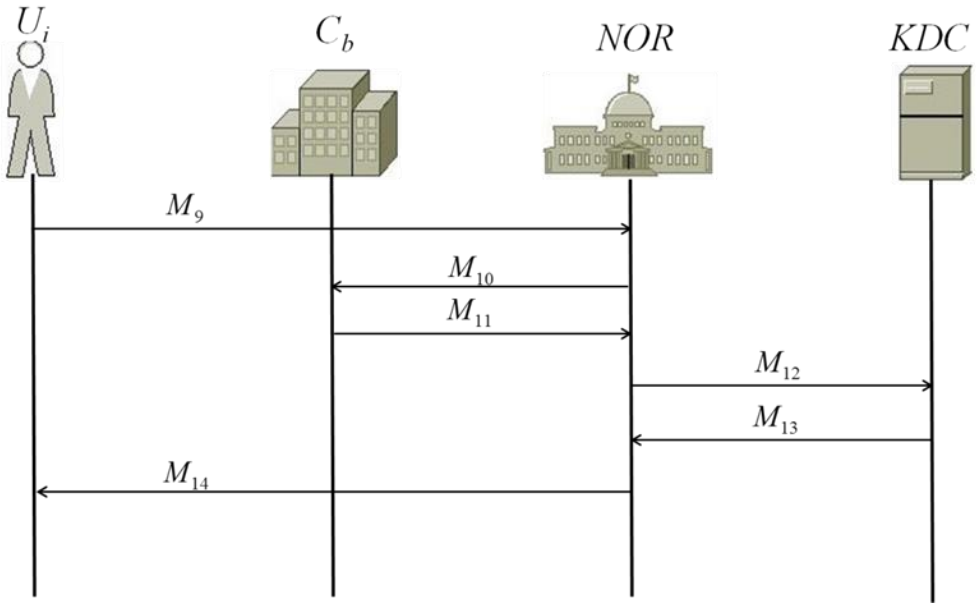
最終，NOR 會告知 U_i 說 D_i 已經被成功從 C_a 移轉至 C_b。首先，NOR 會先計算 $H(NID_n, CID_a, CID_b, s_i^u \oplus T_s)$，接著將此雜湊值與 NID_n、時間戳打包成訊息 $M_8 = \{NID_n, H(NID_n, CID_a, CID_b, s_i^u \oplus T_s), T_s\}$ 傳給 U_i。

U_i：

當 U_i 收到 M_8 後，會驗證 $H(NID_n, CID_a, CID_b, s_i^u \oplus T_s)$ 是否正確，若正確，則 U_i 確定 D_i 已經從 C_a 移轉至 C_b。

III、使用者資料授權階段(User Data Authorization Phase)

圖五為使用者資料授權階段，D_i 從 C_a 移轉至 C_b，U_i 得到從 C_b 存取資料的權限，其步驟如下：



圖五：使用者資料授權流程

9、$U_i \rightarrow NOR$：

當U_i取得從C_b讀取D_i的權限後，U_i會提供K_i^s給 NOR。首先，U_i會先產生雜湊值$H(s_i^u \oplus T_s)$，而後將此雜湊值與K_i^s、時間戳用K_n^p作加密產生$E_{K_n^p}(K_i^s, H(s_i^u \oplus T_s))$。最後，$U_i$將此加密的訊息與$UID_i$、時間戳打包成訊息$M_9 = \{UID_i, E_{K_n^p}(K_i^s, H(s_i^u \oplus T_s)), T_s\}$轉給 NOR。

NOR：

當 NOR 收到M_9，會使用K_n^s解密出$E_{K_n^p}(K_i^s, H(s_i^u \oplus T_s))$。然後 NOR 使用收到的$UID_i$找到相對應的$s_i^u$，並確認其雜湊值是否相等。最終，NOR 會刪除先前驗證階段所儲存的雜湊值$H(E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p))$。

10、$NOR \rightarrow C_b$：

當 NOR 確認U_i得到C_b的存取權限後，會提供K_i^s給C_b。首先，NOR 會計算出雜湊值$H(s_b^c \oplus T_s)$，並用K_b^p加密得到$E_{K_b^p}(K_i^s, H(s_b^c \oplus T_s))$。最後，NOR 會將此加密訊息與$UID_i$、$NID_n$、時間戳打包成訊息$M_{10} = \{UID_i, NID_n, E_{K_b^p}(K_i^s, H(s_b^c \oplus T_s)), T_s\}$傳送至$C_b$。

C_b：

當C_b收到訊息M_{10}後，會解密出$E_{K_b^p}(K_i^s, H(s_b^c \oplus T_s))$。接著$C_b$會計算出雜湊值$H(s_b^c \oplus T_s)$來驗證其正確性。此外，$C_b$會用$K_i^s$來解密得到$E_{K_i^p}(D_i, Sig_{K_a^s}(D_i), K_a^p)$，進而驗證$Sig_{K_a^s}(D_i)$並得到$D_i$。

11、$C_b \rightarrow NOR$：

當C_b解密出D_i後，會發送成功訊息給 NOR。首先，C_b會先計算出雜湊值$H(s_b^c \oplus T_s)$，接著與UID_i、CID_b與時間戳打包成訊息$M_{11} = \{UID_i, CID_b, H(s_b^c \oplus T_s), T_s\}$轉送至 NOR。

NOR：

當 NOR 收到M_{11}後，會驗證$H(s_b^c \oplus T_s)$之正確性，便能確認是否成功。

12、$NOR \rightarrow KDC$：

當U_i授權給C_b，NOR 會要求 KDC 更新U_i的金鑰對。首先，NOR 會針對UID_i、NID_n與時間戳簽章得到$Sig_{K_n^s}(UID_i, NID_n \oplus T_s)$，接著與$UID_i$、$NID_n$與時間戳打包成訊息$M_{12} = \{UID_i, NID_n, Sig_{K_n^s}(UID_i, NID_n \oplus T_s), T_s\}$轉送至 KDC。

KDC：

當 KDC 收到 M_{12} 後，會驗證 $Sig_{K_n^s}(UID_i, NID_n \oplus T_s)$ 之正確性，此時 KDC 便能確認 NOR 要求更新 U_i 的金鑰對之請求。

13、*KDC→NOR*：

KDC 將 U_i 之新的金鑰對用舊的公鑰 K_i^p 加密得到 $E_{K_i^p}(K_i^{p'}, K_i^{s'})$，再對此加密訊息簽章得到 $Sig_{K_k^s}(E_{K_i^p}(K_i^{p'}, K_i^{s'}))$，接著將 UID_i 、KID_k 與時間戳作雜湊得到 $H(UID_i, KID_k \oplus T_s)$。然後 KDC 用 K_n^p 將上述三個訊息作加密，並與 UID_i 、KID_k 與時間戳打包成訊息 $M_{13} = \{UID_i, KID_k, E_{K_n^p}(E_{K_i^p}(K_i^{p'}, K_i^{s'}), Sig_{K_k^s}(E_{K_i^p}(K_i^{p'}, K_i^{s'}))$, 傳至 NOR。

NOR：

當 KDC 收到 M_{13} 後，會驗證 $Sig_{K_k^s}(E_{K_i^p}(K_i^{p'}, K_i^{s'}))$ 與 $H(UID_i, KID_k \oplus T_s)$ 之正確性，此時 NOR 確認拿到 U_i 的新金鑰對。

14、*NOR*→U_i：

當 NOR 拿到 U_i 的新金鑰對後，會通知 U_i 。首先，NOR 針對新的金鑰對作簽章得到 $Sig_{K_n^s}(E_{K_i^p}(K_i^{p'}, K_i^{s'}))$，爾後計算雜湊值 $H(s_i^u \oplus T_s)$。最後將上述兩個訊息與 NID_n 、$E_{K_i^p}(K_i^{p'}, K_i^{s'})$ 打包成訊息 $M_{14} = \{NID_n, E_{K_i^p}(K_i^{p'}, K_i^{s'}), Sig_{K_n^s}(E_{K_i^p}(K_i^{p'}, K_i^{s'})), H(s_i^u \oplus T_s)), T_s\}$ 送至 U_i 。

U_i：

當 U_i 接收到 M_{14} 後，會解密出 $E_{K_i^p}(K_i^{p'}, K_i^{s'})$ 並驗證 $Sig_{K_n^s}(E_{K_i^p}(K_i^{p'}, K_i^{s'}))$ $H(s_i^u \oplus T_s)$ 之正確性。最終，U_i 更新了新的金鑰對，完成了所有程序。

肆、安全性分析

在這章節，將描述我們的機制如何抵抗竊聽攻擊、替換攻擊、中間人攻擊及偽造攻擊，我們假設 NOR 及 KDC 都是安全且不會受到攻擊。

一、Eavesdropping attack 竊聽攻擊

竊聽攻擊為攻擊者攔截私密通道的即時訊息並分析其封包，但不會竄改該封包。然

而，我們機制中所有單位互相傳遞的訊息都是經過加密的，即便被有心人士攔截了封包，也無法找到相對應的私鑰解開該訊息。故攻擊者無法以竊聽攻擊對本機制造成影響。

二、Replay attack 替換攻擊

替換攻擊為攻擊者攔截兩個單位間傳輸的封包，在竄改該封包後送至接收方單位。在本機制中，所有傳輸的訊息都帶有時間戳，而時間戳必須由相對應的接收者在一定時間內驗證；若攻擊者攔截封包並竄改，則此次通訊會失效，且會被偵測出來。

三、Man-in-the-middle attack 中間人攻擊

中間人攻擊指的是攻擊者攔截訊息並分別對收送雙方建立通道以控制兩方所傳遞的訊息。在本機制中，採用了非對稱式加密演算法對傳遞的訊息加密，且只有收送雙方持有相同的秘密值。攻擊者在攔截訊息後，因為無法得知該秘密值故無法解開該訊息。

四、Forgery attack 偽造攻擊

偽造攻擊為攻擊者截取舊有的認證訊息且重新產生一個新的認證訊息，以喬裝成合法使用者來得到合法的認證。若攻擊者截取傳遞至 NOR 的認證訊息並享偽裝成合法公司或使用者，由於所傳遞的訊息有經過加密且使用秘密值產生雜湊值，攻擊者無法解密該訊息，也因為沒有秘密值而無法產生新的訊息，故無法喬裝成公司或使用者。只有合法的公司及使用者能驗證成功，攻擊者無法偽造。

伍、結論

因應醫療保健相關記錄的重要性，我們提出了一個支援長期檢驗電子健康記錄管理之身份識別與授權機制來確保每個人自身的歷史健康相關記錄在一生都是有效的。為了達到此目的，我們使用了累積公證式簽章、驗證機制以及授權機制，並可以抵制竊聽攻擊、替換攻擊、中間人攻擊及偽造攻擊。本文的貢獻為利用可信賴之公正第三方與 PKR 加密系統使得 HER 能夠長期且安全地被保存著；此外，還達到了完整性、不可否認性、真實性及真實性，並能讓使用者決定自己的記錄移轉至任何的合法單位。

致謝

本文為科技部補助的研究計畫(MOST 103-2221-E-011-091-MY2 、MOST 104-2119-M-011-003、MOST 104-2923-E-011-005-MY3)成果之一部分，特此致謝。

參考文獻

[1] J. Akinyele, M. Pagano, Encryption on Mobile Devices," *SPSM '11 Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices,* pp. 75-86, Oct. 2011.

[2] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," *CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security,* pp. 103-114, 2009.

[3] P. Burnap, I. Spasić , W. Gray, J. Hilton, O. Rana, and G. Elwyn, "Protecting Patient Privacy in Distributed Collaborative Healthcare Environments by Retaining Access Control of Shared Information," *International Conference on Collaboration Technologies and Systems (CTS),* pp. 490 - 497, May 2012.

[4] K. Chen, Y. Chang, and D. Wang, "Aspect-oriented design and implementation of adaptable access control for Electronic Medical Record," *International journal of medical informatics,* pp. 181-203, 2010.

[5] T. Gondrom, R. Brandner, and U. Pordesch, "Evidence record syntax (ERS) ", http://www.ietf.org/rfc/rfc4998.txt.

[6] L. Guo, C. Zhang , J. Sun , and Y.Fang, "A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks," *IEEE Transactions on Mobile Computing,* vol. 13, pp. 1927 – 1941, 2014.

[7] Health Insurance Portability and Accountability Act (HIPAA), http://health.state.tn.us/hipaa/

[8] T. Hyla, I. Fray, W. Mac´ko´w,J. Pejas´, "Long-term preservation of digital signatures for multiple groups of related documents," *Information Security, IET ,*vol. 6, pp. 219 – 227, 2012.

[9] J. Jin, G. Ahn, M. Covington, and X. Zhang, "Access Control Model for Sharing Composite Electronic Health Records," *Collaborative Computing: Networking, Applications and Worksharing, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering,* vol.10, pp. 340-354, 2009.

[10] F. Khan, A. Ali, H. Abbas, and N. Haldar, "A cloud-based healthcare framework for security

and patients' data privacy using wireless body area networks," *Procedia Computer Science,* vol. 34, pp. 511–517, 2014.

[11] T. Lee, "Verifier-based three-party authentication schemes using extended chaotic maps for data exchange in Telecare medicine information systems," *Journal of Medical Systems* , April 2014.

[12] D. Lekkas, D. Gritzalis, "Cumulative notarization for long-term preservation of digital signatures," *Computers & Security,* vol. 23,pp. 413–424, July 2004.

[13] D. Lekkas and D. Gritzalis, "Long-term verifiability of the electronic healthcare records' authenticity," *International Journal of Medical Informatics,* vol. 76, pp. 442-448, May/June 2007.

[14] S. Narayan, M. Gagné and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-based Infrastructure," *Proceedings of the 2nd ACM Cloud Computing Security Workshop,* Oct. 8, 2010.

[15] PKI, ftp://ftp.rsa.com/pub/pdfs/understanding_pki.pdf

[16] P. Ruotsalainena, and B. Manningb, "A notary archive model for secure preservation and distribution of electrically signed patient documents," *International Journal of Medical Informatics,* vol. 76, pp. 449–453, May–June 2007.

[17] S. Sabnis and D. Charles, "Opportunities and challenges: Security in eHealth," *Bell Labs Technical Journal,* vol. 17 , pp. 105–112, 2012.

[18] M. Shin, S. Yoo, K. Lee , D. Lee, "Electronic Medical Records privacy preservation through k-anonymity clustering method," *Joint 6th International Conference on Soft Computing and Intelligent Systems (SCIS) and 13th International Symposium on Advanced Intelligent Systems (ISIS),*pp. 1119 – 1124, 2012.

[19] A. Tamersoy, G. Loukides, M. Nergiz, Y. Saygin, and B. Malin, "Anonymization of Longitudinal Electronic Medical Records," *IEEE Transactions on Information Technology in Biomedicine,* vol. 16, pp. 413 – 423, 2012.

[20] C. Troncoso, D. D. Cock, B. Preneel, "Improving Secure Long-Term Archival of Digitally Signed Documents," *StorageSS'08 Proceedings of the 4th ACM international workshop on Storage security and survivability,* pp. 27-36, 2008.

[21] A. Uherek, S. Maier, U. Borghoff, "An Approach for Long-Term Preservation of Digital Videos based on the Extensible MPEG-4 Textual Format," *International Conference on Collaboration Technologies and Systems (CTS),* pp. 324 - 329, May 2014.

[22] M. Vigil, D. Cabarcas, J. Buchmann, and J. Huang, "Assessing trust in the long-term protection of documents," *IEEE Symposium on Computers and Communications (ISCC),* pp. 185-191, 2013.

[23] M. Vigila, J. Buchmanna, D. Cabarcasb, C. Weinerta, A. Wiesmaierc, “Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: A survey,” *Computers & Security,* vol. 50,pp. 16–32, May 2015.

[24] J. Zhou, X. Lin, X. Dong, and Z. Cao, “PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System," *IEEE Transactions on Parallel and Distributed Systems,* vol. 26, pp. 1693-1703, 2014.

[25] https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.01_60/ts_101903v010401p.pdf (2009/6).

[26] https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/01.08.03_60/ts_101733v010803p.pdf (2011/1).