行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※　　　網路銀行交易事項的不可否認服務之研究　　　※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：¦**個別型計畫**　　æ**整合型計畫**
計畫編號：NSC 89－2416－H－009－038－
執行期間：　89 **年**　08 **月**　01 **日至**　90 **年**　07 **月**　31 **日**

計畫主持人：　黃景彰
共同主持人：

本成果報告包括以下應繳交之附件：
□**赴國外出差或研習心得報告一份**
□**赴大陸地區出差或研習心得報告一份**
□**出席國際學術會議心得報告及發表之論文各一份**
□**國際合作研究計畫國外研究報告書一份**

執行單位：　國立交通大學資訊管理研究所

中　華　民　國　　　年　　　月　　　日

行政院國家科學委員會專題研究計畫成果報告
網路銀行交易事項的不可否認服務之研究

計畫編號：NSC 89－2416－H－009－038－
執行期限：89 年 8 月 1 日至 90 年 7 月 31 日
主持人：黃景彰
計畫參與人員：沈曉芸、邵敏華（研究生）
執行機構及單位名稱：交大資管所

一、中文摘要

面對數位化的交易模式，可被信賴的安全環境已成為網路商務成功發展的關鍵因素，此外，建立一個能夠解決電子商業行為糾紛的機制，更是博取消費者信心的重要課題。事件發生的不可否認服務即是支援爭議解決的機制。本計畫探討不可否認服務的相關國際標準與文獻，研究國內網路銀行的交易活動與流程，並以轉帳、付款交易事項為主，建議此種作業環境所需使用的證據、證據的內涵與其產生、傳遞、儲存與使用的過程，將不可否認服務的機制納入網路銀行的交易活動。

關鍵詞：網路銀行、不可否認服務、資訊安全、爭議解決

Abstract

Creating a secure transaction environment is a critical factor for successful e-commerce. In addition to implementing secure fraud prevention techniques, dispute resolution systems should be developed to provide non-repudiation services. In this research, the authors offer solutions to meet demand on non-repudiation for the network banking business. The authors have surveyed the current network banking business and international standards on the subject of non-repudiation services. Also, the authors have chosen adequate standard as a base to design the contents of evidence and to design the procedure to create, collect, and apply the evidence in non-repudiation services.

Keywords: Internet banking, non-repudiation, information security, dispute resolution

二、緣由與目的

隨著網路社會的興起，網際網路已成為各種商業活動與應用的媒介，金融服務可說是最適合網路交易的行業之一。以網路銀行為例，根據 IDC 的調查預測，至公元 2004 年時，美國網路銀行的用戶將可達到 2280 萬人，而 Datamonitor 的研究報告則指出，歐洲網路銀行的用戶數可望在 2005 年成長至 7500 萬人 (章志彬，民 89；陳怡伶，民 90)，也因此，銀行產業正積極投入網路銀行業務，提高網路服務的品質，以迎合不可逆轉的時代趨勢。

然而，如同其他網路交易，網路銀行最為客戶所關切的問題，就是安全問題。為此，我國財政部 (民 88) 已發佈「金融機構辦理電子銀行業務安全控管作業基準」，規範電子銀行交易與管理層面中安全的需求，以保障金融機構透過各種電子及通訊設備與客戶業往來的安全。此外，在數位化的環境中進行商業活動，必須建立適當的規範與機制，以解決商業行為可能發生的紛爭，提昇消費者利用電子商務的信心。

而為解決交易的糾紛，必須引用能夠證明事件發生的真實性的「證據」，以為仲裁的依據；因此，建立一個可以產生、蒐集、記錄交易證據，並確保證據的可用性，有能力在糾紛發生時，將證據取出以供仲裁的機制是必須的工作。一般說來，證據是用來證明事件是否曾經發生的資訊，使得參與事件的當事人無法否認他的行為，故一系列證據處理的工作，即稱之為事件的不可否認服務 (non-repudiation)。

本計劃的主要目的即在於探討不可否認服務的相關文獻、相關的國際標準與網路銀行的業務，將不可否認服務機制納入網路銀行的交易活動中，研究此種作業環境所需用的證據，與證據處理的過程。

三、文獻探討

1. 相關國際標準

國際標準組織 (International Organization for Standardization, ISO) 與國際電工協會 (International Electrotechnical Commission ,IEC) 制定的標準文件 ISO/IEC 10181-4 (ISO/IEC JTC 1, 1997a) 自證據處理的角度出發，將事件發生的不可否認服務分為四個階段：

(1) 證據產生階段：為證明特定事件的發生，可以由事件參與的當事人或是要求公正的、被信賴的第三者 (Trusted Third Party (TTP)) 負責產生證據。

(2) 證據的儲存、傳遞與取用：主要是處理已產生的證據，包括證據的儲存與傳遞。例如，由證據的產生者將證據傳遞至證據的保管處，或是傳遞給證據的檢驗者；另外，也可能是在日後由請求產生證據的當事人取用已儲存的證據。

(3) 檢驗證據的階段：在必要時，使用證據的個人或團體可以要求檢驗證據，以證明使用的證據是值得信賴的。如此一來，證據的使用者可以獲得信心，相信爭議發生時，可以提出具有可信度的證據。

(4) 爭議解決階段：不可否認服務的關鍵任務即是要能支援爭議的解決。當爭議發生時，仲裁者自原告、被告、或被信賴的公正機關蒐集證據，並依據仲裁政策來解決爭議，或者，爭議的雙方也可以自行引用證據來處理，不一定會需要仲裁者的介入。這個工作階段的作法與法制環境有相當程度的關係，較沒有標準的程序可以依循。

此外，在 ISO/IEC 13888-1 (ISO/IEC JTC 1, 1997b) 標準文件中，則定義了網路上訊息往來所需要產生的證據，以支援不同類型的不可否認服務。

- 來源證明 (proof of origin)：用來證明訊息是由誰建立與傳送的, 以反制發文者否認訊息來源
- 送達證明 (proof of delivery)：用來反制訊息的接收者在收到訊息並獲知訊息的內容後卻加以否認。
- 送件證明 (proof of submission)：在某些商業活動的訊息傳遞系統中，可以透過一個訊息的傳遞機構負責在交易的雙方之間傳遞訊息，因此必須提供適當的證據，以防止傳遞機構否認其曾經接受訊息傳遞要求的事實。
- 傳遞證明 (proof of transport)：當傳遞機構確實協助訊息傳遞之後，必須建立適當的證據，以證明傳遞機構已將訊息傳遞給訊息接收者。因此，傳遞證明可用來反制傳遞機構否認他已經送出訊息給接收方。
- 轉送證明 ((proof of transfer)：若有二個或更多的傳遞機構介入訊息的傳遞過程時，其中一個機構接收到前一個傳遞機構轉送來的訊息，他有必要產生轉送證明，並交付給前一機構，以證明自已確實接受了傳送訊息的工作，而無法否認曾經接收其他傳遞機構所轉送的訊息。

送件證明與傳遞證明僅適用於有傳遞機構 (delivery authority) 協助訊息傳遞的環境，另外，如果有二個或多個傳遞機構介入訊息傳遞的過程，則會有轉送證明的需要。

而證據中的事實陳述至少應包涵所依循的安全政策、證據的類型、證據當事人的唯一識別、證據產生者的唯一識別、事件發生與產生證據的日期與時間、以及訊息的本身與簽章等。

2. 事件不可否認服務協定

本節主要探討目前已提出的一些不可否認服務機制與協定。根據 ISO/IEC 13888(ISO/IEC JTC 1,1997) 系列標準文件，分別以對稱式與非對稱性密碼方法來建構不可否認服務的機制；此外，依據可信賴的第三者參與的方式與其扮演的角色，也有不同的協定設計。

一般來說，在使用公開金鑰密碼系統的環境中，證據的當事人可以使用他的私密金鑰 (private key) 產生簽章式證據，如所示，但是，此協定無法強制收文方產生送達證明，而不具有「公平」(fairness) 的性質。此外，金鑰的真實性與有效性必須被保證，憑證機構 (CA) 或目錄伺服器即扮演一輔助性的 off-line TTP，他們以離線作業的方式提供不可否認服務所需要的資訊。許多相關研究都是將不可否認服務的工作建立在使用公開金鑰密碼方法的環境中，並藉由 TTP 的參與達成「公平」的要求 (Coffey & Saidha; ISO/IEC JTC 1, 1997d; Zhou & Gollmann, 1997a, 1997b; You, Zhou, & Lam, 1998)。

而在使用對稱式密碼學架構的限制下，產生及驗證證據 on-line TTP 是必要的，產生證據與驗證證據的 TTP 可以是同一者，也可以是不同的二個機構。在這一類型的機制中，證據的當事人與證據的產生者之間共享一把秘密金鑰 (secret key)，而證據的驗證者與證據使用者之間共享另一把秘密金鑰；如果證據產生者與驗證者非為同一人時，他們彼此之間也會共享一把秘密金鑰。

此外，如果進行商業交易的雙方之間欠缺信任，或者溝通不便時，也可以採用完全依賴 TTP 介入的 in-line 模式 (Coffey & Saidha, 1996; ISO/IEC JTC 1, 1997c)，有 in-line TTP 參與的爭議解決機制並沒有限定在特殊的密碼學應用環中建構，事實上，不論是使用非對稱式或對稱式密碼學方法的應用系統，皆可能會有 on-line 或 in-line TTP 參與其中。

四、研究成果與討論

1. 網路銀行交易事項

我國財政部 (民 88) 發佈之「金融機構辦理電子銀行業務安全控管作業基準」，規範電子銀行交易與管理層面中安全的需求，以保障金融機構透過各種電子及通訊設與客戶業往來的安全。根據「金融機構辦理電子銀行業務安全控管作業基準」對電子銀行的業務分類，網路銀行的交易類別可概分為二種：(1) 電子轉帳及交易指示類 —— 係指與資金移轉有關或直接影響客戶權益之服務項目，例如，轉帳、付款、及網路交易等， (2) 非電子轉帳及交易指示類 —— 指與資金移轉無關或不直接影響客戶權益之服務項目，如申請服務、查詢服務及金融財經資訊的提供等。依業務性質，其交易安全的需求亦有所不同，電子轉帳及交易指示類應確保訊息的隱密性 (confidentiality)、真確性 (integrity)、來源辨識 (original authentication)、不可重複性、與無法否認訊息的傳送與接收。

目前，國內網路銀行所採用的安全機制分為 SET (Secure Electronic Transaction)、Non-SET、SSL (Secure Sockets Layer) 三類。使用 SET 機制，用戶

表 1 網路銀行交易安全機制使用情形

交易類別 / 安全機制	非電子轉帳及交易指示類	電子轉帳及交易指示類	
		低風險性	高風險性
SSL	Í	Í	Č
SET	Í	Í	Í
Non-SET	Í	Í	Í

必須以銀行帳號為基礎申請電子憑證 (即每一帳號需要一張憑證)，並安裝電子錢包； Non-SET 機制是由銀行業者自行建置的交易系統，用戶申請以身分證字號或公司統一編號為基礎的電子憑證，配合客戶端安控程式使用，必須同時使用電子憑證金鑰及密碼，才可進行交易；而 SSL 機制，則不需申請電子憑證，直接以用戶身分證字號、網路代碼、網路通行碼為權限，進入網路銀行系統。依據交易事項，各類安全機制使用情形如表 1 所示。在此表中的「低風險性」交易係指同戶名或約定轉入帳戶、或非約定轉入帳戶小金額 (以每戶每筆不超過五萬元、每日最高十萬元、每月累積不超過二十萬元為限) 之各類電子轉帳。財政部乃是於 89 年 8 月方才開放金融機構可以採用 128 bits 以上 SSL 版本，從事此類型的交易。

2. 不可否認服務機制之設計

根據對網路銀行交易事項的討論，本研究以即時轉帳、預約轉帳、與付款類的交易活動為主，探討使用不同安全交易機制時，不可否認服務機制的設計原則。

依據個人電腦銀行業務及網路銀行業務服務契約範本 (財政部，民 88 年) 第十六條指出：「雙方應保存所有含數位簽章之電子訊息及經由網路所提供相關電子訊息之紀錄，並應確保紀錄之真實性及完整性。客戶如未保存者，推定以銀行所保存之紀錄為真正。」又，在第十七條中則註明電子訊息可為仲裁爭議的效力：「雙方同意依本契約交換之電子訊息，其效力與書面文件相同，雙方就所生之任何糾紛，於審判、仲裁、調解或其他法定爭議處理程序中，均不得主張該電子訊息不具書面或簽名要件而歸於無效或不成立。於前項之審判、仲裁、調解或其他法定爭議程序中，雙方同意相關之訊息推定以銀行保存之電子訊息紀錄證明之。銀行不得拒絕提供。」

也就是說，在使用 SET/Non-SET 安全機制時，交易雙方是以契約簽訂的方式，強制電子簽章的效力，並經由此達成事件發生的不可否認性。其證據的處理與傳遞方式如圖 1 所示。

「交易訊息」中所表達的為客戶所要求的交易事項。舉例來說，一個轉帳交易訊息至少應具備轉帳型態、轉出帳號、轉入帳號、轉帳日期、轉帳金額與交易序號等資訊。「交易要求」為用戶端 (C) 所建立傳送的來源證據。

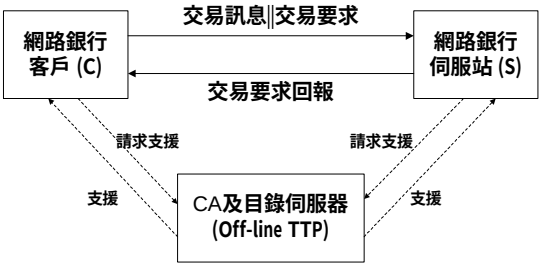

圖 1 不可否認服務模型 — 使用於 SET/Non-SET

表 2交易要求 (來源證明) 的內涵

資料項目	內涵	符號
證據類型	交易要求	f_O
訊息發送方唯一識別	A123456789 王小明	C
訊息接收者唯一識別	XX Bank 網路銀行系統	S
訊息發送時間	2001/01/05 10:00	T_1
證據建立時間	2001/01/05 09:00	T_{g1}
SGN(交易訊息)	交易訊息 (m) 的簽章	SGN(m)

若將「交易要求」以符號表示，則為 $z_C \parallel SGN_C(z_C)$。 z_C 為事實的陳述，$SGN_C(z_C)$ 表示 z_C 的數位簽章，$\parallel$ 則是連結的意思。其中，z_C 應具備的資料項目為 {證據的類型，證據當事人的唯一識別，訊息傳送的時間、證據產生的時間、SGN_C(交易訊息)}。即，

$$z_C = \langle f_O, S, C, T_1, T_{g1}, SGN(m) \rangle$$

當銀行伺服端 (S) 收到交易要求後，驗證用戶端的簽章，確認之後，建立「交易要求回報」作為網路銀行端 (S) 送達證明，傳送給用戶端。「交易要求回報」= $z_S \parallel SGN_S(z_S)$，其中，

$$z_S = \langle f_R, S, C, T_1, T_2, T_{g2}, m^*, SGN(m^*) \rangle$$

其中，f_R 表示送達證明、T_1 為用戶端執行時間、T_2 為伺服端執行時間、T_{g2} 為證據產生的時間、m^* 表示交易訊息。與前述交易訊息內涵不同之處在於，m^* 可以加入轉帳成功的通知與帳戶餘額等相關資訊。如果此筆轉帳交易的類型為「預約轉帳」，則 $m^* = m$。

至於使用 SSL 機制從事低風險性的交易 (也就是金額較低的交易) 時，並沒有強制達成「無法否認傳送/ 接收訊息」的安全需求。但是，電子商務交易有許多小額交易的情形，這一類的交易不表示不會發生糾紛。故本研究認為，即使是低風險性的交易，仍應提供適當的不可否認服務與爭議解決的機制，如此方能建構實際的商業環境，並建立消費者或企業跨區域交易的信心。為了在以 SSL 機制為基礎的交易環境中，建立有效率的爭議解決機制，本研究提出一個與 Online ADR (Online Alternative Dispute Resolution) 結合的不可否認服務模型，如圖 2。

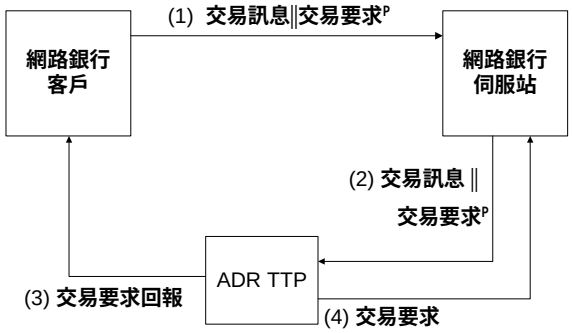

圖 2 不可否認服務模型 — 使用於 SSL 機制

On ADR **是由非法庭但公正的第三者透過網路，以調解、仲裁等多樣化的方式，為企業或個人解決因電子商業交易行為所發生的紛爭** (GBDe, 2000; Katsh, 2001)**；由於不必進入法院的訴訟程序，故可節省時間及金錢的成本。本研究將產生證據的** TTP **與** Online ADR **業者二者的角色相互結合，由** ADR **業者提供建立證據的服務，圖** 2 **為本研究建議的不可否認服務模型。**

在這個模型中，三方的連線都受到 SSL **的保護，以保持資訊的機密性與真確性。此外，以** ADR/TTP **的簽章產生來源與送達證明，確保證據的效力。其運作流程如下所述：**

(1) **客戶端提出交易要求，傳送交易訊息** m **及** z_C，z_C = 〈f_O, S, C, T_1〉，**其中，**T_1 **為交易訊息的時間**

(2) **銀行端收到交易要求後，傳送** m ‖ z_C ‖ SGNS(m, z_C) **給** ADR/TTP**，請求產生「交易要求」。**

(3) ADR/TTP **檢驗銀行的簽章後，產生「交易要求」**(**來源證明**) **與「交易要求回報」**(**送達證明**)**，並將「交易要求回報」傳給客戶端。交易要求回報的內涵為** $z2_{TTP}$ ‖ $SGN_{TTP}(z2_{TTP})$ **，此時，**$z2_{TTP}$ = 〈f_R, S, C, TTP, T_1, T_2, T_{g2}, m, SGN_{TTP}(m)〉**；而交易要求** = $z1_{TTP}$ ‖ $SGN_{TTP}(z1_{TTP})$**，**$z1_{TTP}$ =〈f_O, S, C, TTP, T_1, T_2, T_{g1}，SGN_{TTP}(m)〉。

(4) ADR/TTP **回傳「交易要求」給銀行伺服端。**

經由本研究所提出的模型，即使使用安全性較低的 SSL **機制，仍可提供交易事項的不可否認服務。**

3. 結論與討論

網路銀行是一個有效率且低成本的金融服務通道，銀行業者莫不積極投入，如何建構安全、私密與可信任的應用系統，將成為客戶使用網路銀行的重要考量。除了符合高標準的資訊安全技術外，建構一套法庭之外的公平便利的爭議解決機制，將有助於提昇客戶的信心，也有利於銀行業務的拓展。尤其是，安全無法全然仰賴艱困的技術，而必須能與其他制度互相搭配，才能夠創造真正的價值。

本研究自技術的觀點出發，探討爭議解決機制中，證據處理的過程與方法，並以網路銀行的轉帳、付款交易事項為應用環境，設計證據的內涵與證據處理的流程，將不可否認服務的機制納入其中。事實上，不可否認服務並非只具有技術上的特質，還牽涉到法律上的架構，線上替代性爭議解決機制即具有相當程度的法律意涵，在本研究中，也以不可否認服務的機制作為 Online ADR **解決紛爭的基礎，以期在不同的密碼學應用與商業環境中，均能建構出一個公平、有效率的電子交易的爭議解決機制。**

五、計畫成果自評

本計畫的研究方向與研究方法與原計畫建議書所提相當一致，在研究成果方面，也達成預期的目標 —— 研究不可否認服務之理論 (包含國際標準與學術文獻)，並提出網路銀行交易事項不可否認服務的可能解決方法，及適當的運作模型，作為我國構建網路銀行系統所需的不可否認服務機制之參考。如此，相信可提昇社會大眾對於網路銀行安全性的瞭解與信賴，創造市場的新機會，更有助於我國推行金融電子化商務的成功發展。

此外，為建立消費者信心，美國聯邦貿易委員會 (Federal Trade Commission, FTC)**、全球電子商務論壇** (Global Business Dialogue on Electronic Commerce, GBDe)**、經濟合作發展組織** (The Organization for Economic Co-operation and Development, OECD)**、美國仲裁協會** (American Arbitration Association, AAA)**、及美國律師協會** (American Bar Association) **等組織正積極支持並推動線上替代性爭議解決機制** (Online Alternative Dispute Resolution, ADR) **的發展** (FTC/DOC, 2000；GBDe, 2000；OECD, 2001)**，以期在法庭之外，解決因商業行為而產生的紛爭。本研究將繼續深入研究** Online ADR **的運作程序，以期建立更完整的爭議機制系統模型。**

在本計畫進行過程中，也已深入研究國際標準，以此為基礎，整合出不可否認服務的一般化模型，撰寫一學術論文(註 1)**，投稿至資訊管理學報，現已通過初步之審查，小幅度修改後，進行第二次的審查中。**

[**註** 1] **黃景彰、沈曉芸**. (**民** 90 **年**). **電子商業交易之爭議解決機制**. 資訊管理學報, **審查中**.

六、參考文獻

財政部金融局，(民 88 年)，個人電腦銀行業務及網路銀行業務服務契約範本。於民國 89 年 4 月 25 日，由 http://www.boma.gov.tw/8872563-1.htm 取得。

財政部金融局，(民 89 年)，金融機構辦理電子銀行業務安全控管作業基準。八十九年度金融法規，由 http://www.boma.gov.tw/index_dir02.htm 取得。

陳怡伶，(民 90 年 8 月)，歐洲 2005 年網路銀行用戶數將逾 7,500 萬人。於民國 90 年 9 月 5 日，由 http://www.find.org.tw/0105/news/0105_news_disp.asp?news_id=1675 取得。

章志彬，(民 89 年 7 月)，網路銀行競爭激烈 服務觀念將成致勝關鍵。於民國 90 年 7 月 25 日，由 http://www.e21times.com/ei/fortune.asp?rtid=2964&sid=27 取得。

American Bar Association Task Force on E-commerce & Alternative Dispute Resolution. (2001). Draft Preliminary Report & Concept Paper. Retrieved August 18 ,2001, from the World Wide Web: http://www.law.washington.edu/ABA-eADR

Coffey, T., & Saidha, P. (1996). Non-repudiation with mandatory proof of receipt. Computer Communication Review, 26(1), 6-17.

FTC/DOC. (2000). Summary of public workshop: Alternative dispute resolution for consumer transactions in the borderless online marketplace. Retrieved May 25, 2001, from the World Wide Web: http://www.ftc.gov/bcp/altdisresolution/index.htm

GBDe. (2000). Alternative dispute resolution. Retrieved May 15, 2001, from the World Wide Web: http://www.ftc.gov/bcp/altdisresolution/index.htm

ISO/IEC JTC 1. (1997a). Information technology – Open systems interconnection – Security frameworks for open systems: Non-repudiation framework (ISO/IEC 10181-4).

ISO/IEC JTC 1. (1997b). Information technology – Security techniques – Non-repudiation – Part1: General. (ISO/IEC 13888-1).

ISO/IEC JTC 1. (1997c). Information technology – Security techniques – Non-repudiation – Part2: Mechanisms using symmetric techniques. (ISO/IEC 13888-2).

ISO/IEC JTC 1. (1997d). Information technology – Security techniques – Non-repudiation – Part1: Mechanisms using asymmetric techniques. (ISO/IEC 13888-3).

Katsh, E. (2001).Online dispute resolution as a solution to cross-border e-disputes: An introduction to ODR. Retrieved July 25, 2001, from the World Wide Web: http://www1.oecd.org/dsti/sti/it/secur/act/online_trust/vandenheuvel.pdf

OECD. (2001). Building trust in the online environment: Business to consumer dispute resolution. Retrieved July 25, 2001, from the World Wide Web: http://www1.oecd.org/dsti/sti/it/secur/act/Online_trust/documents.htm

You, C. H., Zhou, J., &Lam, K. Y. (1998). On the efficient implementation of fair non-repudiation. Computer Communication Review, 28(5), 50-60.

Zhou, J., & Gollmann, D. (1997a). Evidence and non-repudiation. Journal of Network and Computer Applications, 20(3), 267-281.

Zhou, J., & Gollmann, D. (1997b). An efficient non-repudiation protocol. Proceedings of 10th IEEE Computer Security Foundations Workshop, 126-132.