網路銀行多行帳戶整合模式之研究

A Study on Account Aggregation for Multiple Internet Banking

黃明達
Ming-Dar Hwang

淡江大學資訊管理系副教授兼資訊中心主任
Associate Professor of Information Management Department
& Director of Information Processing Center, TamKang University
mdhwang@mail.tku.edu.tw

摘　　要

從網路銀行（Internet Banking），如美國 Citibank 銀行的 MyCiti 網路銀行，客戶可以透過單一登入（Single Sign-on）來獲知 Citibank 及非屬於 Citibank 的帳戶餘額、交易明細、整合式投資資訊、整合式 Email 訊息、整合式紅利等資訊。反觀台灣的網路銀行，客戶只能擁有單一金融機構或及其關係企業金融機構的帳戶整合（Account Aggregation），而尚未擁有不同銀行，亦即多行，帳戶整合的功能。本論文乃針對台灣金融環境，希望探討出可行的多行帳戶整合的模式。

本研究以模式闡述研究方法，分析網路銀行中，欲進行多行帳戶整合功能時，可能會有那些可行模式。研究中，計列出八種可行模式，並分析其優點、缺點、及安全性等。當安全性及隱私性為主要考量時，本研究所提之運用 PKI（Public Key Infrastructure, 公開鑰基礎建設）環境的 Web-PKI 法及 Agent-PKI 法，應為未來進行帳戶整合功能時，較為可行的模式。

關鍵字：網路銀行，帳戶整合，公開鑰基礎建設。

Abstract

From the internet banking, such as the MyCiti internet banking of Citibank, customers could retrieve the information of account balances, transaction details, integrated investment messages, integrated Email messages, integrated bonuses of Citibank and non-Citibank by single sign-on.

But, from the internet banking of Taiwan, customers can only retrieve the integrated financial information of a single financial institution or add more with other financial institutions of their related enterprises. The Internet banking of Taiwan still has no the functions of account aggregation for multiple internet banking. This paper wishes to find out the feasible models of account aggregation for multiple internet banking against Taiwan financial environment.

This study uses the model description method to analyze the feasible models of account aggregation for multiple internet banking. This paper gives eight feasible models, and their advantages, disadvantages, and security were analyzed. As the security and privacy are major concern, then the proposed Web-PKI and Agent-PKI model could be more feasible models to apply to the account aggregation functions.

Keywords: Internet Banking, Account Aggregation, PKI (Public Key Infrastructure)

壹、緒　論

一、研究動機

於網路銀行（Internet Banking），將相同或不同金融機構（Financial Institution）的多種業務整合，以供查詢，於國外，已行之多年（Coulter 2001）。譬如於美國 Citibank 銀行的 MyCiti 網路銀行網站（網址爲 http://www.myciti.com/），可以透過單一登入（Single Sign-on）來獲知 Citibank 及非屬於 Citibank 的帳戶餘額、交易明細、整合式投資資訊、整合式 Email 訊息、整合式紅利等資訊。

反觀國內的網路銀行，只能擁有單一金融機構或及其關係企業金融機構的帳戶整合，而尚未擁有不同銀行，亦即多行，帳戶整合的功能。譬如台灣的建華銀行（原爲華信銀行，其網址爲 http://www.banksinopac.com.tw/ ）的 MMA（Money Management Account，投資管理帳戶）客戶，可以透過建華銀行網站，快速查詢建華銀行存放款餘額、建華證券股票庫存及市值、建華銀行所發行信用卡消費金額、建華銀行所銷售基金淨值等建華銀行相關企業的整合性帳戶資訊，而尚未擁有多行（譬如建華銀行與華南銀行）帳戶整合的功能。對一般客戶（可能爲個人或公司）而言，可能會因地點的方便性或業務的須要性等因素，而在多個不同銀行開戶。如此，當客戶欲查詢各銀行的帳戶餘額或交易明細時，必須分別登入於各銀行網站方可。

登入網路銀行網站時，一般皆會要求客戶輸入如使用者名稱、密碼、…等資料。對客戶而言，每次登入只能看到個別金融機構的資訊，而無法瀏覽到多行的整合性資訊，相當不方便。

本論文乃針對台灣金融環境，希望探討出可行的多行帳戶整合的模式。

二、研究目的

本研究希望能達到下列目的：

- 探討可能的多行帳戶整合模式。
- 分析各模式的優點、缺點、及安全性。
- 由模式中，找出較可行的模式。

三、研究方法

本研究以模式闡述（Description of Model）研究方法（Alavi and Carlsion 1992），分析於網路銀行中，欲於多行之間，進行帳戶整合功能時，可能會有那些可行模式，並由模式中，找出較可行的模式。

四、研究對象

中華民國經濟部技術處所推動的 C（Cash）計畫，其實施期間是從 2001 年 7 月至 2003 年 12 月。全部計有八家銀行加入 C 計畫，其主要目的，除了期望使屬於中小企業的供應商，能夠輕易、快速、以較低利率取得國內銀行的融資，且使用者端（如供應商）也擁有多行帳戶整合的功能。C 計畫預計連結 12 個資訊大廠及近 3,000 家供應商（吳文玲 2002; 林真真 2002; 潘維忠 2002）。

本研究乃針對這八家銀行進行相關研究。於 C 計畫中，作者爲其中四家銀行的主審，主要負責計畫的規劃書審查、每季進度查訪會議的主持、工作項目的監督、調整、與查核等。

本研究建議的較可行模式，有其普及性，所以應可適用於欲加入多行帳戶整合服務的國內任何一家銀行。

貳、文獻探討

一、網路銀行及多行帳戶整合的定義

- **網路銀行**

是指銀行客戶，可透過網際網路，來進行財務帳戶的開戶、存取，與進行財務交易（Coulter 2001; Furst, Lang and Nolle 2000, 2001, 2002）。

- **多行帳戶整合**

於多行帳戶整合（Account Aggregation）環境，可使任何人只須按一下滑鼠按鍵，即可以於單一網頁呈現出跨越於多個網站的所有線上帳戶資訊（方翊人 2001; Coulter 2001; Derkley 2000; Poquette 2000; Pullara 2002; McMahon 2001; Mugavero 2000）。於多行帳戶整合環境，不只是登入（Sign-on）程序的簡化，更重要的，可將資訊加以重組、整合，甚或進行分析，使其呈現出更具附加價值的資訊。

二、網路銀行多行帳戶整合的現況

根據 Forrester Research Inc. 研究，目前已提供多行帳戶整合服務的金融機構有 Citigroup、JP Morgan Chase、Wells Fargo、Morgan Stanley Dean Witter、First Union 等。於 2002 年底前，76%的美國金融機構，可將提供多行帳戶整合的服務。美國的多行帳戶整合市場，目前僅服務約百萬餘的客戶。Morgan Stanley Dean Witter 預估，於 2003 年，將服務 2,200 萬客戶（Coulter 2001）。

三、網路銀行多行帳戶整合的相關研究

網路銀行多行帳戶整合的國外相關研究，可分爲市場調查及研究類（Buhl and Will 1998; Coulter 2001; Merrick 2002; Sciglimpaglia and Ely 2002; Yan and Paradi 1998; Yasin 2000）、功能概述類（Charski 2000; Derkley 2000; Ginovsky 2001; Hackett 2000; Kersnar 2001; Massaro 2000; McMahon 2001; Mearian 2001; Miller 2001; Mugavero 2000; Poquette 2000; Scott 2001; Wagner 2002）、模式概述類（Coulter 2001; O'Brien 2000; Weisul 2000）、風險分析類（Koreto 2002; Robert 2002; Valentine 2001）、及法律層面類（Ferguson 2000; Mugavero 2000; Valentine 2001）。國內相關研究，主要有以 XML 爲基礎的研究類（呂理玄、楊建民 2001; 張子文、楊建民 2001）及法律層面類（方翊人 2001）。各相關領域的研究皆有其貢獻。而有關多行帳戶整合模式的相關研究，於上述文獻中，較相關的爲模式概述類。但這些研究，皆較偏重於模式的簡易描述，並沒有進一步的探討。爲了讓

有興趣於相關研究的學術界、金融界、或第三服務提供者（The Third-Party Service Provider），對多行帳戶整合的可行模式有整體的輪廓，本論文將列出可行的模式，並探討各模式的優點、缺點、及安全性。

參、多行帳戶整合模式

一、現有模式

【模式一】網頁挖取（Screen Scraping）法

爲目前美國金融機構進行多行帳戶整合時，較多使用的方法之一（Coulter 2001; Weisul 2000）。其負責整合服務的公司（一般爲非金融機構，如第三服務提供者，但也可能爲金融機構），或稱整合商（Aggregator），每天（一般是於深夜）會利用一套稱爲挖取器（Screen Scraper）的軟體，自動到客戶的相關金融機構網站，擷取客戶的相關網頁資料（一般是以 HTML 呈現）且儲存之。當客戶欲使用帳戶整合服務時，可採用 Web 方式登入到整合商網站，然後由整合商程式，將已擷取的客戶相關網頁資料整合顯示之，如圖 1。

本論文的圖中，Bi 表示第 i 個金融機構且皆假設有 n 個金融機構參與多行帳戶整合服務。

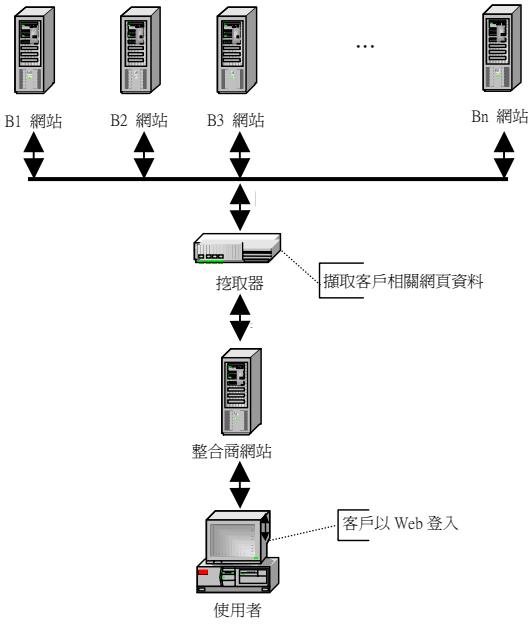

圖 1 網頁挖取法之示意圖。

【優點】

1. 直接由網頁挖取相關資料，而不會存取到金融機構的資料庫，所以較單純。譬如不必事先與金融機構溝通協調、不要修改金融機構的後端程式。
2. 主要在進行網頁瀏覽及資料挖取，所以成本低，較符合成本效益。

【缺點】

1. 由於挖取的資料並非隨時更新，所以整合時，可能屬於非最新資訊。
   或者，當客戶如需要即時更新資訊時，本模式可以改爲，當客戶欲使用

帳戶整合服務，整合商會利用挖取器

2. 相關金融機構網站，擷取客戶的相關網頁資料。於此模式下，客戶須花費到相關網站擷取資料的等待時間。
3. 由於相關金融機構網站的網頁格式可能改變，挖取器如未隨之修改程式，可能擷取到不正確的資訊。
4. 挖取器須擁有著客戶於存取其相關金融機構網站的所有使用者名稱及密碼等，因而產生安全的顧慮。譬如，整合商可能洩露客戶的使用者名稱及密碼，或者，於存取客戶相關網站時，網站無法辨識該存取動作是由客戶本人或挖取器所發出。

軟體，馬上到客戶的

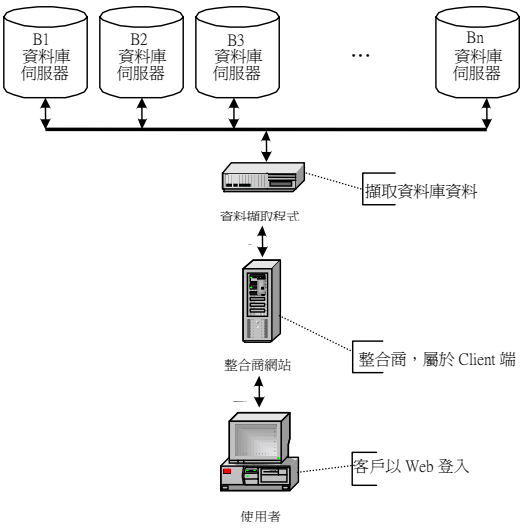

圖 2 OFX 法之示意圖

【模式二】OFX 法

OFX（Open Financial eXchange，開放式金融交換）法，亦爲目前美國金融機構提供多行帳戶整合服務所使用的方法之一（Coulter 2001; O'Brien 2000）。它是採用 Client-Server 架構。Server 端爲金融機構，而 Client 端爲整合商。客戶欲使用帳戶整合服務時，可採用 Web 方式登入到整合商網站，然後由整合商的 Client 端程式，自動到客戶的相關金融機構網站資料庫擷取客戶的相關資料，且整合顯示之，如圖 2。

【優點】

1. Server 端與 Client 端之間，一般會使用 SSL（Secure Sockets Layer，安全槽層）的通信協定，與網頁挖取法比較起來，會有較佳的資訊傳送安全性。
2. 整合商是以直接或間接方式，擷取客戶於金融機構資料庫的相關資料，所以不會有擷取到非最新資訊的困擾。

【缺點】

1. 於提供多行帳戶整合服務前，整合商及金融機構之間，須先簽約，以建立合作夥伴關係。譬如，協調如何提供金融機構資料庫內容給整合商及相關安全措施。
2. 金融機構的 Server 端相關程式，一般須配合各別整合商的 Client 端程式功

能，稍作修改。

4. 商的 Client 端，須擁有著客戶於存取其相關網站的所有使用者名稱及密碼等，因而產生安全的顧慮。譬如，整合商可能洩露客戶的使用者名稱及密碼，或者，於存取客戶相關網站時，網站無法辨識該存取動作是由客戶本人或整合商所發出。

【模式一及模式二綜合分析】

交易的安全性，是金融活動最重要考量因素之一。以下將探討各模式的安全性。

網頁挖取法，一般是由整合商主導，金融機構並未參與運作。由於挖取器儲存著客戶於存取其相關金融機構網站的所有使用者名稱及密碼等，因而整合商的可靠度，是一般客戶考慮是否採用多行帳戶整合功能的最大因素。

OFX 法，是由整合商及金融機構共同參與運作。但整合商的 Client 端，仍須擁有著客戶於存取其相關網站的所有使用者名稱及密碼等，因而仍有安全的顧慮。

模式一及模式二的優點、缺點、及其安全性，如表 1。

3. 整合

表 1　模式一及模式二的優點、缺點、及其安全性

模式 / 項目	網頁挖取法	OFX 法
優點	較單純。符合成本效益。	使用 SSL 安全通信協定。會擷取到最新的資訊。
缺點	資料可能屬於非最新資訊。挖取器如未隨網頁格式之修改來改寫程式，可能擷取到不正確的資訊。挖取器擁有客戶的使用者名稱及密碼。	整合商及金融機構之間須先簽約。金融機構的 Server 端相關程式一般須稍作修改。整合商擁有客戶的使用者名稱及密碼。
安全性	整合商的可靠度，是一般客戶考慮是否採用多行帳戶整合功能的最大因素。	整合商須擁有客戶的使用者名稱及密碼等，因而有安全的顧慮。

二、台灣可採用的建議模式

【模式三】改良式網頁挖取法

如上述，網頁挖取法有其安全顧慮的缺點。本研究的改良式網頁挖取法，Server 端仍爲金融機構，而 Client 端則改爲客戶。客戶欲擁有帳戶整合服務時，須先於本身電腦安裝整合商所提供 Client 端的「代理程式」（Agent）。當要啓用多行帳戶整合服務時，須啓動代理程式，且會自動到客戶的相關金融機構網站擷取客戶的相關網頁資料，然後整合顯示之，如圖 3。

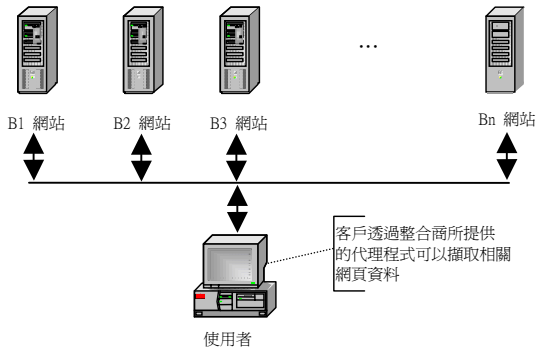

圖 3 改良式網頁挖取法之示意圖。

【優點】

1. 擁有網頁挖取法的所有優點。
2. 客戶於存取其金融機構相關網站的所有使用者名稱及密碼等，是置於客戶端而非整合商，因而較無安全的顧慮。

【缺點】

1. 客戶須先於本身電腦安裝整合商所提供的代理程式。而網頁挖取法只須使用瀏覽器（如微軟公司的 IE）。
2. 客戶須花費到相關網站擷取資料的等待時間。
3. 由於相關金融機構網站的網頁格式可能改變，挖取器如未隨之修改程式，可能擷取到不正確的資訊。

【模式四】改良式 OFX 法

如上述，OFX 法有其安全顧慮的缺點。本研究的改良式 OFX 法，Server 端仍爲金融機構，而 Client 端則改爲客戶。客戶欲擁有帳戶整合服務時，須先於本身電腦安裝整合商所提供的 Client 端代理程式。當要啓用多行帳戶整合服務時，須啓動整合商所提供的代理程式，且會自動到客戶的相關金融機構網站資料庫擷取客戶的相關資料，然後整合顯示之，如圖 4。

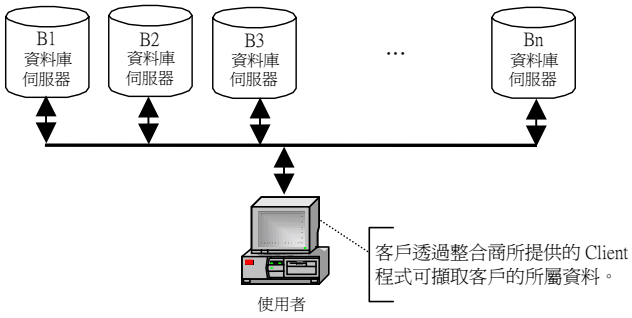

圖 4 改良式 OFX 法之示意圖

【優點】

1. 擁有 OFX 法的所有優點。
2. 客戶於存取其金融機構相關網站的所有使用者名稱及密碼等，是置於客戶端而非整合商，因而較無安全的顧慮。

【缺點】

1. 於提供多行帳戶整合服務前，整合商及金融機構之間，須先簽約，以建立合作夥伴關係。

2. 金融機構的 Server 端相關程式，須配合各別整合商的代理程式功能，稍作修改。
3. 客戶欲擁有帳戶整合服務時，須先於本身電腦安裝整合商所提供的代理程式。而 OFX 法只須使用瀏覽器。

【模式五】Hub 法

由參與多行帳戶整合服務的所有金融機構，共同建置一個整合平台。當客戶欲使用帳戶整合服務時，可採用 Web 方式登入到整合平台，然後由整合平台的程式，自動到客戶的相關金融機構資料庫，擷取客戶的相關資料，且整合顯示之，如圖 5。

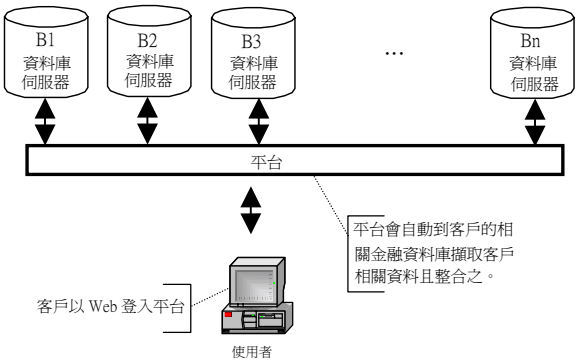

圖 5　Hub 法之示意圖

【優點】

1. 只須建置一個平台，所有參與多行帳戶整合服務的金融機構，皆可共用之，因而可以減少各別金融機構的建置與維護成本。
2. 有了共用平台後，不但可進行多行帳戶整合服務，亦可以提供其他有關多行間的附加價值服務（譬如多行間的徵信服務）。
3. 客戶於存取其相關網站的所有使用者名稱及密碼等，是置於安全控管較嚴密的單一平台端，而非置於整合商，因而可以減少安全的顧慮。

【缺點】

1. 須整合參與多行帳戶整合服務的所有金融機構。但可能由於經營模式、競爭優勢、或商業機密的考量，會導致某些機構不願意加入平台的運作。
2. 平台的擁有機構（Owner）及運作機構（Operator）的權利義務，須明確界定，以保障交易資料的安全性（譬如，運作者不能洩露交易資訊）。
   於台灣金融環境，平台的運作機構可爲財金公司。
3. 於提供多行帳戶整合服務前，所有參與金融機構之間，須先簽約，以建立合作夥伴關係。
4. 各金融機構的 Server 端相關程式，須配合平台端程式功能，稍作修改。
5. 平台端須擁有著客戶於存取其相關網站的所有使用者名稱及密碼等，因而仍然有安全的顧慮。
6. 欲擁有多行帳戶整合服務前，客戶須先到運作機構，進行如開戶的工作。

【模式六】TTP(Trusted Thirty Party)法

當客戶欲使用帳戶整合服務時，可採用 Web 方式登入到金融機構 Bi，然後由 Bi 請求可信任的第三者（如台灣的財金公司）自動到客戶的相關金融機構資料庫，擷取客戶的相關資料，且整合顯示之，如圖 6。

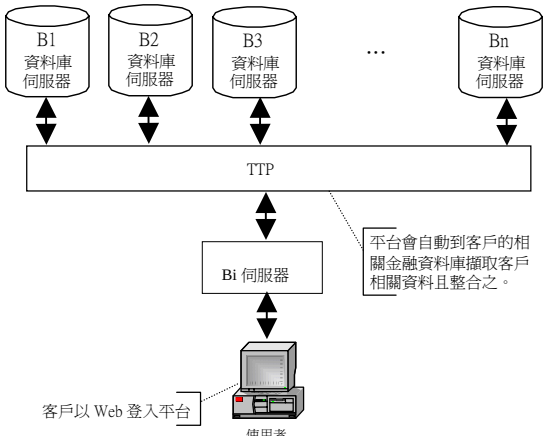

圖 6　TTP 法之示意圖

【優點】

1. 擁有如 Hub 法 1~3 項的優點。
2. 客戶是直接面對 Bi（一般爲客戶的往來銀行），所以可以免除重新開戶的動作。

【缺點】

1. 擁有如 Hub 法 1~5 項的缺點。
2. 客戶於存取其相關網站的所有使用者名稱及密碼等，是由 Bi 傳到平台；換言之，於 Bi 及平台，皆擁有使用者名稱及密碼等，因而更增加安全的顧慮。

【模式七】Web-PKI 法

於 Web-PKI（Public Key Infrastructure, 公開鑰基礎建設）法，參與多行帳戶整合服務的所有金融機構，須提供 CA（Certification Authority，認證機構）功能。當客戶欲使用帳戶整合服務時，可採用 Web 方式登入到任何一家參與多行帳戶整合服務的金融機構（一般爲往來銀行），然後由該金融機構自動到客戶的相關金融機構資料庫，逐次擷取客戶的相關資料，且整合顯示之，其示意圖如圖 7、客戶的操作流程如圖 8、系統內部流程如圖 9。

圖 7 至圖 9，假設某客戶 C（Customer）已與 B1、B2、…、Bn 等 n 個往來金融機構，約定擁有多行帳戶整合功能。

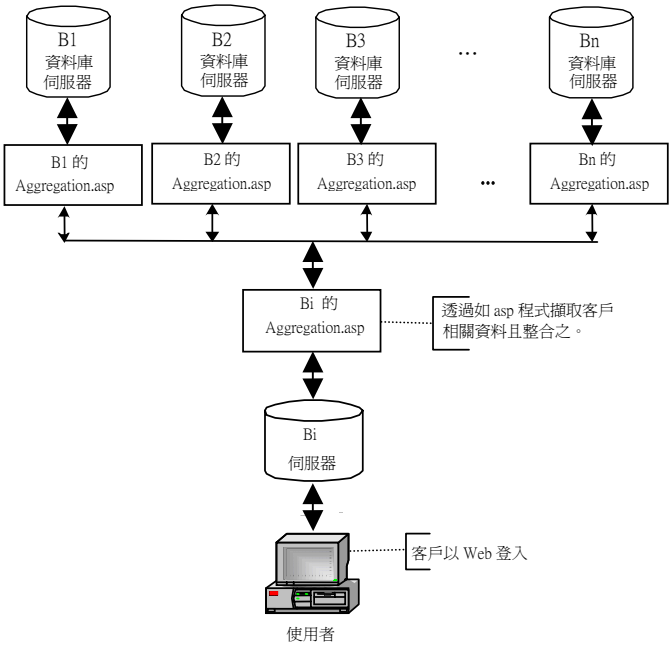

圖 7　Web-PKI 法之示意圖

欲查詢 n 個往來金融機構各別餘額、總餘額、及各金融機構交易明細。客戶 C 的操作流程例子如下：

1. 進入 Bi（i 可爲 1,2,…,n）首頁
2. 進入「多行帳戶整合」的網頁
3. 插入 RSA Smartcard 卡
4. 輸入密碼
5. 按「查詢」。可顯示多行帳戶的各行餘額、交易明細、及 n 家金融機構總餘額等訊息。

圖 8　客戶的操作流程

當客戶 C 登入於 Bi 金融機構且按「查詢」時，其系統內部處理流程如下：

1. FOR j（j 屬於 1,2,..,n）
2. 於C端向附屬於Bj主機的Aggregation.asp程式，送出查詢餘額及交易明細資訊之指令。
3. 由 Bj 主機送出一個與時間有關的時間郵戳（Time Stamp）Mj 到 C 端。
4. 於 C 端利用私鑰 cs 對 Mj 簽名，亦即由 C 端送出 Dcs(Mj)到 Bj。
5. 於 Bj，如果利用 C 的公開鑰 cp 解密得 Mj ，亦即 Ecp(Dcs(Mj))=Mj 時，則由 Bj 送出 C 於 Bj 金融機構之加密後餘額及交易明細資訊，爲 Ecp(INFOj) ，到 C 端。
6. 於 C 端利用私鑰 cs 對加密之餘額及交易明細資訊解密，爲 Dcs(Ecp(INFOj))，得 INFOj。
7. NEXT j
8. 由附屬於 Bi 主機的 Aggregation.asp 程式，進行多行帳戶整合，且顯示多行帳戶的各行餘額、交易明細、及 n 家金融機構總餘額等訊息。
   執行多行帳戶整合的程式 Aggregation.asp，是置於參與多行帳戶整合服務的各金融機構 Server 端，所以須經具公信之機構，譬如金融機構公會，的認證且簽署相關保密合約，以防止 Bi 金融機構擷取客戶 C 於 Bj（j<>i 且 j 屬於 1,2,...,n）金融機構的相關訊息。

圖 9　系統內部流程

【優點】

1. 由於使用 RSA Smartcard 卡（Brands 2000; Burnett and Paine 2001; Coutinho 1999; Pfleeger 1997），所以只有客戶本身，才能夠擷取其相關金融機構資料庫的相關資料。
2. 餘額及交易明細等資訊，是以加密方式傳遞，具有相當的安全性。
3. 當 CA 互通時，客戶登入於任何一家參與多行帳戶整合服務的金融機構，皆可以執行多行帳戶整合的功能。

【缺點】

1. 須有 PKI 環境。惟我國已於 2001 年 10 月通過電子簽章法，且機構陸續成立，如 GCA、HCA、自然人 CA（黃泰元 2002; 楊佳政 1998; 樊國楨 1998；潘維忠 2002; Pfleeger 1997; Stallings 1999）。相信近年內，PKI 環境會具相當成熟度。
2. 各金融機構的 Aggregation.asp 程式，須配合其後端資料庫系統，稍作修改。但各金融機構的 Aggregation.asp 程式大同小異。
3. 由於執行多行帳戶整合的程式 Aggregation.asp ，是置於金融機構 Server 端。爲防止金融機構任意竄改程式內容（譬如擷取客戶於它行的金融資訊），所以須有如金融機構公會

認證並簽署相關保密合約。

【模式八】Agent-PKI 法

於 Agent-PKI 法，參與多行帳戶整合服務的所有金融機構，亦須提供 CA 功能。當客戶欲使用帳戶整合服務時，可採用「代理程式」方式，擷取相關金融機構客戶的相關資料，且整合顯示之，其示意圖如圖 10、客戶的操作流程如圖 11、系統內部流程如圖 12。

圖 10 至圖 12，亦假設某客戶 C（Customer）已與 B1、B2、…、Bn 等 n 個往來金融機構，約定擁有多行帳戶整合功能。

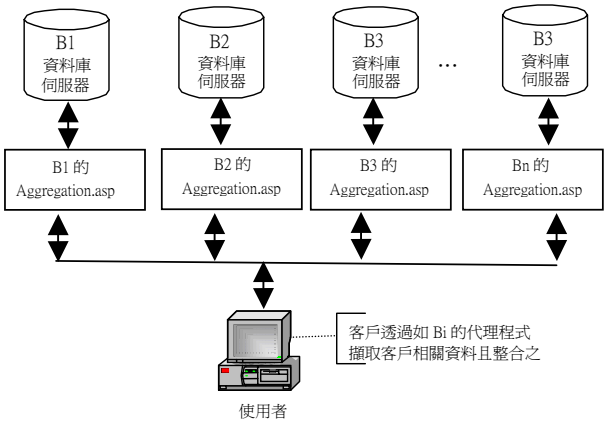

圖 10　Agent-PKI 法之示意圖

欲查詢 n 個往來金融機構各別餘額、總餘額、及各金融機構交易明細。客戶 C 的操作流程例子如下：

1. 啓動 Bi 所提供的代理程式且進入「多行帳戶整合」的功能
2. 插入 RSA Smartcard 卡
3. 輸入密碼
4. 按「查詢」可顯示多行帳戶的各行餘額、交易明細、及 n 家金融機構總餘額等訊息。

圖 11　客戶的操作流程

當客戶 C 按「查詢」時，其系統內部處理流程如下：

1. FOR j（j 屬於 1,2,..,n）
2. 於 C 端向附屬於 Bj 主機的 Aggregation.asp 程式，送出查詢餘額及交易明細資訊之指令。
3. 由 Bj 主機送出一個與時間有關的時間郵戳 Mj 到 C 端。
4. 於 C 端利用私鑰 cs 對 Mj 簽名，亦即由 C 端送出 Dcs(Mj)到 Bj。
5. 於 Bj，如果利用 C 的公開鑰 cp 解密得 Mj ，亦即 Ecp(Dcs(Mj))=Mj 時，則由 Bj 送出 C 於 Bj 金融機構之加密後餘額及交易明細資訊，爲 Ecp(INFOj) ，到 C 端。
6. 於 C 端利用私鑰 cs 對加密之餘額及交易明細資訊解密，爲 Dcs(Ecp(INFOj))，得 INFOj。
7. NEXT j
8. 由 C 端的代理程式，進行多行帳戶整合，且顯示多行帳戶的各行餘額、交易明細、及 n 家金融機構總餘額等訊息。

執行多行帳戶整合的代理程式，是置於 C 端，所以須經具公信之機構，譬如金融機構公會，的認證且簽署相關保密合約，以防止 Bi 金融機構擷取客戶 C 於 Bj（j<>i 且 j 屬於 1,2,...,n）金融機構的相關訊息。

圖 12　系統內部流程

【優點】

1. 擁有如 Web-PKI 法的優點
2. 客戶可以不必透過 Bi，而直接擷取所有的相關訊息。

【缺點】

3. 擁有如 Web-PKI 法的缺點
4. 客戶端須安裝代理程式。

肆、結論

交易的安全性，是金融活動最重要考量因素之一。

改良式網頁挖取法及改良式 OFX 法，是將客戶於存取其相關金融機構網站的所有使用者名稱及密碼等，置於客戶端而非整合商，因而較無整合商可靠度的顧慮。但由於非使用瀏覽器登入，所以客戶須先於本身電腦，安裝整合商所提供的 Client 端程式，因而，導致不同 Client 端，皆須安裝程式，較不具可攜性（Portable），且會常有因不同的安裝環境（譬如不同的作業系統版本或電腦設備）而產生不同問題的困擾。

Hub 法及 TTP 法，其平台端仍須擁有著客戶於存取其相關金融機構網站的所有使用者名稱及密碼等，因而仍然有安全的顧慮。譬如，平台運作者可能洩露使用者名稱、密碼、或交易資訊等。

Web-PKI 法及 Agent-PKI 法，皆採用 RSA 私鑰簽名，所以擁有不可否認性、無法僞造性、及身份辨識性（Burnett and Paine 2001; Seberry and Pieprzyk 1989）；採用時間郵戳，所以不會發生訊息重複使用（Replay）的弊端（Imai and Zheng 1999; Pfleeger 1997）；採用 RSA Smartcard 卡，所以不會發生客戶私鑰被竊取的風險；餘額及交易明細等資訊，是以公開鑰（一般爲 1,024 Bits）加密方式傳遞，具有相當的隱私性。

根據 Morgan Stanley Dean Witter 的調查分析，於多行帳戶整合服務中，客戶最關心的

前面五項議題，分別爲安全性（33%）、隱私性（16%）、不信任帳戶整合服務（14%）、較喜愛採用金融機構網站而非整合商網站（13%）、不願意將使用者名稱及密碼告知整合商（11%）（Coulter 2001）。當安全性及隱私性爲主要考量時，本論文所提 Web-PKI 法及 Agent-PKI 法，應屬可行的模式。

如果對網路銀行多行帳戶整合信心不足，或者可以考慮多行帳戶整合的功能僅止於如多行帳戶餘額、交易明細等訊息的查詢，而如果要進行較重要的工作，如轉帳、變更密碼等功能時，需透過一般個別網路銀行進行之。

伍、建議

未來研究之建議如下：

1. 本論文所提多行帳戶整合，偏重於金融資訊。後續研究可探討，當整合多種行業的多種線上服務資訊，譬如整合銀行、證券、基金、債券、理財、電子錢包、信用卡、支票、Email 訊息、News、紅利、…等時，可能採用的模式及其風險分析。
2. 多行帳戶整合環境中，如何整合多種不同格式的資料來源，也是一個重要課題。譬如，可以研究如何利用 XML（eXtensible Markup Language，可延伸標記語言）（呂理玄、楊建民 2001; 張子文、楊建民 2001; 梁中平、徐子淵、謝鎮澤 2000），來進行多種資料來源的整合，以解決安全性的相關問題（譬如，可廣泛性的進行資料追蹤及稽核、可區分資料擷取者爲客戶本身或整合商等）。
3. 法律責任方面。譬如，因使用者名稱及密碼告知整合商而衍生的洩密弊端；整合商去擷取使用者帳戶資訊，所衍生的財務資訊洩密等法律相關問題的探討。

參考文獻

1. 方翊人，『淺談帳戶整合業者法律責任』，資訊與電腦，第 252 期，2001 年 7 月，頁 118-120。
2. 吳文玲，『C 計畫催化金融業金融電子化』，財金資訊雙月刊，第 21 卷，2002 年 4 月。
3. 呂理玄、楊建民，XML-Enabled 網路銀行個人理財整合帳戶系統設計與實作，政治大學資訊管理研究所碩士論文，2001 年 6 月。
4. 呂學錦，『公開金鑰基礎建設與政府憑證管理中心之服務及應用』，研考雙月刊，第 23 卷第 1 期，1999 年 2 月，頁 59-71。
5. 林真真，『從企業 e 金流 C 計劃談企業金融共用中心』，財金資訊雙月刊，第 21 卷，2002 年 4 月。
6. 張子文、楊建民，XML-Based HTML

Wrapper 建置之研究—在網路銀行個人帳戶資訊彙整服務上之應用，政治大學資訊管理研究所碩士論文，2001年6月。

7. 梁中平、徐子淵、謝鎮澤， XML 與電子商務標準，財團法人資訊工業策進會，2000 年 11 月，頁 1-136。
8. 黃泰元，『跨國交互認證所衍生的技術問題與解決方案』，經濟部商業司/NII 產業發展協進會/台灣國際電子商務中心/數位時代雜誌---PKI 論壇系列，2002 年 5 月。
9. 楊佳政，『認證中心法律責任研究』，資訊法務透析，1998 年 6 月，頁 27-35。
10. 樊國楨，『金鑰憑證驗證中心與法律淺析—技術的觀點』，資訊 安全通訊，第 4 卷第 2 期，1998 年 3 月，頁 65-83。
11. 潘維忠，『金流作業導入產業運疇 focus：C 計畫』，財金資訊雙月刊，第 21 卷，2002 年 4 月。
12. Adams, C. and Lloyd, S. Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations, New Riders, 1999, pp. 33-34, 134-148.
13. Alavi, M. and Carlsion, P. “A Review of MIS Research and Disciplinary Development,” Journal of Management Information Systems, Vol. 8, No. 4, Spring 1992, pp. 45-62.
14. Albro, W. "Account Aggregation News," Banking Marketing, Vol. 33, May 2001, pp. 8.
15. Brands, S.A. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy, the MIT Press, 2000, pp. 15-19.
16. Buhl, H.U. and Will, A. "Economic Aspects of Electronic Commerce in Financial Services and Advantageous Steps to Extended Offers in Internet Banking," Proceedings of the 31st Hawaii International Conference on System Sciences (HICSS'98), 1998.
17. Burnett, S. and Paine, S. RSA Security's Official Guide to Cryptography, Osborne/McGraw-Hill, 2001, pp. 98-105, 171-207.
18. Charski, M. "One-Stop Banking--Banks Get in on Account Aggregation Services," Interactive Week, Oct 30, 2000, pp. 58.
19. Coulter, C. "Account Aggregation: Realizing the value," Perspectives E-business, 2001, pp. 34-39.
20. Coutinho, S.C. the Mathematics of Ciphers: Number Theory and RSA Cryptography, A K Peters, 1999.
21. Derkley, K. "Account Aggregation: Whole in One," Personal Investor, Nov 2000, Vol.18, No.10.

22. Ferguson, R.B. "Data Aggregation Poses Risks: Security, Responsibility for Errors Are Key Issues," eWeek, Oct 2, 2000, pp. 44.
23. Furst, K., Lang, W.W. and Nolle, D.E. "Internet Banking," Journal of Financial Services Research, Vol. 22, 2002, pp. 95-117.
24. Furst, K., Lang, W.W. and Nolle, D.E. "Internet Banking: Developments and Prospects," Office of the Comptroller of the Currency Economic and Policy Analysis Working Paper, Sep 2000.
25. Furst, K., Lang, W.W., and Nolle, D.E. "Internet banking in the U.S.: Landscape, Prospects, Industry Implications," Journal of Financial Transformation, 2001, pp. 45-52.
26. Ginovsky, J. "Account Aggregation Update: Is it time for community banks?" ABA Bankers News, Vol. 9, Dec 25, 2001, pp. 1-4.
27. Hackett, J. "Domesticating Account Aggregators," Bank Technology News, Vol.13, Oct 2000, pp.1-40.
28. Housley and Russ, Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure, Wiley, 2001.
29. Imai, H. and Zheng, Y. Public Key Cryptography, Springer, 1999, pp. 290-304.
30. Kersnar, S. "National City's Account Aggregation System Includes Mortgages," National Mortgage News, Vol. 25, Aug 20, 2001, pp. 19.
31. Koreto, R.J. "Aggregation Aggravation: It Helps Clients. It Builds Loyalty. Several Vendors Provide Affordable Solutions. So How Come Hardly Anyone Wants Account Aggregation?" Financial Planning, May 1, 2002, pp. 65-70.
32. Massaro, K. "Financial Institutions Embrace Account Aggregation," Wall Street & Technology, Vol.18, Oct 2000, pp. 31-34.
33. Massaro, K. "The Big Picture: Account Aggregation," Wall Street & Technology, Vol.18, Sep 2000, pp. 90.
34. McMahon, S. "Account Aggregation and Small-business Banking," Commercial Lending Review, Vol.17, Winter 2001/2002, pp. 11-19.
35. Mearian, L. "Banks See Online Account Aggregation as Necessary Evil," Computerworld, Vol. 35, Jul 23 2001, pp. 7.
36. Merrick, B. "E-Scan Insight: Projected Growth in Online Account Aggregation," Credit Union Magazine, Vol. 68, Apr 2002, pp. 12.

37. Miller, K. "Account Aggregation," Memphis Business Journal, Vol. 23, Sep 7, 2001, pp. 31.
38. Mugavero, P.S. "Opportunities in Account Aggregation," Mortgage Banking, Vol. 61, Dec 2000, pp. 64-66.
39. Nash, A., Duane, W., Joseph, C. and Brink, D. PKI Implementing and Managing E-Security, Osborne/McGraw-Hill, 2001, pp. 63-64, 229.
40. O'Brien, J. "Financial Software Firm Offers Account Aggregation," Bank Systems & Technology, Vol. 37, Feb 2000, pp. 46.
41. Pfleeger, C.P. Security in Computing, Prentice-Hall International, Inc., 1997, pp. 91-99, 143, 411-418.
42. Poquette, B. "Account Aggregation," Bank News, Vol.100, Oct 2000, pp. 18-19.
43. Pullara, J.M. "Understanding the Rewards & Hazards of Account-aggregation Services," Wall Street & Technology, Mar 2002, pp. 53-54.
44. Robert, D. "Birth, Growth, and Life or Death of Newly Chartered Banks," Economic perspectives, 1999, pp. 18-35.
45. Robert, K. "Account Aggregation: Consolidation on the Cutting Edge Security Concerns Trust Standardized Formats," Independent Banker, Vol. 52, Feb 2002, pp. 48-54.
46. Sciglimpaglia, D. and Ely, D. "Internet Banking: A Customer-Centric Perspective," Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.
47. Scott, R.W. "Account Aggregation: A New Tool Takes Off," Accounting Technology, Vol. 17, May 2001, pp. 34-38.
48. Seberry, J. and Pieprzyk, J. Cryptography: An Introduction to Computer Security, Prentice-Hall, 1989, pp. 154-171.
49. Stallings, W. Cryptography and Network Security: Principles and Practice, 2nd ed., Prentice Hall, 1999, pp. 173-182, 299-303.
50. Valentine, E.L. "On-Line Account Aggregation: Benefits and Risks," Federal Reserve Bank of Philadelphia, Fourth Quarter 2001, pp. 1-4.
51. Wagner, V. "Key Offers Account Aggregation Service," Bank Systems & Technology, Vol. 39, Jan 2002, pp. 16, 20.
52. Weisul, K. "Screen Scraping Makes

Web Comeback," Inter@ctiveWeek, Apr 17, 2000, pp. 34.

53. Yan, G. and Paradi, J.C. "Internet - the Future Delivery Channel for Banking Services?" Proceedings of the 31st Hawaii International Conference on System Sciences (HICSS'98), 1998.
54. Yasin, R. "Financial Firms Push Everything Online," InternetWeek, Oct 30, 2000, pp. 31-43.

作者簡介

黃明達

淡江大學管理科學研究所 MIS 組博士，美國伊利諾大學博士後研究。現任淡江大學資訊管理系副教授兼資訊中心主任。曾任淡大資管系系主任及所長。目前主要擔任中華民國資訊管理學會理事長及淡江人資訊協進會理事長。爲經濟部技術處 ABCDE 計畫主審、商業司商業 e 化主審等。研究領域主要爲資訊安全管理、電子簽章、電腦稽核等。