以電子傳送方式提交申報表

香港金融管理局於1997年12月推出「以電子傳送方式提交申報表」系統(電子傳送系統)，以提高認可機構提交申報表的效率和保安。使用這系統的認可機構可以在其個人電腦上填報銀行申報表，並修改有關數據，然後經由一個保安完善的專用網絡把數據傳送至金融管理局。首批為數約30家認可機構於1998年1月開始使用新系統，預計其餘認可機構將於稍後分批開始採用新系統。本文旨在闡釋該系統為保障所傳送的數據而運用的保安措施。

引言

背景

金融管理局在1995年推出「以電子媒體提交申報表」系統(電子媒體系統)，讓認可機構以軟盤提交申報表。電子媒體系統是一項電腦軟件，用戶可以編製申報表文本，以及將輸入的數據儲存在軟盤上。認可機構中超過98%採用這個系統提交申報表。

隨着電子媒體系統得以成功推行，監管申報工作小組建議利用電子傳送方式，使提交申報表的過程更加自動化，這樣認可機構便毋須派專人遞交申報表文本和軟盤。金融管理局就此展開可行性研究，並於1996年4月完成有關工作。研究結果指出，香港的電訊設施優良，只要合理的成本就能夠以電子傳送方式提交申報表。此外，利用強勁的訊息密碼方法和數碼簽署，就可以把數據保密。

金融管理局在1996年6月7日把可行性研究結果知會各認可機構，並諮詢它們對推行以電子方式提交申報表的系統的意見。大部分認可機構都支持這個構思。金融管理局遂展開系統設計工作，並於1996年12月完成。1997年4月，金融管理局向部分認可機構介紹系統的設計，得到的回應也相當理想，絕大部分認可機構均贊成系統的設計。

系統發展的工作隨之展開，並成立了一個由8家認可機構組成的工作小組，對系統發展提供意見，以及進行系統試行。所有系統發展和測試工作在1997年11月順利完成。

主要特色

電子傳送系統的主要特色包括：

- 利用密碼技術，確保銀行申報表所載數據保密和完整；
- 以數碼簽署取代申報表文本上的親筆簽署，並由金融管理局作為證明發出商；
- 把申報表所載數據壓縮成為電子郵件訊息，方便經由網絡傳送；
- 自動化核實申報表程序；
- 引進保安完善的傳送訊息機制，確保傳送的銀行申報表數據保密，這個機制在將來更可能發展為個人通訊渠道；及
- 引進一套可以互用的數據保安技術和管理安排，能夠與金融業內的其他系統合併。

資料保密

電子傳送方式是經由專用網絡進行。這即是說，由發件人的個人電腦輸出的訊息會直接傳送至收件人，不會經過其他網絡或侍服器，與經由互聯網發出的電子郵件不同。因此，訊息在未獲授權情況下遭截取的可能性得以減低。

由於訊息已加碼，因此萬一訊息真的被截取，未獲授權人士也無法讀取訊息。電子傳送系統選用公用密鑰加密法 (public key cryptography)，這種方法是利用兩組數字，由第一組數字加密的訊息，只可由第二組數字解碼，反之亦然。此外，要由一組數字的算法得出另一組數字也是不可能的。其中一組數字稱為公用密鑰，另一組則為專用密鑰。訊息會由金融管理局的公用密鑰加密，並只可以金融管理局的專用密鑰解碼。電子傳送系統使用的加密方法是目前最先進的加密技術之一。以目前的電腦計算能力而言，估計破譯者要數以十年才能成功破解密鑰。

確定身分和驗證資料

這些問題可透過密碼、聰明卡和數碼簽署等方法來解決。

第一防線是接達專用網絡的方法。只有具備適當密碼的獲授權人士才可接達專用網絡，同時，亦有政策禁止獲授權人士向其他人透露密碼。假如未獲授權人士成功接達網絡，也無法發出有效訊息，或更改任何資料，原因是要發出訊息或更改資料，必須有數碼簽署。要在提交予金融管理局的文件上加上數碼簽署，必須利用以專有密碼保護的聰明卡，卡上記錄了發件人的個人資料和專用密鑰，而且不能複製。這種雙重保障方法的好處是，除非同時擁有密碼和聰明卡，否則未經授權，根本無法接達系統。即使外界可以在密碼擁有者不知情的情況下破解密碼，聰明卡物主一旦發覺遺失了聰明卡也會即時報失。

數碼簽署與親筆簽署的作用一樣，是要確定發件人的身分，並確保所傳送的資料完整。數碼簽署涉及運用算法把訊息編成獨一無二的「散列訊息」，並由發件人以其專用密鑰把散列訊息加密。已加密的散列訊息成為數碼簽署，並連同原有訊息一併由金融管理局的公用密鑰加密。此舉就如把加了數碼簽署的訊息放進電子信封內，只有相應的金融管理局專用密鑰才可開啟。金融管理局經由網絡收到「信封」後，會用其專用密鑰開啟信封，並取得訊息和數碼簽署。然後，以公用密鑰 (經證明為發件人所有) 將數碼簽署解碼。如果能成功解碼，金融管理局便會取得散列訊息，並知道訊息的確來自發件人。接着，金融管理局會以同一算法利用訊息另行編成散列訊息，並將之與解除數碼簽署的密碼所得的散列訊息比較，如果兩個散列訊息相同，金融管理局便可以確定訊息沒有被更改。圖1以圖解方式說明這個過程。

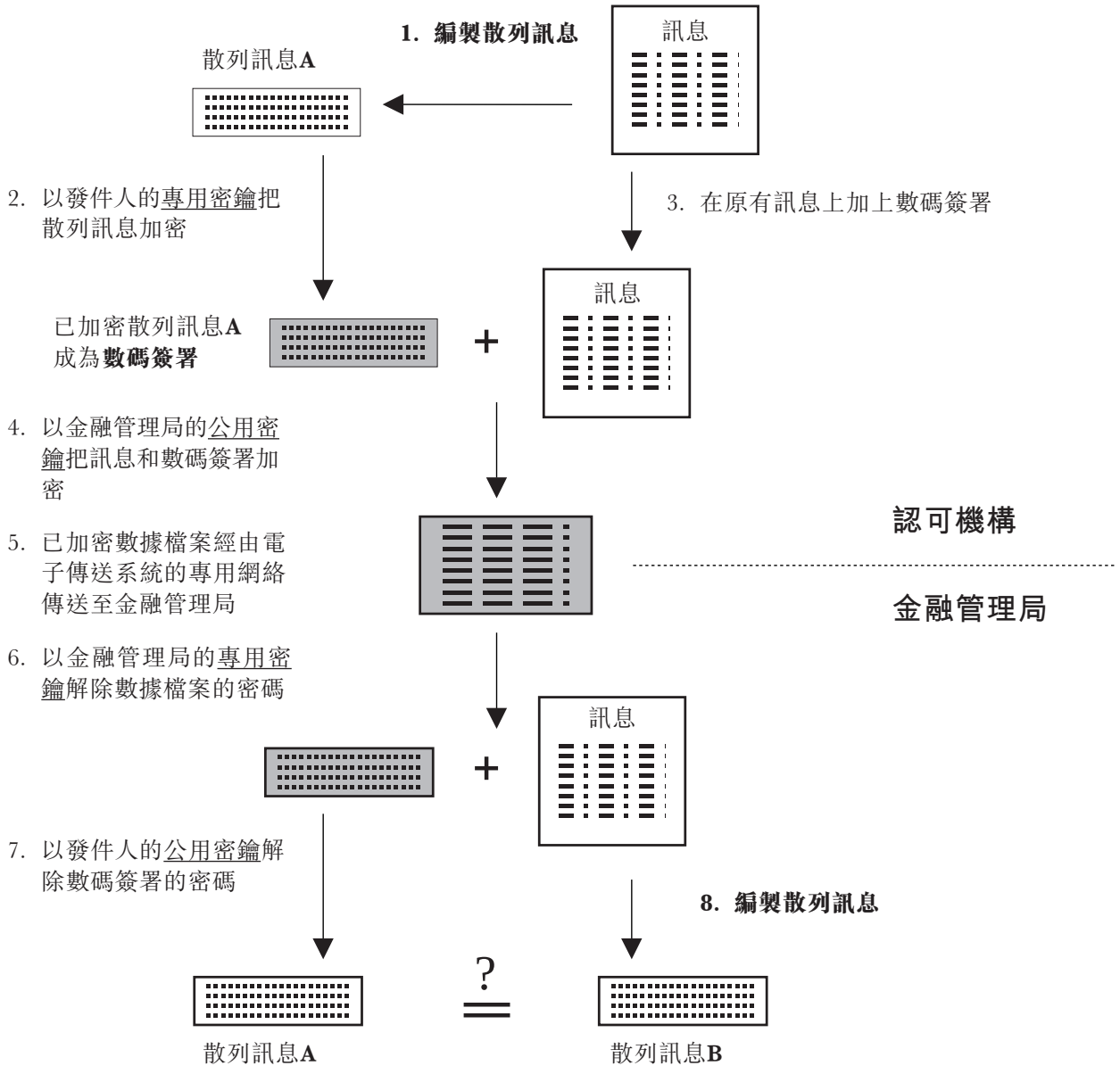
證明發出商發出公用密鑰證明書

整個過程最關鍵的一點，就是要鑒定公用密鑰的真偽。機構會利用金融管理局的公用密鑰來把非常敏感的資料加密，它們自然希望確定所用的公用密鑰的確屬於金融管理局，這樣便只有金融管理局以其專用密鑰才可把訊息解碼。另一方面，金融管理局也希望確定用作解除數碼簽署的密碼的公用密鑰確實屬於有關發件人，以確保資料並非其他人發出。因此，必須有證明發出商來證明與公用密鑰有關的人士的身分。

在電子傳送系統下，金融管理局會作為證明發出商。金融管理局會核准授權簽署人，一般為機構的總裁和總會計主任。簽署人獲金融管理局核准後，可經由電子傳送系統軟件自行編製一對密鑰。專用密鑰會儲存在個別簽署人的聰明卡上，而公用密鑰則會連同身分證明文件 (即證明申請書) 一併交予金融管理局。簽署人須親筆簽署證明申請書，並

〔圖1〕

以數碼簽署驗證身分及核實資料



9. 比較散列訊息**A**和散列訊息**B**

寄交金融管理局以便核實。金融管理局核實證明申請書所載資料後，會經由網絡向簽署人發出數碼證明書。簽署人收到數碼證明書後，就可以啟動聰明卡，簽署申報表。圖2列出整個發出證明書的過程。金融管理局的公用密鑰會連同電子傳送系統軟件一併發出，軟件會安裝在核准發件人的個人電腦上。

撤銷證明書

在若干情況下，可能需要撤銷某位簽署人的證明書，例如：

- 遺失了聰明卡；
- 密碼被泄露；或
- 更換簽署人。

如發生上述任何情況，機構需向金融管理局報告。金融管理局會立即撤銷有關證明書，簽署人需編製一對新密鑰，並就密鑰取得適當證明書。

推行

金融管理局於1997年12月推出電子傳送系統，首批為數約30家認可機構已開始使用該系統。金融管理局將於1998年初分階段向其餘認可機構發放該系統。

– 本文由銀行政策部提供

〔圖2〕

發出公用密鑰證明書