[農產品電子商務]系列報導 之十二

網路安全～如何安心的在網路上做生意

高雄區農業改良場　鄭文吉
jwj@mail.kdais.gov.tw

※本文已於2002年6月發表於農業世界雜誌226期91-101頁※

前言

隨著寬頻網路的日漸普及，許多人的電腦都是一開機就是在上網路的狀態，因此也給了駭客可趁之機，駭客入侵不再是電影中的情節。因此在上期的內容中，小弟大致介紹了一些網路安全的基本概念，說明駭客入侵電腦的過程和防制之道，以及我們如何利用簡單的防範措施，例如使用個人防火牆軟體，來攔截外來的偵測，避免我們的電腦變成駭客的目標。這些看起來似乎跟我們的主題～農產品電子商務沒什麼關聯，但是卻是攸關大家基本權益的大事。因爲我們的電腦裡面或許沒有什麼國家機密，但如果駭客拿我們的電腦當作跳板來攻擊別人，到時候人家追查到我們頭上，也是會讓人傷透腦筋。

要入侵別人的電腦來竊取資料，畢竟還需要一點專業技術；但由於網路傳輸太方便了，只要在電子郵件軟體更改發信人的資料，任何人都可以輕易的假借他人名義傳送資訊，如果對方不察，就會造成困擾。因此，如何確定我們所收到的訊息眞的是對方寄出來的，而且中間不會遭到偷聽或竄改，就成爲網路交易的重要關鍵。如果買賣雙方彼此無法確定所收到的訊息是對方寄出來的，那麼生意就作不成了。因此，在介紹完自家用電腦的防駭之道後，接下來讓我們談談網路交易的安全問題，看看要如何才能安心的在網路上做生意。

小心隔牆有耳

在討論網路交易的安全問題前，讓我們先看看眞實世界裡的交易可能會有什麼樣的問題，這樣或許能讓大家比較容易想像網路交易的狀況。

假設現在我想訂購一箱蓮霧，準備分送給親朋好友。因此我就打電話給某個水果超商，說明想要什麼品級的蓮霧，數量多少，然後什麼時候可以取貨等等。如果這時商家那邊並沒有現貨，他可能就得再聯絡上游的蓮霧產銷班，來取得這箱蓮霧，並且通知物流業者何時送貨，最後再通知我幾時可以送貨，如何交錢等等。整個交易過程，就是在一通通的電話裡完成～這也就是前面所提過的「資訊流」。

現在，請發揮一點想像力，把電影裡的情節套用進來。假設現在有某個人，他事先在商家的電話裡裝了竊聽器，因此得知我來訂購蓮霧的交易細節。

這時，他可以先假裝成我打電話給商家，說蓮霧不要了，取消這個交易。然後找他自己認識的產銷班和物流業者出貨，再跟我聯絡說幾時可以送貨，如何交錢等等。這樣一來，整個交易就不知不覺的被他搶過去了。當然，除了搶生意外，他也可以沒事搗蛋一番。例如假裝顧客來跟商家訂貨，等人家送貨後發現沒這回事，讓人家白忙一場，這樣也會造成很大的困擾。

當然，要在人家的電話裡裝竊聽器並沒有電影裡演的那麼容易；而且電話裡面可以聽到聲音，因此要假裝別人的聲音來打電話，或許也沒有那麼簡單。但是當我們把交易搬到網路上之後，由於雙方都是用電腦來聯繫，整個資料傳輸的過程可能要在台灣繞一大圈，過程中是否會被竊聽，那就很難說了。加上電腦檔案的文字看起來都一樣，不像聲音還可以拿來辨認對方的身分；任何人只要在電子郵件的發信人處改一下，就可以輕易的假藉他人的名義來寄信。因此，要在網路上做生意，對於資料傳輸的安全性勢必要加以注意。不但要預防被竊聽，更要預防被竄改(如圖1)。

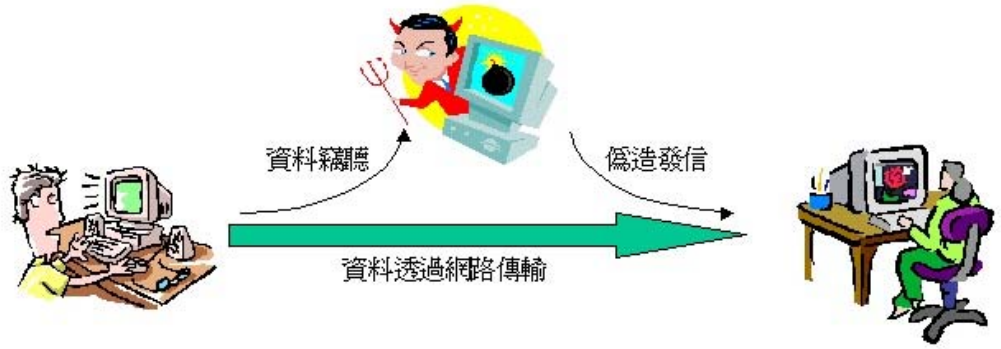

圖1. 網路資料傳送可能遇到的問題：資料被竊聽或假借別人名義發信

然而，由於網際網路是四通八達的，任何資料的傳送，都必須經由中間許多台電腦主機的轉送才能作到。對於有心人來說，要攔截這些過路的資料並不是什麼難事。而且不只「壞人」才會去偷聽網路上的資料，其實許多正常的網路管理工作，例如上一期所提到的防火牆，就必須依賴事先檢測這些在網路上流通的資訊，才能作到過濾把關的安全監管措施。

因此，利用網路來傳送資料，就像兩個人在火車裡面聊天一樣，其實身旁的人也都會聽到他們的談話內容，差別在於人家有沒有注意聽而已。一般來說，旁邊的人不是當事者，所以通常都會當作沒聽到，不會在意他們是在講什麼；但若旁邊的人就是專程來偷聽的，那自然就會注意他們談話的內容是不是有值得利用的地方了。

舉例來說，日前舉辦的國中基本學力測驗，就有民意代表開記者會說中間有問題。因爲只要在負責閱卷的電腦上裝了竊聽鍵盤按鍵的程式，就可以偵測到他們輸入的帳號密碼，這樣就可以利用這個帳號密碼去偷改裡面的成績。這個就是前面提過「專程來偷聽」的行爲，因爲網路上流通的資料量非常大，而且這些資料都會先被拆解成小單位來傳送，稱之爲資料封包。但是因爲不同人發送的資料封包都是透過同一條網路線傳送，只有到達目的地才會加以分送，如果是在中間攔截，就會混在一起了，因此不可能由人去一一研究所擷取到的

資料封包裡面的內容。但是，我們可以讓電腦去搜尋裡面有沒有特定的字句，以這個例子來說，只要利用所謂的竊聽鍵盤按鍵的程式，找看看所擷取到的資料封包裡，在電腦傳出「帳號：」和「密碼：」這兩個字句時，使用者用鍵盤在後面打了什麼字，自然就知道他的帳號密碼是什麼了。這樣一來，駭客就可以用這個帳號密碼來登錄網站，作他想做的事情，看是要更改成績或者是隨便搗蛋，都隨他高興。

當然，理論上是這樣沒錯，不過這個例子其實也有點奇怪。因爲閱卷的電腦是專用的，跟我們家裡的個人電腦不一樣，根本沒有連上網際網路，因此就不太可能會被駭客從網路入侵，去裝設那個竊聽鍵盤按鍵的程式。除非駭客是像電影裡演的那樣，親自跑到閱卷公司裡，從電腦上直接安裝程式。問題是，如果駭客眞的能跑到那台閱卷電腦上安裝程式，那也不需要那麼麻煩去攔截鍵盤按鍵的訊號，再從網路輸入管理員的帳號密碼來改資料了，直接開電腦來改裡面的檔案資料，豈不是更方便?

電子商務上的安全需求

前面提到的是網路交易上可能遇到的問題，由於買賣雙方無法面對面接觸，因此所有的訊息都只能靠網路來聯繫。因此如何確保網路通訊的安全，就成了最大的問題。因此一般來說，在電子商務的應用上，對於資訊安全大致有下面幾個需求：

1. 保密：買賣雙方的通訊內容必須加密，以免被不相干的人看到。
2. 完整：通訊內容必須能確定是原來的樣子，中間沒有遭到修改。
3. 認證：買賣雙方可以確認對方的身分是本尊，而不是別人假冒的。
4. 不可否認：由於身分已確認，因此訂單一但寄出，買方就不能抵賴不付錢。
5. 使用方便：不管加密解密等等動作，都必須容易操作，不可增加買賣雙方的困擾。最好是由電腦自動完成，減少使用者的負擔。

如果上面幾項能夠獲得解決，電子商務才有可能繼續進行下去。否則如果買賣雙方都在互相猜疑，不能互相信任，那生意就作不下去了。到最後，大家都只是透過網路來看廣告，眞正買東西時還是要到商店去買，那電子商務就沒什麼搞頭了。

資料加密與解密

經由前面的說明，我們應該可以知道，要防止資料在網路傳輸的過程中被竊聽，其實是不太可能的。因此我們能作的就是，設法將資料的內容加以變化，只有收信的對方才能夠將它轉換回正常的內容；這樣其他人即使竊聽到，也不知道裡面寫些什麼。這個轉換的動作，也就是所謂的「加密」和「解密」。

對電腦來說，我們所傳送的檔案、文件、照片等等資料，其實都是一堆二進位的數字而已。因此所謂「加密」的動作，就是將原來的文件檔案裡的每一

個字，經過某種數學公式的運算，而產生另一份讓人完全看不懂的文件；而「解密」，則是反過來將經過加密後的「密文」再經過運算後，而回覆爲原來的文件。至於如何設計這個運算的數學公式才能讓人家難以破解，而且公式計算所需的時間不會太久，讓加密解密的動作對使用者本身來說不會花太多時間來作運算，這部分資訊界的學者有很多的研究，有興趣的朋友可以去參考「密碼學」方面的書籍，這邊就不再詳細說明～不然大家可能會睡著。

以下就爲大家介紹幾種常見的加密方式：

1.秘鑰法

雖然加密的方法有很多種，但要使用前，雙方得先協調好要使用哪一種方法，才能正確的作加密與解密。由於各種方法都已經寫成電腦程式來作運算了，因此這部分各位可以想成是雙方要協調使用哪種程式來處理。一般來說，在加密與解密的過程中會使用到一個特定的字串檔案，這個檔案我們可以把它當成「鑰匙」。因此所謂的加密，就是把原來文件檔案中的每一個字都經過程式套用這個字串來加以運算，而得到另外一個字。這樣一來，整篇文章就會變成另一篇完全看不懂的密碼文件；對方收到後，就用同樣的方式套用那個字串，來將密碼文件還原成原來的樣子。如果這份文件在傳遞的過程中被外人截獲，因爲他沒有這個秘鑰檔案，因此就沒法加以解密，而得到保密的效果(如圖2)。

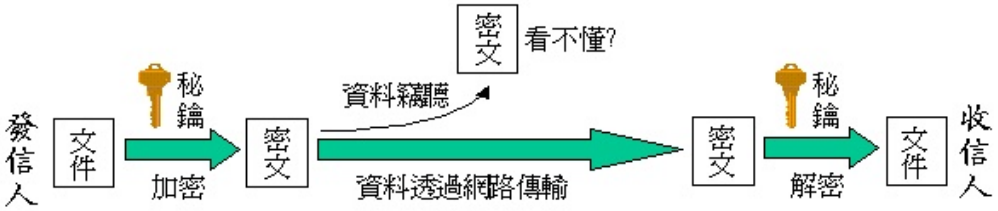

圖2．祕鑰法：發信人和收信人使用同一個秘鑰來作加密與解密

這種方式的好處是，由於秘鑰是由程式產生，我們可以自行製作祕鑰，然後將這個秘鑰檔案交給收信人。以後寄信時，就可以使用這個秘鑰來加密，這樣其他不相干的人就不知道信件的內容了。因此所謂的保密，其實重點在於祕鑰檔案，至於使用哪個程式，則是大家都知道的事，不需要保密。

或許有人會問，這樣眞的就萬無一失了嗎?因爲用什麼程式來作加解密大家都知道，而且現在電腦運算速度又那麼快，那麼只要像電影裡演的那樣，讓電腦一一嘗試所有可能的組合，不就可以把祕鑰嘗試出來了?

當然，這樣做理論上是可以的，問題是你得花多少時間才能破解出來?舉例來說，前面提過祕鑰是一個字串檔案，假設它的長度是4個英文字，也就是32個位元(bits)，那麼就有2的32次方(約43億)種可能的祕鑰組合，要破解它所需測試的組合數期望值爲全部的一半，也就是2的31次方(約21.5億)種。這樣的數字看起來好像很多，但因爲電腦運算速度很快，我們假設測試一次只需一微秒，也就是一秒鐘就可以嘗試一百萬種組合，那麼要破解這種祕鑰所需的時間爲2的31次方微秒，換算起來大約是36分鐘。

使用這樣的祕鑰看起來好像很危險，因爲只要讓電腦算個半小時，就有被

破解的危險，但我們只要增加祕鑰的長度，要破解它所需的時間立刻就以幾何級數增加。例如過去電腦保密常用的DES演算法，它就使用56位元的祕鑰。以上面的算法，就需要1142年才能嘗試找出破解的祕鑰。這麼一來，當然沒有人有辦法去等那麼久，因此就可以達到保密的效果。

問題是，電腦功能日新月異，計算速度不斷提昇，現在的個人電腦已經比二三十年前的大型電腦還要厲害，更別說那些超級電腦了。假設現在有人動用比前面所用的電腦功能快一百萬倍的超級電腦來嘗試破解，那麼前面所用的56位元祕鑰，要破解它就只需要10小時，而不是一千多年。也就是說，早期常用的DES演算法，如果遇上今天的超級電腦，還是有被破解的可能。

然而，就算超級電腦再厲害，只要我們把祕鑰長度再增加，例如增加到128位元的長度，那麼就算使用超級電腦，也得花上540萬年。因此，目前電腦傳輸所使用的保密標準，已經在1990年重新制定，採用128位元的祕鑰，稱之爲IDEA演算法，以取代1977年提出的DES演算法。

表1. 各種長度的祕鑰破解所需的時間比較

祕鑰長度(bits)	32	56 (DES法)	128 (IDEA法)
祕鑰的所有可能組合數	$2^{32}\fallingdotseq 4.3\times10^{9}$	$2^{56}\fallingdotseq 7.2\times10^{16}$	$2^{128}\fallingdotseq 3.4\times10^{38}$
一般電腦(1微秒測試1次)破解所需時間	2^{31}微秒$\fallingdotseq$35.8分	2^{55}us$\fallingdotseq$1142年	2^{127}us$\fallingdotseq 5.4\times10^{24}$年
超級電腦(1微秒測試1百萬次)破解所需時間	2.15微秒	10小時	$5.4\text{x}10^{6}$年

當然，如果你覺得這樣還是不夠安全的話，還可以再增加祕鑰的長度。例如目前非常流行的PGP加密程式，就使用長達1024位元的祕鑰，如果你不滿意甚至可以改用2048位元的祕鑰。由於每增加一個位元的長度，所需的時間就要增加一倍，有興趣的朋友，不妨算算破解這樣的祕鑰要花多少時間?我想就算電腦速度再快，要破解這樣的祕鑰，恐怕也是不可能的。

2.金鑰法

前面所提到的祕鑰法雖然簡單明瞭，而且效果不錯。但雖然破解所需的時間很長，問題是只要祕鑰本身被竊取，那就完全失去保密的效果了。由於收信人與發信人都是使用同樣的祕鑰，如果你的朋友很多，那麼祕鑰就會被複製很多份；而且，你也不能確定人家會不會再把你的祕鑰檔案轉交給別人。這樣一來，祕鑰越來越氾濫，保密的效果就越來越差了。

爲改善這個問題，便有所謂的金鑰法的加密方式。就是使用兩把祕鑰來分別作加密與解密的動作。首先你可以用程式自行製作出一對祕鑰檔案，一把自己保存，稱爲「私藏金鑰」，或簡稱爲「私鑰」；另一把則交給你的朋友或客户，稱爲「公開金鑰」，或簡稱爲「公鑰」。公鑰和私鑰是成對互補的，兩者都可以拿來作加密與解密的動作，一個作加密，另一個則作解密。

跟前面所說的祕鑰法相比，將鑰匙分成兩隻就有許多優點：

(1)保密

假設現在我想寄信給你，那我就使用你事先給我的公鑰來作加密，然後把密文寄給你，你再用自己的私鑰來作解密，而看到本文。這麼一來，由於私鑰只有你自己才有，因此這封信也只有你看得到。就算這份文件被別人偷看到也看不懂，因此可以得到保密的效果。如果是前面所說的祕鑰法，因爲擁有祕鑰的人太多了，任何人只要擁有你的祕鑰，就都可以看到信件的內容(如圖3)。

對於電子商務來說，這樣的保密特性就很有用。例如商家可以將自己的公鑰放在網站上面讓客户下載使用，當客户要傳送資料給商家時，像寄送訂單、身分資料等等敏感的資料，就可以用這個方式把文件加密，而且因爲解密用的私鑰只有商家本身才有，因此可以確定這份文件只有商家本身才能收看得到。

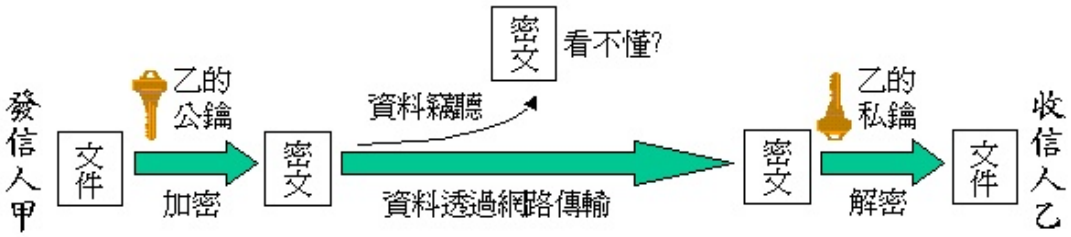

圖3．金鑰法的保密性：發信人以收信人給的公鑰加密，收信人使用自己的私鑰來解密。私鑰只有收信人才有，旁人看不懂。

(2)身分確認

除了上面所說的方式，金鑰也可以反過來使用。你可以用自己的私鑰來將文件加密，然後將密文寄出；對方收到後，就用你事先給他的公鑰來作解密，而能看到你的文件內容。這部分的原理看起來跟前面的祕鑰法是一樣的，但祕鑰法由於鑰匙只有一把，就有可能被持有祕鑰的人僞造成你所發的密文。但現在你給大家的都是公鑰，私鑰只有你自己才有，因此別人沒辦法假借你的名義來發信(如圖4)。

對於電子商務的交易來說，這樣的方式優點反而不在於保密(雖然也有這個功能)，而在於身分確認。例如商家可以在客户登錄資料加入會員時，要求客户提供一把公鑰。在寄送訂單時，客户使用自己的私鑰加密再傳送，商家就可以用來確認發信人是不是本尊，不用擔心是別人僞造亂填的訂單，而能達到信任的目的，因此可以安心送貨。對客户來說，這樣寄出的訂單也就具有不可否認的特性，一但寄出，就不能推說是別人亂填的，對商家也多一分保障。

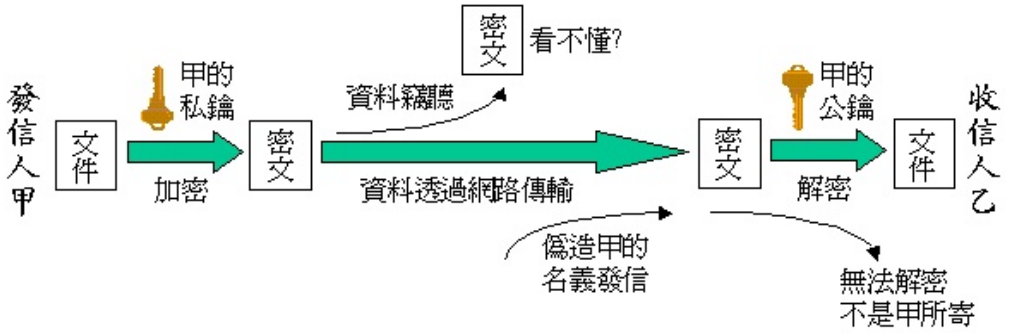

圖4．金鑰法的不可否認性：發信人以自己的私鑰加密，收信人使用發信人的公

鑰來解密，旁人看不懂，也無法僞造。

電子簽章

有時候，我們的需求重點可能不在對於文件本身的保密不讓人看，而是要能確認這份文件是由什麼人所簽署，並且確定在傳送過程中不會被外人修改，這就是所謂的完整性與有效性需求。例如在簽署支票、契約、合約書、備忘錄時，我們會在文件中簽名或蓋章；如果文件頁數很多，可能還會蓋上騎縫章；如果中途不小心有錯誤作了些修正，也必須在修正的地方蓋章以視負責。這些都是爲了要確定文件的完整性及有效性。

但對於網路交易來說，由於雙方沒法實際蓋章簽名，要如何做到上述的需求呢?爲解決這個問題，便有了「電子簽章」的產生。

所謂的電子簽章，是一個在傳送資料時，伴隨文件附帶寄送的小檔案。它是將文件本身先經過某種數學公式運算後，產生一個較短的訊息摘要，然後再利用文件簽署者本身的私鑰進行加密，而產生一份摘要的密件檔案，接著再將文件與數位簽章檔案一併寄出。對方收到後，就先以同樣的數學公式將文件轉換爲訊息摘要，同時以簽署者的公鑰將數位簽章解密，而產生另一份訊息摘要。然後，再將這兩份訊息摘要加以比對，如果相同，就表示文件確實是由發信人簽署，並且在傳送過程中並未遭到竄改。萬一不同的話，表示文件可能是他人僞造的，或者是中途被修改過了。不論是哪種原因，這份文件就已經失去它的法律效力，必須重新簽署寄發(如圖5)。

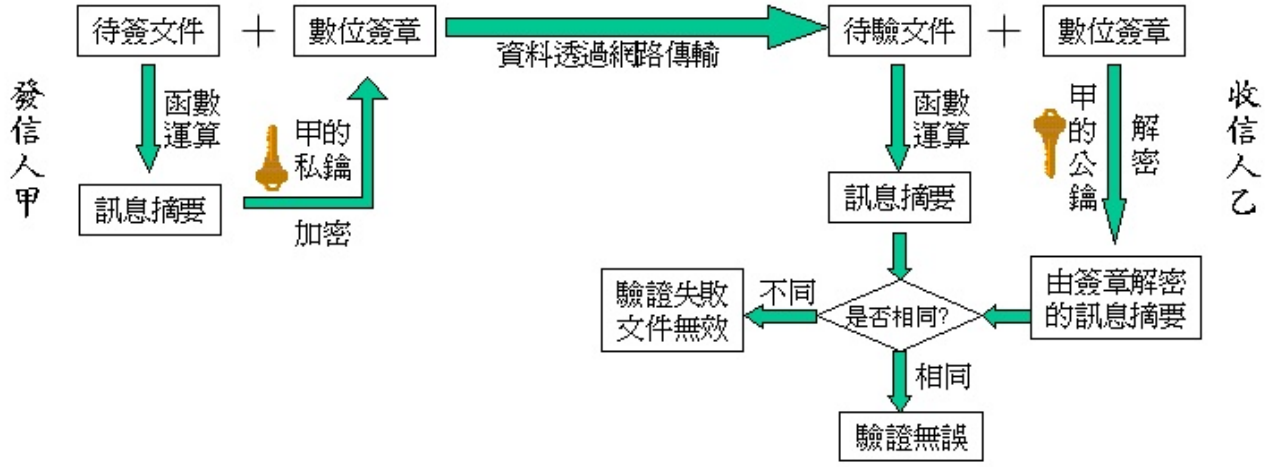

圖5. 電子簽章的運作流程，可用以確認文件的簽署者和內容的完整性

至於爲什麼製作電子簽章時，要先將文件轉換爲摘要，再進行加密呢?這是因爲我們的需求重點不在於將文件本身保密，因此爲了縮短加密與解密的時間，就先將文件簡化再進行加密而製成電子簽章。如果是將整份文件加密，所需的時間可能就比較久了。

數位憑證

前面所說的金鑰法除了用在私人信件的寄送外，由於它具有保密和不可否認的特性，使得它在電子商務的應用更是廣泛。由於所有必須使用保密方式傳送訊息的場合，都需要先取得公鑰，因此如何將公鑰安全而有效的提供給所有需要的人，就成爲一個問題。因此，也就有所謂「數位憑證」的觀念產生。

所謂數位憑證(Digital Certificate)，其實就是一對由公正單位所核發的公鑰和私鑰。這個公正單位可能是政府機構或者具有公信力的民間組織，專門負責核發使用者的數位憑證，稱爲憑證管理中心(CA，Certificate Authority)。使用者可以到憑證管理中心設在各地的服務窗口申請，同時繳驗身分證件以證明確實是本人。接著各地服務窗口會將這些申請資料彙整到管理中心作認證，通過後就由管理中心分別製作該使用者的公鑰和私鑰對，然後將私鑰傳回申請窗口，再轉存到磁片交給申請人保管。至於公鑰的部分，則轉送到一個目錄管理中心集中存放，任何人有需要的話，就可以到目錄管理中心查詢到你的公鑰。

當然數位憑證不只是公鑰和私鑰而已，爲了確認公鑰的確是由憑證中心所發出，使用者在目錄管理中心取得的其實不只是一個公鑰，而是包含憑證中心的相關資料，以及經過憑證中心私鑰加密產生的數位簽章。根據前面提過的不可否認特性，我們可以驗證這個數位簽章，以確定這份文件是由憑證中心所發出。而由於當初申請人必須繳驗身分證明文件，因此可以進一步確認這個數位憑證確實屬於這個申請人所有。

這麼一來，我們就可以把數位憑證當作是我們在網路上面的身分證。有了這個網路身分證，而能放心的進行各種網路交易，或者像報稅、繳錢等等必須確認身份的活動，不會再有信任的問題產生。但另一方面，這同時也表示，只要是經由數位憑證確認過的網路行爲，就可以視爲是該使用者所親自進行的行爲，是具有法律效力的，不能抵賴不認帳。

或許你會說，萬一我手中的私鑰檔案被偷了，或者因爲磁片損壞等等而無法使用了，這樣怎麼辦?其實，就像身分證掉了可以申請補發那樣，使用者可以視自己需要，隨時向憑證中心申請更改或補發數位憑證。這樣憑證中心就會重新產生一份公鑰和私鑰對，並且自動更新放在目錄管理中心的數位憑證。這樣即使有人竊取了你的私鑰檔案，由於憑證中心的公鑰已經更改了，因此也無法利用這個私鑰來假冒你的身分。不像現實世界中身分證掉了雖然申請補發，結果原先遺失的身分證還是有可能被歹徒拿去做壞事。比較起來，網路上的數位憑證甚至比身分證還要安全。

安全電子交易協定

有了上面幾種進行電子商務所需的保密與認證措施，我們就可以綜合這些措施來進行網路交易，使得下訂單和付款得以安全地透過網路進行。這部分目前也已經有了標準的步驟，稱之爲安全電子交易協定(Secure Electronic Transaction)，簡稱爲SET。

在安全電子交易協定的規範下，消費者首先必須向信用卡發卡銀行申請一

個帳號，銀行則轉向憑證認證中心認證後，核發另一個銀行用的數位憑證給消費者，作爲他在網路交易時的身分證明。當消費者再網路進行購物時，就會將訂單(包含貨物種類與數量)及付款指令(包含信用卡帳號與付款金額等)傳送給商家網站，並附上自己的數位憑證。這時，商家本身可以拿這個消費者提供的數位憑證，向憑證管理中心確認這個消費者的身分，再將付款指令傳送給商家習慣結帳用的銀行，請這個收單銀行協助向消費者的發卡銀行確認他提供的信用卡有效期限。如果都確認無誤，商家就可以放心的出貨。至於付款的部分，則由商家所屬的收單銀行定期與消費者的發卡銀行進行結算，將錢從消費者的發卡銀行帳户轉移到商家的收單銀行帳户裡面，這樣就完成了付款的手續(如圖6)。如此消費者收到貨品，商家透過收單銀行向消費者的發卡銀行收到貨款，銀貨兩訖，皆大歡喜。

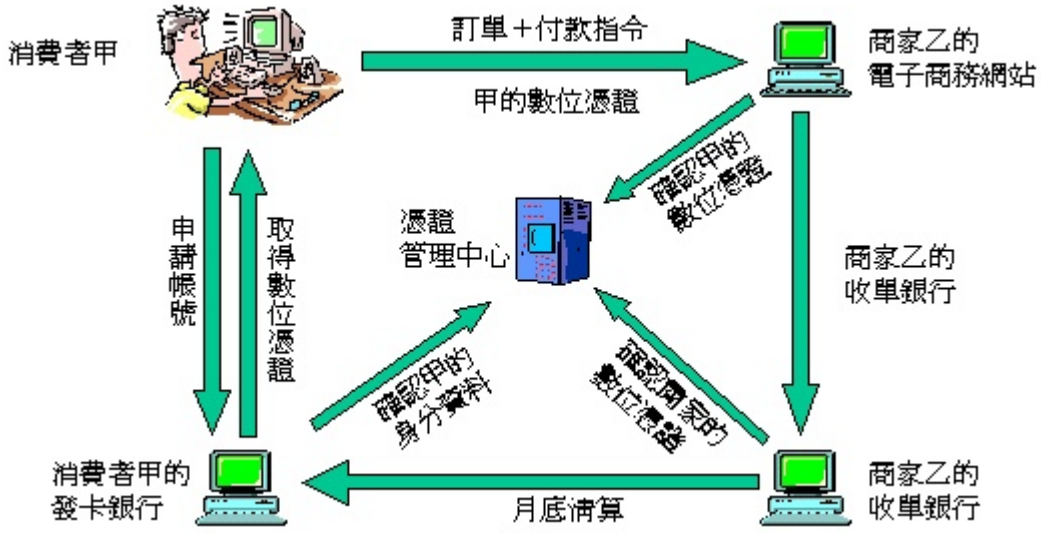

圖6．安全電子交易協定SET架構的運作流程

電視上常常會有這樣的新聞：不肖商家利用消費者使用信用卡刷卡購物時，偷偷竊取消費者的信用卡資料，然後複製一片假的信用卡到處刷卡騙錢。既然現實世界有這樣的事發生，或許有人會擔心，我們透過網路傳送的這些資料，會不會有被盜用的危險?例如我們傳送的付款指令裡，包含了信用卡帳號與付款金額等資料，商家會不會利用這些資料，另行僞造假的付款指令來向發卡銀行收錢?或者直接更改付款金額，來收取更高的貨款?

其實這一點倒是不用擔心，因爲在安全電子交易協定SET架構中，我們傳送給商家的訂單和付款指令資料其實都經過加密處理，並不是簡單的一封電子郵件而已。這個加密的步驟稱之爲雙元簽名(Dual Signature)，它使用了消費者本身的私鑰、付款銀行的公鑰，以及一個在消費當時隨機產生的祕鑰來分別進行加密措施，以確保商家只能看到訂單的內容，而付款指令裡的內容則只有發卡銀行才能看到，其他不相干的人士則什麼都看不到。另外，過程中也大量使用函數運算產生摘要，再加密成爲電子簽章，以確保所傳送的訂單和付款指令在過程中不會被更改。由於過程十分繁複，在此不作詳細說明，有興趣的朋友

可以自行到書店裡參考相關的書籍。

簡單的說，透過這個雙元簽名的方式，除了可以確保資料不會被更動之外，更可以讓傳送的內容只有當事者知道。銀行不知道消費者究竟買了什麼東西，而商家本身則連消費者的卡號是什麼都不知道。這樣嚴密的保護措施，使得在網路上購物，甚至比在現實世界中刷卡消費還要安全。

電子貨幣

那麼，對消費者來說，我們要如何在網路上消費購物呢?因爲買賣雙方見不到面，所以不能一手交錢一手交貨，因此必須經由網路交錢。這時，就可以採用電子貨幣。

電子貨幣的觀念跟信用卡有點像。在現實世界中，消費者先向發卡銀行申請信用卡，然後銀行會給他設定一個銀行帳號和一張信用卡，這時消費者就可以拿這張信用卡在商店裡刷卡消費。當他刷卡時，商家的刷卡機就會與銀行連線，確認這張信用卡是否可用，然後就會記錄這筆交易，月底時再統計整個月的消費金額寄送帳單，請消費者繳錢。因此，消費者不需要隨身帶著一大筆現金，不用怕被偷被搶。就算信用卡眞的被偷了，只要打個電話掛失，重新補申請一張信用卡就行了，先前被偷的那張信用卡就變成無效。因此，信用卡本身又被稱爲「塑膠貨幣」。

那麼，在網路交易上要怎麼刷卡消費呢?過去通常是請消費者把自己的信用卡帳號透過網站的對話框輸入，然後商家那邊再拿這個信用卡號碼來向銀行刷卡收錢。但這樣一來就有點危險，先不說信用卡號碼在網路傳輸時會不會被竊聽(這可以用加密方式解決)，問題是商家那邊得到你的身分資料和信用卡號碼後，會不會趁機亂刷你的信用卡，或者複製一份新的信用卡?由於有這樣的疑慮，使得許多人不敢在網路上刷卡消費。

不過，利用前面提到的安全電子交易協定SET機制，我們可以不用讓商家知道我們的信用卡號碼，就可以在網路上消費。這時我們可以採用所謂的「電子貨幣」，方法有以下幾種：

1. 電子信用卡

我們可以先在銀行申請帳號，經由認證後，取得一份銀行核發的數位憑證、私鑰和信用卡資料。然後，我們就可以在家裡的電腦安裝一個程式，把這些資料放在裡面。這個程式會自動管理和儲存銀行發給我們的私鑰，並且紀錄我們在銀行中登記的基本資料，包括我們的數位憑證以及銀行本身的電子簽章。當我們在網路消費時，程式就會幫我們傳送加密好的訂單和付款相關資料，並且紀錄交易過程以便日後查詢。這樣一來，這個程式本身就成爲一個「電子信用卡」。而且交易時不用簽名和刷卡的動作，一切由電腦自動處理，比現實社會的信用卡更方便好用。

2. 數位現金

使用信用卡雖然方便，不過由於使用後會留下紀錄，例如某某人在某某時候在某處買了什麼東西。這樣一來，消費者的行爲可能就會暴露出來，失去隱

私。因此在某些特殊場合(例如要去花天酒地吃喝嫖賭等等)，有時候我們不希望使用信用卡，寧可付現金。以免月底收到帳單時，被人發現我們到了不該去的地方，引起更大的麻煩。

在網路上交易，其實也會有相同的問題，因此就有所謂的「數位現金」出現。它是由消費者先在銀行申請一個帳號，然後拿現金轉換成等值的數位現金，存在這個帳號中。而且，就像現實社會中的鈔票會有號碼以免僞造，數位現金本身也都有編號，因此就算有駭客入侵把帳號裡的數字增加，也無法使用。由於數位現金具有和現實社會中等值的現金相同的效力，因此在網路消費時，就可以使用這種數位現金來付款。商家方面不用知道使用數位現金的人是誰(因爲裡面沒有個人基本資料)，只需由銀行內部查驗這筆錢是否有被重複使用就行了。整個交易並不會被紀錄下來，因此也不用擔心別人知道你買了什麼東西。

數位現金的觀念雖然不錯，但實際使用時，卻面臨一些問題。例如在消費時必須查驗數位現金本身是否有重複使用，不然這筆錢就變成僞鈔了。但這樣一來相對的就會浪費許多時間(雖然電腦速度很快)，造成消費者的不便。另一方面，由於數位現金必須先用眞正的現金來購買轉換，當我們在外國消費時，就會面臨到匯率轉換的問題，可能會無形中浪費不少錢。因此在實際使用上，數位現金並不普及。

結語

以上談的都是各種網路交易的安全機制，經由這些說明，我們可以知道，雖然網路通訊有被竊聽的危險，但只要事先做好加密措施，在完善的網路認證機制下，網路交易其實比現實世界還要安全。

然而，正如同先前在介紹金鑰加密措施時所說的，這些網路加密措施雖然能保證我們在網路傳送的資料不會外洩或遭到竄改。但正由於有這種保證，因此經由這樣的方式所傳送的資料也同時具有不可否認性。因爲私鑰只有你本人手中才有，因此經由你的私鑰加密過的資料，就具有法律效力，你也不能推託說是別人假借你的名義來使用的。因此數位憑證和私鑰，其實就跟現實社會中的身分證和印鑑一樣，都必須加以妥善保管。如果別人能夠任意的使用你的電腦裡已經安裝好的數位憑證和私鑰，就可以用你的名義來作任何行爲，而且這些行爲事後都必須由你負責。這樣就像你把自己的身分證和印鑑隨便亂放，結果被人拿去簽合約、賣房子，這時想要補救就很難了。

問題是，身分證和印鑑很重要，人人都知道，大概也不會有人隨便亂放。但是，對於電腦的安全使用觀念，許多人卻都還是一知半解。於是我們往往可以看到許多高層長官由於本身不懂電腦，因此就由底下的小妹來幫他打字。因此長官的帳號密碼，小妹也都知道。如此一來，就會出現小妹批公文的詭異現象。

因此，雖然電子商務在技術上並無問題，但目前最大的問題，卻可能是「人」的問題。由於社會進步太快，許多人可能一時無法適應，甚至產生抗拒

排斥的心理。特別是在傳統的農業界，這樣的現象更是嚴重。這些都可能阻礙到我們本身的進步與發展，喪失許多競爭先機。下期就讓我們談談這方面的問題，敬請期待。