CA 制度對期貨網路及專屬線路 DMA 下單之高階決策分析

委託單位: 中華民國期貨業商業同業公會

主持人：游張松 台大商研所教授

共同主持人：譚修齊 思源智庫

計畫期間：2006/9/1~2006/12/31

目　錄

圖　表

表　格

壹、計畫緣起：

自從網際網路蓬勃發展以來，無遠弗屆的電子商務順勢興起。因此，消費者可以從遠端瀏覽、購物、支付購物款項、查詢銀行帳戶餘額等等，不受到營業時間的限制且免除舟車勞頓，便利異常，於是乎電子商務日益發達。

然而只要有交易就可能產生交易糾紛，所有交易糾紛都必須有效地避免。電子交易的一個特性就是處理的速度快，並且可以同一時間內大量處理。直覺上，一旦有詐騙交易發生，則很有可能以更快的速度、在更短的時間內造成比實體交易更大的詐騙風險。於是，更有事先防範的必要。

電子商務因為其不需臨櫃辦理的便利性，更有不肖之徒因而行詐騙之實。源自於「電子化---虛擬化」所引發的糾紛，相對於實體交易而言，就成為一般人較無法理解的 「虛擬」問題，例如舉證的困難。其中，所謂的電子交易人身份難以確認，以及交易可能被交易人否認等等都是最常被提及的問題，也都是相當不易處理的技術問題。

為了確保交易不致發生糾紛，甚至，在糾紛發生時得以順利處理，很多防範交易詐騙的方法因而被提出，包括 IP 紀錄、MAC 位址鎖定，以及憑證確認等等，都是大家耳熟能詳的方法；其中，DMA 及 CA 是我國政府對證券或期貨網路下單所要求的法定防範方法。而且我國也是全世界要求期貨交易網路下單時，必需要 CA 認證的唯一國家。於是，我們有了下列值得探討的課題：

1. 期貨交易網路下單之 CA 認證及專屬線路 DMA 的法令規定，當然有其必要性。然而，CA 認證及專屬線路 DMA 規定的目的為何？
2. 期貨網路下單 CA 認證及專屬線路 DMA 之必要性?

3. 專屬線路 DMA 之意義為何？能達成哪些功能？

4. CA 之意義為何？能達成哪些功能？

5. 期貨網路下單 CA 認證及專屬線路 DMA 之比較?

6. 法定執行 CA 認證時，所付出的代價為何？

(1) CA 真的是絕對的必要嗎？如是，為什麼先進國家如美國就沒有 CA 的法定要求？他們是用什麼方法？怎麼做到問題防範的？

(2) 我國法定執行 CA 認證時，所付出的代價為何？

(3) 推動國際化時，CA 認證之法定要求會造成哪些困擾？

對絕大多數的高階主管而言，CA 是一個技術問題，也是一個不容易探討的問題。其系統化的真相，有待對其作近一步的分析，作為高階主管決策的參考。

貳、計畫目標：

本計畫之目的為對 CA 及 DMA 的網路交易技術及規定作一個適合高階主管所需的模組化拆解、分析、闡釋；對 CA 與 DMA 做法作一個比較；分析其與國際化接軌之難題；同時討論是否有替代方案的存在以及其可行性和成本效益。

全球目前最大的 CA 發行公司為 VeriSign，而且 VeriSign 的 2005 年度毛利高達 US$1.1 billion [6]。 可見只要營運得當，CA 認證是一個利潤極其豐厚的行業。CA 認證絕對是一個值得探討的主題。

參、CA 與 DMA 之目的及其必要性：

期貨交易網路下單之 CA 認證及專屬線路 DMA 的法令規定，當然有其必要性。為釐清立法的精神，本節就以下的課題進行分析：

CA 認證及專屬線路 DMA 規定的目的為何？

期貨網路下單 CA 認證及專屬線路 DMA 之必要性？

憑證授權，Certificate Authority，簡稱 CA，係一個公正的第三者作為 CA 憑證審核及發放的單位，提供彼此信賴的平台環境。CA 認證意指 CA 的使用者是經過 CA 發證單位認證之後才獲得這個 CA 的使用權。利用專屬線路（Direct Market Access）委託下單時，這種下單方式或者該專屬的線路，就稱作 DMA。

CA 認證的目的：在現行期貨網路下單的情境之下，網路下單者若依照 CA 認證的規定，則該下單者必須採用 CA 憑證才能執行網路下單的程序，從而完成下單。因為該下單者的 CA 憑證是經過認證之後才獲得的，因此該下單者的身分及其下單程序是可靠的。

專屬線路 DMA 的目的：在現行期貨網路委託下單的情境之下，網路下單者若依照 DMA 的規定，則該下單者必須使用被核可的專屬線路才能執行網路下單。因為該線路係屬 “專屬” 性質，並非一般人等所能接觸、使用，所以該下單的作業是在被保護／管制之下完成的，因此，該下單的單程序也是可靠的。

身份認證或專屬線路的必要性：金融服務為嚴密考核之特許業務，參與者之身分及其作業都必須在嚴格監管之下進行。因此，期貨下單者的身分及其下單作業程序的確認與監管，都有其必要性。

雖然，身份確認及作業流程監管都是必須執行的稽核作業；其中，CA 認證是身份確認的方法之一，而 DMA 則是確保線上下單作業不被侵入竄改的方法之一。因此，期貨下單者的身分及其下單作業程序的確認與監管，都有其必要性，但是 CA 認證或專屬線路 DMA 卻都只是執行的方法之一而已。換言之，CA 認證或專屬線路 DMA 雖有其需要性，其實作方法有很多種；在某些情況之下，可能就有其他的執行方式，或者有其他方法可以取代；甚至，在某些特別的情況之下，根本就不需要了。

肆、現況概述

一、台灣期貨電子交易現況

投資人透過網路下單的方式交易證券，自 1996 年起隨著網際網路的普及開始在美國風行，而隨著這股熱潮，我國也在民國八十七年導入，時至今日，網路下單已經成為期貨交易的主要管道之一。

期貨交易網路下單提供了投資人一個全然不同的交易管道，使得投資人不必受限於時間、空間等因素，交易的便利性大幅提升。網路下單的流程當然也與傳統上透過電話或是親自臨櫃的方式明顯不同，以下將簡短介紹之。

首先，網路下單的客戶經由網路將委託單送至期貨商的網站主機，通過初步檢驗後，就可以用終端機下單。網路的下單經期貨商的網站主機確認後，即會利用內部網路傳送至交易主機，再透過 X.25 分封網路傳送到期交所主機撮合。

網路下單與一般傳統下單最大的不同在於，所有資料的傳遞皆是透過電腦完成，資料在傳送過程中很容易遭到他人不法的增減，竊讀等，通訊安全於是成為一項重要的議題。

針對電子商務安全性的問題，我國自民國 90 年通過電子簽章法草案，以及期貨商營業規則，規定期貨商全面採行電子憑證(Certificate Authority，以下稱 CA)認證制度。投資人必須先經過第三者憑證機構認證，方得下單。

二、遭遇問題與機會點

資料顯示，絕大多數的電子交易安全事件都不是技術問題，而是管理的問題；而且政策的決定關鍵，應該超越技術，以長遠的發展為決策依據。

台灣期貨市場正朝著國際化進行，希望能夠吸引大量外資進入。為了增加國外投資人交易的便利性，因此目前來說國外投資人在我國下單是不需要通過

電子憑證認證的，這樣的雙重標準，對台灣邁向國際化實屬不利，是否有通盤統一的作法，值得討論。

使用 CA 認證尚有成本面的問題。投資人網路下單前都必須經過憑證管理機構的認證，而認證的同時必須支付憑證管理機構一筆費用，隨著期貨交易的日漸盛行以及交易量的提升，這筆費用將不容忽視，所以我們不禁會想，是否有其他方法可以減少這筆花費呢？

期貨交易網路下單的全盤採行 CA 認證，的確增加了網路交易的安全性，但是實際上還是無法保證所有的網路交易都是安全的。民國九十年七月，刑事警察局偵破了一件電腦駭客入侵網路下單系統的案件[20]，也證明了 CA 認證制度上仍有作業上的漏洞，並非有了 CA 就可萬無一失。

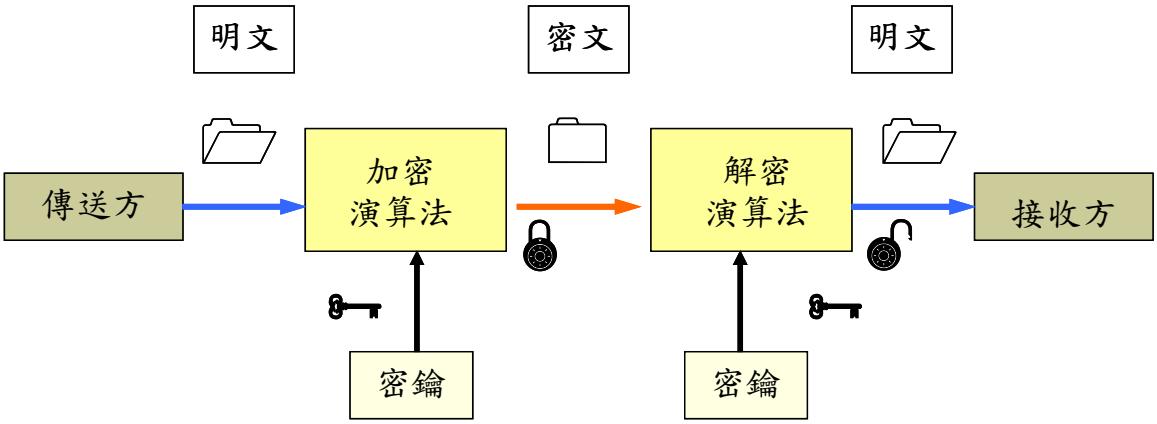
該事件為駭客入侵至電子下單系統盜取客戶資料。該駭客連續入侵了兩家券商的電子下單系統，共竊取了兩千餘位客戶的帳號及密碼等資料，然後再利用這些資料委託下單炒作股票並從中牟取暴利。

該事件的第二段為取得客戶電子憑證。該駭客入侵第二家券商系統時，因客戶端需電子憑證方能交易，因此該張姓嫌犯冒用客戶的身份申請電子憑證，竟也順利向認證中心取得電子憑證。電子憑證正是電子交易機制中扮演身份認證最重要的依據，於是該駭客就具有被害人所能行使的所有權利。

伍、技術分析

在進一步探討電子憑證之前，首先說明網路通訊安全的設計。基本上，為確保訊息在網路上傳遞的安全性，最直接的做法是將傳送的資料以某種密碼格式加以轉換，以避免非關係人的解讀。一般性的密碼系統，可以下圖表示之：

圖表 1：密碼系統

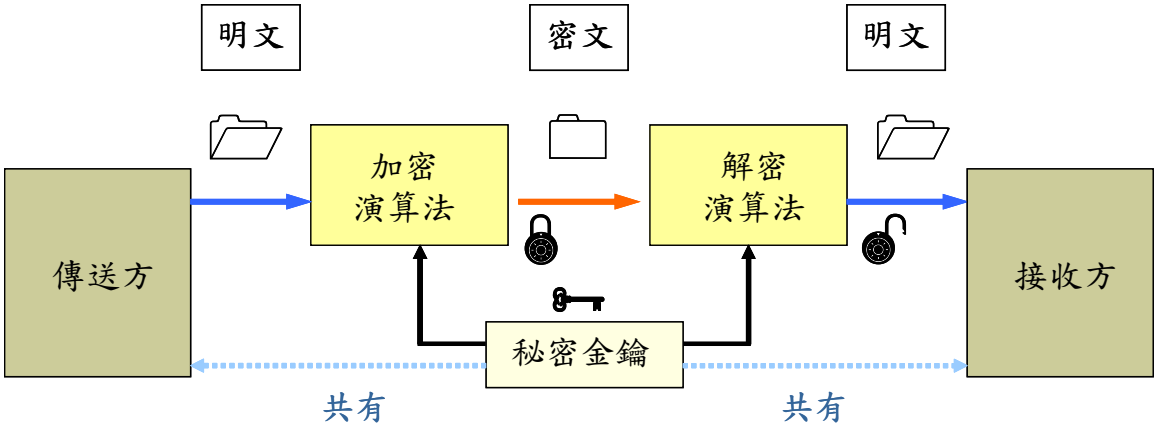


資料來源：Shieh, S.P.; 本研究整理

傳送方透過加密演算法(Encryption Algorithm)和密鑰將明碼訊息編譯成密碼資料後，經由網路傳遞給接收方，再經過解密演算法(Decryption Algorithm)和密鑰，將密碼資料還原為明碼訊息。

若是傳送方與接收方共用同一秘密金鑰，則該密碼系統稱為對稱式(如下圖)：

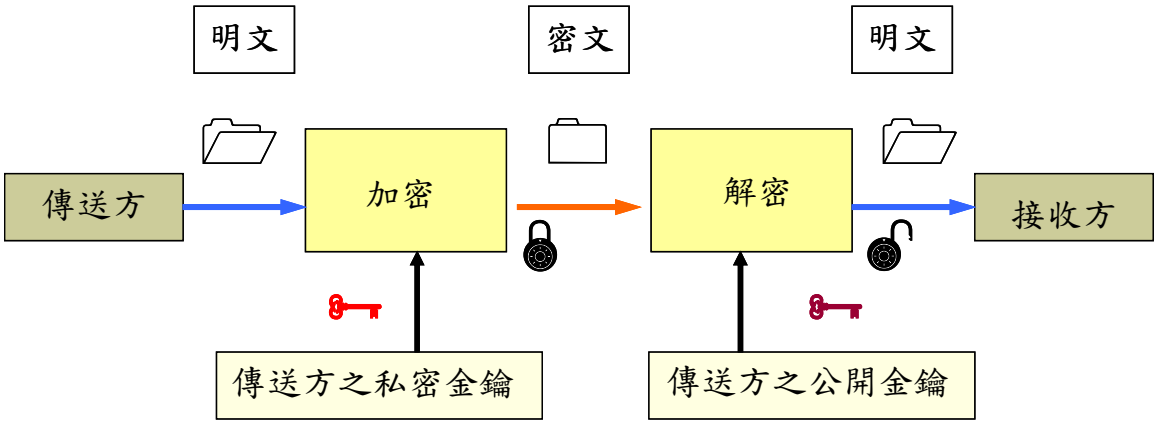
圖表 2：對稱式密碼系統



資料來源：Shieh, S.P.; 本研究整理

若是傳送方與接收方各使用不同的秘密金鑰，則該密碼系統稱為非對稱式(詳如下圖)：

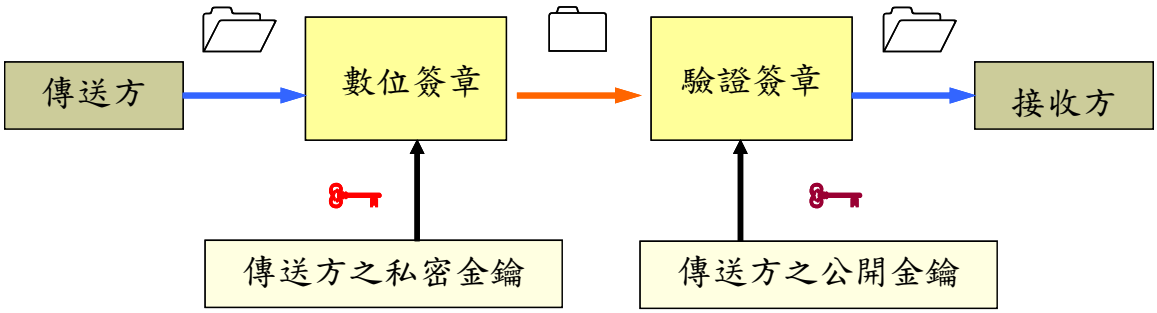
圖表 3：非對稱式密碼系統



資料來源：Shieh, S.P.; 本研究整理

然而，在資料傳輸量極為龐大時，將所有的資料加密所耗費的時間及資源並不經濟；亦或是傳遞資料的敏感性有限，但其真偽具備高度的重要性，因此，另一項變通的做法是以明碼的方式傳遞資料，但是產生一數位簽章附加在傳遞的訊息之上，以做為接受方驗證之用，其概要如下圖所示：

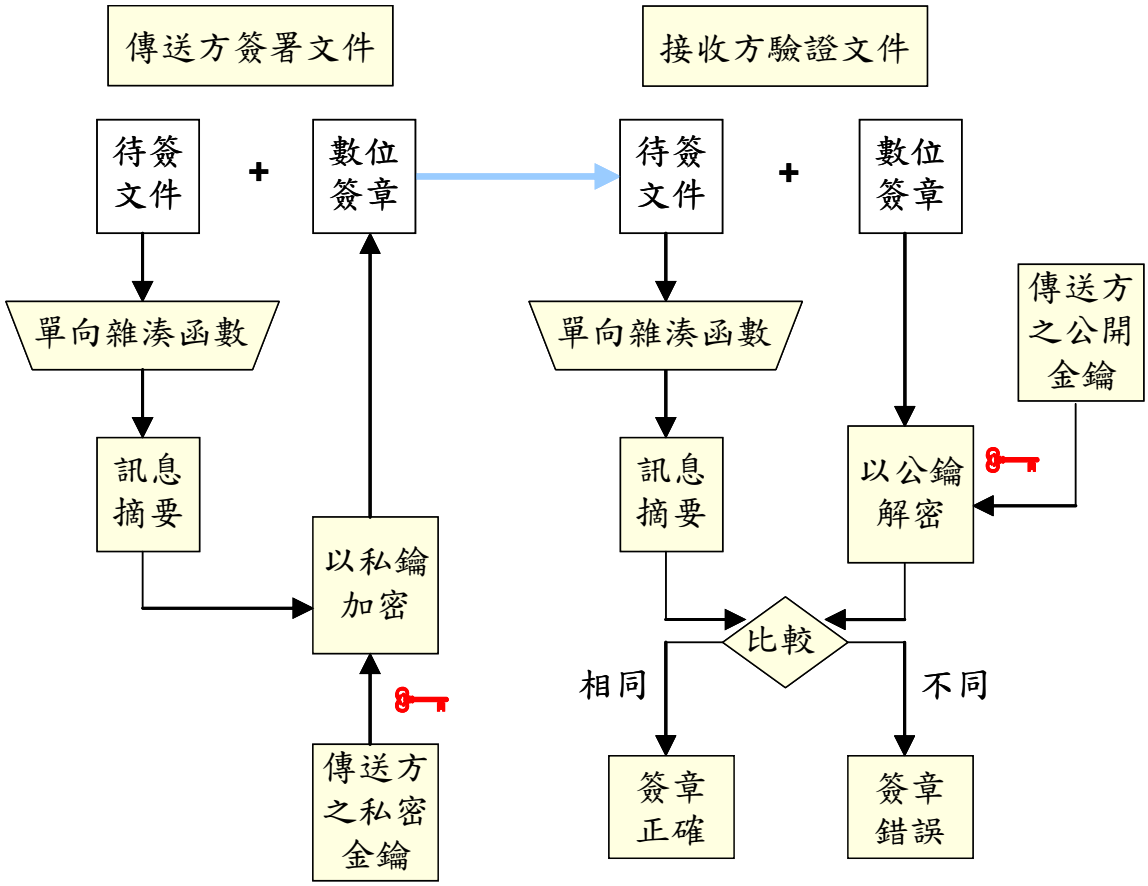
圖表 4：公開金鑰密碼系統簽章



資料來源：Shieh, S.P.; 本研究整理

為達到上述資料交換與驗證的目的，並維護傳送方資料之安全性，數位簽章是透過傳送方保管的私密金鑰加密產生，接收方則是透過傳送方的公開金鑰加以解密驗證。具體言之，傳送方欲傳遞的資料經過一單向雜湊函數(Hash Function)的運算後產生一訊息摘要，並透過其私密金鑰加密產生數位簽章一併透過網路傳遞給接收方。接收方收到資料後同樣經由雜湊函數產生訊息摘要，並且將收到的數位簽章以傳送方的公開金鑰解密後，兩相比較，若是相同則表示簽章無誤；若否則表示簽章錯誤，有可能在傳遞的過程中發生問題。

圖表 5：數位簽章與簽章驗證



資料來源：Shieh, S.P.; 本研究整理

一、電子簽章與數位簽章

傳統上文件的簽章是在實體紙本上實施，如此方能經由辨別簽章之真偽確認使用者之身份，簽章具有身份確認及不可否認性的效力。在現今的環境下，網路交易及電子檔的使用日益頻繁，然而網路上交易雙方彼此無法見面，安全性也有待評估，若要確認資料是否為特定人所發以及是否遭到竄改，則需要使用電子簽章加以驗證。

電子簽章法對電子簽章及數位簽章之定義[17]：

電子簽章(Electronic Signature)

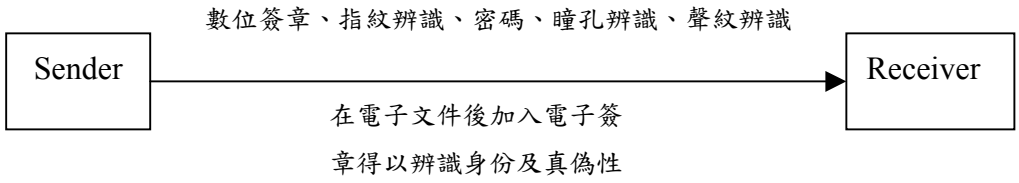
指依附於電子文件並與其邏輯相關，用以辨識及確認電子文件簽署人身份、資格及電子文件真偽者。

數位簽章(Digital Signature)

指將電子檔以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。

根據電子簽章法的定義，電子簽章是指一種依附於電子文件，用以辨識及確認身份、真偽性之事物。任何的電子技術，只要能做到滿足身份確認、完整性、及不可否認性，均可做為電子簽章。故使用非常廣泛，如數位簽章、指紋辨識、密碼、瞳孔辨識、聲紋辨識等均可做為電子簽章之用途。

圖表 6：電子簽章



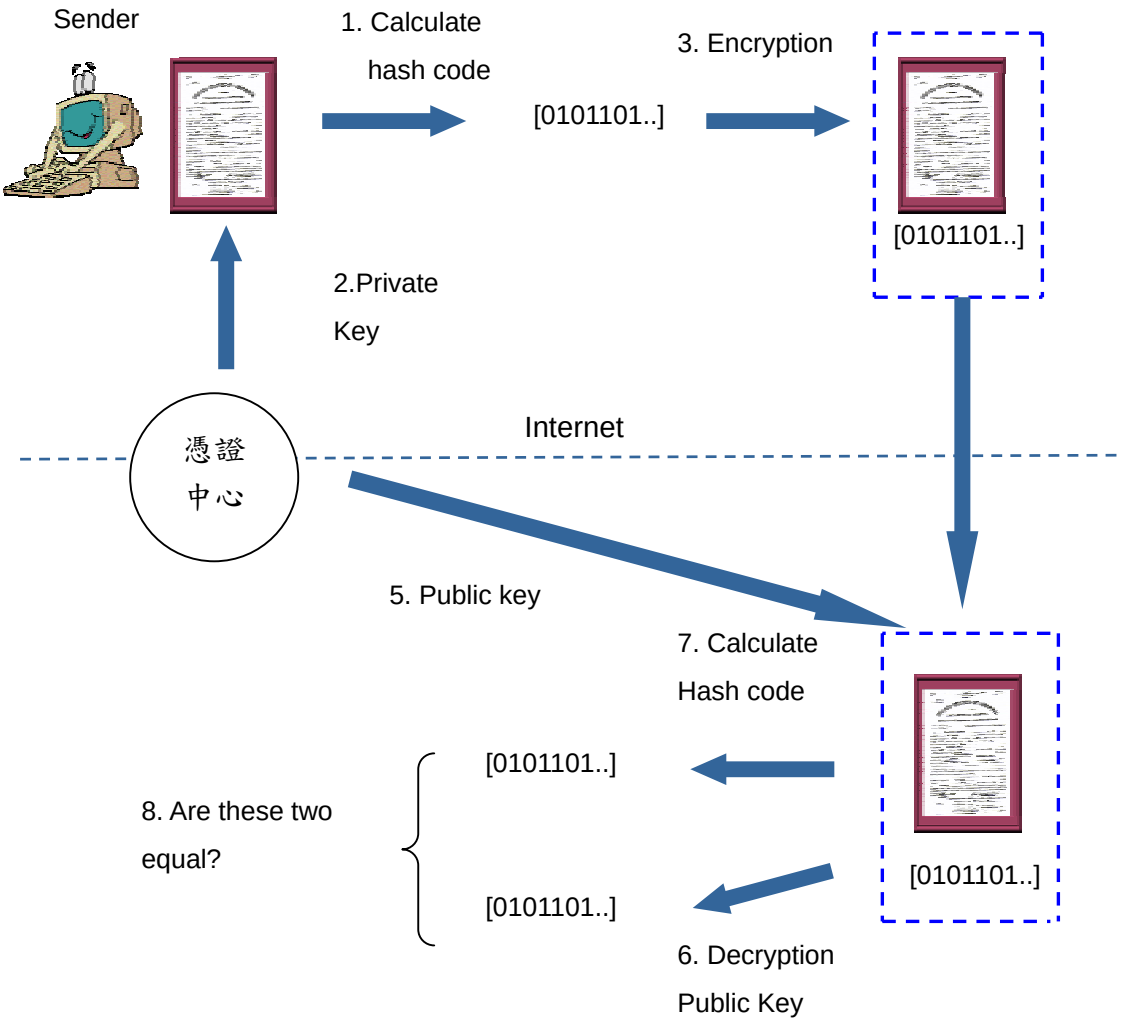
資料來源：本研究整理

目前應用最廣泛及最成熟的電子簽章技術為數位簽章。數位簽章為「非對稱密碼系統（Asymmetric Cryptosystem）」加密技術之應用，其流程如以下所示：

1. 首先將電子檔以特殊演算法運算出一定長度之數位資料雜湊碼(hash code)
2. 向憑證機構申請憑證服務，憑證機構驗證身份後發給私鑰(Private key)
3. 利用私鑰將電子文件及其雜湊碼加密
4. 傳送加密檔案
5. 接收方接到加密檔案，可從憑證中心取得對應私鑰之公鑰(Public Key)
6. 利用公鑰解密後得到電子文件及其雜湊碼

7. 利用特殊演算法計算文件之雜湊碼
8. 比對算出之雜湊碼與傳送之雜湊碼是否一致

圖表 7：數位簽章流程圖



資料來源：本研究整理

由以上得知，數位簽章不但是電子簽章的一種，也是公開金鑰基礎建設(Public Key Infrastructure “PKI”)機制的運用。

PKI 交易流程

1. 傳送方先利用雜湊函數得到欲傳遞訊息之雜湊值，並將該雜湊值附加在訊息中
2. 傳送方利用接收方的公開金鑰為訊息加密
3. 傳送方再利用自己的私密金鑰為訊息加密 (私密金鑰僅傳送方本身持有，加密後傳送

方將不可否認其身分，同時透過私密金鑰的保存將可達到存取控制的要求)

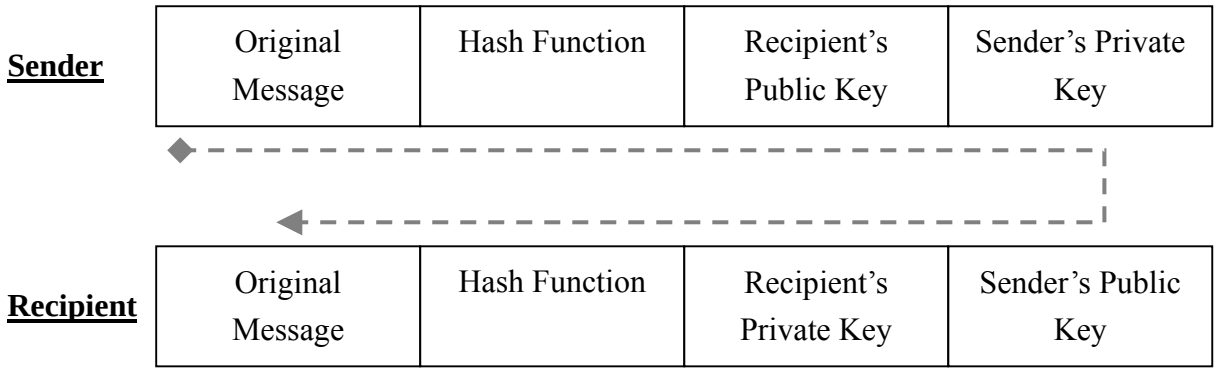
4. 加密後的訊息透過網路傳遞給接收方

5. 接收方利用傳送方的公開金鑰解密 (確認此訊息的確為該傳送方所加密送出)

6. 接收方再利用自己的私密金鑰解密 (確保訊息不會被非接收方的人攔截解密)

7. 接收方再利用雜湊函數得到訊息的雜湊值，與收到訊息中的雜湊值比對 (確認訊息內容未被他人修改，確保其完整性)

圖表 8：PKI 機制運作流程示意圖



資料來源：本研究整理

二、現行技術應用

1. CA

(1) CA 簡介：

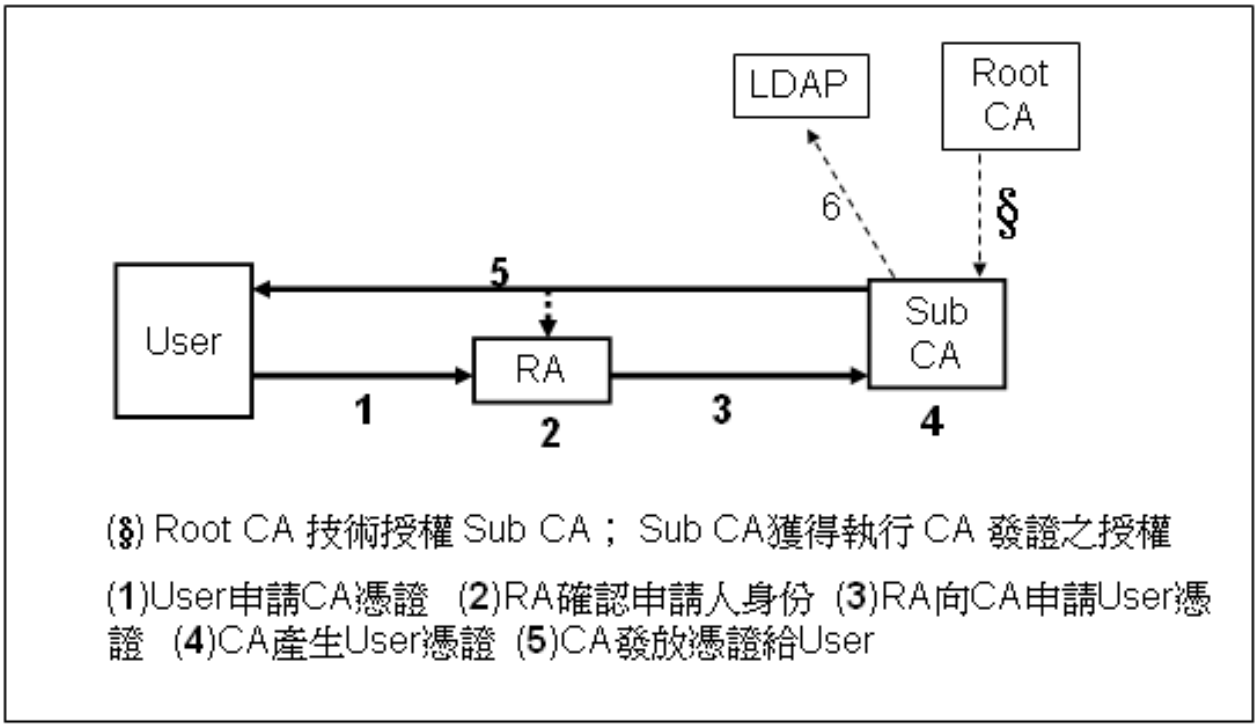
憑證授權(Certificate Authority 或 Certification Authority)，簡稱 CA。CA 的身份像是公正第三者，必須是可被傳送者和接收者信賴的角色，依據合法申請者的請求發出數位憑證，數位憑證裡面包含了申請人的「辨識資料、公鑰及 CA 對這把公鑰的簽章」，有 CA 的簽章背書後，我們就可以信賴這把公鑰。在網路上透過 CA 的公鑰的驗證使交易雙方得以辨識對方的身份，彼此在高度的信賴下進行電子商務。

網路交易之雙方，通常彼此互不相識，為避免交易危機，需要一個「公正的憑證中心」（Certificate Authority）提供身份證明的服務，該機構核發「網路印鑑證明書」（又稱電子憑證）以建立買賣雙方於網路交易之信任基礎。

CA，即憑證管理中心，負責執行憑證簽發、註銷、管理等核心作業，以及將簽發之憑證資料及憑證註銷清冊（Certificate Revocation List, CRL）公佈於目錄伺服器，以供外界查詢及下載。

(2) CA 發放流程機制：

圖表 9：CA 發放流程機制



資料來源：本研究整理

註：Lightweight Directory Access Protocol (LDAP)是一種可讓任何人找到網路中的組織，個人或檔案或裝置等其他資源的一種軟體協定，不論是公共網際網路或企業內網路。顧名思義，LDAP 是「輕量級」 (程式碼較少 smaller amount of code) 版本的 DAP（Directory Access Protocol)，DAP 是網路目錄服務標準 X.500 的一部分。LDAP 因不包含安全措施而使程式碼比較少。

LDAP 由美國密西根大學所發明，目前已有 40 家公司採用，如 Netscape 已將之包含在最新版的 Communicator 套裝產品中，它也被微軟加入 Outlook Express 等產品一項名為「Active Directory」中。Novell 的 NetWare Directory Services 可與 LDAP 相容，Cisco 的網路產品也支援。

在網路中，目錄可協助尋找特定物件的位置。在 TCP/IP 網路(including the Internet)中相對於特定網路位置的網名，構成的是目錄系統稱為網域名稱系統（DNS）。LDAP 可幫助尋找到個人，即使其位置並不清楚。

LDAP 的目錄，為一層層分支出去的樹狀圖，從根目錄下，細分國家、地區、組織、小組織及個人。整個目錄分布在許多伺服器中，每個伺服器都複製了一個整體分支圖，定期同步化資料。一個 LDAP 伺服器被稱作 Directory System Agent (DSA)，由使用者處接受到要求指令，並在必要時傳給其他 DSA，並確保有單一伺服器可真正執行任務。 (資料來源: Taiwan.CNET.com)

(3) CA 之特性：

1. 機密性：在公開金鑰基礎建設(Public Key Infrastructure)加密機制中，利用接收者的公開金鑰(Public key)為訊息加密，接收者再利用自己的私密金鑰解密，則確保訊息不會被他人攔截解密。
2. 身分認證:每一參與交易者皆需向公正可信賴的第三者(CA)取得合法的交易憑證，以確認其身分，故交易資料不會被冒名傳送。
3. 完整性：於網際網路上傳輸的任何訊息皆以雜湊函數(Hash)產生訊息摘要,再以訊息發送者的私密金鑰(Private key)對摘要後的訊息執行數位簽章保護(Digital Signature)；接收者利用發送者的公開金鑰解密與雜湊值比對，以確認訊息內容完整性，未被他人非法竄改。
4. 不可否認性：傳送者以自己的私密金鑰(Private key)為訊息加密，執行數位簽章，接收者用傳送者的公開金鑰解密，確認此訊息的確為該傳送者所加密送出。由於私密金鑰僅有傳送方才擁有，只要留存每筆包含電子簽章的交易紀錄，則交易的收發雙方均不能否認已傳輸的交易。
5. 存取控制：一個安全系統由確認、認證和授權三個不同元素所組成，結合起來便形成所謂的存取控制，只有獲得授權的各方能夠保護和存取資源。CA 可防止未經授權的電腦存取，並透過 PKI 私密金鑰保管機制的設計，達到存取控制的要求。

2. SSL

(1) SSL 簡介

SSL 為 Secure Socket Layer[1]之簡稱。由於 WWW 並不會將通過它的資料予以加密，任何攔截 WWW 資料者均可獲知其內容。為了安全起見，網景公司發展出 SSL 網路安全傳輸協定，已成為最為廣泛使用的網路安全協定。在網路傳輸協定層級中，SSL 層屬於 TCP(傳輸層)與應用程式層中間的一個層級，它提供網路傳遞資料的安全保護，避免資料在傳輸過程中被截取或竄改。目前較常見的應用為 SSL Web 網站，若網頁的 URL[2]是以 https:// 為開端者，其中的 s 即代表 SSL 之意。

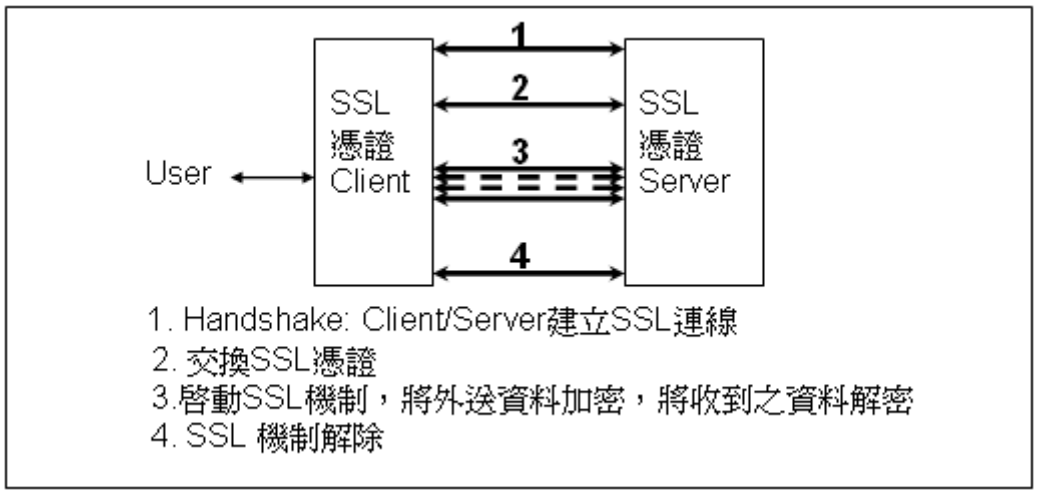
基本上 SSL 是一種網頁的加密機制，對客戶端與伺服器之間的網頁資訊做加密處理，保障資料傳送過程中的安全。主要用來預防如網路監聽側錄(Sniffer)等擷取封包的方式來竊取傳輸資料，因為 sniffer 擷取到 SSL 加密過的封包只會看到一堆亂碼，並無法了解其內容。

[1] SSL 為 TLS (Transport Layer Security)之前身

[2] Uniform Resource Locator

(2) SSL 流程機制

圖表 10：SSL 流程機制



資料來源：本研究整理

運作流程：

1. 使用者(client)與交易對象(server)透過 handshake 確認使用之 SSL 技術與瀏覽器版本，建立一個安全的溝通管道，稱之為 secure negotiated session。
2. 雙方交換憑證，以確認彼此身份。但實際應用上通常只有伺服器端擁有 SSL 憑證，故此一確認身份的程序僅為用戶端單向確認伺服器身份之真實性。
3. 一旦用戶端確認伺服器身份後並願意信任，雙方接下來即可透過上述安全溝通管道的建立，在上面傳遞加密過只有對方才能解讀的訊息，以達到訊息傳遞的完整性與機密性。

(3) SSL 基本運作

SSL 通訊協定包含兩大部份：

a. SSL Handshake 協定

為 SSL 協商處理協定，用來協商伺服器和用戶端之間資料加密的演算法和身份識別的模式，主要目的是讓通訊雙方進行交談協商，決定採用何

種資料加密演算法與辨識通訊對方身份的模式，目前 SSL 有三種身份辨識模式如下：

1. 全匿名式
2. 經認證的伺服主機與未經認證的使用者
3. 通訊雙方均獲身份認證

SSL Handshake 協定是執行 SSL 加密機制的前置步驟，其過程猶如初見面的兩人互相打招呼，自我介紹一番後再進行對話協商一樣。

b. SSL 記錄處理通訊協定

用來定義 SSL 內部資料的格式，並對資料進行解/加密的服務。由於 SSL 協定是介於應用層與網路層之間，因此它會接受來自上層應用層的訊息加以包裝成為一定的格式的記錄，再交由下層的網路層來傳送。

一個 SSL 記錄格式主要分為表頭與資料兩部份：

1. 表頭：包含了訊息的種類、訊息的時間與記錄的長度等資訊。
2. 資料：為傳送資料本體，包含三部分：訊息驗認碼、實際傳輸資料、附加資料。

(4) SSL 之特性：

1. 機密性：每一筆於網際網路上傳輸的訊息皆經加密(encryption)，防止訊息被非法竊知。
2. 身份認證：客戶端(cilent)與伺服器(server)進行建立連線的訊息交換(handshaking)時，由伺服器先產生一組私鑰與公鑰(private/public key)，公鑰傳給客戶端，客戶端把要傳給伺服器的訊息用公鑰加密，而伺服器則以私鑰加密來傳給客戶端的訊息，使客戶端能確認伺服

器的身份[3]。

3. 完整性：每一筆於網際網路上傳輸的訊息皆有雜湊函數(Hash)產生的訊息驗證碼(Message Authentication Code，MAC)保護，經由雜湊值的比對，確認訊息是否被非法竄改。

3. 其它技術

(1) S-HTTP〈安全性超文件傳輸協定〉

S-HTTP 是一以文件為基礎的安全協定，為一般 HTTP 的延伸。

S-HTTP 所提供的安全功能是針對 HTTP 協定中傳輸的文件功能提供直接的安全保護機制，使超文件檔案中的每一個連結都能內含安全性的資料，只需修改原有的 HTML 文件就可以馬上應用，甚為方便。S-HTTP 允許網路客戶端與伺服器端各自進行驗證功能，並且協商出一套共用的加密演算法，使其不需受限於任何特別的演算法。

S-HTTP 的安全保護機制可以分為下列四項：

a. 機密性

b. 完整性

c. 身份驗證

d. 不可否認性

(2) SET

SET 是安全電子交易(Secure Electronic Transaction)的簡寫，用來保護消費者在開放型網路持信用卡付款交易安全的標準，包含交易雙方的身份認證

[3] [註] 若通訊雙方均使用憑證(Certificate)可互相辨識身分的真實性，無法冒名傳送訊息。但 SSL 執行時只使用伺服器單方之 SSL 憑證，且 SSL 的安全機制係架構在通訊協定的傳輸層上，用戶端與伺服器間只有在交易前建立連線時才執行身分辨識，雙方在傳輸每一交易內容時並不執行身分辨識。

及傳送資料加密。具 SET 規格的軟體，存在持卡人的個人電腦及特約商店的電腦網路中；收單銀行的電腦以特殊的科技解讀金融資訊密碼，以及確認 SET 認證中心所發出的數位憑證。SET 由 VISA、MasterCard、IBM、Microsoft、Netscape、GTE、VeriSign、SAIC、Terisa 等公司聯合制訂，運用 RSA[4]資料安全的公開金鑰加密技術，保護交易資料之安全及隱密性。

SET 的架構包含：Electronic Wallet(電子錢包)，Merchant Server(商店端伺服器)，Payment Gateway(付款轉接站)，和 Certification Authority (認證中心)。

運用這四項要素，即可構成於網際網路上符合 SET 標準的信用卡授權交易。SET 1.0 版於 1997/6 正式問世。迄今，SET 已成為國際上所公認在網際網路進行電子商業交易的安全標準。

三、比較

(1) 安全機制比較：

表格 1：CA、S-HTTP、SSL 安全機制比較

	CA	S-http	SSL
機密性	✓	✓	✓
身分認證	✓	✓	✓
完整性	✓	✓	✓
不可否認性	✓	✓	
存取控制	✓		

[4] 公開金鑰加密演算法的一種，由 Ron Rivest、Adi Shamir、Leonard Adleman 三人於 1977 年所發表，並以其姓氏的縮寫命名。

(2) CA 與 SSL 的比較：

表格 2：CA 與 SSL 之比較

	CA	SSL
優點	➢ 親自拿身份證明的文件到認證中心取得認證，使用者身分明確。 ➢ 加密之外，「使用者認證」可以確定誰發送資料，達到資料「不可否認性」。 ➢ 第三方認證中心資料保密，保障安全隱私。 ➢ 比 SSL 提供更嚴謹的安全規範。	➢ 是目前線上交易最普及使用的安全協定。 ➢ 不需事先取得認證，使用較方便。 ➢ 使客戶端確認伺服器的身份。
缺點	➢ 只要電子憑證被他人備份，備份者就被視為代當事人，具有進行所有交易的權利。 ➢ 需向認證中心取得認證，手續較麻煩。 ➢ 電子憑證遺失或者被冒用時，均需臨櫃再申辦，相當麻煩。	➢ 店家無法知道消費者的真實身份，也無法防範盜刷的問題。 ➢ 購物網站仍可取得消費者的信用卡資料，亦可能讓資料外洩被盜刷。

(3) SSL 與 S-HTTP 的比較：

為最典型的兩種網際網路上的安全傳輸協定，兩者間主要的差異如下：

(1) 應用層級的不同

- S-HTTP 的安全機制如加密或簽章都是在 OSI[5]網路協定七層架構的上層—應用層或交談層完成之後再將加密的訊息透過傳輸層等底層網路結構完成傳送，未對傳輸的網路進行保護。

[5] Open Systems Interconnection，由下而上分別為實體層(Physical Layer)、鏈結層(Data Link Layer)、網路層(Network Layer)、傳輸層(Transport Layer)、交談層(Session Layer)、表達層(Presentation Layer)、應用層(Application Layer)。

- SSL 是將訊息以原本格式傳到中層如傳輸層及網路層，然後才對訊息進行加密等安全處理，並透過事先協商的安全傳輸通道進行傳送。

(2) SSL 應用範圍較為廣泛

- S-HTTP 主是針對 HTTP 元件進行安全性的改進。
- SSL 的應用包含了 HTTP 及其以外的檔案傳送 FTP、遠端登錄、電子郵件等應用協定，應用層面較為廣泛。

(3) 設計原理不同

- S-HTTP 是一種以保護文件為主的協定，直接在發送端將文件進行加密及簽章等安全處理，基本上不管傳輸的網路通道是否安全。
- SSL 則是以提供一個安全的傳輸路徑為主，只要協定中的安全機制不被破壞，基本上在此路徑上傳送資料都是安全的。

(4) 不可否認性

- S-HTTP 中定義了數位簽章的機制，因此較 SSL 增加了不可否認性的明顯定義。
- SSL 中沒有明確定義數位簽章的安全機制，因此並沒有提供不可否認性的保護。

(5) 使用量及使用範圍

- 由於美國政府對密碼產品管制出口，以 S-HTTP 為基礎的應用僅限於美國境內使用，而採用 SSL 為安全機制的軟體如網景則分為美國版及海外版，兩者在加密演算法及金鑰長度都有所不同。

- 目前在美國以外地區僅限於 SSL 基礎應用，SSL 成為網路安全傳輸協定的主流。

陸、現行環境與法令規章

一、國內現況

利用 CA 認證以確保電子交易的安全性如今已被廣泛的運用在各個行業中，但是被應用在期貨交易網路下單上，台灣算是首開先例，也是全世界唯一一個實施的國家。台灣之所以會採行 CA 認證制度，除了要改善資通安全，保障投資人以及期貨商在交易過程中的安全性以外，最重要的原因還是來自法律的規定。

電子簽章法

電子簽章法為一新興之科技立法，於民國九十年十月三十一日經立法院三讀通過，並送請總統公布。電子簽章法中，明確的定義了電子簽章與數位簽章，賦予數位簽章法律的效力並闡明出問題十之責任歸屬。

電子簽章法第二條：「二、電子簽章：指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。三、數位簽章：指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。六、憑證：指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。」

簡單的來說，數位簽章屬於電子簽章技術中的一種。電子簽章的涵義較為廣泛，除了數位簽章外，還包括其他許多生物辨識技術，例如以指紋、聲紋來達到簽章之目的。但就實務上來說，「數位簽章」是最早發展且成熟度較高者，因此也是最常被應用的。

而數位簽章於實際應用上，應依一定之程序製作始生效力。

電子簽章法第十條：「以數位簽章簽署電子文件者，應符合下列各款規定，始生前條第一項之效力：一、使用經第十一條核定或第十五條許可之憑證機構依法簽發之憑證。二、憑證尚屬有效並未逾使用範圍。」

依據市場導向原則：「政府對於憑證機構之管理及電子認證市場之發展，宜以最低必要之規範為限。今後電子認證機制之建立及電子認證市場之發展，宜由民間主導發展各項電子交易所需之電子認證服務及相關標準」。故目前採行的憑證管理制度為「志願性」的證照制度，也就是政府只規定一個標準，透過適當的誘因（例如其所簽發憑證的證據力）鼓勵憑證機構申請執照。主管機關審查通過核發營業執照之後，憑證機構即可對外營業。但是，如果憑證機構以經營財務金融交易認證為主要業務者，另應取得財政部許可。

至於憑證機構所應負的損害賠償責任也有明文規定。

電子簽章法第十四條：「憑證機構對因其經營或提供認證服務之相關作業程序，致當事人受有損害，或致善意第三人因信賴該憑證而受有損害者，應負賠償責任。但能證明其行為無過失者，不在此限。 憑證機構就憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，不負賠償責任。」

損害責任歸屬之問題，GCA(政府憑證管理中心)有更明確的定義：

首先，憑證機構及其所屬身分註冊、代理機構，應就下列事項對合理信賴其所簽發憑證之當事者，負損害賠償責任：1、憑證簽發錯誤，除非憑證機構及其代理機構可以證明已經採行與該項憑證目的相稱之所有合理可行之避免憑證錯誤之措施。2、未依本法或憑證實務作業聲明書所訂之程序或方法註銷、中止或簽憑證，致相關當事者利益受損時。3、所屬人員故意或無意之過失或管理疏失，致合理信賴其所簽發之憑證為真之相關當事者利益受損時。

而憑證機構及其註冊、代理機構，就下列事項不負損害賠償責任：1、對於任何信賴其憑證當事者之錯誤及偽造之數位簽章所致之損失，已依本法規定採行所有合理可行之預防措施。2、對於相關當事者將憑證應用在與簽發目的相違背之事項，或超出憑證所載之限制事項。

假使有以下情形，憑證當事者要負損害賠償責任：

(1) 故意以不當或不法方法，使憑證機構誤信其提供之資訊為真，並據以簽發憑證，致相關當事者利益受損。

(2) 未依本法規定註銷憑證，致任何信賴者利益受損。

(3) 未善盡保管責任，致其簽章設施遭未經授權之使用，且未依本法規定通知相關當事者，致相關當事者利益受損。

而為了避免損害求償時憑證機構無力償還，憑證機構在檢核通過設立時，會被政府要求要提存營業保證金，如果憑證機構無償還能力時，使用者可以獲得營業保證金的優先清償。

期貨交易相關規章

數位簽章目前已經廣泛的被運用在各個行業中，當然也包括了期貨交易網路下單。目前不論是在證券暨期貨交易相關法規中，亦或營業規則中都有明確規定期貨交易經由網路下單時必須採用數位簽章，經由 CA 認證。

證券暨期貨交易相關法規：

✓ 建立期貨商資通安全檢查機制

發布日期 95.07.24 法規名稱 建立期貨商資通安全檢查機制

中華民國九十五年七月二十四日臺灣期貨交易所股份有限公司台期稽字

第 09500068090 號函修正發布全文 12 點；並自九十五年八月一日起實施

中華民國九十五年五月二日行政院金融監督管理委員會證券期貨局證期

七字第 095114195 號函准予備查

7.通訊與作業管理

（1） 網路安全管理（**適用網際網路下單期貨商**）

a. 網路系統安全評估：

(i) 應定期評估自身網路系統安全（例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等），並留存相關紀錄。

(ii) 定期或適時修補網路運作環境之安全漏洞（含伺服器、攜帶型、個人端及營業處所內供投資人共同之電腦等），並留存相關文件。

(iii) 有關電腦網路安全（如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等）之事項應隨時公告。

(iv) 各電腦主機、重要軟硬體設備應有專人負責。

b. 防火牆之安全管理：

(i) 應建立防火牆。

(ii) 防火牆應有專人管理。

(iii) 防火牆進出紀錄及其備份應至少保存兩個月。

(iv) 重要網路及伺服器系統（如網路下單系統等）應以防火牆與外部網際網路隔離。

(v) 防火牆系統之設定應經權責主管之核准。

c. 網路傳輸安全管理：

網路下單畫面應採加密方式（例如：SSL） 處理。

d. CA 認證與憑證管理：

(i) **網路下單期貨商應訂定憑證交付程序，避免非本人取得**

憑證。

(ii) **網路下單期貨商應全面使用認證機制。**

e. 電腦病毒及惡意軟體之防範：

(i) 應安裝防毒軟體，並及時更新程式及病毒碼。

(ii) 應定期對電腦系統及資料儲存媒體進行病毒掃瞄（電子郵件）。

(iii) 防毒應涵蓋個人端（含攜帶型及營業處所內供交易人共用之電腦等）及網路伺服器端電腦。

(iv) 勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤應特別小心開啟。

(v) 為防範電腦病毒擴散，影響電腦安全，公司應訂定電子郵件使用安全相關規定。

f. 網路下單系統功能檢查：

應定期檢查網路下單系統提供之功能，並留存紀錄。

業務規則：

◆ 臺灣期貨交易所股份有限公司業務規則 (民國 95 年 06 月 30 日 修正)

第 48 條：期貨商與採行 IC 卡、網際網路等電子式交易型態之委託人間，其期貨交易買賣之委託、委託回報及成交回報等電子文件之傳輸，應使用憑證機構所簽發之電子簽章簽署，憑以辨識及確認。

期貨商建立 CA 憑證過程之金流

✧ 期貨商與電子憑證公司

期貨交易商使用 CA 憑證，首先需向憑證公司(例如網際威信)購買一套 PKI 系統，此費用是一次性費用，往後每年則是有另外的維修費用。之後，需支付

系統整合費用，將所購買的 PKI 系統與自身的交易系統結合，此部分同樣也是一次性費用，往後同樣也是每年另付維修費用。最後是憑證發放的部分，每年以張數計算來收取所需給付的費用。

表格 3：期貨商建立 CA 憑證之費用

建立 CA 憑證之步驟	費用收取	後續費用
1.購買 PKI 系統	一次性費用(僅在第一年收取)	另外簽訂每年所需給付的維修費用
2.將 PKI 系統與自身交易系統整合	一次性費用(僅在第一年收取)	另外簽訂每年所需給付的維修費用
3.憑證費用	每年依發放之憑證張數來計算所需給付之費用	

✧ 期貨商與使用者

目前的線上期貨交易，期貨商並未對使用者收取額外的費用，使用者僅須在開戶之初，一併申請網路下單功能的開啟，即可線上下載 CA 憑證，進行網路下單。然而，目前的情況可能是因為期貨商仍在推廣網路下單的功能，因此將 CA 憑證部分的費用自行吸收，將來網路下單功能為多數使用者所能接受時，期貨商仍有可能將 CA 憑證的費用轉嫁給消費者。

國內現行 CA 廠商

著眼於未來網路應用將帶來之龐大市場，國內已有許多業者競相投入資金，設立公司、部門，積極爭取憑證機構這一塊極具潛力價值之市場，以下列出目前幾個主要廠商。

(1) 中華電信股份有限公司「政府憑證管理中心」（Government Certification Authority，GCA）：曾負責我國網路報稅試辦作業之業務。

(2) 網際威信股份有限公司（HiTRUST）：

網際威信（HiTRUST）成立於民國 87 年，主要業務是發展安全電子商務服務及解決方案。主要股東成員包括宏碁集團 (Acer Group)、香港上海匯豐銀行(HSBC)、香港新世界集團 (New World Group)、美國國際集團 (AIG)以及美商 VeriSign 公司。為台灣唯一代理美國 VeriSign 公司之電子認證產品及技術者，並提供電子認證服務及電子商務服務。

(3) 台灣網路認證公司(TWCA)：

TWCA 成立於民國八十八年十二月，主要是由臺灣證券交易所、財金資訊公司、臺灣證券集中保管公司及網際威信公司等四家合資成立。臺灣網路認證公司擁有獨特股東背景優勢，結合各股東在金融業、證券業、保險業與安全電子商務領域多年累積的專業技術與實務經驗，提供國內有關證券金融等方面之認證服務。

二、美國期貨電子交易現況

美國期貨交易市場現主要有六大交易所，分別為 Chicago Board of Trade (CBOT)[6] 芝加哥期貨交易所、Chicago Mercantile Exchange (CME) 芝加哥商品交易所、New York Mercantile Exchange (NYMEX) 紐約能源商品交易所、Coffee, Sugar and Cocoa Exchange (CSCE) 咖啡糖可可交易所、Commodity Exchange Inc. (Division of NYMEX, COMEX) 紐約商品交易所與 New York Cotton Exchange (NYCE) 紐約棉花交易所。主管機關為美國商品期貨交易委員會(commodity futures trading commission, CFTC)。

目前美國商品期貨交易委員會 (CFTC) 對期貨商所提供的網路下單服務之

[6] CBOT 與 CME 在 2006 年 10 月 17 日宣佈合併，預計在 2007 年中完成交易；合併後的交易所為全球最大的衍生性商品交易中心(每日平均交易量為 9 百萬口，金額為 4.2 兆美元)。

安全性並無明確的規章要求其需使用的安全技術。不過多數期貨商 (如 ADM Investor Services) 為保障交易的安全性，避免資料外洩或被竄改，通常都會採用 SSL 以達到交易內容保密的目的，也有部分交易所 (如 NYMEX) 或期貨商採用 VeriSign 的 SSL 認證來提高使用者的信心，即使過去也曾發生過幾起 VeriSign 承認錯發憑證給非正常營運公司的事件。

圖表 11：NYMEX 的 VeriSign 認證

資料來源：New York Mercantile Exchange

相較之下，PKI 機制的電子憑證雖較單純 SSL 提供了不可否認性，保障交易的執行，並提供了不同於一般只需一組帳號密碼就能登入的保護機制，但目前仍較少為美國期貨商所使用，可能的原因有：

1. 期貨網路交易詐騙情形不多

   相較於國內目前各式詐騙行為橫行的歪風，美國這方面的案件數量較少，也降低了期貨商額外投入資金建立 PKI 機制的誘因

2. 相關法令無強制規定

目前美國政府對期貨網路下單安全性並無強制規定要使用憑證來驗證使用者的身分

3. PKI 機制使用方式較繁瑣

一般來說使用 PKI 的使用者多需臨櫃申請金鑰，可能造成使用者，尤其是國外投資者的不便而轉向其他家期貨商

4. 其他技術使用

除了 SSL 外，部分期貨商可能轉而使用 s-http，此技術也提供了不可否認性，保證了交易的執行

5. 投資者保護意識

美國向來以極高的消費者意識而著稱，因此期貨商所提供的交易保護機制除對交易內容保密外，主要是為了提供投資者確認期貨商身份，而較少反向地來驗證投資者的身份，以避免投資者產生不滿的情緒

綜合上述各項因素，使得電子憑證與 CA (Certificate Authority) 在美國線上期貨交易市場始終處於非主流的地位。然而，因為各種外在環境與法律規章及責任歸屬的差異，這樣的交易規範是否適合台灣則仍有待仔細的評估與研究。

柒、替代方案評估與可行性分析

一、期交所自行開發 CA 認證機制

1. 可行性評估

法令規定

由於現行 CA 認證機制是使用於用戶對期貨商下單的部分，因此若由期交所來做兩者中間的認證，並不違反證券暨期貨交易之業務規則所敘述需交由獨立第三人認證的規定。

期交所

首先期交所本身並沒有相關技術及人員可供使用，因此，可能需要擴大其編制或委外交由專業人員來處理。具體的做法包括向現有 CA 認證技術之廠商代理其專業技術(則角色將與 TWCA 或台灣網際威信相同)；或是自行開發一套新技術，然而在基礎設施的建置以及往後的維修費用上，可能會需要投入相對的投資成本，需要再做財務上的評估。

2. 自行開發 CA 認證機制替代方案之優缺點

優點

a) 期交所本身對於期貨交易較一般技術廠商有更深入的了解，較清楚其交易過程中潛在的問題及風險，因此更可以針對此部分做出改善。

b) 從事 CA 認證之工作，可為期交所帶來另外一筆收入。

缺點

a) 期交所本身並無相關經驗，因此在建置的過程中，其成本的投入與能獲得的效益仍不確定，需再進一步做評估。

3. 風險暨障礙及事故責任歸屬

從事 CA 認證之單位，需提出憑證實務作業基準(Certification Practice Statement，CPS)，詳列各種可能風險、及各單位所需負擔之責任。一般而言，若是因認證程序出現問題而造成他人損失，將由認證單位賠償(在此替代方案下，即為期交所)，然而即便如此，仍然會對賠償部分做出一上限的限制，因此認證單位並不需太過擔心其財務狀況可能無法負荷。此外，若是依照正常使用程序，認證部分並沒有問題，則其他意外損失的發生，則需由期貨商自行承擔責任。

二、不強制使用 CA 認證機制

2. 可行性評估

法令規定

現行法令在〈建立期貨商資通安全檢查機制〉中，有明確規定網路下單期貨商應全面使用認證機制，因此，此替代方案是在法令有釐清的必要。

期貨商

首先，各期貨商本身對風險承擔的能力不同，且其所從事之交易大小也不相同，應先評估自身條件後，再決定其網路交易之安全防護機制應做到何種程度。因強調安全性，可能使其成本增加，且讓使用者更不便利(交易所需經過多重認證確保)，因此需決定安全防護的程度。

然而，因網路交易的便利性，使得網路交易量越來越大，期貨商勢必需要對線上交易的部分做出更完善的規劃，而 CA 認證如前述具備有多項安全性的基本功能，因此在現行技術下，仍不失為一個認證的好方式。各期貨商仍可選擇自行做 CA 認證，或是將 CA 認證的部份委外，亦或是利用其他的認證方式以及安全機制。

3. 不強制使用 CA 認證機制替代方案之優缺點

優點

a) 由各期貨商自行評估其 CA 認證之必要性，可針對期貨商本身的條件做調整，並且可以節省 CA 認證部分的支出。

缺點

a) 期貨商本身對於風險有較大的承擔責任，或是需自行尋找其他認證機構等來分散其自身在交易上的風險。

4. 風險暨障礙及事故責任歸屬

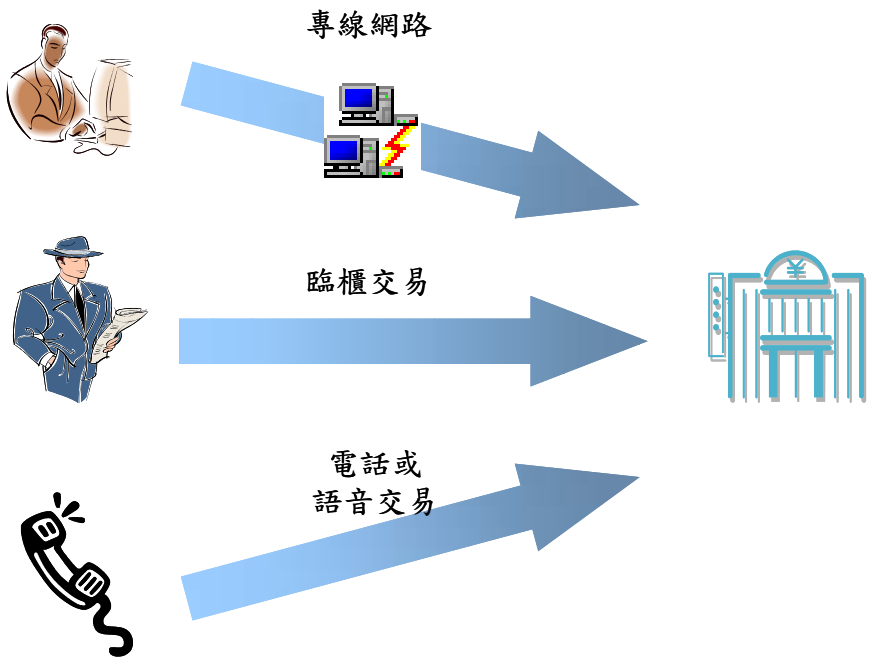
若期貨商自行做 CA 認證，則需注意其必須取得使用者簽署同意—使用 PKI 的電子商務交易可視為一種契約行為，否則在法律上，彼此之間的交易只能當做一記錄，並不具有實質的契約效力。然而，在取得使用者的簽署同意之下，則其在法律上的責任歸屬部分，將與之前所述相同，在憑證實務作業基準裡將會對各部分的責任有清楚的規定。

而期貨商若是自行利用其他的認證方式，由於現存法律除了對數位簽章以外，並沒有對認證方式做一嚴謹的規定，其目的為因應未來其他更多新技術的發展；然而相對的，也就代表其他未被提到的技術，法令上並沒有太大的規範，若其發生問題，在責任歸屬上將無法有明確的規範。

捌、DMA 概觀

DMA 即 Direct Market Access[7]，其直觀的意義為直接與交易市場連結的交易方式，主要的著眼點為快速與低交易成本。目前指稱應用在期貨或證券交易上的 DMA 通常都是在交易人與經紀商之間，透過電子連線的方式，不受到業務人員的第三方介入與干擾，因此提高投資人下單的速度與隱私性。廣義來說投資人親自臨櫃的電子下單、或者以電話語音方式的電子化直接下單都屬 DMA 概念的應用。

圖表 12：廣義之 DMA



資料來源：本研究整理

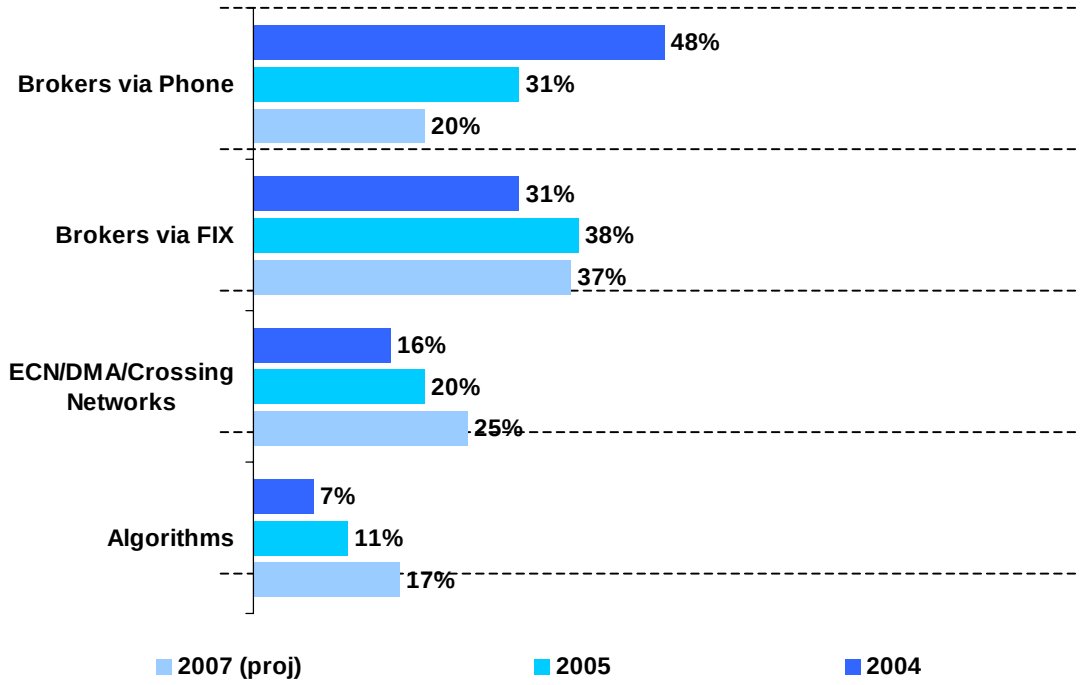
[7] DMA 指稱令買方以較為直接的方式交易金融證券的電子設施。在使用 DMA 時，買方仍然使用賣方的交易平台但卻能夠掌控交易執行的方式。DMA 較低的交易成本也獲得短線進出頻繁的投機型投資人或是避險基金的青睞。

根據 Tower Group 的定義， DMA 係指將金融商品的交易直接下單至交易地點的自動化程序，因而規避了第三者的干預；所謂的交易地點包括了交易所、替代性交易系統(Alternative Trading Systems)、金融商品電子通訊網路(Electronic Communication Network)。而根據 UBS 的定義，DMA 指稱買方的交易檯(Trading Desk)將買單直接傳遞至市場中心(Execution Venue)而不需賣方交易員的介入；賣方的價值在於提供交易所的會員資格、交易技術、支援以及授信。

探究 DMA 興起的原因，實與買方追求交易速度有密切的關係。對於特定的法人(例如風險基金)而言，主要交易目的之一在於針對市場資訊的迅速反應和風險之轉嫁，交易執行的速度對於成交與否有決定性的影響。降低交易延遲的手段除了 DMA 之外，尚包含市場交易資訊的直接擷取和特定的交易分析、交易決策、交易平台等交易能量的提升。換言之，交易的主控權逐漸由賣方移轉向買方，由買方控制交易的流程，並藉由自動化的交易方式(例如演算法交易「Algorithmic Trading」或是程式交易「Program Trading」)，達成電光火石速度的交易(節省 100-200 毫秒)[4]。

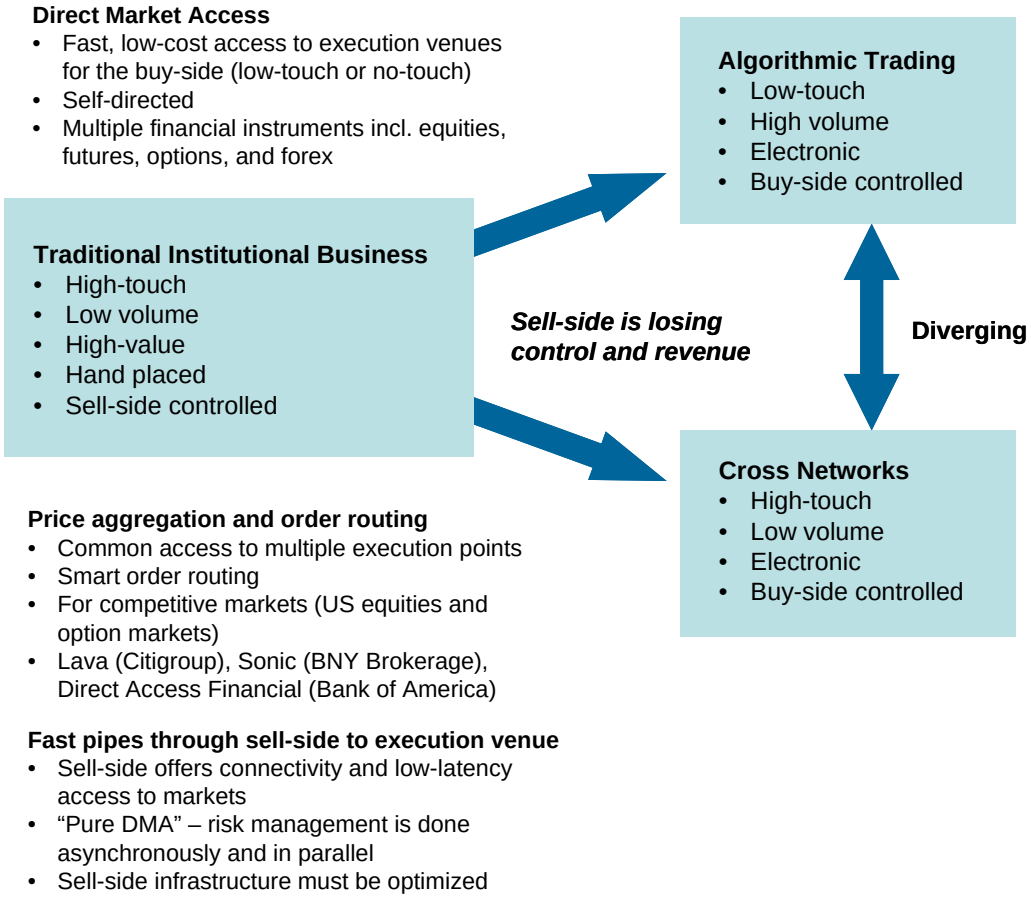
與傳統的交易方式相比，DMA 存在幾項優勢，包括匿名性(Anonymity)、交易執行的穩定性(Stability)、速度(Speed)、處理大單及複雜交易的效能(Performance)、較短的延遲(Latency)、易於使用(Ease of Use)以及與主流的交易管理系統(Order Management System，「OMS」)既有的功能。因此，根據 TABB Group 的一項研究，廣義的 DMA 證券交易(DMA/ECN/Crossing Networks)預計 2007 年達到 25%，與 DMA 息息相關的演算法交易(Algo trading)也將成長至 17%；反之，透過券商電話下單者則萎縮至 20%(自 2004 年的高鋒 48%)[10]。

圖表 13：證券交易方式



資料來源: TABB Group Institutional Equity Trading 2005

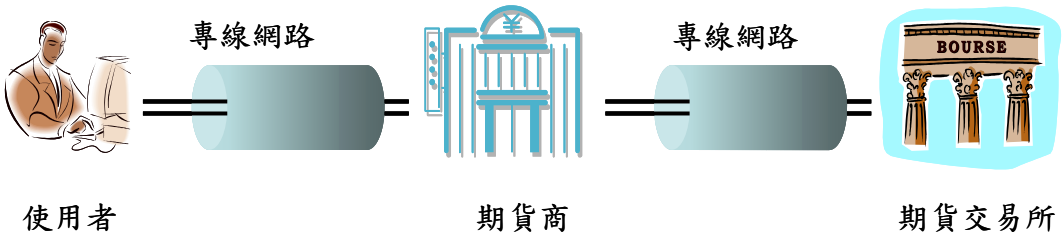
圖表 14：DMA 與演算法交易



資料來源: IBM

不過在此吾人所要探討的主要目標是由行政院金管會證期局於今年(2006)發佈的「開放證券經紀商接受投資人採行電子式專屬線路下單 (Direct Market Access)」相關規定，也就是將 DMA 概念運用在證券甚至是期貨交易之電子下單的研究。因此，以下報告內容中所稱之 DMA 均指電子下單的應用。

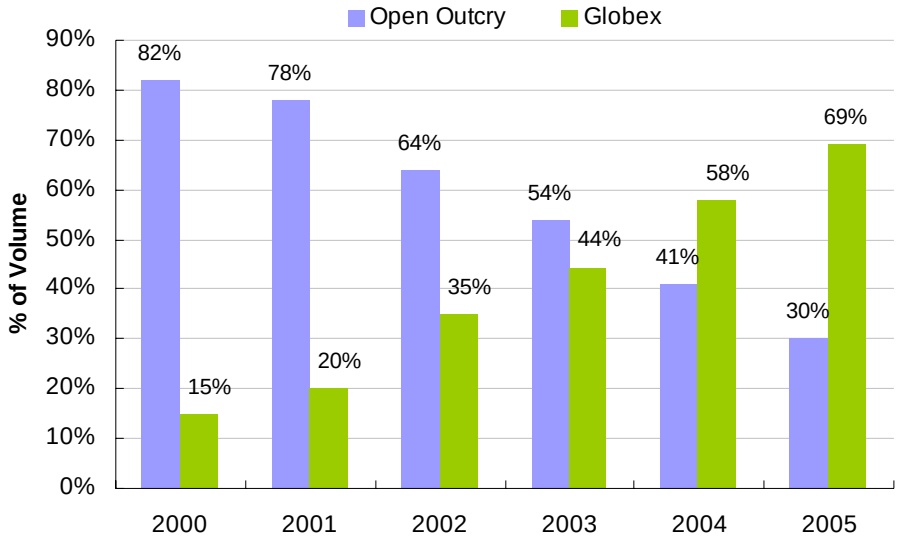
圖表 15：狹義之 DMA (電子式專屬線路下單)



資料來源：證期局; 本研究整理
（詳細運作流程參照附錄）

期貨交易的電子化與日俱增，據 CME (Chicago Mercantile Exchange)的統計，電子交易(透過 CME 的 Globex 交易平台)的比重，自 2000 年佔所有交易量的 15%成長至在 2005 年的 69%，而且該項比例還在持續攀升[5]。

圖表 16：CME 電子交易方式比重

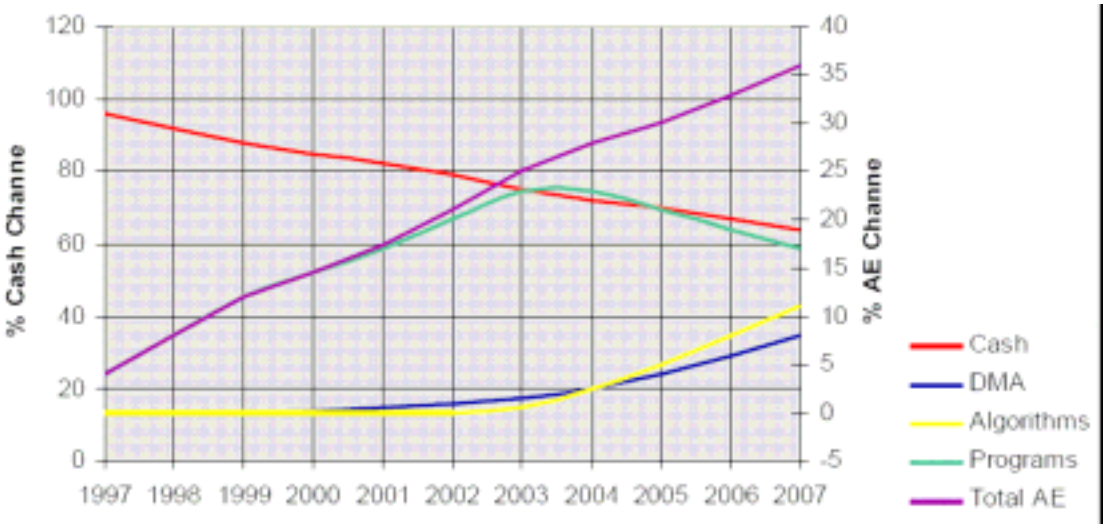


資料來源：CME; Bear Sterns

DMA 在期貨及選擇權交易的應用雖然不及股票交易，但市場的接受度愈來愈高。根據 Citigroup 的統計[12]，目前在歐洲，以 DMA 方式交易的股票已經佔 5%，至 2007 年則可望達到 8%。導致 DMA 快速成長的原因主要為較低的佣金、

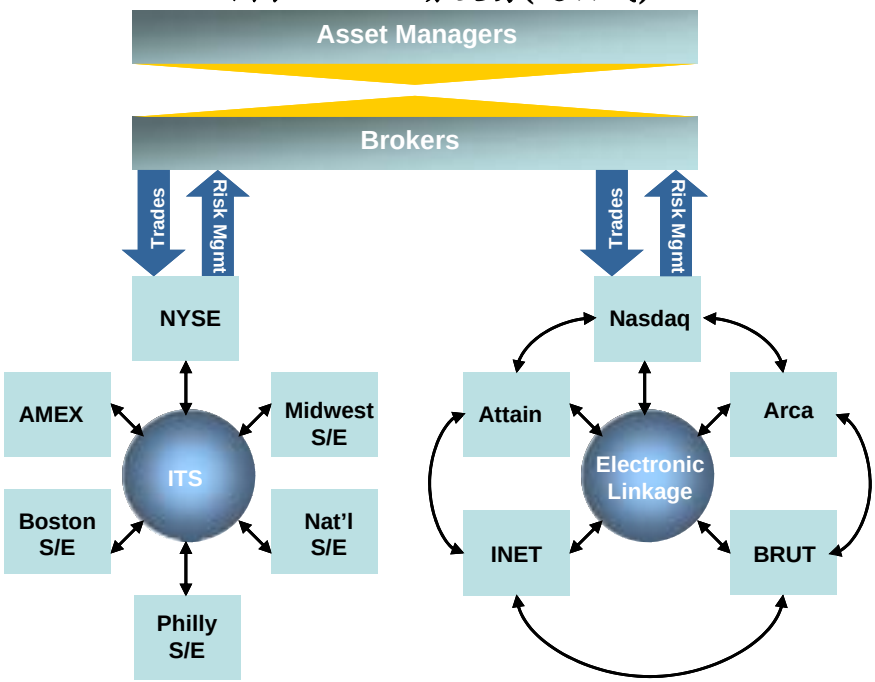
匿名、速度、避險基金的增加、法規要求(例如美國的 NMS[8]規範和歐洲的 MiFID[9])、集中交易檯的發展、以及下單管理系統(Order Management System)的精進。

圖表 17：歐洲替代性交易執行方式比重



資料來源: Citigroup

圖表 18：證券交易(過去式)

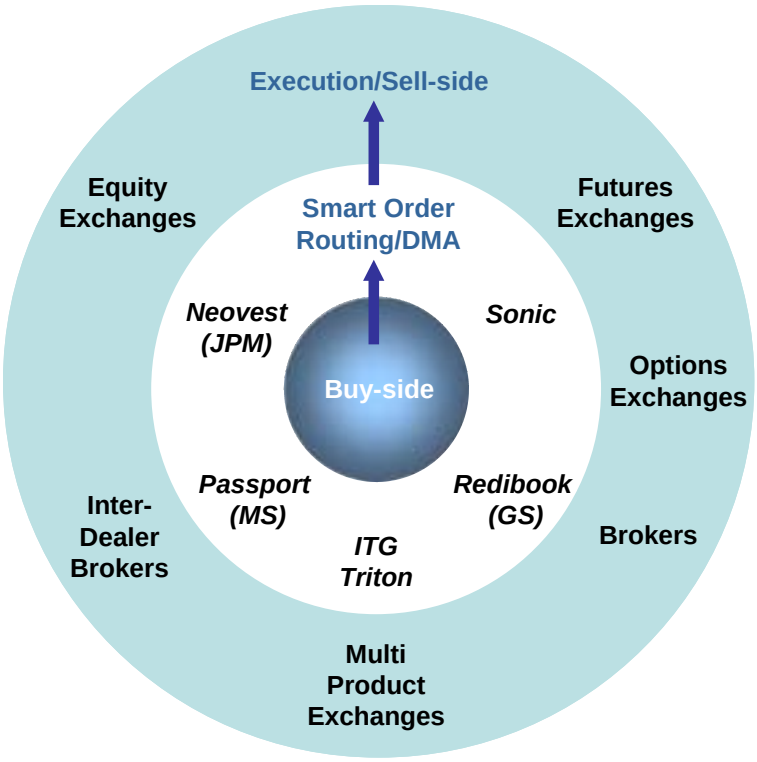


資料來源：JPMorgan

[8] Regulation National Market Systems
[9] Markets in Financial Instruments Directive

金融商品的交易模式已由過去的賣方轉為買方為中心，買方透過 DMA 或是 Smart Order Routing，得以與賣方或是交易中心買賣各式金融商品(包括證券、選擇權、期貨等)。目前較著名的平台包括 JPMorgan 的 Neovest、Morgan Stanley 的 Passport、Goldman Sachs 的 Redibook、ITG 的 Triton 等[15]。

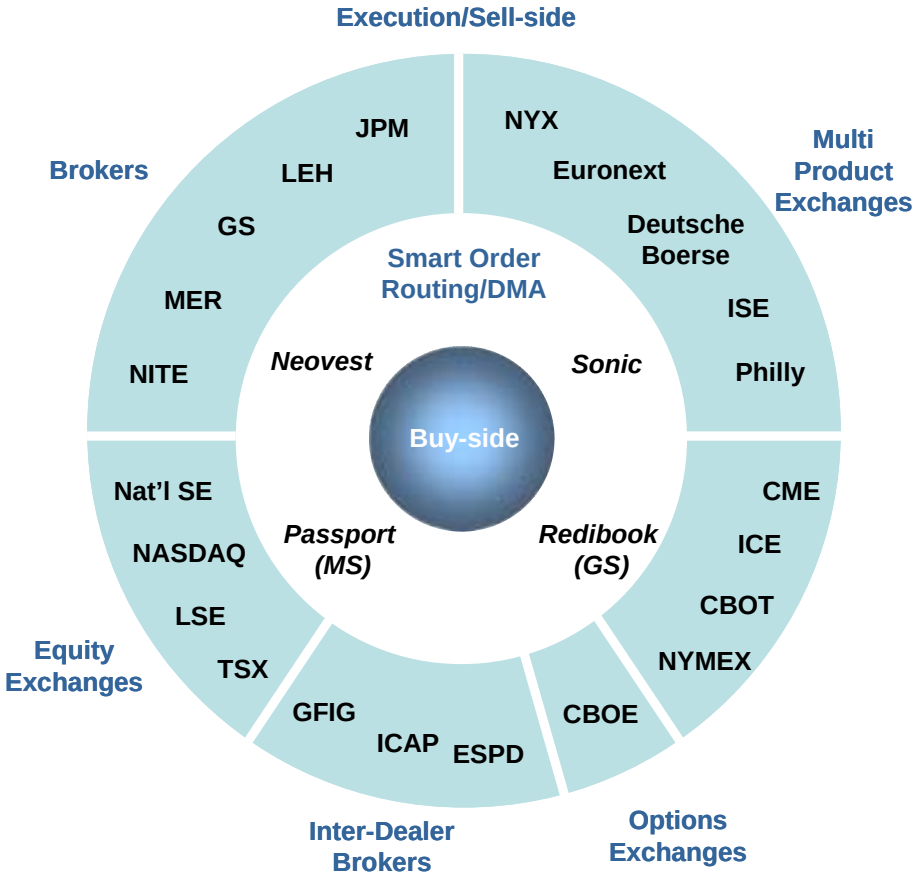
圖表 19：金融商品交易(未來式)



資料來源：JPMorgan

另一方面，交易中心也日趨多元化，跨國、跨境或是跨交易中心(金融商品)的交易方式，均可透過 DMA 及 Smart Order Routing 的方式遂行，買方可透過單一的交易平台，交易多種的金融商品，其交易對象可以是承銷商、期貨交易所、選擇權交易所、證券交易所等等。

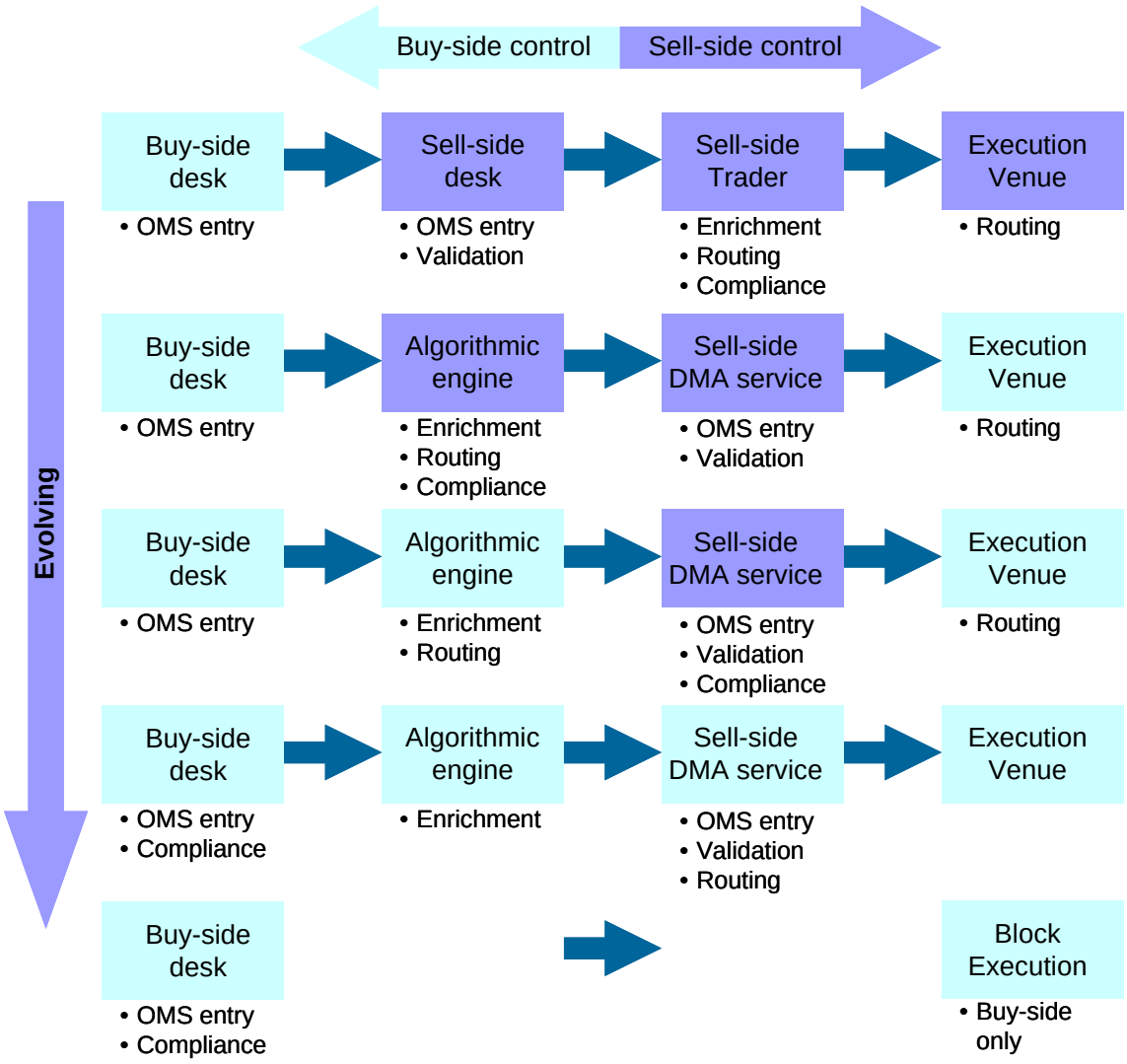
圖表 20：多元化之金融商品交易中心



資料來源：JPMorgan

總體而言，金融商品交易市場(含期貨)的結構已然改變，買方對於交易流程的控制與日俱增；另一方面，賣方則因為對於下單流程喪失主控權而導致業務量及珍貴市場資訊的流失。

圖表 21：多元化之金融商品交易中心[1]



資料來源: IBM; 本研究整理

玖、 DMA 相關法令

根據金管會發布的「財團法人中華民國證券櫃檯買賣中心證券經紀商辦理電子式專屬線路下單（Direct Market Access）作業要點」，定義了 DMA 為「*電子式專屬線路下單，係指委託人端與證券經紀商端之交易系統直接以專線或封閉型專屬網路聯結，藉由該項聯結，委託人之委託指示可直接傳送至證券經紀商的電腦系統，通過證券商電腦檢核後，即傳送至本中心，毋須再由證券商人員介入之自動化下單流程*」。因此，為電子化的期貨交易開啟了另一個操作與應用的機制。

法令中的作業要點明確提到了要『*達到身分確認性、資料完整性、資料隱密性、交易不可否認性之管控機制*』，然而，該法令中並未規範實作機制上的技術要求。在未有明確定義讓各家期貨商具自行解讀的空間下，造成了 DMA 無法『*達到身分確認性、資料完整性、資料隱密性、交易不可否認性之管控機制*』的錯誤印象。

壹拾、 DMA 技術分析

(1) 背景

隨著網路科技的進步與普及，越來越多有經驗的客戶(如法人、Instividual[10])意圖免除交易員的人為介入，提升其交易主控權與交易速度，藉由更完整地控制交易執行的過程，直接進入市場進行撮合。目前有不同的方式來因應這項趨勢，但最廣為運用的仍屬 DMA---電子式專屬線路下單(Direct Market Access)。根據 Barclays Capital 的估計[11]，來自北美地區客戶的期貨電子交易中有 45%-55%是採用某種形式的 DMA，歐洲地區客戶此採 DMA 方式者的比例大約在 20%-30%，亞洲區的比例則在 5%-10%[3]。

(2) 技術機制

DMA 可概略區分為兩種模式---傳統的模式和純粹的模式。

a. 傳統 DMA 模式

傳統 DMA 模式通常在 FIX（Financial Information eXchange）金融資訊交換平台下，以其通訊協定進行操作：由客戶輸入電子指令，透過券商的指令分配系統來進行傳輸以及交易。FIX 金融資訊交換平台之發展，可以依據國際標準 FIX 通訊協定為交換機制的平台系統建置之，然後透過各期貨、基金、投信、投顧、銀行等業者，於交換平台上提供客戶網路下單的電子交易服務。

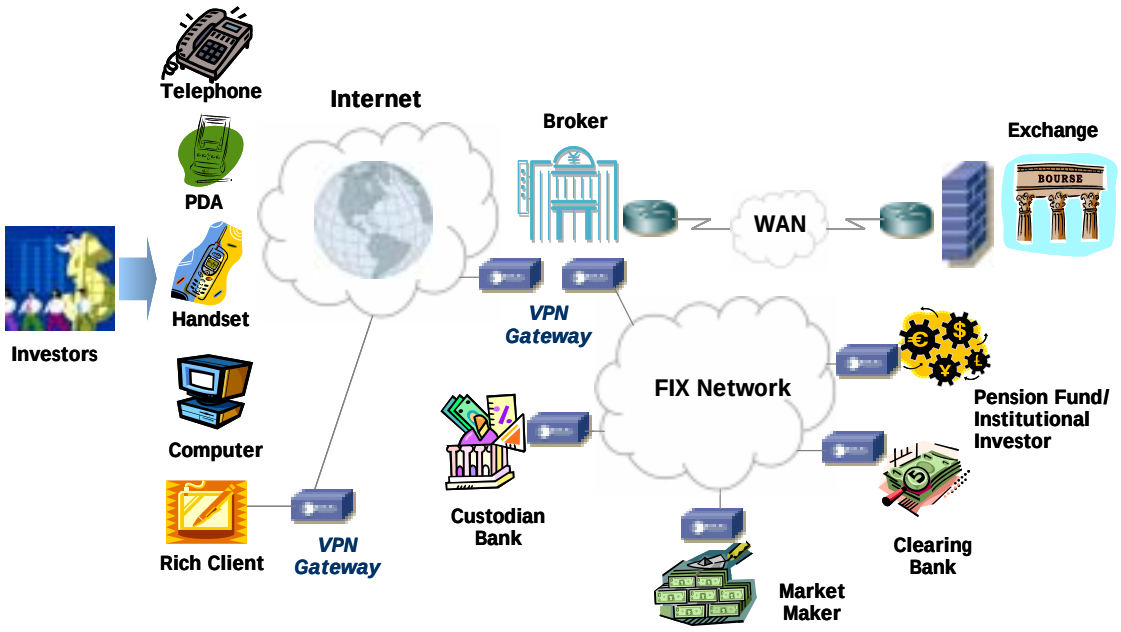
傳統 DMA 模式內的各個客戶，以撥接線路(Dial-up Link)、專線網路(Private Network) 或者以虛擬專線網路(Virtual Private Network，「VPN」)的方式與中央交易系統連線，形成 Client/Server

[10] 由 Institutional + Individual 結合而成，意指法人或是專業投資人(非任職於投資機構者，以個人資產為之)
[11] 此一數據是根據客戶的所在地、而非交易所的所在地推算出來的。

的模式架構。

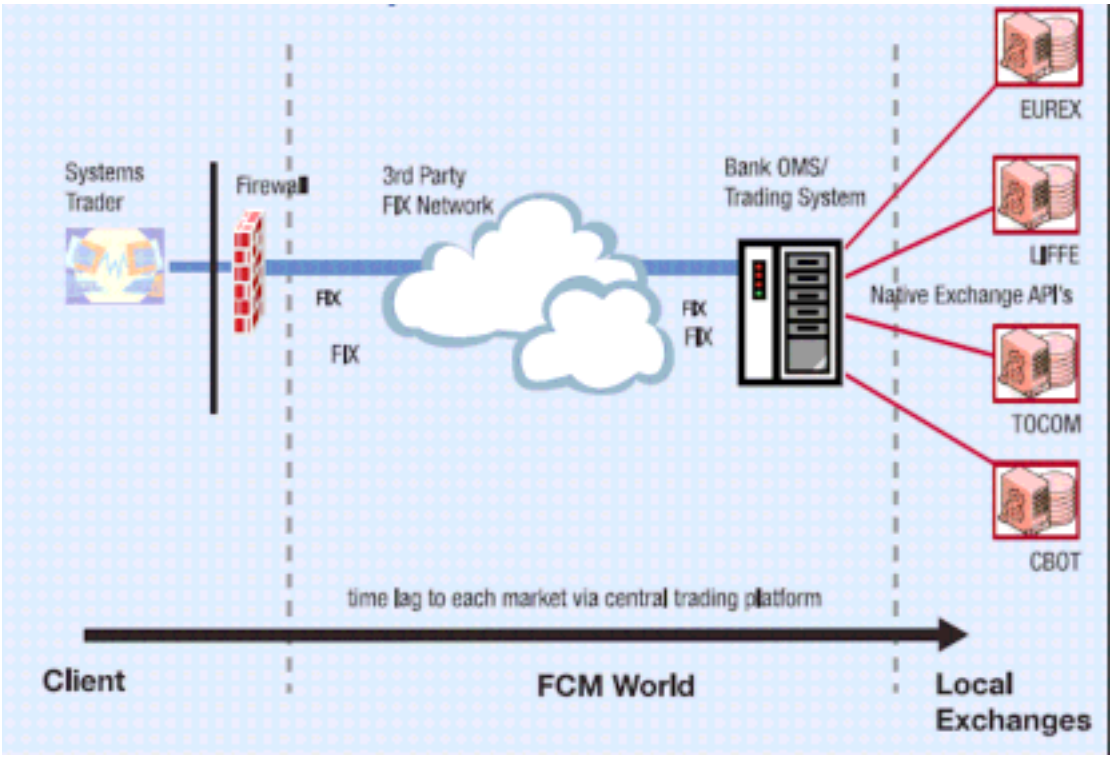
常見的實務作法有三項方式：客戶可以親自打電話將指令報給期貨商，也可以通過期貨商提供的網路平台親自輸入指令，或通過獨立軟體提供商提供的交易軟體輸入指令。常見方式有：臨櫃、或以語音、網際網路、專線、封閉式專屬網路等電子式交易型態委託──目前證交所推行者應屬傳統式的 DMA 模式。

圖表 22：FIX 金融資訊交換平台



資料來源：本研究整理

圖表 23：傳統式 DMA 期貨交易



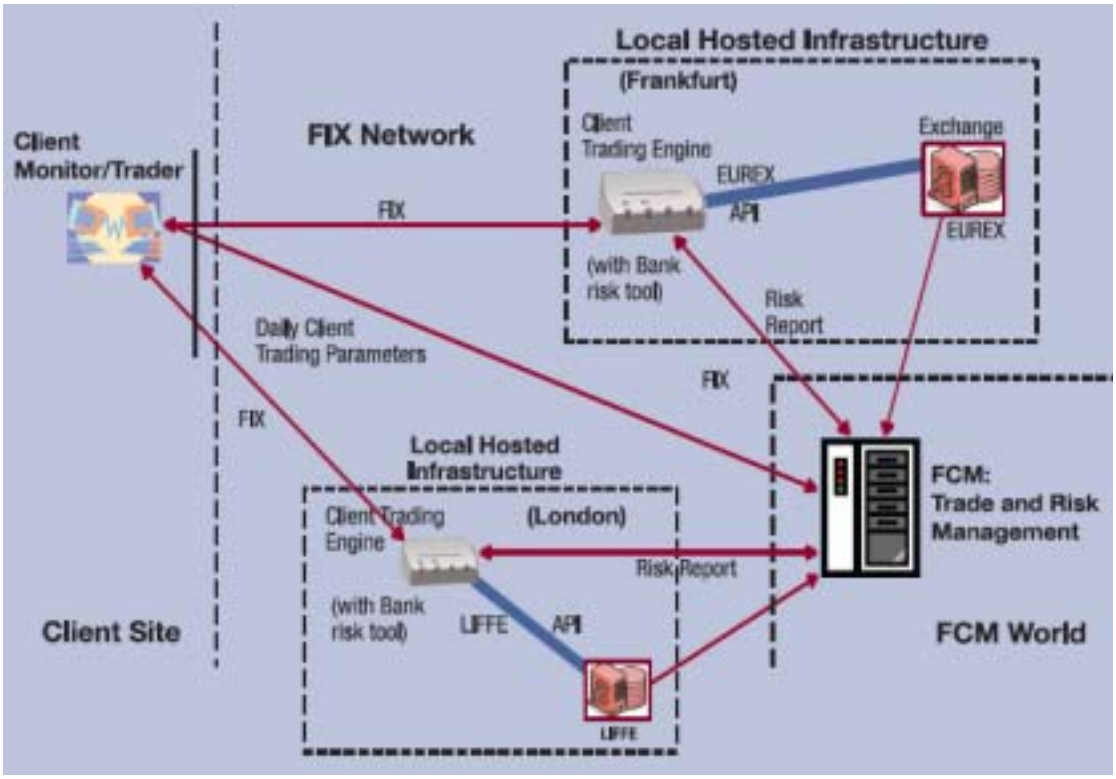
資料來源：Barclays Capital

b. 純粹 DMA 模式 (Pure DMA Model)

目前尚處於初步發展階段，但其架構業已獲得大型交易商的肯定。純粹 DMA 模式要求具備高水準的技術專才和風險管理專業人員，客戶可以直接與交易所的客戶交易引擎(Client Trading Engine)連線，並使用交易所提供的應用程式介面(Application Programming Interface，「API」)。由於規避了券商提供的集中指令分配系統，加上客戶交易引擎與交易所的撮合系統鄰近(以區域網路或 collocation 的方式連接)，客戶獲得的速度和效率優勢，將遠遠超過所耗成本及時間。

採用純粹的 DMA 模式使客戶快速取得市場資訊，允許客戶更快速地下達交易指令。純粹 DMA 模式所需要的執行時間可能只有幾毫秒。在這個的電子交易的時代，這種優勢對某些特定客戶(例如風險基金、法人投資者)來說是非常重要的。純粹的 DMA 模式重新定義了客戶如何連接交易所，以及期貨商如何服務客戶的內涵。

圖表 24：純粹 DMA 期貨交易



資料來源：Barclays Capital

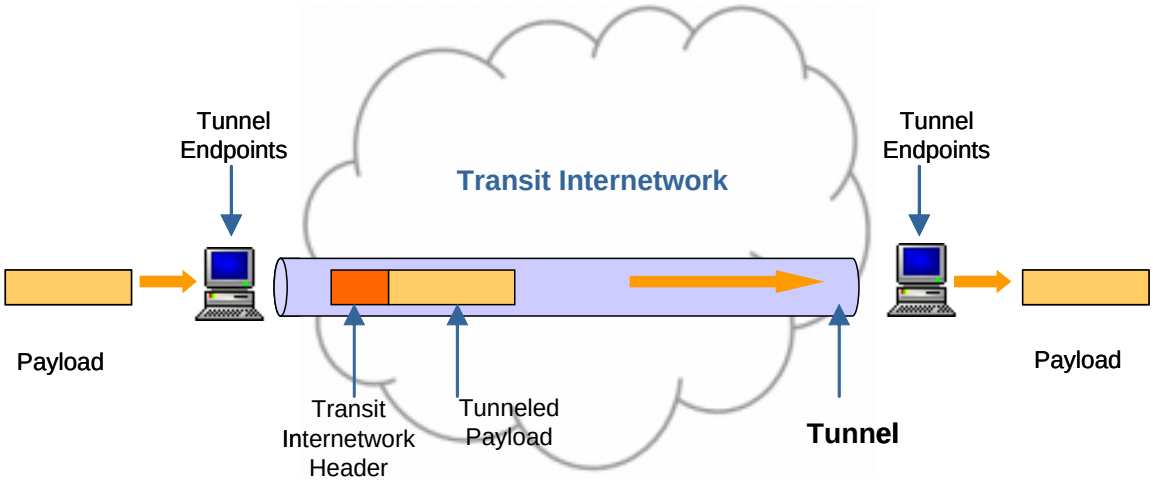
(3) 基本運作單位

(1) *金融資訊交換平台（Financial Information eXchange,「FIX」）*為全球證券業界即時電子金融交易通訊協定的標準，支援眾多的金融商品，廣為投資法人、證券公司和交易所所使用。

(2) *內容供應商*：期貨／券商、銀行、金融商品。

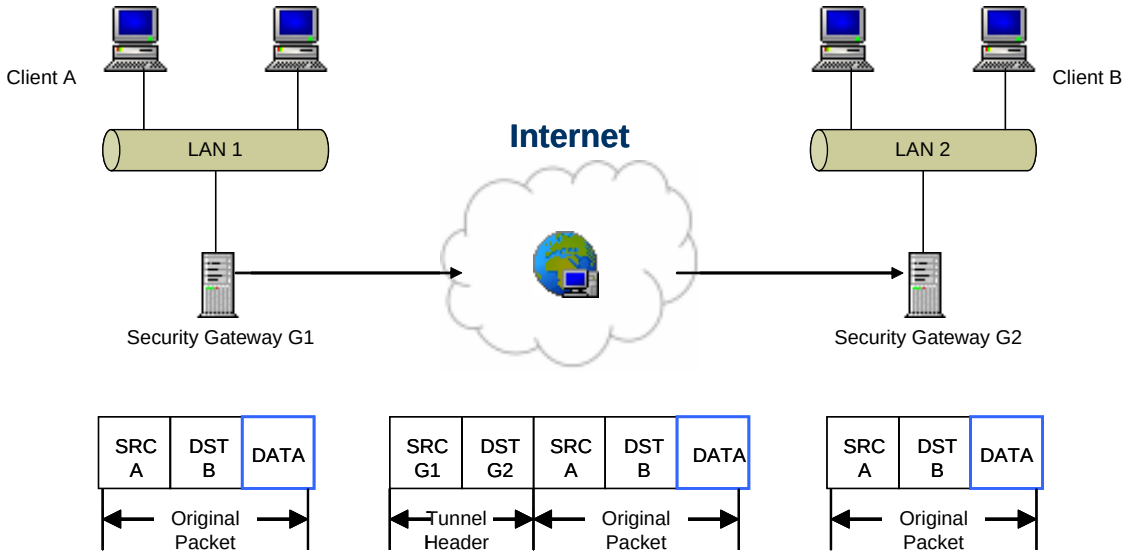
(3) *VPN 虛擬專屬網路*：供應臨櫃、語音、專線、封閉式專屬網路等各種電子式交易型態之介接與連結。

圖表 25：虛擬專線網路[12]



資料來源：Shieh, S.P.; 本研究整理

圖表 26：LAN-LAN 虛擬專線網路



資料來源：Shieh, S.P.; 本研究整理

[12] 虛擬專屬網路係透過所謂的穿隧(Tunneling)方式，將私密性的資料加上特殊的封裝標頭(encapsulation header)，在公眾網路上傳遞。由於封裝標頭不易破解，因此雖然是透過公眾網路傳輸，其實質的效果如同專屬線路，但成本卻大幅降低。

λ **風險管理**

在電子交易之前，期交所的風險管理主要為管理交易撮合及其基礎結構，與監督期貨商的行為，以確保交易市場秩序。實施 DMA 交易方式後，期交所除了原有的交易撮合及內容風管之外，還得加上對於期貨商 DMA 交易風險的監管。

純粹的 DMA 模式指的是客戶的交易指令直接下單到交易所，因此並不經過期貨商的交易處理系統。所以，期貨商必須建立 DMA 作業的風險管理系統，即時且動態地密切監督客戶的即時風險，並且與位在(或鄰近)交易所的客戶交易引擎交換風險管理報告。

λ **其他資產類型的 DMA**

高度安全性且自動化的交易系統為現代化金融市場營運的基礎，幾乎每一種金融工具的市場參與者，都積極採取各式的自動交易系統和模型，也因此產生新的交易思維(trade ideas)。例如，商品交易顧問(Commodity Trading Advisor)，發現與其透過期貨商的交易台下達交易指令，不如建立自有的系統，或從軟體供應商購買交易系統，自行處理交易之執行。

DMA 交易模式也逐漸應用到其他資產類型，以美國證券市場為例，許多金融工具的交易---如期貨、外匯和固定收益類產品，正逐步採用各類型複雜的自動交易系統。由於期貨與證券的交易方式有許多雷同之處，證券交易系統擴及期貨交易相對比較容易。大部分的主力期貨合約現在均採用電子交易方式，期貨商均已習慣透過 FIX 應用程式介面進行電子化交易。

(4) 安全機制特徵

電子化交易的安全機制共包含五大項：

(a) *機密性(Confidentiality)*：保護資料不被竊取，以及被竊取之後也無法被解讀。

(b) *身份認證(Authentication)*：對於所收到的資料，得以證明其傳送者的身份。

(c) *完整性(Integrity)*：確保所收到資料並沒有遺漏或遭篡改。

(d) *不可否認性(Non-repudiation)*：使發送端不可否認送出某一資料，接收端不可否認曾接收某一資料。

(e) *存取控制(Access control)*：防止非法存取資料。

表格 4：安全機制比較表

	CA	DMA	SSL
機密性 Confidentiality	●加密演算法 非對稱式演算法 (PKI)	●加密演算法 專有線路 虛擬專線網路 (VPN)	●加密演算法 非對稱式演算法 (公鑰、私鑰)
身分認證 Authentication	●向公正可信賴第三者取得交易憑證。憑公鑰、私鑰確認	●憑 IP、MAC 專有線路 虛擬專線網路 確認資料來自特定單位。	●只使用伺服器單方之 SSL 憑證。憑 IP、MAC 確認
完整性 Integrity	●雜湊函數(hash) 數位簽章(私鑰)	●雜湊函數 專有線路 虛擬專線網路	●雜湊函數
不可否認性 Non-Repudiation	●PKI：憑公鑰、私鑰送收皆不可否認	●IP、MAC 專有線路 虛擬專線網路	
存取控制 Access Control	●憑公鑰、私鑰確認、認證和授權。	●專屬場地、專線管道確認	

λ **SSL 的安全機制**

1. 機密性：將網際網路上傳輸的訊息加密(encryption)，防止訊息被解讀。
2. 身分認證：客戶端(client)與伺服器(server)建立 SSL 連線進行交換時，採用 IP 與 MAC 的客戶端資訊，確認身份，並同時發行使用憑證，防止冒名傳送[#]。
3. 完整性：將傳輸的訊息以雜湊函數(Hash Function)產生訊息驗證碼(Message Authentication Code，MAC)保護，經由雜湊值的比對，確認訊息是否遭非法竄改。

λ **CA 的安全機制**

1. 機密性：以 PKI (Public Key Infrastructure)加密機制為基礎，傳送者利用接收者的公開金鑰(Public key)將訊息加密，接收者再利用自己的私密金鑰將信息解密。其目的為訊息將無法被他人解密。
2. 身分認證:由公正可信賴的第三者(CA 憑證管理機構) 對每一使用者以確認其身分，然後核發交易憑證。其目的是只有當事人擁有私密金鑰。
3. 完整性：將傳輸的訊息以雜湊函數(Hash)產生訊息摘要；以傳送者的私密金鑰(Private key)對摘要後的訊息執行數位簽章 (Digital Signature) 保護；傳送者以接收者的公開金鑰加密傳送；接收者以自己的私密金鑰將資料解密成明文；接收者再以發送者的公開金鑰解密並與雜湊值比對，以確認訊息內容並未被他人篡改，也沒有遺漏。
4. 不可否認性：在完整性的作業前提之下，由於公開／私密金鑰為特定的收／送方才擁有，因此，可以利用公開／私密金鑰比對文件加解密、電子簽章及其交易紀錄，確認收送雙方的傳輸交易。

[#] [註] 若通訊雙方均使用憑證(Certificate)可互相辨識身分的真實性，無法冒名傳送訊息。但 SSL 執行時只使用伺服器單方之 SSL 憑證，且 SSL 的安全機制係架構在通訊協定中的傳輸層上，用戶端與伺服器間只有在交易前建立連線時才執行身分辨識，雙方在傳輸每一交易內容時並不執行身分辨識。

5. 存取控制：收送兩方使用 CA 的授權憑證，並且在 CA 的確認核可之下，才能存取資源。CA 可防止未經授權的電腦存取，加上 PKI 透過公開／私密金鑰的保存，達到存取控制的要求。

λDMA 的安全機制

由於證交所對電子式專屬線路下單的定義，只要求委託人端與證券經紀商端之交易系統直接以「專線或封閉型專屬網路」聯結，藉由該項聯結，委託人之委託指示可直接傳送至證券經紀商的電腦系統，通過證券商電腦檢核後，即傳送至證券交易所，毋須再由證券商人員介入之自動化下單流程。除了對資料隱密性、身分確認性、資料完整性、交易不可否認性之管控機制外，該法令中並未提及實作上的技術要求，故實際達成的作法將依各家券商有所不同。以下就達成以上安全機制的可能作法探討之：

1. 機密性：DMA 達成機密性的方式有二層：(1)確保資料不會被讀取，及(2)及時被讀取，資料也無法被解開。第一項是專線或私有專線網路(VPN)的全時監控，確保通訊的過程未遭入侵；第二項是透過資料的加解密以進一步確資料不會被解開。傳送端使用加密演算法(encryption) 將通訊的資料由明碼文字轉變成第三者無法辨識的密碼文字傳送，接收端則以相對的解密演算法(decryption)將密碼文字轉換回純文字。加解密的方式可以採用對稱式加密演算法---在加密和解密時使用相同的金鑰；也可以採用非對稱式演算法---使用公開/私密金鑰組為之。
2. 身份認證：確保資料來自特定被認可之單位或個人。DMA 伺服器端可以根據所登錄的客戶端 IP 位址、MAC 位址、連線電路、客戶密碼、生理特徵資料、無線射頻(或 USB)鑰匙等方式混合，驗證客戶的真實身份。
3. 完整性：避免遭到竄改，一般以訊息驗證程式碼或雜湊值(hash)來確認資料的完整性。雜湊值是由一系列資料計算出來的固定長度的數值，用於

驗證傳送資料的完整性。比對接收端所計算出的雜湊值和傳送資料的雜湊值，以可判斷資料是否已遭到變更。

4. 不可否認性：使用特定的場地及其既定的連線電路(PN or VPN)是 DMA 強於 CA 的安全機制，也是更加強化的不可否認性基礎，傳送與接收兩方均不可否認其專有電路的資料傳輸交換行為。除此之外，傳送端的 IP 位址、MAC 位址之外，透過網路交易的時間戳記(Time Stamp)、事件紀錄(Event Log)、交易授權/監控等手段，更能增加交易的不可否認性。
5. 存取控制：期交所要求各期貨商提供上列四大安全性的專線網路交易機制，並預設使用者應負有保管發送端存取權限的責任，以達存取控制的安全性。除密碼、生理特徵資料、電子鑰匙(無線射頻卡/USB)等不可複製的存取要件外，尚包括期貨商交易場所的監控以及 DMA 交易過程的監控與授權。

壹拾壹、 DMA 與 CA 在應用上之比較

λ 責任負擔

→ DMA：一旦在申請之初經過身份確認，在期貨商與使用者之間建立起專屬路線後，由於專線本身沒有被截取盜用的問題，為了防止他人冒用下單，期貨商只需負責 DAM 場地進出及其交易終端設備的安全。因此，在建立 DMA 專屬線路時，期貨商也必需要評估使用者是否有能力可以擔負交易檯監督管理的責任。至於下單的內容如數量、金額等，則由下單者自行負責(期貨商為提供更貼心的服務，可以做一定程度的審核)。一旦發生交易糾紛，責任的歸屬相對明確。

→ CA：線上 CA 電子交易的問題，多半為 CA 資料遭到冒用或竊取，其相關責任的歸屬將視發生問題的原因而定，然後判定由使用者、期貨商或電子憑證管理機構來承擔責任。但目前而言，責任的歸屬向期貨商傾斜。

λ 建置成本

→ DMA：建置 DMA 專屬路線及其需求環境，為期貨商追求競爭力之 IT 基礎建設的延伸，其增加成本有限。尤其，一次建置之後，可以長久使用，並且可以供應 VIP 客戶以及大量客戶使用，不只易於管控，單位的平均使用成本也低。

→ CA：透過第三方來做電子憑證的驗證，使用者並不需要花費成本去建置新的設備等，然而，卻有 CA 電子憑證的相關維運成本[13]---發放、使用、註銷以及年度登錄／換發等等。

λ 使用者觀點

使用者進行交易時，所選擇的交易方式，多半以其效能、安全性與收取的手

[13]然而，使用電子憑證需支付憑證管理機構費用，只是目前多半是期貨商自行吸收。電子憑證的發行、註銷成本則由使用者負擔部份。

續費多寡等做為主要的考量因素。

→ DMA：以專屬線路的方式來進行交易，不但在安全上有一定程度的保障，另外也可提高其交易效能(以更快的速度進行連線)，再者，由於不需要經過交易員來進行交易的操作，因此也可以降低手續費的部分。

→ CA： CA 認證是設定在瀏覽器內，使用者在連上網頁時，即已在背景自動確認其身份，因此並不會影響使用上的方便性，同時在安全性上也有一定程度的保證[14]。而在手續費上，因為不需經過交易員處理，因此也有較透過交易員下單為低的優惠。

[14]相對於 DMA，使用電子憑證的電子交易效率較低，原因是須經過憑證管理機構的驗證。

壹拾貳、 DMA 適用客群分析

經由上述觀點的比較，吾人認為 DMA 較適用於法人或大額/專業投資人，一方面是一旦使用者端遭到盜用必須能夠自行負責；另一方面，其大量、頻繁的交易行為，方便性與速度為其主要的考量，比較具備成本效益。

對於一般民眾，DMA 的申請建置過程專業的方式，顯然太過繁瑣，有可能會降低其使用意願；而且，一般散戶極有可能無法或不願自行承擔專線被盜用的風險。針對一般民眾所在意的方便性以及手續費等考量，雖然交易的效率較 DMA 為低，使用 CA 認證的線上交易即可滿足其需求。因此對於一般民眾，吾人以為使用 CA 認證進行交易即可。

上一節中比較了 CA 與 DMA 在各方面的特性，因而吾人推論 DMA 與 CA 應該適用於兩種不同的客群。本節將針對比較適合採用 DMA 方式下單的客群，也就是所謂交易量大的顧客，先探討其現有的下單方式，再與 DMA 進行比較。

現行投資大戶買賣期貨的方式與一般散戶相同，主要也是透過親自臨櫃、電話語音、及網際網路三種方式為之，但是服務的品質則存在實質上的差異。

服務上的差異性以網路下單為最小。由於網路下單提倡所謂的網路平民化待遇，不論交易金額大小、交易次數多寡，都一視同仁，投資量小的投資人不會因此而受到冷落；而投資量大的客戶除了交易手續費較為低廉外，並沒有較大的便利性與安全性。因此實際上，所謂的大戶較少透過網際網路下單。一方面，一般大戶雖然很常投資買賣期貨，但並不盡然非常熟悉電腦，利用網路下單一旦輸入錯誤，其後果都是要自行負責，而交易量大之顧客一旦下單輸入有誤，所造成的財務影響將不堪設想。此外，大戶也不太放心如此巨額的交易完全經由電腦完成，不熟悉及不信任是其不熱衷於網路下單的原因之一。而另一項考量則是交易

的時效性，透過網路下單，大戶的速度並不會比一般投資人來得快，而操作過程的耽誤(如輸入帳號密碼或交易資料)所造成的時間落差，將導致其交易無法撮合或是引發重大損失。

相較於網路下單，一般大戶比較偏愛的還是透過電話直接跟營業員下單，因為他們可以獲得特殊尊榮的服務，尤其是在交易的便利性及速度上。交易量達到一定程度以上之顧客，通常都會擁有一支電話專線，由專人接聽，並且擁有專屬的輸入交易單人員，顧客一邊下達交易指示的同時該輸單人員就會一邊輸入，之後就立刻送出交易指令，可以確保所委託之交易在第一時間內被送出。這一點對於交易頻繁且龐大的顧客至關重要，速度為其交易的關鍵，因為一旦出現時間的落差，將會影響買進或賣出的價格，對於這些大額投資人來說會導致其成本重大的變動；此外，透過電話下單，大戶的手續費將享有比一般散戶低廉許多的優惠，並且可以把輸單錯誤的風險轉嫁給營業員，以上這些都是大額投資人較常採用電話下單的原因。同理，當大戶有空時會親自臨櫃，利用 VIP 室之看盤系統再透過內部線路下單，也是因為以上種種考量。

在美國或是歐洲其他許多國家中，DMA 已經在法人或是大額投資人的交易中被廣泛的使用，而投資人之所以使用這種方式，主要的原因不外乎較為低廉的手續費、較快的速度以及匿名性。台灣於 2006 年六月一日開始，明文規定 DMA 也為現行下單方式的一種，以下，我們將站在大額投資人的立場，針對就他們目前較常使用的方式--電話下單，與未來可能實行的方式--DMA 去做一個較詳盡的比較，進而深入探討何者近較為可行。

λ **手續費**

DMA 的手續費將較電話下單更為低廉，雖說大部分期貨商會對大額投資人進行退佣的動作，使得實質的手續費變的較低，但是 DMA 因為不需要透過

券商的營業員，一切交易動作都是客戶自己透過交易平台進行，理所當然手續費會更為低廉。

λ **速度**

一方面對於熟悉電腦的投資人來說，透過 DMA 可以在第一時間下單，無需經過撥電話接通營業員的步驟；另一方面，DMA 可以結合自動化的交易程式和策略(如 Algorithmic Trading)，其速度絕對比人為輸單更快速。

λ **主控權**

透過 DMA，期貨商的功能將蛻變為清算與風險管理，而非提供交易服務的場所，投資人對於自己的交易流程握有主控權。同時，期貨商的服務品質與差異化對客戶而言並非最主要的關鍵因素，相對的，交易平台的開發、分析性工具(交易前及交易後)與即時性市場資料的提供才是期貨商的區隔因素。

λ **匿名性**

相較於透過電話下單，DMA 擁有匿名性。由於委託單並不會經過營業員的手中，因此交易內容具有隱密性的，對於不想要讓非關係人在第一時間得知下單內容的大戶而言，DMA 有相當程度的安全性和隱匿性。

綜合以上要點，吾人認為針對大額投資人而言，推行 DMA 可能會讓部份客戶覺得優於傳統電話下單，因為主控權增加了，手續費降低了，也較以往網際網路下單的速度要來得快上許多；但是仍然有一群顧客對於電腦具有很深的不安全感與使用障礙，因此低廉的手續費並不足以構成充分的誘因；此外，交易流程的主控權也不是其交易的關鍵，對於這樣的客戶，傳統電話下單或是臨櫃交易似乎更為合適。

壹拾參、 結論與建議

一、 CA 與 DMA 之安全性比較

我國對於證券與期貨的電子交易，目前均依據電子簽章法，要求以公正第三者發放之電子憑證為交易真實性之確認。然而探究其適法性與必要性，以及法人和專業投資人的交易需求，吾人以為 DMA 之安全機制無虞，實無必要再透過電子憑證的認證。事實上，透過專線或專屬網路與交易所連線，其原生的安全性即遠高於一般散戶所使用的公共網路；再者，DMA 尚可配合特定的安全機制，例如設定可交易終端設備的 IP 位址加上其硬體的 MAC[15]位址，交易者非使用其指定的終端設備，無法進行交易。

二、 CA 與 DMA 之作業成本比較

從成本面考量，電子憑證均有一定的時效，因此有發行、註銷、再發行的成本。加以每一筆使用電子憑證的交易均須支付電子憑證管理中心使用費，對於交易頻繁的客戶，需負擔一筆不小的使用開銷。

相對而言，透過電子憑證的方式遠高於使用 IP、MAC 位址或是生理特徵資訊(Biometrics)，原因在於後者的費用皆為一次性 (如登錄、Biometrics 讀取設備)，而電子憑證卻有發放、使用及註銷的週期性維護成本。

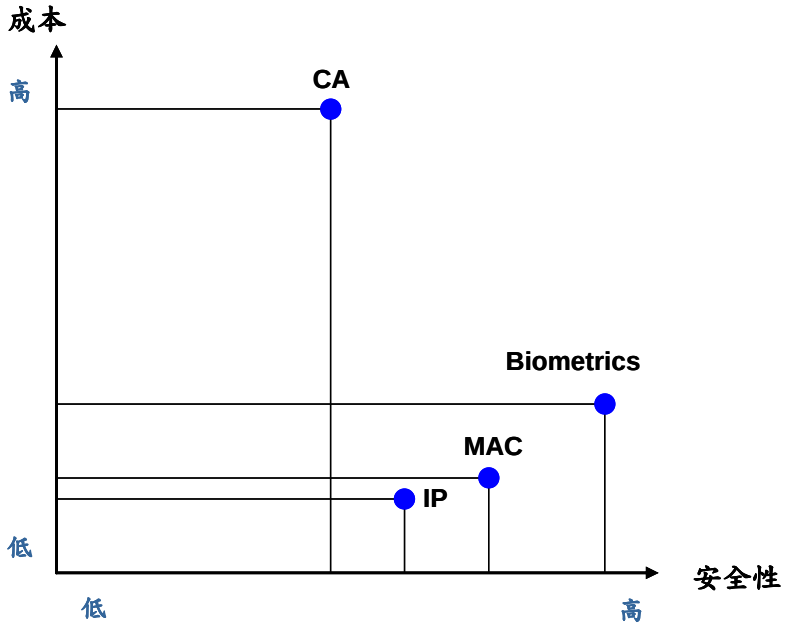
三、CA 與 DMA 之安全性及作業成本綜合比較

下圖綜合描述了 CA 及 DMA 之安全性與作業成本的相對效益。圖中，CA 採用 PKI 認證機制，付出每年度的電子憑證發放／維護成本；然而，DMA 則以一次性的基礎建設完成 DMA 環境設置，並且可以搭配 IP 及 MAC 認證機制以大

[15] Media Access Control 位址，為網路卡獨一無二的位址，實體 MAC 位址通常燒錄在網路卡的 EEPROM 上，無法輕易竄改。

幅提高交易安全性，爾後的作業成本就相對的低廉。

圖表 27：安全機制之成本效益



資料來源：本研究整理

四、CA 與 DMA 速度考量

對於法人及專業投資人而言，交易的速度是另一項重要考量因素。對於法人客戶而言，電子憑證則拖累其交易速度，甚或因延遲而致使交易失敗，並且不利於演算法交易等高度自動化交易方式的執行。

目前使用電子憑證的交易方式，整個期貨交易完成時間需時 1.5-1.8 秒(在網路未擁塞、無大量等候交易單的情況下；包含加密所需 0.3 秒左右)，相較於國外法人毫秒等級的 DMA 交易實在不可同日而語。再者，國外的期貨交易並未要求電子憑證，我國特有的交易規範，對於國外客戶實有窒礙難行，因此不利於我國期貨交易市場的國際化。

五、電子交易安全機制的根本要件及其他作業方式

滿足機密性、身份認證、完整性、不可否認性、存取控制等五大要項

即電子交易安全機制的根本要件。

1. *機密性(Confidentiality)*：保護資料不被竊取，以及被竊取之後也無法被解讀。
2. *身份認證(Authentication)*：對於所收到的資料，得以證明其傳送者的身份。
3. *完整性(Integrity)*：確保所收到資料並沒有遺漏或遭篡改。
4. *不可否認性(Non-repudiation)*：使發送端不可否認送出某一資料，接收端不可否認曾接收某一資料。
5. *存取控制(Access control)*：防止非法存取資料。

CA 電子憑證為交易安全機制的選項之一，實作上還有其他的安全機制可供選擇。CA 與 DMA 電子交易之安全機制比較表如下圖。

表格 5：CA 與 DMA 交易安全機制之比較

	CA	DMA
機密性 Confidentiality	☆加密演算法, 非對稱式演算法 (PKI) Encrypted (Text + hash-value (PK))	∨加密演算法, 虛擬專線網路(VPN) Text transferred under Link Protection (DMA: Authorized/Monitored) over leased line/VPN
身分認證 Authentication	☆向公正可信賴第三者取得交易憑證。憑公鑰、私鑰確認 Check PK ONLY!	∨確認資料來自特定單位。虛擬專線網路 Check PW (Biometrics,…), MAC, IP addresses
完整性 Integrity	☆雜湊函數(hash)數位簽章(私鑰 hash value) Text + hash-value (PK)	∨雜湊函數 虛擬專線網路 Text + transferred under Link Protection (DMA: Authorized/Monitored) over leased line/VPN
不可否認性 Non-Repudiation	☆PKI：憑公鑰、私鑰送收皆不可否認 Timestamp, hash-value (PK), Event-log (CA: third-party)	∨虛擬專線網路 PW (Biometrics, …) MAC, IP (location-based), Time-stamp (or nonce, event number) Event-log (DMA: Authorized/Monitored)
存取控制 Access Control	☆憑公鑰私鑰確認、認證和授權。 PK log-on	∨專線管道確認 Password (Biometrics, …) DMA: On-Site, equip.. Authorized/Monitored

資料來源：本研究整理

綜合而言，CA 電子憑證的交易安全機制，其適用範圍可以涵蓋安全性脆弱的一般化／個人化網際網路環境，但非唯一的方案。在 DMA 核可的環境之下，其安全條件較高，被授權可以使用的使用者相對地安全可靠，便可以採用更簡單且更快速，如 IP+MAC+Biometrics，的認證方法。

在先進科技的引進之下，還可以規範其他替代方法。例如，電子交易透過用戶端設備安全管控機制，如 IP+MAC，加上無線射頻(RFID)卡做為另一項存取的鑰匙，以及主從端的 SSL 交易機制，亦可達到使用電子交易安全機制的五大根本要件，不只可以大幅提高其方便性，成本卻大幅簡省。

六、綜合建議

吾人以為，因為公眾網路在安全方面有其脆弱性，對於使用公眾網路的散戶而言，要求使用 CA 電子憑證可以提高其交易的安全性。然而，若對外國人強行要求 CA 認證，則必須要求該人到我國臨櫃申請 CA，本身就是一項業務執行上非常困難的任務，不利於國際化推廣。此外，目前透過 CA 認證方式對於新興的交易型態如手機下單，存在執行上的困難(最主要是交易執行的遲滯)，不利於大量推廣。

對於使用 DMA 專線或是專屬網路與期貨商(或是期交所)連接的法人或是專業投資人而言，透過特定安全機制(如上述之 IP+MAC 位址、存取密碼、生理特徵資訊、智慧卡、USB 鑰匙等)，加上專線或專屬網路本身的安全性，即可達成比電子憑證更高效力的交易要求。同時，其交易成本、效率和穩定性卻遠為優越。

換言之，對於使用 DMA 的環境而言，電子憑證實屬累贅：一方面導致交易之延遲；另一方面對於安全性(包括機密性、身份確認、完整性、存取控制、不可

否認性)並未有所謂的顯著提昇。

從促成我國期貨市場之國際化之觀點考量，吾人以為，考慮免除 DMA 交易方式之法人、專業投資者再度使用 CA 電子憑證之要求的可行性，俾利其交易效率和新型態交易策略如演算法交易之執行，以擴大市場規模並和國際接軌。

綜合言之，審視網路交易電子憑證認證之必要性及其替代性方案，加強先進技術之引進，以提升散戶之交易速度及方便性(如透過手機下單)，並減輕期貨商的負擔(主要為電子憑證之使用及管理成本)，除了 CA 之外，還有其他更好的方法。

附　錄

開放證券經紀商接受投資人採行電子式專屬線路下單---自 95 年 6 月 1 日起實施

來源:「行政院金管會證期局第二十五期新聞信」
http://www.sfb.gov.tw/e-sfb/e-newsletters/200607/200607-002.doc

---

行政院金管會證期局第二十五期新聞信

壹、 重要公告

一、 修正證券交易法取得股份申報事項要點

為符合司法院大法官會議第 586 號解釋之意旨，並強化取得人相關資訊之公開，以使投資人更充分瞭解公司股權重大異動資訊，進而提高資訊揭露之效益及保障投資人權益，俾促進對大量取得公開發行公司股權之管理效能，爰於 95 年 5 月 19 日修正發布本要點。

二、 訂定證券交易法重大消息範圍及公開方式管理辦法

依證券交易法第 157 條之 1 第 4 項修正條文規定，授權主管機關訂定重大消息之範圍及其公開方式等相關事項。有鑑於「罪刑法定原則」及「構成要件明確性原則」，並因應未來市場之變化及符合市場管理之需要，爰訂定本辦法，並於 95 年 5 月 30 日發布。

三、 健全證券暨期貨市場各服務事業內部控制及內部稽核制度

本會於 95 年 5 月 30 日修正發布「證券暨期貨市場各服務事業建立內部控制制度處理準則」，除強化內部控制制度及提昇內部稽核執行效果及獨立性外，並增列法令遵循制度及落實公司治理規定，以健全證券暨期貨市場各服務事業內部控制制度及內部稽核制度。

四、 限縮境外基金之銷售機構 2 年未受一定處分之範圍

本會 95 年 5 月 16 日修正發布境外基金管理辦法第 19 條規定，原規定擔任境外基金銷售機構必須最近 2 年內未曾受一定處分，考量對境外基金銷售機構則可採較低度管理，爰限縮上述受處分之範圍，如其受處分之事由與辦理基金業務無關，或受處分金融機構之違規事由已確實改善並經主管機

關認可，則不受上述資格條件之規範。

五、 開放境外華僑及外國人投資證券投資信託事業私募之證券投資信託基金

為擴大外資投資我國證券市場，本會於 5 月 16 日發布令開放境外華僑及外國人投資證券投資信託事業私募之證券投資信託基金。

六、 *開放證券經紀商接受投資人採行電子式專屬線路下單*

開放證券經紀商接受投資人採行電子式專屬線路下單 (Direct Market Access)，自 95 年 6 月 1 日起實施。

七、 規範證券商以分割公債或金融債券充當營業保證金

本會 95 年 5 月 25 日發布令，規範證券商以分割之公債或金融債券充當證券商管理規則第九條規定之營業保證金，應以該分割債券到期面額之百分之八十五作為計價標準。

八、 研擬開放外資投資我國投信業者發行之外幣計價基金

本會研議開放外資投資我國投信業者發行之外幣計價基金，並比照現行外資投資我國有價證券方式由保管銀行每月代為申報，俟證交所完成電腦開發作業後，本會將發布令開放外資投資該項商品。

證券經紀商辦理電子式專屬線路下單(Direct Market Access)業務：

來源：臺灣證券交易所股份有限公司　函
http://www.tse.com.tw/docs1/data01/set/public_html/09500106461.htm

臺灣證券交易所股份有限公司　函
受文者：如行文單位
發文日期：中華民國 95 年 5 月 29 日
發文字號：台證交字第 09500106461 號
速別：普通件
密等及解密條件或保密期限：普通
附件：無

主旨：證券經紀商辦理電子式專屬線路下單(Direct Market Access)業務，應依說明事項辦理，請　查照。

說明：

一、依據行政院金融監督管理委員會 95 年 5 月 18 日金管證二字第 0950111250 號函辦理。

二、證券經紀商辦理電子式專屬線路下單業務，應於開辦二週前，檢具「證券經紀商辦理電子式專屬線路下單業務申請書」，將開辦日期與所採行的資訊傳輸架構、流程，經合理評估可達到身分確認性、資料完整性、資料隱密性、交易不可否認性之管控機制說明文件，函報本公司備查，並於「證券商申報單一窗口」完成各項開辦基本資料之申報作業，俟本公司函復同意備查後，始得辦理。

三、證券經紀商接受委託人採行電子式專屬線路下單前，應利用「證券商申報單一窗口」向本公司申報該委託人之帳戶資料。

四、「證券商申報單一窗口」之電子式專屬線路下單申報功能建置完成後，本公司將另行公告周知，屆時已辦理本項業務之證券商，應依時限完成相關資料的補申報作業。

五、證券商辦理電子式專屬線路下單業務，應確實遵循本公司「營業細則」、「證券經紀商受託契約準則」、「證券經紀商辦理電子式專屬線路下單作業要點」等證券市場相關規定，落實資通安全與風險管控，不得有影響證券集中交易市場秩序與效率之行為。

正本：各證券商

副本：行政院金融監督管理委員會證券期貨局（第二組）、中華民國證券商業同業公會、財團法人中華民國證券櫃檯買賣中心、臺灣期貨交易所股份有限公司、法源資訊股份有限公司、精融網路科技股份有限公司、台北國際金融資訊協會、博仲法律事務所、本公司稽核室、資訊服務部、電腦規劃部、電腦作業部

財團法人中華民國證券櫃檯買賣中心證券經紀商辦理電子式專屬線路下單（Direct Market Access）作業要點:

開放證券經紀商接受投資人採行電子式專屬線路下單（Direct Market Access），自 95 年 6 月 1 日起實施。

發布日期 95.07.11 **法規名稱** 財團法人中華民國證券櫃檯買賣中心證券經紀商辦理電子式專屬線路下單（Direct Market Access）作業要點
中華民國九十五年七月十一日財團法人中華民國證券櫃檯買賣中心證櫃
交字第 0950017252 號公告訂定發布全文 3 點；並自公告日起實施
中華民國九十五年七月五日行政院金融監督管理委員會金管證二字第 0950128052 號函辦理
來源：http://www.selaw.com.tw/Scripts/Query4A.asp?FullDoc=all&Fcode=G0101723

法規名稱：**財團法人中華民國證券櫃檯買賣中心證券經紀商辦理電子式專屬線路下單（Direct Market Access）作業要點（民國 95 年 07 月 11 日 修正）**

壹、定義

電子式專屬線路下單，係指委託人端與證券經紀商端之交易系統直接以專線或封閉型專屬網路聯結，藉由該項聯結，委託人之委託指示可直接傳送至證券經紀商的電腦系統，通過證券商電腦檢核後，即傳送至本中心，毋須再由證券商人員介入之自動化下單流程。

貳、作業要點

一、證券經紀商辦理電子式專屬線路下單業務，應配合增修內部控制、稽核相關規定，並於開辦二週前，將開辦日期，與所採行之資訊傳輸架構、流程，經合理評估可達到身分確認性、資料完整性、資料隱密性、交易不可否認性之管控機制說明文件，函報本中心備查，並於「證券商申報單一窗口」完成各項開辦基本資料之申報作業。已向臺灣證券交易所股份有限公司申辦並取得該公司備查函者，毋須重複向本中心申辦。

二、證券經紀商接受委託人採行電子式專屬線路下單前，應向本中心申報該委託人之帳戶資料。

三、證券經紀商辦理電子式專屬線路下單時，應建置電腦篩檢功能與管理程序，確保每筆委託符合相關規定；電子式專屬線路下單之委託同其

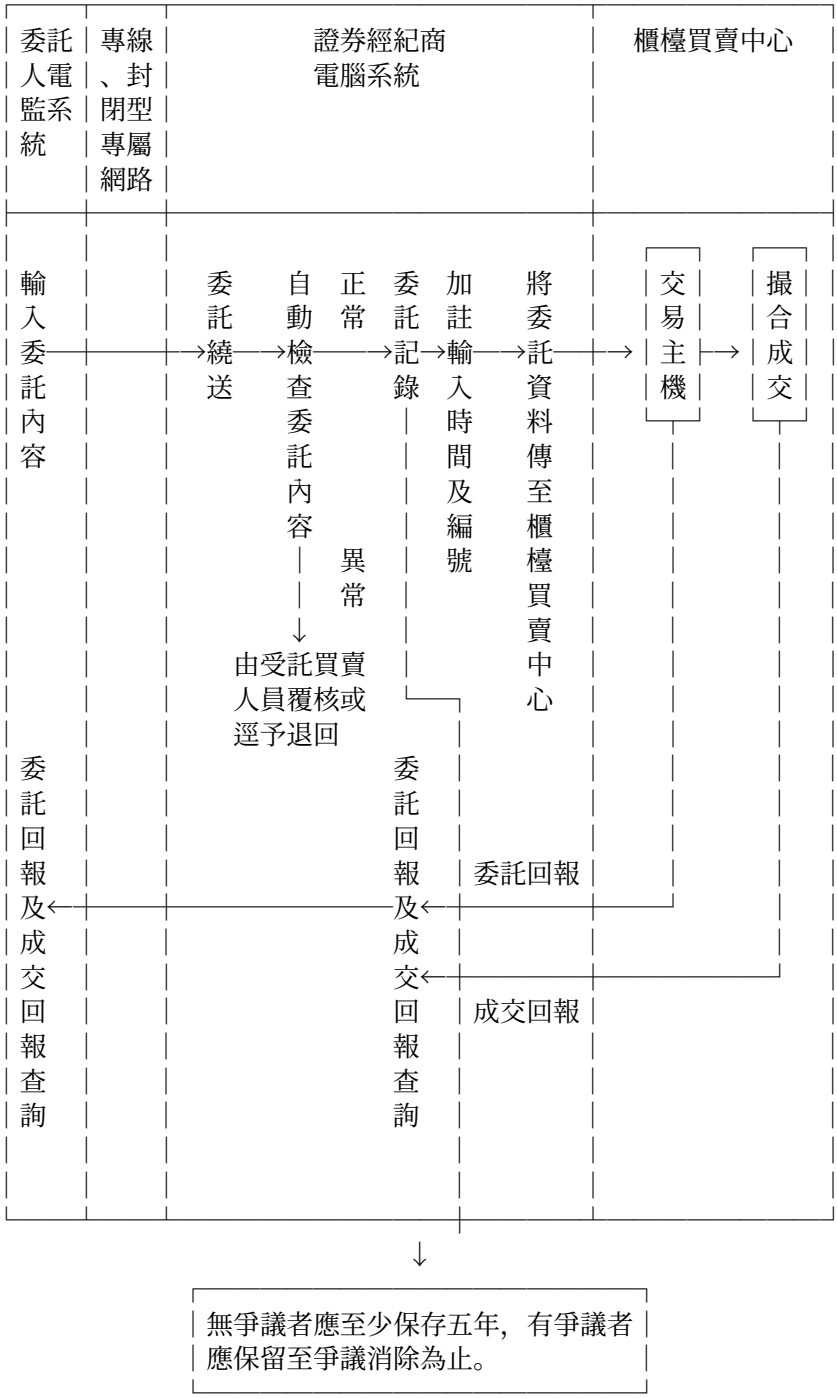
他方式之委託，傳送至本中心時，應加註委託傳送之時間及編號，並不得有跳號、漏號或重複編號等情事；對於採行電子式專屬線路下單與其他下單方式之委託應有公平的先後次序。

四、採行電子式專屬線路下單之委託人與證券經紀商（或其海外分支機構）之聯結入口皆在中華民國境外時，其間連線方式必須符合所在國當地的法令規定，且該聯結入口與證券經紀商在台分（總）公司之交易系統，應以專線或證券商專屬交易網路聯結。

五、證券經紀商辦理電子式專屬線路下單或其他委託方式，皆應確實遵循證券市場相關規定、落實資通安全與風險管控，不得有影響證券櫃檯買賣市場秩序與效率之行為。

六、證券經紀商辦理電子式專屬線路下單業務如發生異常狀況致有影響市場交易秩序之虞時，本中心得要求證券經紀商暫停、限制或禁止其特定、部分或全部客戶使用電子式專屬線路下單。

參、證券經紀商辦理電子式專屬線路下單業務，製作買賣委託紀錄之處理流程：



註：Pure DMA 用戶可否直接下單至期交所?

若使用者可直接以 Pure DMA 的方式，直接連線到期交所系統直接下單，則可減少中間經過期貨商的這個步驟，對使用者而言，交易進行的速度可能可以更快。然而，在目前的方式之下，使用者並無法直接以 Pure DMA 的方式連線到期交所系統下單。

期貨下單之委託方式與基本流程：

期貨下單之委託方式：

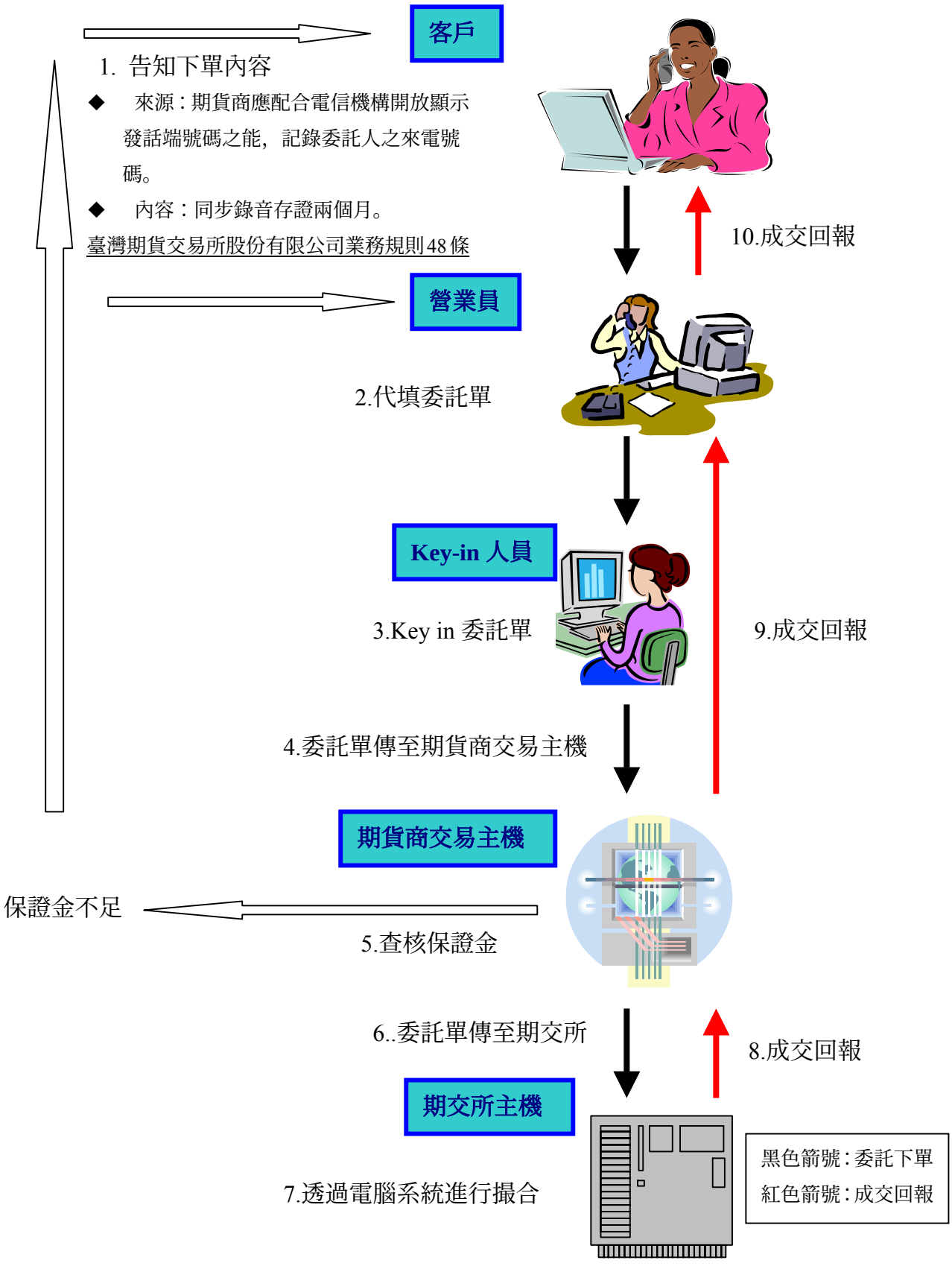
現行期交所允許之期貨下單委託方式非常的廣泛，大致上包括了臨櫃下單、透過書信、電報或使用傳真機下單，電話或語音下單，透過 IC 卡或網際網路下單，以及今年六月一號開始實施的電子式專屬線路下單(Direct Market Access)。其中，有部份委託方式已經漸漸沒落或是被取代，例如書信電報等方式；而有幾種方式則是大多數人所採用的，包括臨櫃、電話以及網際網路，以下將先介紹委託下單的基本流程，再透過流程圖詳細介紹之。

期貨下單之基本流程：

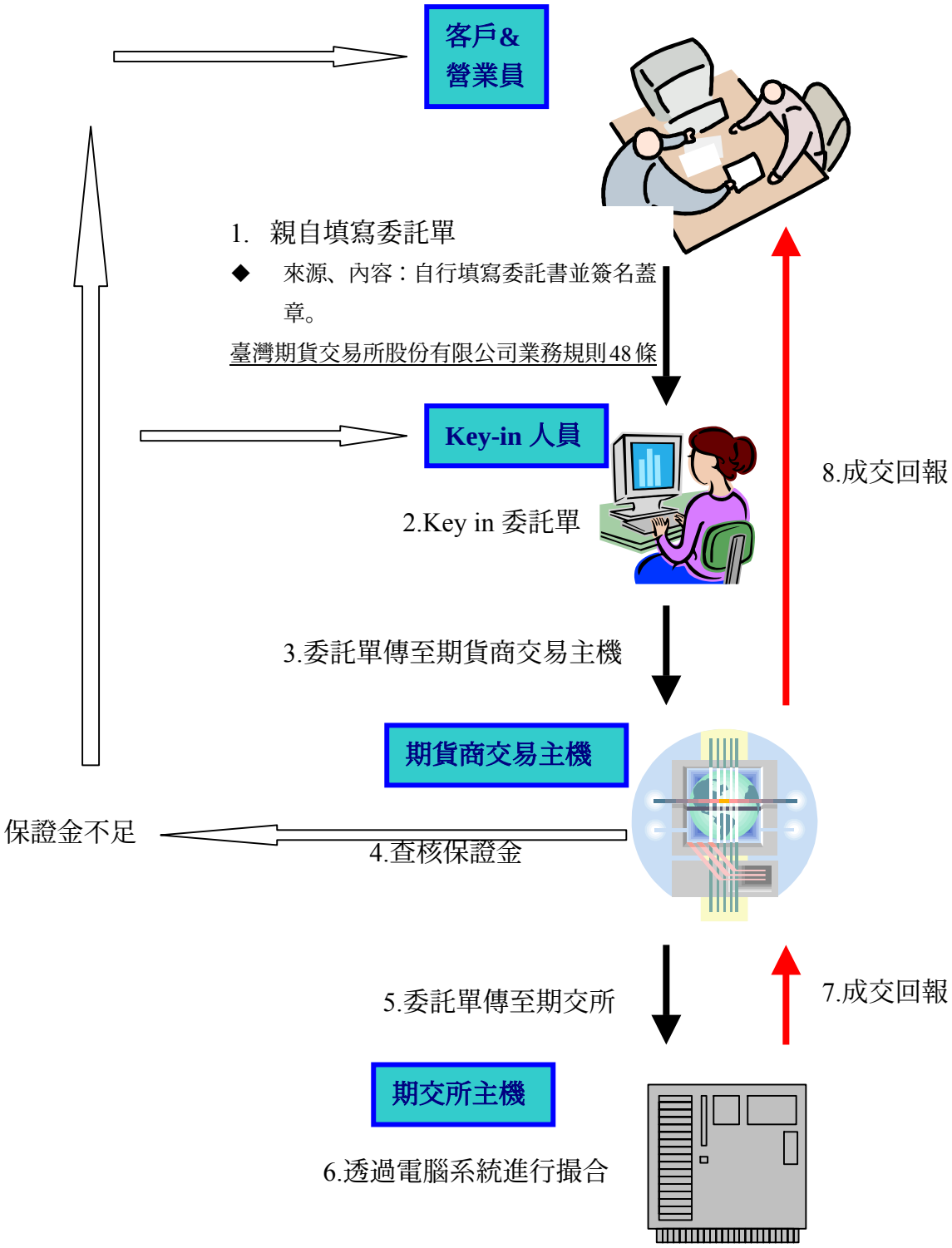
其實不論是哪一種下單方式，其原理都是一樣的，大致上都是經過以下幾個步驟：

1. 期貨交易人執行委託：期貨交易人自行填寫委託單(當面委託)、經由電話告知營業員代填委託單(電話委託)、或是透過網路自行輸入委託單(網路委託)。委託單內容必須載明帳號、戶名、買賣方向、口數、交易月份、商品名稱、價位與委託條件。
2. 查核保證金：期貨商之電腦系統會查核保證金是否足夠。
3. 接受委託：保證金足夠後期貨商接受該筆委託。
4. 進行措合：接受委託後，委託單會透過期貨商交易主機傳至期交所主機進行措合。
5. 成交回報：成交後期交所主機將回報給期貨商，期貨商再透過網路下單平台、語音或電話告知投資人。
6. 製作買賣報告書及對帳單：期貨商會每日發出「期貨交易人買賣報告書」，詳列交易日期、買入賣出口數、成交價格、手續費、期交稅、帳戶餘額等，以及每月對帳單給投資人。

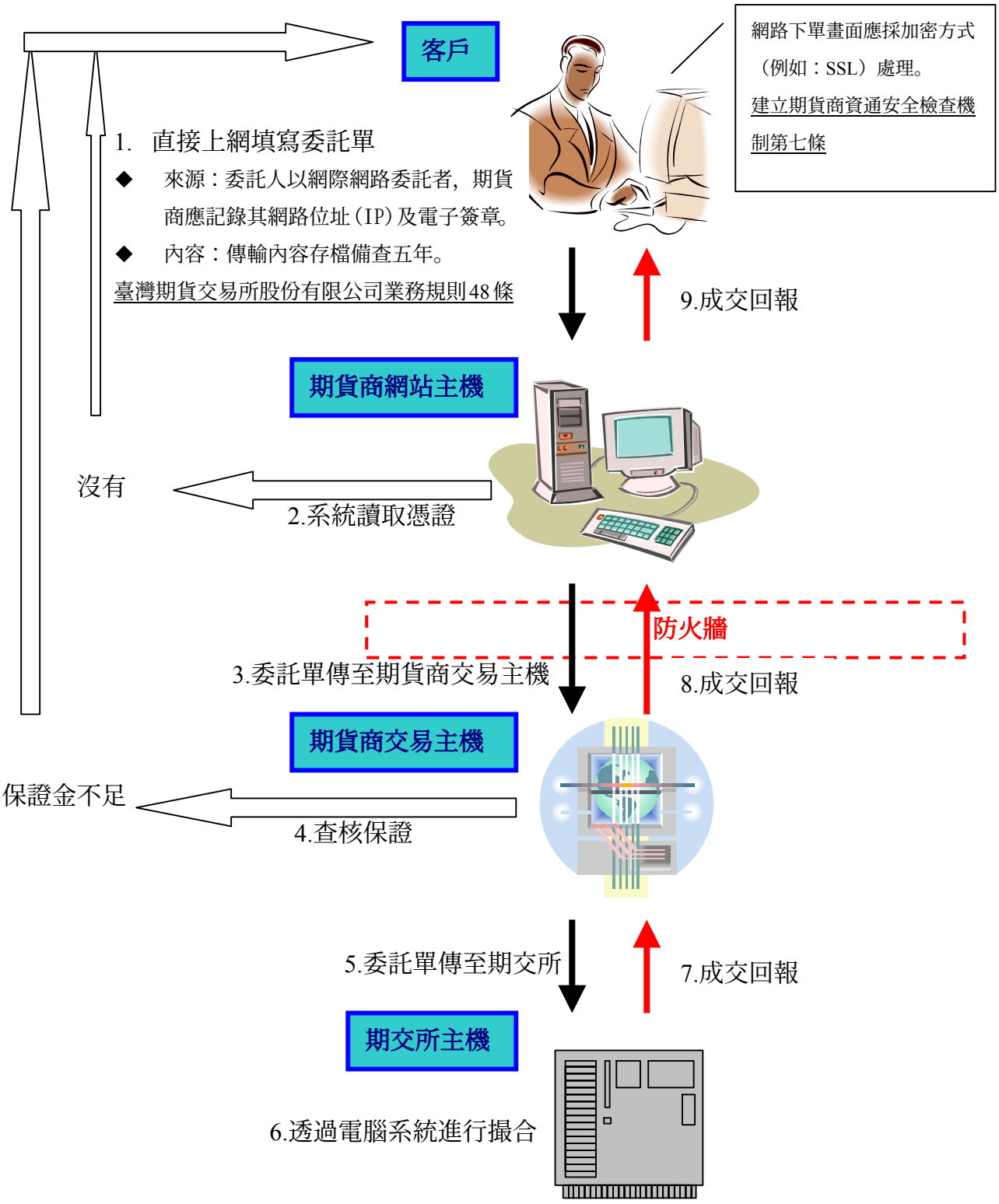
電話委託下單流程：


客戶
1. 告知下單內容
◆ 來源：期貨商應配合電信機構開放顯示發話端號碼之能，記錄委託人之來電號碼。
◆ 內容：同步錄音存證兩個月。
臺灣期貨交易所股份有限公司業務規則48條
10.成交回報
營業員
2.代填委託單
Key-in 人員
3.Key in 委託單
9.成交回報
4.委託單傳至期貨商交易主機
期貨商交易主機
保證金不足
5.查核保證金
6..委託單傳至期交所
8.成交回報
期交所主機
7.透過電腦系統進行撮合
黑色箭號：委託下單
紅色箭號：成交回報

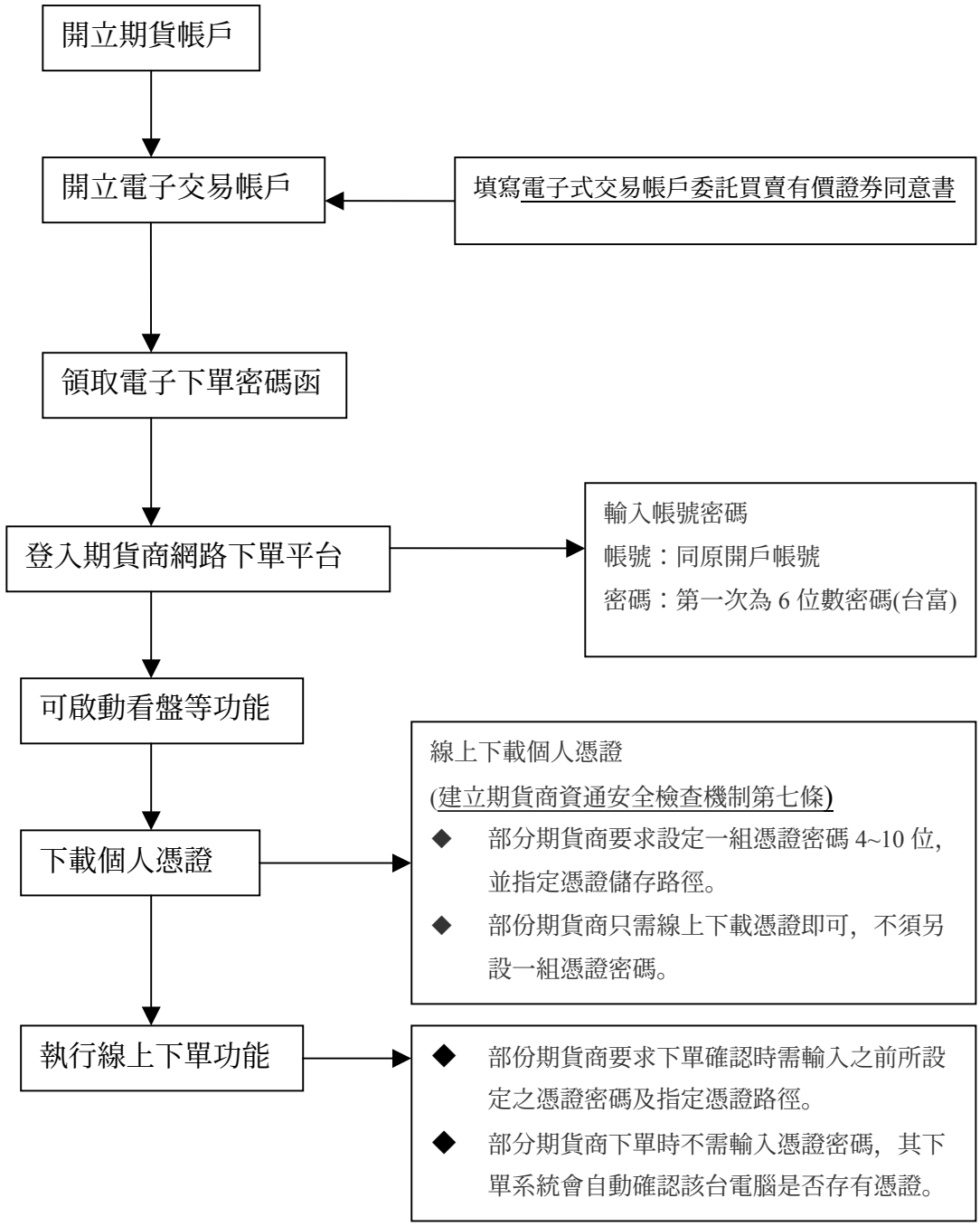
臨櫃委託下單流程：


客戶&
營業員
1. 親自填寫委託單
◆ 來源、內容：自行填寫委託書並簽名蓋章。
臺灣期貨交易所股份有限公司業務規則48條
Key-in 人員
2.Key in 委託單
3.委託單傳至期貨商交易主機
期貨商交易主機
保證金不足
4.查核保證金
5.委託單傳至期交所
期交所主機
6.透過電腦系統進行撮合
7.成交回報
8.成交回報

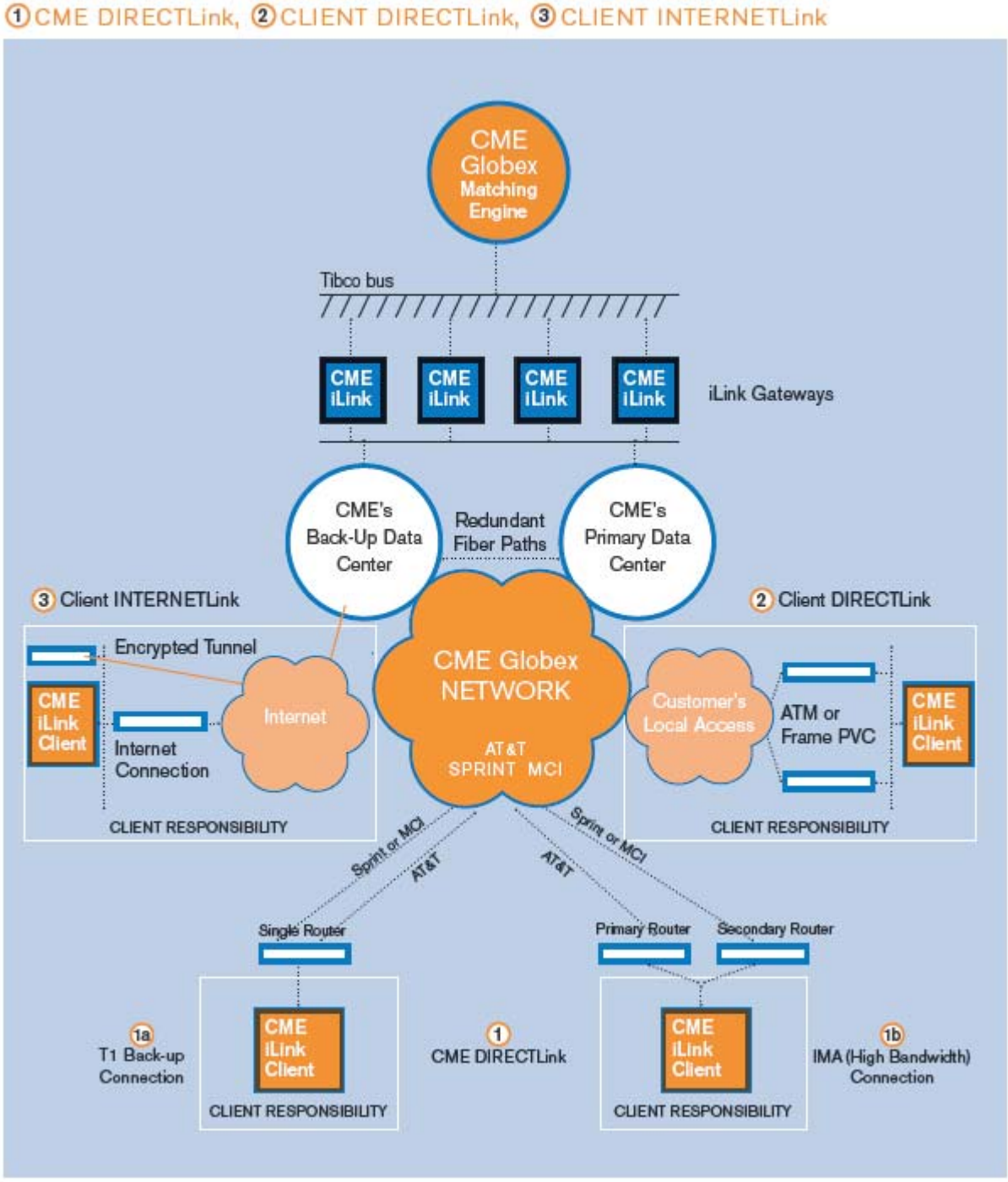
網際網路委託下單流程：


客戶
網路下單畫面應採加密方式（例如：SSL）處理。
建立期貨商資通安全檢查機制第七條
1. 直接上網填寫委託單
◆ 來源：委託人以網際網路委託者，期貨商應記錄其網路位址（IP）及電子簽章。
◆ 內容：傳輸內容存檔備查五年。
臺灣期貨交易所股份有限公司業務規則48條
9.成交回報
期貨商網站主機
沒有
2.系統讀取憑證
防火牆
3.委託單傳至期貨商交易主機
8.成交回報
期貨商交易主機
保證金不足
4.查核保證
5.委託單傳至期交所
7.成交回報
期交所主機
6.透過電腦系統進行撮合

開立電子式交易帳戶及憑證下載：

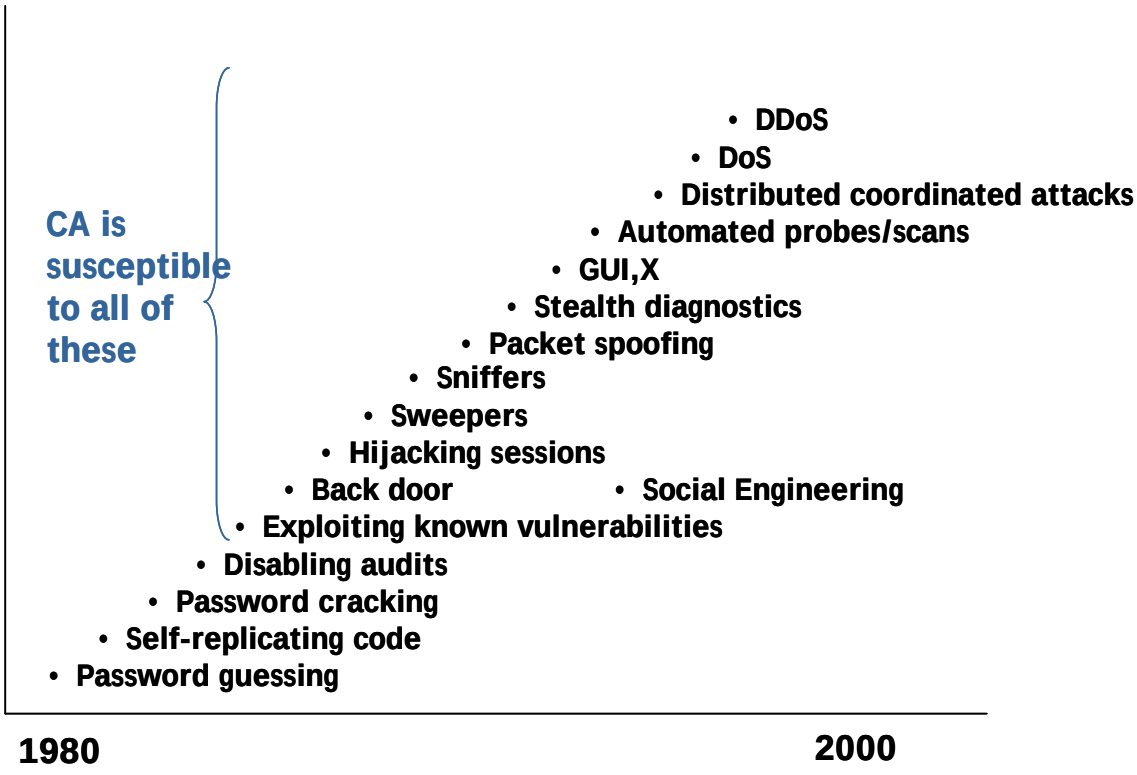


圖表 28：CME Globex 網路架構



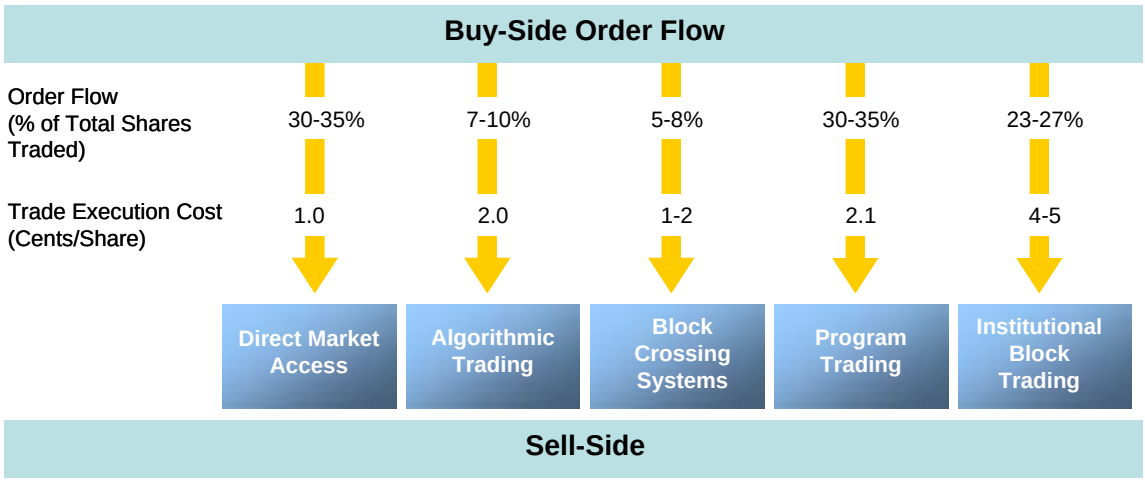
資料來源：CME

圖表 29：已知網路攻擊類型



資料來源：Pilot Network; 本研究整理

圖表 30：Buy-Side Order Flow and Cost for Various Trade Strategies and Order Destinations



資料來源：TowerGroup, 2006

參考資料

1. Bear, K., Hod, Z., Enness P., Graham, A. (2006), "Tackling Latency – the Algorithmic Arms Race," IBM Corp.
2. "CME Globex Overview," Chicago Mercantile Exchange.
3. DiTullio, S. (2005), "Pure Direct Market Access On the Rise," Barclays Capital.
4. DiTullio, S., Brent, D., "Low-Latency DMA to Futures & Options Exchanges Globally," Barclays Capital.
5. Goldberg, D. (2006), "The Birth of "Instividual" *Blurring the Lines between Institutions and Individuals*," Bear Sterns.
6. Evan, D. (2006), "VeriSign Financial Overview, *VeriSign Analyst Day*," VeriSign.
7. Hansen, L. (2006), "Challenges — and Opportunities — in the Institutional Markets," IDA Conference, Greenwich Associates.
8. Mason, M., Callahan, M., Dimitrion, G. (2006), "SIA's Cross Border Outlook and Initiatives," SIA.
9. Ramistella, A. (2006), "Crossing Networks: Bringing Back Large Block Trades to Institutional Trading," TowerGroup.
10. Shand, E. (2006), "Integrated Financial Markets: The Drive towards Increased Efficiency & Liquidity," OMX.
11. Shieh, S.P. (2006), "Introduction to Network Security," National Chiao Tung University.
12. Siokos, S. (2006), "Trading Technologies: The impact of Direct Market Access," Citigroup Sunlive Financial Services 2006.
13. Shriver, R. (2005), "Introduction to FIX and the FAST Protocol," Jordan and Jordan.
14. Spivack, J., Goldberg, S. (2006), "Reg NMS, NASD 3012/3013 and NYSE 342: Satisfying Regulators and Improving Your Organization," Grant Thornton LLP.
15. Worthington, K., Harris, D., (2006), "Equity Execution Venues *As the Market Turns Up the Volume, Exchanges Expand Frequency through Mergers*," JPMorgan.
16. http://www.pki.gov.tw/gcasite/dilaw/dilaw3.htm 政府憑證管理中心--電子簽章法草案四十問
17. http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm 經濟部商業司--電子簽章法
18. http://www.selaw.com.tw/Scripts/Query1A.asp?no=1G0101501&K1=期貨&K2=CA
19. http://www.selaw.com.tw/Scripts/Query1A.asp?no=1G0101415&K1=電子簽章&K2=期貨
20. http://www.cib.gov.tw/news/news01_2.aspx?no=8 刑事警察局--偵破電腦駭客入侵網路下單系統案
21. http://www.twca.com.tw/ 台灣網路認證公司
22. http://www.hitrust.com.tw/hitrustexe/frontend/default_tw.asp 網際威信