

第二十四章 電子付款系統

指導教授：黃正聰博士
報告人：陳彥廷

第二十四章 電子付款系統

- 一、電子支付系統名詞介紹
- 二、電子付款系統的架構
- 三、電子交易系統所要考慮的因素
- 四、電子付款系統的種類
- 五、代幣式付款系統
- 六、信用卡電子付款系統
- 七、結論

24.1 電子支付系統名詞介紹

- 1. 買方(Buyer)

指在線上交易中，購買商品的一方，即是付款者(Payer)

- 2. 賣方(Seller)

指在線上交易中，販賣商品的一方，也就是收款者(Payee)

- 3. 發行機構(Issuer)

發行機構的目的是提供顧客線上支付工具及服務，建立持卡人身分認證及授與證書的各項過程，並提供安全電子商業的運作規範

●4. 收單機構(Acquirer)

即是提供商店收款金融服務的銀行，它負責代理商店進行應收帳款的清算、管理商店帳戶等。並建立特約商店認證、註冊的各項過程，提供了安全電子商業的運作規範

●5. 公正第三者(Trusted Third Party)

公正第三者，其目的在於調解Internet上交易所發生的問題及爭執。他可能具有判決爭議的權力，或是從事強制性控制機制的核發

- 6. 電子證書認證中心(Certificate Authorities)

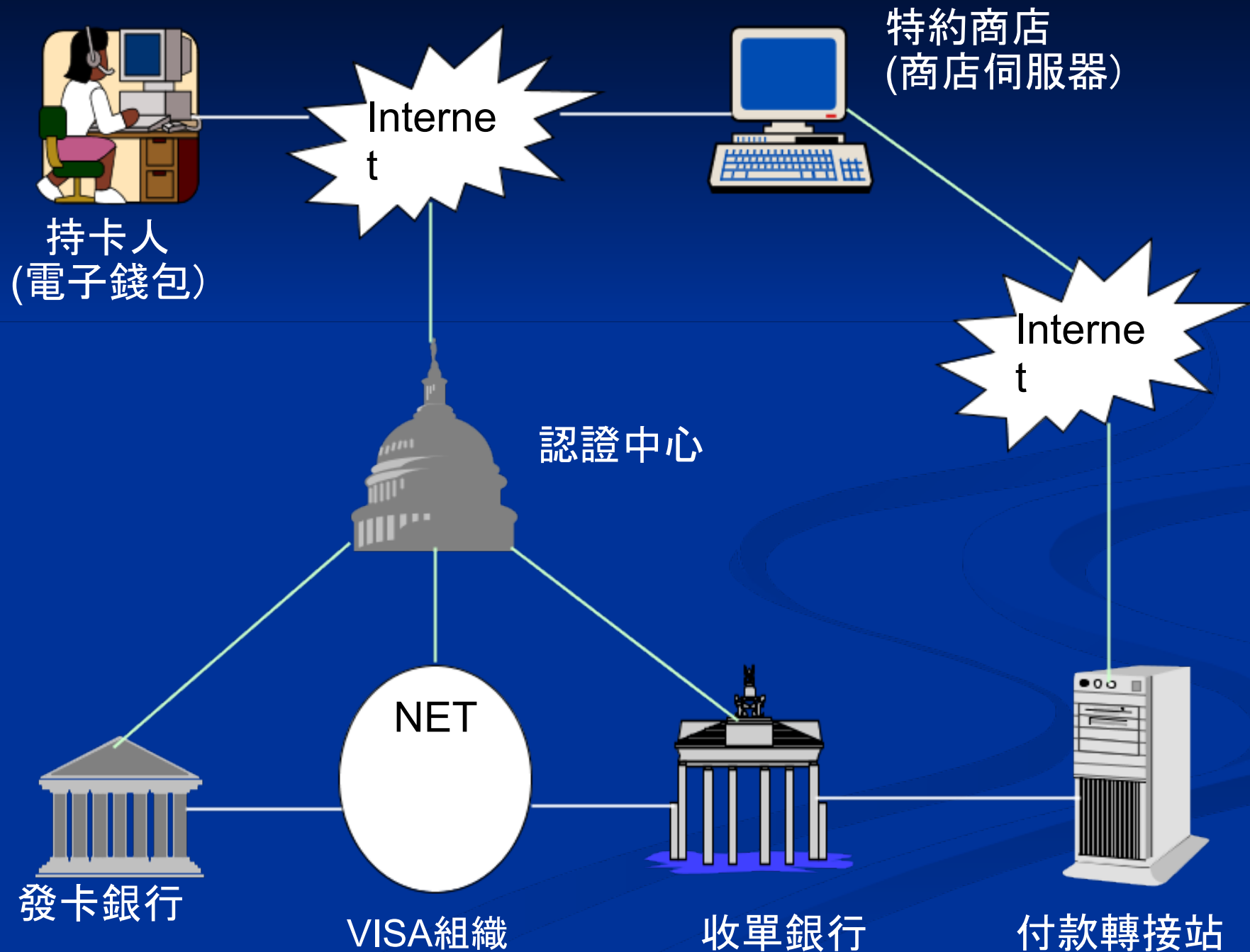
電子證書認證中心核發的電子證書(Certificate)，可以用來確認交易者的身分。認證中心接受持卡人和特約商店的申請，他會向發卡銀行及收單銀行核對申請者的資料是否一致，而對外發出、管理，和取消電子證書並存證

24.2 電子付款系統的架構

- 電子付款系統還必須要有硬軟體設備的支援，這些設備分別是：
 - 1.電子錢包(Electronic Wallet)
 - 2.商店端伺服器(Merchant Server)
 - 3.付款轉接站(Payment Gateway)
 - 4.認證中心(Certification Authority)

必須利用這四者才可構成於Internet上符合SET標準的信用卡授權交易

電子付款系統的架構



24.3 電子交易系統所要考慮的因素

- 24.3.1 交易者的需求
- 24.3.2 環境因素

24.3.1 交易者的需求

● 1. 買方的需求

- (1) 確定交易商店的合法性
- (2) 私人資訊的保密
- (3) 確保購買商品的取得
- (4) 跨國的交易能正確的進行
- (5) 簡單的電子支付程序

● 2. 賣方的需求

- (1) 顧客身分的判定
- (2) 訂單的無法否定性
- (3) 付款保證

24.3.2 環境因素

● 1. 安全因素

安全因素是電子付款系統中最重要因素考量。網路上的傳輸經由網際網路的媒介，會產生許多安全上的問題，而電子付款系統時所必須考慮的安全性因素，歸納出四點：

- (1) 身分辨識
- (2) 防止機密資料遭竊取
- (3) 交易訊息的正確性
- (4) 秘密金鑰的保護

● 2. 隱密性因素

交易雙方的資料是否能有某種程度的隱密，以保障交易者的隱私，同時又必須兼顧交易的安全與合法性

● 3. 技術性因素

交易技術是否易於被交易雙方所接受且信任、交易方式是否易於學習了解，而不會造成交易參與者任何一方對交易系統的抗拒

● 4. 經濟性因素

對交易者雙方而言，電子付款系統是否易於安裝，安裝成本是否能被接受，而不會加重交易雙方的額外負擔

●5. 合法性因素

電子交易是否在現行法律上具有合法地位，且受到完善的法律保障；在發生糾紛時，是否有適合的法律及仲裁機構負責仲裁

●6. 與現行金融體制的整合性因素

電子交易技術是否能與現行金融機構整合，利用既有的金融工具即可使用；或是要使用特殊的交易工具，是否會增加交易雙方的困難度，這些也都是重要的考量

- 7. 效率因素

電子付款系統是否比傳統的付款方式更具效率，及能否縮減使用時間和成本

- 8. 彈性因素

電子交易系統是否能因應商店的擴充、交易人數的增加、網路使用習慣及技術更新，而進行彈性調整

- 9. 可使用因素

可以向與現實世界付款一樣便利，且能廣泛被大眾使用

24.4 電子付款系統的種類

● 1. 代幣式付款系統

- (1) 電子現金
- (2) 電子支票
- (3) 智慧卡

● 2. 信用卡式付款系統

- (1) SET電子安全交易
- (2) SSL電子安全交易
- (3) NON-set電子安全交易

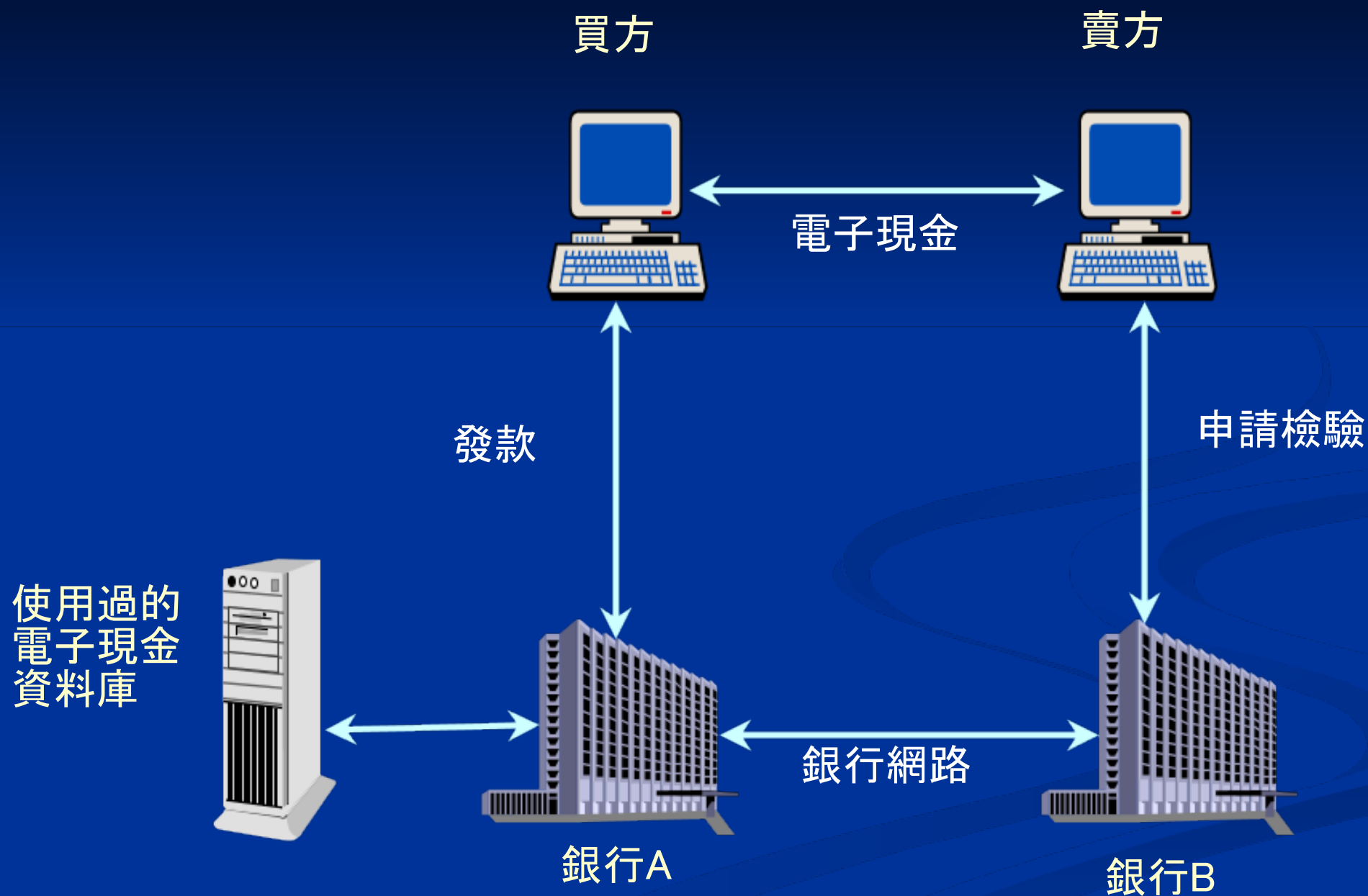
24.5 代幣式付款系統

- 24.5.1 電子現金(E-cash)
- 24.5.2 電子支票
- 24.5.3 智慧卡

24.5.1 電子現金(E-cash)

- 1. 電子現金的實際運作方式
- 電子現金的使用者在網路上的數位銀行中都擁有一個帳戶，此數位銀行多半是由傳統銀行來負責線上的業務，而使用者可以利用個人的帳戶提領電子現金，此筆現金的數額會經由使用者電腦的「數位簽名」技術加密，並產生一隱藏亂數序號，再將資料傳給銀行
- 銀行則會利用此客戶的「數位簽名」解密後，自用戶的帳號中提領此筆金額，再將經認證後的隱藏亂數序號回傳給使用者，使用者就可以在網路上使用此筆金額付款

電子現金的運作方式



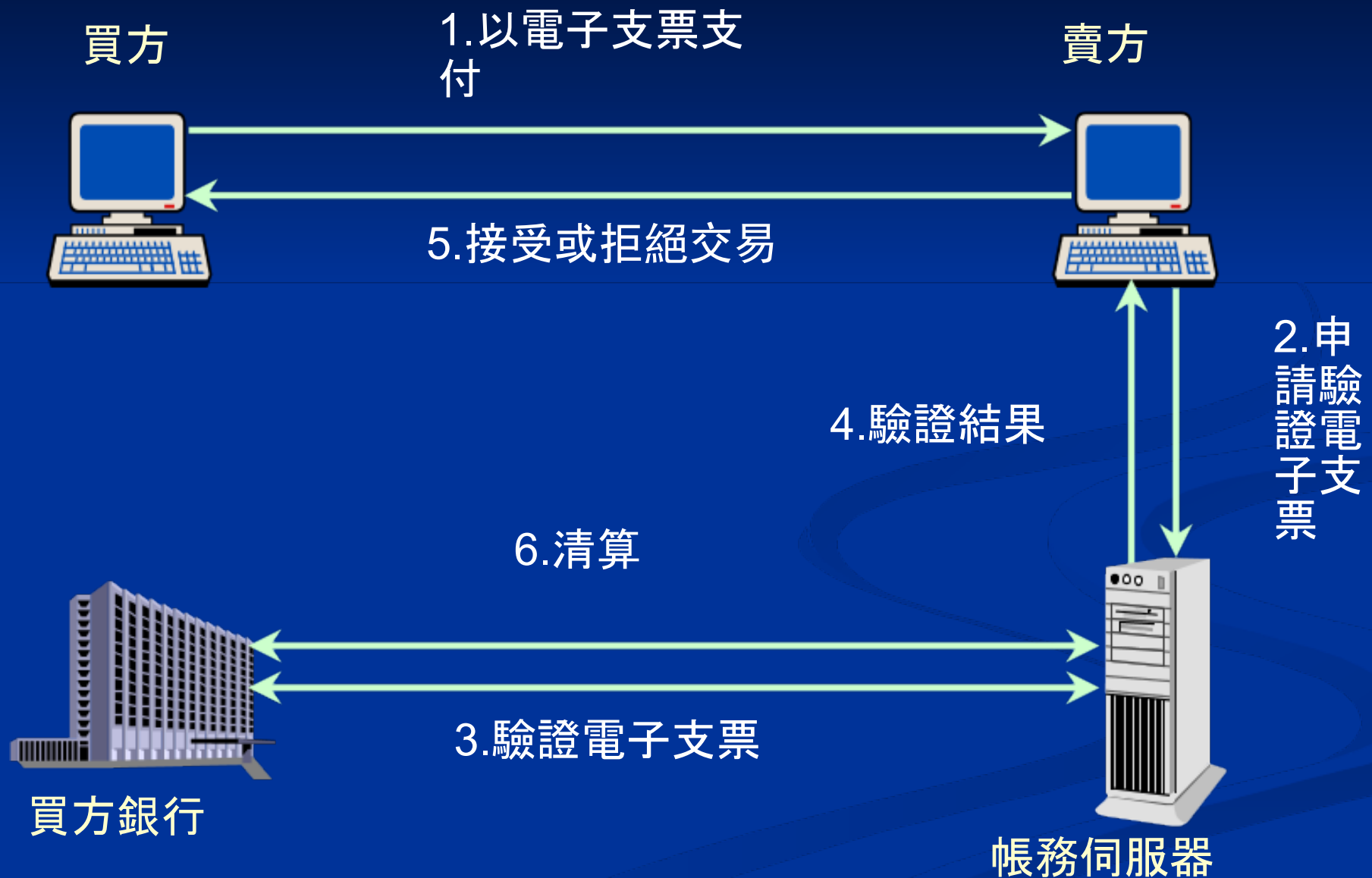
- 2. 電子現金的特性
 - (1) 具有貨幣價值
 - (2) 具備相通性
 - (3) 具備存提轉帳的功能
 - (4) 必須不易被複製及修改

24.5.2 電子支票

- 1. 電子支票的實際運作方式

買方在使用電子支票前，必須先在第三方帳務伺服器上註冊，待註冊後買方就可持具有一定金額的電子支票與賣方進行交易

電子支票運作方式



●2. 電子支票的優點

電子支票具有以下的優點：

- (1) 使用方式如同傳統支票，可減少學習時間及成本
- (2) 電子支票使用傳統的加密方式，執行速度比使用公開金鑰加密法的電子現金快，故適合小額付款
- (3) 財務的風險由帳務伺服器經營者負擔，故提高了電子支票的接受程度

24.5.3 智慧卡

- 1. 智慧卡的形式

- (1) 關係型智慧卡

是由金融機構發行的晶片式卡片，其功能包含了：

- a. 信用卡功能
- b. 借貸卡功能
- c. 多重財務帳號的存取功能
- d. 加值型行銷程式
- e. 資料儲存，包括了持卡者姓名、生日、個人消費索引，及購買記錄
- f. 各家銀行正試圖增加智慧卡所能提供的服務

- (2) 電子錢包

電子錢包是如同口袋大小的智慧卡，卡片上有一個可供計算儲存的微晶片，其內儲存了持卡人可用的總金額，持卡人可用電子錢包來支付各種費用

- 電子錢包的優點是：

- (1) 電子錢包不需像關係型智慧卡要等待信用認證，減少交易時間
- (2) 付款快速，適合小額付款
- (3) 包含了原先智慧卡的功能
- (4) 硬體成本低廉
- (5) 微晶片的技術難以模仿

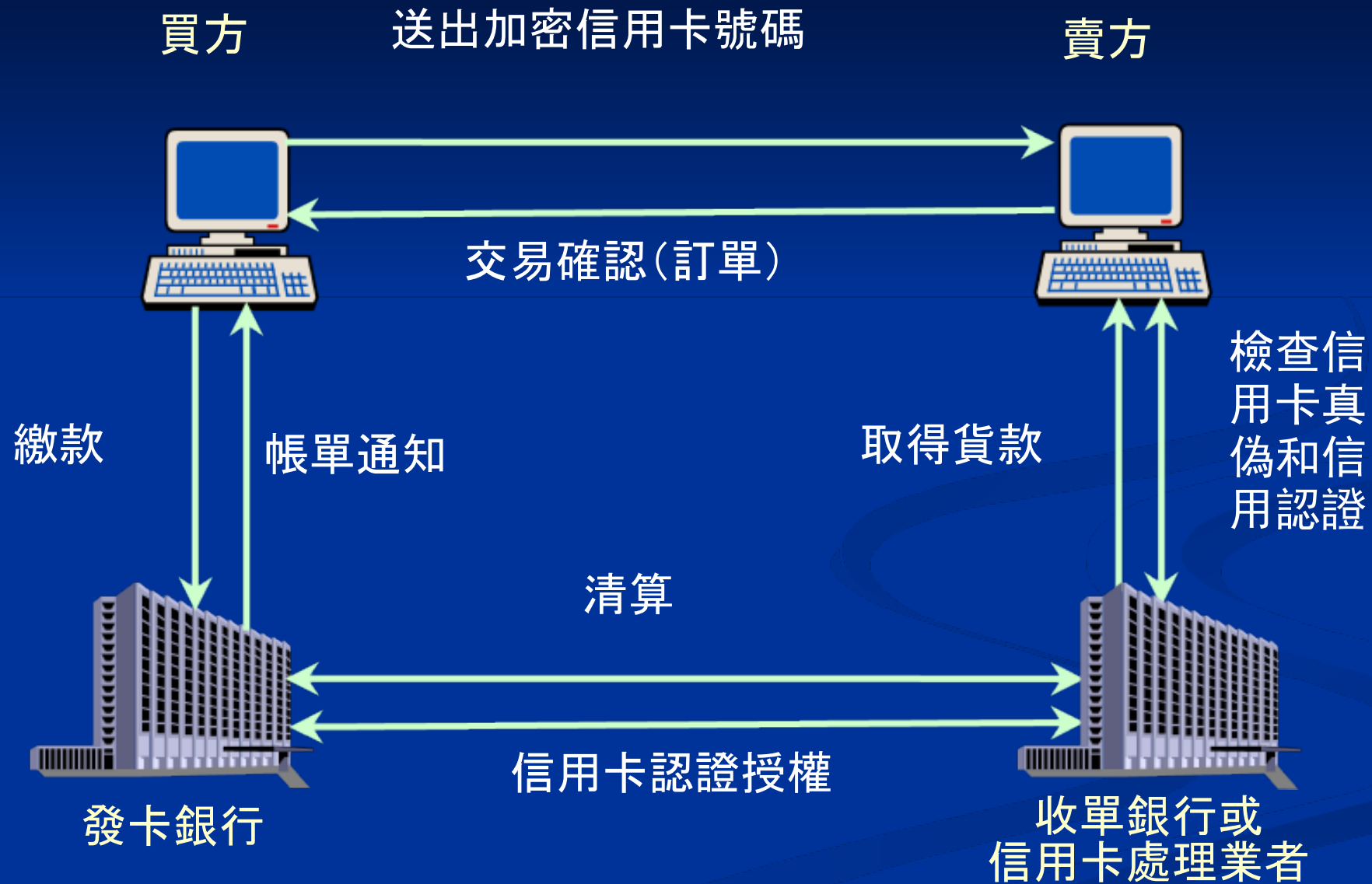
24.6 信用卡電子付款系統

- 24.6.1 信用卡電子付款流程
- 24.6.2 SET安全電子交易機制
- 24.6.3 SSL電子安全交易
- 24.6.4 NON-set電子安全交易

24.6.1 信用卡電子付款流程

- 付款程序 如下：
- (1) 買方向商家傳送其信用卡安全資訊。
- (2) 商家驗證買方，即信用卡持卡人的身分
- (3) 商家依據信用卡號碼及持卡人姓名，向發卡銀行申請提領交易金額
- (4) 發卡銀行依據商家提供的資料，向買方所屬銀行進行授權認證
- (5) 買方所屬銀行再將信用卡資料、交易認證及授權交給商家

信用卡電子付款流程



24.6.2 SET安全電子交易機制

- VISA國際組織及其他公司如Master Card, Microsoft, IBM, NetScape, GTE, SAIC, Terisa和Verisign等，共同制定了安全電子交易(Secure Electronic Transactions; SET)規格
- SET規格融合了從RSA資料安全的公開金鑰(Public Key)編成密碼文件(Cryptography)的使用，以保護任何網際網路上個人和金融資訊的隱密性

- **1. SET的目標**

- (1) 確認在Internet線上交易的每一節點，其訊息的傳遞通路都是安全可行的
- (2) 確保資料輸入的私密性
- (3) 確認訂單及付款資料在傳輸的過程中不致於被更改
- (4) 確認商店及持卡人雙方身分的正確性
- (5) 確認銀行和商店的系統可以處理來自Internet上的交易訊息

● 2. SET的技術

● (1) 數位電子證書(Digital Certificate)

數位電子即是SET的核心，因為它提供了簡易的方法來確保進行電子交易的人們能夠相互信任。這份信賴可以透過如VISA國際組織這樣的共同第三者來建立

● (2) 證書的發給(Certificate Issuance)

- a. 持卡人和發卡銀行
- b. 特約商店和收單銀行

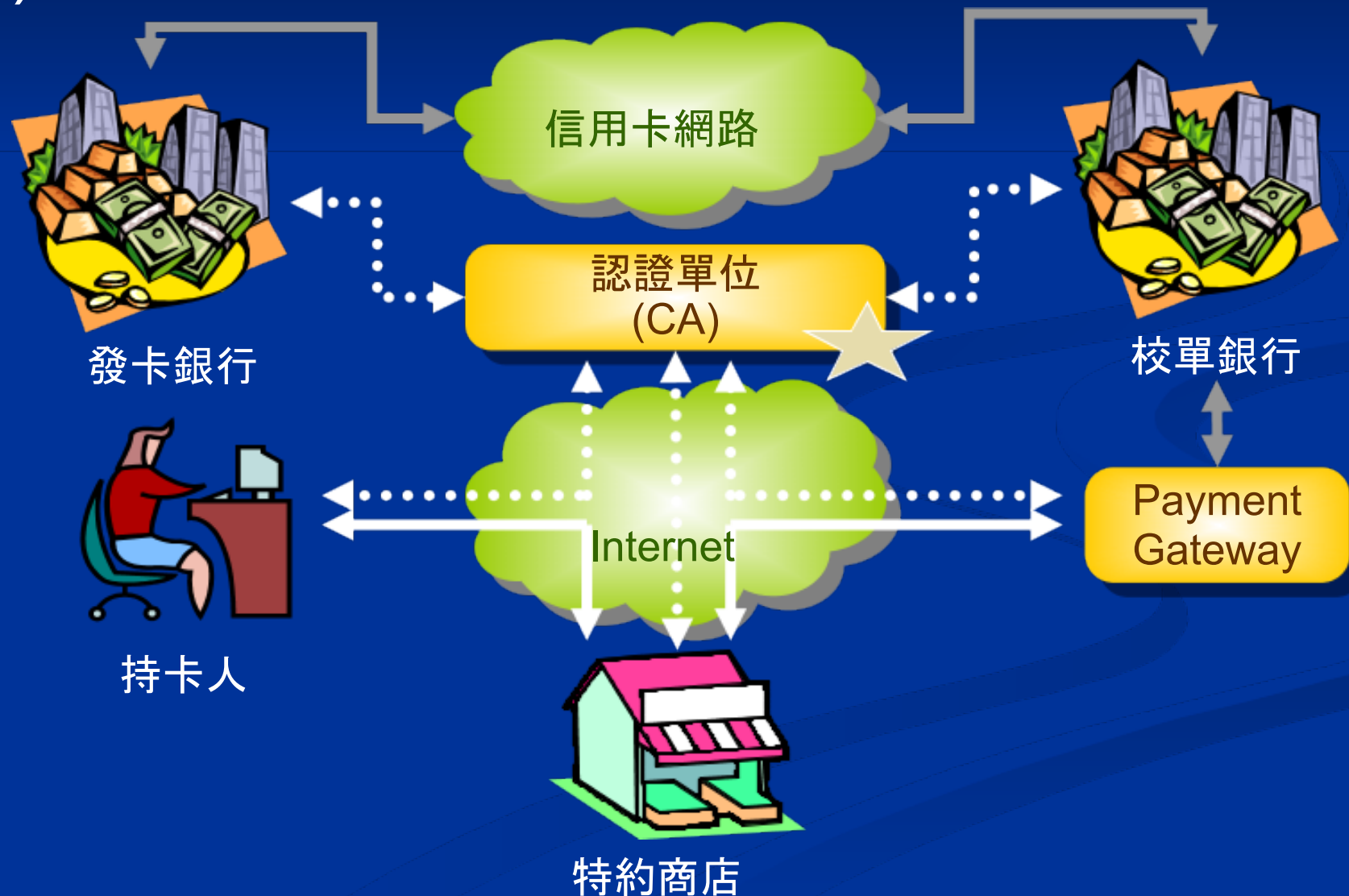
- (3) 開放性金鑰加密(Public Key Cryptography)

一把公開金鑰(Public Key)提供不同種類的目錄給大眾；同時，您也會有一把私有金鑰(Private Key)以確保私人的資訊不會被他人得知。如果一起運用這兩把鑰匙，就可將資料加密及解密，且任何資料，只要被其中一把金鑰加密，就只有另一把金鑰才能將其解密

- (4) 電子數位簽字(Digital Signatures)

● 3. SET的訂購流程

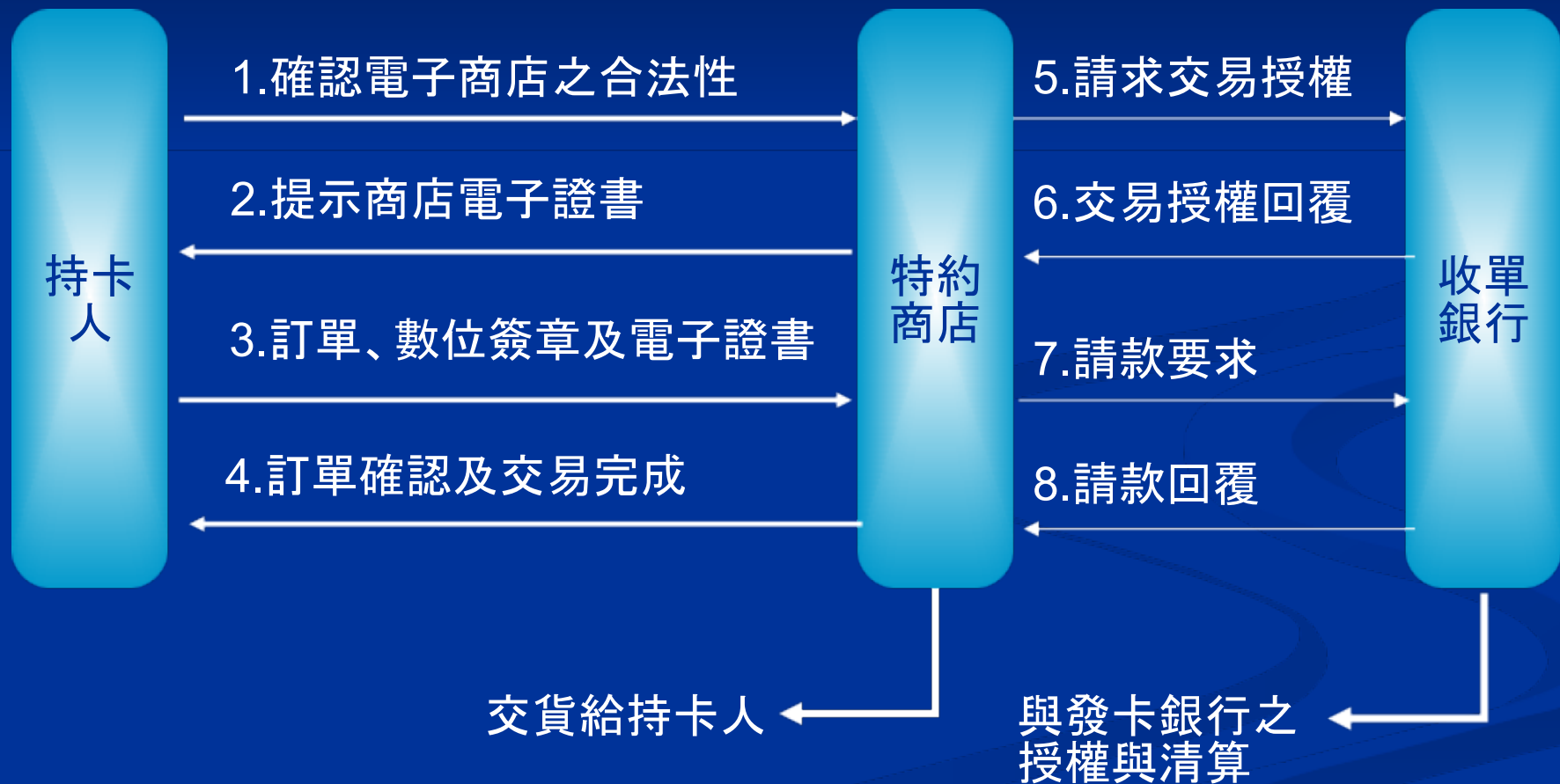
- (1) 消費者申請電子證書
- (2) 購買商品與交易授權



● 4.整個SET的交易流程

- a.持卡人向特約商店要求確認其電子商店的合法性
- b.特約商店向持卡人提示商店的電子證書持卡人下
訂單、使用數位簽章，以及出示電子證 書
- c.特約商店向收單銀行請求交易授權
- d.收單銀行回覆交易授權給特約商店
- e.特約商店與持卡人確認訂單，並完成交易，交貨
給持卡人
- f.特約商店向收單銀行提出請款要求
- g.收單銀行回覆特約商店的請款要求，收單銀行並
接著與發卡銀行確認之間的授權與清算

SET交易流程



- **5.SET的優缺點分析**

- **優點：**

- (1).安全可靠
- (2).成本節省

- **缺點：**

- (1).麻煩
- (2).額外負擔

24.6.3 SSL電子安全交易

- SSL (Secure Socket Layer) 是 Netscape 首先發表的，其可算是目前最普及的線上交易技術，主要是 SSL 加密的協力廠商眾多，且交易流程簡單，所以一般網站會選擇 SSL 來處理線上交易

使用SSL付款機制的網站



- SSL的優缺點分析：

- 優點：

- (1) 建置簡單
- (2).付款容易
- (3).可降低金流成本

- 缺點：

- (1).消費者的安全有漏洞
- (2).交易不確定

24.6.4 NON-set電子安全交易

- NON-set(安全認證作業)指的是不使用SET之安全電子交易協定，即使用SET及SSL以外之電子化銀行各項服務，其交易訊息格式及處理流程係由銀行依業務需求自行規劃設計，制定之交易訊息標準適用於付款訊息的傳送
- 與set同樣提供電子數位簽章功能，可確保交易資料之不可否認性及完整性，安全性高

SSL、SET、NON-SET安全機制比較

	SSL	SET	NON-set
便利性	免申請憑證，較便利。	客戶必須申請憑證，安裝電子錢包及上網下載憑證（私鑰和憑證存於硬碟內，若要使用另一部電腦進行交易時，須將原作業電腦的私鑰及憑證匯出至磁片，再匯入另一部電腦）。	客戶必須申請憑證，安裝客戶端安控軟體及上網下載憑證（私鑰及憑證均存於磁片中，只要攜帶磁片，即可到各電腦進行交易）。
安全性	可作為低風險交易之安控機制。	提供數位簽章，安全性高。	提供數位簽章，安全性高。
適用服務項目	低風險性轉帳	多用於轉帳、繳稅、繳費或其他需要確認身分之交易。	多用於轉帳、繳稅、繳費、整批傳檔轉帳、政府採購電子押標金或其他需要確認身分之交易。

24.7 結論

- 電子商務的熱度不斷擴張，未來的網路社會願景更是令人期待，然而在發展初期的現階段中，仍有不少人對電子商務裹足不前，可見仍有許多的困難仍需要被突破，其中包括消費者的習慣等，因此若消費者與廠商間能接受網路的付款方式，相信有一天將能被這更具多元化的線上工具所取代