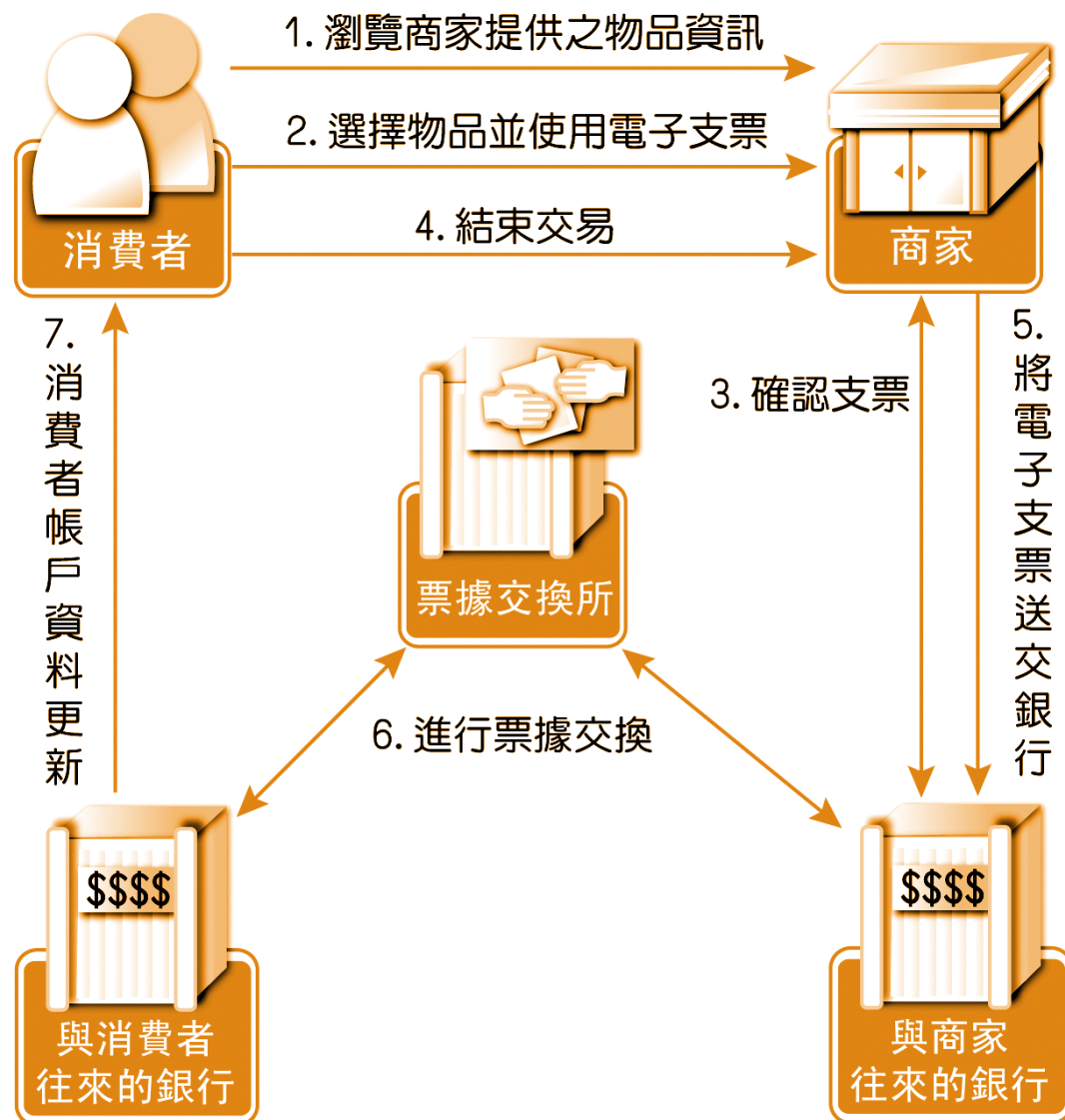


16.7 電子支票

- 電子支票可以看成是電子化的紙本支票，在紙本支票的使用上，使用者必須在支票上簽名作背書之後，這張支票才算有效。電子支票，需由使用者用數位簽章來作背書。

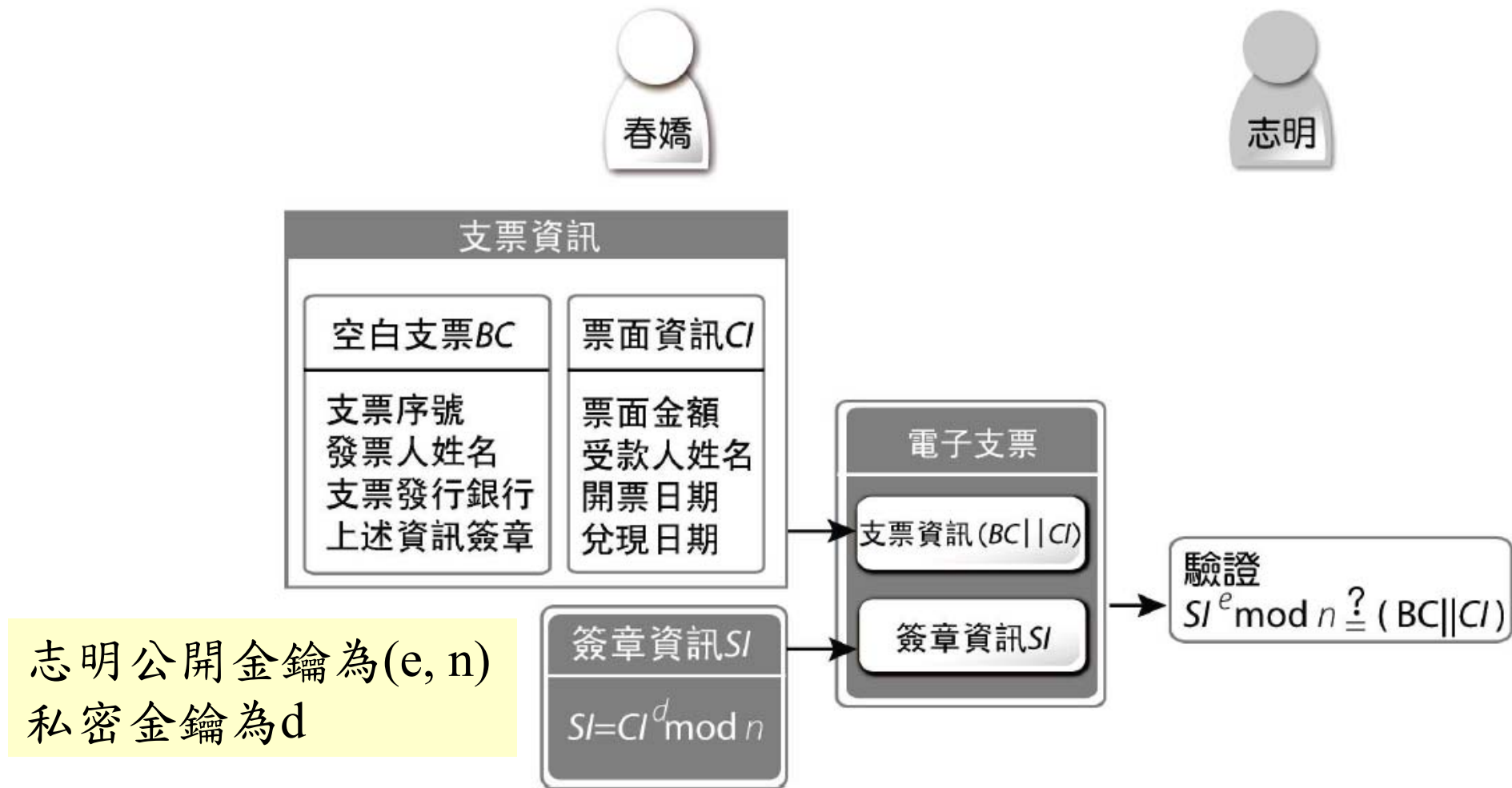
電子支票付款系統



電子支票系統

- 一、消費者消費交易階段
 - 步驟1：瀏覽選購
 - 步驟2：交易
 - 步驟3：查核
 - 步驟4：完成現階段交易
- 二、商家存入支票階段
 - 步驟5：存入支票
- 三、銀行票據交換階段
 - 步驟6：票據交換
 - 步驟7：更新資料

使用RSA所建構的電子支票機制

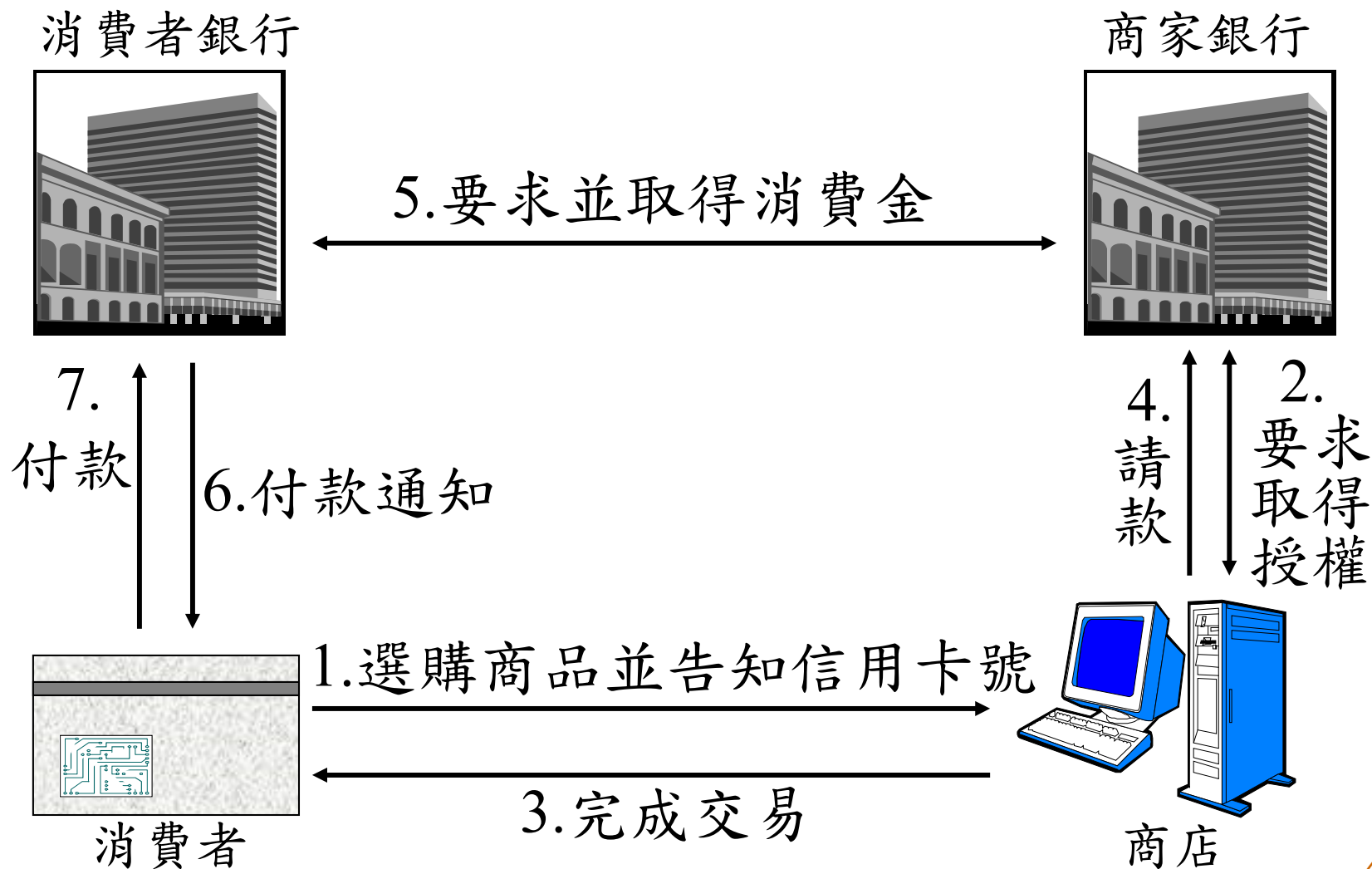


16.8 線上信用卡付款

電子信用卡之安全策略

- 考量電子信用卡系統之安全，必須存在一能夠確認商店所屬銀行、商店及消費者之機制，以避免詐欺行為產生。例如在傳送交易資訊時，配合電子簽章和電子證書的使用，來鑑別交易資料的真偽。
- 消費者的私密金匙亦必須妥善保護，以防止遭到別人的竊取、破解，進而冒用身分進行消費。
- 對於信用卡號碼、有效日期、持卡人姓名、消費金額、以及其他所有相關資訊，都必須經過加密處理，以確保不在傳輸過程中外洩。此外，必須有機構來負責處理消費者、商店、與銀行之紛爭。

電子信用卡交易系統



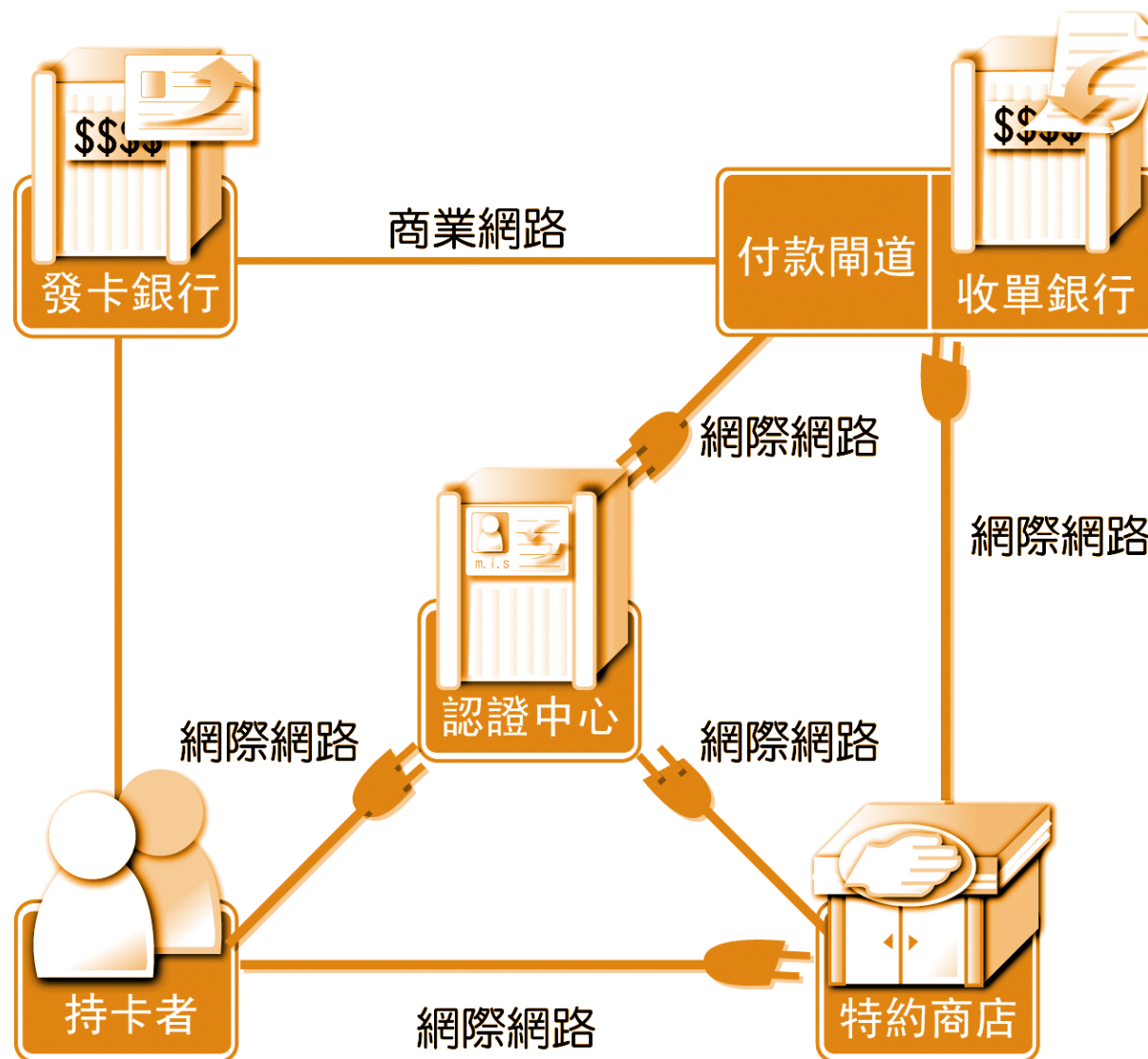
安全的電子交易(SET)

- SET全名Secure Electronic Transcation
- 用來保護消費者在開放網路(如Internet)持卡
- 付款交易安全的標準
- 1996年由VISA、MasterCard、IBM、Microsoft、
- Netscape、GTE、VeriSign、SAIC、Terisa等公司
聯合制訂
- 運用RSA資料安全的公開鑰匙加密技術

SET的安全需求

- 身分鑑別 (Authentication)
- 交易資料的機密性 (Confidentiality)
- 交易資料的完整性 (Integrity)
- 不可否認性 (Non-repudiation)
- 隱私性 (Privacy)

SET安全付款系統



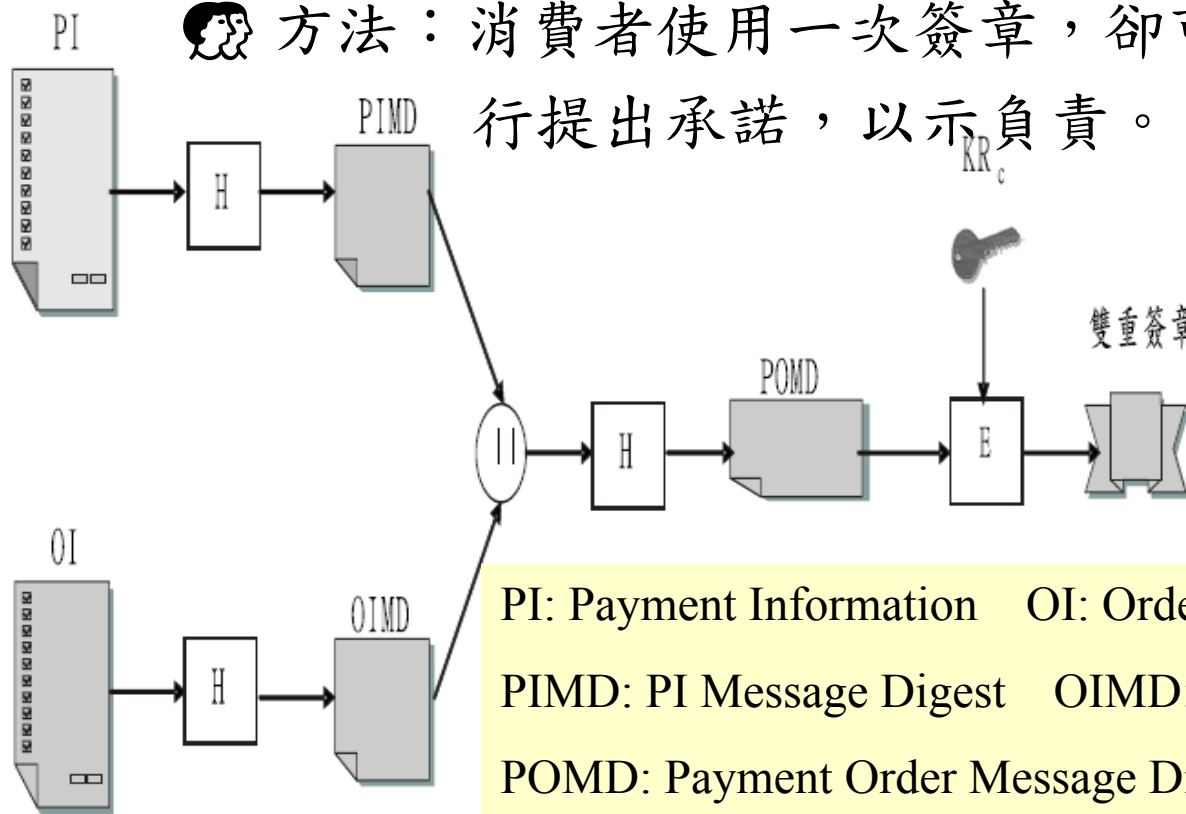
SET的背景

特 點	方 法
付款資料的隱密性 (Confidentiality)	訊息加密(Encryption)及 雙重簽章(Dual Signature)
資料完整性(Integrity)	數位簽章(Digital Signature)
持卡人帳戶之認證 (Cardholder Acc. Authen.)	數位簽章及持卡人證書 (Certificate)
特約商店認證 (Merchant Authentication)	數位簽章及特約商店證書
互通性 (Interoperability)	特殊協定與訊息格式

雙重簽章(Dual Signature)

目的：將訊息分為付款資訊與訂購資訊，提供消費者隱私權的保護

方法：消費者使用一次簽章，卻可以同時對商店與銀行提出承諾，以示負責。



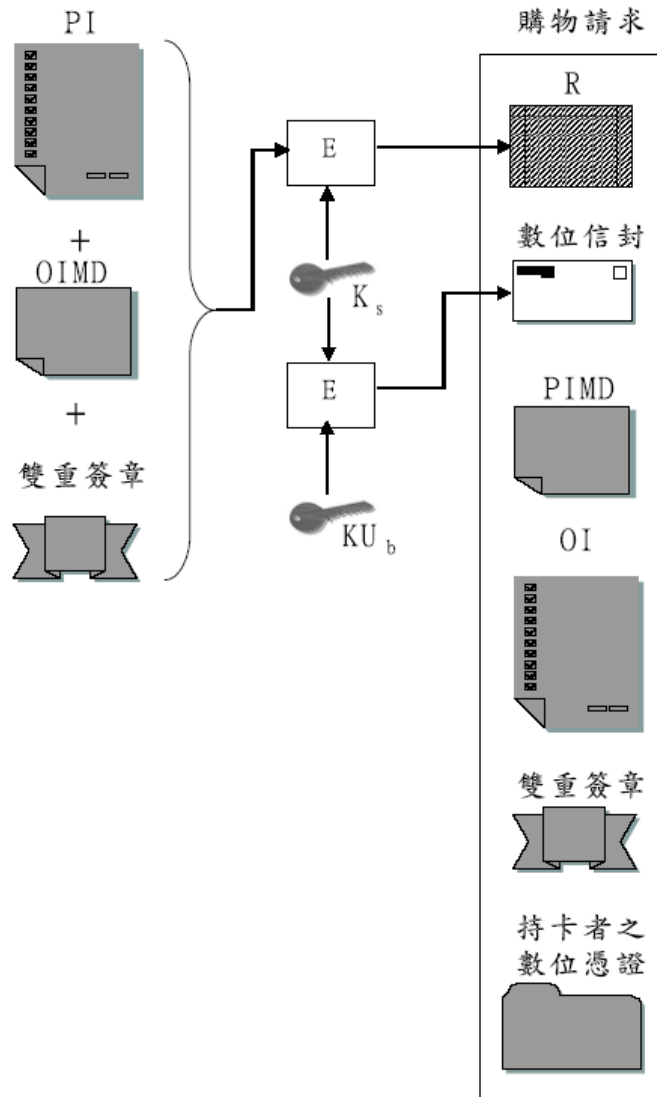
PI: Payment Information OI: Order Information

PIMD: PI Message Digest OIMD: OI Message Digest

POMD: Payment Order Message Digest KR_c : 持卡者的私密金鑰

H: 一公開之赫序函數

雙重簽章：顧客傳送購買請求



PI: Payment Information

OI: Order Information

PIMD: PI Message Digest

OIMD: OI Message Digest

POMD: Payment Order Message Digest

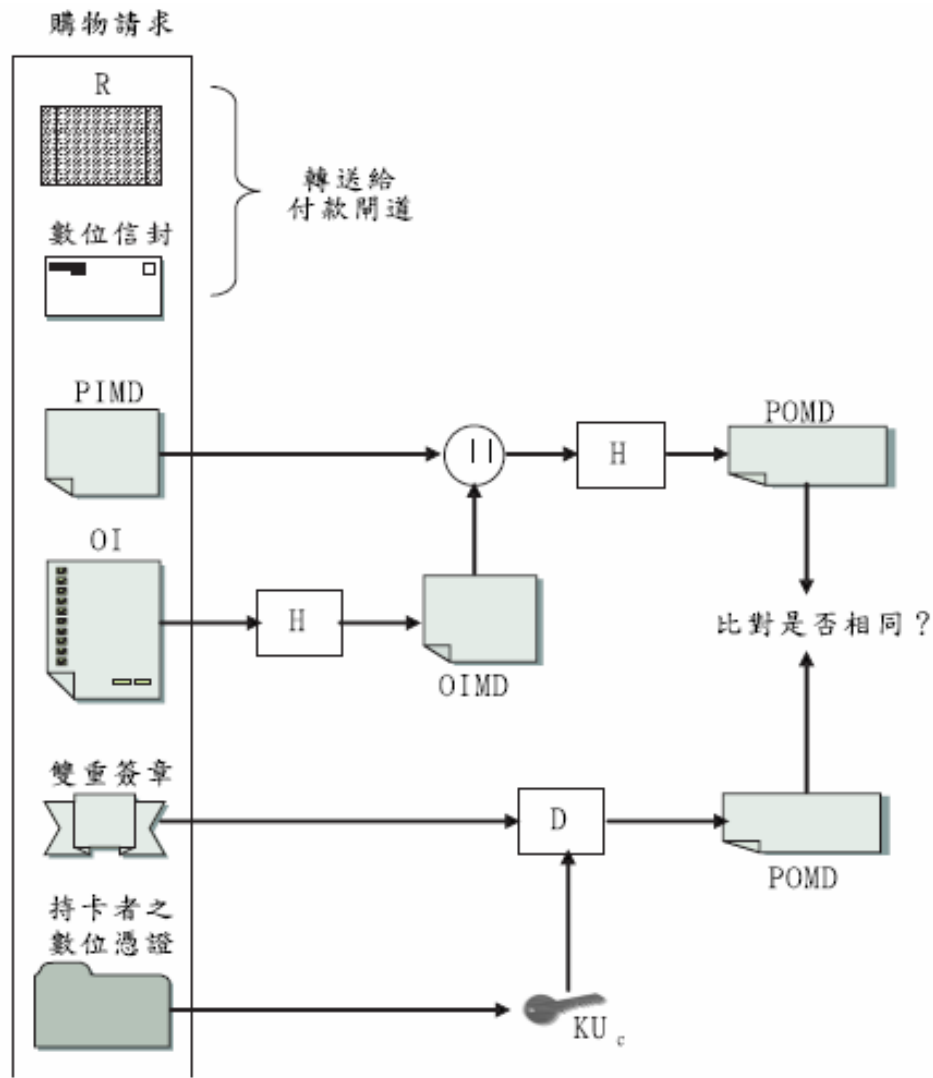
R: 密文

K_s: 會談金鑰

KU_b: 銀行的公開金鑰

H: 一公開之赫序函數

雙重簽章：商店驗證顧客的購買請求



PI: Payment Information

OI: Order Information

PIMD: PI Message Digest

OIMD: OI Message Digest

POMD: Payment Order Message Digest

R: 密文

K_s : 會談金鑰

KU_c : 持卡者的公開金鑰

H: 一公開之赫序函數

SET的實施情況

目前實施SET的商店，還是少之又少，主要原因就是SET的太複雜，不易被一般大眾所接受，是否能夠再簡化SET的流程，或是有更簡單的系統出現？

16.9 比特幣

- 比特幣(Bitcoin)是一種目前被使用最廣泛的電子貨幣之一，在2009年由化名的開發者中本聰(Satoshi Nakamoto)以開源軟體(Open Source Software)形式推出。
- 比特幣是利用密碼技術來控制貨幣的生產和轉移，也被稱之為加密電子貨幣(Cryptocurrency)，而比特幣是經由一種稱為「挖礦」(Mining)的過程產生，沒有發行單位，它透過P2P網路的參與者來對比特幣進行確認，因此政府或任何人都無法操控比特幣的貨幣總量，也不會有通貨膨脹的問題產生。

比特幣的價值

- 2010年在比特幣論壇上開始了第一筆交易，那時一位比特幣的擁有者用了一萬個比特幣買了一個披薩。
- 到了2013年底在日本東京的市場交易中，比特幣對美元匯率已經飆升至一個比特幣對九百美元。
- 若一個披薩價值以10美元來計算，短短四年間比特幣已經漲了近九十萬倍。

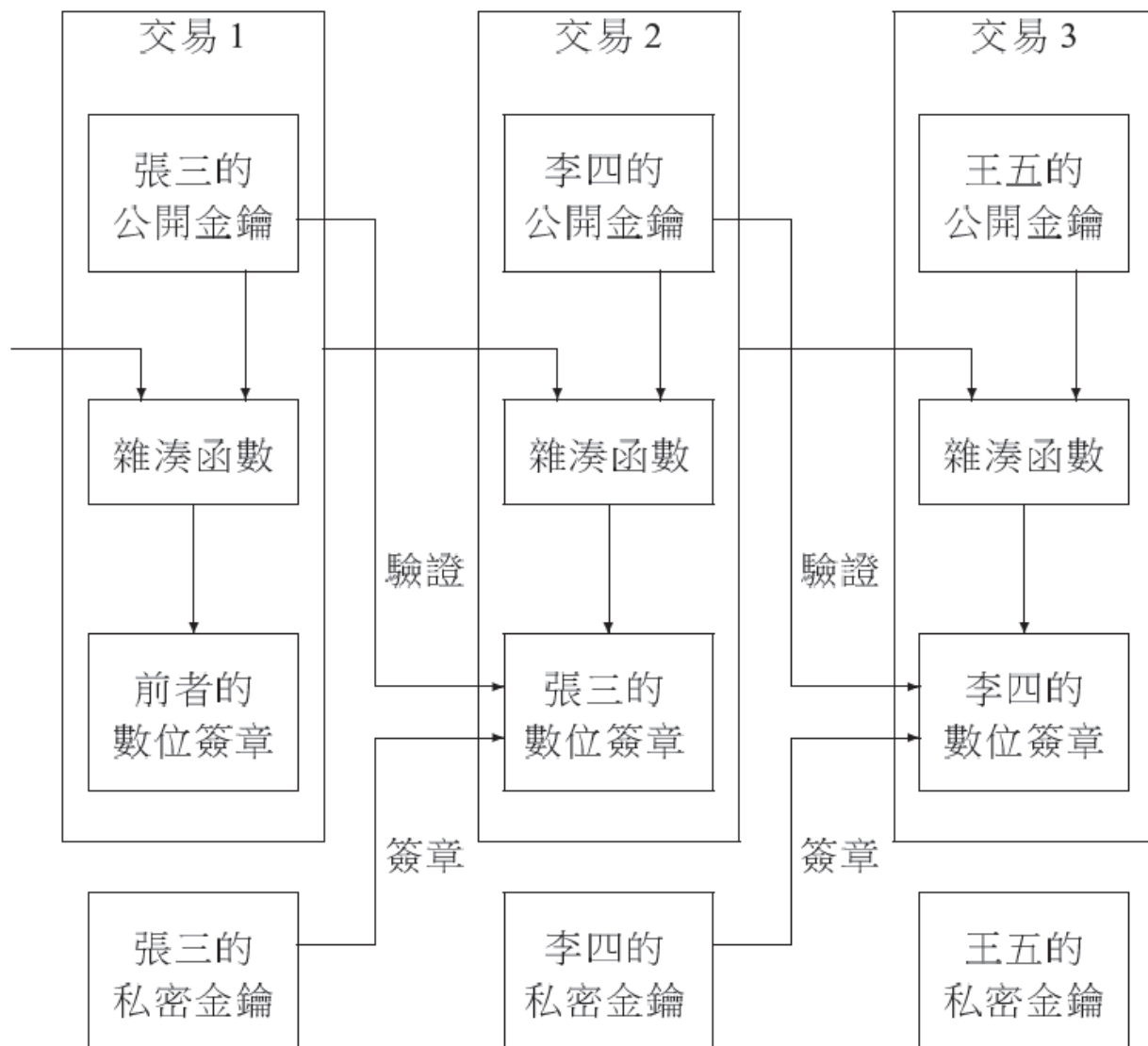
比特幣的地址及錢包

- 比特幣是在P2P對等網路上被運行，貨幣的產生、管理和流通等環節務必公平、安全、可靠，因此比特幣利用了許多密碼技術來確保比特幣不會被偽造及重複消費。
- 在比特幣的運行機制中，每一個參與者都會有一個「比特幣地址」，比特幣地址就像E-mail地址或銀行帳號一樣，可以利用這個地址來接收他人的比特幣，也可以從這個地址將比特幣移轉給他人。

比特幣錢包

- 「比特幣錢包」可以用來產生比特幣地址，比特幣的地址可以視為是「非對稱式密碼系統」中的公開金鑰(Public Key)，產生的過程中會有一把跟比特幣地址相對應的私密金鑰(Private Key)被產生出來。
- 私密金鑰可用來做簽章，證明你是這個帳戶的擁有者，就如同銀行帳號的提款密碼，因此比特幣的地址可以被公開，只要對應的私密金鑰不被知道，就可確保存放在比特幣地址內的比特幣不會被盜領。
- 一般比特幣地址的長度大多是由34個位數的字母或數字所構成，且總是由1或者3開頭，例如
"1DwunA9otZZQyhkVvkLJ8DV1tuSwMF7r3v"。

比特幣的交易過程



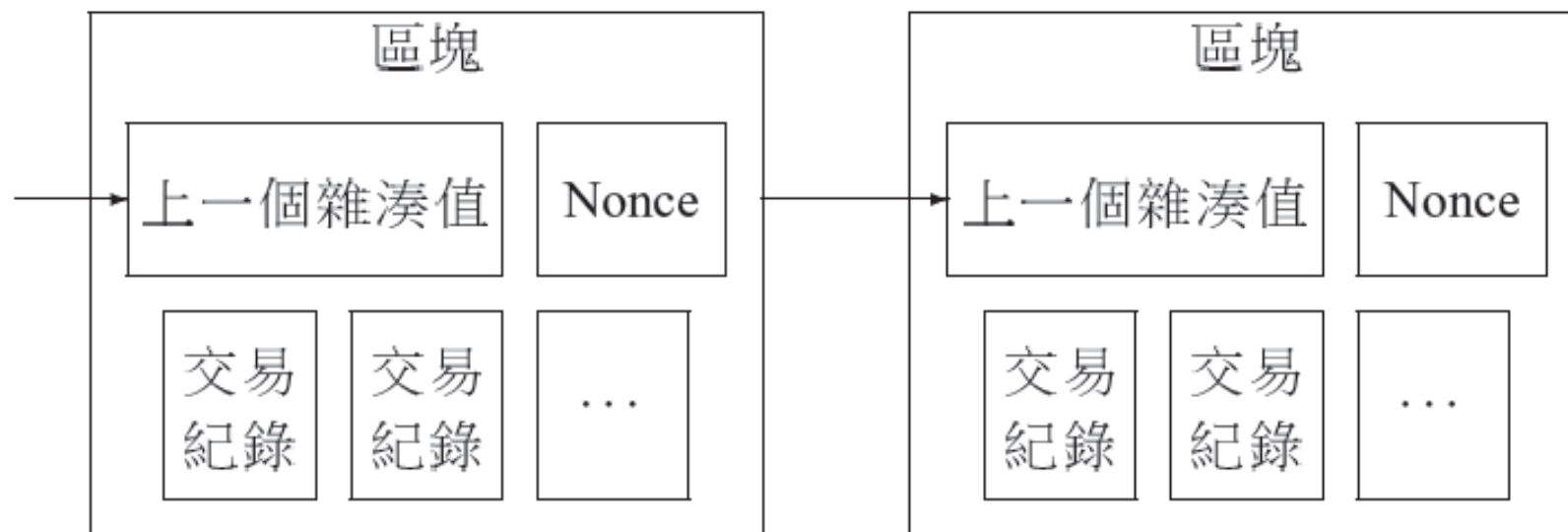
比特幣的交易過程

區塊鏈(Chain of Blocks)

- 所有經確認的交易紀錄都會依序放在區塊上，且每個區塊的產生都需要上一個區塊的雜湊值，它是一個共享的公開交易紀錄，在P2P網路上只有一套區塊鏈。
- 因此，若付款者重複花費了比特幣，這樣的交易內容廣播出去，網路上的參與者會檢視區塊鏈內的交易紀錄，很容易發現問題所在。

比特幣的交易過程

區塊鏈(Chain of Blocks)



比特幣的挖礦程序

1. 參與的挖礦者必須隨時在網路上監聽，把最新區塊的雜湊值和最新收到的交易確認合併在一起，準備創造一個新的雜湊值。
2. 找出一個特定的Nonce值，這個Nonce值必須讓計算出來的雜湊值其開頭是連續n個0，n的大小也決定了挖礦的難度。

以目前的技術來說，並沒有有效的方法來找出符合規定的Nonce值，參與者必須用**暴力法**去嘗試每一個Nonce值，然後比對其結果，若成功找出符合n個0開頭規則的Nonce值，就成功創造了一個新區塊。

比特幣的挖礦程序

3. 新區塊產生後，必須立刻將這個區塊廣播出去，當獲得足夠多的確認回應後，則挖礦成功。

在比特幣的規範中，每個成功創造一個新區塊的人就可以獲得**50BIT**。認可後的區塊會被加入區塊鏈中，這個區塊的雜湊值也會被納入下一個準備創造的區塊中。

4. 一旦發現有新的區塊被發布，挖礦者就必須重置計算，將最新的區塊的雜湊值與最新收到的交易合併，準備去創造下一個新區塊。

比特幣的特性

- 比特幣的總量固定

比特幣的數量不會無限制成長，而是會趨近一個數值，所以不會有通膨的問題。

- 比特幣產率固定

在最初的四年預計要有10,500,000個比特幣被製造出來，然後每四年產值減半，第4到第8年中會有5,250,000比特幣被製造，第8到第12年中會有2,625,000個比特幣被製造。以此類推，最終比特幣的數額會趨近於2,100萬個。

比特幣的特性

- 交易無法取消

在比特幣的交易中，交易一旦送出並得到足夠的確認後，交易就算完成了，此交易內容也會被蒐集準備去產生下一個新區塊。因此，一定交易完成，並得到足夠的確認，交易就無法取消。

- 不具有匿名性

所有交易紀錄細節都是公開的，且會永久留在網際網路上。任何人都可以查看每個帳號內的交易內容及金額，雖然我們不見得知道某個帳戶是誰所擁有的，但追本溯源還是有機會可以知道這個帳號的擁有者是誰。

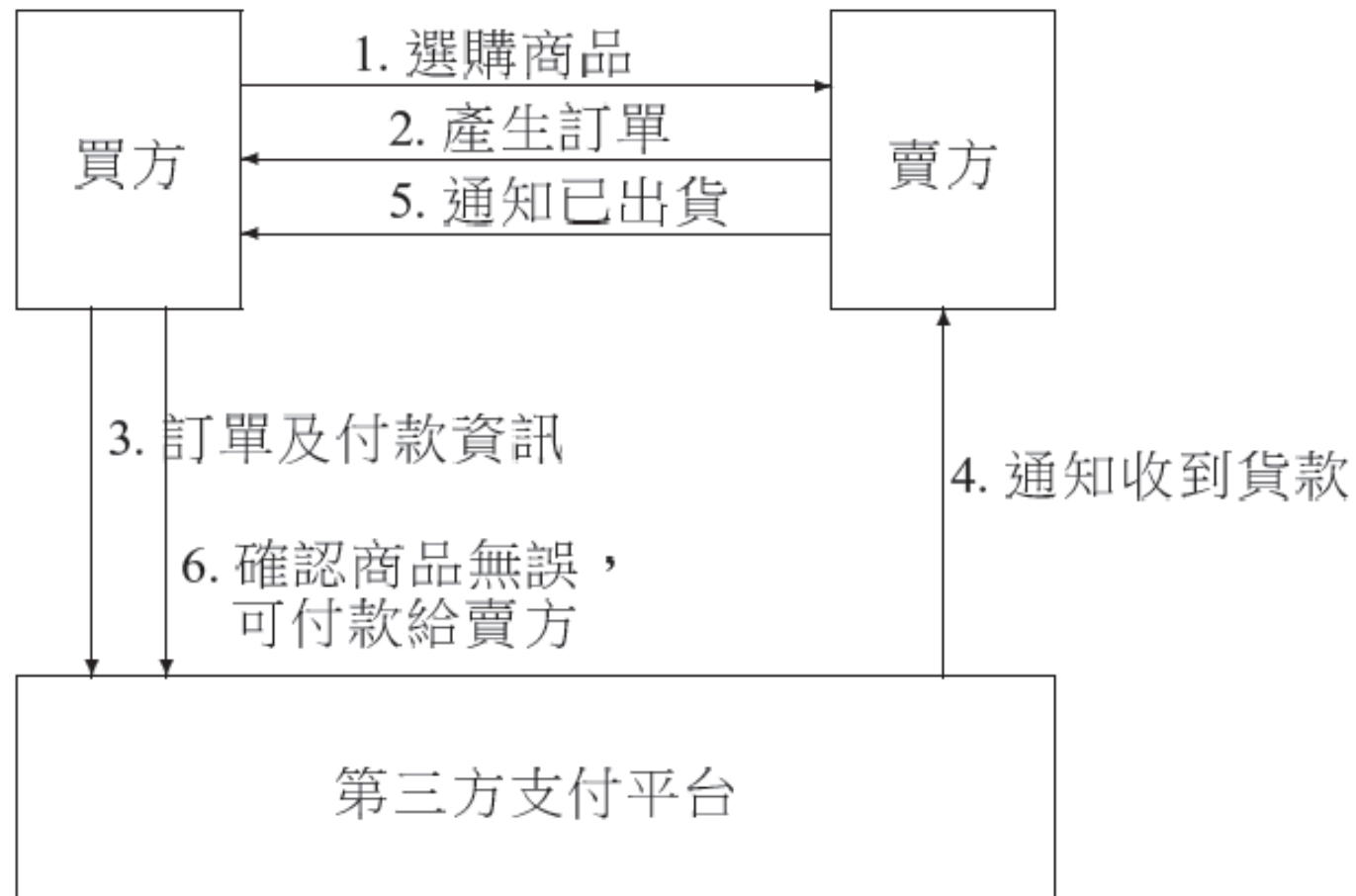
16.10 第三方支付服務

- 第三方支付服務是指在網路上為交易雙方建立一個中立的支付平台，這個平台不涉入任何有關電子商務的行為，僅提供個人或企業網路交易的支付結算。

16.10 第三方支付的交易流程

1. 買方瀏覽賣方網頁，選購商品。
2. 賣家依據買方選購的商品，產生訂單。
3. 買方選擇使用第三方支付服務進行貨款支付，與第三方支付平台確認訂單內容後，將付款資訊傳送給第三方支付平台。
4. 第三方支付平台收到代收款項後，會通知賣方該訂單貨款收訖。
5. 賣方收到通知後，即依買方約定出貨，並通知買方商品已寄出。
6. 買方收到商品並確認無誤後，通知第三方支付業者付款給賣方。

第三方支付的交易流程



第三方支付的優缺點

優點

1. 可避免網路詐欺
2. 提供消費者多元且便利的付款方式
3. 商家免去安裝各種付款認證機制的麻煩
4. 降低開發及維護成本

缺點

1. 費者的資金可能遭不肖第三方支付業者挪用或惡意倒閉，衍生索償的問題
2. 成為犯罪洗錢的溫床

16.11 Google 電子錢包

- Google 電子錢包 (Google Wallet) 是一項使用手機以 NFC 近場通訊 (Near Field Communication, NFC) 技術進行的電子支付系統。
- Google 電子錢包的行動載具須內建安全晶片，且安全元件中儲存了虛擬信用卡的資訊，其他使用者登錄的銀行帳戶、現金卡或信用卡資訊則是經加密後儲存在 Google 的伺服器中，無法透過行動載具直接去存取這些敏感資訊。
- 當使用者拿 Google 電子錢包到實體商店消費時，商家只能讀取在行動裝置內的虛擬帳號資料，無法得知消費者真正的帳戶資料。
- 消費者的消費明細則是被紀錄在 Google 的線上服務中心中，消費者可透過使用者鑑別的技術來存取個人的消費明細。

16.12 電子競標

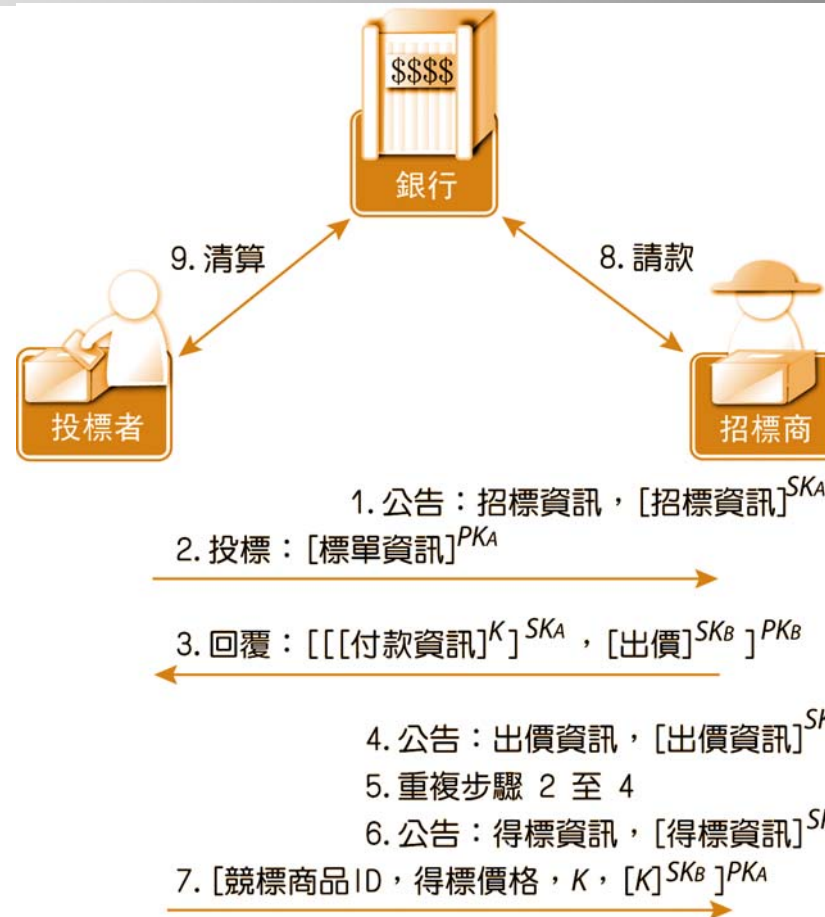
電子競標系統可分為以下二種類型：

- 公開標單 (Public Bid)
- 密封標單 (Sealed Bid)

公開標單

- 每次投標的投標價需一直向上攀升，直到沒有投標者願意出更佳的投標價為止，最後出價最高者即為此次競標的得標者，此種拍賣方式其一特色便是投標者可進行多次喊價，所以又稱為多次投標型的競標方式(Multi-Bidding Auction)。

公開標單的電子競標系統



標單資訊= $[\text{競標商品ID, 公開金鑰}PK_B, \text{核發金鑰之機構, } [\text{付款資訊}]^K, \text{出價資訊, } [\text{出價資訊}]^{SK_B}]$

招標資訊包含拍賣商品的描述、拍賣商品的ID、及列出該招標商所認可的公正單位。

公開標單電子競標機制

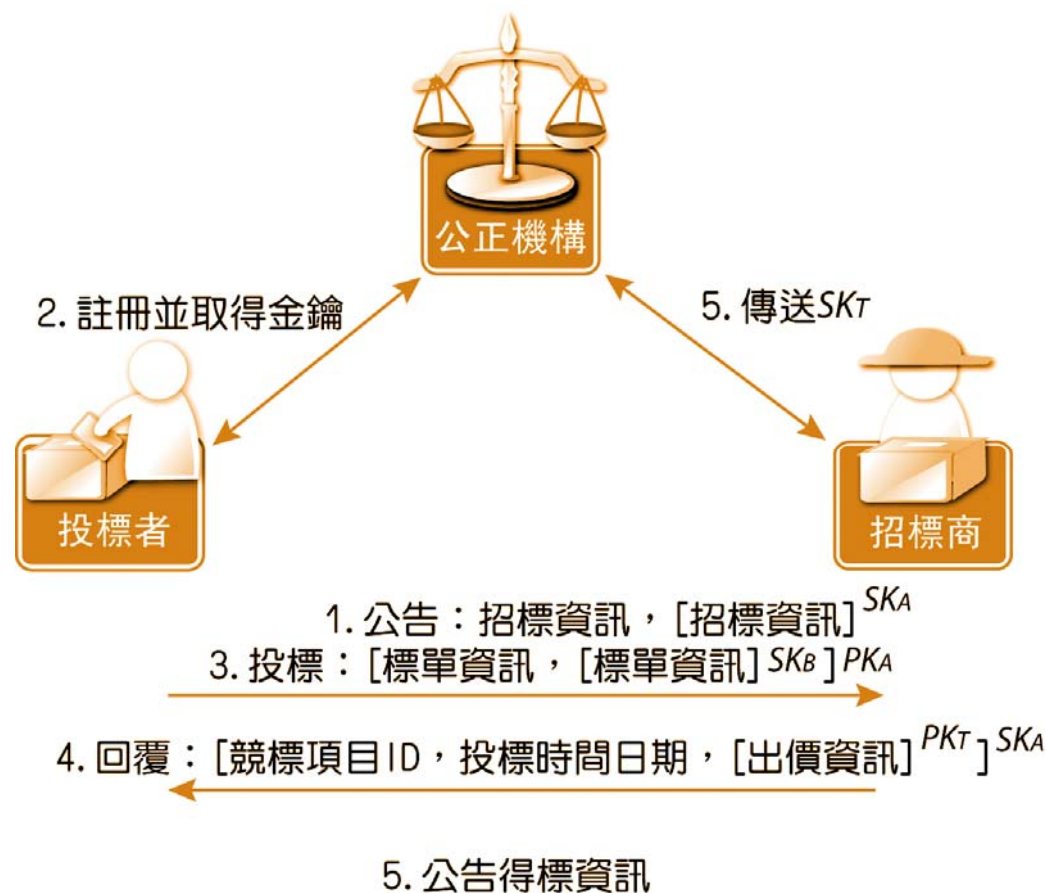
一個完善的公開標單電子競標機制有下列的基本需求：

- 拍賣過程中投標者的身分具有匿名性。
- 拍賣結束後參與投標者及得標者其身分均具有匿名性。
- 所有人均可驗證標單的來源的正確性及標單內容的完整性。
- 在傳輸過程中，標單內容無法被竄改。
- 沒有人可以假冒合法投標者身分進行投標。
- 投標後，投標者無法否認曾投出此標單。
- 投標者對所投過的標單都握有證明，得標者亦可證明自己得標。
- 得標後招標商可輕易向得標者索款。
- 招標商無法向未得標者索款。

密封標單

- 投標者送出一密封標單，待投標時間終止招標商進行開標作業，以投標價值較佳者為得標者，因為此種競標方式投標者只進行單次投標，所以又稱單次投標方式(Single-Bidding Auction)。

密封標單的電子競標系統



標單資訊=[競標項目ID、公開金鑰PK_B、核發金鑰之機構、投標時間日期、[出價資訊]^{PK_T}]。

招標資訊包括競標項目、競標項目的ID、開標時間日期、專屬此競標項目之公開金鑰PK_T、及參與之公正單位。

密封標單電子競標機制

密封標單的競標機制需具備有下列需求

- 拍賣過程中投標者的身分具有匿名性。
- 開標後參與投標者及得標者其身分均具有匿名性。
- 開標後所有人均可驗證標單來源的正確性及標單內容的完整性。
- 在傳輸過程中，標單內容無法被竄改。
- 沒有人可以假冒合法投標者身分進行投標。
- 投標後，投標者無法否認曾投出此標單。
- 投標者對所投過的標單都握有證明，得標者亦可證明自己得標。
- 標單必須在投標截止時間前送達，過期標單則視為無效標單。
- 開標前沒有人能得知標單內容。
- 遇到有相同標價的情況時，可以有一個公平且有效率的解決方案。