電子商務安全
Secure Electronic Commerce

交易安全、系統安全、IC卡安全、電子付款

(Transaction Security, System Security, IC Card Security, Electronic Commerce Payment Systems)

992SEC12
TGMXM0A
Fri. 6,7,8 (13:10-16:00) L526

Min-Yuh Day
戴敏育
Assistant Professor
專任助理教授
Dept. of Information Management, Tamkang University
淡江大學 資訊管理學系

http://mail.im.tku.edu.tw/~myday/

2011-05-20

Syllabus

週次	月／日	內容（Subject/Topics
1	100/02/18	電子商務安全課程簡介 (Course Orientation for Secure Electronic Commerce)
2	100/02/25	電子商務概論 (Introduction to E-Commerce)
3	100/03/04	電子市集 (E-Marketplaces)
4	100/03/11	電子商務環境下之零售：產品與服務 (Retailing in Electronic Commerce: Products and Services)
5	100/03/18	網路消費者行為、市場研究與廣告 (Online Consumer Behavior, Market Research, and Advertisement)
6	100/03/25	電子商務 B2B、B2C、C2C (B2B, B2C, C2C E-Commerce)
7	100/04/01	Web 2.0, Social Network, Social Media
8	100/04/08	教學行政觀摩日
9	100/04/15	行動運算與行動商務 (Mobile Computing and Commerce)
10	100/04/22	期中考試週

Syllabus (cont.)

週次	月／日	內容（Subject/Topics
11	100/04/29	電子商務安全 (E-Commerce Security)
12	100/05/06	數位憑證 (Digital Certificate) [Module 4]
13	100/05/13	網路與網站安全 (Network and Website Security) [Module 5]
14	100/05/20	交易安全、系統安全、IC卡安全、電子付款 (Transaction Security, System Security, IC Card Security, Electronic Commerce Payment Systems) [Module 6, 7, 8, 9]
15	100/05/27	行動商務安全 (Mobile Commerce Security)
16	100/06/03	電子金融安全控管機制 (E-Finance Security Control Mechanisms)
17	100/06/10	營運安全管理 (Operation Security Management)
18	100/06/17	期末考試週

教育部顧問室編輯 “電子商務安全”教材

委辦單位：教育部顧問室資通安全聯盟

執行單位：國立台灣科技大學管理學院

- Module 6：交易安全
- Module 7：系統安全
- Module 8：IC卡安全
- Module 9：實務應用案例--電子付款

Module 6：交易安全

學習目的

1. 介紹交易的不可否認性與認識安全標章。
2. 不可否認服務可提供交易的證據，以解決交易所產生的糾紛。
3. 瞭解安全標章之意義，藉由驗證安全標章，可建立對交易網站的信賴

Module 6：交易安全

- Module 6-1：不可否認服務
- Module 6-2：安全標章

Module 6-1：不可否認服務

Module 6-1：不可否認服務

- 不可否認服務的目標是產生、收集、維護及查證(verify)與已宣稱事件或動作有關之證據，並使這些證據為可用，以解決關於已發生或未發生事件或動作的糾紛。
- 不可否認之機制提供基於密碼核對值(cryptographic check value)的證據，使用對稱或非對稱密碼技術產生密碼核對值。
- 不可否認服務的證據建立與特定事件或動作相關的可歸責性(accountability)。

Module 6-1：不可否認服務

- 對於證據產生之相關動作或其事件負有責任之個體被稱為證據主體(evidence subject)。有兩種主要的證據類型：
  - 由證據產生機構(evidence generating authority)使用對稱密碼技術所產生的安全信封(secure envelope)。
  - 由證據產生者(evidence generator)或證據產生機構(evidence generating authority)使用非對稱密碼技術所產生的數位簽章(Digital signatures)。

Module 6-1：不可否認服務

- 涉及不可否認交換的個體需滿足下列需求：
  - 不可否認交換的個體應信賴可信賴第三方。當使用對稱密碼演算法時，一定需要可信賴第三方；當使用非對稱密碼演算法時，一定需要可信賴第三方來產生公鑰憑證或產生證據的數位簽章。
  - 在產生證據之前，證據產生者必須知道查證者可接受的不可否認政策、要求證據種類以及查證者可接受的機制組。
  - 產生或查證證據的機制必須可用於特殊不可否認交換的個體，或可信賴機構必須可用於提供此機制，並且代表證據請求者履行必要的功能。
  - 有關個體要持有/分享適用於所使用之機制的金鑰(亦即，非對稱技術的私鑰，與對稱技術的密鑰)。
  - 證據使用者與判決者要有能力查證證據。
  - 證據所需的時間資訊，是由事件發生時的時間與證據產生時的時間兩者所組成。
  - 若個體在產生證據時要求可信賴時戳，或它所提供的時間不被信賴時，則證據產生者或證據查證者應到時戳機構取得可信賴時戳。

Module 6-1 ：不可否認服務

- 不可否認服務：產生不可否認、發送不可否認、收件不可否認、知悉不可否認、投件不可否認以及傳送不可否認。
- 可由群組化這些基本服務的某些服務，提供其他的不可否認服務。
- 來源不可否認可藉由結合產生不可否認與發送不可否認來提供。
- 遞送不可否認可藉由結合收件不可否認及知悉不可否認來提供。
- 發佈不可否認符記後，可能有必要變更其生命期，例如，若發現針對特定簽章方案的攻擊行為，便縮短其生命期。
- 在另一方面，若不可否認符記在超過其生命期後，仍可視為安全，則不可否認政策可能允許延長此符記的生命期。

不可否認服務類型

- 來源不可否認 (Non-repudiation of origin，簡稱NRO)
- 遞送不可否認 (Non-repudiation of delivery，簡稱NRD)
- 投件不可否認 (Non-repudiation of submission，簡稱NRS)
- 傳送不可否認 (Non-repudiation of transport，簡稱NRT)

Module 6-2：安全標章機制

Module 6-2-1：線上安全認證標章
Module 6-2-2：信賴標章

Module 6-2-1：線上安全認證標章

- McAfee「 Hacker Safe」
- 阿碼科技「HackAlert」
- 趨勢科技「Worry Free Security 」
- 網駭科技「Web Alert」

線　上　安　全　認　證　標　章　種　類				
標章名稱	Hacker Safe	HackAlert	Worry Free Security	Web Alert
標章樣式	 中文版　英文版			
推出公司	McAfee	阿碼科技	趨勢科技	網駭科技
認證內容	系統安全掃描	監控瀏覽器的零時差攻擊	網頁是否隱含惡意連結或惡意程式	網頁是否隱含惡意連結或惡意程式

Module 6-2-2：信賴標章

- VeriSign/HiTRUST「 全球安全認證網站標章 」
- 寰宇數位「GlobalTrust安全網站標章」
- 台北市消費者電子商務協會「優良電子商店標章」
- 台北市消費者電子商務協會「資訊透明化電子商店標章」

Module 6-2-2：信賴標章

- 中華民國網路消費協會「網站認證」
- 中華民國網路消費協會「網站購物補償制度」
- 中華民國旅行業品質保障協會「旅行業品保協會標章」
- 中華民國旅行業品質保障協會「旅行購物保障標章」

Module 6-2-2：信賴標章

- 臺灣網路認證公司「 TWCA 全球安全網站認證標章 」
- 威利全球憑證中心「安全認證網站標章」
- WIS匯智SSL數位憑證中心「 Geotrust 」
- BSI「 ISO/IEC 27001」

信賴標章種類				
標章名稱	全球安全認證網站標章	GlobalTrust安全網站標章	優良電子商店標章	資訊透明化電子商店標章
標章樣式	 全球安全網站認證標章	 中文版  英文版		
推出公司	VeriSign/ HiTRUST 網際威信	寰宇數位	台北市消費者電子商務協會	台北市消費者電子商務協會
認證內容	SSL加密網頁憑證	SSL加密網頁憑證	為消費者除卻網上交易之不安全	提供消費者更快速便捷的辨認工具

信賴標章種類				
標章名稱	網消會認證標章	網消會購物補償標章	旅行業品保協會標章	旅行購物保障標章
標章樣式				
推出公司	中華民國網路消費協會	中華民國網路消費協會	中華民國旅行業品質保障協會	中華民國旅行業品質保障協會
認證內容	確保消費者的網路購物權益	確保消費者的網路購物保障	確保消費者的旅遊消費權益	確保購物店業者的商品品質

信賴標章種類				
標章名稱	TWCA 全球安全網站認證標章	安全認證網站標章	Geotrust	ISO/IEC 27001
標章樣式				
推出公司	臺灣網路認證公司	威利全球憑證中心	WIS匯智SSL數位憑證中心	BSI
認證內容	SSL加密網頁憑證	SSL加密網頁憑證	SSL加密網頁憑證	保護資訊財產

全球安全認證網站標章

全球安全網站認證標章

- 目的
- 安全保證
- 認證標章
- 驗證標章

目的

- 將「信任」(Trustworthiness) 經由安全的網站予以具體化，以提升企業的優質形象
- 藉由啟動SSL(Secured Socket Layer)安全傳輸機制，提供與網站用戶之間經由瀏覽器進行資料加密通訊。

安全保證

全球安全網站認證標章

- 身分辨識：網站訪客藉此確認是否登入正確的網站，避免進入仿冒網站。
- 安全加密：企業與用戶間資料傳輸，將因憑證啟動此SSL加密後得到保護，包括信用卡資料、個人隱私、交易內容及各項機密資料等。

認證標章

全球安全網站認證標章

驗證標章

- 點選標章，立即顯示認證網址與認證結果(注意商店網址須與顯示的認證網址相同)
- 實例：資料來源擷取自博客來網路書店

驗證標章

- 於認證機構的網址上查詢認證清單(注意商店網址須與認證清單上的網址相同)
- 顯示認證結果視窗中的網址要與商店網址一致
- 必須要知道認證機構的網址

GlobalTrust安全網站標章

- 目的
- 安全保證
- 認證標章
- 驗證標章

目的

- 提供與全球同步的加密等級服務。
- 促進網際網路及無線網路上的電子商務及電子訊息溝通的安全性與便利性。

安全保證

- 身分辨識：網站訪客藉此確認是否登入正確的網站，避免進入仿冒網站。
- 安全加密傳輸：企業與用戶間資料傳輸，將因憑證啟動此SSL加密後得到保護，包括信用卡資料、個人隱私、交易內容及各項機密資料等。
- 防釣魚網站： 寰宇數位提供防盜拷備的即時認證標章，可防止釣魚網站不肖的盜取資料，確實即時做到身分認證的功效。

認證標章


Step1
提出申請表
Step2
交付相關必要文件
Step3
產生 CSR
Step4
登錄申請
Step5
繳付費用
Step6
身份核驗
Step7
完成確認
Step8
憑證核發
Step9
安裝及啓動

驗證標章

- 點選標章，立即顯示認證網址與認證結果(注意商店網址須與顯示的認證網址相同)
- 實例：資料來源擷取自全虹企業股份有限公司

STEP 1

STEP 2

www.bbcity.com.tw 網站之安全資料	
憑證種類:	GlobalTrust Pro SSL 專業伺服器憑證 三年 此憑證加密等級依瀏覽器等級及伺服器種類而定，可依客戶端動態調整為40、56、128，最高可達256位元，為目前全球最高加密等級憑證
安全狀況:	驗證合格. 該申請人所提之認證內容與證明文件經查屬實，確認為一合法公司(組織)
申請者:	全虹企業股份有限公司(ARCOA COMMUNICATICN CO., LTD.)
認證網址:	https://www.bbcity.com.tw
憑證內容:	CN=www.bbcity.com.tw OU=Communication Service Division O=ARCOA COMMUNICATION CO., LTD. L=Taipei S=Taiwan C=TW
有效期限:	自 2008/3/28 到 2011/3/28 止

驗證標章

- 實例：資料來源擷取自全虹企業股份有限公司

STEP 1

STEP 2

http://www.bbcity.com.tw/ has been validated and is authentic.
Please ensure the following credentials match the site you are currently visiting:

Company:	ARCOA COMMUNICATION CO., LTD.
URL:	http://www.bbcity.com.tw/
Address:	6F., No.18, Sec. 6, Mincyuan E. Rd., Neihu District, Taipei City 114, Taiwan (R.O.C.) Taipei, Taiwan, 114, Taiwan, Province of China
Telephone:	Unregistered
Fax:	Unregistered
Email Contact:	Unregistered

驗證標章

- 於認證機構的網址上查詢認證清單(注意商店網址須與認證清單上的網址相同)
- 顯示認證結果視窗中的網址要與商店網址一致
- 必須要知道認證機構的網址

優良電子商店標章

- 目的
- 安全保證
- 認證標章
- 驗證標章

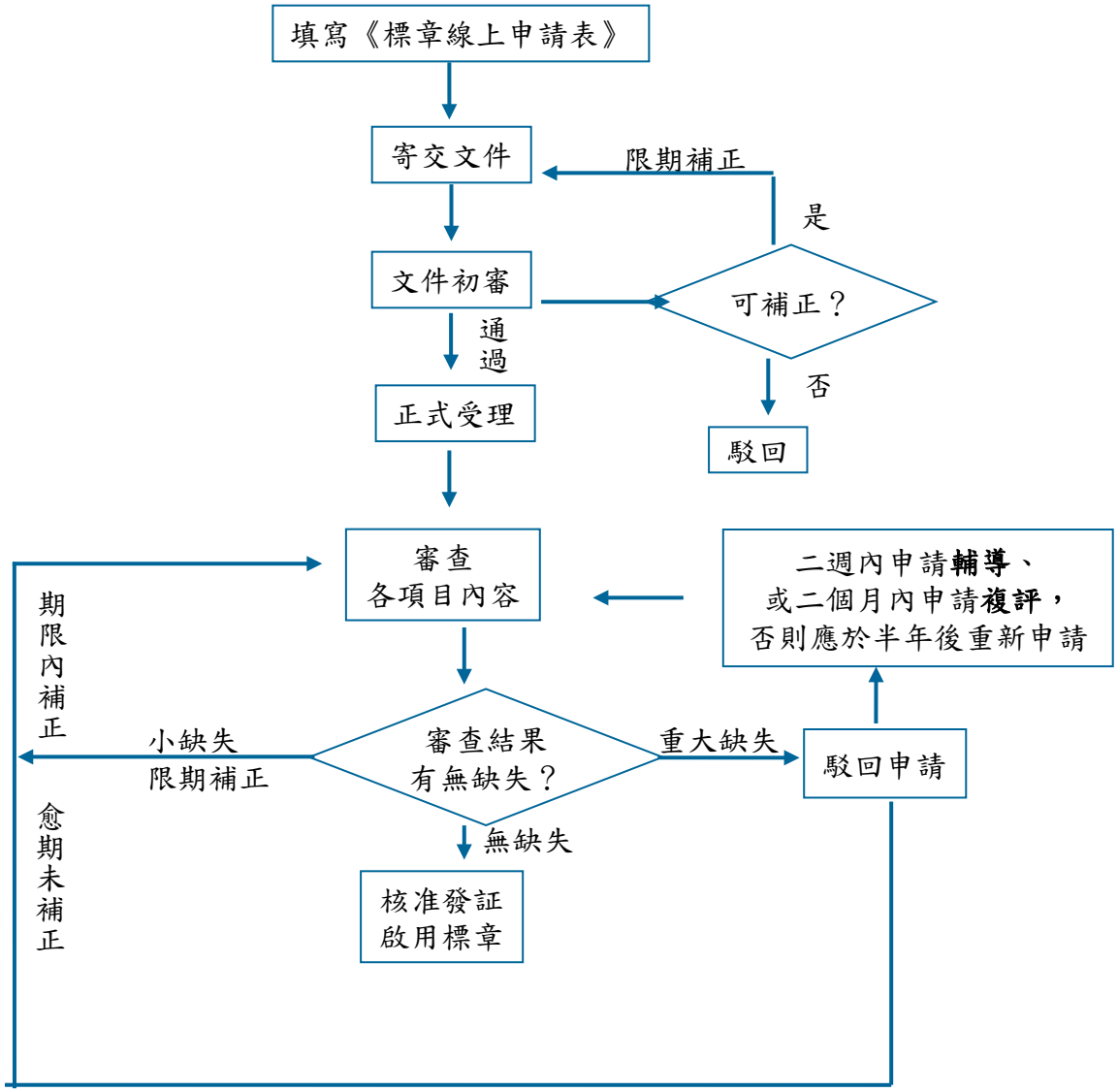
目的

- 為建立自律有序、公平效率、明確安全的電子商務環境。
- 使消費者藉由『優良電子商店』標章之辨識，除卻網上交易之不安全，以吸引更多消費者之青睞，進而達成該電子商務業者與消費者雙贏之局面。

安全保證

- 為消費者除卻網路交易之不安全，以增加其於網際網路上進行消費行為的信心。

認證標章


填寫《標章線上申請表》
寄交文件
限期補正
是
文件初審
可補正？
通過
否
正式受理
駁回
審查
各項目內容
二週內申請輔導、
或二個月內申請複評，
否則應於半年後重新申請
期限內補正
小缺失
限期補正
審查結果
有無缺失？
重大缺失
駁回申請
逾期未補正
無缺失
核准發証
啟用標章

驗證標章

- 點選標章，立即顯示認證網址與認證結果(注意商店網址須與顯示的認證網址相同)
- 實例：資料來源擷取自日盛證券

驗證標章

- 於認證機構的網址上查詢認證清單(注意商店網址須與認證清單上的網址相同)
- 顯示認證結果視窗中的網址要與商店網址一致
- 必須要知道認證機構的網址

TWCA 全球安全網站認證標章

- 目的
- 安全保證
- 認證標章
- 驗證標章

目的

- 確保訊息在網際網路上流通時，不會被網路上的駭客中途攔截解讀(資料保密)或被網路上的駭客擅自修改資料(資料完整)防止第三人經由網路窺知傳輸之任何訊息。

安全保證

- 身分辨識：雙方建立交談時身分辨識 。
- 安全加密：使用者之間所傳輸內容經過加密保護 、保護訊息完整性 。

認證標章


Step 1
申請憑證
所需檢附資料
Step 2
Email寄發
審核完成通知信
Step 3
上傳
CSR (WEB)
Step 4
憑證費用
及繳費方式
Step 5
核發電子憑證
Step 6
安裝與設定
1.電子憑證
2.認證標章

驗證標章

- 點選標章，立即顯示認證網址與認證結果(注意商店網址須與顯示的認證網址相同)
- 實例：資料來源擷取自日茂證券

STEP 1

STEP 2

trade.gmstock.com.tw為TWCA安全認證過之安全認證網站　2008-09-01 23:31:08.505

認證內容	
網站名稱(Common Name)	trade.gmstock.com.tw
憑證狀態(Condition)	有效
有效期限(Validity)	2008-02-29 14:46:25.0至2009-03-02 18:00:00.0
安全認證鑑別(Security)	此網站使用TWCA SSL伺服器數位憑證之安全加密等級。其安全加密等級，視瀏覽器所能提供的強度，最高可達到 40 位元。
擁有者單位名稱	日茂證券股份有限公司

驗證標章

- 於TWCA網站的客服專區，查詢SSL伺服器憑證，輸入商店網址，即可確認
- 顯示認證結果視窗中的網址要與商店網址一致
- 必須要知道認證機構的網址

參考文獻

- 中華民國國家標準CNS 14510：資訊技術－安全技術－不可否認
- McAfee：「http://www.mcafee.com/tw/」
- 阿碼科技：「http://www.armorize.com.tw/」
- 趨勢科技：「 http://tw.trendmicro.com/tw/home/」
- 網駭科技：「 http://www.net-hack.com/」
- 網際威信：「 http://www. hitrust.com.tw/hitrustexe/frontend/default_tw.asp 」
- Global Trust寰宇數位認證中心：「http://www.globaltrust.com.tw/」
- 台北市消費者電子商務協會：「http://www.sosa.org.tw/index.asp 」
- 中華民國網路消費協會：「http://www.nca.org.tw/」
- 中華民國旅行業品質保障協會：「http://www.travel.org.tw/ 」
- 臺灣網路認證公司：「http://www.twca.com.tw/Portal/Portal.aspx 」
- 威利全球憑證中心：「http://www.egca.com.tw/」
- WIS匯智SSL數位憑證中心：「http://myssl.com.tw/index.asp」
- BSI：「http://www.bsigroup.tw/

Module 7：系統安全

學習目的

- 系統安全基本觀念與涵蓋的知識範圍
- 安全管理人員日常之系統管理
- 資訊系統內軟體的安全與硬體的安全
- 常見之整合安全系統
- 可信賴電腦

Module 7：系統安全

- Module 7-1：系統安全
- Module 7-2：可信賴電腦

Module 7-1：系統安全

本模組內容係引用教育部顧問室資通安全聯盟「系統安全」課程教材之「Module 1-系統安全概論」

Module 7-1：系統安全

- 系統安全管理
- 軟體安全
  - 十大軟體安全守則與常見軟體攻擊方式
- 硬體安全
  - 如何防止駭客攻擊
- 整合安全系統
  - 常見之不當安全設定

系統安全管理

- 實體設備安全管理
- 主機系統安全管理
- 網路安全管理
- 憑證安全管理

系統安全管理(Cont.)

- **實體設備安全管理政策：**
  - 機房內設備例行性檢查。
  - 機房內資訊設備及資訊媒體使用管理。
  - 門禁管理。
  - 設備安全管理。

系統安全管理(Cont.)

- 主機系統(大型電腦、伺服器、資料庫等)安全管理政策：
  - 作業平台建置標準，安裝、修補、更新。
  - 日常操作管理、系統日誌處理。
  - 異常狀況排除。

系統安全管理(Cont.)

- **網路安全管理政策：**
  - 網路設備安裝維護。
  - 防火牆建置與管理。
  - 網路安全監控。
  - 電腦病毒防治。
  - 入侵偵測系統建置。

系統安全管理(Cont.)

- 憑證(Certificate)安全管理：
  - 憑證申請。
  - 憑證簽發。
  - 憑證下載。
  - 憑證管理。
  - 憑證註銷。

軟體安全

- 定義：指安裝或企業內部設計不當的應用軟體系統，因軟體設計瑕疵而發生安全上的顧慮。
- 軟體安全的十大原則
- 駭客攻擊三大階段

軟體安全–十大原則

- 原則1：保全最弱環節(Securing the weakest link)
- 原則2：深度防禦(Defense in depth)
- 原則3：系統錯誤情況處理設計(Secure failure)
- 原則4：最小額度的使用權限控制(Least privilege)
- 原則5：權限劃分(Compartmentalization)
- 原則6：簡單化(Simplicity)
- 原則7：保護使用者隱私(Promote privacy)
- 原則8：機密難以保護(It's hard to hide secrets)
- 原則9：勿輕易擴大信任度(Don't extend trust easily)
- 原則10：相信團隊(Trust the community)

軟體安全–常見軟體攻擊方式

- 準備階段：
  - 主要是在獲取目標主機上各種資訊之行為，對於主機一般還未造成任何損害。
- 攻擊及攻佔後之階段：
  - 主要是在設法取得、提升、利用目標主機之存取權，這個部份對目標主機所造成之損害需視駭客取得之權限大小而定。
- 阻絕階段：
  - 主要是阻絕服務，讓合法使用者不能使用目標主機之服務。這種行為可能是駭客在無法完成上一階段之攻擊時所作。

軟體安全–常見軟體攻擊方式

- WHOIS、NSLOOKUP查詢工具
  - 可藉此類工具調查入侵或攻擊目標的基本網路資料及相關公司資訊。
- IPSPOOFING
  - 藉此手段來偽造來源端，以擾亂司法人員調查的方向並隱藏自己的真實位址。
- IP/PORT SCANNING
  - 藉由IP或通訊埠掃瞄的工具來提供的服務及DMZ區各種的安全機制(如防火牆POLICY、弱點掃瞄及應用系統伺服器等資訊)。

軟體安全–常見軟體攻擊方式

- 網路監聽
  - 如Ethereal 、Sniffer等封包監聽工具常被利用來做為駭客工具最重要的資訊蒐集工具，可以透過封包的擷取，建立企業網路的各項交易封包複本，做為後續各種分析及破解的資訊來源。
- 漏洞調查
  - 結合已知開放的服務、系統版本及監聽到封包可以分析到攻擊目標可能存在的系統或軟體漏洞，最常見的是緩衝區溢位問題。
- 密碼破解
  - 如Stake公司的LC4/LC5系列軟體，常被用來做為破解工具。

軟體安全–常見軟體攻擊方式

- 木馬程式(Trojan)
  - 被入侵的主機被建立一個開放遠端控制的後門，進行不法的破壞。
- 間諜程式(Spyware)或p2p程式
  - 被植入的主機會將資訊開放分享，提供植入者或不特定者使用。至於p2p則是在商業公司管理下的程式，當被惡意使用，亦能變為入侵的工具。
- 傀儡程式(Bot-Net)
  - 利用傀儡程式來替代傳統的IPSPOOFING工具，使攻擊者的身份更加隱匿，達到更高的匿名性，及調查的難度。
- 開放代理伺服器(Open Proxy Server)
  - 利用公/民機關較封閉的網管政策，在開放網路架設不同服務(如P2P、MSN、網路遊戲)的代理伺服器，吸引無知使用者在連線過程中留下機密資料。

硬體安全

- 硬體安全的概念可以是將安全機制或安全軟體轉向產品化。也可以解釋成透過搭配不同的硬體設備來提高企業系統及網路的安全度。
  - 網路安全裝置
    - 防火牆軟體、防火牆硬體
    - 掃毒軟體、防毒閘道
    - 入侵偵測軟體、入侵偵測及弱點掃瞄閘道
  - 人員管理裝置
    - 身份金鑰、IC卡
    - 生物特徵辨識設備

硬體安全-網路安全裝置

- (動/靜)態防火牆、入侵偵測防禦、VPN、多線寬頻負載平衡、伺服器負載平衡及頻寬管理等多種安全機制的硬體裝置。
- 防火牆：提供封包過濾、阻擋、協定開放及關閉、各種連線情況(成功、失敗、特定服務)的日誌記錄等。
- 入侵偵測系統：通常建立有相當大的特徵資料庫來比對線上的連線活動是否符合特徵，來判斷為合法或惡意的連線，排除潛在的攻擊活動。

硬體安全-網路安全裝置

- VPN(Virtual Private Network)：硬體式的VPN將IPsec的概念轉換成硬體線路，提供企業建立總公司與各地分公司的企業內部網路。
- 多線寬頻負載平衡、伺服器負載平衡及頻寬管理：依靠網路服務為主要業務的公司(如入口網站、網路遊戲、部落格網站)對於頻寬管理尤期重視，不能讓線上服務塞車、中斷。

硬體安全-人員管理裝置

- 硬體安全模組(Hardware Security Module、Host Security Module，HSM)：是一種符合RS232、SCSI或USB的外接硬體，提供一般電腦某些特定的資訊安全功能。
  - HSM通常會結合密碼學公開金鑰系統來提供使用者在建立、修改、儲存、刪除等工作上的資料安全，或者以對稱金鑰的演算法管理硬體的安全。
  - 常見的如使用者的USB Tokey或儲有軟體授權金鑰的硬體鎖、憑證IC卡、iButton及SIM卡。

硬體安全-人員管理裝置

- HSM的開發主要有二個方向：
  - 自動櫃員機(Automated Teller Machines，ATM)與銷售點終端機(Point of Sale，POS)
    - 主要功能是著重在晶片卡上的加密元件電路設計與保護載入存有金鑰的記憶體。
  - 授權及個人化模組
    - 認證線上的PIN資料庫與加密PIN碼相符。
    - 至少支援一種Smart Card要應用的加密函數介面。(如Europay、Master、Visa所提的EMV標準)。
    - 可以針對一張Smart Card產生金鑰集(KeySet)並支援個人化的處理工作。

硬體安全-硬體攻擊概念

- 時序攻擊法
- 物理密碼攻擊法
- 電力攻擊法
- 硬體錯誤攻擊法

整合安全系統(Integrated security System)

- 整合二種以上的安全機制與技術建立而成的系統，可以稱之為整合安全系統。常見有以下幾種：
  - PKI公開金鑰基礎建設
  - 電子商務安全
  - VPN技術
  - PGP
  - Kerberos

Module 7-2：可信賴電腦

本模組內容係引用教育部顧問室資通安全聯盟「資訊安全導論」
課程教材之「Module 3-5-可信賴電腦簡介」

可信賴電腦
(Trusted Computing Platform)

- 在數位的網路化潮流下，一個合適的、安全的資訊運作平台將使我們在工作或生活上能夠平穩、順暢，而不會因為 平台的失常或是錯誤資訊而導致損害

可信賴電腦 (Trusted Computing Platform)

- 可以完全信賴電腦嗎？
- 系統內的程式設計或硬體設計是否夠周延
- 是否有弱點？
- 是否內部程式會遭惡意的篡改、資料或植入病毒和木馬程式造成系統的不正確性或不穩定性
- 重要資料的外流？

可信賴電腦的概念

- 可信賴電腦較具體的概念是由TCPA 聯盟（TCG 的前身）率先提出
  - 目的就是在於建構一個誠信的電腦網路環境與系統
  - 每個網路終端都應具有合法並可被鑑別的網路身份
  - 而且網路終端具有對惡意程式有防範的功能

可信賴的安全功能

- 終端設備的鑑別
- 資料完整性的檢驗
- 使用者身份的鑑別
- 使用者存取權的合法性
- 各種輸出入連接埠埠 (I/O Port) 控制和管理
- 儲存資料的加解密
- 保護重要資訊的硬體

系統的可信賴性

- ISO/IEC 15408 標準
  - 可信賴的元件
  - 操作的行為是可預測的
  - 能抵抗惡意程式軟體、病毒及其他物理干擾的破壞
  - 可信賴性應
    - 可用性、可靠性、強健性、可維護性、安全性及可測試性

TCG 組織的可信賴電腦概念及相關規範 (1/2)

- TCG 組織制定三個基本規範

私密性
(Confidentiality)

認證
(Authentication)

完整性
(Integrity)

TCG 組織的可信賴電腦概念及相關規範 (2/2)

- TCPA聯盟所制定的TCPA 主規範(TCPA Main Specification)來定義一個可信賴平台模組(Trusted Platform Module; TPM)的硬體安全架構的標準
- 於2003 年，TCG 組織也公佈了一份新的標準：TCG Software Stack 規範1.1 (TSS 1.1)

Microsoft 公司的可信賴電腦概念

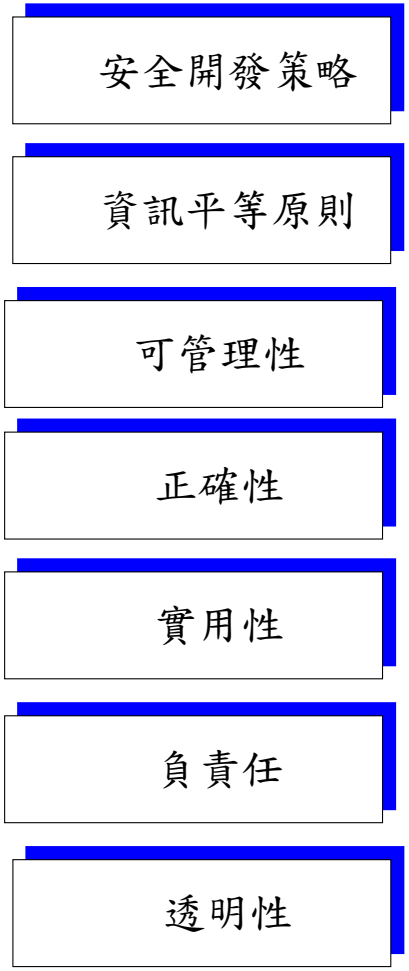
(1/2)

- 其目標包括四個方面

Microsoft 公司的可信賴電腦概念

(2/2)

- 遵循的策略



可信賴電腦運作模式

- TCG 組織延續TCPA 聯盟的作法來達成可信賴電腦的目標
  - 可信賴平台模組
  - 數位版權管理(Digital Rights Management; DRM)
  - 強制性存取控制(Mandatory Access Control; MAC)機制

可信賴平台模組

- 其主要的核心技術是透過一個硬體模組搭配軟體的方式來運作

數位版權管理

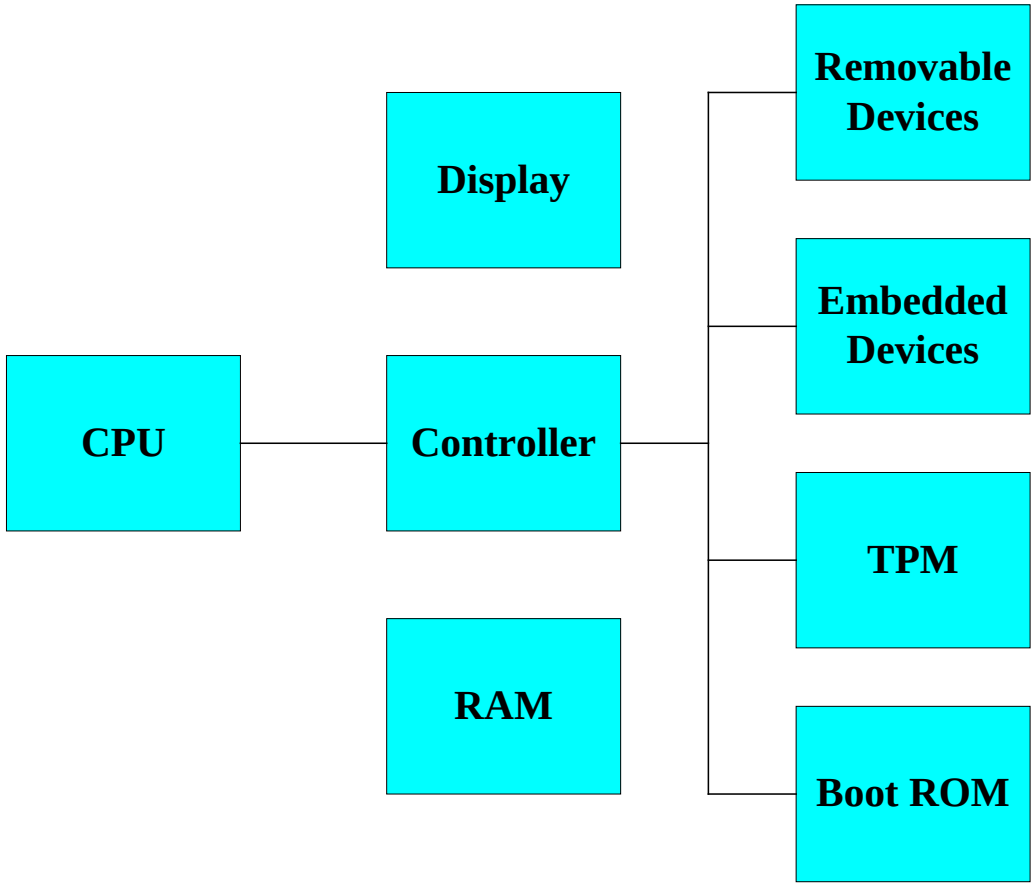
- 透過軟體來對系統中的作業系統、應用程式、檔案文件或多媒體資料進行檢核授權的工作
- 也就是說TCG 組織所建議的機制系統中所能被執行的每一個程式或資料都經過信任檢核與保護

強制性存取控制機制

- 強制性存取控制由系統來統一決定物件被存取的策略
  - 通常用於政府機關或對資料安全有極端保密需求的組織

可信賴平台模組簡介

- 可信賴計算模組



軟體解決安全問題的弱點

- 以軟體來解決安全問題的弱點
  - 作業系統本身的弱點與漏洞會造成軟體程式無法正常或正確地運作
  - 軟體程式有潛在被破壞或不當修改的危機
- 以硬體來解決軟體的弱點
  - 破壞硬體晶片來達到攻擊的目的，其難度遠比破壞軟體程式高出許多

參考資料

- 實戰 Linux 防火牆 -- iptables 應用全蒐錄, Robert L. Ziegler著, 上奇科技出版, ISBN 986752969-3
- 軟體安全與資訊戰爭
  http://www.csie.nctu.edu.tw/~skhuang/soft-sec.htm
- 軟體品質與資訊安全
  http://www.csie.nctu.edu.tw/~skhuang/
- 企業防護不可或缺的一環：整合的用戶端安全
  http://www.symantec.com/region/tw/enterprise/article/client/security.html
- 駭客攻擊之分析與主機系統安全之設定
  http://linuxweb.tccn.edu.tw/NewUpgrade
- 可信賴電腦的簡介與發展趨勢
  http://ics.stpi.org.tw/Treatise/doc/12.pdf
- 時序攻擊法(Timing Attack)與安全防護說明
  http://www2.nsysu.edu.tw/cc/20050829.pdf
- Linux Server Hacks 駭客一百招, Rob Flickenger 著, 林長毅,林班侯 編譯, O'REILLY 出版, ISBN 986-7794-19-2
- Linux 系統安全防禦手冊, 劉祖亮著, 學冠行銷出版, ISBN 986-7961-74-9
- Linux 網路管理實務 – 調校,帳號,監控,安全 , 施威銘實驗室, 旗標出版, ISBN 957-442-111-2
- UNIX 與 INTERNET 安全防護 – 系統篇 , Simon Garfinkel & Gene Spafford 著, 陳志昌,林逸文 ,蔣大偉 譯, O'REILLY 出版, ISBN 957-8247-60-5
- Web 應用軟體安全之研究
  http://www.sinica.edu.tw/as/advisory/journal/13-2/101-105.pdf

參考資料

- SANS Network Security Roadmap, 8th Edition, 2003, http://www.sans.org.
- Bruce Schneier, *Applied Cryptography*, 2nd Ed., 1996.
- Charles P. Pfleeger, *Security in Computing*, 2nd Ed., 1997.
- Dorothy E. Denning, *Information Warfare and Security*, Addison-Wesley, 1999.
- Dieter Gollmann, *Computer Security*, Wiley, 1999.
- William Stallings, *Cryptography and Network Security*: *Principles and Practices*, 4th Ed., Prentice Hall, 2006.
- 陳奕明等著，資訊與通訊系統之程式安全，行政院國家科學委員會科學技術資料中心，民國92年
- 高宏傑著，建立零缺點的安全軟體系統，培生教育出版集團，民國91年
- 孫宇安著，採用Color Petri Net方法偵測程式原始碼緩衝區溢位問題，中央大學資訊管理研究所碩士論文，民國90年6月
- D. Evans and D. Larochelle, “Improving Security Using Extensible Lightweight Static Analysis,” *IEEE Software Magazine*, Vol. 19, No. 1, 2002, pp.42-51.
- W. Stackpole, “Security Realities in Software Development,” *Computer Security Journal*, Vol. 8, No. 1, 2002, pp. 9-14.

參考資料

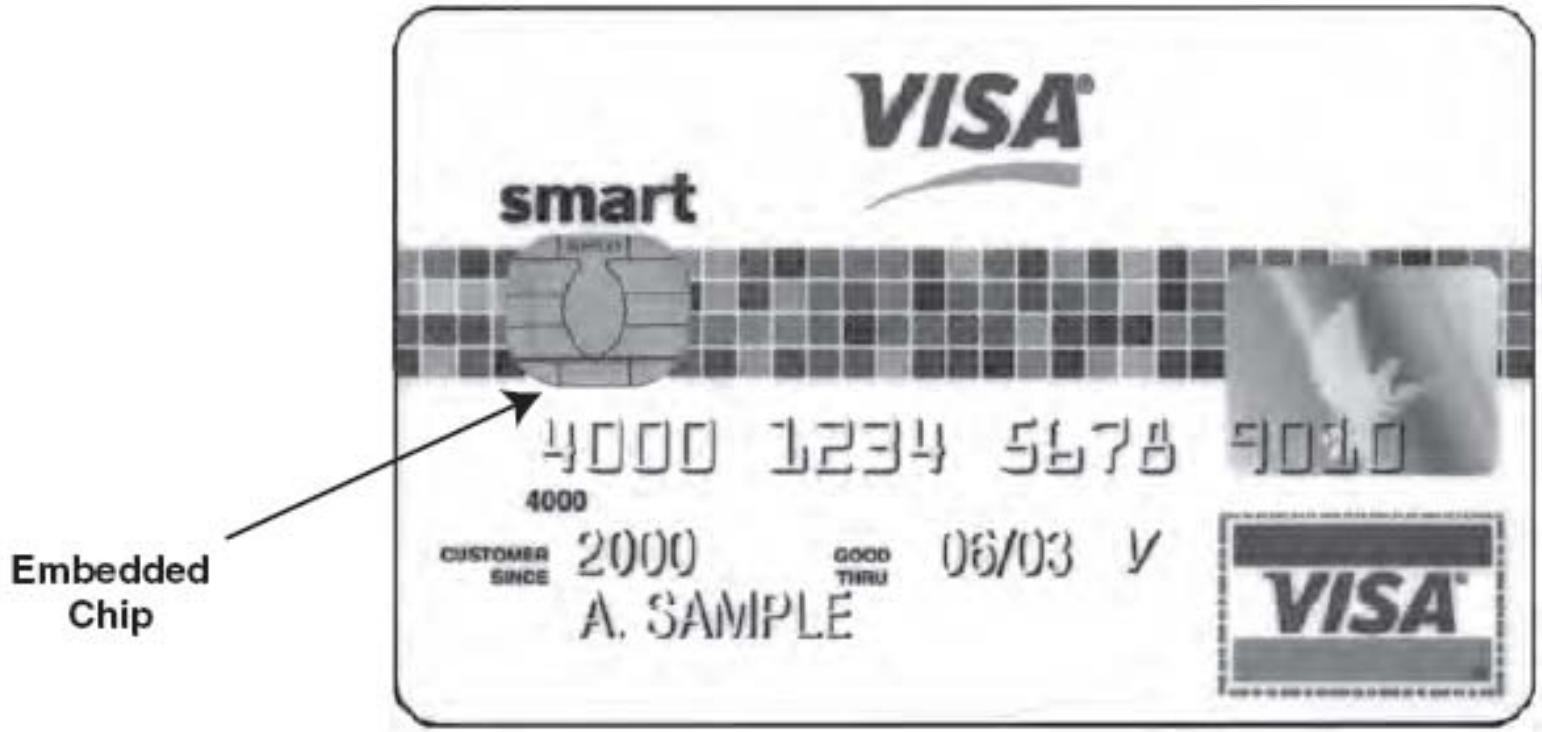
- 邱榮輝著，資訊與通計系統之硬體安全，行政院國家科學委員會科學技術資料中心，民國92年
- 賴溪松等著，近代密碼學及其應用，松崗，台北，民國89年，頁7-27
- 凱薩琳・艾倫等著，陳曉開譯，智慧e卡，麥格羅希爾，台北，民國89年
- D. G. Abraham, G. M. Dolan, G. P. Double, and J. V. Stevens, Transaction Security System, *IBM Systems Journal*, Vol. 30, No. 2, 1991, pp. 206-229.
- Security Requirements for Cryptographic Modules, FIPS PUB 140-2, May 2001, http://csrc.nist.gov/publications/fips/fips140-2/
- 樊國禎等著，系統安全，行政院國科科學委員會科學技術資料中心，民國91年
- 陳至哲等著，資訊訊安全關鍵技術發展藍圖，財國法人資訊工業策進會，民國92年
- 林祝興、張真誠著，電子商務安全技術與應用，旗標出版股份有限公司，民國94年
- Trusted Computing Group, TCG Specification Architecture Overview, Revision 1.2, Apr. 28 2004.
- Microsoft Incorporated, Trusted Platform Module Services in Windows Longhorn, WinHEC 2005 Version, Apr. 25 2005.

參考資料

- 樊國禎等著，系統安全，行政院國科科學委員會科學技術資料中心，民國91年
- 陳至哲等著，資訊訊安全關鍵技術發展藍圖，財國法人資訊工業策進會，民國92年
- 林祝興、張真誠箸，電子商務安全技術與應用，旗標出版股份有限公司，民國94年
- Trusted Computing Group, TCG Specification Architecture Overview, Revision 1.2, Apr. 28 2004.
- Microsoft Incorporated, Trusted Platform Module Services in Windows Longhorn, WinHEC 2005 Version, Apr. 25 2005.

Module 8：IC卡安全

Smart Card



(Source: Turban et al., 2010)

IC卡之類型

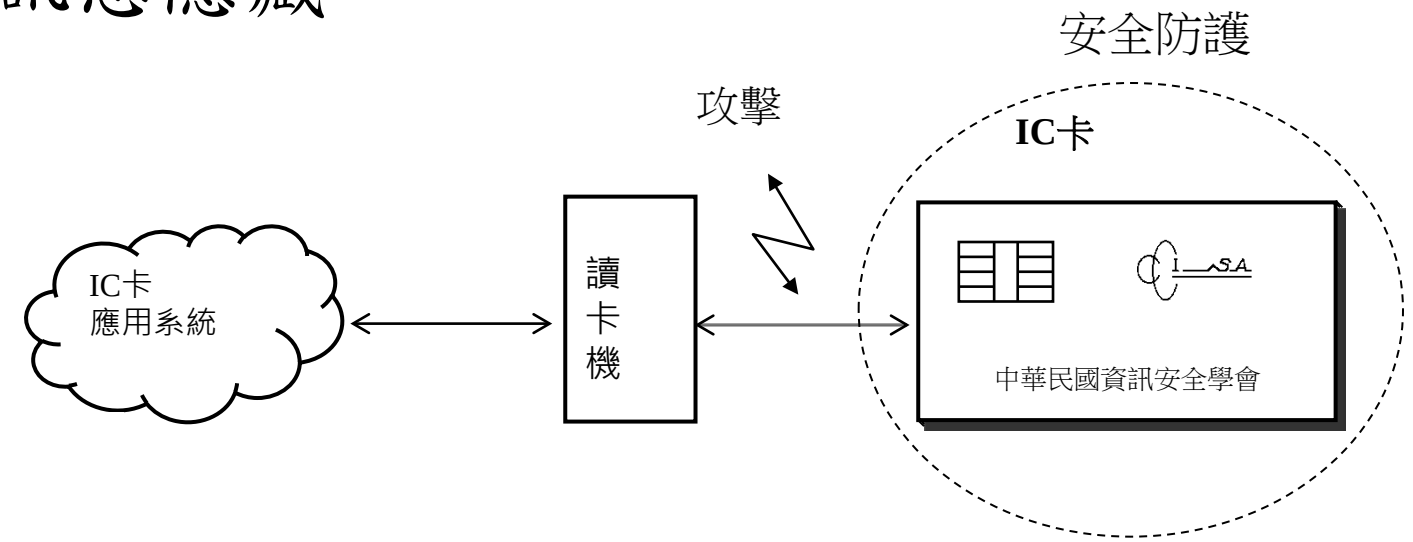
- 接觸式IC卡
- 非接觸式(contactless)IC卡
- 混和式(hybrid) IC卡
  - 含有接觸式與非接觸式兩種介面之IC卡 (ICC)
    - 接觸式與非接觸式各用其獨立之IC晶片
    - 接觸式與非接觸式共用一顆IC晶片

IC卡之安全防護概念

- IC卡是一密碼模組。
- IC卡主要用於
  - 儲存公開金鑰或私密金鑰之憑證(certificate)裝置。
  - 儲存使用者之祕密參數。
  - 儲存個人私密資料。
  - 儲存隨附高階物品之產品資料

IC卡之安全防護

- 卡片身分鑑別
- 檔案存取控制
- 檔案加密處理
- 運算訊息隱藏



IC卡之安全威脅與攻擊

- 側錄：經由有線或無線從旁盜錄資料
- 假冒：假冒系統或使用者
- 洩漏：經由有線或無線從內部洩漏資料出去
- 攔截：經由有線或無線攔截通訊資料
- 竊取：竊取非經授權之內部資料
- 竄改：竄改所竊取之內部資料或所攔截之通訊資料
- 隱私：揭露個人隱私資料

IC卡之安全防護服務

- 鑑別性
- 機密性
- 完整性
- 存取控制
- 不可否認

IC卡的應用

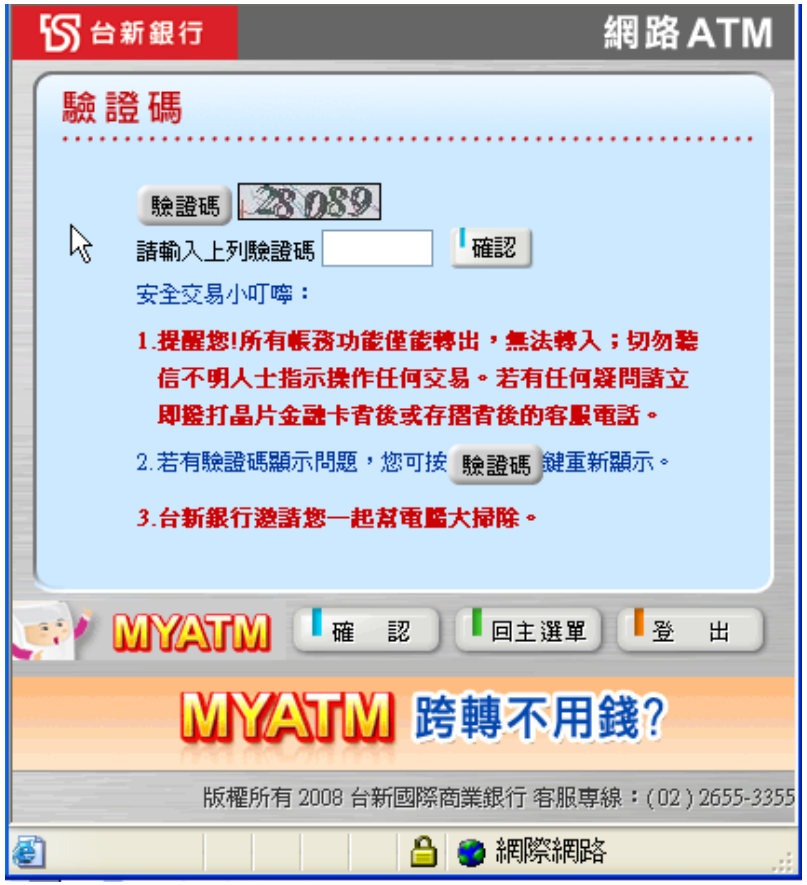
一般IC卡的應用有下列用途：

1. 金融交易(轉帳)
2. 電子錢包(交通運輸儲值卡，例如：捷運悠遊卡，高速公路ETC卡，7/11的Icash卡)
3. 載具(存放憑証資料，例如：自然人憑証卡)
4. 身份ID(健保卡)
5. 購物(金融卡轉帳，晶片信用卡)
6. OTP(One Time Password)
7. 電信(SIM卡)

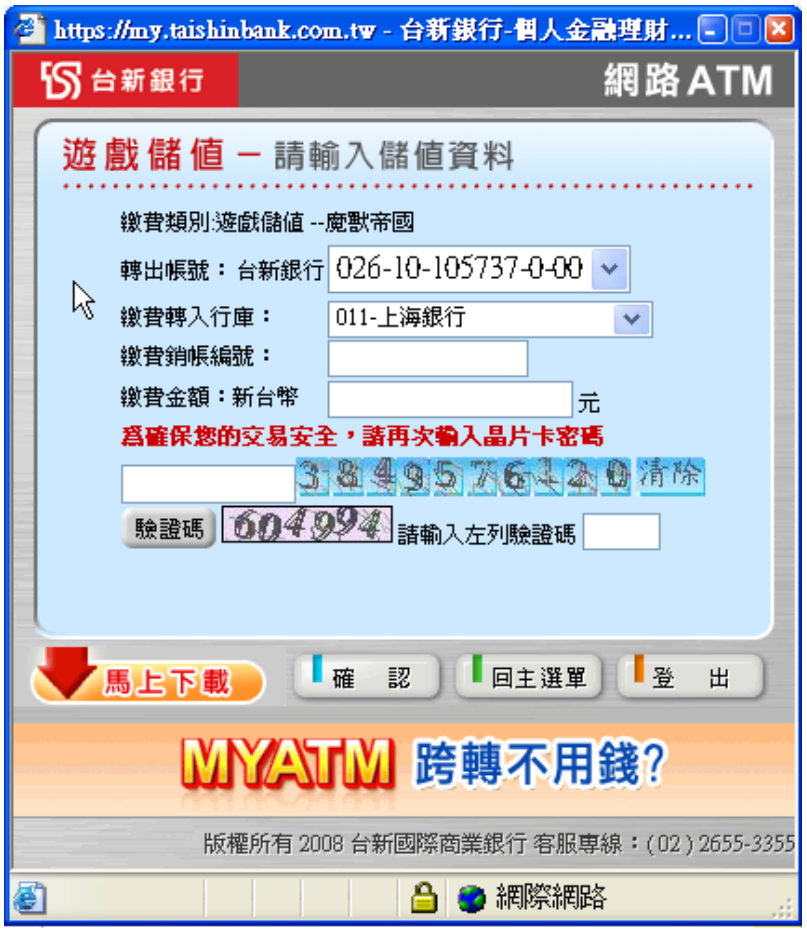
IC卡的應用模式-晶片金融卡應用

以晶片金融卡與Server端相互驗証，完成身分鑑別，合法登入網站

晶片金融卡電子商務金流服務範例(1/3)



晶片金融卡電子商務金流服務範例(2/3)



晶片金融卡電子商務金流服務範例(3/3)

參考資料

- ISO 7816/1-6
- Smart Card Tutorial, http://www.smartcard.co.uk/tutorials/sct-itsc.pdf
- Gemplus, smart cards introduction part 3, smart card operating systems, http://www.cs.uku.fi/kurssit/ads/SC_OperatingSystems.pdf
- J. Kelsey, B. Schneier, D.Wagner, and C. Hall, Side channel cryptanalysis of product ciphers, Proceedings of ESORICS '98, Lecture Notes in Computer Science, vol. 1485, Springer-Verlag, pp. 98-110, 1998.
- R. J. Anderson and M. G. Kuhn, Tamper resistance- a cautionary note, Proceedings of Second USENIX Workshop on Electronic Commerce Oakland, California), pp. 1-11, 1996.
- R.J. Anderson, M.G. Kuhn: Low Cost Attacks on Tamper Resistant Devices. In M. Lomas, et al. (eds.), *Security Protocols, 5th International Workshop*, LNCS 1361, pp. 125-136,Springer-Verlag, 1997
- E. Biham and A. Shamir, Dierential fault analysis of secret key cryptosystems, Proceedings of CRYPTO '97 (Burton S. Kaliski Jr., ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag , pp. 513-525, 1997.
- 邱榮輝 ，認識IC卡 ，資訊安全通訊 第四卷第三期， pp. 18-30, 民國87.06
- 財金資訊股份有限公司，晶片金融卡規格書
- www.taishinbank.com.tw

Module 9：實務應用案例--電子付款

學習目的

- 電子商務對於電子付款機制的需求
- 介紹常用的幾種電子付款系統
  - 電子支票
  - 電子信用卡
  - 電子錢包

Module 9：實務應用案例--電子付款

- Module 9-1：電子付款系統架構
- Module 9-2：帳戶型付款系統
- Module 9-3：電子支票
- Module 9-4：電子信用卡
- Module 9-5：安全電子交易標準SET
- Module 9-6：智慧卡電子錢包
- Module 9-7：晶片金融卡消費扣款
- 參考資料

Module 9-1：電子付款系統

電子付款

- 電子付款：利用數位訊號的傳遞，代替一般貨幣的流動，達到實際款項支付的目的的機制
- 常用工具：
  - 電子現金
  - 電子支票
  - 電子信用卡
  - 智慧卡電子錢包
  - 晶片金融卡

電子付款系統需求

- 技術面
  - 安全性、軟體或硬體、連線或離線、擴充性、彈性、效率
- 經濟面
  - 交易成本、交易實質性、使用者範圍、價值可轉移性、財務風險
- 社會性
  - 匿名性、使用友善性、可移動性
- 管理面
  - 符合法律、政策與相關規範

電子付款系統需求－技術面

- 安全性是系統架構最主要的考量因素：
  - 鑑別性（Authenticity）
    - 可鑑別確認身分合法性，且不影響匿名性
  - 機密性（Confidentiality）
    - 防範機密資訊（如：密碼）遭竊取或複製
  - 完整性（Integrity）
    - 保護交易訊息或付款指示的正確完整
  - 不可否認性（Non-repudiation）
    - 提供不可否認證據，防止交易雙方反悔，解決糾紛

電子付款系統需求－技術面(續)

- 軟體或硬體
  - 硬體軟體與資料整合至IC卡，安全性較高
- 連線或離線
  - 交易過程中或交易後分批次與第三方連線確認交易
- 擴充性（Scalability）
  - 系統架構可隨交易量增長而擴充
- 彈性
  - 因應社會與網路環境變化而調整
- 效率
  - 簡化流程或加速計算，可能犧牲部分安全性

電子付款系統需求－經濟面

- 交易成本（Cost of transaction）
  - 買賣雙方進行交易所需成本，含直接和間接成本
- 交易實質性（Atomic exchange）
  - 交易發生時，商品所有權和實際金錢之實質交換
- 使用者範圍（User reach）
  - 系統所能接觸的使用者範圍（如：年齡限制）
- 價值可轉移性（Value mobility）
  - 是否不限定於發行機構所授發之個體，價值可轉移
- 財務風險（Financial risk）
  - 個人資料遭竊或外洩所需負擔之財務風險大小

電子付款系統需求—社會面

- 匿名性（Anonymity）
  - 保護資料，防範有心人士得知交易使用者真實身分
- 使用友善性（User friendliness）
  - 系統是否容易使用，使用介面是否友善
- 可移動性（Mobility）
  - 不限定必須於特定電腦上使用

Module 9-2：帳戶型付款系統

帳戶型付款系統

- 由一個帳戶（付款方）將金額轉出，付給另一個帳戶（收款方）
- 電子付款指示（轉帳）：
  - 付款指示包含帳戶資訊、商品清單、交貨期限等
  - 商店取得消費者的付款指示，向開戶行查證帳戶資訊，並授權銀行決定帳戶結算時點
- 電子支票：
  - 現實世界中紙本支票付款在網路的延伸
  - 以電子簽章取代紙本支票的紙筆簽章

Module 9-3：電子支票

電子支票

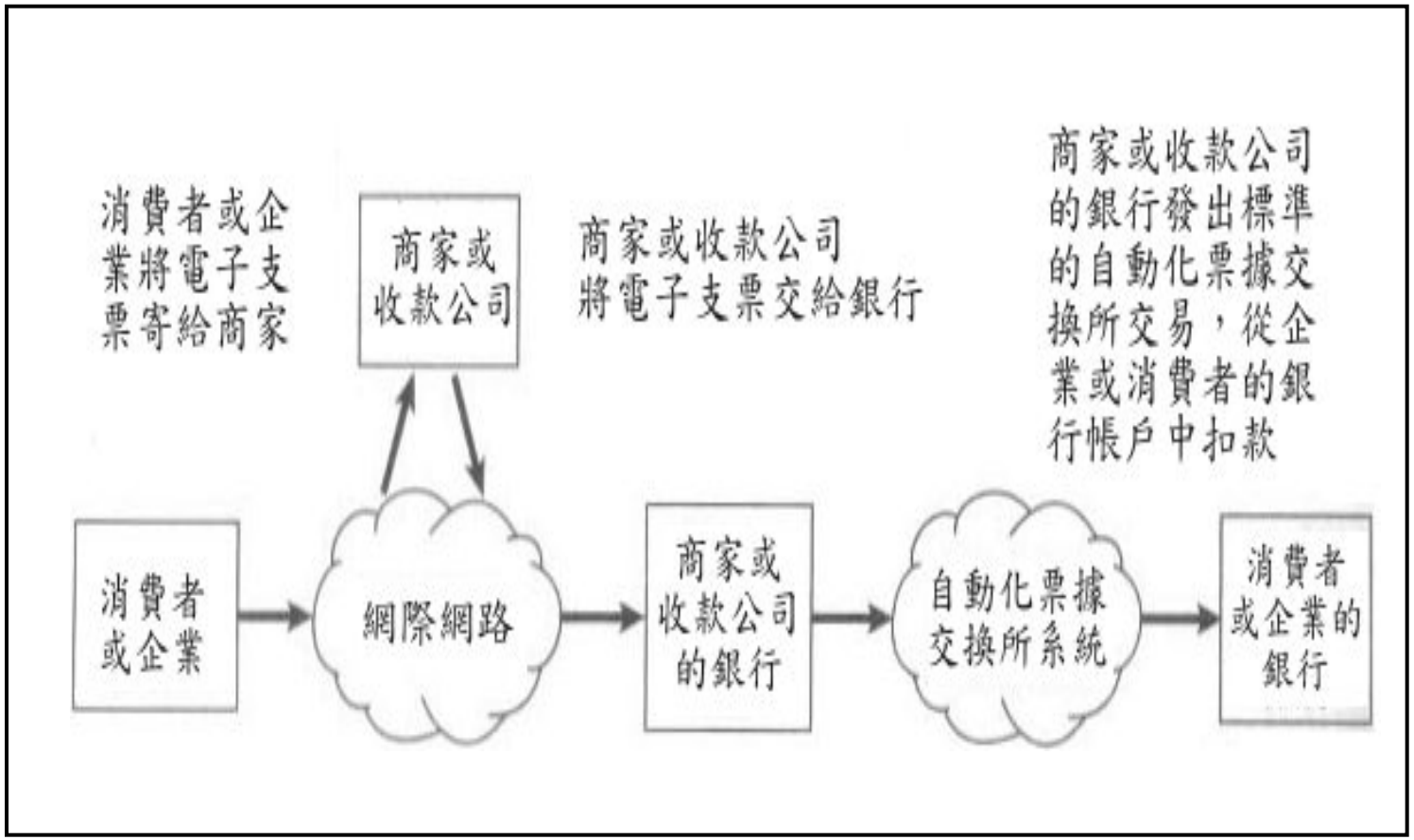
- 電子支票（Electronic Check）用以吸引不想使用現金，而採信用方式的個人或公司組織
- 可取代傳統書面支票的電子文件，使用於網路付款時如同簽發紙本支票
- 以簽章卡（Signature Card）及電子簽章技術，取代傳統以筆或印鑑簽章的方式
- 可即時查詢發票人的信用情況

電子支票使用程序

參與個體：憑證中心(CA)、銀行、發票人、受款人、受讓人、票據交換所

1. 參與個體先向CA申請公鑰憑證
2. 發票人向銀行申請簽發電子支票
3. 發票人簽發支票給受款人
4. 受款人視實際情況需要，決定是否要將支票轉讓給受讓人
5. 受款人持支票向銀行提示，要求兌現
6. 銀行將其他銀行支票送往票據交換所，進行票據交換

電子支票交易圖



資料來源：比爾本漢著，許梅芳譯，民89，電子商務產業版圖，財訊出版社，p.164。

電子支票安全機制

- 金鑰類別
  - 公鑰（Public Key）
  - 私鑰（Private Key）
  - 交談金鑰（Session Key）
- 密碼機制
  - 加/解密（交談金鑰）
  - 電子簽章（公鑰及私鑰）
  - 金鑰交換協定（公鑰、私鑰、交談金鑰）

申請電子支票

- 發票人與銀行進行金鑰交換，分享一把交談金鑰
- 發票人準備電子支票及對支票之簽章，以交談金鑰加密後，將結果傳送給銀行
- 銀行以交談金鑰解密後，驗證發票人對支票的電子簽章
- 若驗證成功，則銀行加入電子簽章，將支票以交談金鑰加密後傳回給發票人
- 發票人驗證銀行的電子簽章，回應確認收到支票

簽發電子支票

- 發票人簽署電子支票，以受款人的之公鑰加密支票及其簽章，將結果傳送給受款人
- 受款人以私鑰解密，驗證發票人的電子簽章
- 受款人與銀行進行金鑰交換，分享一把交談金鑰
- 受款人以交談金鑰加密支票，將結果傳送給銀行
- 銀行驗證自己的簽章，回應受款人支票是否有效

轉讓電子支票

- 受款人與銀行進行金鑰交換，分享一把交談金鑰
- 受款人將背書後的支票以交談金鑰加密後，傳送給銀行簽署
- 銀行將簽署後的支票傳回給受款人
- 受款人以受讓人的公鑰加密支票，將結果轉給受讓人
- 受讓人以私鑰解密，向銀行查驗支票有效性
- 銀行驗證自己的簽章，回應受讓人支票的有效性

兌現及交換電子支票

- 受款人遵循現行支票的兌現及交換程序進行支票兌現及交換
- 銀行需維護一個資料庫，記錄兌現或交換後的支票，以防止支票重複使用
- 銀行之資料庫可以開放供受款人或受讓人查詢支票之兌現及交換現況

Module 9-4：電子信用卡

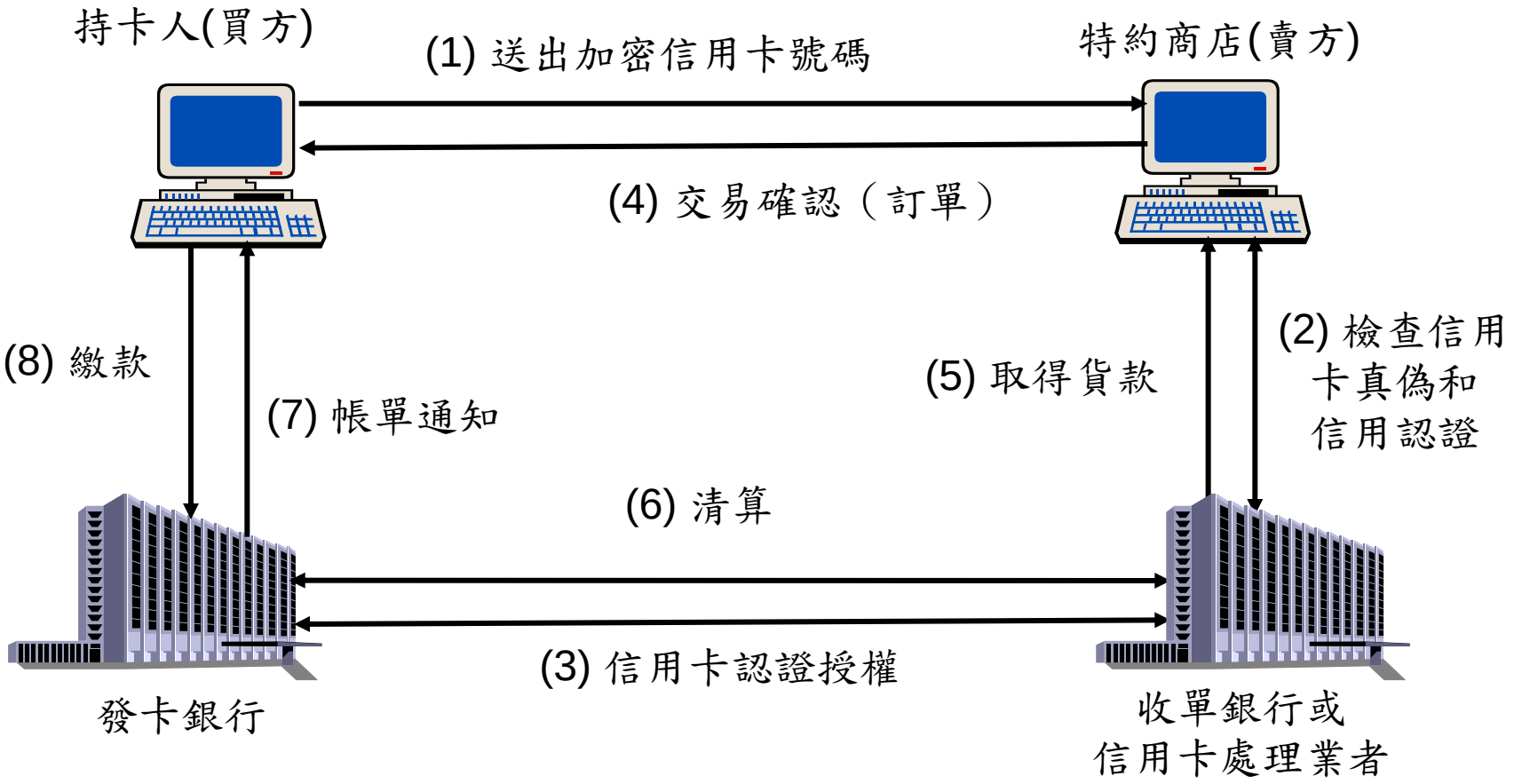
電子信用卡

- 以電子傳送的形式，使用信用卡進行線上交易的付款，亦稱線上信用卡
- 安全需求：
  - 確認持卡人、特約商店及其所屬銀行之身分
  - 保護持卡人與交易資料（卡號、有效期限、金額等）之正確性與機密性

作業過程

- 第一階段：消費交易
  1. 瀏覽選購
  2. 交易
  3. 授權
  4. 完成現階段交易
- 第二階段：商家請款
  5. 商家請款
  6. 銀行結算
- 第三階段：銀行收款
  7. 更新消費紀錄

交易流程圖


持卡人(買方)
(1) 送出加密信用卡號碼
特約商店(賣方)
(4) 交易確認（訂單）
(8) 繳款
(7) 帳單通知
(5) 取得貨款
(2) 檢查信用卡真偽和信用認證
(6) 清算
(3) 信用卡認證授權
發卡銀行
收單銀行或信用卡處理業者

發展過程

網路環境中，信用卡付款的發展過程分為三類型：

- 未加密的
  - 不需額外機制，方便但不安全
- 經過加密的，如：SSL技術
  - 網際網路最普遍使用的安全通訊協定
- 經過第三方認證的，如：SET技術
  - 被視為最佳解決方案，但機制複雜，不易推廣

SSL協定

- SSL協定：Secure Sockets Layer Protocol
- 網景（Netscape）公司於1994年提出
- 目的：提供網際網路上交易雙方安全保護，避免資料於傳輸過程中被截取、偽造與破壞
- 依憑證等級（40或128位元），對網際網路的資料傳輸進行加密
- 連線雙方以公開金鑰演算機制（如RSA）與電子憑證驗證對方身分

線上信用卡處理流程－SSL

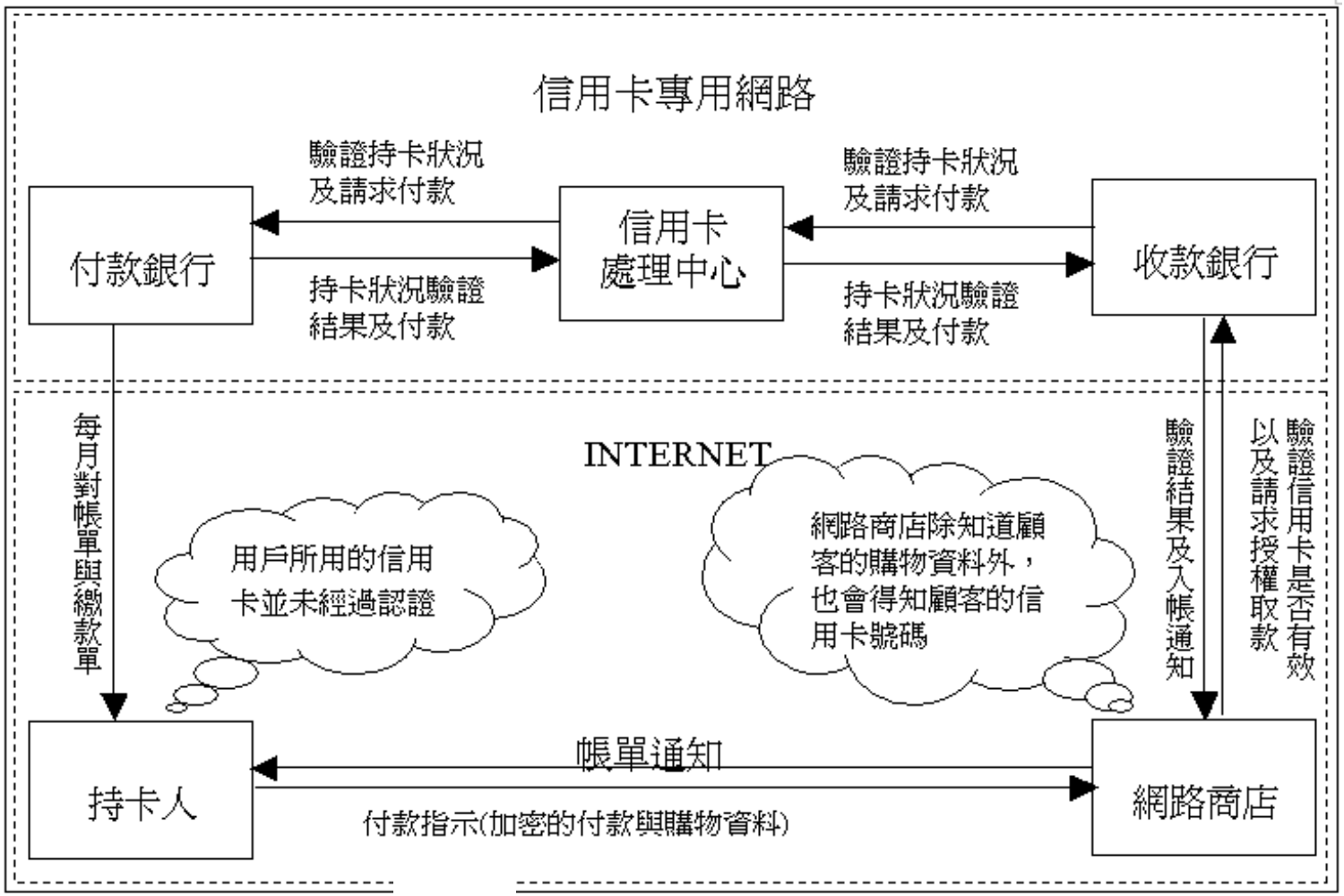


圖 13-6 SSL 線上信用卡處理流程

應用評價

- 優點：
  - 建置簡單，使用方便
  - 付款容易，不需額外申請或認證
  - 使用對稱式加密技術，可防範資料傳輸遭攔截
- 缺點
  - 特約商店可於交易過程得知所有資料
  - 缺少不可否認機制

Module 9-5：安全電子交易標準SET

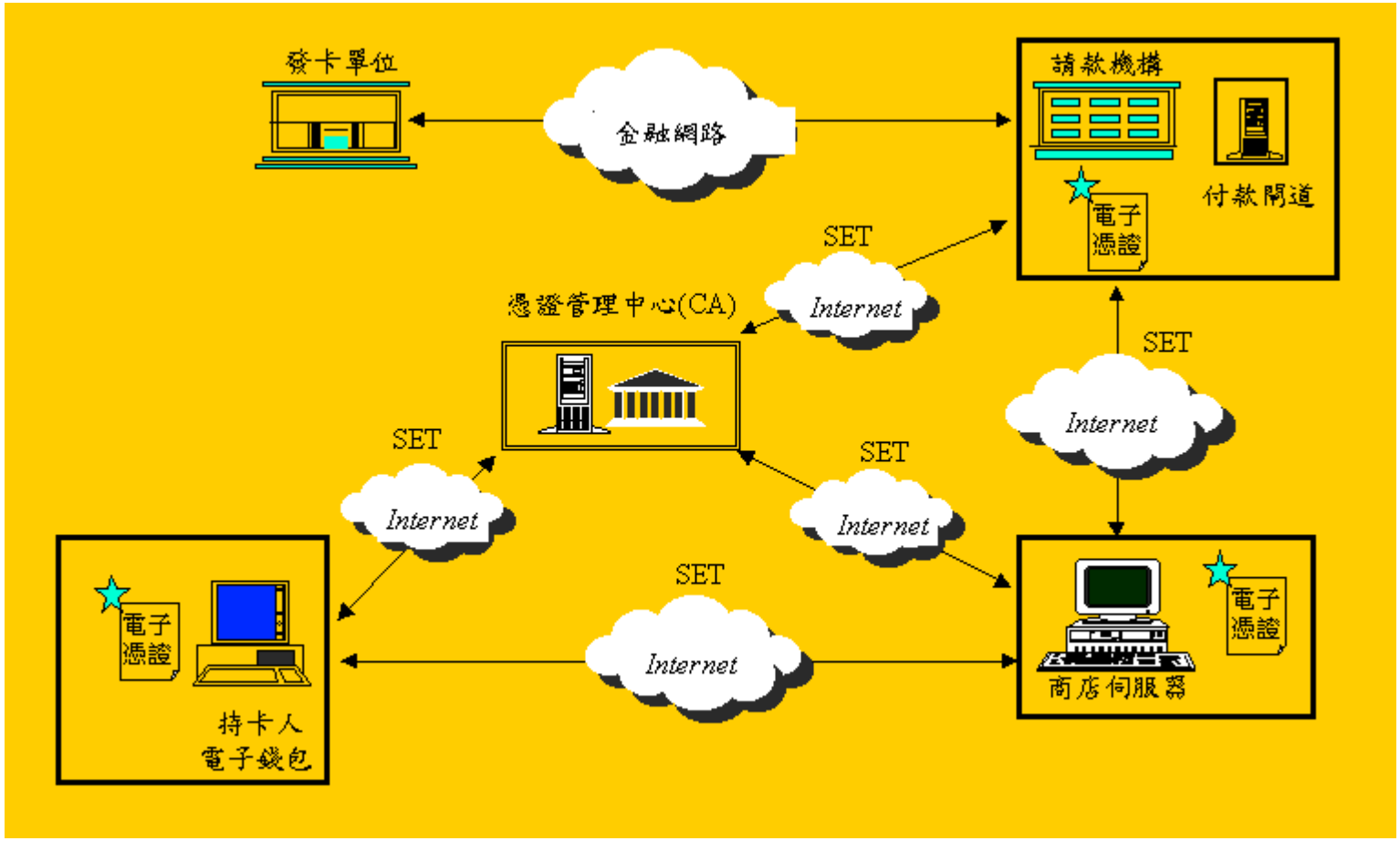
發展背景

- SET：Secure Electronic Transaction安全電子交易標準
- Visa和MasterCard兩大國際發卡組織為確保消費者在公眾網路上，能透過安全付款協定，安心使用信用卡進行交易，與IBM、HP、Microsoft等共同發起制定
- 1996年制定，1998年第一波產品上市
- 使用公開金鑰、訊息摘要與電子簽章等安全技術

主要元件

- 持卡人（Cardholder）
  - 使用含SET標準的電子錢包（Electronic Wallet）軟體儲存與管理電子憑證、密鑰與交易紀錄
- 特約商店（Merchant Server）
- 發卡機構（Issuer）
- 收單機構（Acquirer）
- 付款閘道（Payment Gateway）
  - 處理交易的付款訊息
- 憑證管理中心（Certificate Authority）
  - 可信賴之第三者，核發電子憑證，提供認證服務

系統架構圖


發卡單位
金融網路
請款機構
付款閘道
電子憑證
SET
Internet
憑證管理中心(CA)
SET
Internet
SET
Internet
SET
Internet
電子憑證
持卡人
電子錢包
SET
Internet
電子憑證
商店伺服器

安全需求與機制

- 確保訂單與付款資訊之機密性
  - 訊息加密
- 確保訂單與付款資訊於傳輸過程的完整性
  - 電子簽章
- 可驗證交易雙方（商店與持卡人）身分的合法性
  - 電子憑證與電子簽章
- 可在不同系統、軟體與網路之間相互運作
  - 明確的協定與訊息格式

交易處理流程

1. 持卡人登錄（Registration）
   - 持卡人向CA登錄，取得有效的電子憑證和SET協定所需的持卡人付款銀行資料

2. 特約商店登錄
   - 向CA登錄取得有效的電子憑證

交易處理流程(續)

3. 購物要求（Purchase Request）：採購
   - 持卡人送出交易要求訊息（含付款銀行名稱）
   - 特約商店簽章送出回應訊息，並提示商店與付款閘道的電子憑證
   - 持卡人簽章送出訂單資料(OI)與付款指示(PI)，其中PI與帳號資料經過加密，僅限付款閘道可解密讀取
   - 特約商店驗證OI正確性厚，進行付款認證程序，正確完成後寄送商品

交易處理流程(續)

4. 付款認證（Payment Authority）：授權
   - 特約商店針對交易識別碼與PI等交易資料，以電子信封（Digital Envelop）方式加密簽章，產生認證要求訊息，送交付款閘道
   - 付款閘道驗證確認PI資料與特約商店要求內容相符，再將要求轉送付款銀行處理
   - 付款銀行回覆後，付款閘道產生回覆訊息，將交易記錄符記（Capture Token）送交特約商店

交易處理流程(續)

5. 付款記錄（Payment Capture）：請款
   - 特約商店產生付款記錄要求訊息，送交付款閘道
   - 付款閘道產生付款要求訊息，經付款(收單)銀行向發卡銀行請款
   - 轉帳完成後，付款閘道產生記錄回覆訊息，送交特約商店

應用評價

- 優點：
  - 安全可靠，經由認證機制可增進信任感
  - 使用電子簽章與公開金鑰加密技術，防範資料遭攔截、窺探或竄改
  - 具備不可否認性，交易各方權責分明
- 缺點
  - 須架構於公開金鑰基礎架構（PKI）上，不易推展
  - 各方需額外申請憑證，過程繁瑣，成本提高
  - 交易過程涉及公開金鑰加密運算，效率較差

其他類似機制

- 信用卡國際組織為網路交易提供解決方案，強調持卡人、商家與發卡行三方的驗證
- 現有機制：
  - Visa：VbV (Verified by Visa)
  - MasterCard：SecureCode
  - JCB：J/Secure
- 發展現況：
  - 網路商家導入與消費者申辦皆不普遍
  - 密碼驗證機制不夠嚴謹，仍出現偽冒申辦案例

Module 9-6：智慧卡電子錢包

智慧卡

- 智慧卡：Smart Card，又稱IC卡或晶片卡
- 具備邏輯運算與資料儲存能力，可以處理多種應用內容
- 可線上或離線使用
- 應用類型：
  - 關係型智慧卡，如：會員卡、聯名卡
  - 電子錢包，如：悠遊卡、iCash

關係型智慧卡

- 由金融機構發行，加強原有卡片功能（如：金融卡、信用卡），增加服務項目，例如：
  - 存取多重帳號
  - 提供現金提存、資金轉移等多樣化功能
  - 可用於自動櫃員機（ATM）、個人電腦、雙向電視（機上盒）等多種設備
- 儲存持卡人姓名、生日、消費資料、購買紀錄等資訊，有助於商家規劃提供忠誠度（Loyalty）服務機制。

電子錢（電子貨幣）

- 其設計具流通貨幣的特性，但並非法定貨幣，接受度稍低
- 不需要實體存在的收(付)款人，可藉網路遠距零時差交易
- 交易成本低，適用於小額非線上的零售交易，取代支票或信用卡
- 衍生問題：
  - 不易防範偽造，只能加強監督管理或降低動機
  - 線上洗錢暢行無阻，電子錢的使用必須設限

電子貨幣產品

- 電子貨幣產品
  - 可儲值（Stored Value）或預付（Pre-paid）
  - 發行者以電、磁或光學形式，將傳統貨幣的相等價值儲存在消費者的電子裝置上
- 類型
  - 智慧卡（電子錢包）
  - 安裝於個人電腦的軟體產品
  - 以電子現金形式，用於網路購物小額支付

智慧卡電子錢包

- 電子錢包：Electronic Purse
  - 加值：持卡人利用自動櫃員機或其他加值機制，將錢存入電子錢包。
  - 付款：以讀卡機判讀電子錢包，扣減消費款項。
- 優勢：
  - 交易快速，適合小額付款
  - 可離線使用，適用於偏遠地區
  - 可提供消費之電子記錄
  - 不易遭複製冒用
- 應用：交通票證、電話、購物等

Module 9-7：晶片金融卡消費扣款

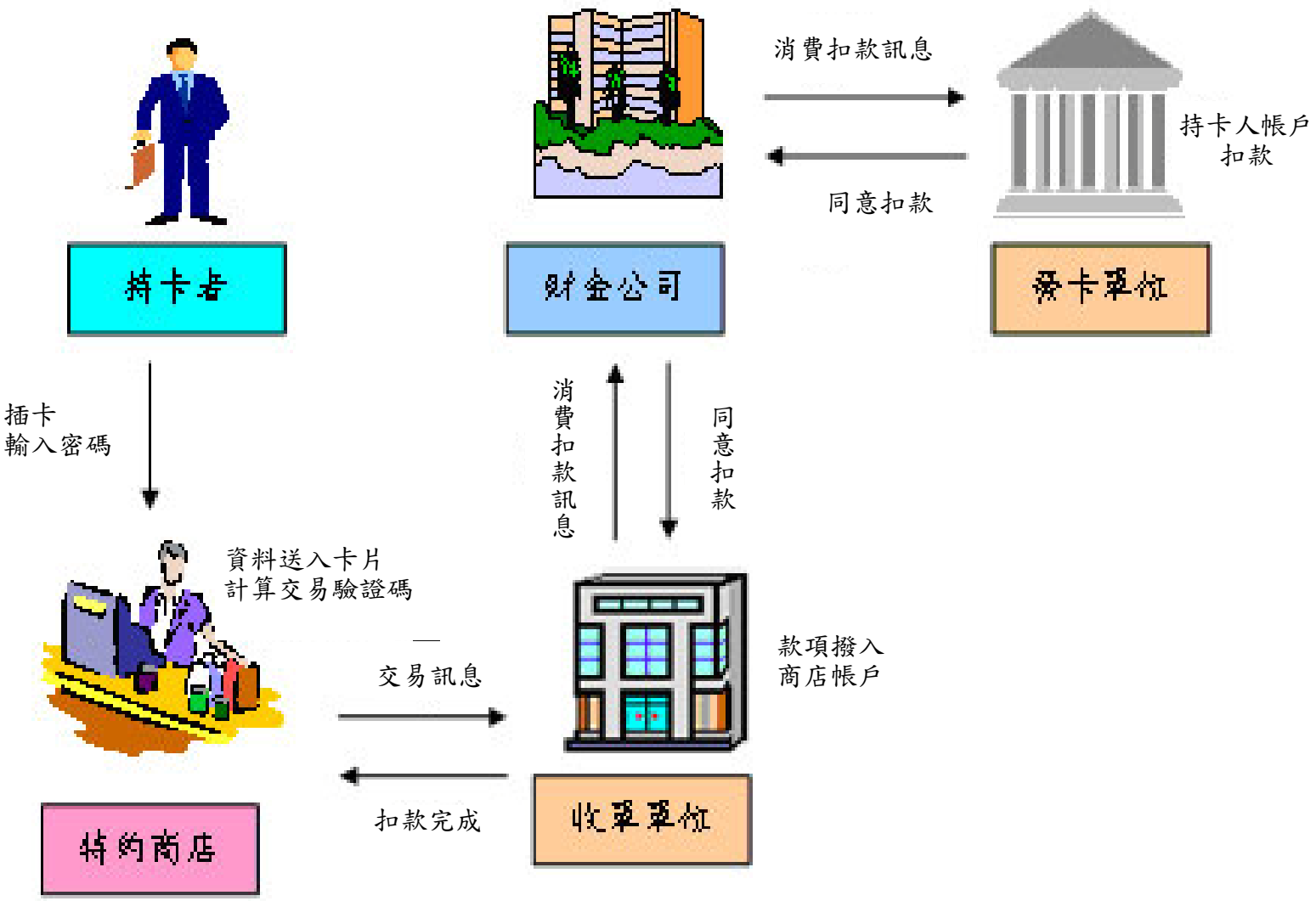
發展歷程

- 91年
  - 銀行公會完成晶片金融卡規格設計
  - 開始推動「磁條金融卡晶片化」專案
- 95年
  - 國內整體晶片金融卡基礎環境佈建完成
  - 取消磁條卡跨行交易
- 96年
  - 開辦晶片金融卡消費扣款作業

發展現況

- 至97年8月底止：
  - 發卡金融機構28家，可支援消費扣款業務之發卡量佔總發卡量約82.6%
  - 代理（收單）金融機構7家
  - 特約商店逾12000家
  - 每月交易金額突破一仟萬元，每筆平均交易金額約二仟元

交易處理流程


消費扣款訊息
持卡人帳戶
扣款
同意扣款
持卡者
財金公司
發卡單位
插卡
輸入密碼
消費扣款訊息
同意扣款
資料送入卡片
計算交易驗證碼
交易訊息
款項撥入
商店帳戶
扣款完成
特約商店
收單單位

應用特色

- 消費者確認交易內容後，直接以晶片金融卡付款
- 商家可即時銷帳，馬上出貨或提供服務
- 晶片金融卡可結合紅利回饋機制，配合商家推展儲值、集點等用途
- 利用網路ATM，可提供安全便利的網際網路付款機制
- 提昇商家效率、降低金流成本、且無呆帳風險

參考資料

- **電子商務安全技術與應用**，林祝興、張真誠著，旗標出版股份有限公司，民國93年9月初版
- **電子商務安全**，吳宗成教授主編，行政院國家科學委員會科學技術資料中心，民國92年12月
- **電子商務安全**，張真誠、江季翰，科學月刊352期，1999年4月
- **財金資訊雙月刊**，第50期，2007年2月
- **財金資訊季刊**，第58期，2008年9月

References

- 教育部顧問室編輯 “電子商務安全”教材
- Turban et al., Introduction to Electronic Commerce, Third Edition, 2010, Pearson