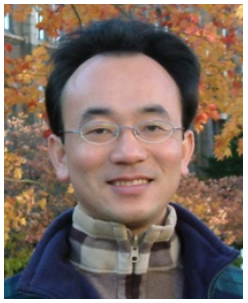
Tamkang University

Electronic Commerce: Transaction Security
(電子商務交易安全)

時間：2014/7/03　(四) 14：00~17：00
地點：精誠資訊股份有限公司R0111會議室
(地址：台北市內湖區瑞光路318號1樓)



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. tku.edu.tw/myday/

2014-07-03

SYSTEX | DATA We Monetize Data, 用IT創新數據價值

消費者交易行為分析
(Consumer Facing Transaction)

Source: http://www.systex.com.tw/

Outline

1. ISO 27001 資訊安全管理系統介紹
   (ISO 27007 Information Security Management System)
2. 電子商務安全架構
   (Electronic Commerce Security Framework)
3. 交易安全
   (Transaction Security)
4. 電子支付系統
   (Electronic Payment System)
5. 行動商務安全
   (Mobile Commerce Security)

ISO 27001
資訊安全管理系統
(Information Security Management System, ISMS)

- 資訊安全管理系統 (Information Security Management System, ISMS)
  - 整體管理系統的一部分， 以營運風險導向(作法)為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全。
    - 備考： 管理系統包括組織架構、政策、規劃活動、責任、實務、程序、過程及資源。
- Information Security Management System (ISMS)
  - that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
    - NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Source: ISO/IEC 27001:2005, CNS 27001

資訊安全 (information security)

- 資訊安全 (information security)
  - 保存資訊的機密性、完整性及可用性；此外， 亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質。
    [CNS 17799]
- information security
  - preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
    [ISO/IEC 17799:2005]

Source: ISO/IEC 27001:2005, CNS 27001

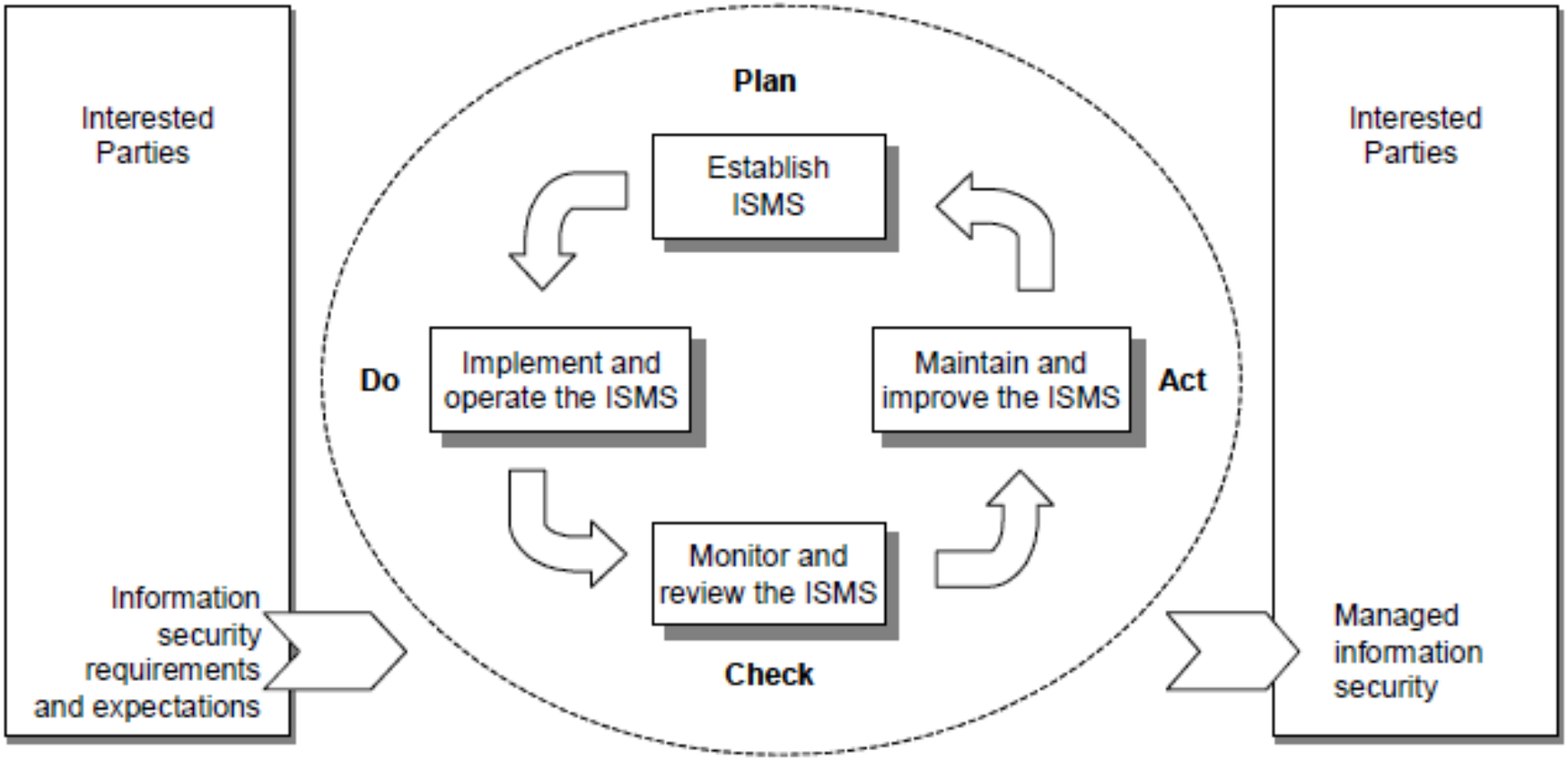
Information Security (CIA)

- Confidentiality (機密性)
- Integrity (完整性)
- Availability (可用性)

- Authenticity (鑑別性)
- Accountability (可歸責性)
- Non-repudiation (不可否認性)
- Reliability (可靠度)

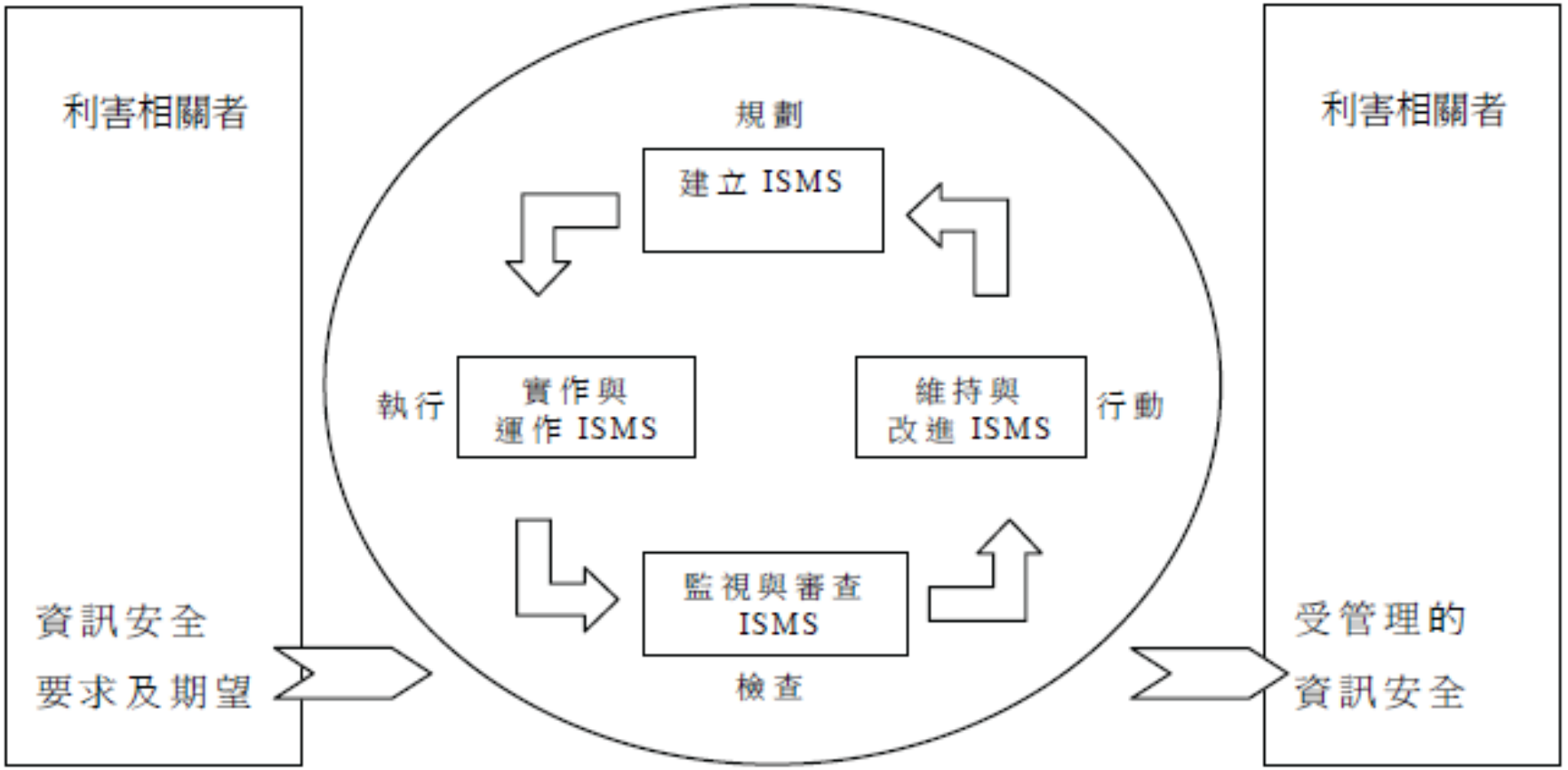
Source: ISO/IEC 27001:2005, CNS 27001

PDCA model applied to ISMS processes



Source: ISO/IEC 27001:2005

適用於 ISMS 過程之PDCA 模型



Source: CNS 27001

ISO 27001 Annex A (normative)
附錄A (規定)

- 11 個控制領域 (附錄A.5 - A.15)
- 39 個控制目標
- 133 項控制措施

- ISO/IEC 17799:2005 Clauses 5 to 15 provide implementation advice and guidance on best practice in support of the controls specified in A.5 to A.15.
- CNS 17799 第5 節至第15 節提供支援本附錄A.5 至A.15 所列各項控制措施之最佳實務的實作建議與指導。

Source: ISO/IEC 27001:2005, CNS 27001

ISO 27001 附錄 A.5-A.15

- A.5 安全政策
- A.6 資訊安全的組織
- A.7 資產管理
- A.8 人力資源安全
- A.9 實體與環境安全
- A.10 通訊與作業管理
- A.11 存取控制
- A.12 資訊系統獲取、開發及維護
- A.13 資訊安全事故管理
- A.14 營運持續管理
- A.15 遵循性

Source: ISO 27001, CNS 27001

ISO 27001:2005 A.10 通訊與作業管理 (Communications and operations management)

- A.10.1 作業之程序與責任 (Operational procedures and responsibilities)
- A.10.2 第三方服務交付管理 (Third party service delivery management)
- A.10.3 系統規劃與驗收 (System planning and acceptance)
- A.10.4 防範惡意碼與行動碼 (Protection against malicious and mobile code)
- A.10.5 備份 (Back-up)
- A.10.6 網路安全管理 (Network security management)
- A.10.7 媒體的處置 (Media handling)
- A.10.8 資訊交換 (Exchange of information)
- A.10.9 電子商務服務 (Electronic commerce services)
- A.10.10 監視 (Monitoring)

Source: ISO 27001, CNS 27001

通訊與作業管理

- A.10 通訊與作業管理
  - A.10.6 網路安全管理
    - 目標： 確保對網路內資訊與支援性基礎建設的保護。
  - A.10.7 媒體的處置
    - 目標： 防止資產被未經授權的揭露、修改、移除或破壞， 以及營運活動的中斷。
  - A.10.8 資訊交換
    - 目標： 維護組織內及與任何外部個體所交換資訊與軟體的安全。
  - A.10.9 電子商務服務
    - 目標： 確保電子商務服務的安全性及其安全的使用。
  - A.10.10 監視
    - 目標： 偵測未經授權的資訊處理活動。

Source: ISO 27001, CNS 27001

A.10.9 電子商務服務

目標： 確保電子商務服務的安全性及其安全的使用。

- A.10.9.1 電子商務
- A.10.9.2 線上交易
- A.10.9.3 公眾可用的資訊

A.10.9.1 電子商務

- 控制措施
  - 應保護在公眾網路上傳輸而涉及電子商務的資訊，
    使不受詐欺行為、
    契約爭議及未經授權的揭露與修改。

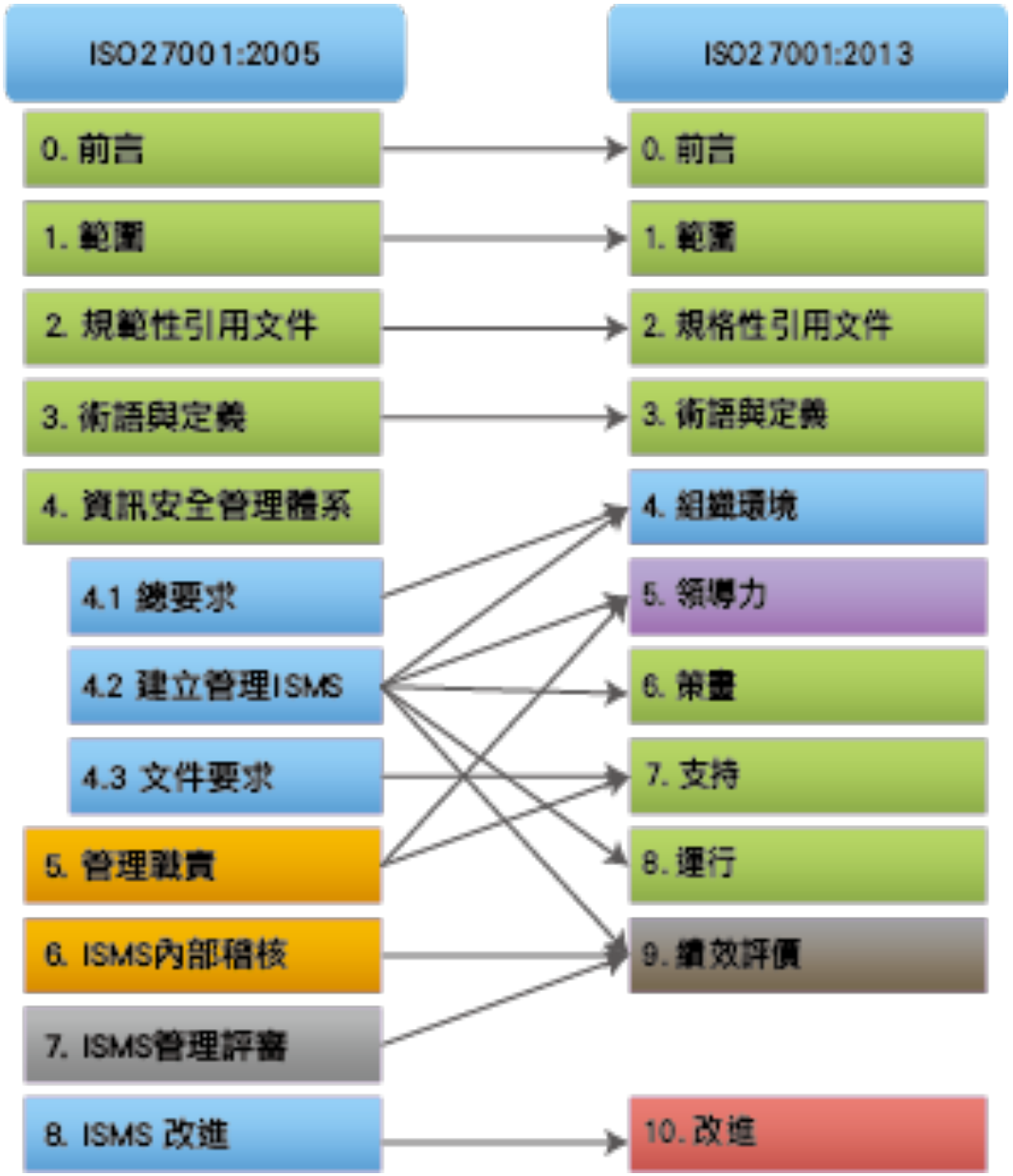
A.10.9.2 線上交易

- 控制措施
  - 應保護涉及線上交易的資訊，
    以防止不完整的傳輸、
    錯誤路由(mis-routing)、
    未經授權的訊息修改、
    未經授權的揭露、
    未經授權的訊息複製或重演。

A.10.9.3 公眾可用的資訊

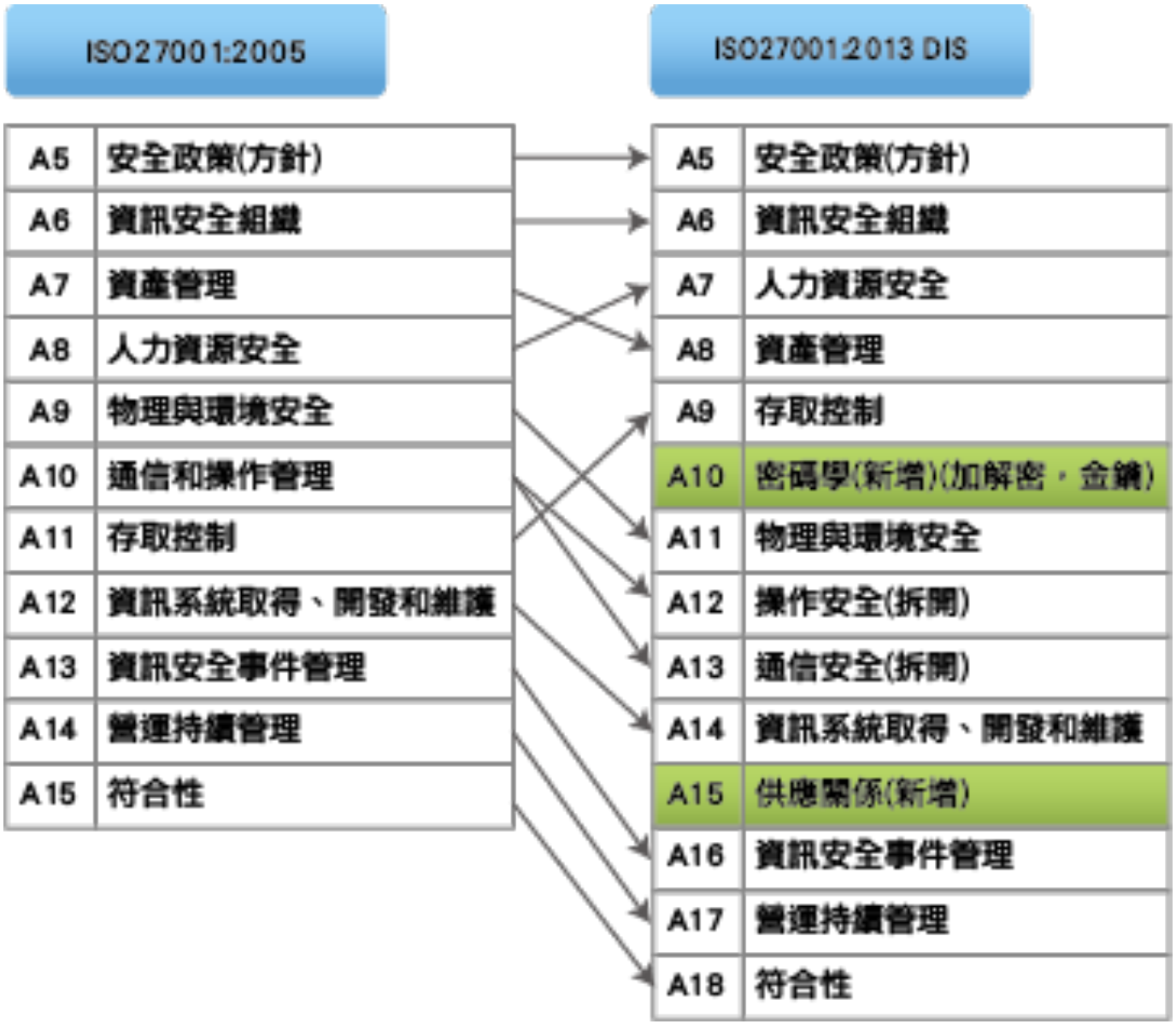
- 控制措施
  - 應保護公眾可用系統上可取得資訊的完整性，以防止未經授權的修改。

ISO27001:2005 → ISO27001:2013



Source: http://www.fineart-tech.com/index.php/ch/home-2/90-fineart-express/coverstory/394-coverstory-2014-q2-1

ISO27001:2013 14領域變化圖



Source: http://www.fineart-tech.com/index.php/ch/home-2/90-fineart-express/coverstory/394-coverstory-2014-q2-1

ISO 27001:2005 →ISO 27001:2013
Annex A (normative)
附錄A (規定)

- 11 個控制領域 ➔ 14
- 39 個控制目標 ➔ 35
- 133 項控制措施 ➔ 114

Source: ISO/IEC 27001:2013

ISO/IEC 27001:2013整合圖

Source: http://www.fineart-tech.com/index.php/ch/home-2/90-fineart-express/coverstory/394-coverstory-2014-q2-1

ISO27001 ISMS
資訊安全管理系統與電子商務

ISO27001:2005	ISO27001:2013
A.10.9.1 Electronic commerce	A.14.1.2 Securing applications services on public networks
A.10.9.2 Online-transactions	A.14.1.3 Protecting application services transactions

Source: http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf

ISO 27001:2013
6.1.3
Information security risk treatment
(Annex A
Control Objectives and Controls)
(附錄A
控制目標與控制措施)

Source: ISO/IEC 27001:2013

A14.1 Security requirements of information systems

- **Objective**:
  To ensure that **information security** is an integral part of information systems across the entire lifecycle.
  This also include the requirements for information systems which provide services over public networks.

ISO/IEC 27001:2013

- A.14
  System acquisition, development and maintenance
  - A14.1
    Security requirements of information systems
    - A14.1.1 Information security requirements analysis and specification
    - A14.1.2 Securing application services on public networks (ISO27001:2005 A.10.9.1 Electronic commerce)
    - A14.1.3 Protecting application services transactions (ISO27001:2005 A.10.9.2 Online-transactions)

Source: ISO/IEC 27001:2013

ISO27001:2013
A14.1.2
Securing application services
on **public networks**
(ISO27001:2005
A.10.9.1
Electronic commerce)

ISO27001:2013
A14.1.3
Protecting application services
transactions
(ISO27001:2005
A.10.9.2
Online-transactions)

ISO27001:2013
A14.1.2

Securing application services on **public networks** (Electronic commerce)

Control:

Information involved in application services **passing over public networks shall be protected** from fraudulent activity, contract dispute and unauthorized disclosure and modification.

Source: ISO/IEC 27001:2013

ISO27001:2013
A14.1.3

Protecting application services **transactions** (Online-transactions)

Control:

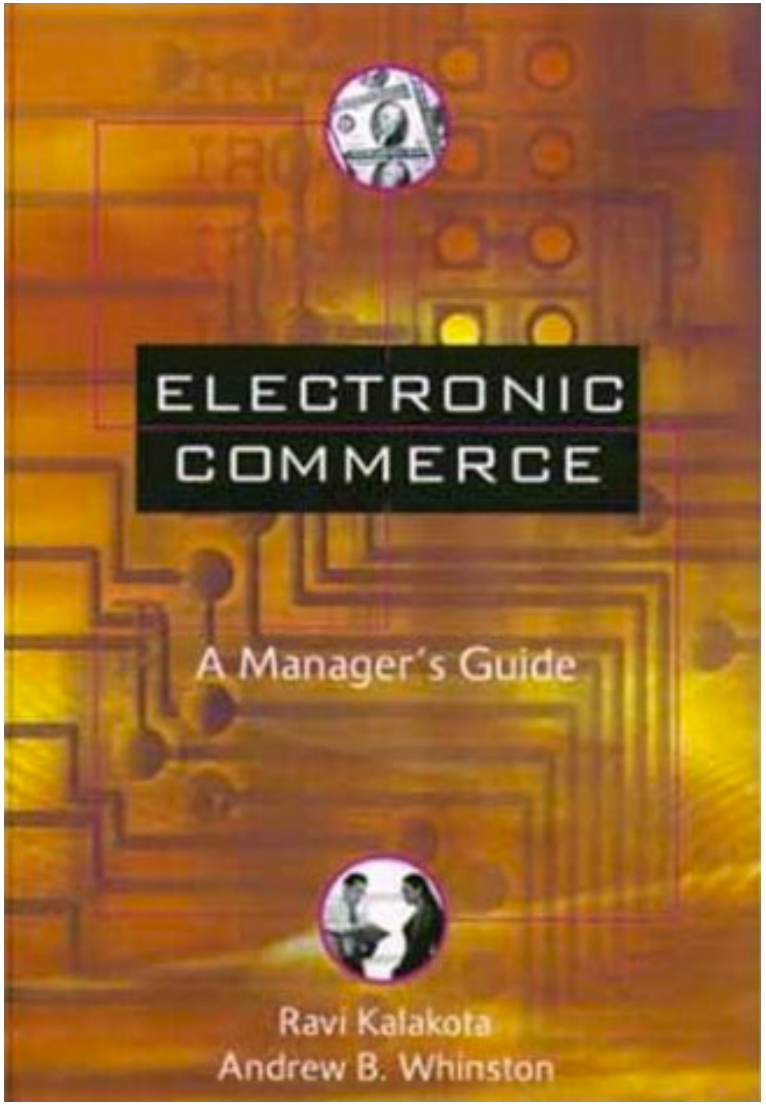
Information involved in application service **transactions shall be protected** to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Source: ISO/IEC 27001:2013

Outline

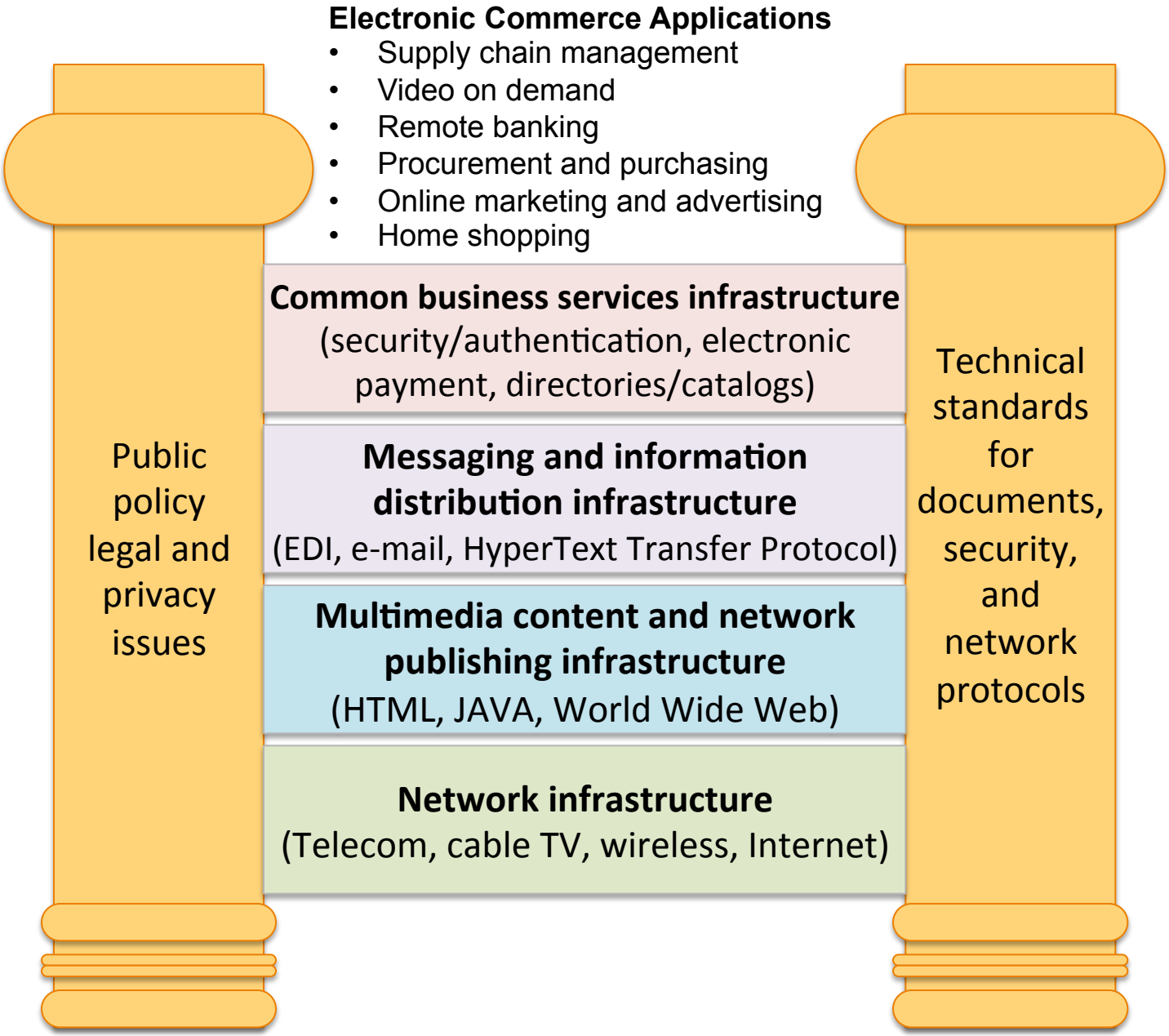
1. ISO 27001 資訊安全管理系統介紹
   (ISO 27007 Information Security Management System)
2. 電子商務安全架構
   (Electronic Commerce Security Framework)
3. 交易安全
   (Transaction Security)
4. 電子支付系統
   (Electronic Payment System)
5. 行動商務安全
   (Mobile Commerce Security)

Ravi Kalakota & Andrew B. Whinston (1997), Electronic Commerce: A Manager's Guide, Addison-Wesley



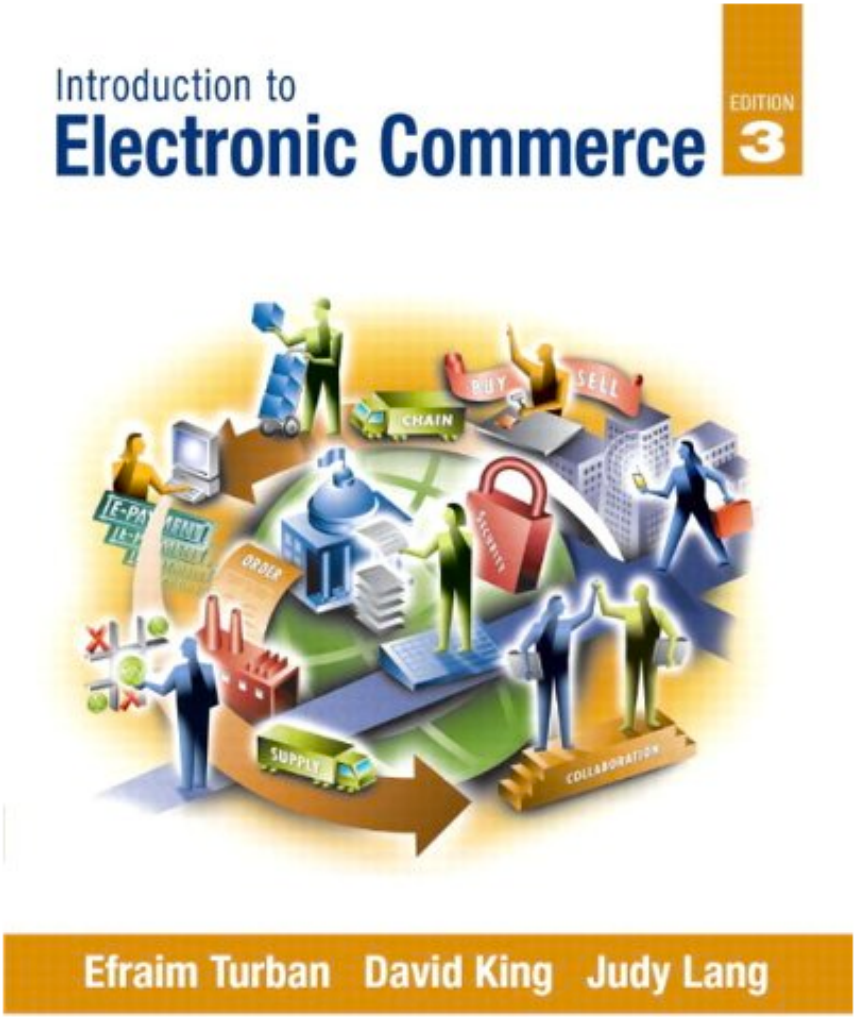
Source: http://www.amazon.com/Electronic-Commerce-A-Managers-Guide/dp/0201880679

Generic Framework for Electronic Commerce



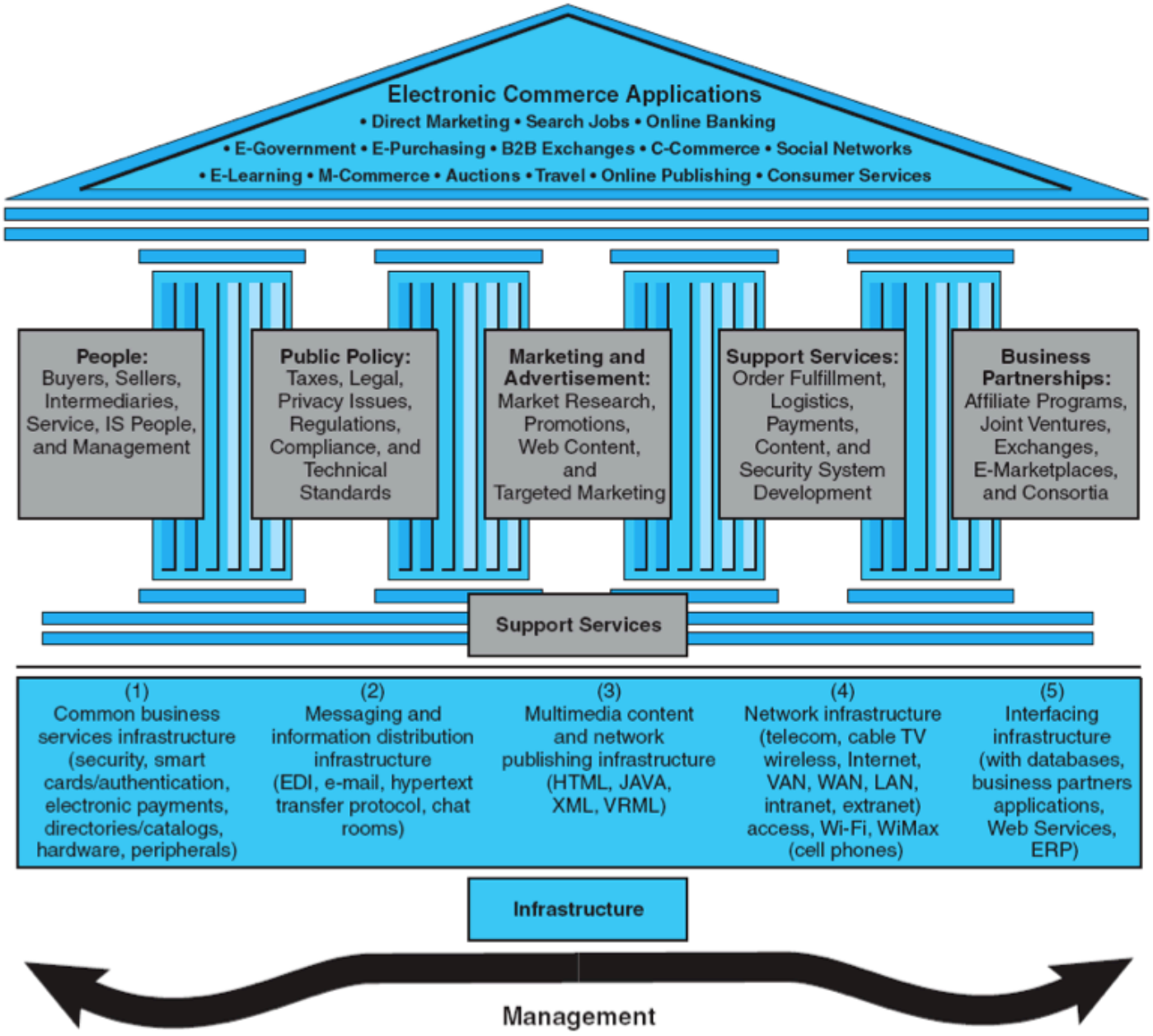
Source: Ravi Kalakota & Andrew B. Whinston (1997), Electronic Commerce: A Manager's Guide, Addison-Wesley Professional

Turban et al. (2010),
Introduction to Electronic Commerce,
Third Edition, Pearson



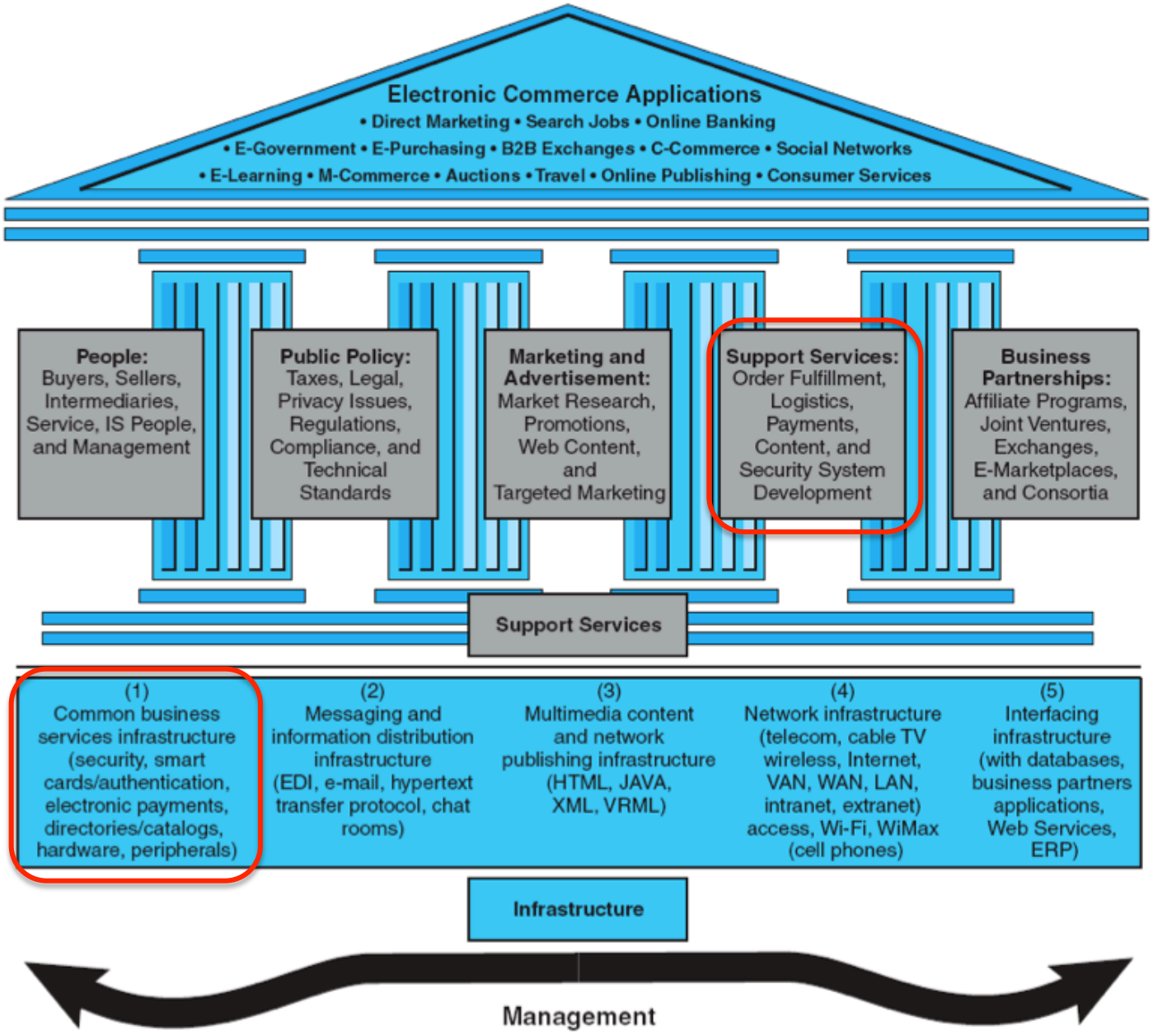
Source: http://www.amazon.com/Introduction-Electronic-Commerce-Business-Resources/dp/0136109233

A Framework for Electronic Commerce



Source: Turban et al. (2010),Introduction to Electronic Commerce, Third Edition, Pearson

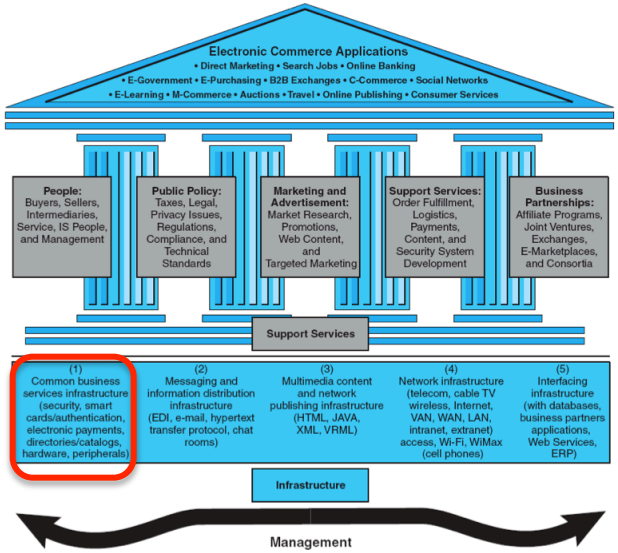
A Framework for Electronic Commerce



Source: Turban et al. (2010),Introduction to Electronic Commerce, Third Edition, Pearson

EC Infrastructure (1)

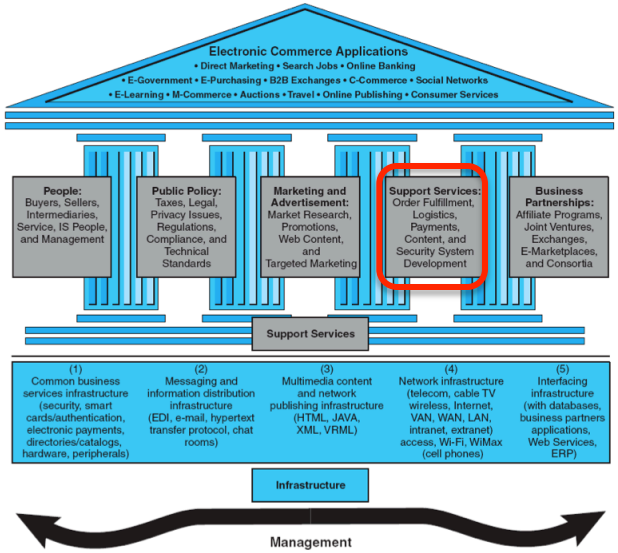
- Common business services infrastructure
  - (security, smart cards/authentication, electronic payments, directories/catalogs, hardware, peripherals)



Source: Turban et al. (2010),Introduction to Electronic Commerce, Third Edition, Pearson

EC
Support Services

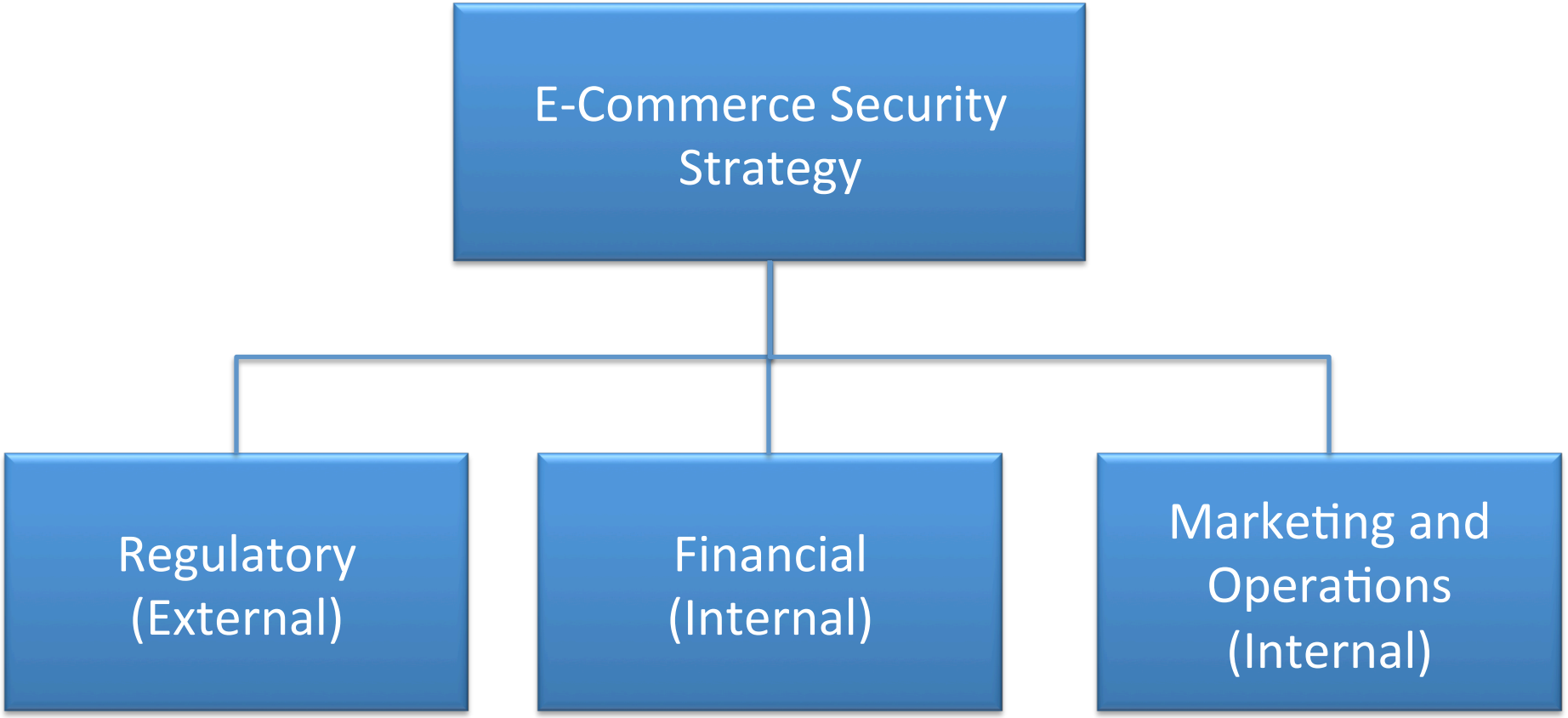
- Order Fulfillment
- Logistics
- Payments
- Content
- Security System Development



Source: Turban et al. (2010),Introduction to Electronic Commerce, Third Edition, Pearson

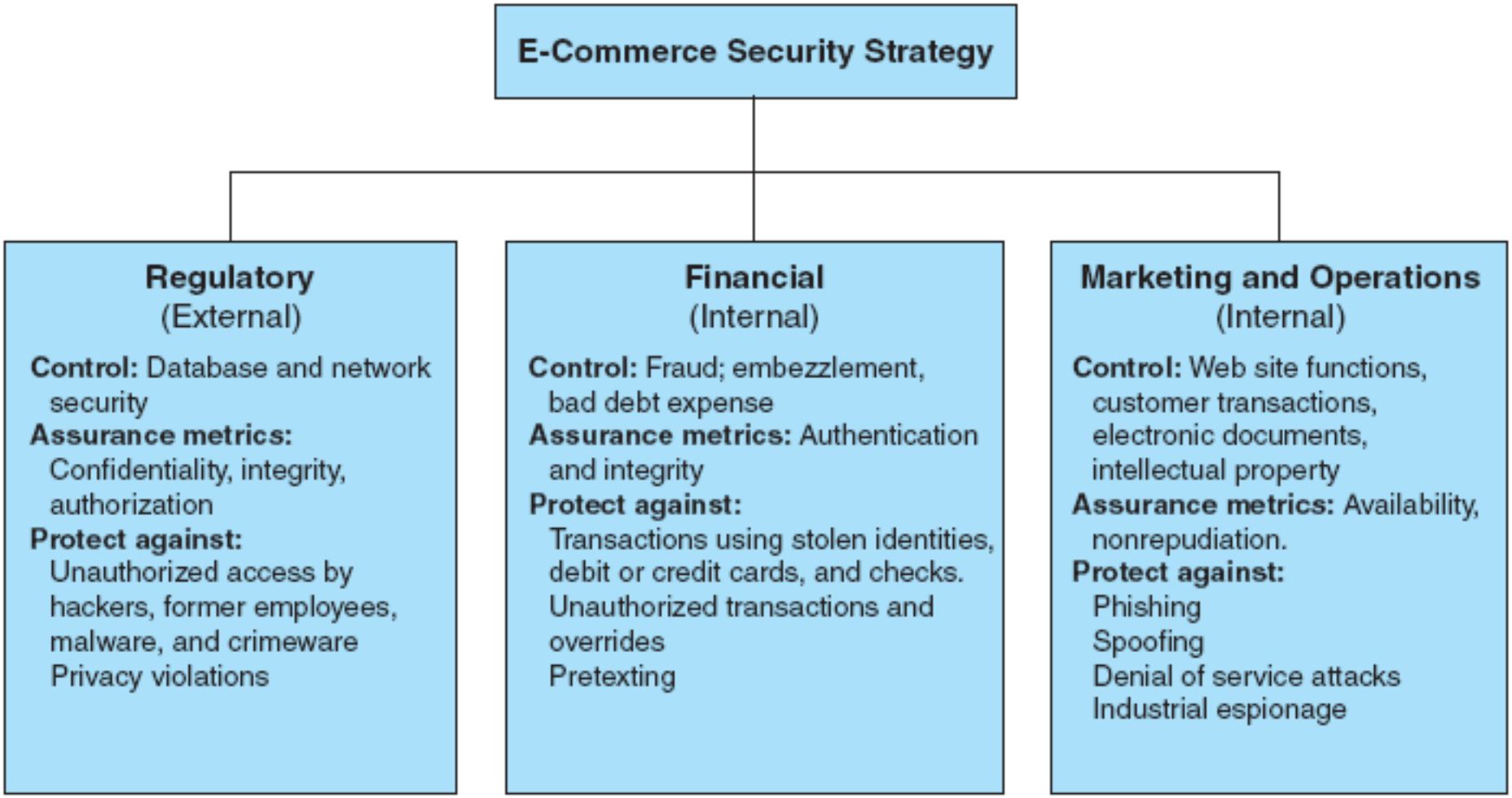
E-Commerce Security and Fraud Protection

E-Commerce Security Framework



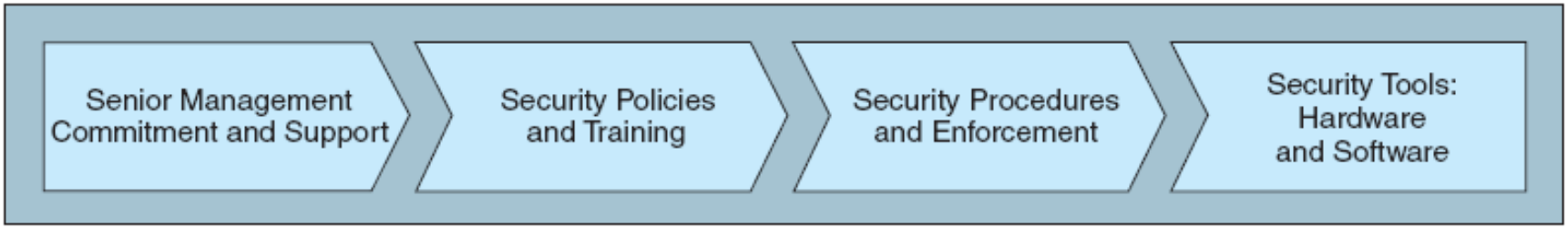
Source: Turban et al. (2010),Introduction to Electronic Commerce, Third Edition, Pearson

E-Commerce Security Framework



Source: Turban et al. (2010),Introduction to Electronic Commerce, Third Edition, Pearson

Enterprise-wide EC Security and Privacy Model



Source: Turban et al. (2010),Introduction to Electronic Commerce, Third Edition, Pearson

Outline

1. ISO 27001 資訊安全管理系統介紹
   (ISO 27007 Information Security Management System)
2. 電子商務安全架構
   (Electronic Commerce Security Framework)
3. 交易安全
   (Transaction Security)
4. 電子支付系統
   (Electronic Payment System)
5. 行動商務安全
   (Mobile Commerce Security)

交易 (Transaction)
支付 (Payment)

交易安全 (Transaction Security)
支付安全 (Payment Security)

交易安全 (Transaction Security)

- 不可否認服務
  (Non-repudiation Service)
- 安全標章
  (Security Seal)

不可否認服務
(Non-repudiation Service)

可提供交易的證據，
以解決交易所產生的糾紛。

不可否認服務
(Non-repudiation Service)

- 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。

不可否認服務
(Non-repudiation Service)

- 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
(Non-repudiation Service)

- 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)。

不可否認證據 (Non-repudiation Evidence)

- 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：
  - 安全信封 (Secure envelope)
    - 由證據產生機構(evidence generating authority)使用對稱密碼技術所產生
  - 數位簽章 (Digital signatures)
    - 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

不可否認服務需求
(Non-repudiation Service Requirements)

- 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。

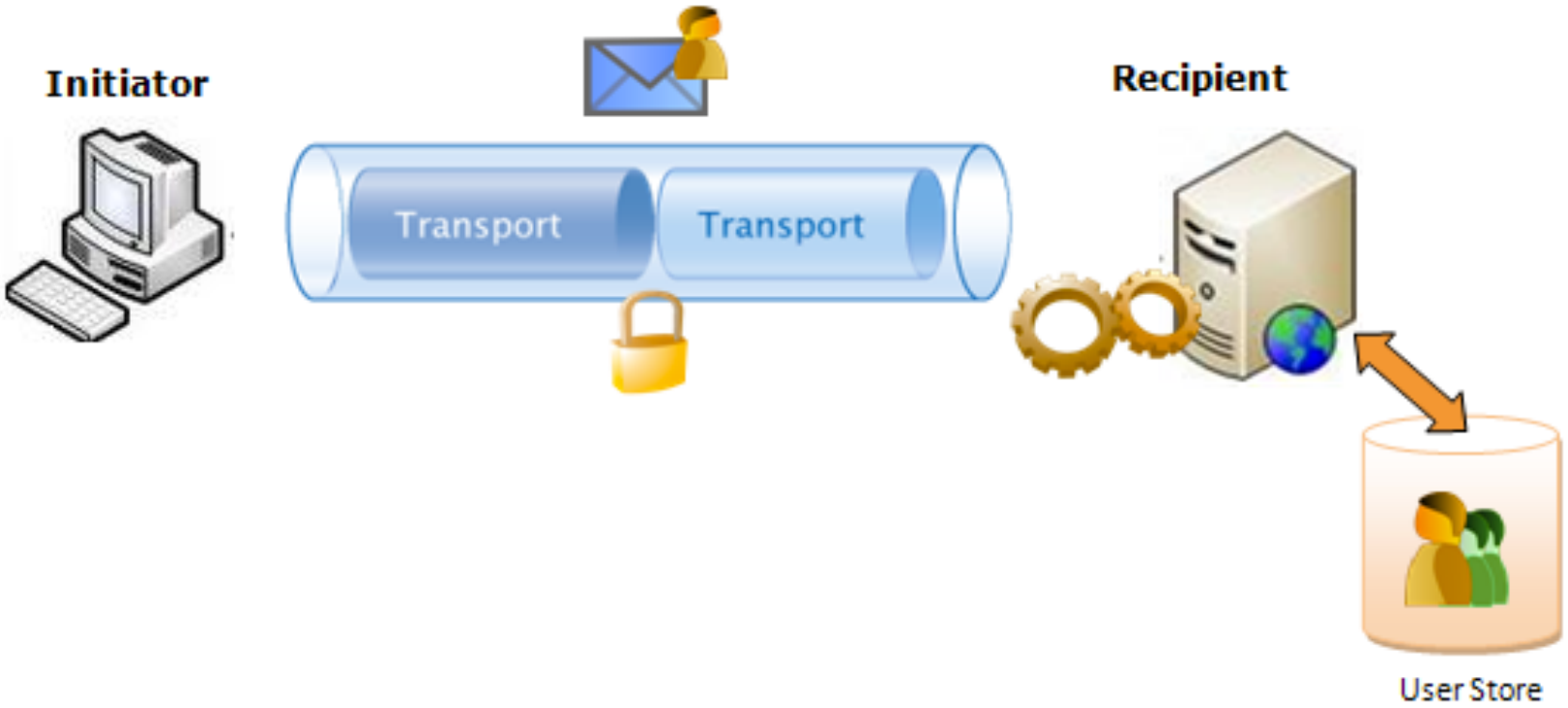
不可否認服務需求
(Non-repudiation Service Requirements)

- 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。

不可否認服務類型
(Types of Non-repudiation Service)

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

UsernameToken over HTTPS

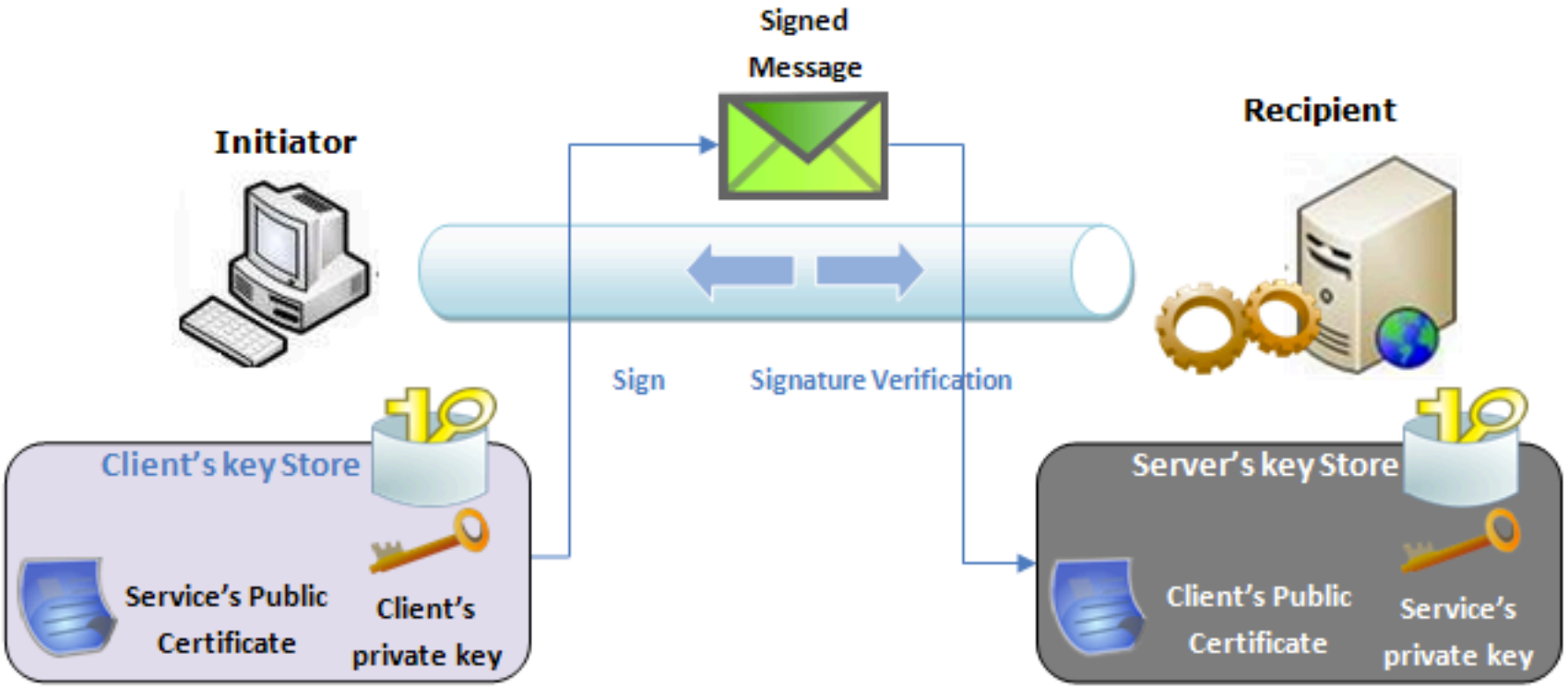


Username Token over HTTPS

Message is secured at the Transport level; Username Token is used for authentication. Client sends the Username Token inside the message which is validated against the entries in user store of the service's end.

Source: http://docs.wso2.com/display/DSS263/Graphical+View+of+the+Default+Security+Scenarios

Non-Repudiation



Non-repudiation Scenario

Clients should have X.509 certificates and Messages are signed using the private key of the sender and verified using the public key of the signing party

Source: http://docs.wso2.com/display/DSS263/Graphical+View+of+the+Default+Security+Scenarios

安全標章
(Security Seal)

- 線上安全認證標章
- 信賴標章

線上安全認證標章

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

Source: 教育部顧問室編輯 “電子商務安全”教材

信賴標章 (Trust Seal)

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

Source: 教育部顧問室編輯 “電子商務安全”教材

信賴標章 (Trust Seal)

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

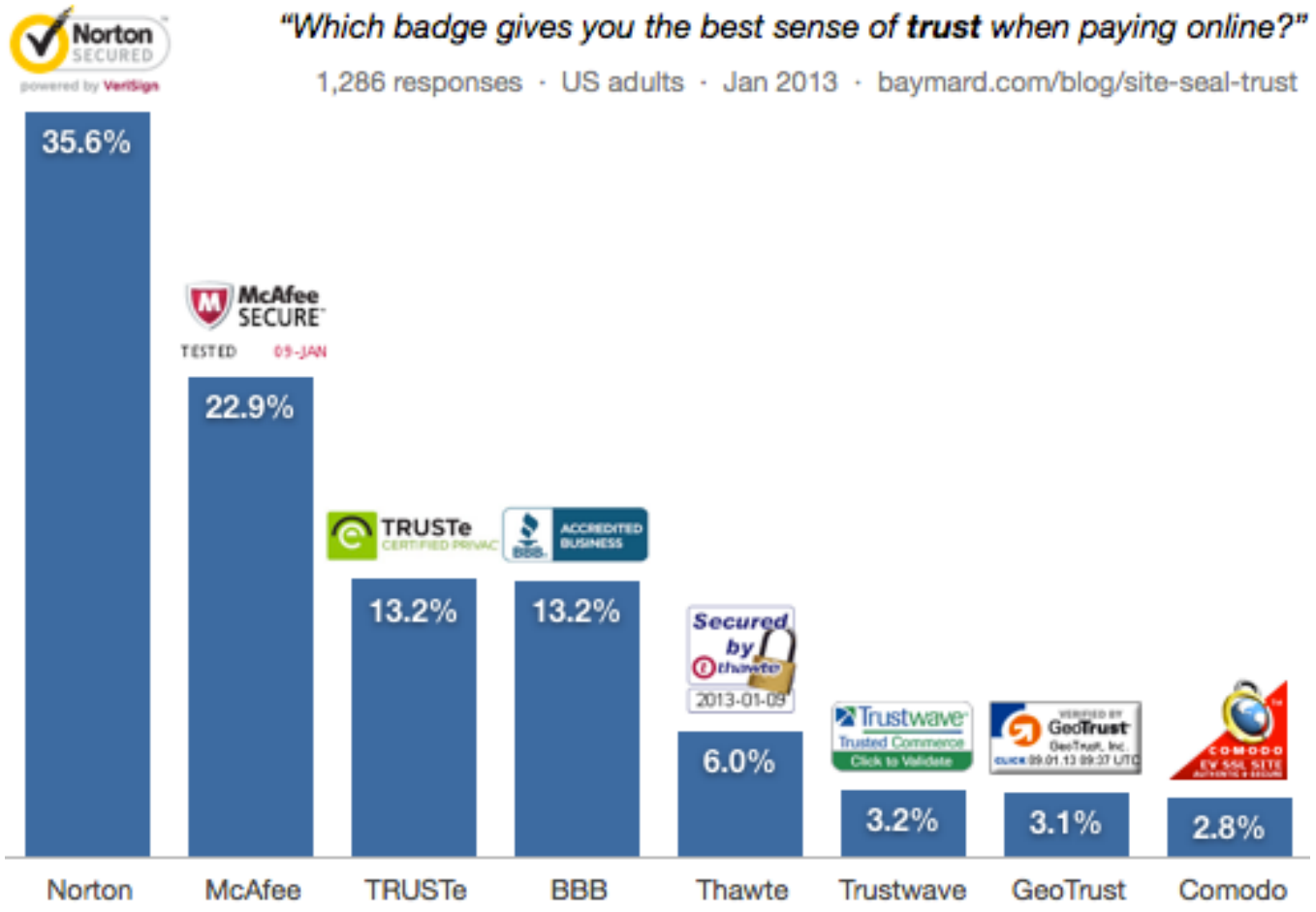
Source: 教育部顧問室編輯 “電子商務安全”教材

信賴標章 (Trust Seal)

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

Source: 教育部顧問室編輯 “電子商務安全”教材

Which Site Seal do People Trust the Most? (2013 Survey Results)



Source: http://baymard.com/blog/site-seal-trust

Outline

1. ISO 27001 資訊安全管理系統介紹
   (ISO 27007 Information Security Management System)
2. 電子商務安全架構
   (Electronic Commerce Security Framework)
3. 交易安全
   (Transaction Security)
4. 電子支付系統
   (Electronic Payment System)
5. 行動商務安全
   (Mobile Commerce Security)

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
  - 第三方支付

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

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

電子信用卡

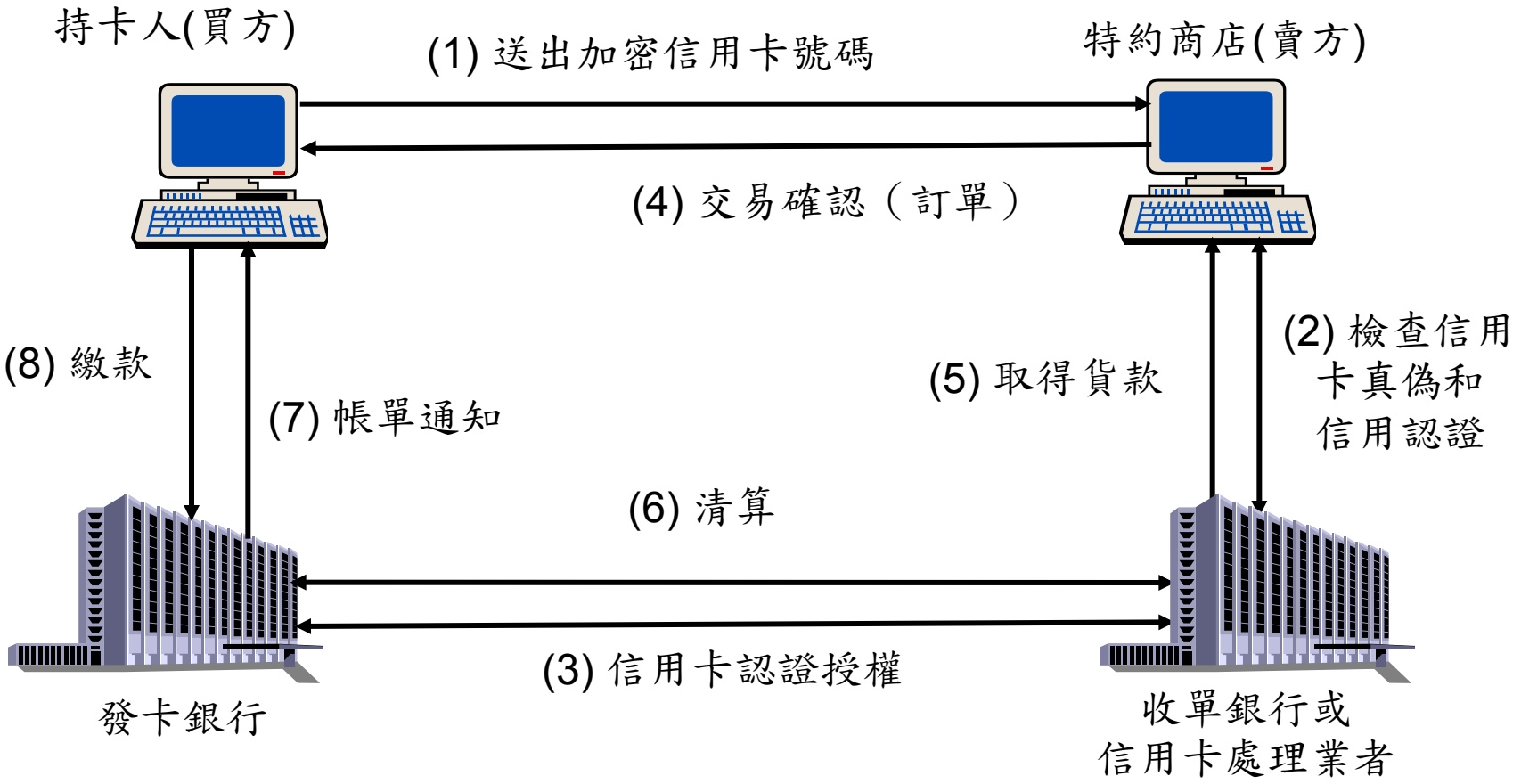
電子信用卡

- 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

信用卡作業過程

- 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

信用卡交易流程圖


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

信用卡付款發展過程

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

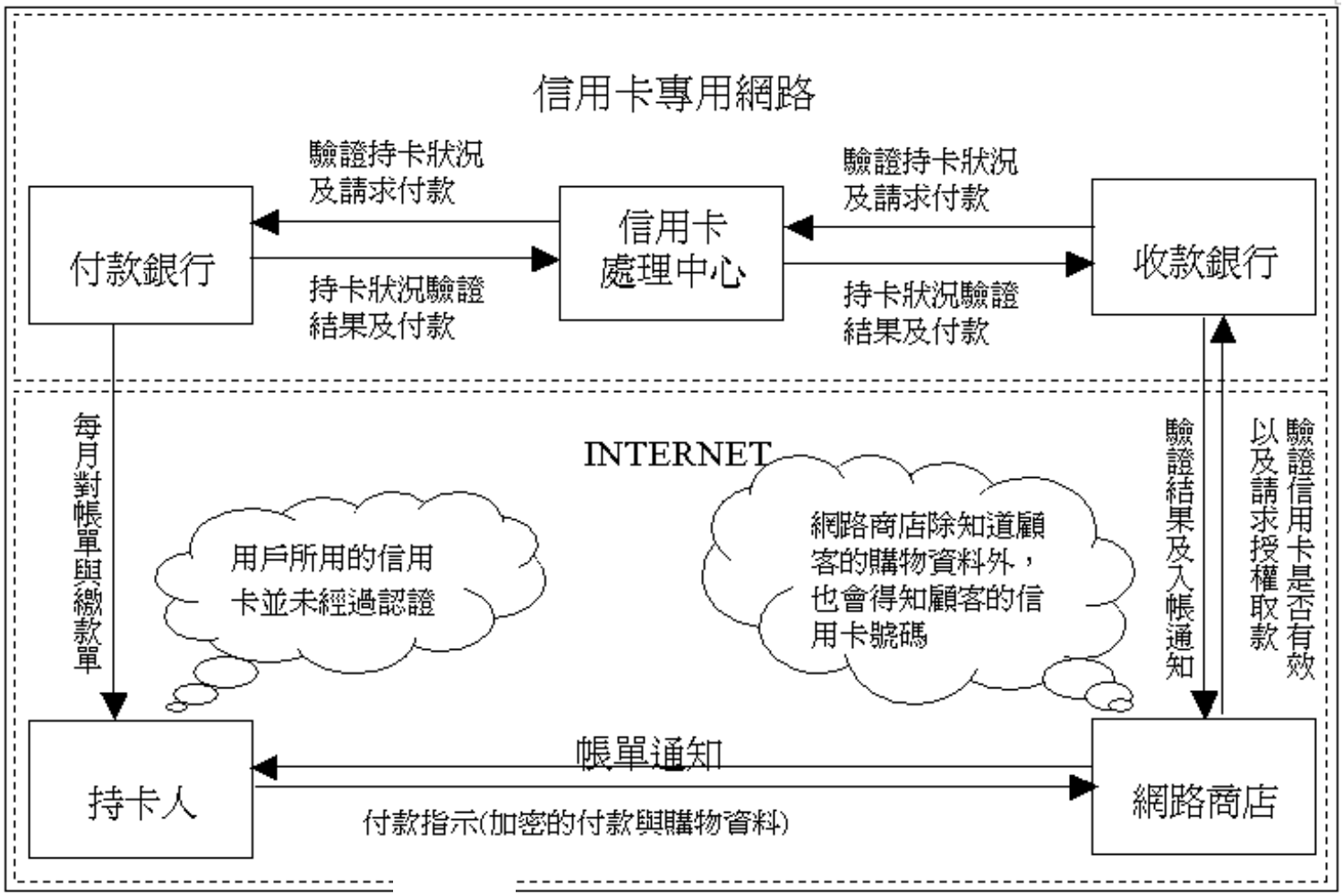


圖 13-6 SSL 線上信用卡處理流程

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

安全電子交易標準SET

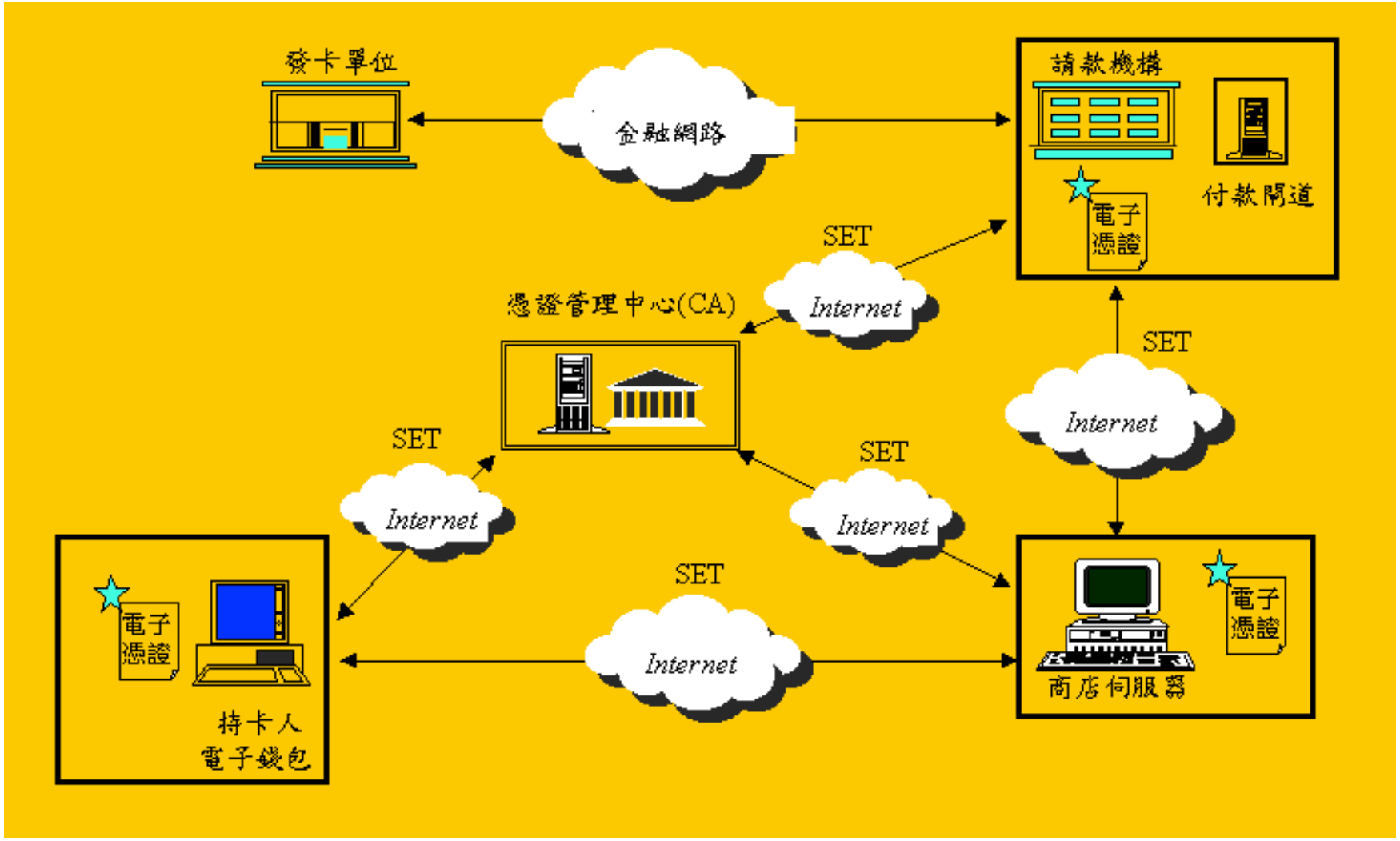
SET 發展背景

- 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

SET 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

SET 系統架構圖



Source: 教育部顧問室編輯 “電子商務安全”教材

SET 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

SET 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

SET 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，進行付款認證程序，正確完成後寄送商品

SET 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

SET 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

SET 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

SET 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

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

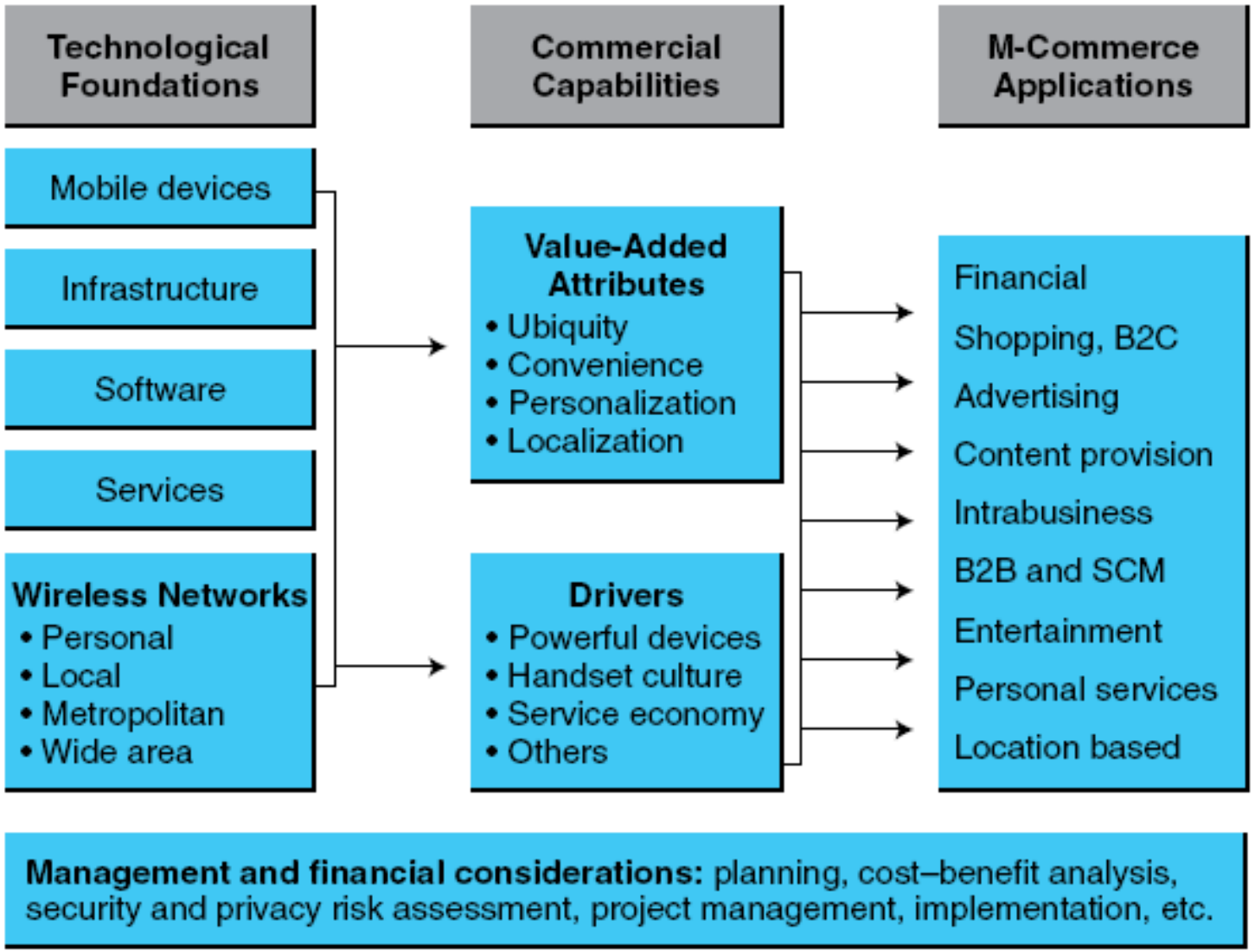
Outline

1. ISO 27001 資訊安全管理系統介紹
   (ISO 27007 Information Security Management System)
2. 電子商務安全架構
   (Electronic Commerce Security Framework)
3. 交易安全
   (Transaction Security)
4. 電子支付系統
   (Electronic Payment System)
5. 行動商務安全
   (Mobile Commerce Security)

Mobile Commerce (m-commerce or m-business)

Any business activity conducted over a wireless telecommunications network
or
from mobile devices.

EXHIBIT 8.1 The Mobile Commerce Landscape



Source: Turban et al. (2010),Introduction to Electronic Commerce, Third Edition, Pearson

Attributes of M-Commerce

- Ubiquity
- Convenience
- Interactivity
- Personalization
- Localization

Source: Turban et al. (2010),Introduction to Electronic Commerce, Third Edition, Pearson

Mobile Computing (wireless mobile computing)

Computing that connects a mobile device to a network or another computing device, anytime, anywhere.

Mobile Financial Applications

- **Mobile Banking**
- **Mobile Payments**

Mobile Marketing Campaigns

1. Information (資訊)
2. Entertainment (娛樂)
3. Raffles (抽獎)
4. Coupons (優惠卷)

Mobile Marketing and Advertising

1. Building brand awareness
2. Changing brand image
3. Promoting sales
4. Enhancing brand loyalty
5. Building customer databases
6. Stimulating mobile word of mouth

A day with NFC technology

A day with NFC technology

Source: https://www.youtube.com/watch?v=_64mAcOn444

A day with NFC technology

Source: https://www.youtube.com/watch?v=_64mAcOn444

A day with NFC technology

Source: https://www.youtube.com/watch?v=_64mAcOn444

A day with NFC technology

Source: https://www.youtube.com/watch?v=_64mAcOn444

A day with NFC technology

Source: https://www.youtube.com/watch?v=_64mAcOn444

A day with NFC technology

Source: https://www.youtube.com/watch?v=_64mAcOn444

Mobile Security Threats

- Toll Fraud
  (話費詐欺)
- Ransomware
  (勒索軟體)
- Mobile Payments via NFC
  (NFC 行動支付)

Source: http://mcommerce-explorer.blogspot.tw/2013/03/top-5-mobile-security-threats-2013.html

Toll Fraud

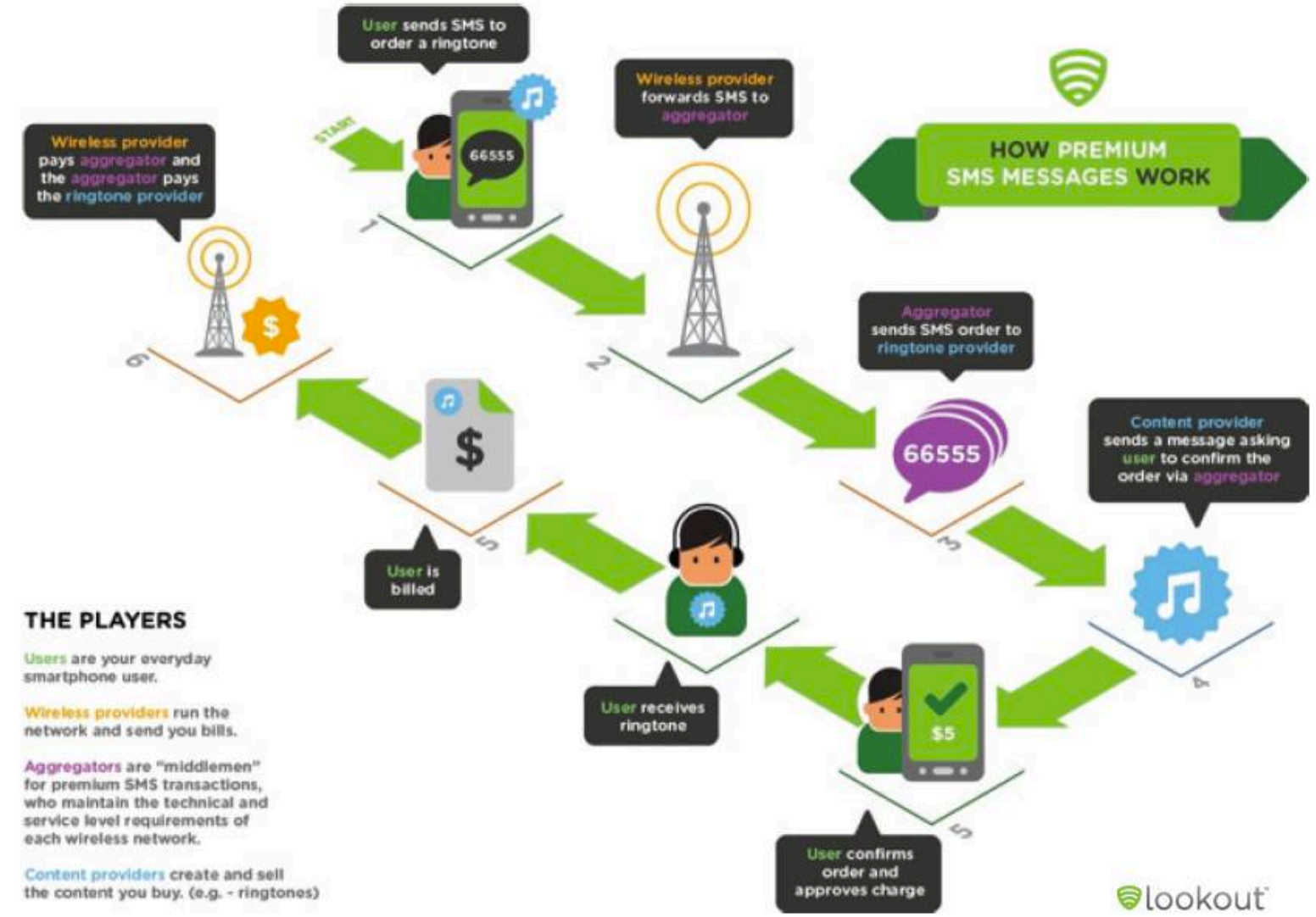


FIGURE 7: HOW PREMIUM SMS WORKS

Source: http://mcommerce-explorer.blogspot.tw/2013/03/top-5-mobile-security-threats-2013.html

Toll Fraud

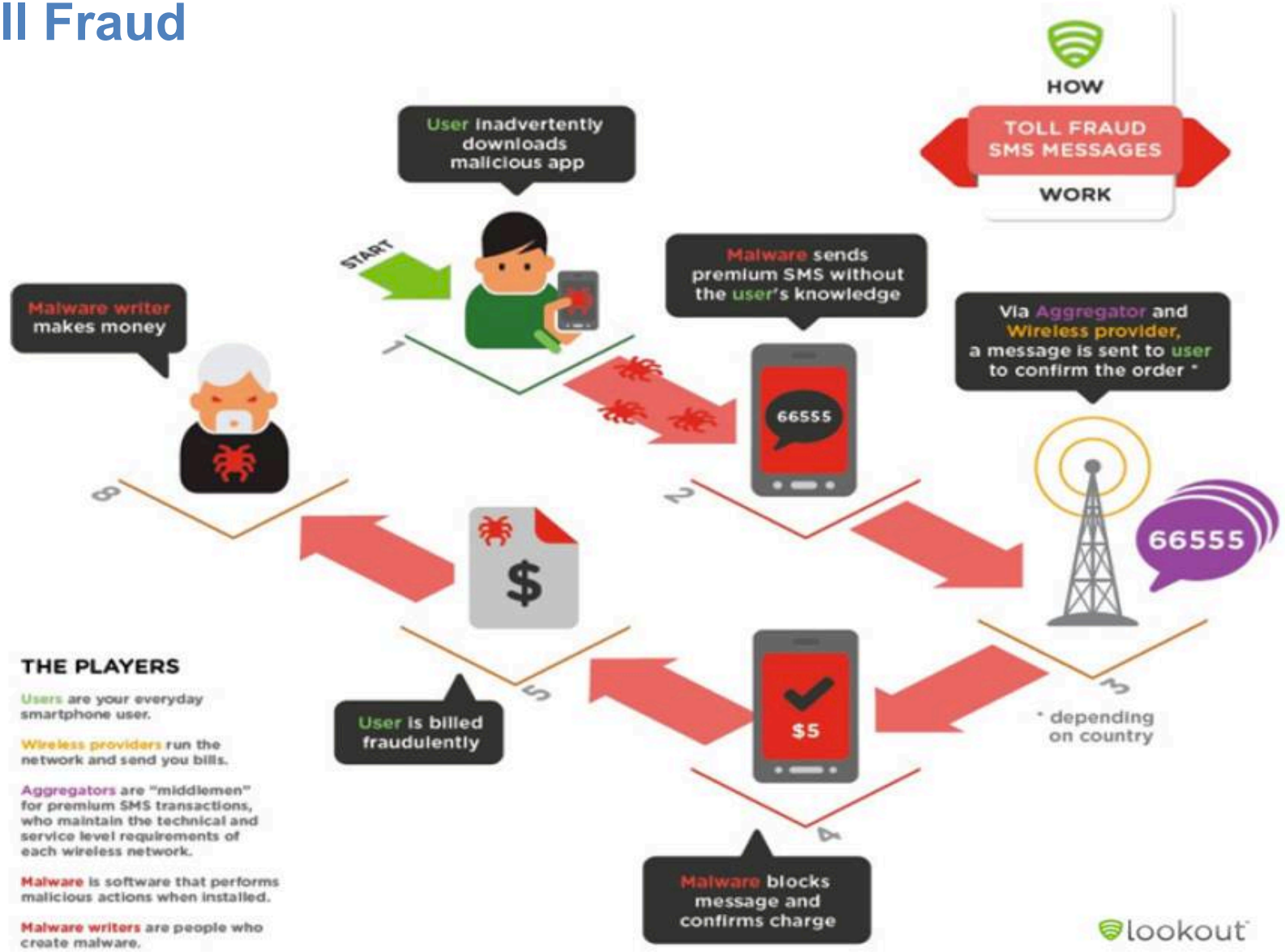
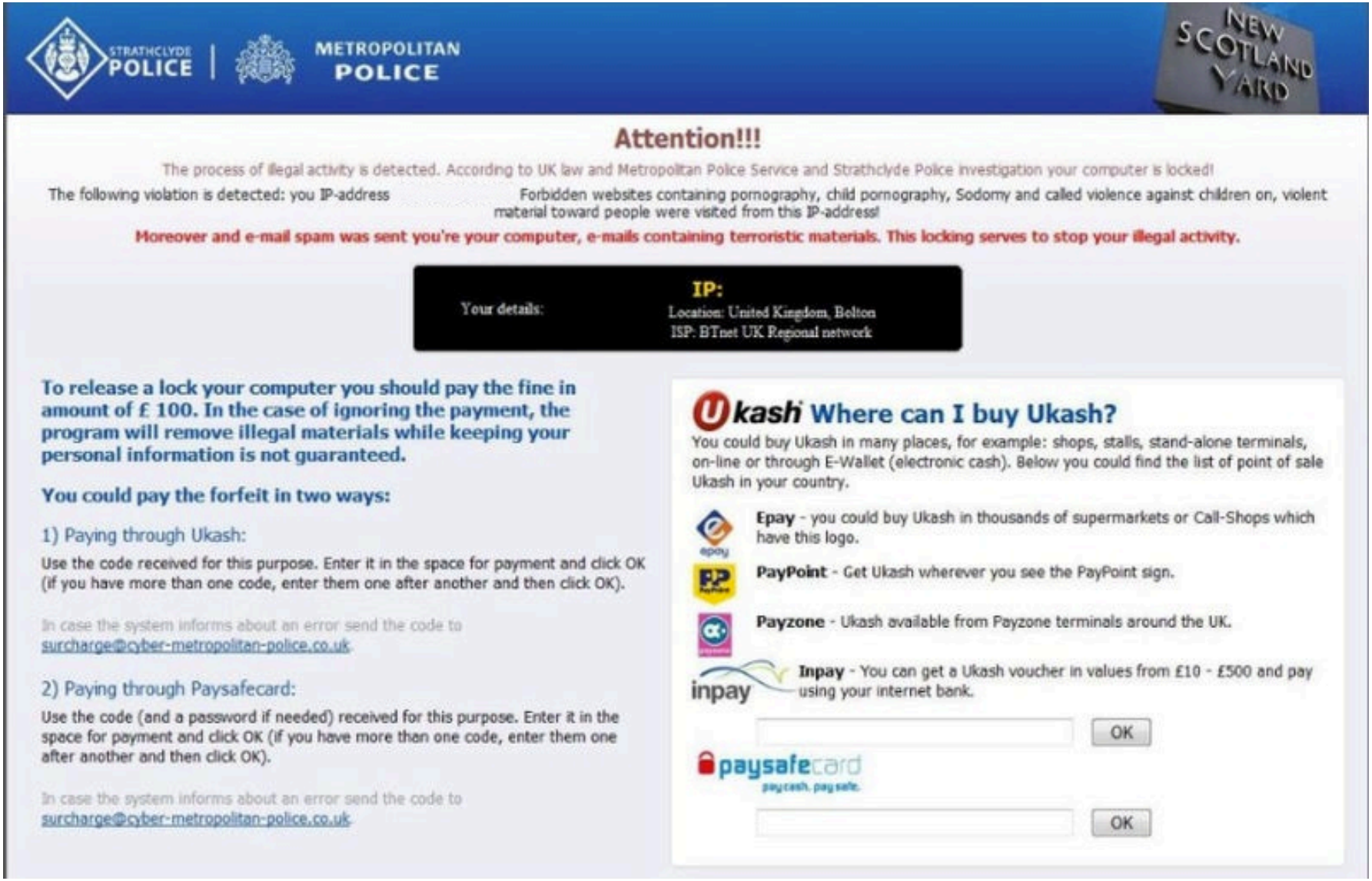


FIGURE 8: HOW TOLL FRAUD MALWARE WORKS

Source: http://mcommerce-explorer.blogspot.tw/2013/03/top-5-mobile-security-threats-2013.html

Ransomware



Source: http://en.wikipedia.org/wiki/Ransomware

Ransomware

Source: http://www.pcworld.com/article/2032767/ransomware-boosts-credibility-by-reading-victims-browsers.html

Mobile Payments via NFC

- steal your money via the classic "bump and infect" method, this means that NFC is actually acting as enabler for theft.

Source: http://mcommerce-explorer.blogspot.tw/2013/03/top-5-mobile-security-threats-2013.html

Mobile Payments Security

Source: http://www.mobilecommercepress.com/merchants-becoming-conscious-mobile-payments-security/8511441/

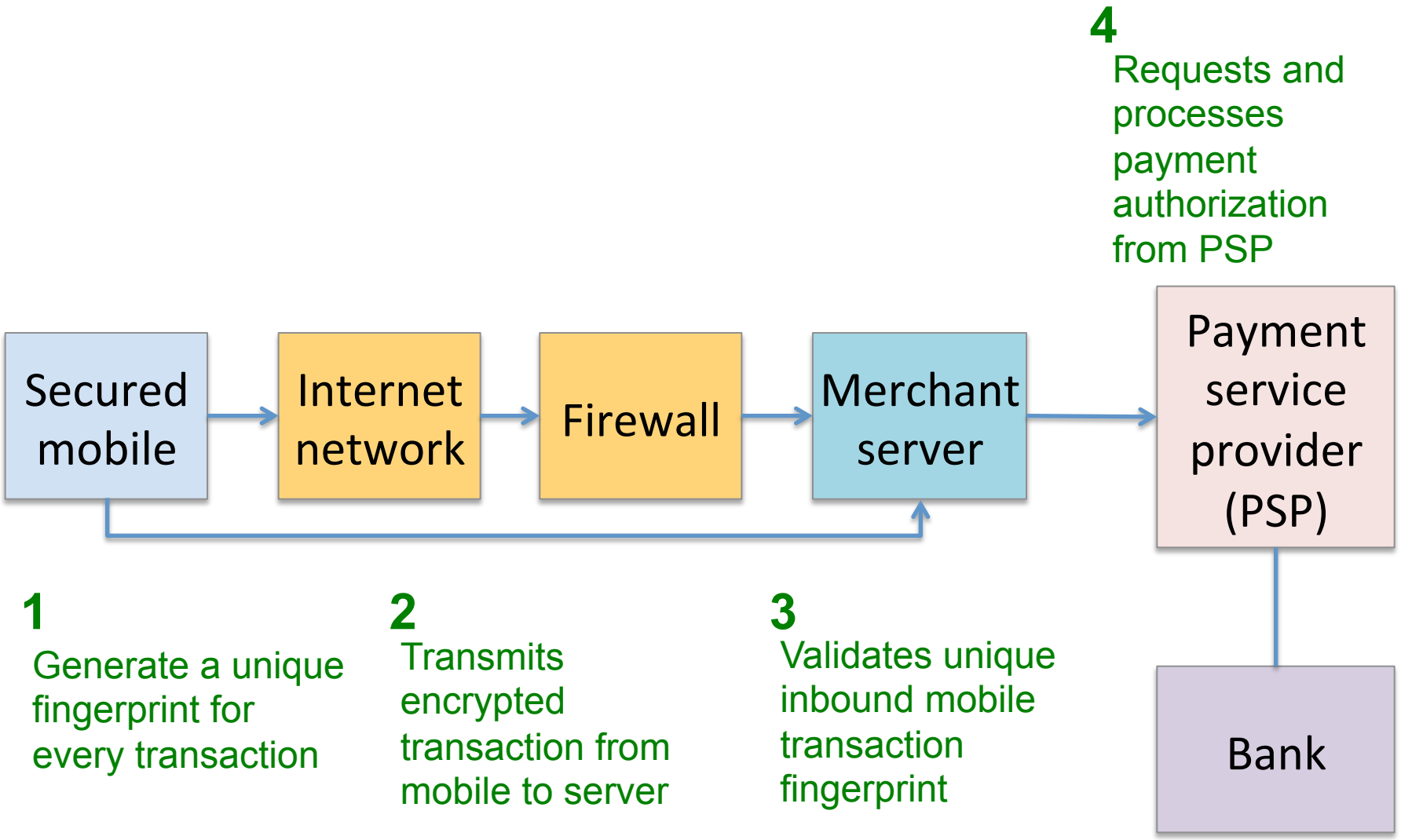
Mobile Security Worm Threat Targets Android Devices

Source: http://www.mobilecommercepress.com/mobile-security-worm-threat-targets-android-devices/8512823/

NFC

Source: http://www.elatec-cards.com/products/telecom/nfc/nfc-sim-cards/

Mobile Commerce Security



Source: http://ecommercesecurity.co.uk/

References

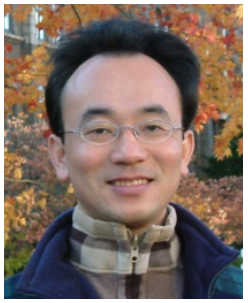
- Turban et al. (2010), Introduction to Electronic Commerce, Third Edition, Pearson
- 教育部顧問室編輯 “電子商務安全”教材

Tamkang University

Q & A

Electronic Commerce: Transaction Security
(電子商務交易安全)

時間：2014/7/03　(四) 14：00~17：00
地點：精誠資訊股份有限公司R0111會議室
(地址：台北市內湖區瑞光路318號1樓)



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. tku.edu.tw/myday/

2014-07-03