零售業《能力標準說明》能力單元

「交易安全技術」職能範疇

名稱	運用加密技術傳送資料
編號	107233L4
應用範圍	利用技術手段把重要的資料變為亂碼（加密）傳送，到達目的地後再用相同或不同的手段還原（解密）。
級別	4
學分	12（僅供參考）
能力	表現要求 1. 掌握加密技術基本概念 • 闡釋加密技術基本術語，包括： • 明文（Plaintext） • 密文（Ciphertext） • 加密（Encryption） • 解密（Decryption） • 加密演算法（Encryption Algorithm） • 解密演算法（Decryption Algorithm） • 發送者（Sender） • 接收者（Receiver） • 金鑰（Key） • 截收者（Eavesdropper） • 密碼分析（Cryptanalysis） • 密碼分析員（Cryptanalyst） • 被動攻擊（Passive attack） • 主動攻擊（Active attack）

零售業《能力標準說明》能力單元

「交易安全技術」職能範疇

能力	2. 運用加密技術
	• 運用對稱加密技術
	  • 瞭解對稱加密技術的5個基本成分
	  • 明文
	  • 加密演算法
	  • 金鑰
	  • 密文
	  • 解密演算法
	  • 瞭解和甄選適當資料加密演算法
	  • 加密體制是資料加密標準（DES）- 使用最廣泛的演算法
	  • 三重DES
	  • 高級加密標準（AES）
	  • Bluefish演算法
	  • RC5演算法
	• 運用非對稱加密技術
	  • 瞭解公開金鑰密碼體制組成，包括：
	  • 明文
	  • 加密演算法
	  • 公開金鑰和私密金鑰
	  • 密文
	  • 解密演算法
	  • 應用公開金鑰密碼體制
	  • 加密/解密：發送方用接收方的公開金鑰對消息加密
	  • 數碼簽署：發送方用其私密金鑰對消息“簽名”。簽名可以通過對整條消息加密或者對消息的一個小的資料塊加密來產生，其中小的資料塊是整條消息的函數
	  • 金鑰交換：通信雙方交換工作階段金鑰
	  • RSA演算法
	  • 認識其他的公開金鑰加密演算法，包括：
	  • ELGamal演算法
	  • 背包加密演算法
	  • 掌握金鑰管理技術
	  • 金鑰分發技術
	  • 金鑰認證技術
	  • 認證中心（Certification Authority，CA）驗證一個公共金鑰是否屬於一個特殊實體（一個人或一個網絡實體）
	  • 數位憑證
	• 認識安全套接字層（SSL）加密技術
	  • SSL是一種廣泛實施的公開金鑰加密技術，主要類型包括：
	  • 無用戶端SSL
	  • 配置VPN設備的無用戶端SSL
	  • 網絡至網絡
	  • 主機至網絡
	3. 展示專業能力
	• 引入最適合該企業的加密技術
	• 確保在運用加密技術時，恪守專業操守，防止任何欺騙行為
	• 確保在運用加密技術時，能遵守相關的法例要求

評核指引	此能力單元的綜合成效要求為： • 能夠瞭解加密技術的基本概念 • 能夠掌握基本加密演算法的設計原理 • 能夠完成基本法加密演算，處理傳送資料
備註	