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	運用認證技術和安全認證協議
編號	107234L4
應用範圍	應用網絡安全認證技術於通信雙方相互確認身份，以保證通信的安全。
級別	4
學分	6（僅供參考）
能力	表現要求 1. 瞭解安全認證技術的基本概念 • 證實被認證物件是否屬實和是否有效 • 通過驗證被認證物件的屬性，來確認被認證物件是否真實有效 • 明白電子商務認證技術的重要性 2. 掌握和應用主要認證技術 • 應用身份認證技術 • 目的是用於鑒別用戶身份 • 應用身份認證的主要方法 • 基於口令的認證方法 • 雙因素認證 • 一次口令機制 • 生物特徵認證 • 掌握身份認證協議系統(Kerberos)概念與應用方法 • 以可信任的企業為基礎的身份驗證協定，採用對稱密碼體制 • 完整的Kerberos系統包括驗證伺服器、授予許可伺服器、網絡應用伺服器以及網絡使用者: • 驗證伺服器的作用是鑒別用戶，並為用戶提供訪問授予許可伺服器的許可 • 許可伺服器負責授權使用者，為用戶發放放問應用伺服器的許可證 • 網絡應用伺服器提供某類網絡應用的伺服器 • 應用消息認證技術 • 目的是用於保證資訊的完整性和抗否認性，例如使用者要確認網上資訊否假的、資訊是否被其他企業修改或偽造等 • 應用消息認證方法 • 加密敏感的檔案，即使別人截取檔案，也無法得到其內容 • 保證資料的完整性，防止截獲人在檔案中加入其他資訊 • 驗證資料和資訊的來源，以確保發信人的身份 • 選擇和應用完整性驗證方法 • 利用摘要與散列函數 • 運用報文摘要演算法MD5 • 掌握散列函數演算法SHA-1 • 確定安全認證協議 • 認識安全認證協議的重要性 • 監察安全協議的機密性、真實性、完整性、不可抵賴性 • 協定採用的資料加密模型 • 協議規定工作流 • 掌握數碼簽署技術 • 瞭解數碼簽署定義 • 掌握數碼簽署主要方式 • 明白數碼簽署的應用範圍 3. 展示專業能力 • 確保在運應用認證技術和安全認證協議時，恪守專業操守，防止任何欺騙行為 • 確保在應用認證技術和安全認證協議時，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： • 能夠瞭解認證技術和安全認證協議的基本概念 • 能夠掌握基本認證技術和安全認證協議的設計原理 • 能夠正確地選擇和應用適當的認證技術和安全認證協議，以保證資料通信安全
備註	