建構以安全的 XML 與 RFID 為基礎之商車營運系統

黃映瑞 逢甲大學 GIS 中心
曹偉駿 大葉大學資訊管理學系
黃美治 中部汽車股份有限公司
林右明 拓凱實業股份有限公司
wjtsaur@mail.dyu.edu.tw

摘要

近年來，網路的普及最直接影響的就是帶動了電子商務的發展，而其所帶來的效益不僅能將企業上、下的供應鏈做有效的管理，也讓企業與消費者之間有了新的通路管道，使得「速度」成為左右企業生存的必要手段及產業競爭力的關鍵。而隨著物流、宅配業的興起，消費者對服務速度的要求也更加嚴苛，如何讓實體商品快速、安全且有效率地送達客戶手中，是物流、宅配服務業者最重要的課題。

然而，交通問題一直是現代人的噩夢之一，雖然政府已逐步開始推動智慧型運輸系統，但對於商業運輸業者而言，其重點仍放在規劃遞送路線，縮短運輸動線距離，達成降低運輸成本的目標，並未考量物流配送過程中交通狀況、車輛狀況、司機行駛狀況及貨品運送過程是否遭到非法盜賣等問題，而這些問題正是消費者能否信賴電子商務的關鍵因素。因此，本研究將結合 RFID 與 XML 金鑰管理規範建構一個安全的商車營運系統平台，將即時物流資訊回饋提供於供應鏈成員，提高安全又有效率的物流資訊，有助於提高整體企業競爭力，同時提升國內智慧型運輸系統的多元服務。

關鍵詞：商車營運系統，CVO，RFID，網路服務，XML

1. 前言

隨著網際網路的快速發展，造就了電子商務的產生，也使得在經濟全球化(Economic Globalization)的趨勢下，供應鏈管理與全球運籌的觀念被廣泛的討論。全球運籌管理的核心精神是快速回應市場的變化和客戶的需求，同時將經營成本、庫存壓力與風險降至最低，進而創造整體的最大效益。而電子商務的蓬勃發展，不僅能將企業上、下的供應鏈做有效的管理，也讓企業與消費者之間有了新的通路管道，使得「速度」成為左右企業生存的必要手段及產業競爭力的關鍵。

而隨著物流、宅配業的興起，消費者對服務速度的要求也更加嚴苛，傳統貨運業所提供的「在所託付的時間內，正確將貨物送達指定地點或收件者手中」的服務已經不敷需求了，取而代之的是如何透過後端支援系統隨時了解客戶的需求，也讓客戶了解物流狀況，進而讓實體商品快速、安全且有效率地送達客戶手中，是物流、宅配服務業者最重要的課題，同時也是消費者能否信賴電子商務的關鍵因素。

目前已有許多國內外學者針對物流配送路線規劃提出相關研究[1][2]。然而，實際運作中仍有許多無法準確得知的因素與問題(像是交通狀況、車輛狀況、司機行駛狀況及貨品運送過程是否遭到非法盜賣等)並未受到重視。因此，如何在整體供應鏈中強化物流資訊的分享，對建構一個完整的供應鏈來說，是不可缺少的一環。

以台灣產業分佈來看，中小企業佔有絕大部份，且多數的公司並未建置自己的配送車隊，因此在整體供應鏈的效率及價值極大化的考量下，通常將物流活動委由第三方的物流業者(Third Party Logistic Provider)運送，因此，能否確實地掌握供應鏈上下游廠商的物料流動狀況成為企業反應市場能力的一項重要指標。

而從企業發展的角度來看，除了上述的物流之外，金流與資訊流也是每個企業發展的必要條件。而隨著電腦技術的一日千里，應用在企業資料處理的電子商務也蓬勃發展。雖然透過電子商務的運

用，可以使得供應鏈中的資訊得以相互分享，但是舉凡是報價、訂單、客戶資料甚至是信用卡記錄，網路上資料傳遞的安全也一直是個重要的問題，但從技術角度而言，公開金鑰基礎建設（Public Key Infrastructure，PKI）[11]的部署過於麻煩，而且成本高昂，因此難以得到廣泛的應用。

因此，本研究將以物流中心管理者的角度切入，透過無線射頻識別（Radio Frequency Identification ,RFID）可即時監控的特性，使得在物流配送過程中的交通狀況、車輛狀況、司機行駛狀況及貨品運送過程是否遭到非法盜賣等問題能得到系統化管理，同時運用RFID對於商車營運系統傳輸過程中的資料進行加解密，並且建構一個包含消費者、供應商與物流中心的網路服務(Web Services)安全平台，來提高物流資訊透明化的程度。

2. 文獻探討

本研究的主要目的是利用 RFID 提高商車營運系統的加值服務，同時建置一個網路服務環境下安全的物流資訊平台，因此以下將針對「無線射頻識別」、「網路服務」、「商車營運系統」與「現有商車營運系統運作方式」等觀念加以了解與探討。

2.1 無線射頻識別

無線射頻識別（Radio Frequency Identification ,RFID）是一種運用無線電波傳輸訊息的識別技術；這種技術主要是將電子標籤晶片中儲存的辨識碼（id code）透過無線電波方式傳送給讀取機，然後由讀取機接收處理訊號。由於RFID屬於非接觸式智慧卡的一種，再加上具備條碼所沒有的防水、抗污、可重覆使用、穿透性佳、儲存容量大且可同時處理多筆記錄等優點[15]，因此其應用範圍相當廣泛。

在國內最常見的應用就是將寵物植入RFID 晶片、台北捷運的悠遊卡及門禁安全管制等應用，此外國內也將RFID 技術應用在嚴重呼吸道症群(SARS)期間，用以追蹤醫護工作人員、病患及探病的親友在院內的移動情形，以確實防制SARS 的傳播。

在RFID電子標籤與讀取機間，可以使用的無線頻率主要可分為低頻(135kHz以下)、高頻(13.56MHz)、超高頻UHF (860 – 960 MHz)和微波(2.4GHz以上) 四大類[2][15]。通常低頻率的傳輸能量小，傳輸距離短，傳送的資料有限，但穿透性佳；相對高頻率的傳輸能量大、距離遠，但容易被金屬隔絕，因此較不適合在有金屬部份的環境中使用。

由於RFID電子標籤的形狀與種類非常多，再加上無線通信所使用的頻率會影響天線的形狀與尺寸，因此，一般可將讀取機分為固定式和手持式二種；像是賣場、倉庫、貨櫃場、機場等出入口都可以見到固定式讀取機的使用；另一種手持式讀取機則輕巧許多，但感測的距離較短，且具有方向性。

2.2 網路服務

網由於網路技術的發展，再加上為了因應電子商務的發達，網路服務(Web Services)的概念因此產生，網路服務是在Internet上利用Web的方式來傳送XML(Extensible Markup Language)文件，並對企業的應用程式來提供服務。要讓網路服務成為企業與企業間(B2B)電子商務的應用架構，將會面臨到的一個問題就是網路安全。而對於網路服務交易的安全考量，除了要能夠確認交易雙方的身份外還必須要保護傳輸資料的隱密性及完整性。目前W3C (World Wide Web Consortium)所架構出網路服務的安全規範，主要包括了XML加密(XML Encryption)、XML簽章(XML Signature) 與XML金鑰管理規範(Key Management Specification，XKMS)三部份，以下就這三者逐一介紹。

(1) XML 加密

XML加密其主要目的是在制訂XML文件的加密的規範[12]。透過數位的加密能夠安全的保存及傳送機密的數位資訊。與傳統的加密方式不同的地方在XML可以單針對文件的部分區段進行加密，而不需要對整份文件進行加密，以提高使用的效率。

(2) XML 簽章

XML數位簽章是XML安全架構裡最基本的組成元件，它可以在網路服務環境中提供驗證基本數據的可靠度，來對於網路上的每筆交易可靠度進行確認[12]。與XML加密相同，數位簽章同樣可以針對XML文件之部分區段進行簽章，而非僅只能針對整份文件進行簽章。

(3) XML 金鑰管理規範

為了要確保資料或訊息在網路上交換時的安全性，目前較常被使用的方法就是公開金鑰密碼系統。然而，公開金鑰密碼系統在金鑰的管理與驗證上，雖然可以透過公開金鑰基礎建設與電子憑證來做到，但是從技術的角度來看，由於公開金鑰基礎建設的架構較為龐大，且部署起來較為麻煩，運用成本也較高。同時，現有販售公開金鑰基礎建設平台的軟體廠商並沒有統一的標準，這使得選用不同公鑰金鑰基礎建設平台的使用者或是應用程式在相互的溝通上產生一定的困難。

所以W3C提出XML金鑰管理規範，結合XML簽章標準及XML加密標準的應用[9][11][16]。使得在XKMS環境下，客戶端與應用伺服器能相互認證與處理彼此之間的要求。其運作流程如圖1：

圖 1 XKMX 運作方式

以下執行步驟詳細說明：

1. 客戶端會連線到 XKMS 伺服器查詢應用伺服器所註冊的金鑰是否正確。
2. 客戶端向應用伺服器提出服務要求。
3. 應用伺服器收到客戶端的請求時，會向 XKMS 伺服器請求驗證客戶端的身份及請求的完整性。
4. 當客戶端的資料通過驗證後，應用伺服器即會處理客戶端的請求服務。

由於XKMS可以針對網路服務提供安全保密的功能，所以企業可以應用XKMS在網路服務環境中傳送具有機密性或安全性很高的交易資訊。此外，XKMS能提供客戶應用系統與PKI之間的界面簡化與標準化，而透過標準化的界面讓PKI與應用系統兩者互動更具有彈性。

2.3 現有商用車輛營運系統運作方式

交通問題一直是現代都市人的噩夢之一，事實上，當一個國家或都市運輸系統的硬體建設達到某種程度後，或政府缺乏資金提供龐大的運輸建設時，為繼續提高運輸容量，就必須考慮如何利用電子、通信、資訊等高科技與管理技術，將既有運輸設施加值或使之更具智慧，以提供更有效率與安全的服務，因此智慧型運輸系統(Intelligent Transportation Systems，ITS)[4]乃應運而生，並且成為未來世界各國運輸系統長期發展的主要趨勢。然而在台灣智慧型運輸系統的發展，要以商用車輛營運系統（Commercial Vehicle Operations, CVO）的運作較為廣泛。所謂「商車」不僅包括大型與重型車輛（如卡車、貨車），也包括緊急救援用車輛（如救護車、拖吊車），以及每日運作的商用小型車（如計程車）等商業營運車輛。由於商業運輸業者每日必須處理頻繁的物流傳遞，因此如何透過技術與管理提升營運效率就成為一個重要課題。目前在貨運業、物流業、計程車業及遊覽車租車業等都開始利用 CVO 建置車隊管理。透過車隊即時定位與管理，不僅能充分掌握車輛派遣與即時動態，同時可以精確規劃遞送路線，縮短運輸動線距離，達成運輸成本降低的目標。

目前國內商用車輛營運系統業者所提供之管理服務[1]，主要是幫助傳統運輸產業利用全球定位系統與GSM/GPRS系統來建立智慧型車隊管理；只要車輛安裝GPS接收器與GPRS無線通訊設備，就能主動將行車狀態、行車速度與座標位置等資訊，透

過GPRS傳回至物流中心。而透過運輸系統所即時接收的行車資料，調度人員就可以瞭解車輛所在位置即時進行調度派遣，而物流中心亦能藉由運輸系統透過資料統計，計算公司營運成本。運作方式如圖2：

圖 2 現行商用車輛營運系統運作方式

以下執行步驟詳細說明：

1. 物流運輸車輛結合 GPS 衛星定位系統，計算運輸車輛座標、行車速度與方向等資訊。
2. 運輸車輛透過無線通訊的方式，將 GPS 定位資訊、車輛狀態與運送物品資訊，回傳至後端系統。
3. 車輛回報資料經由 GPRS 無線通訊傳送至電信業者，透過網際網路的方式與物流公司進行介接。
4. 物流公司運輸管理系統經由網際網路連結到電信業者，透過 GPRS 取得與車輛物流資訊。
5. 派遣中心調度人員，透過運輸管理系統瞭解車輛即時資訊與任務派遣。

然而現有架構在貨物運送管制上或是運輸過程資料的傳遞，都沒有提供足夠的安全保護，此外，當貨物送達時則必須透過司機以行動電話回報，再由調度中心以人工方式逐一將貨物送達時間輸入電腦，如此不但得付出昂貴的通話費，同時也因無法即時監控貨物動向使得貨物運輸過程的風險大增。

3. 建構安全商車系統

雖然智慧型運輸系統在世界各國都有不同的發展重點，但不可諱言的，隨著電子商務的不斷發展，商用車輛營運系統的應用將會更加多元。因此本研究主要目的就是利用RFID技術來彌補商用車用營運系統在貨物追蹤及管控上的不足，提高商用車輛營運系統的加值服務，同時建立一個包含消費者、供應商與物流中心的網路服務(Web Services)安全平台，來提高整體供應鏈中物流資訊的透明化。

在本研究架構下，無論是消費者透過網路向通路商下訂單，或是通路商、供應商與物流中心之間的資料傳遞，都可以透過XML金鑰管理做到安全的資料交換；而在實際的貨物運輸上，除了透過商車營運系統監控車輛所在位置外，同時利用RFID增加貨物運送管制上的追蹤以及確保物流運送過程中GPRS/3G資料傳輸的安全。整體架構如圖3所示。

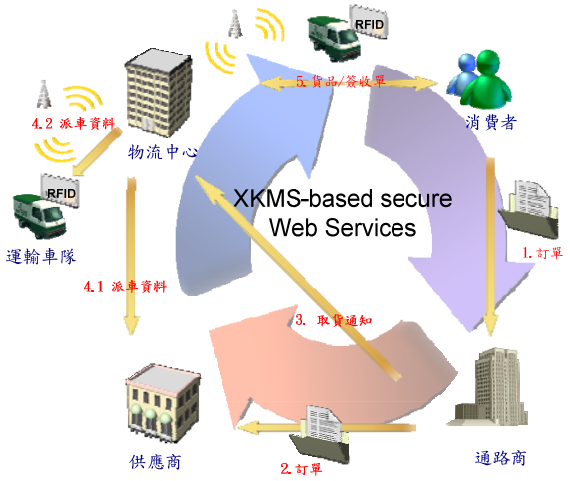

圖 3 基於 XML 與 RFID 之安全商車營運系統服務流程

其運作流程如下說明：

1. 消費者可透過網路服務向通路商下訂。
2. 通路商在整合消費者訂單後，即可向供應商下訂。
3. 當通路商收到供應商的確認訊息後，即可向物流中心發出取貨通知。
4. 物流中心依據商車營運系統所提供的資訊，找出最近的物流車將車號、司機名稱等資訊傳給供應商，同時透過商車營運系統通知司機取貨。
5. 而在實際配送過程中，物流中心可透過商車

營運系統及 RFID 對配送的物品、交通、司機行駛狀況等訊息，得到直接快速的回饋，同時透過網路服務提供消費者、供應商與通路商等準確的物流資訊。

以下分別就本研究所提架構下之訂貨階段、物流階段與營運交易統計階段，說明其運作流程：

3.1 訂貨階段

當消費者透過網路服務的方式向通路商訂貨後，通路商會先利用消費者公鑰檢查訂單的準確性，確認無誤後，再向供應商提出訂貨需求；而供應商會先確認通路商身份及所提出的需求後傳回確認訊息，此時通路商即可通知物流中心前往取貨，整個交易階段透過XML金鑰管理進行身份驗證，消費者、通路商、供應商與物流中心等，提出自有之XML金鑰，透過安全的網路服務的方式，由對方進行XML金鑰驗證，以確保每一位商家與消費者的身份合法性，其系統分析說明如圖4所示：

1. 消費者透過網路服務向通路商所提供的 B2C 交易平台下達訂單。
2. 通路商收到訂單後會先向 XKMS 伺服器驗證消費者身份及訂單是否遭到竄改。確認無誤後，即傳回確認訊息。
3. 通路商將訂單資訊加密後提交給供應商。
4. 供應商獲得通路商的訂單資訊後，同樣先驗證通路商身份並確認資料，並回傳確認訊息給通路商。
5. 通路商向物流中心提出收貨需求。
6. 物流中心確認通路商的身份及收貨通知，並傳回確認訊息。

在每一位商家與消費者進行訂購交易資料，如圖5之步驟3.、4.、7.、8.、11.、12.，經由XML加密機制（圖6）與XML金鑰管理（圖7），保證訂購交易資料傳遞之安全性。

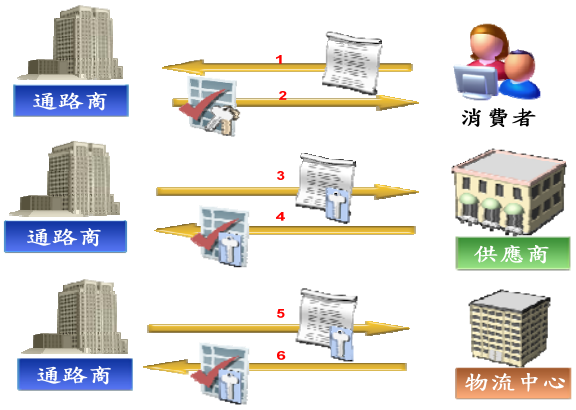

圖 4 訂貨階段系統分析

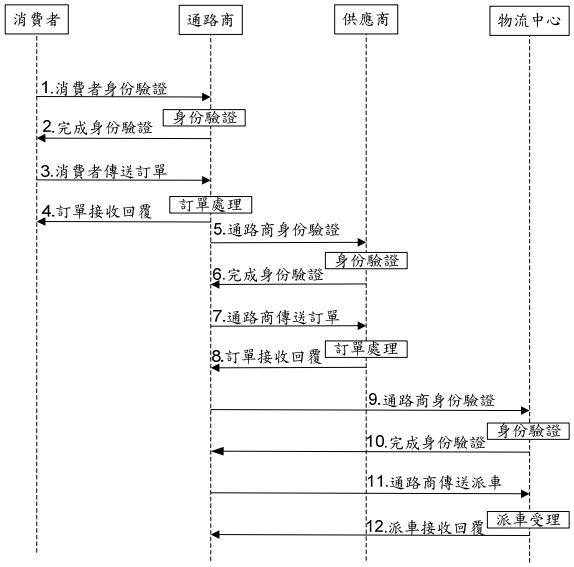

圖 5 訂貨階段系統設計

```
<?xml version="1.0" encoding="UTF-8" ?>
<soap:Envelope
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/
"
xmlns:xsd="http://www.w3.org/1999/XMLSchema"
xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance"
>
<soap:Body>
  <xkms:LocateResult
xmlns:xkms="http://www.xkms.org/schema/xkms-2001-01-
20">
  <xkms:Result>Success</xkms:Result>
  <xkms:Answer soapenc:arrayType="KeyBinding">
  <dsig:KeyInfo>
  <dsig:KeyName>cn=XKMS Connector,o=Entrust XKMS
Demo Service,c=US
</dsig:KeyName>
  <dsig:KeyValue>
  <dsig:RSAKeyValue>
  <dsig:Modulus>Key Modulus</dsig:Modulus>
  <dsig:Exponent>Key Exponent</dsig:Exponent>
  </dsig:RSAKeyValue>
  </dsig:KeyValue>
  </dsig:KeyInfo>
  </xkms:Answer>
  </xkms:LocateResult>
  </soap:Body>
  </soap:Envelope>
```

圖 6 XML 金鑰驗證

```
<xenc:EncryptedData
Id="EncryptedContent-f6f50b24-3458-41d3-aac4-390f476f
2e51"
Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-c
bc" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName>Key Information</KeyName>
</KeyInfo>
<xenc:CipherData>
<xenc:CipherValue>Order Content Encryption
</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
```

圖 7 XML 資訊加密

3.2 物流階段

物流中心在確認供應商的收貨需求後，透過商車營運系統，通知最快抵達的物流車前往取貨；同時將收貨時間及司機車號的相關訊息通知供應商。物流階段所使用無線通訊方式，物流車定時回報物流車GPS資料與貨物狀況與物流中心與物流車之間雙向派遣訊息，其系統分析如圖8所示：

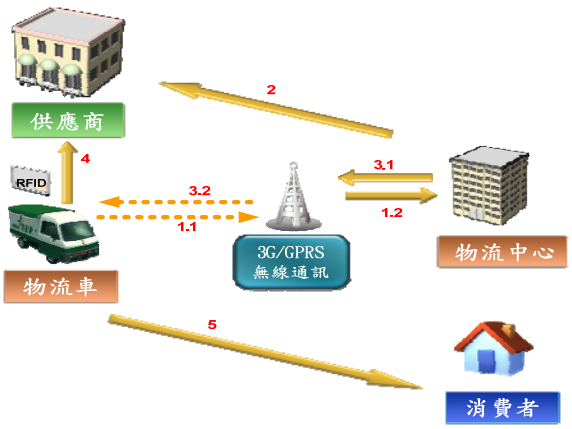

圖8 物流階段系統分析

1. 物流車可透過商車營運系統隨時向物流中心

回報即時位置、車輛狀態、貨物內容等資料，使物流中心能充份掌握行車動態資訊。

2. 物流中心在確認供應商的收貨通知後，回報收貨時間、收貨司機等相關訊息給供應商。
3. 透過商車營運系統通知物流車前往收貨。
4. 司機抵達收貨地點時，以所持有之 RFID 卡辨識身份。
5. 在實際物流派送階段，物流車會依據送貨單資料將貨物送至消費者手上，使用者完成簽收，取得使用者訂單階段授權碼。

物流階段之系統設計，如圖 9 所示，因物流車與物流中心為了確保資料在無線傳輸下的安全，將利用司機所持有的 RFID 智慧卡進行資料加密，如圖 9 之步驟 1.、6.、10.、14 所示；同時，當司機到達收貨地點後，供應商可透過司機的 RFID 智慧卡，驗證司機的身份，達到供應商出貨的安全，如圖 9 之步驟 7. 、8. 、11. 、12 所示，物流車之無線通訊安全，資料的加密如圖 10 所示。

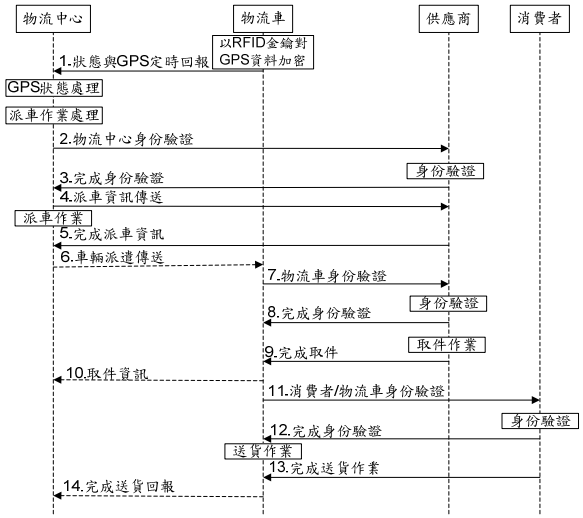

圖 9 物流階段設計

```
<xenc:EncryptedData
Id="EncryptedContent-f6f50b24-3458-41d3-aac4-390f476f
2e51"
Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod Algorithm=
"http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
<KeyInfo mlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName>RFID KeyInformation</KeyName>
</KeyInfo>
<xenc:CipherData>
<xenc:CipherValue>Dispatch                    Information
</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
```

圖 10 XML 物流車派遣資料加密

3.3 營運交易統計階段

當物流車在外實際進行配送過程中，物流中心可透過商車營運系統及RFID監控，即時取得貨物及司機行駛狀況的最新資訊回饋；同時當貨物送交消費者手中時，也可即時取得簽收資訊，其系統分析如圖11 所示：

1. 物流車完成送貨，並取得客戶的訂單授權碼，再透過無線通訊將授權碼傳送至物流中心。
2. 物流中心依照消費者所簽回的訂單授權碼回報給通路商，做為送達確認。

營運交易統計階段系統設計如圖 12 說明，是商車營運系統延伸效益，透過即時物流資訊回饋，與上下游供應鍊商家資料交換，商家可以透過資訊系統計算績效、成本與提供決策資訊，如圖 12 步驟 1 所示。因此以 XML 金鑰管理與 XML 加密簽章與物流車之 RFID 金鑰認證，在營運交易統計達到不可否認，每一參與商家與消費者之交易記錄無法篡改，如圖 13 所示。

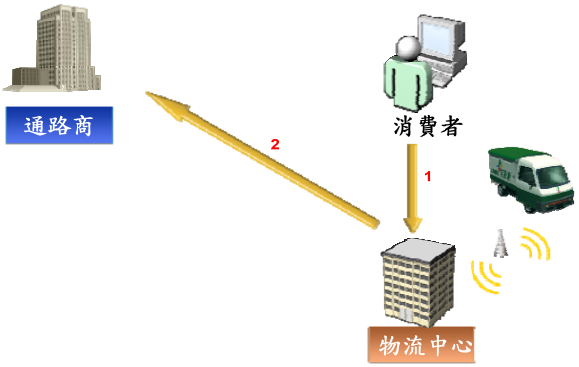

圖11 營運交易設計

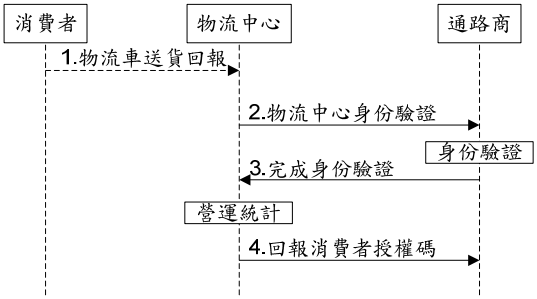

圖12 營運交易設計

```
<xenc:EncryptedData
Id="EncryptedContent-f6f50b24-3458-41d3-aac4-390f476f
2e51"
Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod                    Algorithm=
"http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<KeyName>KeyInformation</KeyName>
</KeyInfo>
<xenc:CipherData>
<xenc:CipherValue>Verify                    Accept
Code</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
```

圖 13 XML 驗證訂單交易授權碼

4. 系統模擬

本研究針對建構安全之商車營運系統之網路服務系統模擬分就如下說明。

消費者透過網路服務，利用瀏覽器瀏覽通路商提供之網路交易平台，消費者登入通路商交易平台程序，由消費者產生訂單交易資料，如圖14所示。

圖 14 通路商交易平台

物流中心監控系統結合衛星定位系統與GPRS通訊，物流車衛星定位系統計算車輛位置、時速、方位角與車輛狀態資訊，透過GPRS無線通訊，物流車定時回報物流車行車資料，如圖15所示。

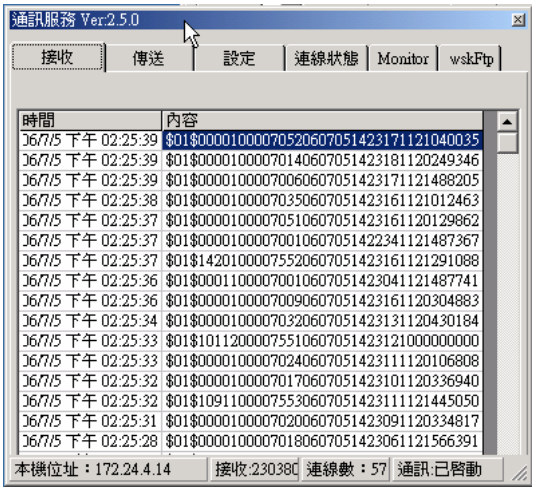

圖 15 物流中心與物流車無線通訊

物流車透過無線通訊(GPRS)方式，將GPS定位資料回報物流中心，物流中心可即時掌握物流車物流狀態，如圖16所示。

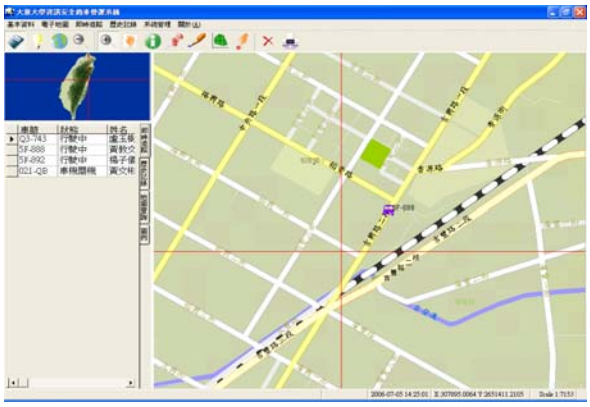

圖 16 物流中心車輛管理系統

在本研究之安全商車營運系統，物流中心透過XML的方式，建立上下游供應鏈廠商之資訊交換平台，將物流即時資訊透過安全的通道回饋給供應鏈之成員，提升整體供應鏈之效益。

5. 效益分析

在本研究所提架構中透過XML金鑰管理規範，將消費者、通路商與物流中心之間不同的後端系統，在統一的Web平台進行資料交換，解決傳統電子資料交換需要一致性格式與金鑰管理的問題，因此本機制與傳統商車營運系統更能適用於企業電子商務，由表1表示

表 1 本機制與傳統商車營運系統表較表

項目	傳統商車營運系統	**安全商車營運系統**
作業系統	封閉式架構	**開放式架構**
程式架構	外部異質系統整合	**使用XML為基礎**
安全性	安全不易掌控	**XML金鑰管理 XML加密 RFID金鑰加密**
系統建置成本	成本偏高	**成本較低**
適用範圍	B2B	**B2B，B2C**

本機制結合RFID運用於商車營運系統，將物流中心與物流車之間的無線通訊進行資料傳輸加密，使得物流中心的派車資訊與物流車出勤狀態、商品資訊等能透過安全的無線通訊，達到即時雙向傳輸。其所帶來效益說明如下：

（一）提升商車營運系統服務效益與安全

(1) 透過物流人員之 RFID 金鑰驗證可以有效識別物流人員的身份，同時可利用監控機制確保車上物品不會遭到非法盜賣。

(2) 整合安全的網路服務有效利用商車營運系統了解交通狀況、車輛狀況、司機行駛狀況，做為安全便利的後台管理的參考。

(3) 針對物流資訊傳送的過程，提供加解密機制，以確保資料在無線網路環境下傳送過程的安全性。

（二）即時資訊的安全傳遞與物流資訊回饋

利用XML金鑰管理與XML加密簽章提供安全的網路服務平台，商車營運即時資料透過安全的網路服務回饋至供應鏈成員，消費者網路購物的動機，引發商家與物流接單處理效應，消費者從下訂單到收貨可隨時查詢物流狀況，提高供應鏈成員在網路服務環境中的整體效益。

6. 結論

目前許多PKI廠商，如Java Security Packages、Microsoft CAPI、RSA BSAFE等，因為各自擁有憑證與金鑰管理的方式，使得各平台之間的相容性較差，也使得以往供應鏈上下游廠商在建置電子資料交換時，因為缺乏相容的安全軟體而產生諸多的困難。此外，在實體物流運輸方面，隨著物流、宅配業的興起，消費者對服務速度的要求也更加嚴苛，雖然商車營運系統的逐漸發展，使得運輸系統不再只是單純的路線規劃，但現有商車營運系統並未考量資料傳輸過程中的安全需求，使得貨品在運輸過程中的安全性大打折扣。

要如何透過商車營運系統，讓客戶了解物流狀況，讓實體商品快速、安全且有效率地送達客戶手中，是物流、宅配服務業者最重要的課題，同時也是消費者能否信賴電子商務的關鍵因素。

因此，本研究結合RFID與XML金鑰管理規範

建構一個安全的商車營運系統平台，提供供應鏈成員安全又有效率的物流資訊，提昇整體產業競爭力。以安全的商車營運系統，建立標準的XML網路服務機制，未來可以由商車營運系統延伸至智慧型運輸系統其他子系統，例如整合至電子付款(ETC)等、先進交通管理、緊急事故處理系統等，因此企業在電子商務的使用，結合安全的商車營運系統，有助於提升企業整體競爭力。

參考文獻

[1] 交通部運輸研究所, http://www.iot.gov.tw。

[2] 陳宏宇，「RFID 系統入門-無線射頻系統」，松崗出版社，2004 年。

[3] J. Kim and K. Moon, "Design of Unified Key Management Model using XKMS," *Advanced Communication Technology, 2005*, ICACT 2005. Vol. 1, pp. 77-80, 2005.

[4] R. L. Courtney, "A Broad View of ITS Standards in the U.S.," *IEEE Conference : Intelligent Transportation System*, pp.529-536, 1997.

[5] W. Leavitt, "Speed Reading: RFID for Fleets," *Fleet Owner Overland Park*, Vol. 99, p.82, 2004.

[6] C.L. Liu, "Best-path Planning for Public Transportation System, *"The IEEE 5th International Conference: Intelligent Transportation System*, pp.834-839, 2002.

[7] K. Michael, L. McCathie, "The Pros and Cons of RFID in Supply Chain Management," *Proceedings of the International Conference on Mobile Business, 2005.*

[8] N. Park, K. Moon, S. Sohn, "A study on the XKMS-based Key Management System for Secure Global XML Web Services," *Advanced Communication Technology, 2004. The 6th International Conference*, Vol. 1, pp. 492-495, 2004.

[9] N. Park, K. Moon, S. Sohn, "XML Key Management System for Web-based Business Application," *Network Operations and Management Symposium 2004*. NOMS 2004. IEEE/IFIP, Vol. 1, pp. 903-904, 2004.

[10] A. Slater, "Specification for a Dynamic Vehicle Routing and Scheduling System," *International Journal of Transport Management*, Vol.1, pp.29-40, 2002.

[11] W. Stallings, "Cryptography and Network Security," *3rd ed. New Jersey: Prentice Hall*, 2003.

[12] W3C XML Encryption, <http://www.w3.org/Encryption/2001>, 2001.

[13] K. Toyota, T. Fuji, T. Kimoto and M. Tanimoto, "A Proposal of HIR（Human-Oriented Image Restructuring）System for ITS," *Proceedings of the IEEE: Intelligent Vehicles Symposium*, pp. 540-544, 2000.

[14] Y. N. Wang, R. G. Thompson and I. Bishop, " A Gis Based Information Integration Framework for Dynamic Vehicle Routing and Scheduling, " *Proceedings of the IEEE International：Vehicle Electronics Conference*, Vol. 1, pp. 474-479, 1999.

[15] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-cost Radio Identification Systems," *Proc. International Conference on Security in Pervasive Computing*, pp. 454-469, 2003.

[16] XML Key Management Specification ,<http://www.w3.org>

[17] S. Yoo, K. Lee, and K. Lee, "An XML-based mediation framework for seamless access to heterogeneous internet resources," *Lecture Notes in Computer Science*, Vol. 797, pp.396-405, 2003