國立交通大學

網路工程研究所

碩 士 論 文

(Draft)

建立 RFID 安全物流系統之研究

A study on RFID-based secure logistic system

研 究 生：黃昱華

指導教授：蔡文能　教授

中 華 民 國 九 十 八 年 五 月

建立 RFID 安全物流系統之研究

A study on RFID-based secure logistic system

研 究 生：黃昱華　　Student：yu-hua huang

指導教授：蔡文能　　Advisor：Wen-Nung Tsai

國 立 交 通 大 學

網 路 工 程 研 究 所

碩 士 論 文

A Thesis

Submitted to Institute of Network Engineering

College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science

June 2008

Hsinchu, Taiwan, Republic of China

中華民國九十八年五月

建立 RFID 安全物流系統之研究

學生：黃昱華　　指導教授：蔡文能

國立交通大學資訊工程學系（研究所）碩士班

摘要

近年來物流運輸系統已漸漸開始導入無線射頻辨識技術(RFID)，成功的改變物流運輸產業的執行流程。在尚未導入 RFID 系統時，當物品抵達集散中心需依靠人力的方式一箱一箱的去比對貨物的條碼(Bar Code)，但在導入後，貼有 RFID 識別標籤的貨物可直接由 RFID 讀寫器一次讀取大量的貨物且自動識別其正確性。

目前導入無線射頻辨識機制的物品驗證平台，在 RFID 讀寫器讀取貨物資料後，須經由網路將資料送至後台伺服器進行辨識的動作，由於驗證時須依賴網路的支援，因此當貨物集散中心的網路發生問題時便無法進行貨物的驗證，且後台伺服器是依據廠商所提供的產品清單來比對貨物是否正確，所以當貨物量大時貨物驗證所需的時間會相當的冗長。

本論文提出在離線的狀態下驗證貨物的平台，解決驗證貨物須依賴網路傳遞資料的問題，且導入密碼學中的雜湊函數以及簽章演算法，當驗證的貨物量變大時，驗證所需的時間不會隨之增加。

A study on RFID-based secure logistic system

Student：Yu-Hua Huan　　Advisor：Wen-Nung Tsai

Institute of Computer Science and Information Engineering
National Chiao-Tung University

ABSTRACT

Before RFID system introduced, the validation of cargo were checked by manpower with bar code. Since RFID system has been introduced and accepted by logistics industries years ago, the validation processes are changed from using manpower with bar code to using RFID readers with tags, which could be performed automatically to shorten the processing time.

In current logistics system, all the data obtained by the RFID readers have to be sent to back-end server via network to validate these cargos. Once the network occurs problems, the process of cargo validation has to be delayed.

In this thesis, we proposed a solution, the fast offline validation platform, to solve this problem. In this platform, we utilized cryptographic functions such as message digest, digital signature, etc., to ensure security compliance during the validation process.

誌謝

經過碩士班兩年的努力，克服了相當多的困難，終於完成了我的碩士論文。這篇論文之所以能順利完成，首先要感謝我的指導教授 － 蔡文能教授，給予我知識上的啓發以及學業上的指導。再來要感謝的是實驗室博士班蔡宗易學長，給予我一些在實作上的建議，讓我得以迅速的發現自己的盲點，使學生受益良多。此外當然還有學長姐、同學、學弟妹們熱心的討論與幫忙，這篇論文才可以順利的完成。

目錄

表目錄

圖目錄

一、緒論

無線射頻識別技術(Radio Frequency Identification, RFID)使用電磁頻率訊號，來達到非接觸式的資料傳輸。在進入二十世紀後無線射頻識別技術快速的往大型整合系統發展，目前企業使用 RFIID 改善管理系統以及相關運作流程以提升競爭力，尤其在物流企業將 RFID 標籤黏貼至出口貨物上提升貨物檢驗的便利性且所需的成本並不高，更可取代原供應鏈所使用的條碼機制(barcode)[7] ，可提升供應鏈管理的效率以及便利性。

在物流管理系統導入 RFID 後，將原先各自獨立的物流系統(買賣、倉儲、銷貨…等)整合成一個平台，且據點跟據點之間的訊息傳遞也從先前的電話及傳真轉變成網路，大大的提升貨物管控的效能，由於 RFID 標籤擁有唯一的識別碼，所以透過網路隨時查看貨物目前的狀態，強化傳送物流所不足的物品監控能力。

但目前 RFID 物流管理系統，其貨物驗證機制皆是由 RFID 讀寫器接收 RFID 貨物標籤所含資料後，經由網路傳送至後台伺服器執行貨物驗證的動作如圖 一所示，此貨物驗證流程會有兩個問題的產生，其一爲若網路發生問題時 RFID 讀寫器便無法將貨物資料傳送至後台伺服器驗證其正確性，而導致集散中心的動作停擺。另一個問題則是後台伺服器在驗證貨物時，是將所讀取到的貨物資訊與產品供應商所提供的清單進行比對，因此當傳送至後台伺服器的驗證資料量很大時，會導致驗證的時間變得冗長。

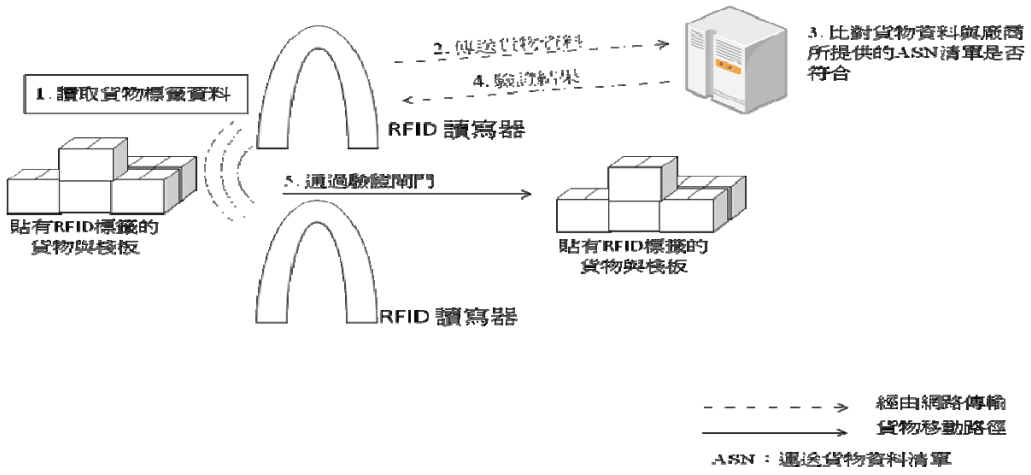


圖 一：目前物流貨物驗證流程

1.1 研究動機

爲解決上述所提及的網路斷線問題以及驗證貨物量大時系統效率不彰的問題，本論文提出快速離線驗證平台如**圖 二**所示，與現有驗證系統最大的不同點爲將**圖 一**中的驗證伺服器改由中界軟體來進行貨物合法性的識別。

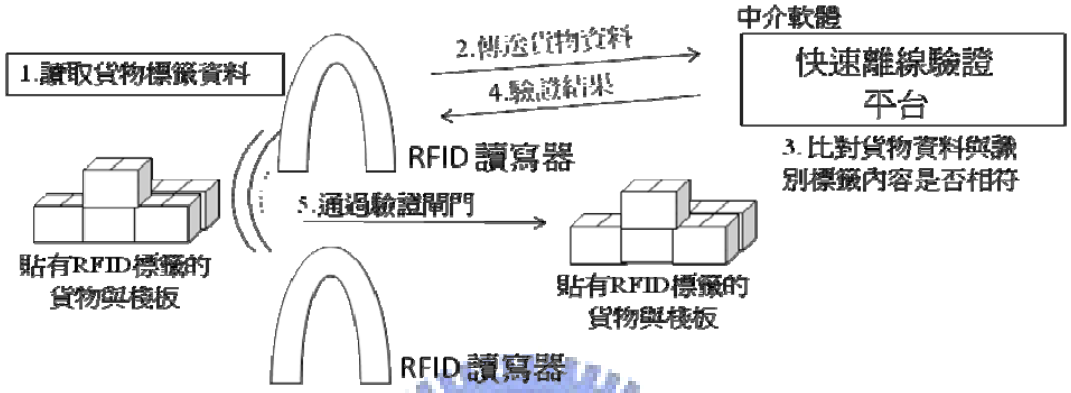


圖 二：快速離線認證平台

圖 二中快速離線驗證平台利用 RFID 讀寫器所傳送的貨物標籤資料、棧板標籤資料以及識別標籤資料，經由 SHA1 雜湊函數以及 DSA 簽章演算法運算後，即可判別在驗證閘門中棧板所承載貨物的正確性。

快速離線驗證平台執行貨物正確性的審核時，會將從 RFID 讀寫器傳送過來的貨物標籤資料，經雜湊函數運算以判斷貨物的正確性，不管資料量大小經雜湊運算後，所產生的摘要值其大小皆固定不變，本論文所設計的驗證平台藉由此特性達到當驗證的貨物量大時並不會影響系統的效率。

1.2 論文架構

本論文總共分爲六章，依序爲緒論、背景知識、相關研究、驗證平台設計與實作、系統測試、結論。

第一章「緒論」，除了點出論文的主題外，主要說明本論文的研究動機與目的；並且介紹本論文的整體架構及各章節的內容。

第二章「背景知識」，則是在介紹閱讀本論文所需的相關基礎知識；在此章節首先說明有關 RFID 系統的基本原理，之後再更深入的去說明 EPC Global 所制定的標籤格式，最後再以密碼學的相關應用作爲結束。

第三章「相關研究」在此章節將目前的 RFID 驗證協定分爲中央集權式以及非集權式兩類別來進行討論，且針對這兩類在個別舉出建立在該類別上的驗證機制來進行說明。

第四章「驗證協定設計與實作」主要是說明論文所設計的快速離線驗證協定，其設計概念、實作環境以及如何達成 Non-Server 的限制下進行同時大量物品驗證的動作。

第五章「系統測試」在此將列出五個情境，來驗證在第四章所設計的快速驗證協定，分別爲無異常情況、部分貨物遺失、貨物數量過多、未授權貨物供應商以及貨物遭置換，上述五種情況皆是貨物由供應地運往目的地時有可能會發生的情況。

第六章「結論」在這個章節中爲總結本論文的貢獻，且說明未來可能的研發工作以及思考方向。

二、背景知識

快速離線驗證平台建立在無線辨識技術(RFID)的系統架構上，且使用 EPC global Class1 Gen2 標準的 RFID 標籤建製實驗所需貨物，而當貨物抵達集散中心時快速離線驗證平台，利用密碼學相關演算法來識別。本小節將針對這三個部分來進行說明。

2.1 RFID 系統

RFID 的執行步驟，首先由RFID讀寫器（reader）透過無線電波發出請求後，RFID電子標籤（tag）將資料傳送到RFID讀寫器，RFID讀寫器使用中界軟體(Middleware)依不同的應用轉換所收到的RFID標籤資料格式，最後將資料傳送至應用系統(application system)執行如**圖 三**所示：

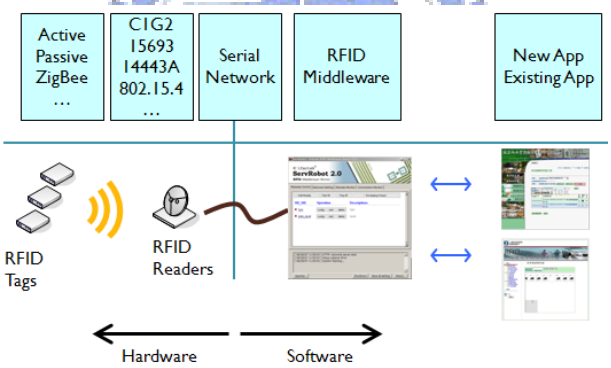


圖 三：RFID 系統架構

從圖三中我們可以看出RFID系統分爲硬體與軟體兩大類，硬體方面可分爲記錄資料的RFID標籤及讀寫標籤資料的RFID讀寫器，在軟體部分則包含負責應用軟體與RFID讀寫器之間的資料格式轉換以及根據不同需求所開發的各類應用軟體所構成。

RFID電子標籤型態：

RFID電子標籤可以依其本身是否具備電池，而區分爲主動式和被動式標籤晶片兩種型態分別爲：

(1) 主動式（Active）標籤晶片：

主動式的電子標籤也稱爲「內建電池的RFID標籤」，其傳輸距離爲1~2 公里，其優點是讀取器的讀取距離可以比較遠且讀取速度較快，但缺點是需要電池，所以標籤晶片產品有使用時間限制，且製造卡片的成本較高；因爲它本身不但擁有晶片與天線，且具有傳輸的能力，能夠自動發送射頻訊號給RFID讀取器。

(2) 被動式（Passive）標籤晶片：

沒有加裝電池的RFID電子標籤即稱爲被動型，其執行傳送動作時所需電源由RFID讀取器所發射的射頻訊號能量取得，並且依照其傳送頻率的不同而有不同的感應方式，被動式的標籤造價就便宜許多，因爲它本身並不具有發送射頻訊號的功能，需要靠RFID讀取器的無線電訊號來做動作，所以其收發的距離大約是在3cm~30cm內。有時短距離的相關應用也能發揮出RFID的重要功效，如台北捷運的悠遊卡等，就需要短距離的RFID 技術。

RFID工作頻率：

目前RFID最常使用的頻率共有5種[18] ，分別是 135KHz 以下、13.56MHz、860M~960MHz（UHF 頻帶）以及2.45GHz，而不同的工作頻率各有其優缺點及其應用範圍。上述五類工作頻率其傳輸距離約爲數公分到數公尺且傳輸速率約爲數十到數百Kbps。一般而言，工作頻率低的RFID其特性爲架構簡單與成本便宜，而高頻率的RFID特性爲傳輸距離較長，且抗干擾性較佳，相較下成本也比較高。**表 一**爲較常用的RFID工作頻率。

頻率	使用案例	訊號傳遞距離	備註
135KHz以下	送洗衣物及動物ID	2 公尺(世界共通)	易於適用於金屬
13.56 MHz	貨盤/品項管理及圖書館的出入管理	1.5 公尺(世界共通)	會受到金屬的影響
860M~960MHz	貨櫃管理	美國7 公尺 歐聯3 公尺	通信距離最長，會受到水分的影響
2.45 GHz	停車場出入管理	日本是1 公尺 美國是2 公尺 歐聯則是0.7~2公尺	標籤尺寸最小，會受到水分的影響

表 一：RFID 工作頻率分類[19]

2.2 EPC Global Class1 Gen2 標籤資料欄位標準

目前無線射頻辨識電子標籤欄位的制定格式，以 EPC global 協會所定義出的標準[20] ，爲世界各國所遵循的規範，在此節將說明 EPC global Class1 Gen2 RFID 電子標籤欄位對應關係。

2.2.1 標頭檔

標頭檔全部的 Bits 長度是用來定義 EPC Tag 的架構以及驗證的型態的編碼。在這一個版本標籤的資料欄位標準定義的標頭檔(Header value)，總長度爲八個 Bits，在此標頭檔 11111111，被保留用來擴充標頭檔空間的特定值，因此標頭檔所支援最大的數值爲 255(8-Bits)。

在 EPC global Class1 Gen2 標籤欄位標準版本(1.41)裡，總共定義 14 種編碼機制，每種機制皆會有特殊的 Header Value 標示如**表 二**所示

Header Value (binary)	Header Value (Hex)	Encoding Length (bits)	Encoding Scheme
0010 1100	2C	96	GDIT-96
0100 1101	2D	96	GSRN-96
0100 1111	2F	96	DoD-96
0011 0000	30	96	SGTIN-96
0011 0001	31	96	SSCC-96
0011 0010	32	96	SGLN-96
0011 0011	33	96	GRAI-96
0011 0100	34	96	GIAI-96
0011 0101	35	96	GID-96
0011 0110	36	198	SGTID-198
0011 0111	37	170	GRAI-170
0011 1000	38	202	GIAI-202
0011 1001	39	195	SGLN-195
0011 1010	3A	113	GDTI-113

表 二：EPC Global C1G2 標籤編碼[20]

2.2.2 欄位編碼規則(Notational Conventions)

EPC Global Class1 Gen2 標籤內 EPC Bank，所記錄的資料是用來標示貨物相關資訊與條碼(Bar Code)的功用相同，EPC Global Class1 Gen2 定義 14 種 EPC Bank 編碼的機制，不同的編碼所使用的欄位皆有所差異，但皆是由**表 三**所示的欄位所組成。

	Header	Filter Value	Partition	Company Prefix	Item Reference	Serial Number
	8	3	3	20-40	24-4	38
SGTIN-96	0011 0000 (Binary value)	如表五所示	如表六所示	999,999 – 999,999,999,999 (Max. decimal range*)	9,999,999 – 9 (Max. decimal range*)	274,877,906,943 (Max. decimal value)

表 三：欄位編碼規則範例[20]

上表爲目前物品運輸系統所使用的 EPC Bank 編碼機制(SGTIN-96)，共由 Header、Filter Value、Partition、Company Prefix、Item Reference 以及 Serial Number 等六個欄位所組成：

- **Header**：使用八個Bits所構成的數值(0011 0000)表示標籤編碼機制。
- **Filter Value**：用以快速過濾資料以及事先選擇所需的貨物標籤型態，Filter Value欄位內符號所表示的意義如**表 四**所示：

Type	Binary Value
All Others	000
Retail Consumer Trade Item	001
Standard Trade Item Grouping	010
Single Shipping/ Consumer Trade Item	011
Inner Trade Item Grouping not to be sold at Point of Sale	100
Reserved	101
Reserved	110
Reserved	111

表 四：SGTIN 產品過濾值[20]

在**表 四**中可以看出 Filter Value 是由 3Bits 所組成，從 000 ~ 111 共有八種不同的形態(Type)，其中 Standard Trade Item Grouping 以及 Single Shipping/ Consumer Trade Item 這兩個類別是用來標示 RFID 標籤爲物流的型態。

- **Company Prefix：** 公司名稱有分隔符號時，用來表示在分隔符號前的文字。
- **Partition：**用來表示在Company Prefix所沒有表示完的公司名稱，也就是說Company Prefix加上Partition後才能表示完整的公司名稱，除了表示部分的公司名稱外，另外會指出Item Reference欄位將被分割成幾個部分。若是機關名稱的架構爲GS1 GTIN則Company Prefix將會加到Item Reference的個數裡，而Item Reference個數總共爲13 digits，Company Prefix的個數爲6到12個digits之間，所以Item Reference可以總7至1個digits之間。Partition、Company Prefix及Item Reference之間的關係如**表 五**所示。
- **Serial Number：** 在SGTIN-96的編碼中，只有代表integer-valued serial numbers界線範圍的能力。在GS1的表示中允許將Serial numbers的範圍擴大，在GS1-128的條碼提供20-character alphanumeric serial number 與GTIN結合作爲應用科技方面的身分驗證(AI) 21 [GS1 GS]。Serial numbers可以在GSTIN-96 tag encoding與AI21的barcodes在符合規範下進行轉換的動作。舉例來說像是在intercom version進行轉換的動作是可行的，當alphanumeric serial number in AI 21是由沒有leading zeros的digits以及整數所組成，將此值依照SGTIN-96 tag的規則進行編碼以及解碼。

Partition Value (*P*)	**Company Prefix**		**Indicator Digit and Item Reference**	
	Bits(M)	Digits(L)	Bits(N)	Digits
0	40	12	4	1
1	37	11	7	2
2	34	10	10	3
3	30	9	14	4
4	27	8	17	5
5	24	7	20	6
6	20	6	24	7

表 五：SGTIN Partitions 欄位數值對應[20]

從表五中可看出 Partition value 是由 3 bits 所構成，在 EPC global Class1 Cen2 所定義 RFID 標籤標準，將 Company Prefix 與 Item Reference 欄位由 Partition value = 0 ~ Partition value = 6，分成七種配置的方式。

2.3 應用密碼學

近年來企業推動無紙化方案，紛紛將公司的資料從紙本的格式轉成電子資料，且資料的傳送由原本人工的方式轉變成透過網際網路來傳遞，在資料電子化後，外洩的可能性也隨之提高，因此在此小節將介紹資料安全保護機制，對稱/非對稱加密演算法。

2.3.1 對稱式加密演算法

對稱金鑰密碼法也就是傳統的加密法。一個傳統加密系統有下列五大元素：明文、加密演算法、秘密金鑰、密文以及解密演算法如**圖 四：對稱式加密演算法**所示[21] 。

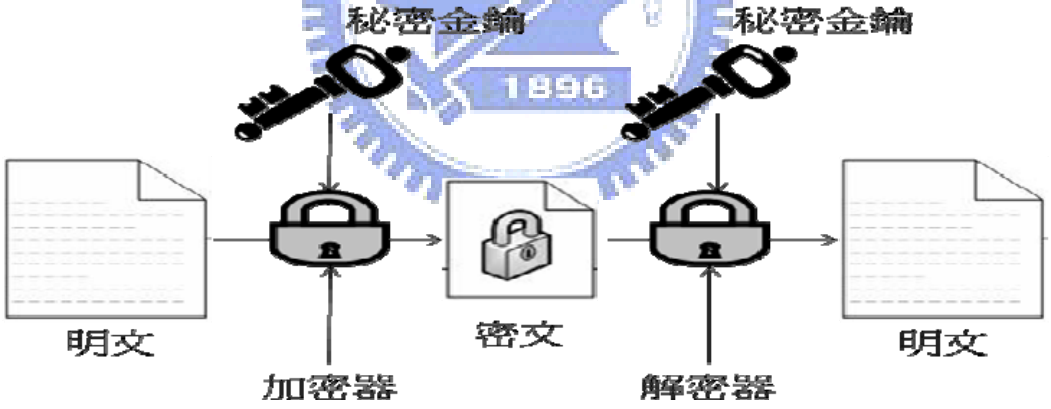


圖 四：對稱式加密演算法

- 明文(Plaintext)：
  未經加密的資料。
- 加密演算法(Encryption algorithm)：
  加密演算法經過替換(substitution)或排列(transformation)的方式來對明文進行加密的運算。
- 秘密金鑰(Secrete key)：
  加密解密過程中，所需要的關鍵資訊。根據這個秘密金鑰，演算法會對加解密的資料採不同的替換或是排列的運算。

- 密文(Ciphertext)：

  明文經過加密演算法處理後，所輸出的不規則資料。密文會根據明文與密密金鑰的不同而有所變化。例如：對同一個 message 來說，兩把不同的 key 便會產生兩種內容截然不同的密文。

- 解密演算法(Decryption algorithm)：

  其實就是加密演算法反向的程序。因此將加密過後的密文以及所用的那把秘密金鑰輸入給解密演算法，便可得到對應的明文。

想要使用傳統加密演算法來達資料保密的效果，要注意到必須滿足下列的兩個條件：

1. 加密演算法要非常堅固。我們希望就算攻擊者知道加解密的過程，而且取得一個甚至多個密文，也無法得知原來對應的明文或者是猜出使用者所使用的 key。甚者，在攻擊者取得幾組明文以及相對應所產生出來的密文，也無法依此爲憑據進行解密或者是推算出 key 來。
2. 因爲加解密的過程都需要 secrete key 來參與，因此傳送以及接收訊息的雙方都必須以極度安全的方式來保存他們所公用的 secrete key。假如不小心被他人竊得，則使用這把 key 所傳送的任何訊息都將會被解密失去其機密性。

2.3.2 非對稱式加密演算法

非對稱式加密演算法共有六個主要的組成元素爲：明文、密文、加密演算法、解密演算法、公開金鑰與私密金鑰如下**圖 五**所示：

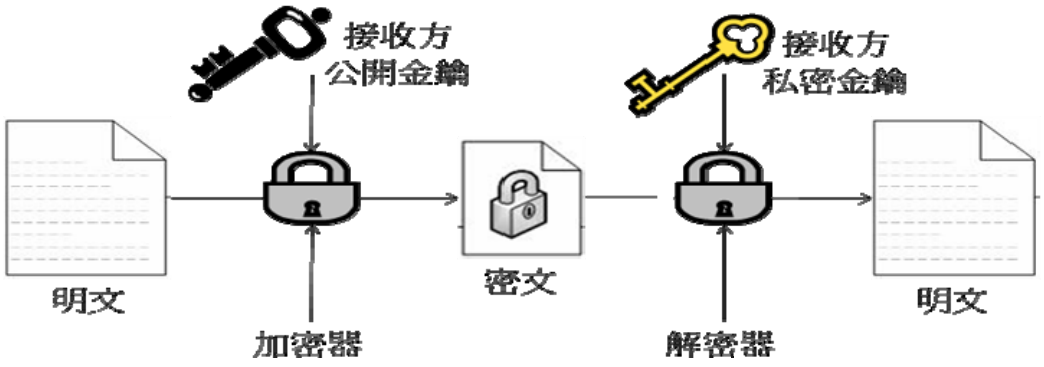


圖 五：非對稱加密演算法

- 明文：

  是一個可閱讀的訊息或資料，用來當演算法的輸入。

- 密文：

  在訊息經由演算法運算後，所產生出來的結果。由明文與金鑰的計算結果決定內容。如果相同的一個訊息，對此訊息分別以兩把不同的金鑰作加密的運算，會產生出不同密文。

- 加密演算法：

  是一個將明文作多重轉換的演算法。

- 解密演算法：

  這個演算法以密文以及對應的金鑰作爲演算法的輸入，而產生的結果即爲原來的明文。

- 公開金鑰和私密金鑰：

  是一對金鑰，當其中的一把用來加密，則另一把金鑰就用來做解密。而加密演算法所產出的密文其效用是取決於提供的輸入金鑰是屬於公開金鑰還是私密金鑰。

依其應用的不同，發送訊息的人可以使用自己的私密金鑰來加密，也可以用接收訊息者的公開金鑰加密。我們可以將公開金鑰加密系統的是使用方式分成下列兩項：

- 加密與解密：發送者將訊息以接收者的公開金鑰加密後，在接收方取得加密訊息後，以自己的私密金鑰將之解開。
- 數位簽章：發送者用自己的私密金鑰作爲輸入，使用加密演算法運算得到密文後，當接收方取得訊息後以發送方的公開金鑰驗證此密文。

雜湊函數(Hash Function)：

對一個變動長度的訊息 M 來說，一個雜湊值(Hash Value)的產生主要是由訊息 M 與雜湊函數 H 運算所得，如下所示[22] ：

$$\text{雜湊值(Hash Value)} = H(M)$$

雜湊值的大小是固定的，通常雜湊值被附加在原始訊息的後面，作爲訊息驗證的依據。當接收者收到訊息時，可以重新計算雜湊值，用以驗證該訊息是否在傳送的過程中遭竄改。

雜湊函數需求：

對於雜湊函數在網路文件安全方面的用途，主要可作爲訊息的「指紋(fingerprint)」看待，一個雜湊函數應該滿足下列幾個特性：

一、應用層面廣與使用簡易：

在訊息驗證方面，雜湊函數應該具有下列幾個特性：

1. 可適用於任何大小的資料區塊。
2. 產生的雜湊值要具備固定長度。
3. 不管用軟體或硬體方式運算雜湊函數，皆要容易實作。

二、單向性：

雜湊函數須具備「單向性(one-way)」，換句話說，由訊息來計算雜湊值是很容易的，但由雜湊值來反推訊息是相當困難的。這個特性相當的重要，由其是在傳送包含機密訊息的資訊密文時，若攻擊者可以由密文去推得機密訊息時，那採用雜湊函數來保護機密訊息的功用便會失效。舉例來說M:原始訊息、S_{key}：亂數、H：雜湊函數、C：密文運算如下所示：

$$C = H(M \,||\, S_{key})$$

如果雜湊函數非單向函數時，則攻擊方可以藉由雜湊函數的反運算以及所竊取到的密文來推得原始訊息如下所示：

$$M \,||\, S_{key} = H^{-1}(C)$$

三、抗碰撞性：

當一個雜湊值使用編碼策略傳送時，必須要能夠抗碰撞(collision resistance)，這種抗碰撞性可以分成兩種，分別是「弱抗碰撞性(weak collision resistance)」與「強抗碰撞性(strong collision resistance)」，說明如下：

弱抗碰撞性：

不管在任何區塊 x 而言，當 $x \neq y$ 時，幾乎不可能找到 H(x)=H(y)的情況出現。

強抗碰撞性：

在任何的情形下幾乎不可能去找到一個對偶配對(x，y)，使得H(x)=H(y)這個式子成立。

數位簽章：

在面對不完全信任的對象時，提供一個驗證其身分的方法是需要的，而在這些方法裡最廣受大家好評的就是「數位簽章」，其具備下列幾個特性[22] ：

1. 要能證明訊息發送者，與簽證的日期與時間。
2. 在簽證時，須能驗證訊息內容。
3. 簽證可被第三者核實，以解決訊息發送者拒絕承認的問題。

由上述特性看來，數位簽章本身就已經具有「驗證(authentication)」的功能，而對一個數位簽章所需要的基本需求有：

1. 產生數位簽章流程需簡易。
2. 數位簽章容易比對與核實。
3. 數位簽章必須要有傳送者的單一識別碼，以避免訊息僞造。

數位簽章可歸納出兩種不同的簽章模式，一種是「直接式數位簽章(direct digital signature)」，另一種爲「仲裁式數位簽章(arbitrated digital signature)」。

直接式數位簽章(direct digital signature)：

這種方式使用的是公開金鑰機制來達成，使用者利用本身私鑰(private key)作爲數位簽章的方式。此種簽章的方法若是基於雙方都是互信的狀態下，訊息認證與數位簽章的公信力是足夠的，但是對方若是信賴關係不明者，使用此法的簽章機制便無法有強制性的證明來源者。因對方可說私鑰遺失，以辯解該訊息並非他所發送。

仲裁式數位簽章(arbitrated digital signature)

此種數位簽章方式，是溝通雙方透過具公信力第三方來傳遞訊息。這種仲裁方式的數位簽章機制大都有共同的基礎特徵，那就是傳訊過程中都參有第三者的見證。第三者所擔任的角色一般可分爲兩種，其一爲擔任「傳送者鑑定」，另一角色爲「訊息傳送見證」。在第一種功能方面，傳送者將訊息傳送至仲裁者 X 時，仲裁者會加上傳送者的識別 ID，並加上本身簽名後轉送到使用者 B；而在訊息見證方面，仲裁者將傳送者訊息加上識別 ID 外，也會在訊息後面加上「時

間簽證(Timestamps)」，並轉送訊息到 B。因此在仲裁式數位簽章協定中，訊息傳送可分成「A→X」與「X→B」兩部分來看。

2.3.3 公鑰基礎管理建設(Open CA)

在 PKI 系統架構下最主要的兩個元件分別爲 CA Server 以及 RA Server。在功能方面 CA Server 包含所有建立及修改憑證以及憑證廢止清冊(CRL)的功能，除了上述的基本功能外尚提供批次處理系統，在 CA Server 收到使用者申請憑證資料後，可自動化的建立該使用者的憑證資料。RA Server 負責處理所有的使用者申請要求，其功能包含編輯申請、核准申請、建立私密金鑰以及刪除錯誤申請資料等等。

OpenCA 管理憑證的架構如**圖 六**所示，CA Server 與 RA Server 透過 Node 模組進行管理的機制，Node 提供匯入及匯出資料的功用且可初始化資料庫。CA Server 與 RA Server 本身也都有各自的介面可以進行系統控制，在權限管控方面只有 CA Server 的管理者才能使用 CA Server 所提供的所有管理機制，而 RA Server 除了其管理功能外，其餘的模組一般的使用者皆可使用。

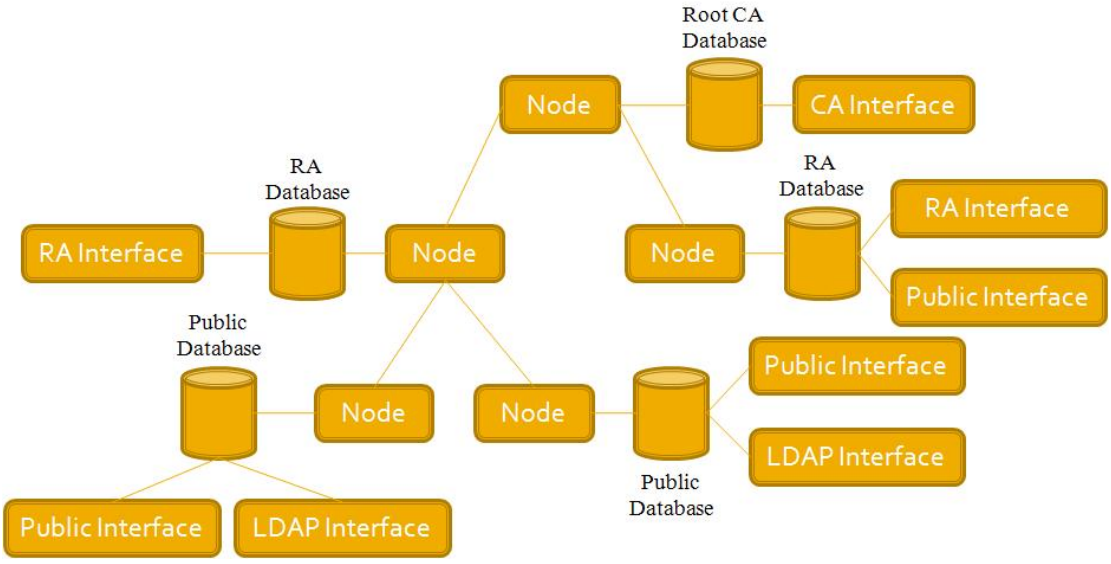


圖 六：OpenCA 憑證管理系統架構

OpenCA 電子憑證申請流程如**圖 七**所示，一開始使用者提出申請後，此申請訊息會先在 RA Server 中等候申請通過，若不通過則刪除此申請請求。在通過 RA Server 的憑證申請審核後，RA Server 會將此請求傳送至 CA Server 進入 Approved Request 的狀態，等待 CA Server 的審核通知。當 CA Server 審核通過後便會核發憑證，且 CA Server 也會將此憑證存入資料庫中。

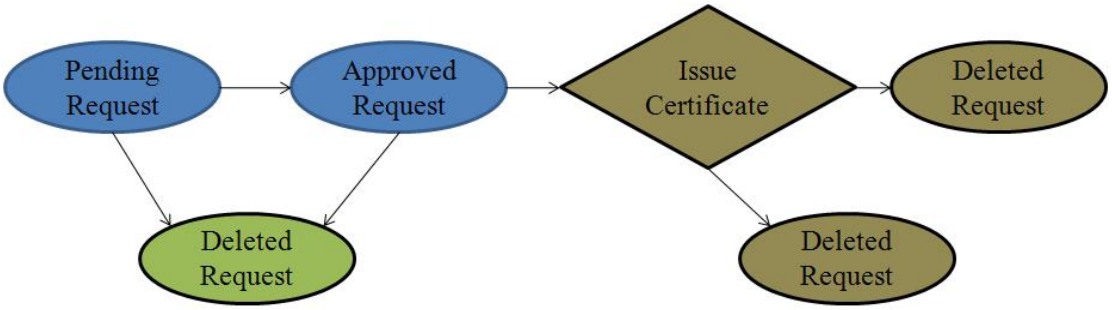


圖 七：OpenCA 申請憑證流程

申請憑證流程中的元件說明：

- **Pending Request：**
  在 RA 和 CA 中所代表的意義不同，在 RA 中是等候證書驗證（proved），在 CA 中是等候證書簽名。
- **Approved Request：**
  通過驗證但未给 CA 簽名時所發出的請求。
- **Deleted Request：**
  所有刪除的請求。
- **Archived Request：**
  通過所有驗證並導到 CA 的證書所發出的請求。
- **Issue Certificate：**
  判斷申請憑證訊息使用者的身分
- Valid/Expired Certificate：
  存放 CA 簽發的憑證資料庫。

三、相關研究

目前 RFID 標籤驗證相關研究可分爲中央集權式(Centralized Server)以及非集權式(Serverless)兩部分，中央集權式驗證系統運作時，須有 Back-End Server 與網際網路輔助，而非集權式驗證系統可在無網路環境下完成標籤驗證，但在系統運行前須至可信任的第三方取得授權資訊，在此章節將說明中央集權/非集權式 RFID 標籤驗證協定。

3.1 RFID 中央集權式認證協定

RFID 中央集權式(Centralized Server)驗證協定，是由 RFID 標籤(Tag)、RFID 讀寫器(Reader)以及 Back-End Server 所構成，其系統運作爲 RFID 讀寫器將所取得標籤資料經由網際網路傳送至後台伺服器(Back-End Server)進行標籤驗證，最後將驗證結果傳回 RFID 讀寫器完成標籤驗證機制，在本節將說明建立在中央集權驗證基礎上的雜湊標籤驗證機制以及互斥標籤驗證機制。

3.1.1 雜湊機制

本小節所介紹中央集權式雜湊驗證機制，在 RFID 電子標籤內儲存識別ID資料以及Secret Key，執行標籤驗證時系統將電子標籤內所存資料利用SHA1雜湊函數運算其摘要值後，將此摘要值傳送至Back-End Server驗證該標籤合法性，接下來說明該機制的符號定義以及細部運作流程。

在表六中Back-End Server存放RFID電子標籤序號($ID_{1\sim n}$)以及RFID電子標籤金鑰($K_{1\sim n}$)，當Back-End Server收到RFID讀寫器所傳送的RFID標籤摘要值時，便使用SHA1雜湊函數以及資料庫內的$ID_{1\sim n}$、$K_{1\sim n}$驗證標籤正確性。IRq、IRs以及SRq為資料清單請求格式被定義在 ISO/IEC1800-3[4] ，在驗證系統傳遞機密資訊時利用ISO/IEC1800-3所定義的資料格式封裝後，在傳送至目的端可增加資料傳送時的安全性。

定義符號：

Tag	RFID 電子標籤
Reader	RFID讀寫器
Back-end Server	爲一資料庫其內容包含電子標籤序號(ID1~n)、電子標籤金鑰(K1~n)以及電子標籤所存資料
K_i、K_0	每一個Tag與server間皆有一對Secret key,K0爲share key
H	雜湊函數
S	雜湊值(S = H(r))
IRq	Inventory request format with S
HT_1	雜湊值(H(S || K1 || D1))
IRs	Inventory request format with HT1
SRq	Inventory request format with K0

表 六：中央集權式雜湊驗證協定符號定義

驗證流程圖：

驗證機制如**圖 八**所示是建立在三次的挑戰與回應(three-way challenge response)，首先由RFID讀寫器產生亂數(r)封裝後傳送至RFID標籤，而後RFID標籤發出回應的資料傳送回RFID讀寫器。此機制所使用的亂數是由RFID讀寫器所產生，在傳統的雜湊驗證機制中亂數皆是由RFID標籤所產生[2] ，所以我們可以比傳統的雜湊驗證機制[2] 使用成本更低的RFID標籤。

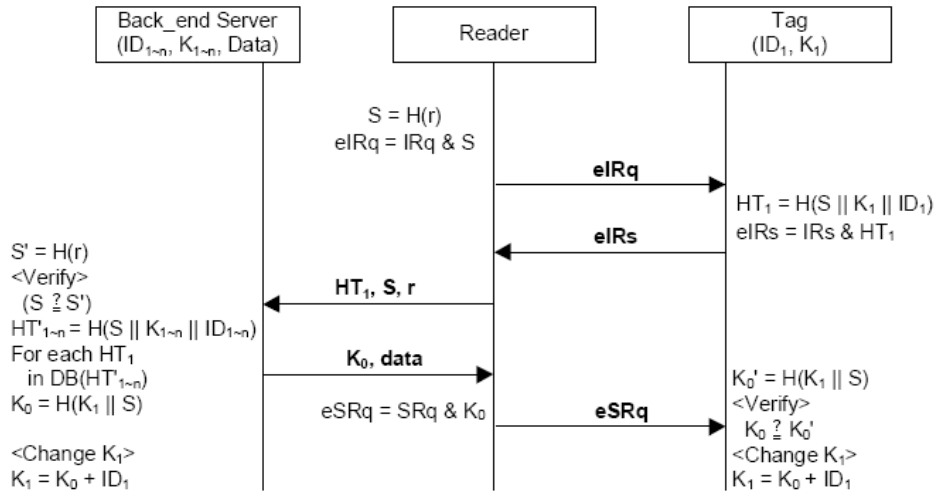


圖 八：中央集權式雜湊驗證機制

中央集權式雜湊驗證機制步驟：

步驟1：

RFID 讀寫器傳送請求訊息 S(H(r)) 至 RFID 標籤。在此我們定義這個請求訊息是延伸的資料清單請求格式如**表 七**所示稱之爲 elRq，其原始的資料清單請求格式被定義在 ISO/IEC1800-3[4] 。

步驟2：

RFID標籤首先運算得到HT1(HT1 = H(S ‖ K_1 ‖ ID_1))，符號‖所代表的意義爲將兩筆資料結合成一筆，然後再將所得到的HT_1插入IRs的欄位中。IRs爲延伸的資料清單請求格式其詳細欄位資料如**表 八**所示，而IRs原始的資料格式爲ISO/IEC1800-3所定義的資料清單回應格式，最後RFID將IRS以及HT1結合成elRs回應至RFID讀寫器，在此所產生的HT1可以保護man-in-the-middle-attack行爲。

步驟3：

RFID讀寫器將雜湊值 S 、亂數 r 以及雜湊值 HT_1傳送至後台伺服器。

步驟4：

後台伺服器利用所接收到的亂數 r 來產生雜湊值 S'(H(r)) ，來與所收到的雜湊值 S 做比對，若s' 與 s一致則表示傳送此訊息的RFID讀寫器是合法的，再來將所收到的HT_1與後台伺服器內所儲存的$HT'_{1\sim n}$比對用以驗證RFID標籤是否合法，若合法則後台伺服器會傳送K_0以及data其中K_0 = H(K_1 ‖ S)，data爲RFID標籤所存的資料。在此步驟RFID讀寫器的驗證已完成，而所傳送的K_0是用來驗證RFID標籤，且在伺服器中所存的K_1也會改變。$K_1 = K_0 + ID_1$。

步驟5：

RFID讀寫器使用K_0重新建構延伸選擇請求的資料格式(eSRq = SRq & K_0)，然後將此eSRq傳送至RFID標籤，SRq詳細資料欄位如**表 九**所示。

步驟6：

RFID標籤計算出K'_0(H(K1 ‖ S))，接下來比對K'_0與所接收到的K_0是否相同，若相同則更新RFID標籤內所儲存的K_1。$K_1 = K_0 + ID_1$，因此RFID標籤可避免重現攻擊。

協定中所使用的延伸資料格式：

在ISO/IEC 18000-3規格書中主要是在描述頻率13.56Mhz的RFID標籤與RFID讀寫器之間的溝通[4] [5] 。在請求與回應的訊息其資料欄位皆包含Start-of-Frame (SOF)以及End-of-Frame (EOF)，在一般的請求訊息欄位是由SOF、Flag、Command Code、Parameters、Data、CRC以及EOF所組成。

Command Code主要是由四個命令型態所組成，其命令定義爲Mandatory、Optional、Custom以及Proprietary。在驗證的機制中主要會使用到定義在Mandatory以及Optional型態裡的Inventory及Select指令來達成兩個裝置之間的溝通。在**表七**的資料格式爲更改規格書裡所定義的Inventory request format(IRq)資料欄位，將本機制所產生的雜湊值S加入到IRq中，形成本機制所需的elRq資料欄位。

SOF	Flags	Invent	Opt. AFI	Mask length	Mask value	S	CRC	EOF
	8bits	8bits	8bits	8bits	0-64 bits	16bits	16bits	

表 七：包含 S 請求訊息延伸的資料清單格式

在規格書中請求訊息的內容欄位包含 Flags、Inventory、Optional AFI、Mask Length、Mask Value 以及 CRC。而在延伸的版本中只是單純的將雜湊值 S 加入到欄位裡，然後將此 elRq 資料傳送至 RFID 標籤。當 RFID 標籤收到 elRq 後，使用延伸的回應訊息欄位格式，在加上 RFID 標籤所產生的雜湊值 HT_1 如表**表 八**所示：

SOF	Flags	DSFID	HT_1	CRC	EOF
	8bits	8bits	64bits	16bits	

表 八：包含 HT1 延伸資料回應訊息格式

在規格書中清單回應訊息欄位包含 Flags、DSFID、UID 以及 CRF，但是在延伸的欄位格式中我們將 UID 的欄位替換成 HT1。此 64-bits 的 HT1 主要是用來驗證 RFID 標籤所送的回應訊息真僞，因此在**圖 八**所示的驗證機制，就算延伸清單回應訊息被攻擊者所截取，對於本驗證機制並不會造成任何的威脅，因爲對於攻擊者來說延伸清單回應訊息裡的所有資料皆是無用的。

在延伸選擇請求封包格式是由ISO/IEC 1800-3規格書中所定義的選擇請求欄位插入K_0所更改而成的，詳細的資料欄位如**表 九**所式：

SOF	Flags	Select	UID	K_0	CRC	EOF
	8bits	8bits	64bits	16bits	16bits	

表 九：包含 K_0 延伸選擇請求資料格式

在ISO/IEC 1800-3規格書中選擇請求資料欄位包含Flags、Select、UID以及CRC，而在本延伸的版本中只是將K_0附加進此資料欄位裡。在本機制裡K_0是由伺服器裡的雜湊函數所產生的雜湊值，此值會與Data一起傳送至RFID讀寫器，再有RFID讀寫器寫入RFID標籤，當RFID標籤收到Select指令後，會產生雜湊值K_0'與K_0作比對，若相符則RFID電子標籤會藉由所收到的K_0雜湊值更新其目前的金鑰K_1($K_1 = K_0 + ID_1$)。

3.1.2 互斥機制

在RFID認證機制中提供一個有效率且低成本的協定，一直以來都是研究RFID認證協定的單位所追求的目標，針對此目的在本小節中將說明使用互斥運算來達成驗證標籤的目地，接下來說明該機制的符號定義以及細部運作流程。

定義符號：

S	RFID電子標籤識別ID
P	部分ID
r,i	亂數
備註： 1. 伺服器與RFID標籤擁有相同的S 2. RFID標籤含ID及S 3. RFID讀寫器內建亂數產生器 4. 亂數產生的值範圍不可超過R; 1 < R < length(TagID)	

表 十：中央集權式互斥標籤驗證機制符號定義

在表十中所定義的亂數(r、i)表示長度不可超出 TagID(S)，因爲亂數(r、i)是用來指定本次 Session 要取出 TagID(S)的哪些欄位做互斥的運算，以產生標籤驗證的資料。Back-End Server 在本機制所存放的資料爲 RFID 標籤的 Serial Number(S)，在收到 RFID 讀寫器所傳送的資料後，運算內部所存的 RFID 標籤 Serial Number 是否有相符。

部分ID(P)產生方程式：

$$P = P_{odd} \oplus P_{even},$$
$$where \begin{cases} P_{odd} = f(S,i,odd) \\ P_{even} = f(S,i,even), \end{cases} \quad (1)$$

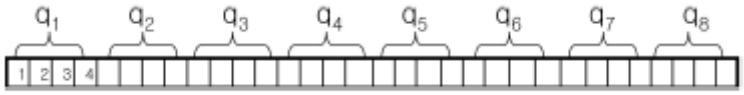


圖 九：部分 ID 產生演算法

f(S; i; b)函式內S爲bit的字串、i爲整數以及b爲布林代數值(True/False)，若b爲T則代表odd反之則爲even。舉例來說 i = 4、S = 32bits則P_{odd} = f(S;4;T) = $q_1 \| q_3 \| q_5 \| q_7$ 以及 P_{even} = f(S;4;F) = $q_2 \| q_4 \| q_6 \| q_8$如**圖 九**所示

互斥驗證流程圖：

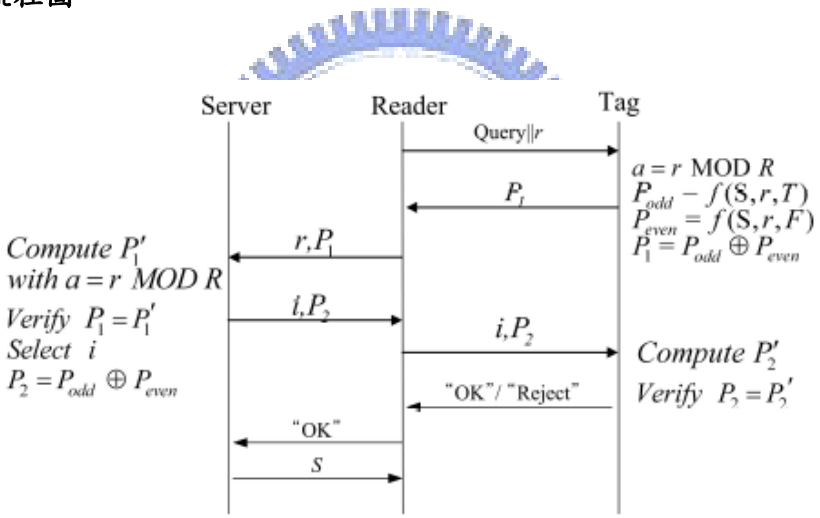


圖 十：互斥認證協定流程

中央集權式互斥標籤驗證演算法流程如**圖 十**所示，由 RFID 讀寫器(Reader)傳送亂數(r)至 RFID 標籤(Tag)發出請求(Query)後，RFID 標籤利用亂數(i)運算出驗證資料(P)，且將此值傳送至驗證伺服器以執行標籤合法性識別詳細步驟如下：

Step 1: Generating P by the tag

1. RFID讀寫器產生亂數r且傳送至RFID標籤。
2. RFID標籤利用本身擁有的S以及從RFID讀寫器所收到的r產生P_1。
3. RFID標籤將此P_1傳送至RFID讀寫器。

Step 2: The tag authentication

1. RFID讀寫器傳送 r 以及 P_1 至伺服器(Back-End Server)。
2. 伺服器將收到的P_1與所儲存的每一個合法RFID標籤運算得出P_i做比對，若有相符則表示此RFID標籤爲合法的。
3. 伺服器產生一亂數值 i 且利用此 i 值，計算出新的部分ID(P_2)後，將此P_2與i傳送至RFID讀寫器

Step 3: The reader authentication

- RFID讀寫器傳送P_2及i至RFID標籤。
- RFID標籤利用所收到的i值以及本身所擁有的S計算出P，然後與P_2做比對動作，若相符則表示此RFID讀寫器爲合法的。
- 若RFID讀寫器爲合法則RFID標籤回傳"OK"反之則回傳"Reject"。

Step 4: Return result

- 若RFID讀寫器收到"OK"訊息，則將此訊息傳送至伺服器。
- 當伺服器收到"OK"訊息後，則將對應的私密值S_i傳送至RFID讀寫器。

3.2 RFID 非集權式認證協定

RFID 非集權式(Serverless)驗證協定採用 RFID 標籤(Tag)與 RFID 讀寫器(Reader)相互認證(Mutual Authentication)，達成驗證 RFID 標籤合法性的目地。在 RFID 非集權式驗證系統 RFID 標籤與 RFID 讀寫器皆擁有相當高的運算能力，因此當 RFID 讀寫器獲得 RFID 標籤資料時即可進行比對的運算，判斷該 RFID 標籤是否合法，所以非集權式驗證系統不需網路傳遞標籤資料且不需要建製 Back-End Server 來處理標籤驗證的相關運算，但當非集權式驗證協定系統運作前，須至可信任的公正第三方取得合法的授權，此小節將說明建立在非集權是基礎上的靜態/動態清單憑證協定驗證機制。

3.2.1 靜態清單憑證協定

ROAD 非集權式靜態清單憑證識別協定，系統執行前 RFID 讀寫器(Reader)須至可信任公正第三方機構取得 RFID 標籤(Tag)ID 以及標籤識別資料($g(id_r \| k_1)$)，RFID 讀寫器取得授權資訊後，即可利用雜湊運算驗證 RFID 標籤的合法性，接下來說明 ROAD 機制的符號定義以及細部運作流程

定義符號：

r_i	亂數
k_t	RFID 標籤 t 的秘密金鑰
id_t	RFID 標籤 t 的識別 ID
id_r	RFID 讀寫器 r 的識別 ID
h, g	雜湊函數
S	h,g 所產生的雜湊值長度
CA	公正第三方授權單位
L	CA 發佈給授權 RFID 讀寫器的授權清單
⊕	互斥函數

表 十一：非集權式靜態授權清單驗證協定符號定義

表 十一中 CA 爲可信任公正第三方，負責 RFID 標籤(Tag)註冊取得合法辨識身份，以及 RFID 讀寫器(Reader)註冊取得授權清單(L)。L(授權清單)紀錄可讀取的 RFID 標籤資料(ID、$(g(id_r \| k_1))$。

ROAD 初始化：

RFID 讀寫器(Reader)連線至具公信力第三方機構(CA)註冊以取得使用系統的合法授權。若 RFID 讀寫器取得合法授權後，可從 CA 取得紀錄可讀取 RFID 標籤的授權清單(L)，授權清單詳細資料如表**表 十二**所示：

$g(id_1 \| k_1)$	id_1
……	……
$g(idr \| k_r)$	Id_t
……	……
$g(id_n \| k_n)$	id_n

表 十二：ROAD 驗證協定授權清單

上表爲ROAD標籤驗證機制所定義的授權清單，紀錄RFID讀寫器(Reader)可讀寫的RFID標籤相關資訊，所記錄的資料爲每一個RFID標籤所對應的識別資料 $g(id_1 \| k_1)$。$g(id_1 \| k_1)$爲RFID標籤識別ID以及私密金鑰(Secret Key)，利用雜湊函數運算所得。

ROAD系統運作：

當RFID讀寫器(Reader)要取得某一個RFID標籤(Tag)私密內容時，RFID讀寫器會發出請求訊息(Request)，在訊號傳遞範圍內的RFID標籤皆會回應訊息($g(idr \| k_r)$)給RFID讀寫器，最後RFID讀寫器將所收到的$g(idr \| k_r)$與授權清單內容進行比對判斷RFID標籤的合法性。ROAD驗證協定詳細步驟如**圖 十一**所示：

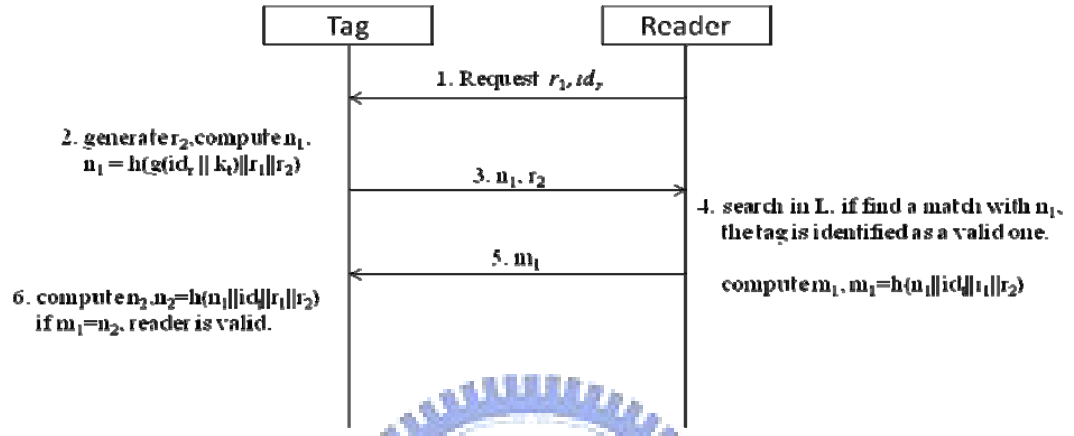


圖 十一：ROAD 驗證協定流程

步驟1：

RFID讀寫器產生一亂數 r_1 後，將此亂數值 r_1 以及RFID讀寫器 r 識別ID(id_r)傳送至RFID標籤。

步驟2：

RFID標籤收到訊息後，產生一亂數值r_2，且將此亂數值與本身識別ID以及本身秘密金鑰再加上亂數值r_1用以產生雜湊值$n_1 = h(g(id_r \| k_t) \| r_1 \| r_2)$，最後將此雜湊值$n_1$與亂數$r_2$回應至RFID讀寫器。

步驟3：

RFID讀寫器尋找授權清單內項目，利用項目內所記錄的值運算出雜湊值與所收到的雜湊值n_1做比對，若符合則表示該RFID標籤爲合法的，則該RFID讀寫器會計算出雜湊值$m_1 = h(n_1 \| id_t \| r_1 \| r_2)$且將$m_1$傳送至RFID標籤。

步驟4：

RFID標籤計算雜湊值$n_2 = h(n_1 \| id_t \| r_1 \| r_2)$ 然後比較n_2與m_1是否相符，若相同則表示該RFID讀寫器爲合法讀寫器，否則RFID標籤將不會再回任何訊息至此RFID讀寫器。

3.2.2 變動清單憑證協定

在 3.2.1 節中 ROAD 非集權式驗證協定，第三方機構儲存的授權清單內容(RFID 標籤識別資料)在短時間內便不會再更動，所以當授權清單資料外洩時 ROAD 非集權式驗證協定會變得無任何安全性可言，針對此漏洞在本節將介紹授權清單內容會隨著每一個回合驗證協定的執行而改變的非集權式驗證協定(S^3PR)，在接下來說明 S^3PR 機制的符號定義以及細部運作流程。

定義符號：

R:	RFID 讀寫器
r:	RFID 讀寫器 R 識別 ID
L:	TC 所發布之授權清單
TC:	公正第三方(授權中心)
id_t:	RFID 標籤 t 識別 ID
t:	RFID 標籤 t 私密值
P(.):	亂數產生器
Seed:	亂數產生種子
$Seed^0$	亂數產生種子(由 TC 所提供)
M(.):	雜湊函數
h(.):	雜湊函數
n_j^k	第 i 個 RFID 讀寫器利用 RFID 標籤 j 第 K 次的亂數種子產生亂數
n_j^k	第 j 個 RFID 標籤利用第 i 個 RFID 讀寫器第 K 次的亂數種子所產生的亂數值

表 十三：S^3PR 認證協定符號表

在**表 十三**中 TC 爲可信任的公正第三方機構負責產生 RFID 標籤(Tag)識別資料以及 RFID 讀寫器的權限控制。L(授權清單)由 TC 所發佈用來指定每一個 RFID 讀寫器可讀取的 RFID 標籤，在 S^3PR 認證協定 L 所記錄的匹配內容爲亂數種子($Seed_j^0$)與 RFID 標籤識別 ID 如**圖 十二**所示：

在下圖中可看出每一列所記錄的配對資料爲 RFID 標籤所持有的相關內容，舉例來說$Seed_j^0 : id_i$ 爲第 i 個合法 RFID 標籤所儲存的內容，因此合法授權 RFID 讀寫器可依授權清單內容驗證 RFID 標籤的合法性。

$$\mathcal{L}_i = \begin{Bmatrix} seed_1^0 : id_1 \\ seed_2^0 : id_2 \\ \cdot \\ \cdot \\ seed_n^0 : id_n \end{Bmatrix}$$

圖 十二：S[3]PR 授權清單資訊

亂數種子產生方程式：

當S[3]PR標籤驗證協定執行時在每一個Session中，皆會執行亂數種子產生方程式，得到RFID標籤新的配對亂數種子且利用此亂數種子更新RFID讀寫器中所存的授權清單，所以執行S[3]PR標籤驗證協定後，該RFID讀寫器所儲存的授權清單內容將會更新，亂數種子產生方程式執行流程如**圖 十三**所示

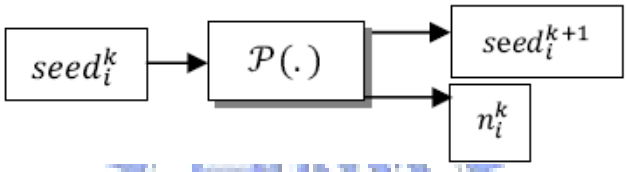


圖 十三：亂數產生方程式流程圖

以上圖來說 RFID 標籤(Ti)使用經過 K 次更新的第 i 個亂數種子產生亂數值，傳送至第 i 個 RFID 讀寫器時，RFID 標籤(Ti)在同時使用$seed_i^k$經雜湊函數產生新的亂數種子$seed_i^{k+1}$。

驗證流程圖：

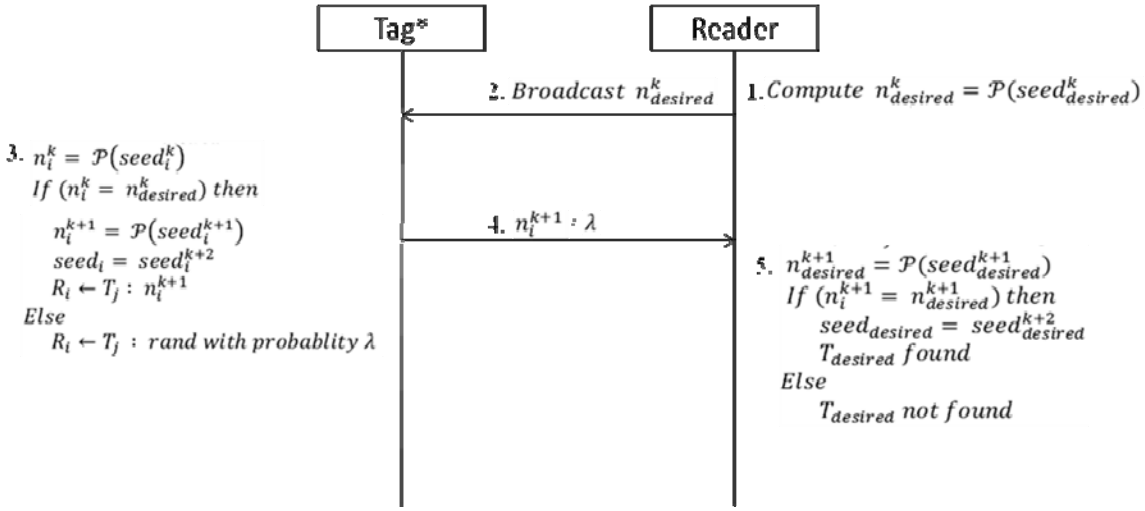


圖 **十四：S[3]PR 認證協定流程**

步驟 1：

RFID 讀寫器(Reader)從授權清單內取出所要驗證 RFID 標籤識別亂數種子$Seed^{k}_{desired}$，且利用$Seed^{k}_{desired}$以及亂數產生方程式 P 運算得到 RFID 標籤識別資料$n^{k}_{desired}$。

步驟 2：

RFID 讀寫器將所要驗證的 RFID 標籤識別資料$n^{k}_{desired}$廣播至溝通範圍內的所有 RFID 標籤。

步驟 3：

RFID 標籤(Tag)使用儲存的亂數種子($Seed^{k}_{i}$)以及亂數產生方程式(P)運算出n^{k}_{i}，且將此值與$n^{k}_{desired}$做比對，若相符則使用$Seed^{k+1}_{i}$產生 RFID 讀寫器識別資料n^{k+1}_{i}，且將亂數種子值更新至$Seed^{k+2}_{i}$若不符則產生 λ 值。

步驟 4：

RFID 讀寫器溝通範圍內的所有 RFID 標籤傳送比對結果n^{k+1}_{i} / λ 至 RFID 讀寫器。

步驟 5：

RFID 讀寫器(Reader) 授權清單內取出所要驗證 RFID 標籤識別亂數種子$Seed^{k+1}_{desired}$，且利用$Seed^{k+1}_{desired}$以及亂數產生方程式 P 運算得到$n^{k+1}_{desired}$，將此值與 RFID 標籤所傳送的n^{k+1}_{i}做比對，若相符則表示該 RFID 標籤爲合法的，且將$Seed^{k+2}_{desired}$更新至授權清單對應的 RFID 標籤配對欄中。

四、驗證協定設計與實作

本研究所提出的系統主要目的在於在無網路輔助的環境下，利用公開金鑰基礎建設(Public Key Infrastructure, PKI)、無線射頻辨識技術(RFID)以及密碼學相關演算法達成驗證貨物正確性的目的。

快速離線驗證系統運作可分成三個階段，首先使用者須至公開第三方認證機構申請合法憑證資料，之後利用此合法憑證至快速離線驗證系統中所建置的授權中心進行註冊以取得合法使用者身份，第二階段(貨物供應商出貨)擁有合法憑證貨物供應商可使用憑證資料經加密演算法運算得到商品識別資料，將此值與商品配對即可完成出貨動作。

第三階段(貨物集散驗證)當商品抵達時，貨物集散中心僅需取得商品上 RFID 標籤資料以及在第二階段所產生的商品識別資料即可識別貨物合法性，此章節將針對系統運作的三個階段進行說明。

4.1 系統概述

快速離線驗證平台是由憑證產生模組、貨物簽章模組以及貨物驗證模組所建構而成，當貨物供應商欲使用快速離線驗證平台時，須使用憑證產生模組所提供的操作介面與可信任的公正第三方(Open CA)以及快速離線驗證平台授權中心(Authentication Center)註冊，且經認證身份後取得系統合法使用權限。

貨物供應商具有系統合法使用權限後，當廠房貨物出口運作流程進行棧版與貨物封模(Wrap)時，須使用貨物簽章模組所提供的雜湊運算(Hash Function, SHA1)以及公開金鑰簽章演算法(Signature Algorithm, DSA)產生貨物識別資料，隨後將此識別資料寫入本論文所設計的識別標籤(V-Tag)中，最後將此識別標籤與出口貨物配對後即完成產品出口流程。

最後當貨物抵達集散中心(Distribution Center)時，使用貨物驗證模組所支援的雜湊運算(Hash Function, SHA1)、公開金鑰簽章演算法(Signature Algorithm, DSA)以及此該批貨物的標籤資料(棧版標籤、貨物標籤、識別標籤)，即可判斷抵達貨物是否合法，快速離線驗證機制架構如**圖 十五**所示。

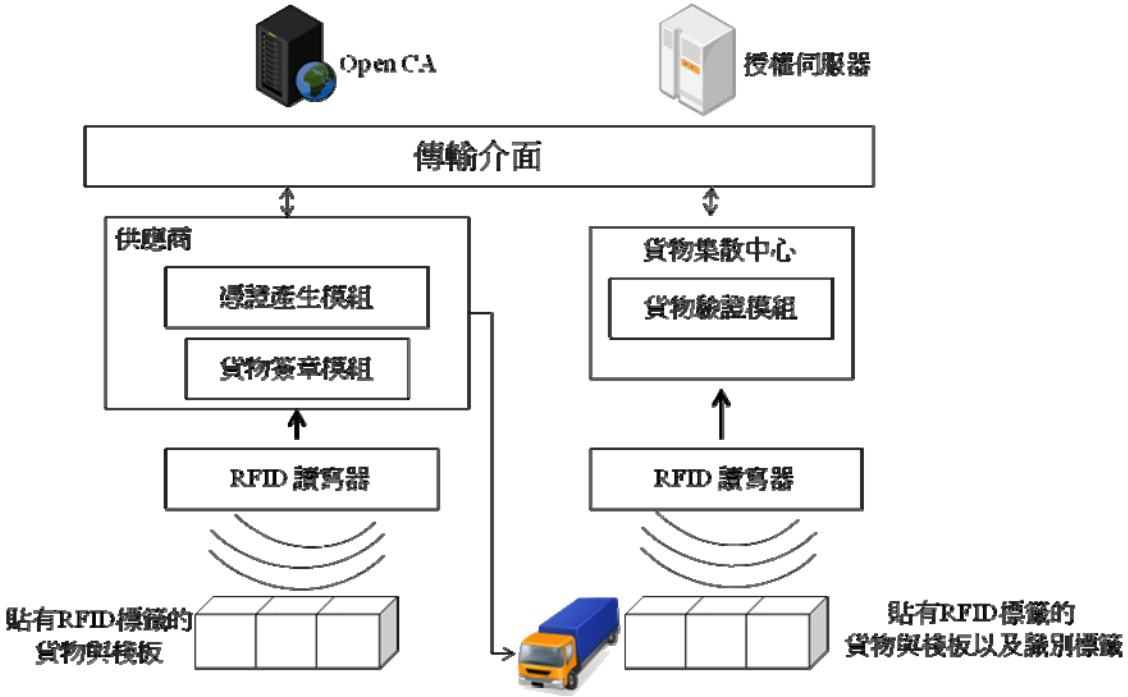


圖 十五：快速離線驗證機制系統架構

憑證產生模組：

在系統設定階段，協助產生供應商憑證資料後，連線至 OpenCA 驗證所產生的憑證資料合法性，且在取得 OpenCA 所授權的憑證後，立即連線至離線驗證平台所提供的授權伺服器(Authority Server)註冊已成爲系統的合法使用者。

貨物簽章模組：

在貨物供應商取得合法使用權限後此模組才可使用，當廠房貨物出口運作流程進行棧版與貨物封模(Wrap)時，將棧版以及棧板上的貨物 RFID 標籤，經由 SHA1 雜湊函數計算出雜湊值，且將利用 DSA 簽章演算法加密此雜湊值產生貨物識別資料，最後將識別資料寫入本論文所設計的識別標籤中即可完成出貨的程序。

貨物驗證模組：

當承載貨物的棧板抵達集散中心驗證閘門時，RFID 讀寫器讀取閘門內的 RFID 標籤資料(棧版、貨物)，且使用 SHA1 雜湊函數運算得到雜湊值(Meta')後，將此(Meta')與識別標籤(V-Tag)記錄的識別資料經 DSA 簽章演算法運算比對即可判別出貨物的供應商是否合法、貨物數量是否正確以及貨物在運送途中是否被置換。

4.2 系統設定階段

快速離線驗證平台採取非集權式(Serverless)驗證協定架構，使用者在執行驗證機制前需至可信任的公正第三方機構取得授權，在本論文所提出的快速離線驗證平台，使用者需至公開金鑰基礎建設(Public Key Infrastructure, PKI)取得合法憑證資料(Certificate)以及利用此憑證資料向快速離線驗證平台所提供的授權伺服器(Authority Server)註冊，成爲合法系統使用者。

接下來將針對公開金鑰基礎建設(Public Key Infrastructure, PKI)授權憑證申請驗證協定以及快速離線驗證平台所提供的授權伺服器(Authority Server)註冊驗證流程進行說明。

4.2.1 合法憑證申請

在使用安全物流系統所提供的服務(快速離線驗證平台)前，須先至可信任的公開金鑰基礎建設(Open CA)所提供的憑證機構(Certification Authorities , CA)註冊，通過憑證機構審核後即可取得合法的憑證，其運作流程如**圖 十六**所示：

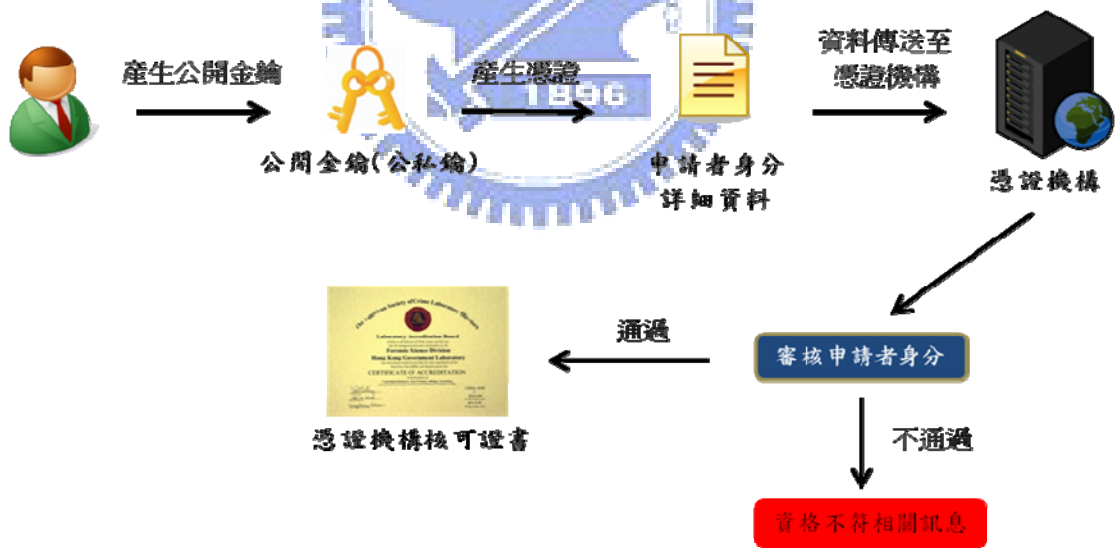


圖 十六：使用者憑證申請流程

使用者利用 FOLVCG 產生公開金鑰對(Public Key/ Private Key)後，使用 FOLVCG 所提供的憑證產生模組執行 PKCS10 封裝後，得到未經 CA 審核的憑證資料(Certificate)，緊接著將此憑證資料傳送至 OpenCA 架構下的憑證機構(CA)審核，當憑證通過審核後，憑證機構會在該憑證內容附加上本身的簽章，以保證此資料已通過驗證。

4.2.2 合法憑證登入

當使用者取得 Open CA 所建製的憑證機構所核發憑證後，接下來須至快速離線驗證平台所建置的授權伺服器(Authority Server)，註冊合法憑證與使用者配對資料，藉由此步驟，當供應商運送貨物抵達目的地時，快速離線驗證平台貨物驗證模組才可經由貨物識別標籤所提供的資訊，篩選符合憑證資料以進行貨物的合法性判別，使用者需填寫的配對資料如**圖 十七**所示：

圖 十七：供應商憑證配對資料

在**圖 十七**中公司統一編號代碼以及註冊憑證編號欄位合併後資料，用來表示此憑證的註冊 ID。

申請人姓名、申請人編制單位、申請人組織名稱、申請人所在縣市或區域以及申請人所在單位二位國碼，這五個資料欄位構成憑證機構(CA)，用來識別憑證資料的名稱(Distinguished Names , DN)。

當使用者送出註冊資料後，授權伺服器(Authority Server)自動連結至憑證機構(CA)，且利用**圖 十七**所填申請人姓名、申請人編制單位、申請人組織名稱、申請人所在縣市或區域以及申請人所在單位二位國碼所構成的憑證識別名稱查詢，憑證機構合法憑證清單中是否有該筆資料，若有則回傳合法憑證資訊且授權伺服器會發送合法使用者通知給該註冊公司，否則回傳 Null 且授權伺服器傳送憑證資訊錯誤訊息給該註冊公司。

4.2.3 有效憑證更新

憑證機構(CA)所核發的憑證會有下列三種合法憑證清單項目變動的情形發生，第一種使用者憑證過期、第二種使用者向憑證機構(CA)申請註銷憑證以及憑證機構主動註銷憑證，當公開金鑰基礎建設(Public Key Infrastructure, PKI)的合法憑證有所變動時，被註銷的憑證資料會被紀錄在證書撤銷列表(Certificate Revocation List , CRL)中，因此授權伺服器(Authority Server)需定期的更新儲存的憑證資料，以避免使用已被註銷的憑證資料來驗證貨物，其運作的情境如**圖 十八**所示。

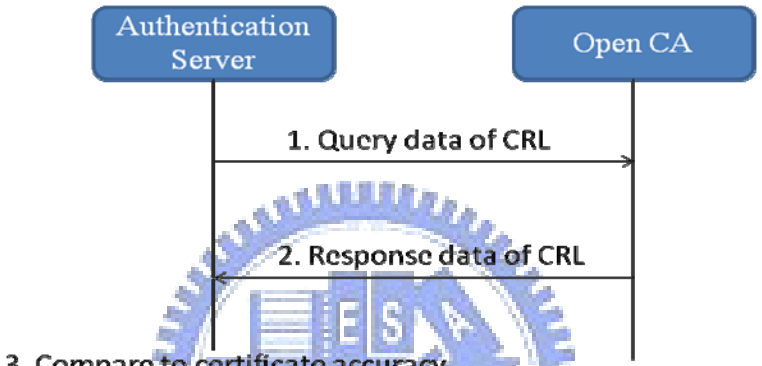


圖 十八：憑證資料更新流程

在**圖 十八**中有效憑證更新流程如下：

步驟 1：

授權伺服器向 OpenCA 所提供的憑證機構要求下載最新證書冊銷列表。

步驟 2：

憑證機構(CA)傳送最新證書冊銷列表(Certificate Revocation List)資料至授權伺服器。

步驟 3：

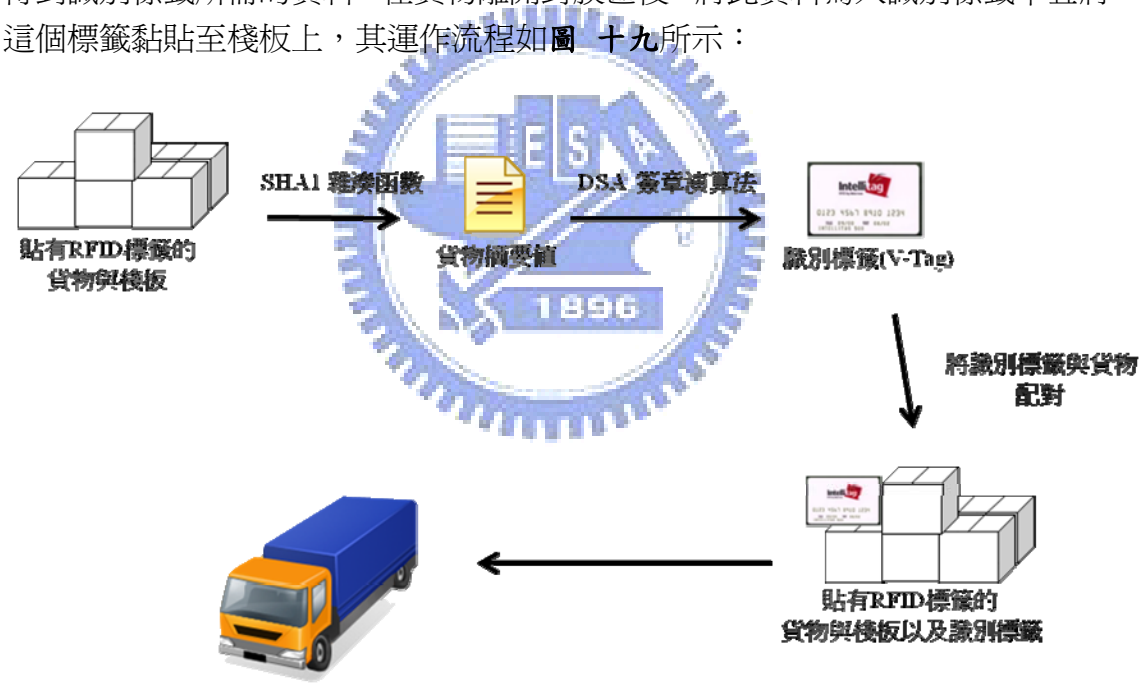
授權伺服器將所收到的證書冊銷列表資料與內部資料庫所記錄的合法憑證做比對，更新資料庫憑證資訊。

4.3 供應商貨物簽章階段

在此小節首先說明供應商使用安全物流系統所設計的產品出貨情境，接著描述出貨協定的運作流程圖，在流程圖中會詳細的解釋如何達成將每一個運送的產品製作出唯一且可提供接收方識別的協定技術，最後講解出貨協定最核心的技術識別標籤設計。

供應商出貨包裝情境：

本論文是以半導體產業的出貨情境爲基礎，在此利基下建構安全物流運輸系統，當半導體製作且裝箱完成後，會將這些紙箱依每次規定的數量放至規定的棧板之上，隨後將此棧板推往封膜區，在此區域封膜的同時 RFID 讀取器會讀取出所有紙箱上的 RFID 標籤資料，在收集到的資料執行雜湊演算法以及簽章演算法得到識別標籤所需的資料，在貨物離開封膜區後，將此資料寫入識別標籤中且將這個標籤黏貼至棧板上，其運作流程如**圖 十九**所示：



V-Tag：識別標籤

圖 十九：供應商出貨情境

一開始將 N 個此次所定義的棧板上所運送紙箱的 RFID 標籤資料，使用 SHA1 Hash Function 得到其 RFID 標籤資料摘要值(digital value)，將此摘要值使用 DSA 簽章演算法搭配本此所選用的公開金鑰對中所含私密金鑰，運算得出此筆貨物的供應商簽章資料，且將所得簽章資料寫入識別標籤(V-Tag)中，最後將此識別標籤與棧板結合便完成此棧板上貨物的出貨所需流程，便可將此棧板運往外銷的鐵櫃中存放以完成此棧板貨物的整個出貨流程。

識別標籤(V-Tag)：

識別標籤採用 EPC Class1 Gen2 規格且記憶體爲 512 bits 的 RFID 標籤，EPC 所定義的 RFID 標籤內含四個區(bank)，識別標籤使用其 EPC Bank 以及 User Bank 來實作

EPC Bank：

使用其 header、company code 以及 serial number 三個欄位，其中 header 是用來與貨物標籤及棧板標籤做區分用，company code 以及 serial number 結合讓接收方用來篩選本次貨物驗證所需憑證資料。

User Bank：

記錄兩個資料以供接收放驗證貨物時使用，其一爲貨物 RFID 標籤簽章資料，另一個爲該棧板所擺放的貨物紙箱數量，當接收方驗證貨物時可利用此資料判定棧板上數量是否讀取完畢，以及驗證棧板上所有紙箱的正確性。

EPC Bank 記憶體容量爲 96 bits 而 User Bank 記憶體容量則有 512 bits，識別標籤所使用的 EPC Bank 以及 User Bank 的記憶體容量如**圖 二十**所示：

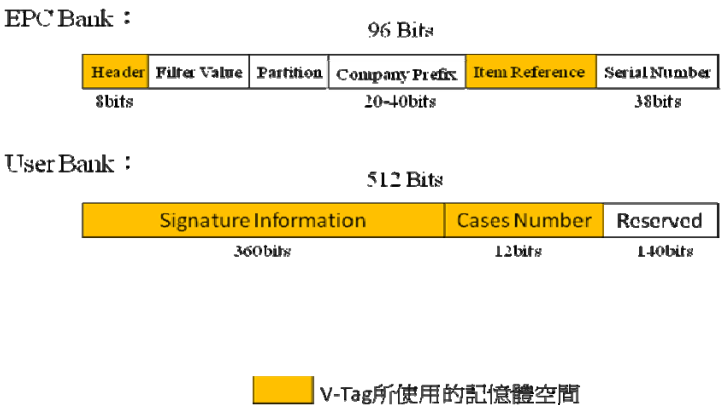


圖 二十：識別標籤記憶體容量配置

圖中橘色的欄位爲識別標籤所使用，且在欄位的下方標示出該欄位儲存資料所佔的空間大小，其中 Company Prefix 爲一個記憶體可變的欄位，其變動的範圍在 20-40bits 之間，白色部分欄位爲閒置的記憶體空間。

供應商簽章演算法：

在了解出貨情境以及識別標籤的設計後，接下來將說明供應商產品出貨協定執行的流程，一開始需定義每個環節所需的系統參數，緊接著當貨物抵達時開始讀取貨物 RFID 標籤資料以及記錄目前所讀取到的箱子個數，當箱子個數與所定義的參數相同時，則將所讀到的 RFID 標籤資料進行排序(由小到大)的動作，排序完成後，系統將此資料輸入雜湊函數裡進行運算以得出該資料的摘要值，此值在經 DSA 簽章演算法處理後可得具有公信力的使用者簽名，最後將此簽名與該棧板所含箱子個數寫入識別標籤中的特定欄位，即完成該筆貨物的出貨流程，其詳細的流程如**圖 二十一**所示：

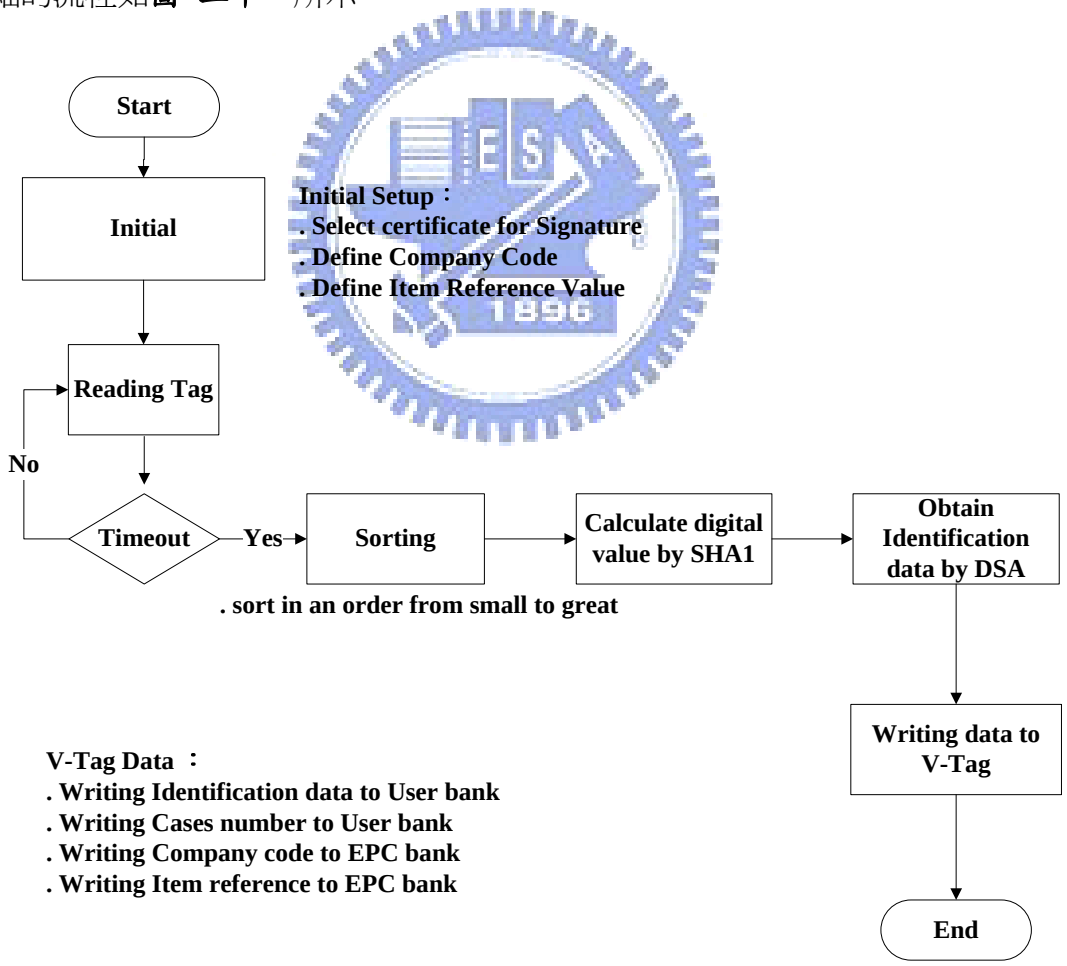


圖 二十一：快速驗證平台供應商出貨協定流程

Initial：

出貨協定參數設定包含，選擇本次出貨所需的憑證資料、棧板標籤標頭值、紙箱標籤標頭值、供應商所屬公司碼以及所使用的憑證編號。

Reading data in cases：

當貨物抵達封膜區時，開始讀取棧板上所有紙箱的 RFID 標籤資料，且滿足停止讀取紙箱標籤的條件時則開始執行計算的動作。

Timeout：

當貨物在封膜區的時間已超過系統所限制時，且 RFID 讀寫器尚未讀取完棧板上所有紙箱的標籤時，則會發生 Timeout 的中斷命令，強制 Reading data in cases 動作停止，且繼續往下執行。

Sorting materials received：

由於經 RFID 讀寫器所取得的紙箱標籤資料，幾乎每次的順序皆會有所不同，因此本系統將資料由小至大排序以便後續的步驟。

Obtain digital value by SHA1 Hash Function：

將排序過後的 RFID 標籤資料，利用 SHA1 Hash Function 來取得 RFID 標籤資料的摘要值。

Obtain signature data by DSA algorithm：

以 RFID 標籤資料摘要值以及供應商本身的私密金鑰當作參數，利用 DSA 簽章演算法得到具公信力的簽章資料。

Writing identification data to V-Tag：

將具有公信力的標籤資料以及系統所定義的棧板所含紙箱數量，寫入識別標籤的特定欄位，以供貨物驗證時使用。

4.4 貨物集散中心驗證階段

在此小節將說明接收方驗收貨物的機制，因此一開始先提出本系統的驗貨情境，說明在執行時是如何判定貨物的合法性，然後以驗貨機制的設計流程圖來解釋如何做到驗證貨物的目的。

接收方驗證貨物情境：

當運送貨物的貨櫃抵達目的地後，首先從貨櫃中以棧板爲單位運往驗證的平台，抵達驗證平台時，RFID 讀寫器便開始讀取棧板上的所有標籤資料(棧板標籤、紙箱標籤、識別標籤)，獲得識別標籤後取出對應的供應商憑證來驗證該識別標籤所存資料是否合法，若合法則將所取得紙箱標籤取其摘要值與識別標籤內所含的摘要值做比對，若兩者內容相等則表示該棧板上的紙箱皆是由合法廠商所製且運送途中也沒有遺失的情形發生，其驗證情境詳細步驟如**圖 二十二**所示：

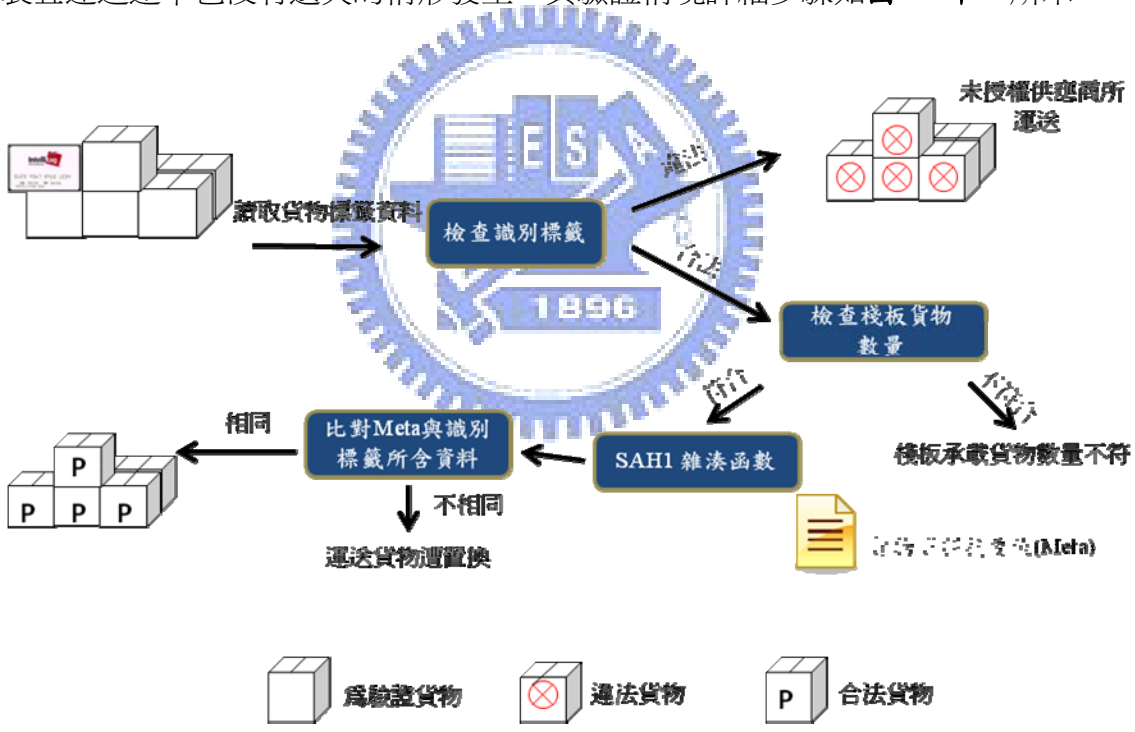


圖 二十二：貨物集散中心驗證情境

當讀取到合法性質不明的棧板時，首先將此棧板上所有的 RFID 標籤資料皆讀取出來，然後比對識別標籤內所儲存經 DSA 簽章所得值與驗證平台裡所挑選出的憑證資料是否可以驗證，若可以則繼續往下執行，否則表示該棧板非系統所核定的合法供應商所送，當 DSA 簽章爲合法時，將所讀取到的紙箱標籤資料利用 SAH1 計算其摘要值，且將此摘要值與識別標籤(V-Tag)內所含的摘要值做比對，若相等則表示該棧板上所有紙箱皆是合法，否則將此棧板所承載的貨物在運

送的途中已遭人置換。

驗證協定流程：

在了解貨物驗證的情境後，緊接著說明如何實作出貨物驗證的協定如**圖 二十三**所示，當貨物抵達後 RFID 讀寫器開始讀取所有的 RFID 標籤資料，在標籤讀取完時開始將所讀資料依棧板、紙箱以及識別標籤來做分類，隨後將識別標籤 EPC Bank 內所儲存的供應商公司碼以及憑證序列號取出，且裡用這兩個欄位資料篩選出系統內所存合法標籤，若存在且可驗證成功則表示該運送貨物爲系統所核定的合法供應商所送，然後將所讀取到的紙箱標籤利用 SAH1 雜湊函數運算得其摘要值，將此摘要值與識別標籤內所含的雜湊值做比對，若符合則表示該棧板上所有的紙箱皆是合法供應商所送且在運送途中並無遭人竄改。

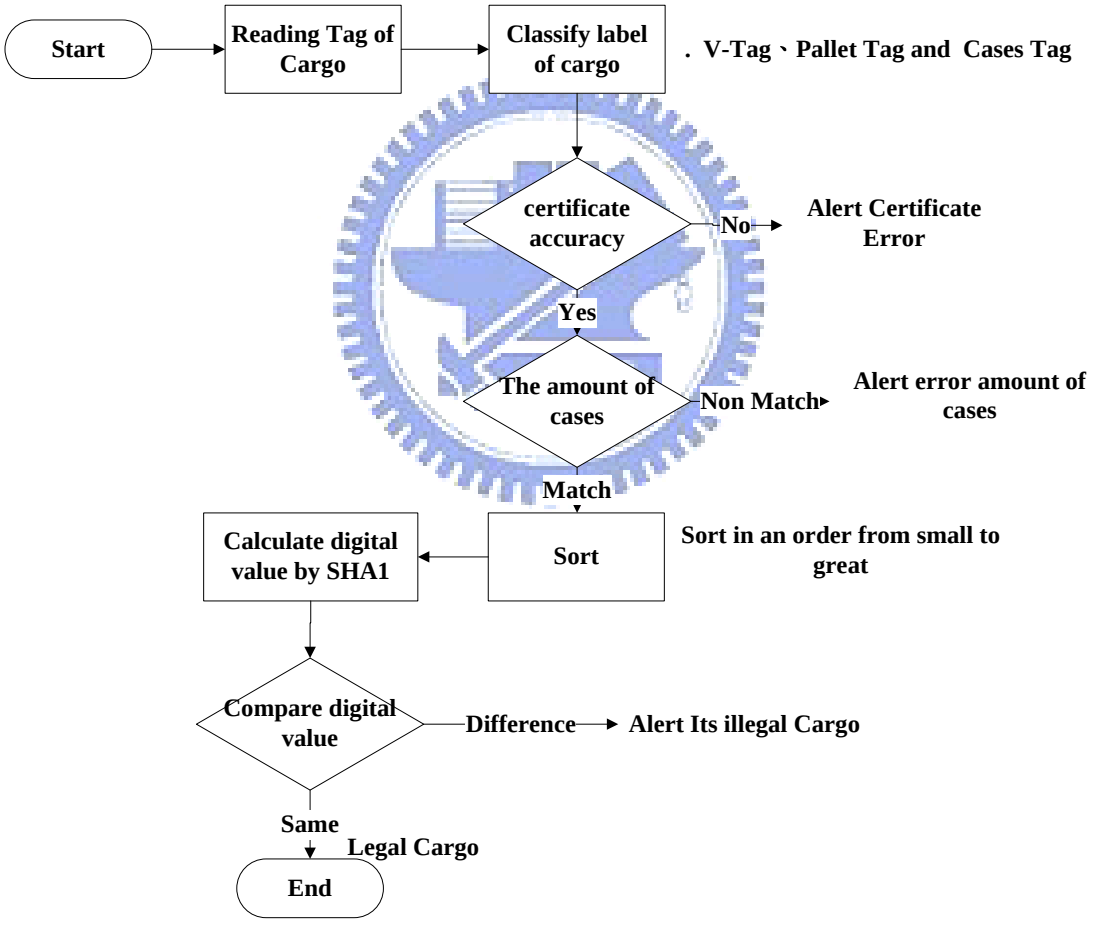


圖 二十三：快速驗證平台貨物驗證流程

Reading data from coming cargo：

當棧板從貨櫃運送至驗證平台時，開始讀取棧板上所有 RFID 標籤資料，所讀取的標籤資料也包含棧板本身。

Classify label of cargo：

將所讀取到的 RFID 標籤資料，依其標頭檔欄位所存的資料分成棧板標籤、紙箱標籤以及識別標籤三類。

Checking certificate accuracy：

取出識別標籤內 EPC Bank 所存的公司碼以及憑證序列號，結合這兩個欄位的資料且在系統所存合法憑證內搜尋相對應的資料，若有這利用此憑證來驗證該識別標籤所存簽章資料是否正確。

Sorting data of label in cargo：

由於經 RFID 讀寫器所取得的紙箱標籤資料，幾乎每次的順序皆會有所不同，因此本系統將資料由小至大排序以便後續的步驟。

Obtain digital value by SHA1 Hash function：

將排序過後的 RFID 標籤資料，利用 SHA1 Hash Function 來取得 RFID 標籤資料的摘要值。

Compare digital value：

將從所讀取到的紙箱標籤所運算出的摘要值，以及識別標籤 User Bank 內所存的摘要值做比對，若相等則表示該棧板上所有的紙箱皆為合法供應商所送且在運送途中並沒有被有心人士竄改。

五、系統測試

此章節首先介紹快速離線驗證平台的實作環境，緊接著利用五個貨物在運輸時所會發生的狀況，分別爲正常情況、部分貨物遺失、貨物數量過多、未授權貨物供應商以及貨物遭置換等，來驗證本論文所提出的驗證平台其可行性以及所保證的安全性。

5.1 實作環境

在此小節首先提出本論文所設計的驗證平台實作環境設置，包含系統運行的作業環境、RFID 標籤以及 RFID 讀寫器……等，接下來介紹驗證平台的使用者介面，其介面分別爲供應方所使用的 Pallet Wrapping Monitoring 以及貨物集散中心所用的 Fast Offline Validation Platform。

環境設置：

作業系統	Windows XP
CPU	Intel Core2 Duo T7300 2.00GHz
Memory	2GB
RFID 中介軟體	Rifartek ServRobot
	Rifartek CliRobot
Develop language	Java、JSP
Trusty Third Party	OpenCA
Internet Server	Apache Tomcat5.5
Database	MySQL
RFID Tags	Cases Label(96 bits SGTIN)
	Pallet Label(96 bits SGTIN)
	Identification Label(512bits)
RFID Reader	MTI RU-820(Pallet wrapping)
	OmronV750(Pallet Validation)

表 十四：快速離線驗證平台環境設置

表 十四 RFID Tags 爲本論文中所使用來，代表運送的貨物標籤(Cases Label, 96 bits SGTIN)、裝載貨物的棧板(貨物驗證的單位)標籤(Pallet Label, 96 bits SGTIN)以及儲存驗證資訊的識別標籤(Identification Label, 512bits)。

RFID Reader 分別爲，貨物供應商所使用的 MTI RU-820 (Pallet wrapping)其功用爲運算貨物驗證資訊且將資料寫入識別標籤中以及集散中心所使用的 OmronV750(Pallet Validation)負責驗證抵達貨物正確性。

Pallet Wrapping Monitoring Platform：

在貨物供應商所使用的系統平台，當使用者向授權伺服器註冊成爲合法使用者後，即可將出口的貨物附上驗證標籤介面如**圖 二十四**所示：

圖 二十四：Pallet Wrapping Monitoring Platform 使用者介面

FOLV Platform State：

說明貨物Pallet Wrapping區域目前的狀態爲何共可分成五個狀態，Idle、Pallet Coming、Count Case、Write V-Tag 以及 Pallet Leaving：

Idle：

貨物尚未抵達 Wrapping 區域。

Pallet Coming：

裝載貨物的棧板即將抵達 Wrapping 區域

Count Case：

貨物到達 Wrapping 區域且開始計算貨物個數以及產生貨物識別資料。

Write V-Tag：

將貨物驗證資料以及簽章所使用的憑證對應資料寫入識別標籤(V-Tag)中。

Pallet Leaving：

將識別標籤(V-Tag)放置於棧板以完成貨物識別流程。

Checking Pallet Information：

當 Pallet Wrapping 進入 Count Case 的狀態時，Checking Pallet Information 所包含的 Pallet 欄位顯示目前正在產生識別資料的棧板 EPC Code、Cases 欄位顯示該棧板上所乘載的紙箱 EPC Code 以及 Cases Num 顯示目前 RFID 讀寫器所讀取到的紙箱個數。

Platform Security Information：

在系統執行的一開始使用者按下”Config”按鈕，選擇本次產生貨物身分驗證資料所需的憑證後，Certificate Information 欄位會顯示所選擇憑證的內容，且當系統開始執行時若有事件發生時 Pallet Wrapping Event 欄位會將所發生的事件標示出來。

Fast Offline Validation Platform：

貨物集散中心使用來快速驗證抵達貨物的正確性，其系統的平台介面**圖 二十五**所示

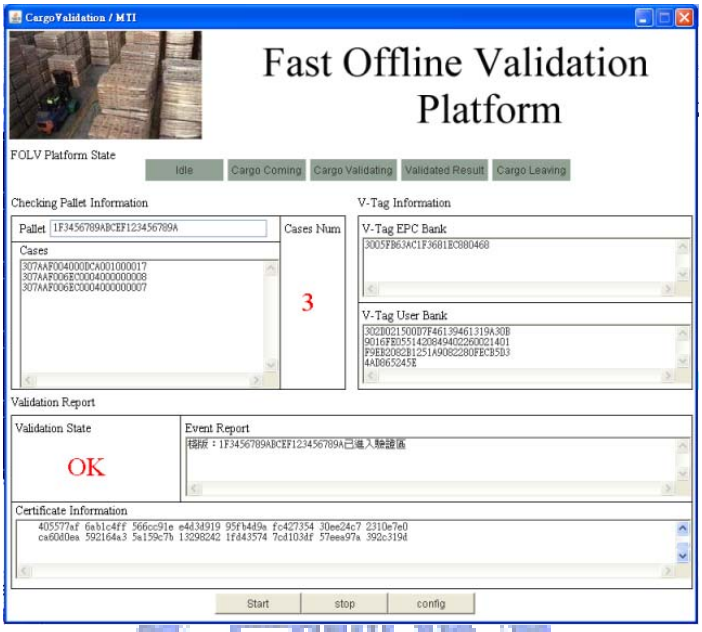


圖 二十五：Fast Offline Validation Platform 使用者介面

FOLV Platform State：

說明貨物在抵達驗證區域時即時的狀態爲何共可分成五個狀態，Idle、Cargo Coming、Cargo Validating、Validated Result 以及 Cargo Leaving：

Idle：

貨物尚未抵達 Fast Offline Validation Platform。

Cargo Coming：

貨物抵達 Fast Offline Validation Platform。

Cargo Validating：

讀取棧板上貨物 RFID 標籤資料、棧板標籤資料以及驗證標籤資料，且當標籤資料讀取完畢後開始驗證資料正確性。

Validated Result：

顯示棧板貨物驗證結果，若驗證出貨物有問題時則會在 Event Report 欄位標明，該批貨物不符合哪項標準。

Cargo Leaving：

合法貨物離開 Fast Offline Validation Platform，或者是不合法的貨物運送至 ASN 比對平台。

Checking Pallet Information：

當 Fast Offline Validation 進入 Cargo Validation 的狀態時，Checking Pallet Information 所包含的 Pallet 欄位顯示目前正在產生識別資料的棧板 EPC Code、Cases 欄位顯示該棧板上所乘載的紙箱 EPC Code 以及 Cases Num 顯示目前 RFID 讀寫器所讀取到的紙箱個數。

V-Tag Information：

當 Fast Offline Validation 進入 Cargo Validation 的狀態時，將所讀取到的識別標籤內容依其 Bank 顯示至對應欄位，EPC Bank 所顯示的資料爲貨物製造商的公司碼以及所使用的憑證編號資料而 User Bank 則顯示此批貨物的簽章資料。

Validation Report：

當 Fast Offline Validation 進入 Validated Result 的狀態時，Validation State 欄位顯示此棧板的驗證結果(OK/Error)、Event Report 欄位則顯示貨物在驗證時所觸法的事件紀錄以及 Certificate Information 欄位顯示本次驗證時集散中心所採用的憑證資料。

5.2 實驗與測試結果

此小節利用五個貨物在運輸時所會發生的狀況，分別爲正常情況、部分貨物遺失、貨物數量過多、未授權貨物供應商以及貨物遭置換等，來驗證本論文所提出的驗證平台其可行性以及所保證的安全性。

5.2.1 實驗 1：正常狀況

（棧板數量：1、貨物數量：5）

貨物由合法的供應商經雜湊函數以及簽章演算法運算後，將所獲得的識別資料寫入辨識標籤中且將此標籤以及貨物合併後運送至集散中心，運作流程如**圖二十六**所示：

圖 二十六：正常情況運作流程

快速離驗證平台辨識結果：

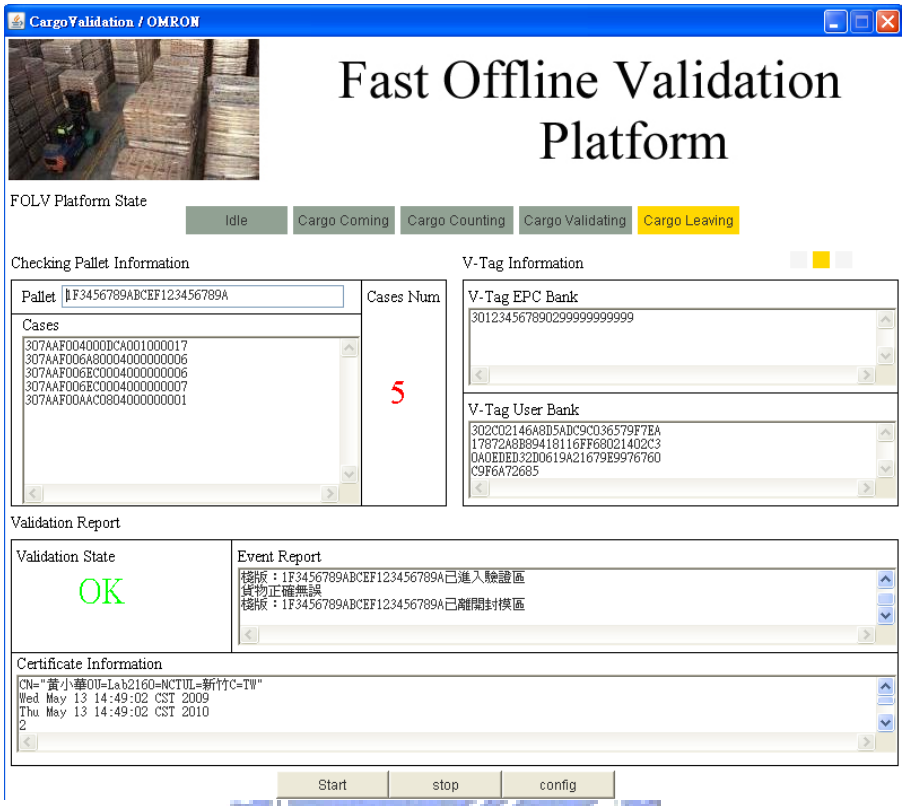


圖 二十七：快速離線驗證平台辨識結果-正常情況

從上圖中 Checking Pallet Information 可看出所驗證的棧板條碼、貨物條碼以及貨物數量，且在 V-Tag User Bank 欄位顯示貨物的識別資料，離線快速驗證模組利用所讀取到的貨物資料與辨識資料比對且將結果顯示在 Validation State。

5.2.2 實驗 2：部分貨物遺失

(棧板數量：1、貨物數量：5)

此情境所要描述的情況爲，當貨物抵達集散中心經過驗證後發現貨物的數量與在生產地時所寫入識別標籤的數量來得少，表示貨物在運送的途中有部份的物品遺失詳細的流程如**圖 二十八**所示：

圖 二十八：部分貨物遺失情境

快速離驗證平台辨識結果：

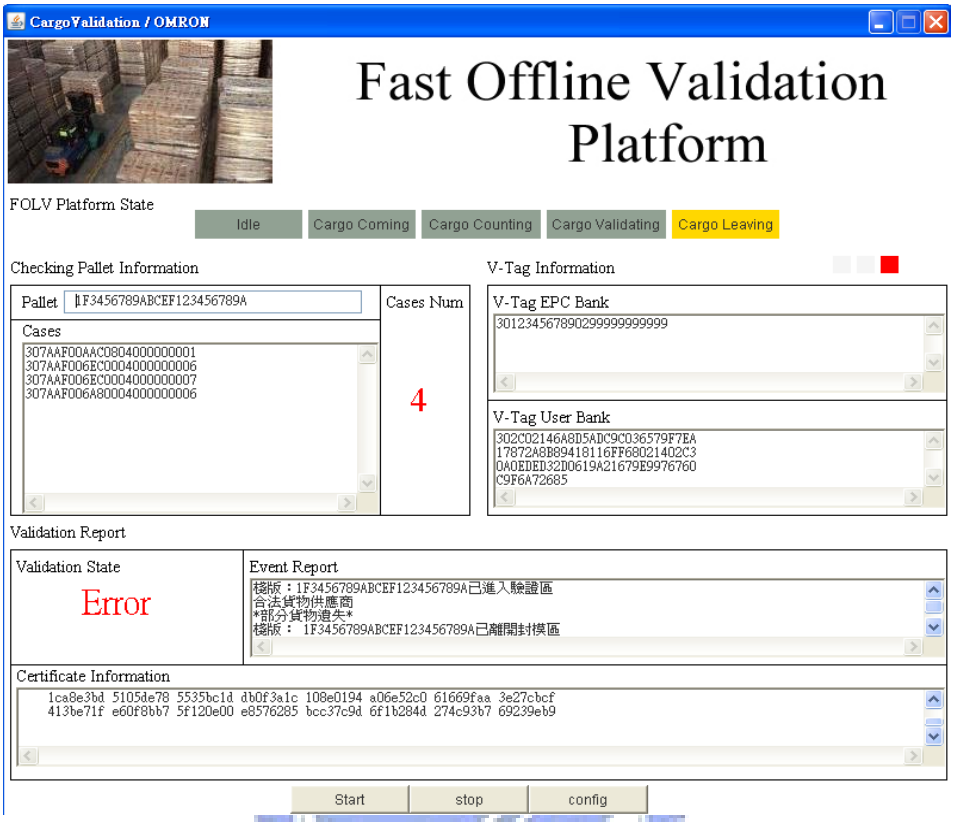


圖 二十九：快速離線驗證平台辨識結果–部分貨物遺失

上圖快速離線驗證系統成功的判別出貨物數量缺少的情形，能夠辨識出此情境是利用產品供應商將出貨的數量寫在識別標籤的 User Bank 中，因此驗證平台可以在不須透過複雜的運算即可成功的判別貨物遺失的狀況。

5.2.3 實驗 3：貨物數量過多

(棧板數量：1、貨物數量：5)

在此情境所要描述的狀況爲，當貨物抵達集散中心驗證後，發現此批貨物數量竟然比當初貨物供應商寫入識別標籤的數量還要多，其貨物運輸的情境如**圖三十**所示：

圖 三十：貨物數量過多情境

快速離驗證平台辨識結果：

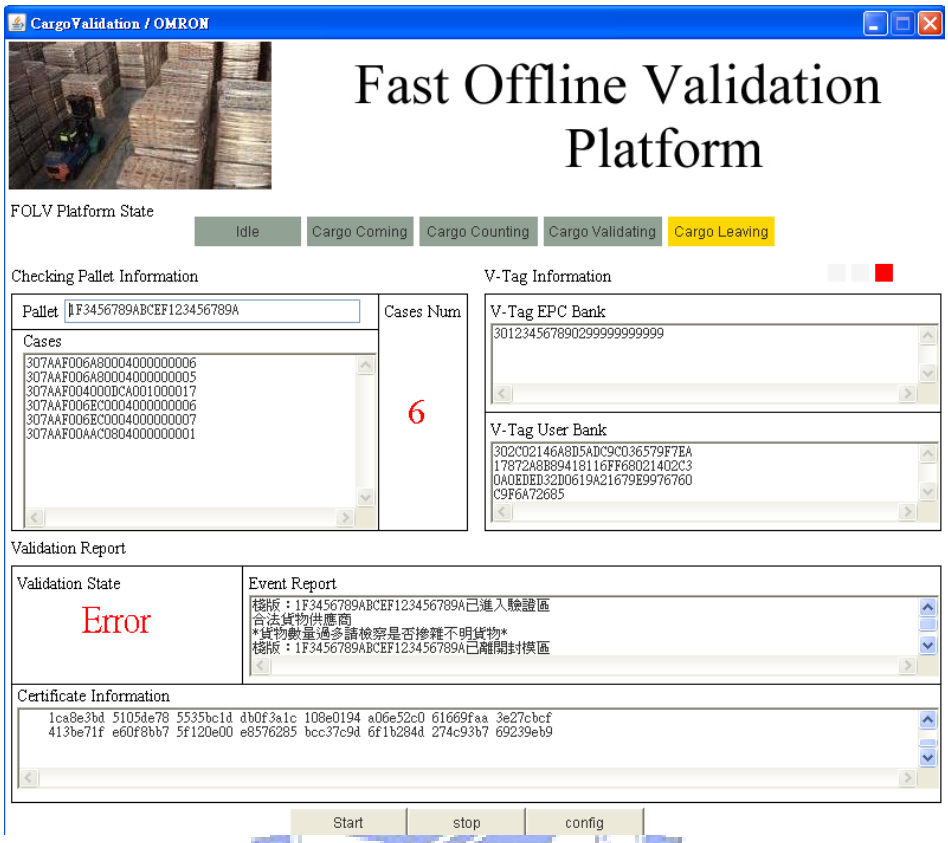


圖 三十一：快速離線驗證平台辨識結果–貨物數量過多

上圖快速離線驗證平台利用貨物供應商所附在棧板上的識別標籤內 User Bank 中所記錄的出場貨物數量以及貨物在驗證閘門時由 RFID 讀寫器所收集到的貨物數量，進行比對發現 RFID 讀寫器所收集的貨物數量竟大於識別標籤內所記錄的資料，因此成功的偵測出此異常狀況。

5.2.4 實驗 4：未授權貨物供應商

(棧板數量：1、貨物數量：5)

在此情境下所描述的狀況爲，貨物供應商沒有到驗證伺服器註冊已取得合法的使用身分，因此該供應商將所要出口的貨物摘要值進行簽章演算法時所使用的私密金鑰是不合法的，所以當貨物抵達集散中心時驗證平台將會偵測出該批貨物所附的驗證標籤是不合法的也就是貨物的供應商其身分並沒有經驗正伺服器所授權其執行流程如**圖 三十二**

圖 三十二：未授權供應商情境

快速離驗證平台辨識結果：

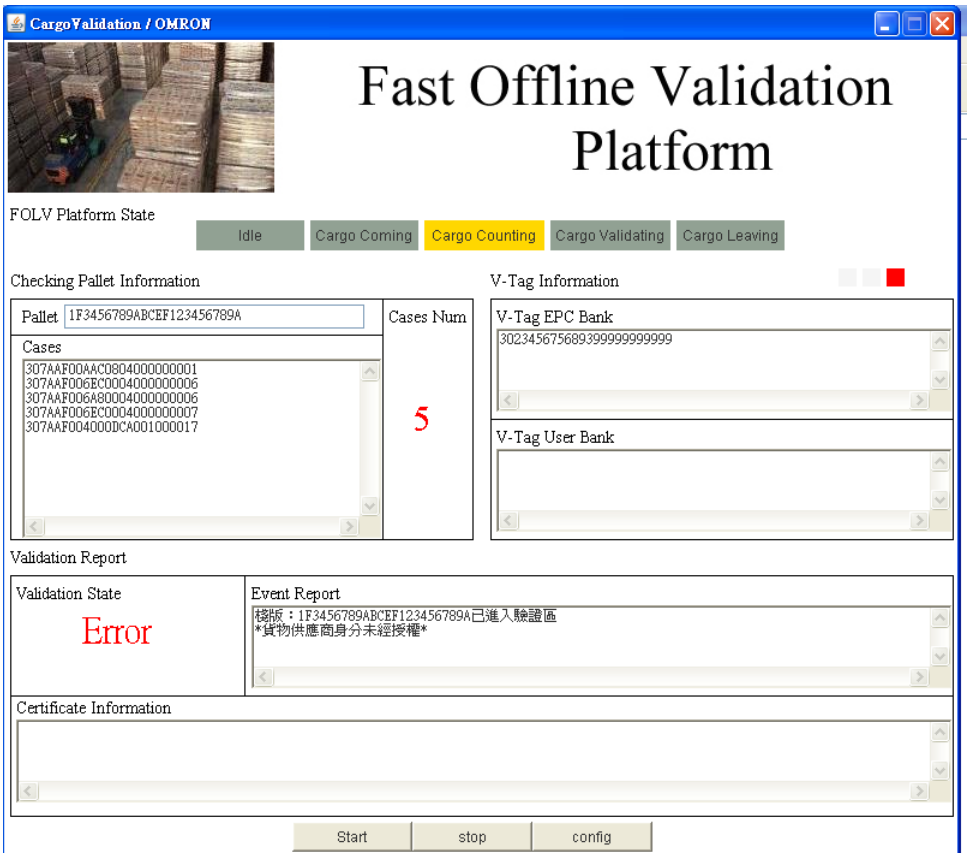


圖 三十三：快速離線驗證平台辨識結果-未授權貨物供應商

上圖快速離線驗證平台在 Cargo Counting 的狀態時，會將所讀取到的識別標籤 EPC Bank 內所記錄的貨物簽章憑證資訊與平台內所儲存的合法授權供應商資料進行比對，判斷該憑證資訊是否爲系統所授權的供應商所擁有，因此此違法的識別標籤在比對授權供應商資料時即可被偵測出來。

5.2.5 實驗 5：貨物遭置換

(棧板數量：1、貨物數量：5)

此情境所要描述的情況爲，貨物是由合法的授權供應商所送出，但在運送途中遭置換，當此批不合法的貨物抵達集散中心時，驗證平台可由識別標籤內 User Bank 所記錄的識別資料判別貨物的正確性，其運作流程如**圖 三十四**所示：

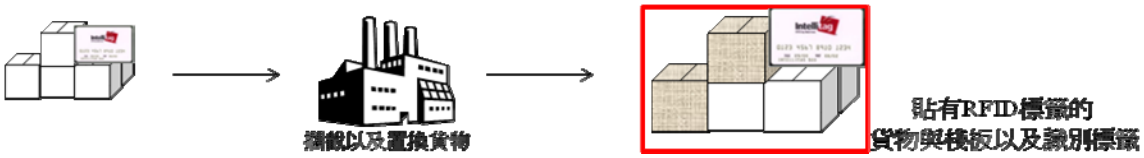


圖 三十四：運送貨物遭置換情境

快速離驗證平台辨識結果：

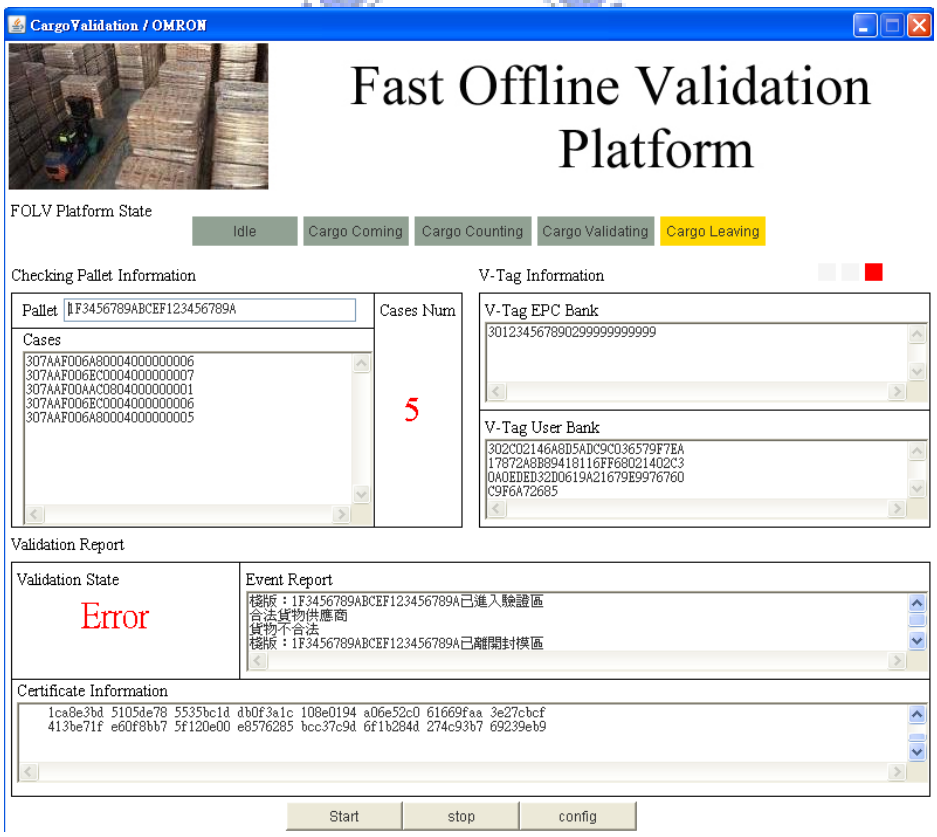


圖 三十五：快速離線驗證平台辨識結果-運送貨物遭置換

上圖快速離線驗證平台利用識別標籤內 User Bank 所儲存的貨物識別資料，以及經由集散中心閘門RFID 讀寫器所取得的貨物資料經雜湊函數運算得出摘要值後進行比對即可發現由閘門所讀取的貨物資料其摘要值與識別標籤內所記錄的不同，而偵測出此批貨物在運送途中遭人置換的狀況。

與傳統安全物流系統比較：

	快速離線驗證平台	傳統安全物流系統
網路輔助	不需要	需要
驗證大量貨物效率	高	低
資料竊取保護	有	無
伺服器輔助	公正第三方(憑證中心)	驗證伺服器
需額外標籤	識別標籤(V-Tag)	不需要
ASN 文件	不需要	需要
建置成本	低	高

表 十五：快速離線驗證平台與傳統安全物流系統比較

表 十五將本論文所提出的快速離線驗證系統與目前已存建立在無線射頻辨識的基礎上的安全物流系統針對七個項目網路輔助、驗證大量貨物效率、資料竊取保護、伺服器輔助、需額外標籤、ASN 文件以及建置成本來進行比較：

網路輔助：

傳統安全物流系統在進行貨物驗證的判斷時，需要將所讀取到的貨物標籤資料經由網路傳送至後台伺服器進行比對，而本論文所提出的驗證平台則式導入密碼學的觀念，將所讀取到的標籤資料經由 RFID 讀寫器的中介軟體進行運算即可判別貨物的合法性。

驗證大量貨物效率：

傳統安全物流系統驗證貨物時，需要網路來進行資料的傳遞，因此當資料量大時，從 RFID 讀寫器傳送資料至後台伺服器所需的時間變長且由於傳統的伺服器驗證是將資料一筆一筆的與資料庫內所存的清單作比對，所以驗證的整體效率會下降許多，而本論文提出的驗證機制則是將標籤資料取其雜湊值，再將此雜湊值經簽章演算法得出驗證資料，因此雖貨物量變大但並不影響整體的驗證效能。

資料竊取保護：

傳統安全物流系統的貨物驗證資料皆儲存在後台的伺服器中，若後台伺服器遭到攻擊時則驗證資料的可信度會立即下降，但快速離線驗證平台的驗證資料皆是從運送的貨物標籤中取出經雜湊以及簽章演算法運算所得出，因此即使驗證平台遭駭客入侵對其貨物的驗證安全性是不會造成任何的影響。

伺服器輔助：

傳統安全物流系統需要後台伺服器輔助來達到驗證貨物正確性的服務，而快速離線驗證系統在使用前，貨物供應商須至公正第三方(憑證中心)申請合法憑證後才可使用快速離線驗證平台。

需額外標籤：

傳統安全物流系統在驗證貨物正確性時不需要任何額外的標籤輔助即可完成，而本論文所提出的快速離線驗證平台，則需要一張額外的驗證標籤來儲存供應商所提供的貨物驗證資料，來完成貨物驗證的目的。

ASN 文件：

傳統安全物流系統需要 ASN(Advanced Shipment Notice)文件的輔助來進行貨物的正確性驗證，本論文所提出的驗證平台則不需 ASN 來進行貨物資料的比對即可完成貨物合法性的判斷。

建置成本：

傳統安全物流系統當貨物包裝完成後，必須要依靠人工的方式將棧版上的貨物資料編寫成文件(ASN 文件)，且將此文件上傳至資料庫中以提供貨物驗證時比對資料用，而本論文所提出的驗證平台檢驗貨物時所需要的辨識資料，只需從本地端驗證區的貨物標籤以及識別標籤資料即可判別貨物的合法性，因此相對於傳統的驗證平台減少資料庫的硬體設備以及編寫文件的人力損耗，且若儲存 ASN 文件的資料庫若損壞時則所有的貨物驗證資料皆毀於一旦反觀快速驗證平台若該棧板的識別標籤損壞時只有該棧板的貨物無法進行驗證，所造成的損失並不大。

六、結論

在本論文中提出使用公開金鑰基礎建設以及 EPC global Class1 Gen2 的技術，建立貨物離線驗證的平台，且此驗證平台相較於傳統的安全物流系統貨物驗證平台，具有更高的效率，且能有效的達到貨物保護的目的，以及無線射頻辨識技術的自動化等特性。

高效率：

快速離線驗證系統在辨識貨物的合法性時，只需要此批驗證貨物上的標籤資料(貨物資料、棧板資料以及識別標籤資料)，即可判斷出貨物的正確與否，完全不需要在經由網路傳遞任何而外的資訊。

有效性：

快速離線驗證平台使用應用密碼學所提出的 DSA 數位簽章演算法以及 SHA1 雜湊函數這兩項技術，有效的達成產品供應商身分的追蹤以及貨物合法性的識別加強貨物安全的防護。

自動化：

快速離線驗證平台利用無線射頻辨識技術所擁有的非接觸式以及物品皆有獨一無二的辨識 ID 特性，達到驗證流程自動化的成果。

本論文利用 EPC global Class1 Gen2 的標籤內部所含的 EPC Bank 以及 User Bank 來達成快速離線驗證平台所需的相關安全機制，此項設計在傳統的無線射頻識別應用是相當罕見的。

6.1 論文貢獻

本論文所提出的快速離線驗證平台，所設計的貨物驗證協定可降低貨物在抵達集散中心時進行驗證所需的時間。當貨物集散中心識別貨物的正確性時只需要使用快速離線驗證平台所提供的 “Validation Module” 即可達成，完全不需任何額外的資源輔助，因此該驗證平台所擁有相當高的可攜性。

快速離線驗證平台利用公開金鑰基礎建設(Public Key Infrastructure)、SHA1 Hash Function 以及 DSA Signature Algorithm，來取代傳動的貨物驗證機制。在此平台上只需要本的端的貨物標籤資訊(貨物資料、棧板資料以及識別標籤資料)即可辨識出該貨物的合法性，完全解決傳統貨物驗證機制需網路傳遞資料以及產品供應商需提供 ASN 文件的需求。

本論文使用標準的 EPC global Class 1 Gen2 的 RFID 標籤內的 EPC Bank 以及 User Bank 等記憶體欄位，成功的防護 Clone attack.

6.2 未來方向

本論文所設計的快速驗證平台所強調的重點爲在離線的狀態下快速的驗證抵達貨物的合法性，因此當貨物發生異常的情況如部分貨物遺失以及貨物數量過多.....等情形只可識別貨物發生異常。

在未來希望能夠加強貨物驗證的演算法，當發生如部分貨物遺失的情形時可以判別出遺失的貨物爲何，亦或是部分貨物遭置換的情況時可以判斷出是哪幾箱貨物遭人置換。

七、參考文獻

[1] Weis, S., Sarma, S., Rivest, R., and Engels, D., "Security and Privacy Aspects of Low-Cost RFIDs," Security in Pervasive Computing, Lecture Notes in Computer Science，Vol. 2802, 2003, pp. 201－212.

[2] Stephen A. Weis, Sanjay E.Sarma, Ronald L. Rivest and Daiel W. Engels, "Security and Privacy Aspectsof Low-Cost Radio Frequency Identification Systems", First International Conference on Security in Pervasive Computing, 2003, http://theory.lcs.mit.edu/ sweis/spc-rfid.pdf.

[3] Jin-Oh Jeon, Su-Bong Ryu, Tae-Min Chang, Ho-Yong Choi, Min-Sup Kang," Digital Codec Design for RFID Tag Based on Cryptographic Authentication Protocol", IEEE Conference Proceeding Future generation communication and networking, Volume 2,pp 119 – 124,2007

[4] International Organization for Standardization, " ISO/IEC 18000-3, Information Technology AIDC Techniques – RFID for Item Management," March 2003.

[5] J. Yang, K. Ren, and K. Kim, "Security and Privacy on Authentication Protocol for Low-cost RFID," Proceedings of SCIS2005, Jan., pp. 25－28.

[6] S. B. Ryu, J. O. Jeon, and M. S. Kang, "FPGA Design of Digital Codec for Passive RFID Tag," IEEE ALPIT 2007, Vol. 6, 2007, pp. 343 － 346.

[7] Zhao Shijun, "Application of RFID Technology in Supply Chain", Journal of Chongqing Jiaotong University, pp.147-150, Feb 2007

[8] Markus Jakobsson and David Pointcheval, " Mutual Authentication for Low-power Mobile Devices," Lecture Notes in Computer Science, 2002, Vol. 178－195.

[9] Martin Feldhofer, "A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags," IEEE Proceedings of MELECON 2004, Vol. 2, pp. 759－762.

[10] D. Eastlake and P. Jones, "US Secure Hash Algorithm 1 (SHA-1)," Internet RFC 3174, September 2001.

[11] Han, S., Potdar, V., Chang, E.: "Mutual authentication protocol for RFID tags based on synchronized secret information with monitor". In: Gervasi, O., Gavrilova, M.L. (eds.) ICCSA 2007. LNCS, vol. 4707, pp. 227–238. Springer, Heidelberg (2007)

[12] Dimitriou, T.: "A Lightweight RFID Protocol to Protect against Traceability and Cloning Attacks". International Conference on Security and Privacy for

Emerging Areas in Communication Networks- SecComm (September 2005)

[13] Peris-Lopez, P., Castro, J.C.H., Estevez-Tapiador, J.M., Ribagorda, "A.: EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags". In: OTM Workshops (1), pp. 352–361 (2006)

[14] C. Chatmon, T. van Le, and M. Burmester. "Secure anonymous RFID authentication protocols". Technical Report TR 060112, Florida State University, Department of Computer Science, Tallahassee, Florida, USA, 2006

[15] T. Dimitriou. "A lightweight RFID protocol to protect against traceability and cloning attacks". In Conference on Security and Privacy for Emerging Areas in Communication Network SecureComm, Athens, Greece, September 2005,IEEE

[16] M. H. Y.C. Chen, W.L. Wang. "Rfid Authentication Protocol for Anti-Counterfeiting and Privacy Protection". Advanced Communication Technology, The 9th International Conference on, pages 255–259, 2007.

[17] C. C.Tan, B. Sheng, and Q. Li, "Severless Search and Authentication Protocols for RFID", In Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07), New York, USA, March 2007.

[18] 余顯強，無線射頻識別技術之應用與效益，中華民國圖書館學會會報，第75期，頁27-36，2005

[19] 朱耀明，林財世，淺談RFID 無線射頻辨識系統技術，生活科技教育月刊，38卷 第2期，2005

[20] EPCglobal Tag Data Standards Version 1.4 June 11, 2008

[21] 蔡文能，網路安全精要(William Stallings 原著中譯本)，培生出版公司，2002

[22] 鍾慶豐，近代密碼學及其應用，儒林圖書有限公司，6月，2005