

100-106-4253
MOTC-IOT-99-MDB005

交通電子票證系統共通技術規範研究 與票證一卡通推動計畫(4/4)



交通部運輸研究所

中華民國 100 年 8 月

ISBN 978-986-02-8807-0

GPN : 1010002648

定價 200 元

100-106-4253
MOTC-IOT-99-MDB005

交通電子票證系統共通技術規範研究 與票證一卡通推動計畫(4/4)

著者：黃文鑑、許安慶、劉明杰、汪經堯、王穆衡、黃立欽

交通部運輸研究所

中華民國 100 年 8 月

國家圖書館出版品預行編目資料

交通電子票證系統共通技術規範研究與票證一卡通
推動計畫. (4/4) / 黃文鑑等著. -- 初版. --
臺北市：交通部運研所，民100.08
面；公分

ISBN 978-986-02-8807-0(平裝)

1. 交通管理 2. IC卡 3. 管理資訊系統

557.15029

100015865

交通電子票證系統共通技術規範研究與票證一卡通推動計畫(4/4)

著 者：黃文鑑、許安慶、劉明杰、汪經堯、王穆衡、黃立欽

出版機關：交通部運輸研究所

地 址：10548 臺北市敦化北路 240 號

網 址：www.iot.gov.tw (中文版>圖書服務>本所出版品)

電 話：(02)23496789

出版年月：中華民國 100 年 8 月

印 刷 者：群彩股份有限公司

版(刷)次冊數：初版一刷 100 冊

本書同時登載於交通部運輸研究所網站

定 價：200 元

展 售 處：

交通部運輸研究所運輸資訊組 · 電話：(02)23496880

國家書店松江門市：10485 臺北市松江路 209 號 · 電話：(02)25180207

五南文化廣場：40042 臺中市中山路 6 號 · 電話：(04)22260330

GPN : 1010002648 ISBN : 978-986-02-8807-0 (平裝)

著作財產權人：中華民國（代表機關：交通部運輸研究所）

本著作保留所有權利，欲利用本著作全部或部分內容者，須徵求交通部運輸
研究所書面授權。

交通部運輸研究所合作研究計畫出版品摘要表

出版品名稱：交通電子票證系統共通技術規範研究與票證一卡通推動計畫(4/4)			
國際標準書號（或叢刊號） ISBN 978-986-02-8807-0(平裝)	政府出版品統一編號 1010002648	運輸研究所出版品編號 100-106-4253	計畫編號 99-MDB005
本所主辦單位：運輸經營與管理組 主管：王穆衡 計畫主持人：王穆衡 研究人員：黃立欽 聯絡電話：(02) 2349-6837 傳真號碼：(02) 2545-0431	合作研究單位：台灣世曦工程顧問股份有限公司 計畫主持人：黃文鑑 研究人員：許安慶、劉明杰、汪經堯 地址：臺北市內湖區陽光街 323 號 聯絡電話：(02) 87973567	研究期間 自 99 年 3 月 至 99 年 12 月	
關鍵詞：電子票證、智慧卡、驗證機制			
<p>摘要：</p> <p>電子票證營運業者除悠遊卡公司外，其餘營運量均未能達規模經濟，故後續的系統維運、擴充與票證系統間的整合將是各票證公司嚴峻的課題。</p> <p>為了使各票證公司能夠達成足以維持正常營運的交易量，「一卡通用、多卡相容」一直都是交通部之政策目標，故政府與民間必須合作以營造一個利於票證整合與相關技術發展的基礎環境。</p> <p>本期研究將對一機多卡交易所衍生之商業技術的問題提出相關方案之初步建議；同時對中國大陸邏輯加密卡升級為 CPU 卡之因應策略進行探討。</p>			
出版日期	頁數	定價	本出版品取得方式
100 年 8 月	236	200	凡屬機密性出版品均不對外公開。普通性出版品，公營、公益機關團體及學校可函洽本所免費贈閱；私人及私營機關團體可按定價價購。
<p>機密等級：</p> <p><input type="checkbox"/> 密 <input type="checkbox"/> 機密 <input type="checkbox"/> 極機密 <input type="checkbox"/> 絶對機密</p> <p>(解密條件：<input type="checkbox"/> 年 月 日解密，<input type="checkbox"/> 公布後解密，<input type="checkbox"/> 附件抽存後解密，<input type="checkbox"/> 工作完成或會議終了時解密，<input type="checkbox"/> 另行檢討後辦理解密)</p> <p><input checked="" type="checkbox"/> 普通</p>			
備註：本研究之結論與建議不代表交通部之意見。			

PUBLICATION ABSTRACTS OF RESEARCH PROJECTS
INSTITUTE OF TRANSPORTATION
MINISTRY OF TRANSPORTATION AND COMMUNICATIONS

<p>TITLE: Universal Technical Specifications Research of Electronic Payment Systems and Universal Traffic Cards Promotion (Phase IV)</p>			
ISBN(OR ISSN) ISBN 978-986-02-8807-0(pbk.)	GOVERNMENT PUBLICATIONS NUMBER 1010002648	IOT SERIAL NUMBER 100-106-4253	PROJECT NUMBER 99-MDB005
DIVISION: Operations and Management Division			PROJECT PERIOD
DIVISION DIRECTOR: Mu-Han Wang			FROM March 2010
PRINCIPAL INVESTIGATOR: Mu-Han Wang			TO December 2010
PROJECT STAFF: Li-Chin Huang			
PHONE: (02) 2349-6837			
FAX: (02) 2545-0431			
RESEARCH AGENCY: CECI Engineering Consultants, Inc.			
PRINCIPAL INVESTIGATOR: Wen-Jian Huang			
PROJECT STAFF: An-Ching Hsu, Jing-Yao Wang, Ming-Jie Liou			
ADDRESS: No.323 Yangguang St , Neihu District , Taipei 11491 , TAIWAN , R.O.C.			
PHONE: (02) 87973567			
KEY WORDS: Electronic Payment, Smart Card, Validation Mechanism			
<p>ABSTRACT:</p> <p>Except for the Taipei Easy Card Company, the usage volume of all the e-ticketing operators in Taiwan have not yet reached a reasonable economic scale. Therefore, the upcoming system operation, expansion and inter-operator integration will be the most critical issue for all those e-ticketing operators.</p> <p>In order to reach a reasonable economic operation scale, for the ticket companies to maintain normal operation of the trading volume, “one card for all systems and all cards mutually compatible” will be the policy goal of the Ministry of Transportation and Communications. Hence, both the public and private sectors should work together to support a suitable fundamental environment for the e-ticketing integration and related technical development.</p> <p>Current researches have suggested some interesting preliminary solutions for the business issues that derived from the “one device fits all cards” policy. In the meantime, the worldwide trend of upgrading the traditional Mifare type of card to the CPU type of cards will be discussed, and some of the existing instances of this trend will also be closely examined.</p>			
DATE OF PUBLICATION August 2011	NUMBER OF PAGES 236	PRICE 200	<p>CLASSIFICATION</p> <p><input type="checkbox"/> RESTRICTED <input type="checkbox"/> CONFIDENTIAL <input type="checkbox"/> SECRET <input type="checkbox"/> TOP SECRET <input checked="" type="checkbox"/> UNCLASSIFIED</p>
The views expressed in this publication are not necessarily those of the Ministry of Transportation and Communications.			

目 錄

第一章 計畫說明	1-1
1.1 計畫背景	1-1
1.2 本期研究範圍與工作項目	1-1
第二章 前期研究成果與產業現況.....	2-1
2.1 本研究前三年成果回顧	2-1
2.2 國內電子票證系統營運現況	2-11
2.2.1 悠遊卡票證系統	2-12
2.2.2 臺灣通票證系統	2-13
2.2.3 南部地區交通 IC 智慧卡票證系統	2-14
2.2.4 高雄捷運一卡通系統	2-14
2.2.5 金門電子票證系統	2-16
2.2.6 高速公路電子收費系統	2-16
2.3 「電子票證發行管理條例」及相關法令	2-17
2.4 MIFARE Classic 卡片遭破解之分析	2-20
第三章 一機多卡整合模式之探討	3-1
3.1 一機多卡整合模式對交易速度的影響及等候時間之分析	3-1
3.2 一機多卡整合模式整體架構分析	3-5
3.3 一機多卡對交易時間之影響及票證技術解決實例	3-13
3.3.1 改善一機多卡交易速度之學理分析	3-13
3.3.2 改善一機多卡交易速度之實例	3-15
3.4 一機多卡整合模式商業技術層面影響因素分析	3-22
3.5 一機多卡整合模式策略期程建議	3-23
第四章 一機多卡整合模式影響因素實例探討	4-1
4.1 一機多卡整合模式實作案例	4-1
4.1.1 背景說明	4-1
4.1.2 整合架構	4-1
4.1.3 整合的前提條件與執行步驟	4-3
4.2 一機多卡整合模式之影響分析與因應作法	4-5
4.2.1 一機多卡整合模式之影響因素	4-6

4.2.2 一機多卡整合模式影響之權益關係人	4-12
4.2.3 一機多卡整合模式跨區優惠對不同角色之權益關係人的影響	4-15
4.2.4 一機多卡整合模式對產業生態的影響	4-19
4.2.5 一機多卡整合模式影響因素之因應作法	4-21
4.2.6 一機多卡整合模式實作案例之實證說明	4-24
第五章 交通電子票證應用 CPU 卡之探討	5-1
5.1 邏輯加密卡驗票機升級為 CPU 卡驗票機之技術探討	5-1
5.1.1 邏輯加密卡升級為 CPU 卡之趨勢與優勢	5-1
5.1.2 CPU 卡的傳輸標準與技術發展	5-3
5.1.3 邏輯加密卡升級為 CPU 卡之問題探討與因應策略	5-5
5.2 交通 CPU 卡技術規範發展與現況之探討	5-19
5.2.1 國際金融/信用卡的主要技術標準--EMV	5-19
5.2.2 中國大陸交通電子票證 CPU 卡規範發展與產業現況	5-19
5.2.3 日本 SONY FeliCa 技術規範發展與現況	5-34
5.3 以 CPU 卡為交通電子票證可能衍生之議題探討	5-43
第六章 電子票證發行管理條例之衝擊與影響分析	6-1
6.1 電子票證營運資格及專營規定對票證公司之影響	6-1
6.2 電子票證發行管理條例對於持卡人的保障	6-2
6.3 電子票證發行管理條例對票證整合之影響	6-4
6.4 電子票證發行管理條例對與現行電子票證業者的影響	6-6
第七章 結論與建議	7-1
7.1 結論	7-1
7.2 建議	7-2
參考文獻	參-1
附錄 1 期中報告審查意見回覆表	
附錄 2 期末報告審查意見回覆表	
附錄 3 專家學者座談會會議紀錄	
附錄 4 專家學者座談會引言簡報	
附錄 5 期末報告簡報	
附錄 6 「第五章 交通電子票證應用 CPU 卡之探討」之 CPU 卡參考規範	

圖 目 錄

圖 2-1 交三版卡片靜態資料驗證系統主畫面	2-6
圖 2-2 交三版卡片模擬情境檢測系統之開放交易減值模組畫面	2-6
圖 2-3 交三版卡片發行架構	2-7
圖 2-4 設備整合多卡交易時間分配	2-8
圖 2-5 以交通電子票證為主要用途之轉換模式	2-9
圖 2-6 大眾運輸系統選擇票證整合方案之流程	2-10
圖 3-1 多卡交易平均等候時間之比較	3-2
圖 3-2 多卡交易最長等候時間之比較	3-3
圖 3-3 多卡交易平均排隊人數之比較	3-4
圖 3-4 多卡交易最大排隊人數之比較	3-5
圖 3-5 電子票證產業結構圖	3-7
圖 3-6 電子票證應用項目平台各權益關係人的關係	3-8
圖 3-7 一機多卡驗票機之交易流程(本研究)	3-14
圖 3-8 富譽公司最佳化「判斷卡片歸屬」流程(本研究)	3-16
圖 3-9 多卡平行驗證之交易流程(本研究)	3-20
圖 3-10 專利證書 M370776 之非接觸式 IC 卡讀寫模組系統架構圖	3-21
圖 3-11 智慧巴士一機多卡(悠遊卡、高捷卡、台灣通、e 通卡)驗票機	3-22
圖 3-12 一機多卡短期整合策略：交易分流	3-24
圖 3-13 一機多卡中期整合策略：管線共構	3-25
圖 3-14 一機多卡長期整合策略：聯合處理	3-26
圖 4-1 一機多卡整合架構示意圖	4-2
圖 4-2 一機多卡整合模式示意圖	4-3
圖 4-3 一機多卡整合模式之執行步驟	4-4
圖 4-4 一機多卡整合模式影響因素分析	4-8
圖 4-5 一機多卡整合模式影響因素、所屬類型與權益關係人之對照圖	4-14
圖 5-1 TypeA 和 TypeB 載波調製深度	5-3
圖 5-2 2000~2009 年中國大陸城市交通領域「一卡通」年發卡量成長圖	5-28
圖 5-3 中國大陸公交「一卡通」業務規模前十大城市發展情況彙整表	5-29
圖 5-4 銀川市「城市一卡通」應用系統架構圖	5-31
圖 5-5 NFCIP-1 與 FeliCa 及 ISO/IEC/IEC14443 的對應關係	5-36

圖 5-6 Suica 卡區間定期票.....	5-38
圖 5-7 以 Suica 購買 JR 東日本定期票畫面	5-41
圖 5-8 Suica 簡易驗票機.....	5-42

表 目 錄

表 2-1 交三版草案資料欄位格式一覽表	2-3
表 2-1 交三版草案資料欄位格式一覽表(續).....	2-4
表 2-2 國內電子票證系統營運現況彙整表	2-11
表 2-2 國內電子票證系統營運現況彙整表(續).....	2-12
表 2-3 高雄捷運一卡通種類	2-15
表 2-4 電子票證交易(接觸式與非接觸式卡片)之安全規定.....	2-19
表 3-1 一卡、二卡、三卡與四卡交易之等候狀況比較	3-2
表 3-2 一機多卡整合模式商業技術之影響因素、所屬類型與權益關係人 的關聯性.....	3-11
表 3-2 一機多卡整合模式商業技術之影響因素、所屬類型與權益關係人 的關聯性(續).....	3-12
表 3-3 多卡交易測試主要階段所需時間	3-14
表 3-4 富譽公司進行一機多卡交易測試之驗票機規格	3-16
表 3-5 富譽公司一機多卡驗票機實機測試結果【單一 SAM 卡】	3-17
表 3-6 富譽公司一機多卡驗票機實機測試結果【加入第二張 SAM 卡】	3-18
表 3-7 富譽公司一機多卡驗票機實機測試結果【加入第三張 SAM 卡】	3-19
表 4-1 一機多卡整合模式受影響之營運邏輯	4-6
表 4-2 營運規則的分類與內容	4-7
表 4-3 一機多卡整合模式影響因素、所屬類型與權益關係人之關係	4-13
表 4-4 具「區域優惠」票卡跨區使用對各方權益關係人的影響	4-15
表 4-5 一機多卡整合模式影響因素與因應作法之矩陣表	4-17
表 4-5 一機多卡整合模式影響因素與因應作法之矩陣表(續).....	4-18
表 4-6 一機多卡整合模式因應作法與各層級權益關係人之關係	4-19
表 4-7 一機多卡整合模式對作業流程與責任角色之影響	4-20
表 4-8 一機多卡整合模式影響因素之因應作法	4-22
表 4-8 一機多卡整合模式影響因素之因應作法(續).....	4-23
表 4-9 一機多卡整合模式實作案例影響因素之解決作法	4-24
表 4-9 一機多卡整合模式實作案例影響因素之解決作法(續).....	4-25
表 4-10 一機多卡驗票機新增票證系統所需成本概算	4-26
表 4-10 一機多卡驗票機新增票證系統所需成本概算(續).....	4-27

表 5-1 MIFARE Classic 與 MIFARE Plus 卡片性能對比	5-8
表 5-1 MIFARE Classic 與 MIFARE Plus 卡片性能對比(續).....	5-9
表 5-2 八達通卡種類.....	5-37
表 5-3 JR 東日本特種車收費標準	5-39
表 5-4 JR 東日本「定期區間」通勤、通學票收費標準超過 5 萬円例舉	5-40

第一章 研究計畫說明

1.1 研究計畫背景

非接觸式交通電子票證目前已有悠遊卡、台灣通、TaiwanMoney、高速公路電子收費系統、高雄捷運一卡通等5個票證系統上線營運，並在其它非交通領域的應用逐漸拓展，如學生證、圖書館借書證、政府規費、社區門禁卡等，「電子票證發行管理條例」已於98年1月正式施行，交通電子票證將可朝小額消費業務推展。

交通電子票證營運業者除悠遊卡公司外，其餘營運量均未能達規模經濟，惟後續的系統維運、擴充與票證系統間的整合將是各票證公司嚴峻的課題。為了使各票證公司能夠達成足以維持正常營運的交易量，「一卡通用、多卡相容」一直都是交通部的政策目標，故政府與民間必須合作以營造一個利於票證整合與相關技術發展的基礎環境。

前期研究已完成在以輪詢法前提下，設備整合多卡交易速度之測試與影響評估及以交三版(草案)為基礎之票證整合驗證機制，本期研究將對「一機多卡交易模式」的票證技術及所衍生之商業技術進行探討並提出相關方案建議；同時對中國大陸邏輯加密卡升級為CPU卡之作法進行初步探討。

1.2 本期研究範圍與工作項目

本研究屬於「智慧型運輸系統」之「先進公共運輸系統」與「電子收付費系統」的相關應用研究，本期為第四年期，將以前三年期計畫的成果為基礎，完成以下的工作內容與項目：

一、確立研究目標與範圍

以工作計畫書所研擬之目標、範圍與方法為研究工作進行之依據，並在研究過程中視需要修正研究目標與範圍。

二、電子票證系統資料蒐集

進行國內電子票證系統營運資料蒐集，以及國際間對於電子票證整合

議題之最新資訊及執行進度。

三、以前端設備整合多卡交易之探討

本研究第三期曾提出「多卡平行驗票機」應用在前端設備票證整合的構想，惟「多卡平行驗票機」乃一概念性的說法，其系統架構及元件規格將因廠商所採用的技術而異，本研究例舉市場上已開發成功之「多卡平行驗票機」的技術原理供相關單位參考。

四、一機多卡整合實作之影響因素分析

本研究將探討「一機多卡整合模式」可能衍生之運輸業者間票證作業流程衝突的問題，並以悠遊卡及台灣通之前端整合工程為例，歸納影響因素分析並提出解決方案建議。

五、交通電子票證應用 CPU 卡之探討

蒐集並分析比較 CPU 卡之技術規範，同時就使用 CPU 卡的效益進行評估，以供我國未來推動及制定 CPU 卡技術規範時之參考。

六、電子票證發行管理條例之影響評估

本研究將探討電子票證發行管理條例施行之後，對於國內交通電子票證產業之衝擊，以及交通電子票證與其它非交通電子票證整合機制之影響。

第二章 前期研究成果與產業現況

2.1 本研究前三年成果回顧

本期為本研究四年期計畫的最後一期，前三年期計畫已先後完成國內電子票證系統營運與設備開發現況調查、臺鐵電子票證系統整合規範需求分析、交三版(草案)資料規式與交易流程定義、交三版(草案)驗證機制規劃與驗證系統開發、驗票機整合多卡交易之速度測試與影響評估等工作項目。

本研究前三期研究成果如下：

一、國內電子票證系統及設備廠商開發現況

在卡片方面，國內各票證系統除南部地區 TaiwanMoney 系統外，其餘系統均使用 MIFARE 系列卡片，因此卡片規格與功能大致相同，說明如下：

1. 卡片規格符合交通部「電子票證系統之多功能卡片規劃書」第二版及 ISO7816、14443 等國際標準。
2. 卡片與讀卡機之讀寫距離至少可達 5 公分以上。
3. 可設定不同身分之票種，包括普通票、敬老票、愛心票及學生票等。
4. IC 卡須能記錄最近六筆交易資料，包括讀寫裝置序號、日期、時間、扣款金額交易地點及餘額。
5. 具備至少 1K Byte 之記憶體空間以儲存各項資料。

MIFARE 卡片的資料儲存於內部所提供的記憶空間，其能被切分成數個相等大小的扇區(Sector)，每個扇區內包含相等數量的區塊(Block)，AC(Access control)可管控每一個扇區的存取權限，包括存取認證金鑰(Key)及存取條件(Access condition)等設定。

在驗票機部份，國內除南部地區 TaiwanMoney 系統同時支援 MIFARE 及 PayPass 卡片外，其餘系統均僅支援 MIFARE 卡片，TaiwanMoney 驗票機之加密算法採用 RSA，MIFARE 系統驗票機均採用 DES 或 3 DES 演算法。MIFARE 系統驗票機若欲讀取經 EMV 認證之 TaiwanMoney 卡片，驗票機也必須取得 EMV 認證；各系統驗票機交易速度均要求在 0.6 秒以下，

部份系統更要求在 0.3 秒以下；各系統驗票機記憶體容量因建置時期的遠近，自 8 至 256MB 不等；而在驗票機 PSAM 卡插槽數量方面，悠遊卡公司大部分驗票機(RC171)僅有 1 個插槽(測試用 SLOT)，少部份驗票機(RC531)則具有 4 個插槽，因此若採用 PSAM 卡進行票證整合，其整合成本較高；其餘票證公司驗票機的 PSAM 卡插槽則在 4 個以上。

二、電子票證跨系統整合模式評估

第一年期計畫評估三種跨票證系統整合技術方案，分別是以 PSAM 卡於前端設備整合發卡組織的金鑰、以 JAVA 整合卡於前端設備整合發卡組織的金鑰、發行交三版(草案)卡片整合不同發卡組織前端設備。經由歷次技術研討會的討論得到第三方案[發行交三版(草案)卡片整合不同發卡組織前端設備]具有整合成本較低的優點，本方案規劃具有整合國內各大眾運輸系統電子票證功能之交三版(草案)卡片資料規格，並利用方案一的 PSAM 卡整合技術，修改各系統既有驗票機使其讀取交三版(草案)卡片。本方案可避免每增加一個票證營運系統就必須更改前端設備軟體、部份票證系統驗票機因未配置兩個(含)以上 PSAM 卡插槽而無法容納多個 PSAM 卡，以及因太多 PSAM 卡在傳統同詢法運作下可能會影響驗票機交易速度的問題。

前期所建議之「發行交三版(草案)卡片整合不同發卡組織前端設備的票證整合方案」，其理念係將目前各票證組織所發行的電子票證定位為「在地票證卡」，該票卡僅能使用於該票證系統內；「交三版(草案)卡片」則由票證組織另外發行，制定統一的票卡檔案資料格式、交易流程及 APDU 以達到跨系統互通的目的，且交三版(草案)卡片不會取代在地票證卡，各票證組織可自行選擇適當策略逐漸過渡到交三版卡片。

三、交三版(草案)卡片規格與交易流程

交三版(草案)以交二版為基礎，其與交二版的主要不同處在於：

1. 彙整並精簡卡片交易所需的欄位：交三版(草案)以持卡人的「電子票證收費模式」作為交易資料檔案欄位規劃的方向，以簡化卡片交易流程並增加交易速度，交三版(草案)資料欄位格式如表 2-1。
2. 明確規範交易流程：規劃卡片交易時主交易流程及參考交易流程，透過統一的交易流程，各系統的驗票機才能彼此讀寫卡片資料。

3. 增加雙介面複合式卡的參考規範：以 TaiwanMoney 為參考規範，供非使用 MIFARE 系列卡片的發卡單位參考。

表 2-1 交三版(草案)資料欄位格式一覽表

資料類別	使用扇區位置	資料內容	存取權限
目錄服務區	0	卡片出廠資料	寫：卡片製造廠 發卡單位 讀：應用系統(固定 Key Value，定義為 A0~A5 共 6 個 bytes)
		目錄服務指標(1)、(2)	
共同資料區	1	發行管理資料	寫：發卡單位 加值單位 讀：應用系統
		票值管理資料	
		卡片防偽驗證資料	
電子票值	2	主要票值	寫：發卡單位 加值單位 讀：應用系統
		票值備份	
		票值加值記錄	減值：交易系統
個別應用資料區	3	卡片交易狀態資料	寫：交易系統
		最近兩筆交易記錄(1)	讀：應用系統
		最近兩筆交易記錄(2)	
	4	最近六筆交易記錄(1)	寫：交易系統
		最近六筆交易記錄(2)	讀：應用系統
		最近六筆交易記錄(3)	
	5	最近六筆交易記錄(4)	寫：交易系統
		最近六筆交易記錄(5)	讀：應用系統
		最近六筆交易記錄(6)	
個別應用資料區	6~8		寫：發卡單位 讀：發卡單位指定系統
交三版應用資料區	9	異機進出連續型封閉交易系統定期票票卡管理資料	寫：交易系統 讀：應用系統
		異機進出連續型封閉交易系統最近兩筆交易記錄(1)	
		異機進出連續型封閉交易系統最近兩筆交易記錄(2)	
	10	同機進出連續型封閉交易系統定期票票卡管理資料	
		同機進出連續型封閉交易系統最近兩筆交易記錄(1)	寫：交易系統 讀：應用系統
		同機進出連續型封閉交易系統最近兩筆交易記錄(2)	

表 2-1 交三版(草案)資料欄位格式一覽表(續)

資料類別	使用扇區位置	資料內容	存取權限
交三版應用資料區	非連續型封閉交易系統	非連續型封閉交易系統定期票 票卡管理資料	寫：交易系統 讀：應用系統
		非連續型封閉交易系統最近兩 筆交易記錄(1)	
		非連續型封閉交易系統最近兩 筆交易記錄(2)	
保留區	12~15		寫：未定義 讀：未定義

註 1：應用系統：僅能提供持卡人查詢及交易過程中「讀」(不包括「寫」)的服務系統，屬於交易系統下的應用功能。

註 2：交易系統：可提供持卡人完整交易的服務系統，包括減值、加值及查詢等，交易資料必須儲存於一個專用的 sector 中，並配屬唯一的 AID(Application Identifier, 應用識別碼)。例如：台北大眾捷運系統(0x02)、臺灣汽車客運系統(0x07)等。

交三版(草案)「資料應用區 S09~S11」所規劃之「連續型封閉交易系統」及「非連續型封閉交易系統」係依據持卡人的「電子票證收費模式」做為交易資料檔案欄位規劃的方向。檢視國內目前可能使用於電子票證的運輸系統，依照扣款行為可概分為二大類，分別是封閉交易系統(有 IN 及 OUT，然後完成扣款)及開放交易系統(一次扣款)；封閉交易系統可再分為「連續性」及「非連續性」兩小類，其扣款模式以「非連續性封閉性系統(深色)接繼連續性封閉性系統(淺色)」最常應用：



例如：

1. 情境一：計時停車場(IN)→[捷運(IN)→捷運(OUT)]→計時停車場(OUT)
2. 情境二：計時停車場(IN)→ [捷運(IN)→捷運(OUT)] → [計次公車]
→計時停車場(OUT)
3. 情境三：計時停車場(IN)→ [捷運(IN)→捷運(OUT)] → [計次公車]
→ [計程公車(IN)→計程公車(OUT)] →計時停車場(OUT)

以上計時停車場屬於「非連續性封閉交易系統」；捷運及計程公車屬於

「連續性封閉交易系統」，必須完成完整的扣款流程之後，才能接續其它交易系統；計次公車及計程車屬於一次收費的「開放性交易系統」。

交三版(草案)在交易資料檔案欄位規劃上力求精簡，以簡化交易流程及增加卡片交易速度，故將「開放性交易系統」的交易資料直接讀寫於「主要票值」欄位，並將「連續性封閉交易系統」再分為「異機進出連續性封閉交易系統」及「同機進出連續性封閉交易系統」，因為前者進/出的驗票機應該不會是同一台，例如捷運；後者進/出的驗票機應該是同一台，例如公路汽車客運以里程計費，二者的交易流程略有不同。

根據以上分析，交三版(草案)規劃三個卡片資料扇區存放所有交通電子票證交易所需的資料及紀錄，分別是「異機進出連續性封閉交易系統」、「同機進出連續性封閉交易系統」以及「非連續性封閉交易系統」。

在交三版(草案)之討論與制定過程中，由本所邀集國內各電子票證公司以及臺鐵、高鐵等運輸業者，共進行 16 次的技術討論會議，完成交三版(草案)，並於 97 年 6 月提報交通部進行後續審查作業。

四、交三版(草案)驗證機制規劃與檢測系統開發

為了建立一套公正的交三版(草案)卡片資料格式及交易流程的檢驗機制，以驗證各家票證系統發行的卡片是否依照交三版(草案)的規範，本研究規劃完成交三版(草案)驗證機制，包括驗證申請作業流程、驗證系統架構及驗證流程。驗證流程分為兩階段，包含卡片靜態資料驗證及卡片模擬情境檢測系統，已分別於第二、三年期計畫開發完成。卡片靜態資料驗證可以檢視送測之卡片資料內容是否符合交三版(草案)資料欄位的定義，包括欄位編碼方式、資料型態及金鑰存取權限檢查等，靜態資料驗證系統開發成果之主畫面如圖 2-1；卡片模擬情境檢測系統即在檢核不同之驗票設備間是否能正確進行減值交易，使卡片能在不同型態之載具中使用，本系統之開放交易減值模組開發成果之畫面如圖 2-2。

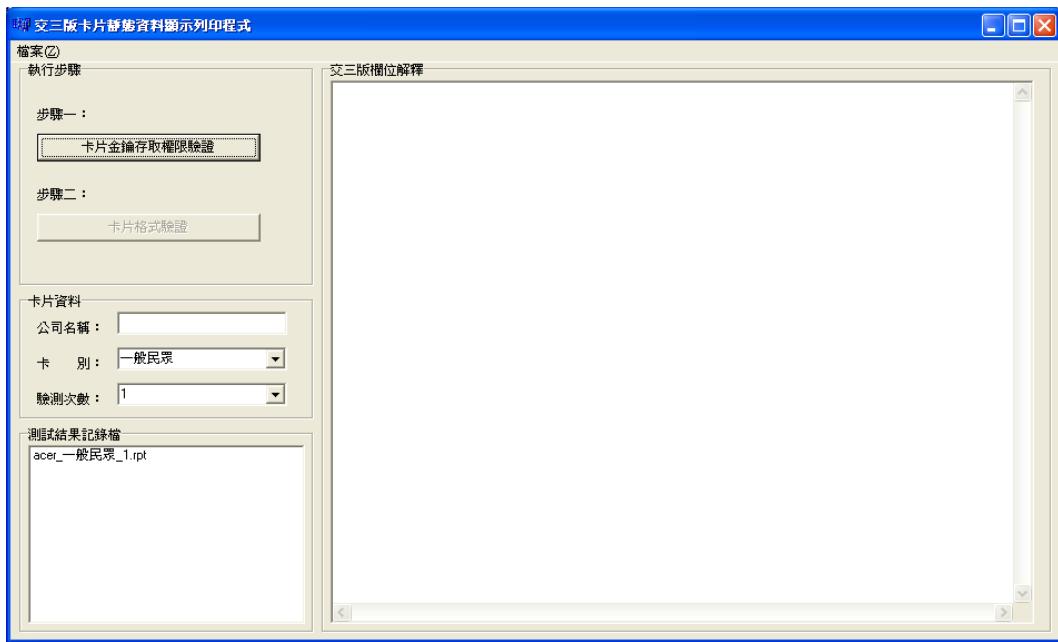


圖 2-1 交三版(草案)卡片靜態資料驗證系統主畫面

資料來源：交通部運輸研究所，交通電子票證系統共通技術規範研究與票證一卡通推動計畫(2/4)，民國 98 年。

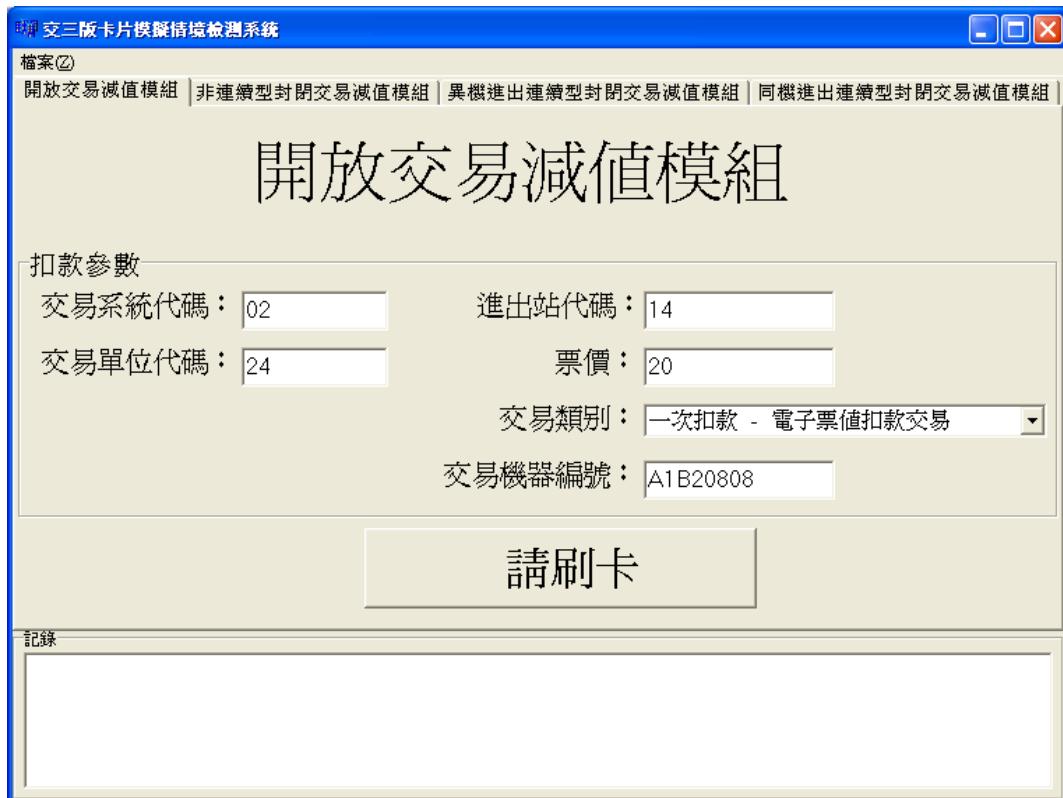


圖 2-2 交三版(草案)卡片模擬情境檢測系統之開放交易減值模組畫面

資料來源：交通部運輸研究所，交通電子票證系統共通技術規範研究與票證一卡通推動計畫(3/4)，民國 98 年。

五、電子票證系統後台功能整合建議

本研究針對票證整合後台部份的問題提出建議，包括金鑰整合、卡片真偽確認、交易真偽確認、後台交易/黑名單交換等後台相關技術的整合機制。其中在金鑰整合方面，本研究規劃的交三版(草案)發卡流程，須先成立電子票證公信單位(如公協會)，由公信單位負責管理交三版(草案)減值主金鑰組及防偽驗證碼母金鑰，保管於各方可信賴的安全機房，並制定金鑰管理辦法及機房管理辦法等相關作業程序，以確保金鑰的安全，各票證公司則負責管理加值主金鑰組，如圖 2-3。

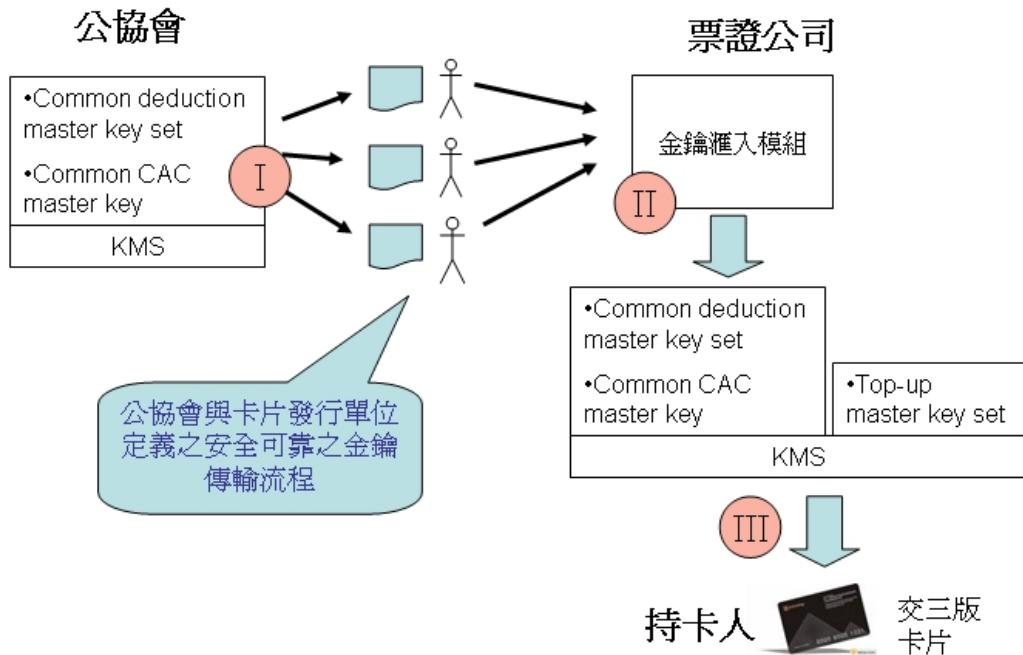


圖 2-3 交三版(草案)卡片發行架構

資料來源：交通部運輸研究所，交通電子票證系統共通技術規範研究與票證一卡通推動計畫(2/4)，民國 98 年。

六、設備整合多卡交易速度之測試與影響評估

不同電子票證系統整合主要可分為卡片資料讀寫整合[如採用交三版(草案)整合]及前端設備互通整合兩種方式。為探討驗票機整合多張不同票證系統卡片後對於交易速度產生的影響，本研究第三年期以營運中同規格之驗票機，採輪詢法對多張由不同票證公司發行的卡片進行整合交易速度的測試，結果顯示：二卡交易時交易時間已超過大多數大眾運輸系統能夠接受的 0.6 秒，三、四卡交易時間均已超過 1 秒以上，多卡交易之時間如圖 2-4。本研究亦針對多卡交易對於未來捷運系統出站乘客等候時間的影響

評估結果，當假設情境由一卡交易改變至二卡交易時，乘客等候時間或排隊人數增加幅度有限(增加 32%，以捷運臺北車站為例)，但到了三卡或四卡交易時，等候時間增加幅度就以倍數成長(分別增加 167%及 412%，以捷運台北車站為例)，已大幅超出捷運系統乘客所能接受的範圍，因此採用現行驗票機一個控制器控制多張 PSAM 卡的票證整合方式無法滿足大眾運輸系統交易速度的需求，必須採用卡片整合的方式，使交易卡片種類限制在二張以內，才是較佳的票證整合方式。

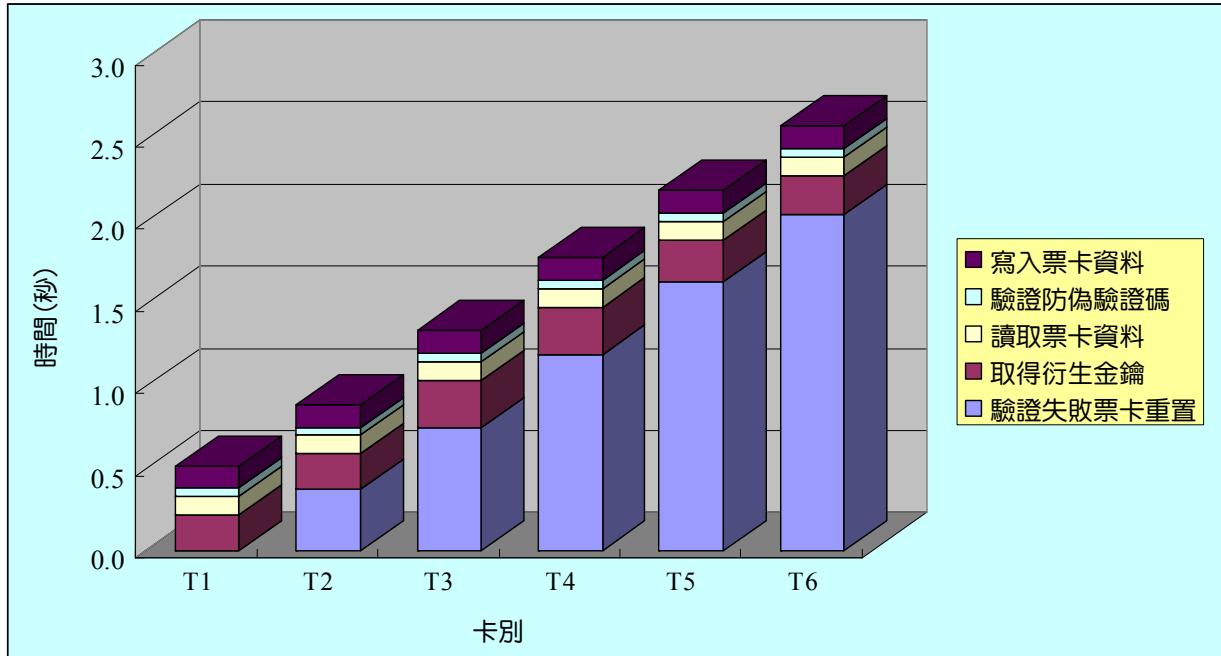


圖 2-4 設備整合多卡交易時間分配

資料來源：交通部運輸研究所，交通電子票證系統共通技術規範研究與票證一卡通推動計畫(3/4)，民國 98 年。

七、對國內電子票證系統從邏輯加密卡轉換為 CPU 卡的過程提出建議模式

本研究針對國內電子票證系統如何從邏輯加密卡轉換為 CPU 卡的過程提出三種建議模式，其中以模式一「以交通電子票證為主要用途之轉換模式」(圖 2-5)對持卡人的方便性最佳、轉換成本最低、完成轉換時間所需時間也最短，因此為本研究建議的最適轉換模式。

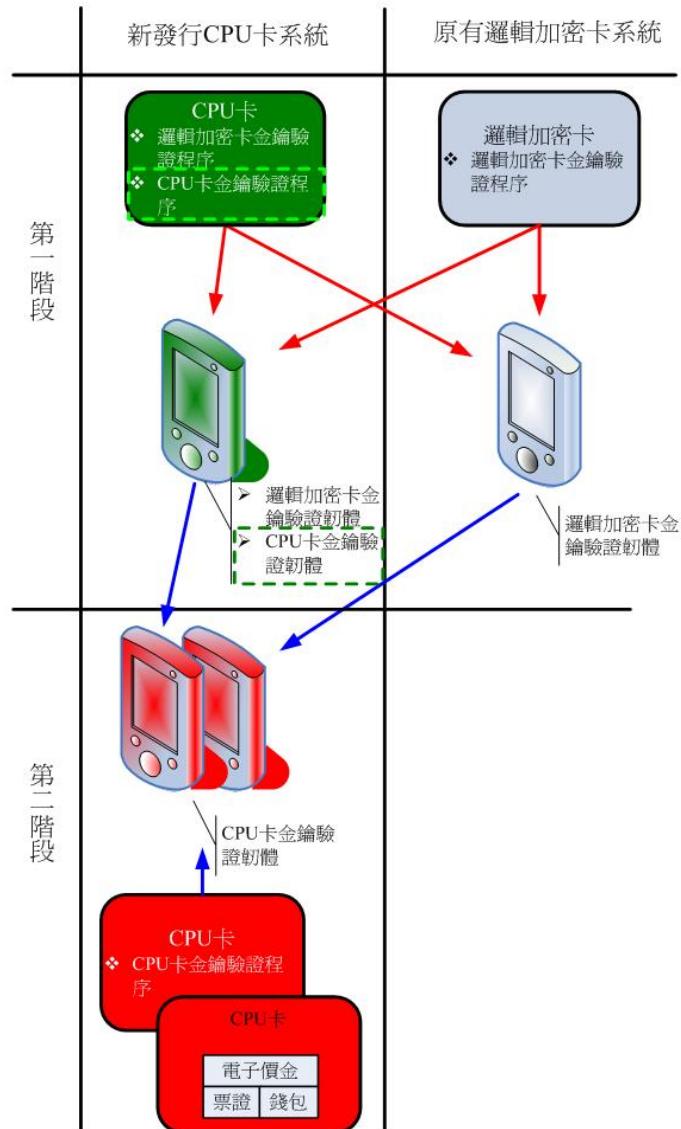


圖 2-5 以交通電子票證為主要用途之轉換模式

資料來源：交通部運輸研究所，交通電子票證系統共通技術規範研究與票證一卡通推動計畫(3/4)，民國 98 年。

八、提出在不同大眾運輸系統的經營環境及策略下，選擇不同票證整合方案的建議。

本研究提出在不同大眾運輸系統的經營環境及策略下，選擇不同票證整合方案的建議，主要考量因子包括外部經濟規模、大眾運輸路網環境、營運整合利基、特殊商業利益及票證整合技術等，其中前四項考量因子的選擇策略分為單向票務整合(本身不發卡)及發卡互通整合兩種方式，票證整合技術則分為採用交三版(草案)模式整合及採用多卡平行驗票機整合兩種方式。交三版(草案)模式整合除了須由交通部公告交三版(草案)的卡片規

範及交易流程建議外，還必須成立具有公信力之電子票證公協會以管理交三版(草案)減值母金鑰組、驗證交三版(草案)卡片與設備等相關配套措施。

若採用多卡平行驗票機方案，則面臨現有驗票機需全數汰換之建置成本高昂的問題，較適合新建置電子票證系統的大眾運輸業者採用。

本研究建議之「大眾運輸系統選擇票證整合方案流程」如圖 2-6。

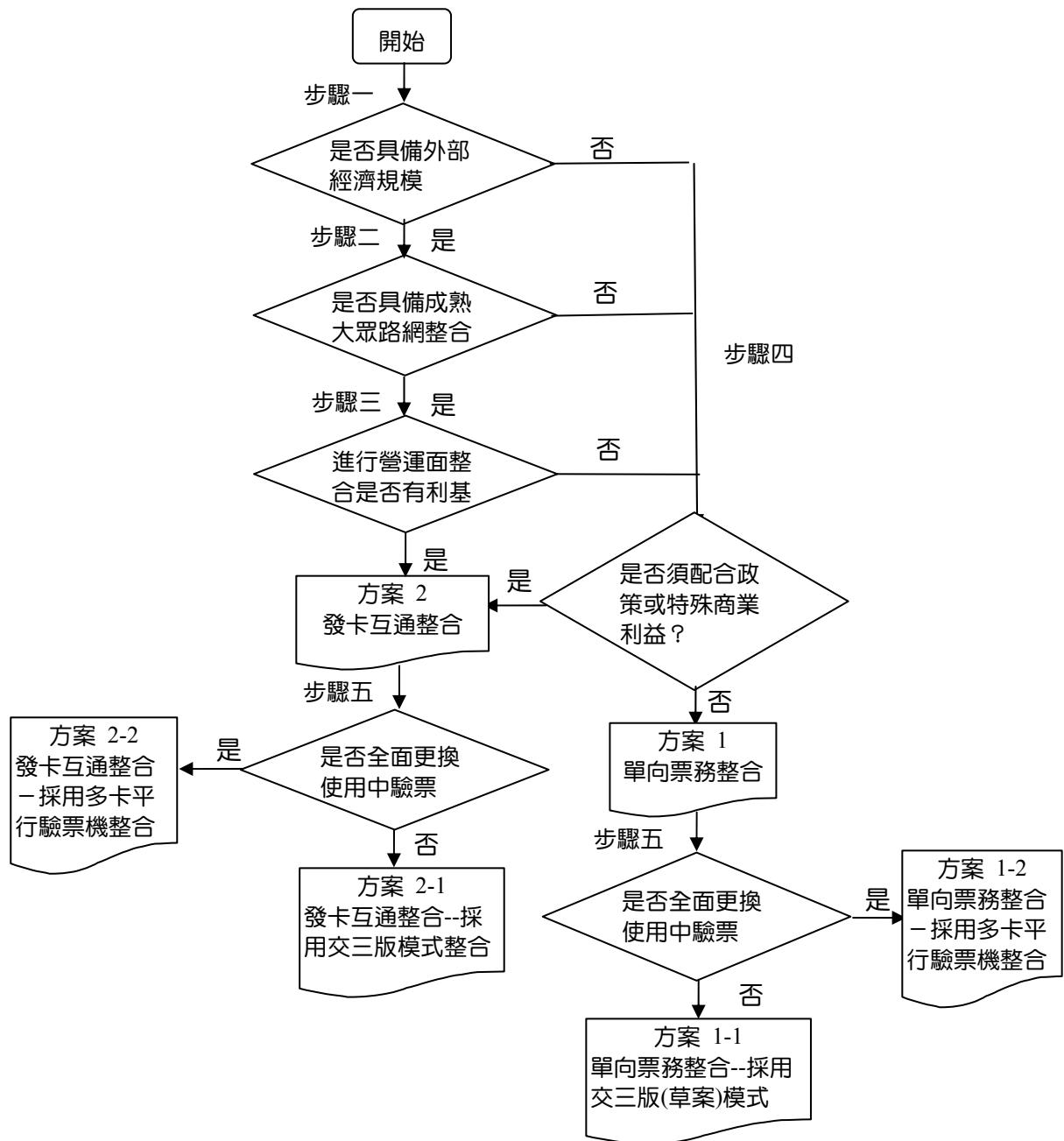


圖 2-6 大眾運輸系統選擇票證整合方案之流程

資料來源：交通部運輸研究所，交通電子票證系統共通技術規範研究與票證一卡通推動計畫(3/4)，民國 98 年。

2.2 國內電子票證系統營運現況

國內第一套大規模採用 IC 智慧卡之電子票證系統可追溯至金門地區於民國 89 年完成建置的大眾運輸電子票證系統，之後台灣省公共汽車客運商業同業公會聯合會(簡稱省聯合會)於民國 90 年在 15 家客運公司、20 條測試路線短暫測試「易行卡」電子票證系統，其他包括悠遊卡、中彰投公車、南部七縣市公車、桃竹苗公車、高雄捷運、馬祖公車等電子票證系統亦陸續營運，其中悠遊卡系統則憑藉著大台北地區大眾運輸系統高使用量，以及非交通運輸應用範圍如數位借書證及學生證的大力推廣，目前已成為國內發卡量最大、使用範圍最廣的電子票證。

除了悠遊卡外，在交通部大力推展電子票證的政策之下，國內各地方政府也著手發展相關的應用，目前票證系統現況整理如下，並將各系統之重要營運現況彙整如表 2-2：

表 2-2 國內電子票證系統營運現況彙整表

統計時間：民國 99 年 10 月

系統別 營運現況	悠遊卡	臺灣通	TaiwanMoney	一卡通	金門 電子票證	e 通卡
營運單位	悠遊卡股份有限公司	台灣智慧卡股份有限公司	萬事達卡國際組織	高雄捷運股份有限公司	金門縣公共車船管理處	遠通電收股份有限公司
開始營運時間	民國 91 年	民國 93 年	民國 95 年	民國 97 年	民國 88 年	民國 95 年
交通應用範圍	台北捷運、聯營公車(台北縣市、基隆、宜蘭、馬祖)、國道客運、纜車、淡水河藍色公路、臺鐵、公有路邊及路外停車場、台北市公共自行車租賃、台中市快捷公車、計程車(敬老愛心車隊)	桃竹苗、中彰投、花東地區及雲林縣部分客運，共 11 縣市、21 家業者；99 年 6 月 15 日於臺鐵新竹-基隆-瑞芳間計 28 站(暖暖站除外)全線售卡；金門縣公車處票證整合建置案進行中。	南部七縣市公車、高雄市輪船、公車、高雄捷運、公有立體停車場	高雄捷運、高雄市輪船、公車(高雄市公車、東南客運、南台灣客運、高雄客運、義大客運及臺南市公車)、高雄市立圖書館	公車、渡輪	高速公路(國 1、3、5)
驗票機	約 16,000 部	3,600 部	2,327 部	2,100 部	60 部	115.6 萬個 OBU
累計發卡量	2200 萬張	151 萬張	28 萬張	177 萬張	10 萬張	140 萬張

表 2-2 國內電子票證系統營運現況彙整表(續)

統計時間：民國 99 年 10 月

系統別 營運現況	悠遊卡	臺灣通	TaiwanMoney	一卡通	金門 電子票證	e 通卡
其他應用範圍	小額錢包、學生證、圖書館借、動物園門票、醫院診療費	學生證、停車場	具有小額消費之電子錢包功能	圖書館借書學生證	無	無
今年營運大事紀	<ul style="list-style-type: none"> • 民國 99 年 1 月成為第一家經金管會核准發行電子票證之專業發行機構。 • 民國 99 年 4 月 1 日悠遊卡小額消費全面上線；該月悠遊卡高雄及台中客服中心正式啟用。 • 民國 99 年 10 月悠遊卡、7-ELEVEN 和中華電信三方攜手合作，成立「悠遊卡紅利積點策略聯盟」。 	<ul style="list-style-type: none"> • 民國 99 年 6 月 15 日於臺鐵新竹-基隆-瑞芳間計 28 站（暖暖站除外）完成建置。 • 民國 99 年 9 月 1 日，臺灣通發行鼎東客山線學生認同卡、通勤認同卡。 	<ul style="list-style-type: none"> • 該系統維運服務將於民國 100 年 6 月 8 日屆滿，系統營運廠商必須與高雄市政府續約方能提供系統營運服務。 	<ul style="list-style-type: none"> • 民國 99 年 4 月提供『一卡通手機貼』功能。 	<ul style="list-style-type: none"> • 民國 99 年度 5 月辦理系統更新招標，由台灣智慧卡公司得標建置。 	<ul style="list-style-type: none"> • 民國 99 年 7 月推出「全民體驗 ETC」及「ETC 成功扣款即享 95 折優惠」，鼓勵民眾裝置 OBU。 • 民國 99 年 11 月 06 日～至 100 年 12 月 31 日止，推出「全民體驗 ETC 方案」。

2.2.1 悠遊卡票證系統

悠遊卡(Easy Card)是以大台北地區為主要營運範圍的非接觸式交通電子票證系統，於民國 91 年始正式營運，由悠遊卡股份有限公司(原台北智慧卡票證公司)發行，可用於搭乘台北、基隆、宜蘭、馬祖地區之捷運、市區公車、公路客運等，並可搭乘部分國道客運班車，為目前國內最大之交通電子票證系統。

由於台北都會區與鄰近縣市通勤頻繁，且台北與基隆間大多數之大眾運輸

系統可使用悠遊卡，因此，臺鐵局與悠遊卡公司於民國 97 年 6 月於樹林—松山 4 個火車站利用悠遊卡試辦短途通勤便捷通過閘門活動，民國 97 年 8 月擴大至基隆—中壢間其他 15 個火車站。

悠遊卡公司於民國 98 年 3 月推出信義計畫區「YouBike 微笑單車」系統，該無人化管理系統採用悠遊卡進行自行車租賃，其中設置 718 個悠遊卡驗票機的自行車停車位。該系統區分為短期卡及長期卡兩類，使用短期卡民眾需先至 Kiosk(互動式多媒體資訊站)利用悠遊卡及晶片信用卡完成開卡動作，之後可持悠遊卡進行自行車租借及歸還扣款動作，使用長期卡民眾須先至服務中心利用悠遊卡及第二證件完成註冊及開卡動作，之後可持悠遊卡進行自行車租借及歸還扣款動作。

民國 98 年 6 月悠遊卡推出 3,400 輛之愛心計程車服務(約佔全市計程車數量之 11%)，車上配備悠遊卡驗票機，除服務老人及身心障礙者外，一般民眾亦可刷卡付費。

民國 99 年 1 月 28 日金管會通過悠遊卡公司申請成為第一家核准發行電子票證之專業發行機構。

民國 99 年 4 月 1 日，悠遊卡小額消費全面上線，包括 7-ELEVEN、全家便利商店、萊爾富、OK 超商等四大超商在內，超過一萬家特約商店可使用悠遊卡付費。同月，悠遊卡台中及高雄客服中心正式啟用。

民國 99 年 10 月，悠遊卡、7-ELEVEN 和中華電信三方攜手合作，成立「悠遊卡紅利積點策略聯盟」，共同發展悠遊卡紅利積點。悠遊卡公司將藉著策略聯盟建立紅利積點機制，促使更多通路加入悠遊卡紅利積點，提供持卡人更多用卡回饋。

2.2.2 臺灣通票證系統

「臺灣通」由台灣智慧卡公司營運的中彰投與桃竹苗地區兩大系統所組成，中彰投地區公車客運的系統原稱「e 卡通」，於民國 93 年 8 月啟用，建置與營運範圍涵蓋台中縣、市、彰化縣與南投縣內之 10 家客運業者(包括 5 家市區公車—台中客運、仁友客運、巨業交通、統聯客運與全航客運等與 5 家公路客運—豐原客運、彰化客運、員林客運、南投客運及總達客運等)；桃竹苗地區之「臺灣通」系統於民國 96 年 3 月開始營運，本套系統的公車客運路線涵蓋整個桃竹

苗生活圈，包括桃園客運、三重客運、新竹客運、中壢客運、亞通客運及苗栗客運等 6 家客運公司。

中彰投之「e 卡通」原與桃竹苗之「臺灣通」原本並不相通，民國 96 年在交通部的票證整合政策的推動與經費補助下，方於民國 97 年 4 月整合完成，卡片均可在對方系統車輛上使用。

民國 98 年，花蓮及台東地區客運業者由公路總局補助建置 IC 卡票證系統，採用台灣智慧卡公司的臺灣通票證系統，建置 209 台驗票機與 96 台人工加值機。

民國 99 年 6 月 15 日，臺灣通於臺鐵新竹-基隆-瑞芳間計 28 站(暖暖站除外)全線完成建置，除原有普通卡外，另增加兒童卡及敬老卡兩卡種。

民國 99 年 9 月 1 日，臺灣通發行鼎東客運山線學生認同卡、通勤認同卡。

2.2.3 南部地區交通 IC 智慧卡票證系統

高雄市政府交通局為配合交通部「國家發展重點計畫—提昇地方公共交通網計畫」，以高雄市為中心，結合南部七縣市之公路及汽車客運，建置具有結合交通票證、金融儲值與消費等付款機制之 TaiwanMoney，該計畫之建置與營運團隊由宏碁公司、國泰世華銀行、玉山銀行、萬碩公司及所組成，由萬事達卡國際組織提供卡片技術。

現行之 TaiwanMoney 種類可分為兩種，分別為 TaiwanMoney 信用卡以及 TaiwanMoney 儲值卡，前者為具有信用卡與電子錢包之多功能信用卡，而後者僅具有電子錢包功能。TaiwanMoney 之營運範圍包括高雄市公車/渡輪、公有停車場、高雄客運、嘉義縣公車、嘉義客運、新營客運、興南客運、屏東客運、國光客運、濱海客運及中南客運等十餘家業者，涵蓋 474 條公車路線及 5 條渡輪路線。

TaiwanMoney 營運團隊與高雄捷運公司依據交通部與高雄市交通局的要求，進行高雄捷運一卡通與 TaiwanMoney 的整合計畫，於公車及渡輪驗票機改裝成具有讀寫高捷一卡通的功能。在高捷車站方面，於通車初期利用公務門加裝 TaiwanMoney 驗票機，專供 TaiwanMoney 持卡人通關，由於目前的使用方式受到公務門位置、現場無服務人員處理卡片問題、卡片無法於捷運站加值等諸多限制，對於 TaiwanMoney 持卡人於高捷系統使用頗為不便。

2.2.4 高雄捷運一卡通系統

一卡通(I Pass)是高雄捷運公司發行之交通票證，於民國 97 年 3 月高雄捷運紅線通車時正式發卡。高雄捷運之一卡通票卡使用 MIFARE 技術，符合國際標準 ISO1443 之規範，並符合交通部「電子票證系統之多功能卡片規劃書第二版」之格式。

目前高雄捷運公司一卡通種類可分為普通卡、敬老卡、博愛卡、博愛陪伴卡、仁愛卡、學生卡、紀念卡、一日卡、旅遊卡等(彙整如表 2-3)。

表 2-3 高雄捷運一卡通種類

種類	售價	記名	計費方式	使用說明/優惠方法
普卡	200 元，可用 100 元，100 元為發卡費用(非押金)	否	全票	
一日卡	200 元，押金 70 元	否	一	一日內無限搭乘高雄捷運
暢遊卡	200 元，賣斷制	否	一	一日內無限搭乘高雄捷運、高雄市公車、渡輪
學生卡	200 元，可用 100 元，100 元為發卡費用(非押金)	否	學生票	
敬老卡	免費	是	半票	65 歲以上之高雄市民 ● 捷運半價計費 ● 高雄市公車每月免費 120 次，超過部分半價優惠 ● 高雄市渡輪每月免費 120 次，超過部分半價優惠
博愛卡	免費	是	半票	高雄市身障人士 ● 捷運半價計費 ● 高雄市公車每月免費 100 次，超過部分半價優惠 ● 高雄市渡輪每月免費 100 次，超過部分半價優惠
博愛陪伴卡	免費	是	半票 全票	高雄市身障人士之陪伴者(無陪伴時依全票計費) ● 捷運半價計費 ● 高雄市公車半價計費 ● 高雄市渡輪半價計費

資料來源：高雄捷運公司網站(www.krtco.com.tw)。

高雄捷運與市立圖書館合作，於民國 98 年 6 月下旬推出「無人微型圖書館」，可利用高雄捷運一卡通直接借書與還書，持卡者必須先憑身分證明與一卡通向市立圖書館登記，才能進行借書作業。

民國 99 年 4 月，高雄捷運推出「非卡式儲值卡」，利用一片「一卡通」手機貼，將原本的卡片變成輕巧的手機貼，不僅可搭捷運、公車及渡輪，功能與優惠折扣一樣不變。「一卡通」手機貼印刷面為電波屏蔽面，黏貼面為感應端，貼妥後可到各車站加值機進行儲值，進站時只要用手機背面去對準感應設備就可搭乘捷運。「一卡通」手機貼長 51mm / 寬 28mm / 厚 0.87mm，有普卡及學生卡兩種版本，適合多款手機搭配使用，但若為金屬背蓋，手機貼則無法使用，因為金屬背蓋會干擾手機貼正常感應。

2.2.5 金門電子票證系統

金門縣電子票證系統自民國 88 年啟用，為國內首先營運的 IC 卡電子票證系統，由金門縣公共車船管理處自行營運，為應用於當地公車及渡輪的電子票證。本系統規模相對較小，自民國 88 年至今之累計發卡量約 10 萬張，驗票機數量為 60 部。金門縣縣民搭乘公車雖然為免費，但必需使用電子票證，因此每位縣民均擁有一張卡，其他購卡者多為當地駐軍，外來訪客使用電子票證者並不多見。

由於本系統建置年代久遠，目前設備故障率較高，公共車船管理處已於民國 99 年度進行系統更新建置招標，係由台灣智慧卡公司得標進行建置。

2.2.6 高速公路電子收費系統

為配合國家交通政策推動，遠通電收公司接受國道高速公路局委託推動高速公路電子收費計畫，遠通電收公司為「遠傳」、「東元」、「精業」、「神通」四家公司共同組成，高速公路電子收費於民國 95 年 2 月正式提供服務。

遠通電收公司採用專用短距通訊(Dedicated Short Range Communication, DSRC)及車輛定位系統(Vehicle Positioning System, VPS)雙軌並行方案，於計畫初期採用 IC 智慧卡與 OBU 相結合之兩件式主動式設備(DSRC 車機+IC 儲值卡)，以提供遠距、非接觸式的電子收費服務，主要考量的因素是 DSRC 的車上單元(On Board Unit, OBU)及 IC 卡兩件式車機，可支援捷運、公車、停車收費的「交通一卡通」，而在未來 DSRC 與 VPS 結合以後，將可達到多樣化 ITS/Telematics 應用的目的。

車輛只需要安裝「高速公路電子收費 e 通機」並加上「高速公路電子收費卡

或 e 通卡」，就可以行駛電子收費 ETC 車道，通過收費站時不必停車即可進行自動扣款。目前所發行的票卡分為「高速公路電子收費卡」、「e 通卡」及「e 通聯名卡」，票卡均可使用於高速公路電子收費，惟「e 通卡」是與銀行共同發行的聯名卡，除了高速公路電子收費之外，亦可提供由銀行推出的加值服務，包括信用卡功能、電子錢包功能等。

遠通電收為提升電子收費利用率，於民國 99 年 7 月推出「全民體驗 ETC」及「ETC 成功扣款即享 95 折優惠」，希望藉此促銷活動鼓勵民眾裝置 OBU。

民國 99 年 11 月 6 日~至 100 年 12 月 31 日止，遠通電收利用「車牌圖像辨識系統」替代 OBU 的功能，用路人只要前往遠通直營門市、7-ELEVEN ibon 或全家 FamiPort 申辦全民體驗 ETC 方案，就可立即上路體驗 ETC。體驗期間每次通過 ETC 車道累計 1 點，每點價值 3 元 e 通機補貼金，最高累積 347 點可免費兌換 e 通機。

2.3 「電子票證發行管理條例」及相關法令

「電子票證發行管理條例」於民國 98 年 1 月正式頒布施行，該法令之重點如下：

- 一、本條例之主管單位為金管會。
- 二、以非銀行之發行機構為規範對象，金融機構依銀行法發行現金儲值卡不適用本條例之規定，而依本條例發行電子票證之發行機構則不適用銀行法第 42 條之 1 及第 47 條之 3 等規定。
- 三、發行機構之實收資本額須達新台幣三億元。
- 四、發行機構應將電子票證收取之款項採取下列方式之一，以確保電子票證發行之履約能力：
 1. 全部交付信託；
 2. 取得銀行十足之履約保證。
- 五、電子票證之儲存金額不得超過新台幣一萬元。
- 六、規定結算及清算方式
 1. 發行機構對以電子票證所為之交易，應每日定時結算應收及應付金額，並依結算結果撥付給特約機構。

2. 發行機構經主管機關核准辦理相關清算作業，應確保交易資料之隱密性及安全性，並負責資料傳輸、交換或處理之正確性。

該法案將對國內電子票證市場產生重大變革，首先，電子票證主管機關已明確訂定為金管會，且採用核准制，未來須經金管會核准才得辦理電子票證業務，既有票證公司則須在半年內申請核准；其次，對於非銀行體系的電子票證發行機構，其電子票證應用範圍將不僅侷限於交通電子票證，還能應用於其他商業體系，例如：小額消費。對於悠遊卡公司、高雄捷運公司與遠通電收公司等積極朝向小額消費應用發展之電子票證發行單位之未來發展有相當大助益；另外，本條例對於電子票證發行機構設立門檻的標準較高，如公司資本額及預付款項履約能力等，除了使未來想要發行電子票證的單位受到限制外，對於現存規模較小的電子票證公司影響甚大，未來必須致力於調整公司體質以符合該條例之規定。

「電子票證發行管理條例」公告後，金管會積極研擬相關施行規則，其中「電子票證發行機構業務管理規則」及「電子票證應用安全強度準則」等已經公布，其主要重點說明如下：

一、電子票證發行機構業務管理規則

本規則之主要內容歸納如下：

1. 電子票證原則上不得訂定使用期限，但訂有使用期限者應於電子票證上記載使用期限及終止使用之處理方式。
2. 電子票證之交易不得為電子票證間之資金移轉。
3. 發行機構不得就所發行之電子票證提供持卡人信用額度或代墊款項，但為單次墊款且使用於大眾運輸事業或停車場業者得不受限制。
4. 對於不符本條例中規定交付信託或取得銀行十足履約保證的發行機構，其調整期間最長不得逾三年。
5. 明定發行機構不得投資於其他企業，但於本條例公布施行前已投資於其他企業並經主管機關核准者，不在此限，惟其投資金額不得再增加。

二、電子票證應用安全強度準則

規定電子票證各項交易類型，應考量電子票證得使用之商品或服務之性質與其交易金額大小等因素，區分應用範圍等級，對於應用範圍等級較

廣之電子票證，其安全防護措施規定較嚴格，其中交通票證、政府規費、支付公用事業費用等不限金額，1,000 元以下之支付各項商品或服務之費用皆屬於第一級安全等級(較寬鬆)，1,000 元以上支付各項商品或服務之費用則屬於第二級安全等級(較嚴格)，安全規定依據五種交易類型(線上即時消費交易、非線上即時消費交易、線上即時加值交易、非線上即時加值交易、帳務清結算交易)，提供交易訊息之隱密性、完整性、來源辨識性及不可重覆性等規範，以及管理面、末端設備與環境面所應採取之防護措施及安全設計標準，其中非線上即時消費交易與即時加值交易的規範如表 2-4。根據該準則，現行電子票證的應用，均已符合第一級的安全規範，意即可以使用在交通票證、政府規費、支付公用事業費用等不限金額及 1,000 元以下之小額消費。

表 2-4 電子票證非線上交易(接觸式與非接觸式卡片)之安全規定

交易類型		非線上即時消費交易		非線上即時加值交易	
應用範圍等級		第一級	第二級	第一級	第二級
訊息隱密性		非必要	非必要	非必要	非必要
訊息完整性		B1	B2	B1	B3
來源辨識性	電子票證認證	D1	D2	—	—
	端末認證	E1	E2	E2	E2
不可重覆性		F	F	F	F

資料來源：電子票證應用安全強度準則(民國 98 年 07 月 16 日發布)。

表 2-4 中的代號簡要說明如下：

1. 訊息隱密性 A：應採對稱性加解密系統或非對稱性加解密系統，針對訊息進行全文加密
2. 訊息完整性 B：針對訊息採用能防止非惡意篡改訊息之檢核碼技術
 - B1：需加入檢核碼
 - B2：需加入押碼或數位簽章
 - B3：除須符合 B2 所要求之強度外，加值交易訊息之金額須參與訊息完整性之運算
3. 來源辨識性 D：對電子票證做認證
 - D1：末端設備需驗證電子票證(不指定加解密演算法)
 - D2：末端設備需驗證電子票證(須符合特定之加解密演算法)

4. 來源辨識性 E：對末端設備做認證

E1：電子票證需驗證末端設備或發卡端(不指定加解密演算法)

E2：電子票證需驗證末端設備或發卡端(需符合特定之加解密演算法)

5. 不可重複性 F：防止以先前成功之交易訊息完成另一筆交易

2.4 MIFARE Classic 卡片遭破解之分析

MIFARE Classic 卡片是一款具有密碼保護的邏輯加密卡，其密碼保護機制主要是由 RF 晶片(意即一般指稱之 RC171 或 RC531)產生具有加密保護之無線資料串送至卡片進行密碼驗證，若驗證成功則該 RF 晶片將可對卡片進行存取之動作。此 RF 晶片與卡片之加密保護機制乃是由 NXP 公司自行研發之 Crypto-1 加密機制來進行資料串加密之行為。因此，若破解 Crypto-1 加密機制，理論上將可算出單一卡片之個別金鑰，如讀取並寫入卡片之個別金鑰後，將可輕易複製一張相同之卡片。

2007 年一位德國的研究者 Henryk Plotz 以及一位美國的博士候選人 Karsten Nohl (University of Virginia)展示了他們破解 MIFARE Classic 的 Crytpo-1 加密機制的作法：他們將一張 MIFARE Classic 晶片一層一層磨去並使用電子顯微鏡進行照相，由此可以得到 MIFARE Classic 完整的實際電路，他們再依據加密電路所應具有之電路特徵進行電路判讀，進而推導出 Crypto-1 加密機制之演算方法，並於西元 2007 年 12 月於著名的德國駭客大會(24th Chaos Communication Congress)發表了整個破解的作法，會中並宣稱將於隔年(西元 2008 年)發表更進一步的細節。西元 2008 年 NXP 公司嘗試使用法律手段禁止該加密演算法之公開發表，然而被法庭以研究自由的原因而駁回。其作法就是先使用一讀卡設備讀取欲破解之讀卡機內之所含金鑰，並使用該金鑰來讀取路人皮夾中的卡片，再據此複製一張相同的卡片。

在西元 2010 年舉辦的第六屆臺灣駭客年會(HIT 2010)中，臺大電機系團隊便將發表的論文，以錄影方式實作如何將悠遊卡透過 Sniffer-Based(監聽封包)的方式，竄改悠遊卡的資料。

由以上的說明可知道 MIFARE Crypto-1 演算法已經被公開，而具有經驗之駭客將可輕易取得儲存於讀卡機中的金鑰，進而進行卡片複製的動作。然而以上的作法都只能針對單一張卡片進行破解及複製，到目前為止尚未有任何團體

宣稱已經破解每張卡片皆具有不同金鑰的 MIFARE 卡片系統，雖然依據理論的推論，破解每張金鑰皆不相同的 MIFARE 系統仍是有可能的，但至少在作法上將不可能如同原破解方式如此簡單。

目前在國內所使用的 MIFARE Classic 卡片之系統安全性皆是採用每張卡片金鑰皆不相同的作法，因此比較起來相對安全。然而必須注意的是，若 MIFARE Classic 卡片只是使用於單筆交易價格較為便宜之交通載具，破解一張卡片所能獲得的利益相對較小，但若是該卡片可以進行小額交易的話，則破解一張卡片所能得到的利益可能增加，因此若有人進行破解，則有可能造成金融秩序上的影響，這是未來電子票證將應用在小額消費市場時必須考量的因素。

第三章 一機多卡整合模式之探討

本研究第三期以模擬驗票機實機測試證實，當驗票機「取得衍生金鑰」及「驗證金鑰」之程序採「輪詢法」時，對於整合多卡交易速度有影響，若新增 SAM 卡在驗票機插槽的序位愈後面，則交易時間愈長，新增 SAM 的數量與交易時間呈遞增關係。

此研究成果發表之後，除引起產業界業者的注意之外，也讓後續電子票證招標機關開始重視驗票機交易時間的規範，故自民國 98 年以後大眾運輸系統有關電子票證建置的招標規範均明定一機多卡交易時間的上限，例如：

- 一、高鐵局桃園國際機場捷運線對非接觸式晶片卡讀寫機(CSCR-W)規定：內置八個 SAM 的驗票機，單一模組下讀取時間應小於 1 秒，並可讀取八種不同種類 CSC 及 CST，且得在設計上考量日後其中部份票證業者將 CSC 記憶卡改為 CPU 卡後之混搭情形下，仍能運作正常且不影響各種功能與效能。
- 二、台鐵局自動驗票系統規範書(TRAS(T))規定：CSC R/W 至少應能容納四個(含)SAM 卡，在單一 SAM 卡交易模式下，其交易時間不得超過 0.6 秒；四種 SAM 卡交易模式下，其交易時間不得超過 1 秒。
- 三、金門公車驗票機功能與規格規定：讀卡機應至少支援四個插槽以上(四種 SAM 卡模式可於 0.6 秒內完成各卡之完整交易)，且至少能實際成功讀取兩個以上 PSAM 裝置在同一讀卡機。

3.1 一機多卡整合模式對交易速度的影響及等候時間之分析

本研究前期以該期模擬驗票機實機測試一機多卡交易時間之結果，進行一機多卡整合模式對於捷運出口閘門等候時間之影響評估。經實際觀察台北捷運新埔站及台北車站乘客候車情形，在四種一機多卡交易模式下(一卡~四卡)新埔站及台北車站等候時間之分析。

根據分析結果，兩個車站的二卡交易等候時間均較一卡交易些微增加，對於乘客而言等候時間仍屬合理範圍。但是三卡及四卡交易的等候時間則大幅增加，三卡或四卡交易所造成的等候時間與一卡或二卡交易比較則呈現倍數增加關係，各種等候狀況比較如表 3-1。

表 3-1 一卡、二卡、三卡與四卡交易之等候狀況比較

		一卡交易	二卡交易	三卡交易	四卡交易
新埔站	平均等候時間(秒)	4.55	6.50	9.48	13.87
	最長等候時間(秒)	8.04	11.60	16.78	24.27
	平均排隊人數	4.0	5.7	8.3	12.2
	最大排隊人數	7.1	10.2	14.8	21.4
台北車站	平均等候時間(秒)	3.61	4.77	9.63	18.49
	最長等候時間(秒)	6.69	9.79	18.18	31.27
	平均排隊人數	3.2	4.2	8.5	16.3
	最大排隊人數	5.9	8.6	16.0	27.5

將表 3-1 新埔站及台北車站「平均等候時間(秒)」繪製成長條圖，如圖 3-1，台北車站二卡交易時平均等候時間比一卡交易增加 32%(二卡交易時間(4.77 秒)：一卡交易時間(3.61 秒)=1.32 : 1)、新埔車站增加 43%(二卡交易時間(6.50 秒)：一卡交易時間(4.55 秒)=1.43 : 1)；台北車站三卡交易平均等候時間比一卡交易增加 167%(三卡交易時間(9.63 秒)：一卡交易時間(3.61 秒)=2.67 : 1)、新埔車站增加 108%(三卡交易時間(9.48 秒)：一卡交易時間(4.55 秒)=2.08 : 1)；台北車站四卡交易平均等候時間比一卡交易增加 412%(四卡交易時間(18.49 秒)：一卡交易時間(3.61 秒)=5.12 : 1)、新埔車站增加 205%(四卡交易時間(13.87 秒)：一卡交易時間(4.55 秒)=3.05 : 1)。

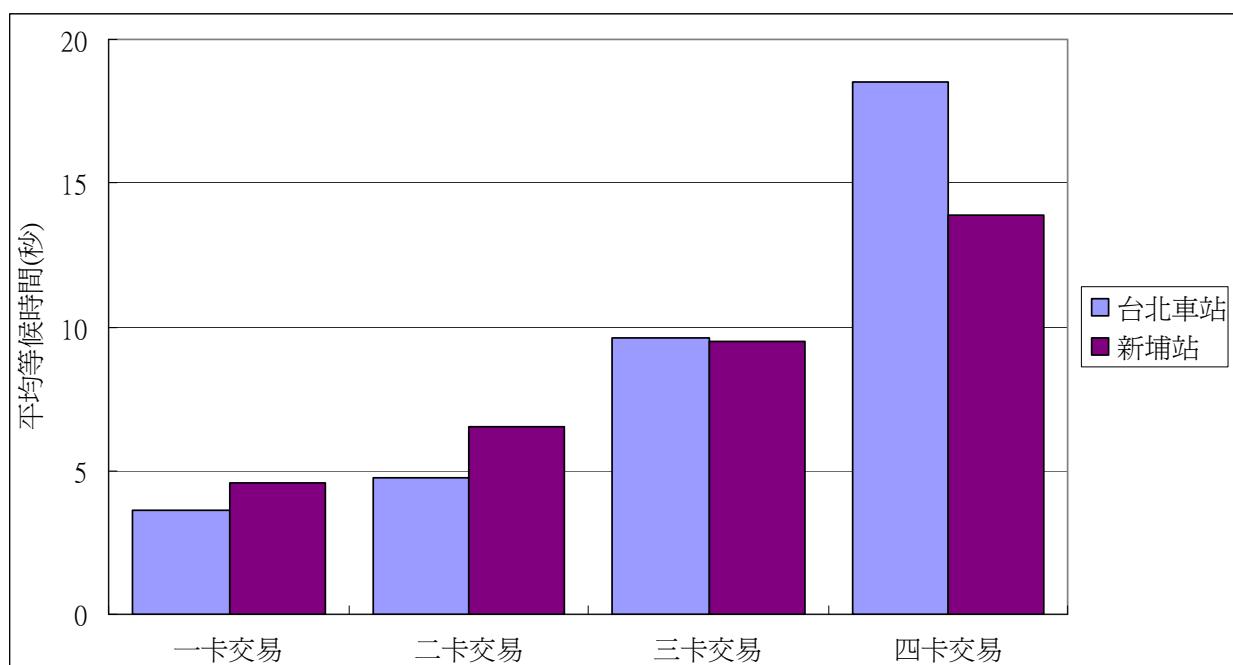


圖 3-1 多卡交易平均等候時間之比較

將表 3-1 新埔站及台北車站「最長等候時間(秒)」繪製成長條圖，如圖 3-2，台北車站二卡交易時最長等候時間比一卡交易增加 46%(二卡交易時間(9.79 秒)：一卡交易時間(6.69 秒)=1.46：1)、新埔車站增加 44%(二卡交易時間(11.60 秒)：一卡交易時間(8.04 秒)=1.44：1)；台北車站三卡交易最長等候時間比一卡交易增加 172%(三卡交易時間(18.18 秒)：一卡交易時間(6.69 秒)=2.72：1)、新埔車站增加 109%(三卡交易時間(16.78 秒)：一卡交易時間(8.04 秒)=2.09：1)；台北車站四卡交易最長等候時間比一卡交易增加 367%(四卡交易時間(31.27 秒)：一卡交易時間(6.69 秒)=4.67：1)、新埔車站增加 202%(四卡交易時間 24.27 秒)：一卡交易時間(8.04 秒)=3.02：1)。

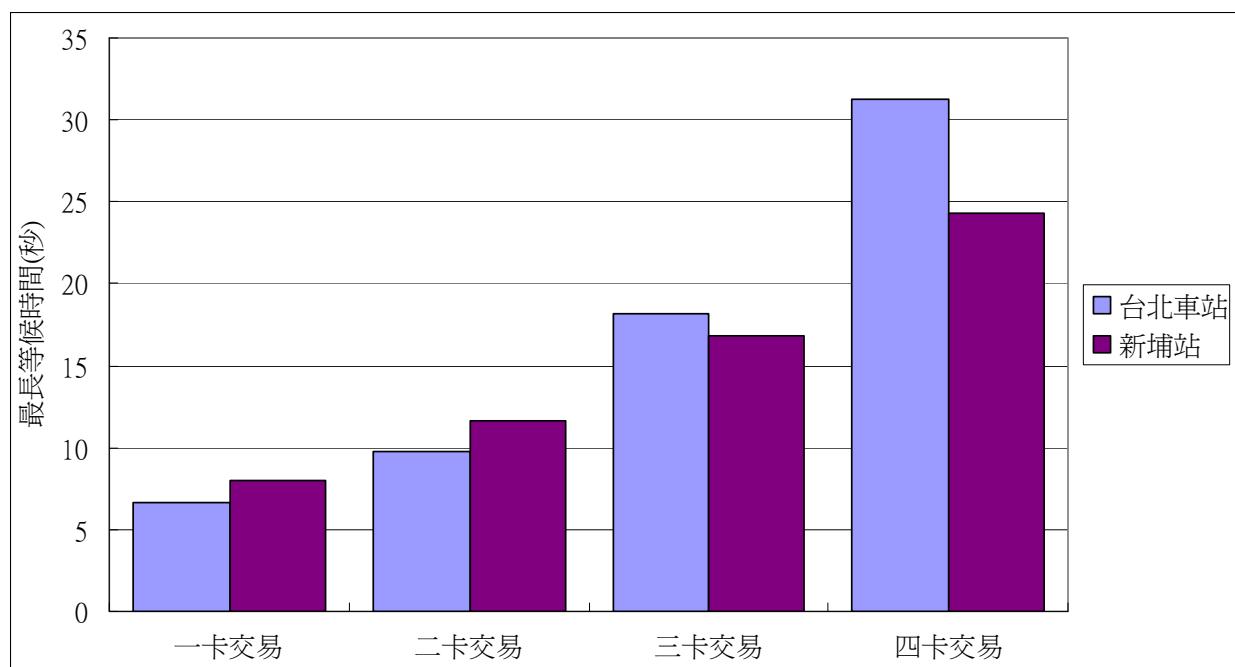


圖 3-2 多卡交易最長等候時間之比較

將表 3-1 新埔站及台北車站「平均排隊人數」繪製成長條圖，如圖 3-3，台北車站二卡交易時平均排隊人數比一卡交易增加 31%(二卡排隊人數(4.2 人)：一卡排隊人數(3.2 人)=1.31：1)、新埔車站增加 43%(二卡排隊人數(5.7 人)：一卡排隊人數(4.0 人)=1.43：1)；台北車站三卡交易平均排隊人數比一卡交易增加 166%(三卡排隊人數(8.5 人)：一卡排隊人數(3.2 人)=2.66：1)、新埔車站增加 107%(三卡排隊人數(8.3 人)：一卡排隊人數(4.0 人)=2.07：1)；台北車站四卡交易平均排隊人數比一卡交易增加 409%(四卡排隊人數(16.3 人)：一卡排隊人數(3.2 人)=5.09：1)、新埔車站增加 205%(四卡排隊人數(12.2 人)：一卡排隊人數(4.0 人)=3.05：1)。

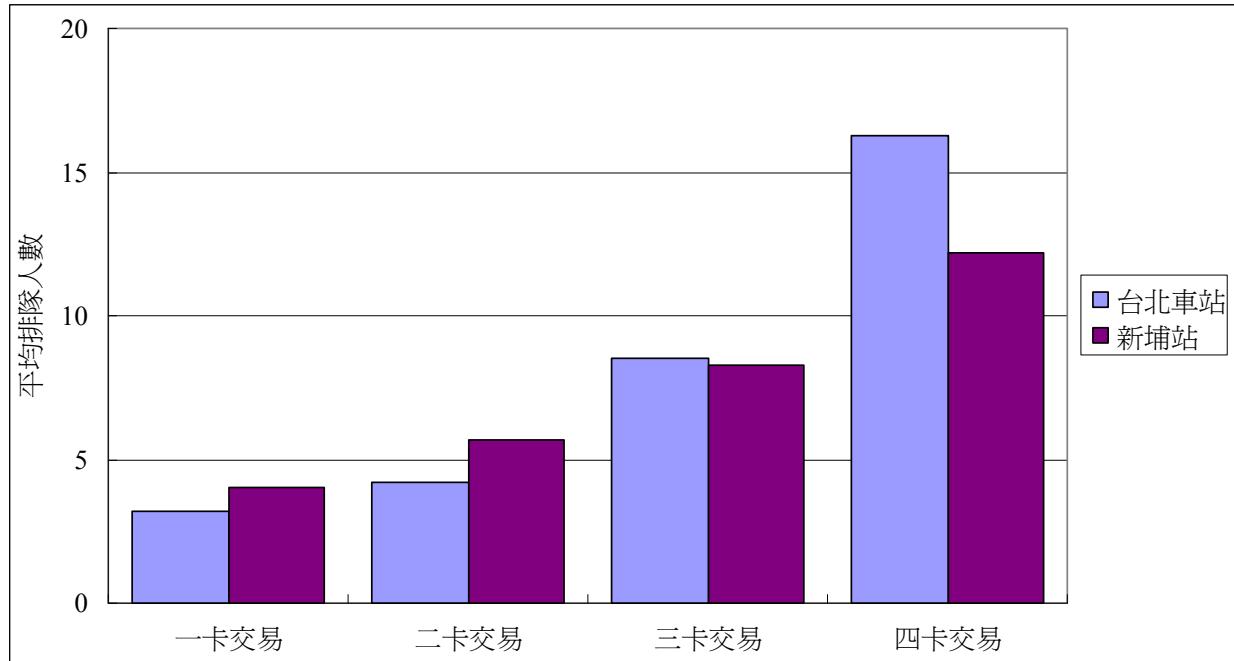


圖 3-3 多卡交易平均排隊人數之比較

將表 3-1 新埔站及台北車站「最大排隊人數」繪製成長條圖，如圖 3-4，台北車站二卡交易時最大排隊人數比一卡交易增加 46%(二卡排隊人數(8.6 人)：一卡排隊人數(5.9 人)=1.46：1)、新埔車站增加 44%(二卡排隊人數(10.2 人)：一卡排隊人數(7.1 人)=1.44：1)；台北車站三卡交易最大排隊人數比一卡交易增加 171%(三卡排隊人數(16.0 人)：一卡排隊人數(5.9 人)=2.71：1)、新埔車站增加 108%(三卡排隊人數(14.8 人)：一卡排隊人數(7.1 人)=2.08：1)；台北車站四卡交易最大排隊人數比一卡交易增加 366%(四卡排隊人數(27.5 人)：一卡排隊人數(5.9 人)=4.66：1)、新埔車站增加 201%(四卡排隊人數(21.4 人)：一卡排隊人數(7.1 人)=3.01：1)。

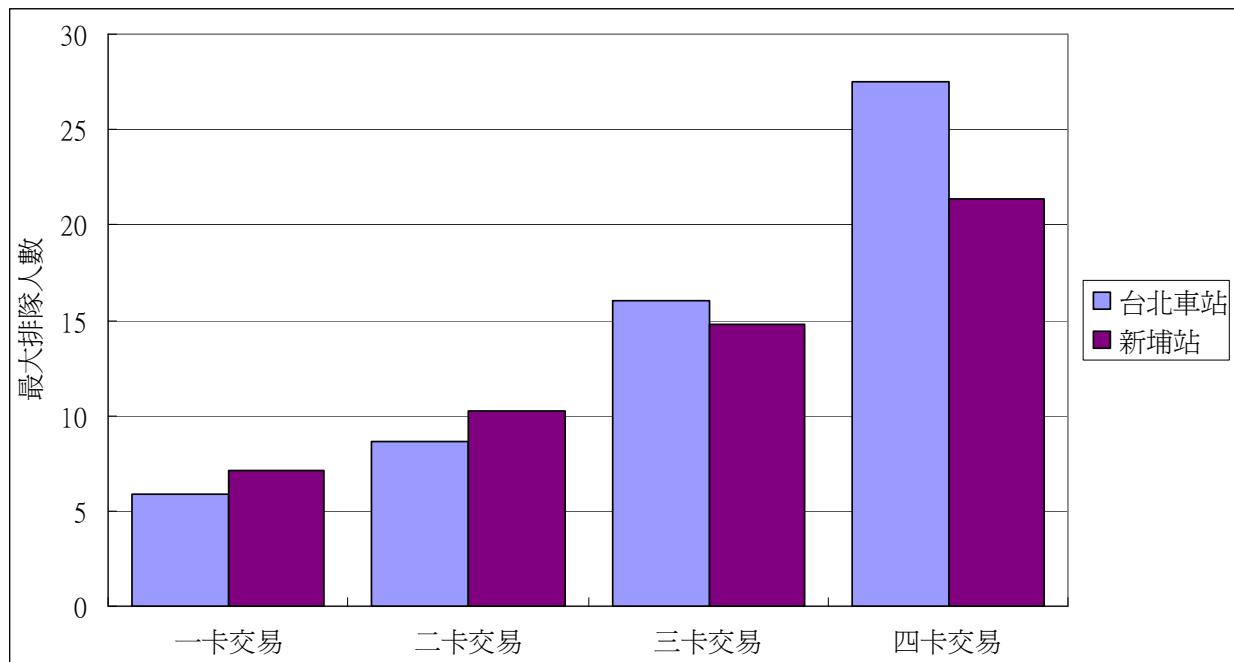


圖 3-4 多卡交易最大排隊人數之比較

由於多卡整合對民眾使用電子票證搭乘大眾運輸系統具有相當大的便利性及誘因，基於大眾運輸系統對電子票證多卡整合的需要，本研究將探討「一機多卡驗票機」整合可能衍生的問題及因應對策，期能供日後相關單位參考。

3.2 一機多卡整合模式整體架構分析

本研究前期採用「輪詢法」方式進行測試，主要參考當時各國票證之作法與卡片原廠技術建議，且當時研究前提為在各票證業者既有設備變更最少之前提下，進行票證整合之研究，而「輪詢法」可以於既存設備進行開發，不涉及設備全面更新，是當時較為可行之研究方向。目前已有廠商號稱以「同詢法」開發平行驗證技術並發表成果，若有政府政策之支持，例如驗票機設備可全面更新，「同詢法」技術也是票證整合之方向之一。目前交通部推動之策略採用同詢法之概念，故可突破多卡整合運算時間延長之障礙限制。因此，對此一議題測試方法選擇之不同，其原因在於假設基礎不同與票證技術發展而異。

惟除運算時間長短問題，一機多卡整合仍會涉及交易主體改變、交易邏輯衝突與交易權責重新定位等課題，後續本研究將針對一機多卡整合模式對於電子票證產業及相關權益關係人的影響分別進行深入分析，並提出對應策略建議。

本研究應用層級分析法將電子票證產業分為內容層、傳輸層、操作層、終端層及包裝層等五個產業。其中內容層、傳輸層、操作層是構成電子票證應用項目的核心產業；持卡人必須透過終端層產業來使用電子票證；整合上述產業

者稱為包裝層，這五種產業層級之間及與周邊系統的關係如圖 3-5。

一、內容層

提供電子票證各種應用項目的產業，例如：運輸、政府、教育、零售、旅遊等，這些產業運用本身的基礎建設可以提供特定服務給特定對象，所以電子票證應用項目的提供者可以來自不同的產業以提供不同的服務。

二、傳輸層

電子票證應用項目提供者的基礎建設為傳輸層，如運輸業已建立車隊、零售業已建置銷售通路等。當某一企業或產業要加入電子票證應用項目或自行發卡時，首先要考慮的就是本身的基礎建設網路是否健全、綿密，否則無法建立足夠的持卡人規模經濟及網路效應。例如客運業若班車不夠密集，即使發行電子票證也不會增加乘客數量。

三、操作層

電子票證的卡片作業系統、卡片規格、資料處理中心的軟硬體等定義為操作層。作業系統構建所有電子票證的應用項目及安全機制，透過晶片內元件(如 ROM、EEPROM)執行資料儲存、運算、驗證、加密、識別等功能。建置卡片作業系統時必須考慮相容性及標準化，這牽涉到未來電子票證功能的擴充、整合及升級。

四、終端層

持卡人與電子票證應用項目平台溝通的工具定義為終端層。終端層與傳輸層的關係密不可分，因為終端設備是建構在傳輸層上，例如持卡人透過車上驗票機支付電子票證、透過零售通路的 POS 支付小額消費等。電子票證終端層的種類將隨著科技的進步而多樣化，持卡人也因此更容易接受電子票證，故建置可以方便使用的終端層是電子票證快速發展的要素之一。

五、包裝層

系統整合者為包裝層。電子票證的包裝層就是發卡組織，該組織通常也是應用項目提供者，而且本身已經有相當完整的傳輸層，它可以結合其他功能的提供者，共同建置開放式的電子票證應用項目平台，例如運輸業結合金融業共同發行電子票證金融儲值卡及信用卡；也可以自行建構封閉式的電子票證，例如某運輸業者發行定期 IC 卡，限定持卡人於一定期間內持卡消費等。

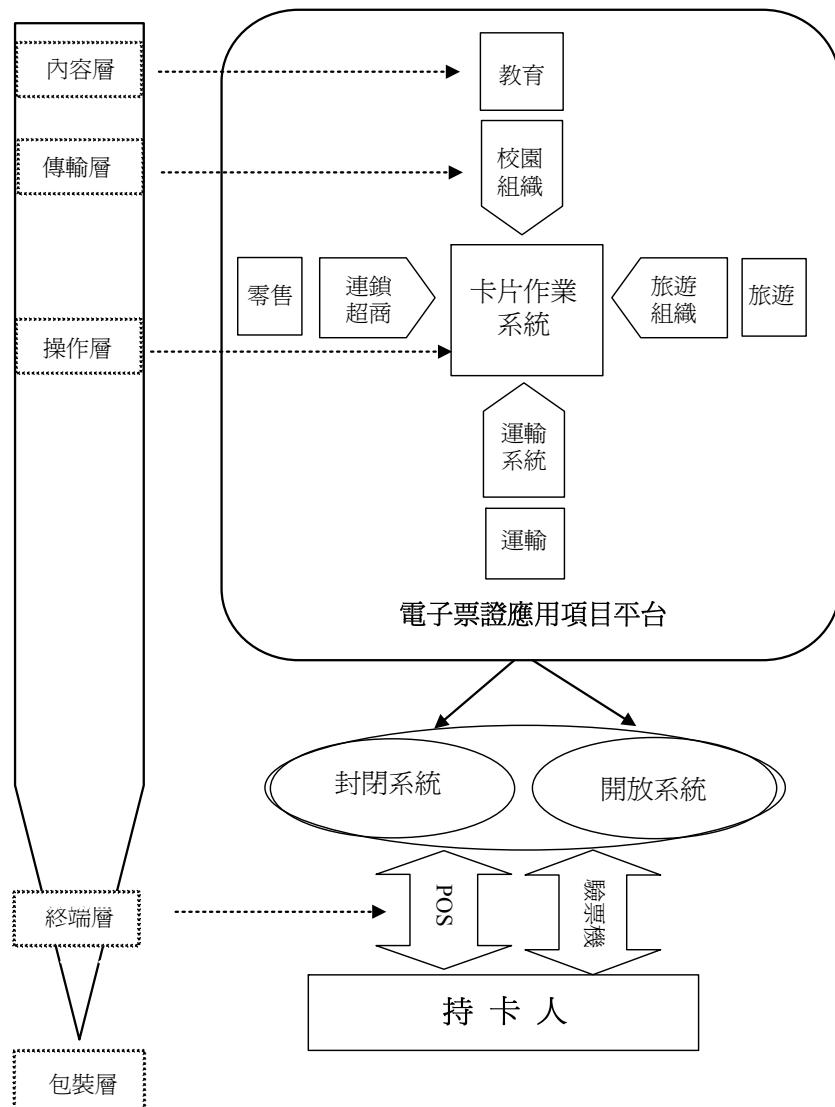


圖 3-5 電子票證產業結構圖

電子票證應用項目平台的核心產業則由三個部門共同協力完成，包括政府部門、軟硬體系統及設備建置商、相關使用業者等。三個部門相輔相成，彼此分工完成電子票證應用項目平台所須要的卡片功能，如運用於交通運輸系統的電子票證、小額消費的電子錢包、與旅遊業聯合促銷的旅遊卡、提供校園服務的校園卡以及某些運輸業者封閉系統使用的定期卡等。

此電子票證應用項目平台能提供持卡人安全便利的付款機制、建立經營客戶關係(CRM)所須的忠誠獎勵機制、收集持卡人消費行為的資料庫、彙整使用業者建立 MIS 所需的原始資料等功能。

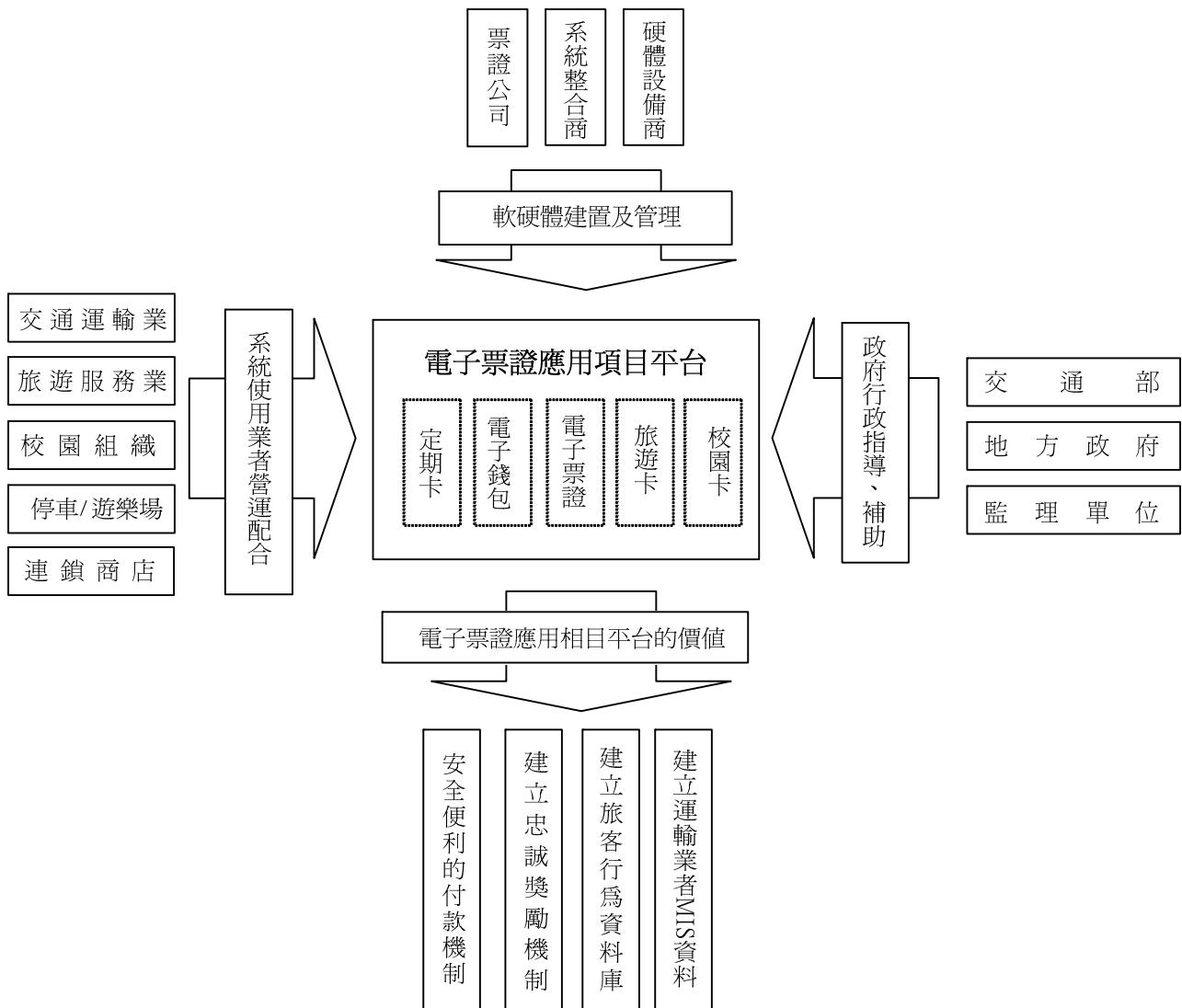


圖 3-6 電子票證應用項目平台各權益關係人的關係

上述電子票證應用項目平台的達成係由三個部門所構成，各方的關係緊密連結，任何一方的改變皆會影響其他方，故彼此互為權益關係人，各方的關係如圖 3-6，各權益關係人的主要功能與分工如下：

一、政府部門：

包括中央政府交通部、地方政府及公路監理單位。交通部負責國家交通整體發展政策的擬定；地方政府及公路監理單位則依照其職權遵照交通部既定政策對轄區內交通運輸業者進行監管、編列補助預算、執行及成效列管等。

二、軟硬體建置者：

包括票證業者、系統整合商及硬體設備供應商等。

票證業者為發卡單位，負責電子票證的發卡、清算、營運及管理；系

統整合商則配合系統使用業者的營運需求，將所購置的前端設備與票證業者的後台系統進行整合及測試；硬體設備供應商則依照系統使用業者的需求研發、生產低成本、實用的硬體設備，並提供日後快速修護服務。

三、系統使用業者：

包括交通運輸業者、旅遊服務業、校園組織、停車/遊樂場、連鎖商店等。該些使用業者皆安裝驗票機供持卡人消費扣款，並每日與票證業者進行清算對帳，並接受票證業者所訂定的票證營運規則。

由以上的產業分析，本研究認為電子票證產業的權益關係人，包括政府部門、軟硬體建置者的票證業者、系統整合商及硬體設備供應商、系統使用業者、持卡人等。

當電子票證產業發生重大政策的改變、票證技術的創新突破、營運規範的巨變等，都將對產業內各權益關係人產生各種不同程度的影響。

以一機多卡驗票機整合模式而言，應分析票證整合對各種因素的影響，包括營運邏輯類、應用代碼類、資安控管類、設定環境類、清分作業類、優惠補助類等六類影響分析，以下分別依據各類說明如下：

一、營運邏輯類

1. 一般扣款基本差異：票證業者針對不同營運區域的運輸業者均有其客制化的營運邏輯。
2. 交易紀錄格式差異：電子票證之交易資料需要上傳到後台清分系統，因為各票證業者間未達成交易檔格式相同或相容的共識，故一機多卡交易模式所產生之交易檔格式、記錄方式與檔案位置等均未統一。
3. 轉乘優惠條件差異：各票證業者因為區域的營運條件不同，對於轉乘優惠的營運邏輯也有所差異。
4. 特殊作業的差異：各運輸業者對於解除逃票作業、路故上下作業、機故上下作業、票卡代墊額度作法等均不相同。

二、應用代碼類：各家票證業者在票卡資料格式與營運邏輯相關欄位中，路線代碼、業者代碼、載具代碼、司機代碼等均未統一，增加資訊交換的困擾。

三、資安控管類：電子票證發行管理條例通過後，悠遊卡對於資安規範、讀寫模組驗證、SAM 卡控管作業、SAM 錄押碼作業等均依照金管會之要求與

規範執行，但是其它交通電子票證業者並未具備相同之規範等級，此為電子票證整合過程中必須突破的重要議題。

四、設定環境類：環境設定主要面臨時區定義差異及設備參數差異等議題。前者指各家票證業者對於時區定義的不同，在特殊狀況下對交易檔之資訊內容會造成差異；後者指各家票證業者對於設備參數之欄位與定義各自不同，會造成系統整合時參數不一致的問題。

五、清分作業類：各家票證業者的清分清算作業差異頗大，尤其是在卡種類別差異、扣點扣錢規範差異、營運求償機制差異、優惠補助類等各有其特殊的作業方式。

六、優惠補助類：為鼓勵公共運輸與實施社會福利政策，各地方政府往往會特定持卡人提供相關優惠與補助，然而因為持卡人持有不同票證業者之卡片，在一機多卡整合模式中可能造成優惠無法同步整合的情況，說明如下：

1. 補助單位差異：各家票證業者雖都可發行優惠記名卡，但是各補助單位對資訊內容的需求不同，因此，不同報表之產製將增加運輸業者請款作業的複雜度。
2. 優惠記名卡優惠差異：各家票證業者雖都可發行敬老卡，但是各縣市優惠上限不同，扣點或扣錢之規定與額度也不同，一來造成駕駛判斷扣款的難度，二來民眾也會對於同車之不同持卡者的優惠差異而產生認知上的落差。

本研究針對影響一機多卡整合的因素，除歸納為六大類型之外，也依據影響類型的屬性分別歸屬不同權益關係人，包括票證業者營運、運輸業者、系統服務廠商與持卡者使用認知等，三者的關係彙整如表 3-2。

本研究認為，一機多卡整合模式雖然可以透過票證技術達到多卡整合的目的，但仍然無法避免不同票證業者在票證資料格式與營運邏輯等商業技術上整合的困難。

表 3-2 一機多卡整合模式商業技術之影響因素、所屬類型與權益關係人的關聯性

影響因素的 類型 影響因素 權益關係人	營運邏輯類 應用代碼類	資安控管類 清分作業類	設定環境類 優惠補助類		
				資料來源	影響程度
票證業者營運	<ul style="list-style-type: none"> ◆ 特殊作業：票卡代墊額度作法 ◆ 路線代碼 ◆ 業者代碼 ◆ 載具代碼 ◆ 司機代碼 	<ul style="list-style-type: none"> ◆ 讀寫模組(讀卡機Module)驗證 ◆ SAM錄碼作業及押碼作業 	<ul style="list-style-type: none"> ◆ 時區定義差異 ◆ 設備參數差異 	<ul style="list-style-type: none"> ◆ 卡種類別差異 ◆ 扣點扣錢規範差異 ◆ 营運求償機制差異 	<ul style="list-style-type: none"> ◆ 補助單位差異 ◆ 優惠記名卡優惠差異
系統服務廠商	<ul style="list-style-type: none"> ◆ 交易紀錄格式差異 	<ul style="list-style-type: none"> ◆ 讀寫模組(讀卡機Module)驗證 ◆ SAM錄碼作業及押碼作業 	<ul style="list-style-type: none"> ◆ 時區定義差異 ◆ 設備參數差異 	<ul style="list-style-type: none"> ◆ 時區定義差異 ◆ 設備參數差異 	<ul style="list-style-type: none"> ◆ 補助單位差異 ◆ 扣點扣錢規範差異 ◆ 营運求償機制差異
運輸業者	<ul style="list-style-type: none"> ◆ 一般扣款基本差異 ◆ 轉乘優惠條件差異 ◆ 特殊作業：解逃票作業差異（特許上下） 	<ul style="list-style-type: none"> ◆ 路線代碼 ◆ 業者代碼 ◆ 載具代碼 ◆ 司機代碼 			<ul style="list-style-type: none"> ◆ 補助單位差異 ◆ 優惠記名卡優惠差異

表 3-2 一機多卡整合模式商業技術之影響因素、所屬類型與權益關係人的關聯性(續)

影響因素 的 類型 及 關 係 人	營運邏輯類	應用代碼類	資安控管類	設定環境類	清分作業類	優惠補助類
持卡者使用認知	<ul style="list-style-type: none"> ◆ 轉乘優惠條件差異 ◆ 特殊作業：解逃票作業差異(特許上下) ◆ 特殊作業：路故障上、路故障下作業 ◆ 特殊作業：機故障上、機故障下作業 ◆ 特殊作業：票卡代墊額度作法 	<ul style="list-style-type: none"> ◆ 轉乘優惠條件差異 ◆ 特殊作業：解逃票作業差異(特許上下) ◆ 特殊作業：路故障上、路故障下作業 ◆ 特殊作業：機故障上、機故障下作業 ◆ 特殊作業：票卡代墊額度作法 	<ul style="list-style-type: none"> --- --- --- --- --- 	<ul style="list-style-type: none"> ◆ 卡種類別差異 ◆ 扣點扣錢規範差異 	<ul style="list-style-type: none"> --- --- --- --- --- 	<ul style="list-style-type: none"> --- --- --- --- ---

3.3 一機多卡對交易時間之影響及票證技術解決實例

3.3.1 改善一機多卡交易速度之學理分析

依據本研究第三期期末報告第三章「設備整合多卡交易速度之測試與影響評估」的分析，影響一機多卡交易速度之主要原因，乃在於判斷處理中的卡片到底屬於那一家票證業者。其主要原因如下：

一、國內電子票證皆採用 MIFARE Classic 1K 卡或是其相容卡片，讀卡機無法於卡片接觸的第一時間判斷出卡片的歸屬。

目前國內電子票證產業(除了 TaiwanMoney 以外)，皆使用 MIFARE Classic 1K 卡或是其相容卡片，這將導致非接觸式讀卡機無法於卡片接觸的第一時間判斷出卡片的發行單位，而必須讀出卡片中受金鑰保護的 S0 區段後才能進行判讀；若卡片分屬不同種類，例如：高捷一卡通以及 TaiwanMoney，即可於卡片接觸驗票機的第一時間依照卡片的種類即時判讀卡種，因此二者在驗票機判讀時不會產生速度的延遲。

二、各家票證業者皆有屬於自己的金鑰管理系統，故各張卡片之金鑰皆不相同，其主金鑰以及金鑰衍生演算法也完全不相同。

驗票機欲判讀 MIFARE 卡片內所儲存的資料必須先通過金鑰驗證，依照各家票證業者對於 MIFARE 卡片金鑰管理機制的作法，每一張屬於該票證業者的 MIFARE 卡片，皆必須擁有專屬的金鑰組來設定該張卡片的存取權限。而每一張卡片的金鑰組由該票證業者存放於 SAM 卡中的母金鑰組及每家業者自行定義之金鑰衍生驗算法(同樣放置於 SAM 卡中)，搭配每一張 MIFARE 卡片的唯一序號，以及票證業者自行定義的卡片參數等進行演算，便可取得每一張卡片各自獨立的存取金鑰組。

因為每一家票證業者皆有屬於自己的 SAM 卡、母金鑰組以及驗算邏輯，想要存取該家票證業者的卡片，必須透過該家業者所提供之 SAM 卡才可取出讀取該張卡片所需之衍生金鑰以存取卡片資料。因此，為了判斷出 MIFARE 卡片到底是由哪一家票證業者所發行，傳統作法驗票機便必須採用試誤法對卡片逐一判讀，因而造成交易速度變慢。因此，當同一台驗票機插入的 SAM 卡變多，對於排序在後的 SAM 卡，其所需的交易時間也相對的變長。

三、卡片歸屬判斷迴圈最佔時間的處理乃在於卡片的金鑰衍生作業。

卡片歸屬之判讀程序如圖 3-7 所示，由流程圖可以看出，判斷卡片歸屬之迴圈(衍生金鑰→驗證金鑰→票卡重置)會對於排序在後的 SAM 卡所需的交易時間造成延遲，就流程探討縮短此一迴圈一次所需要花費的時間，便可找到解決一機多卡交易速度緩慢的方案。要達成此一目標有兩種作法：【作法一：最佳化「判斷卡片歸屬」流程(仍採用「輪詢法」)】；【作法二：多卡平行驗證(即所謂「同詢法」)】。

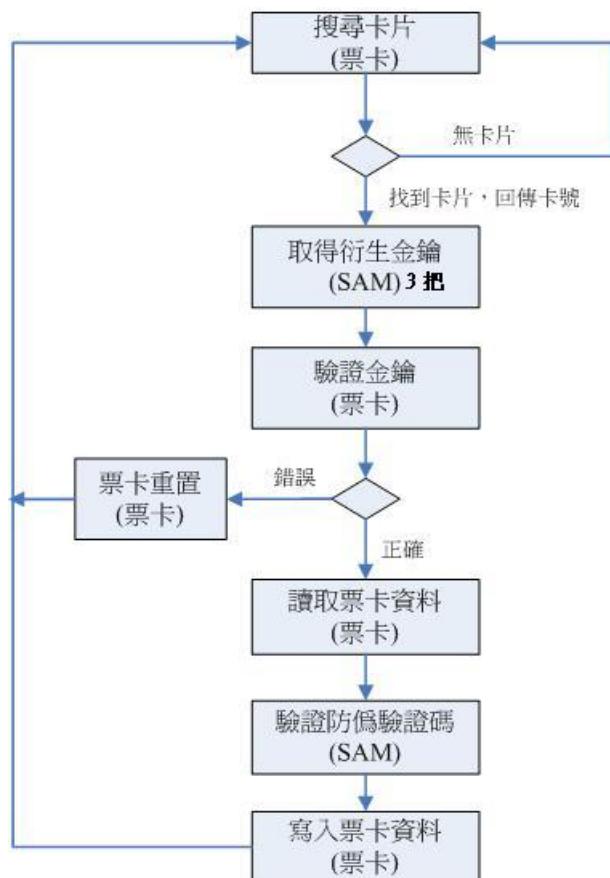


圖 3-7 一機多卡驗票機之交易流程(本研究)

依照本研究案第三期實作成果，其各流程方塊所需花費的時間，粗估統計如下表：

表 3-3 多卡交易測試主要階段所需時間

主要階段	平均所需時間(sec)
取得三把衍生金鑰	0.249
驗證金鑰	0.074
票卡重置	0.083

因此，若將取得三把衍生金鑰變成只取一把，其它兩把金鑰於判斷出卡片

歸屬後再進行取出的動作，如此，將可該處理流程縮短為約接近 0.1 秒左右。此外，對於「驗證金鑰以及票卡重置」此二階段而言，若將硬體效能提升，則可將此階段的交易時間大幅縮短。

3.3.2 改善一機多卡交易速度之實例

本研究調查目前設備業者對一機多卡交易速度改善之作法，可分為兩種，說明如下：

【作法一：富譽公司最佳化「判斷卡片歸屬」流程(採用「輪詢法」)】

此作法主要是提升讀卡機 CPU 處理的能力，並加快所有通訊介面的通訊速度，驗票機在「取得衍生金鑰」及「驗證金鑰」之程序採用「輪詢法」的基本原理，但是其應用了下列票證優化技術，使得該公司研發驗票機的完成交易時間不會隨 SAM 卡數量增加而遞增：

1. 微控制器(Micro-controller Unit, MCU)採用 32bit MIPS Microprocessor，運算效率高。
2. 以虹堡科技 TS1000 讀卡機所提供的開發工具，撰寫多卡輪詢與卡片讀寫應用程式，所以卡片取得衍生金鑰與驗證金鑰之程序，皆在 Rader Module 中處理完成，不需浪費時間與驗票機應用軟體溝通。
3. 將讀卡機 Module 內所開發之卡片驗證與讀寫應用軟體作最佳的優化。
4. SAM 卡與 MCU 之通訊速率可達 115200bps，執行效率高。
5. 驗票機已先規劃好那些票證業者的 SAM 卡要放在那一個 SAM SLOT，於本例中，SA 邏輯加密卡放在第一個 SAM SLOT，SAM2 放在第二個 SAM SLOT，SAM3 放在第三個 SAM SLOT。
6. 驗票機已預設依照各票證業者 SAM 卡的特性，可最快取得卡片 S0 金鑰的 SAM 卡會優先處理，本例中 SAM3 取得 S0 的速度最快，其次是 SAM2，最慢的是 SA 邏輯加密卡，因為該 SAM 卡有其獨特的驗證流程，故時間包括取得卡片 S0 金鑰驗證與資料回傳兩部份，本例中 SA 邏輯加密卡被預設為最後處理的 SAM 卡。

富譽公司並以現行桃竹苗地區公路客運所使用之電子票證驗票機進行實機測試，測試驗票機規格如表 3-4，測試的步驟如下說明：

表 3-4 富譽公司進行一機多卡交易測試之驗票機規格

項次	設備屬性	項目	規格
1	桃竹苗驗票機	CPU	ARM7 50MHZ
2		RAM	8MB
3		FLASH ROM	8MB
4	更換桃竹苗驗票機讀卡機	讀卡機	虹堡科技TS-1000
5	通訊	驗票機與讀卡機傳輸介面	RS232 BAUD RATE 57600

當驗票機啟動同時 TS1000 讀卡機亦自動啟動，並與驗票機端電子票證應用軟體互相溝通，其交易流程如下：

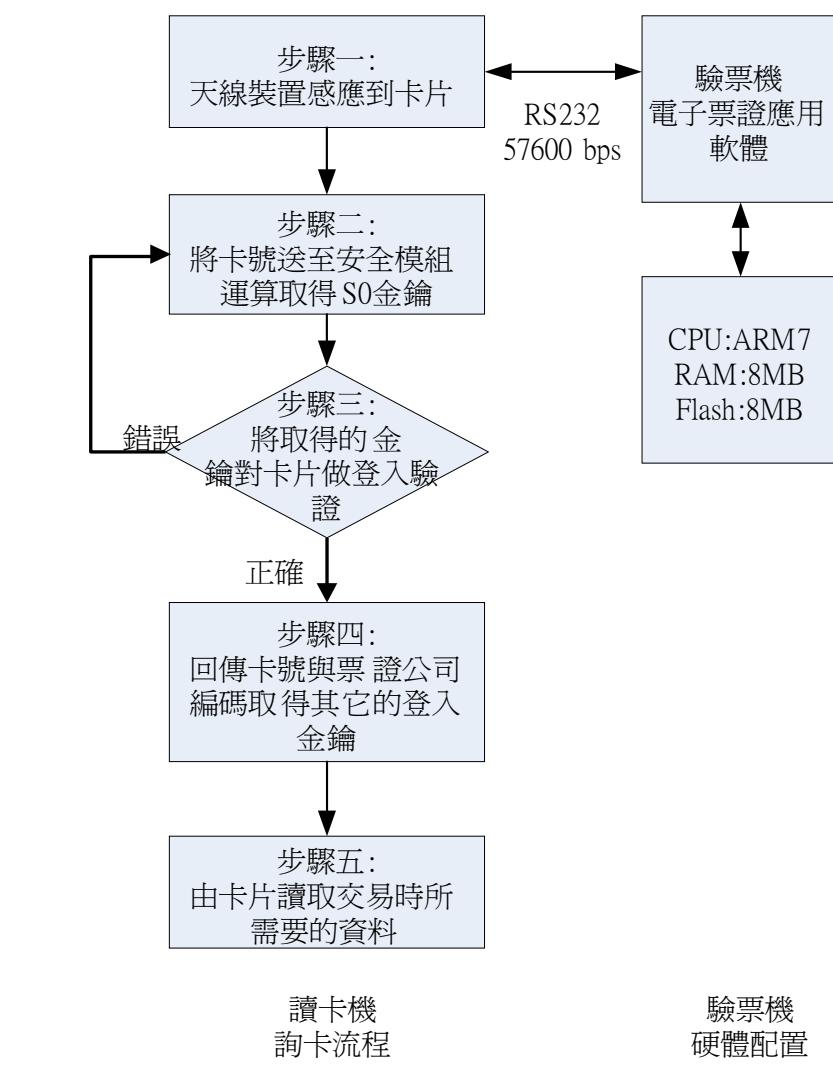


圖 3-8 富譽公司最佳化「判斷卡片歸屬」流程(本研究)

步驟一：TS1000 讀卡機自動偵測天線是否有卡片進入信號。

步驟二：當有偵測到卡片信號時，取出卡片 S0B0 卡片號碼，以 S0B0 卡片序號送給可最快取得卡片 S0 金鑰的 SAM 卡，取得 S0 login Key。

步驟三：以 S0 login Key 驗證卡片 S0 判讀是否成功；若不成功，則回到步驟二，將 S0B0 卡片序號送到次快取得卡片 S0 金鑰的 SAM 卡，以此類推。若都不成功，則通知驗票機非有效卡片並顯示於 LCD，發出語音通知使用者。

步驟四：可被 SAM 卡成功判讀 S0 的卡片則自動將卡片序號送到對應之 SAM 卡，取得所屬票證業者的編碼傳送給讀卡機，並再取出後續交易所需之 Sector login Key，由驗票機應用軟體下達指令要求讀卡機將卡片資料送出。

步驟五：驗票機取得卡片資料後，進行各項交易金鑰驗證流程，以完成整筆交易。

以下為富譽公司所提供之測試資料。驗票機分別裝置 SA 邏輯加密卡、SAM2 及 SAM3 三種測試用的 SAM 卡，三種 SAM 卡的規格及各種情境測試結果如表 3-5~7。

表 3-5 為富譽公司於驗票機 SAM SLOT 1 中僅安裝 SA 邏輯加密卡的 SAM 卡，該 SAM 卡取得卡片 S0 金鑰驗證與資料回傳的時間為 0.3 秒，完成整筆交易的時間為 0.593 秒。

表 3-5 富譽公司一機多卡驗票機實機測試結果【單一 SAM 卡】

SAM SLOT 位置	1
SAM 卡	SA 邏輯加密卡
JAVA CARD 廠牌	GemPlus T=1
取得卡片 S0 驗證與 資料回傳時間	0.3秒
Baud Rates	9600 bps~115200 bps
讀取票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫(API，Application Programming Interface)讀取票卡資料
寫入票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫(API，Application Programming Interface)讀取票卡資料
上車完整交易時間	0.593秒(包含取得卡片 S0 驗證與資料回傳時間，以下皆同)
下車完整交易時間	0.593秒(包含取得卡片 S0 驗證與資料回傳時間，以下皆同)

表 3-6 為加裝第二張 SAM 卡 SAM2 的交易時間，依照富譽公司票證優化技術第 6 點，驗票機優先處理可最快取得卡片 S0 金鑰的 SAM 卡，因 SAM2 取得 S0 金鑰的時間為 0.07 秒，小於 SA 邏輯加密卡的 0.3 秒，故當驗票機偵測到卡片信號時，取出卡片 S0B0 卡片序號先送到 SAM2，若可成功取得 S0 login Key，則完成整筆交易的時間為 0.580 秒；若失敗，再試 SA 邏輯加密卡，若可成功取得 S0 login Key，則完成整筆交易的時間為 0.621 秒。

表 3-6 富譽公司一機多卡驗票機實機測試結果【加入第二張 SAM 卡】

論詢順序	2	1
SAM SLOT 位置	1	2
SAM 卡	SA 邏輯加密卡	SAM2
JAVA CARD 廠牌	GemPlus T=1	Gemalto TOP_IS GX4 (GX4 36K Java Card) T=1
取得卡片 S0 金鑰驗證與資料回傳時間	0.3 秒	--
取得 S0 金鑰時間	--	0.07 秒
Baud Rates	9600 bps~115200 bps	9600~115200 bps
讀取票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API, Application Programming Interface) 讀取票卡資料	Value: S2、S7 Data:S1 B0、S1B1、S3、S6、S10 B0 S1~S5 以交二版標準欄位規劃
寫入票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API, Application Programming Interface) 讀取票卡資料	Value:S2 或 S7 Data:S3 B0 、 S3B1 或 S3B2、S4或S5、S6 B0、S6B2 S1~S5 以交二版標準欄位規劃
上車完整交易時間	0.621秒	0.580秒(包括取得取得 S0 金鑰時間，以下皆同)
下車完整交易時間	0.621秒	0.580秒(包括取得取得 S0 金鑰時間，以下皆同)

資料來源：富譽公司提供

表 3-7 為加裝第三張 SAM 卡 SAM3 的交易時間，因 SAM3 取得 S0 金鑰的時間為 0.04 秒，小於 SAM2 及 SA 邏輯加密卡，故當驗票機偵測到卡片信號時，取出卡片 S0B0 卡片序號先送到 SAM3，若可成功取得 S0 login Key，則完成整筆交易的時間為 0.450 秒；若失敗，則試 SAM2，若可成功

取得 S0 login Key，則完成整筆交易的時間為 0.620 秒；若失敗，再試 SA 邏輯加密卡，若可成功取得 S0 login Key，則完成整筆交易的時間為 0.661 秒。

表 3-7 富譽公司一機多卡驗票機實機測試結果【加入第三張 SAM 卡】

論詢順序	3	2	1
SAM SLOT 位置	1	2	3
SAM 卡	SA邏輯加密卡	SAM2	SAM3
JAVA CARD 廠牌	GemPlus T=1	Gemalto TOP_IS GX4 (GX4 36K Java Card) T=1	OCS V7.0 T=1 ISO7816-3 T=1/0
取得卡片 S0 金鑰驗證與資料回傳時間	0.3 秒	--	--
取得 S0 金鑰時間	--	0.07 秒	0.04 秒
Baud Rates	9600 bps~115200 bps	9600~115200 bps	9600~614400bps
讀取票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API，Application Programming Interface) 讀取票卡資料	Value: S2、S7 Data:S1 B0、S1B1、S3、S6、S10 B0 S1~S5 以交二版標準欄位規劃	Value: S2 Data:S1B0、S1B1、S3 S1~S5 以交二版標準欄位規劃
寫入票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API，Application Programming Interface) 讀取票卡資料	Value:S2 或 S7 Data:S3 B0、S3B1或 S3B2、S4或 S5、S6 B0、S6B2 S1~S5 以交二版標準欄位規劃	Value:S2 Data:S3 B0, S3 B1 或 S3B2、S4 或 S5 S1~S5 以交二版標準欄位規劃
上車完整交易時間	0.661秒	0.620秒	0.450秒(包括取得取得 S0 金鑰時間)
下車完整交易時間	0.661秒	0.620秒	0.450秒(包括取得取得 S0 金鑰時間)

資料來源：富譽公司提供

【作法二：寶錄公司多卡平行驗證(即所謂「同詢法」)】

此一作法，乃是將產生衍生金鑰的動作提出於驗證迴圈之外，並使用硬體修改之方式，使各張 SAM 卡得以獨立同時產生衍生金鑰。如此一來，整個處理流程將變成如圖 3-9 所示：

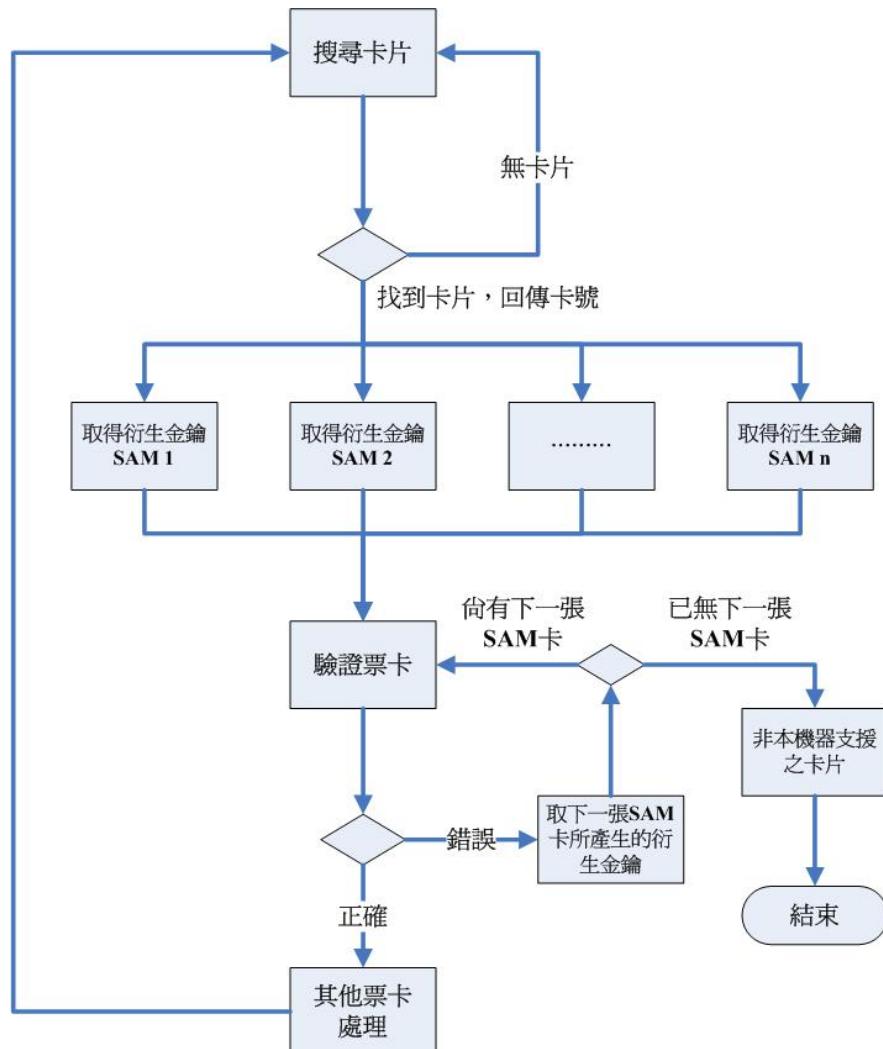


圖 3-9 多卡平行驗證之交易流程(本研究)

由圖 3-9 可知，取得衍生金鑰的動作可利用硬體的支援，而變成在同一時間內於各張 SAM 卡中完成，原本需要 n 乘以“衍生金鑰時間”的迴圈，變成只需產生一次”衍生金鑰時間”，因此，最後的一張 SAM 卡所需的時間跟第一張 SAM 卡所需的時間就幾乎沒有差別(因驗證票卡所需的時間遠小於 0.01 秒，故可以忽略)。

寶錄電子公司於民國 98 年 12 月取得專利證書編號 M370776 之非接觸式 IC 卡驗票機五項專利權，其系統架構示意圖如圖 3-10：

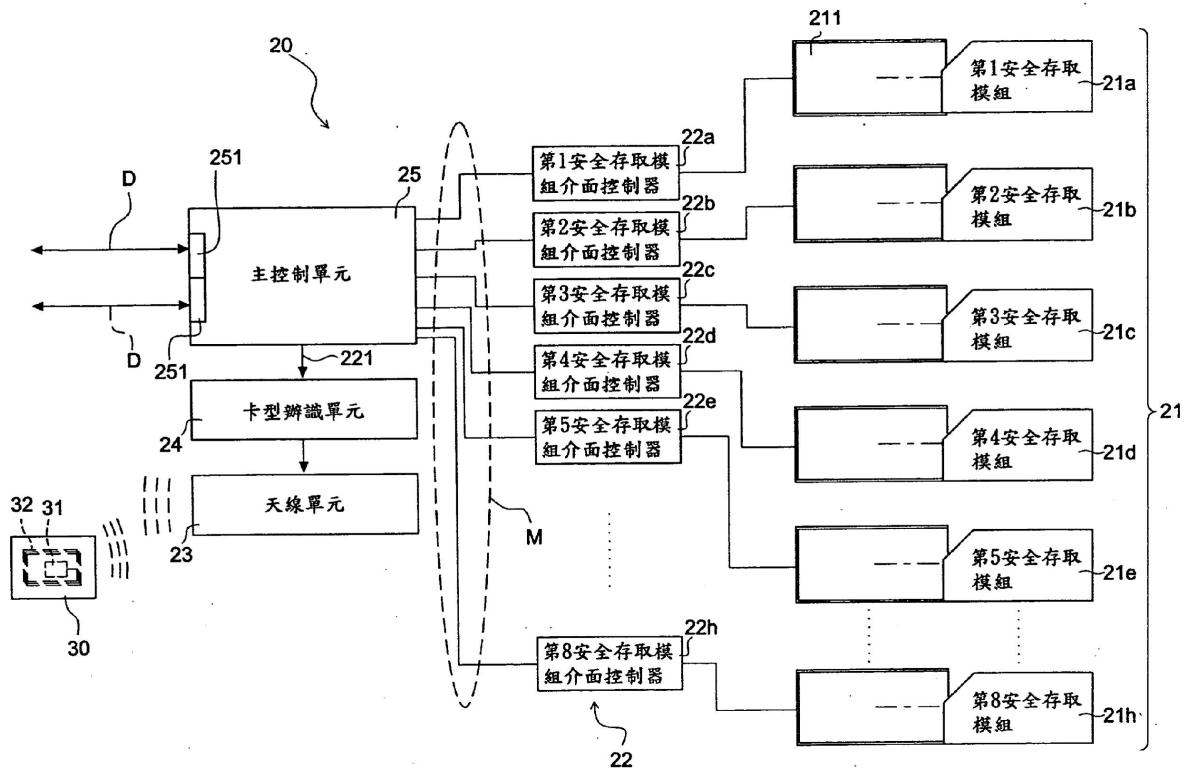


圖 3-10 專利證書 M370776 之非接觸式 IC 卡讀寫模組系統架構圖

資料來源：智慧財產局新型說明書公告本(中華民國 98 年 12 月 11 日公告)

該驗票機由天線單元[23]、卡型辨識單元[24]、主控制單元[25]、安全存取模組(SAM)介面控制器[22]、安全存取模組(SAM)[21]、非接觸式 IC 卡[30]等組成，非接觸式 IC 卡[30]內置線圈天線[32]與晶片[31]。

該非接觸式 IC 卡讀寫模組包含數個 SAM[21a~21h]，在技術上可將 SAM 直接焊死或利用一插槽[211]裝置不同電子票證營運系統之 SAM，也可直接燒錄 SAM 應用程式。每一個 SAM[21]配對一固定之 SAM 介面控制器[22]，並以電性連接以獲得資訊。數個 SAM 介面控制器[22a~22h]則以多工的模式[M]與主控制單元[25]電性連接，每一個 SAM 介面控制器[22a~22h]與其配對的 SAM[21a~21h]可透過主控制單元[25]運算出一組驗證碼[221]。

當非接觸式 IC 卡[30]接近該驗票機天線單元[23]微波所及範圍時，第一組 SAM 介面控制器[22a]將以電性連接第一組 SAM[21a]傳送資訊給主控制單元[25]，主控制單元[25]根據該非接觸式 IC 卡[30]卡號與第一組 SAM[21a]所提供的資訊算出第一組驗證碼；同時間，其它各個 SAM 介面控制器[22b~22h]依照以上模式算出各組所屬的驗證碼。主控制單元[25]再

利用卡型辨識單元[24]將驗證碼[221]調制成符合該非接觸式 IC 卡[30]型態所能接收的資料型態封包，透過天線單元[23]傳送到該非接觸式 IC 卡[30]的線圈天線[32]，並由該非接觸式 IC 卡[30]的晶片[31]確認其正確性並回報給主控制單元[25]。之後，主控制單元再重覆以上流程，逐一依序將各組之驗證碼傳送到非接觸式 IC 卡[30]進行驗證，直到找到可以存取該非接觸式 IC 卡[30]的一組驗證碼[221]之後，即可由主控制單元[25]取的該非接觸式 IC 卡[30]的內容及所屬的票證營運系統[D]，透過主控制單元[25]之通訊介面[251]與所連結之應用系統進行進一步的應用。

該讀寫模組在獲得一組非接觸式晶片卡卡號之後，可多步、同工地驗算個別驗證碼，再彙整後逐一利用該些驗證碼來與該非接觸式晶片卡相互驗證，約可在 0.5~0.6 秒的時間完成卡片交易。



圖 3-11 智慧巴士一機多卡(悠遊卡、高捷卡、台灣通、e 通卡)驗票機

資料來源：中央社 99 年 5 月 25 日

3.4 一機多卡整合模式商業技術層面影響因素分析

根據本研究的訪談及觀察，國內目前有能力開發驗票機的廠商應該都有能力運用硬體平行作業處理的方法，將金鑰衍生的動作縮短至最短；或以提升硬體效能以及韌體最佳化的作法使整體交易速度加快。

故本研究認為，以國內資訊產業的研發能力，無論是提高硬體效能或開發韌體以應用一機多卡整合模式交易並不困難，但是必須另外考量兩個層面的問題：

一、如何因應卡片晶片技術的快速發展？

當全球的晶片運算技術不斷演進，甚至出現與目前完全不同的運算模式時(如邏輯加密卡已逐漸被CPU卡所取代)，為了接受新的卡片技術而修改或重置已建置的前端設備所花費的成本是否符合經濟效益？值得深入評估。

二、如何整合運輸業者差異頗大的票證營運規則？

各運輸業者(尤其是公路客運業者)因為長期以來都有所屬的營運區域，為了滿足各區域的營運特性均已建置一套客制化的營運規則，當跨區域營運的電子票證出現時，運輸業者彼此的營運規都必須互相調整，以重新建構一套大家都可以接受的電子票證營運處理流程，此需要透過商業談判或公權力介入才能完成的協商過程，比票證技術層面的整合更困難。

有關一機多卡整合模式之影響因素分析，請參閱本研究第四章 4.2.1。

3.5 一機多卡整合模式策略期程建議

綜合上述各節之論述，本研究認為票證整合可分短、中、長期三階段執行時程，以分批漸進的方式完成整合。

一、短期建議：交易分流

以目前票證業者具地域性的營運特性，以及迥異的系統規劃與營運邏輯，可採用「一機多卡驗票設備整合模式」，但各票證業者的交易資料仍由運輸業者管理系統各自傳送所屬的票證系統進行清分作業。執行重點說明如下：

1. 策略目的：短期讓民眾體驗票證整合之便利，解決多卡多機之困擾。
2. 整合主體：前端驗票機
3. 整合介面：讀卡機驗證流程、驗票機(含應用軟體)及場站管理系統(DPS)、運輸業者管理系統(CPS)分流機制。
4. 可能問題：同一驗票機各票證業者之營運邏輯必須整合，否則驗票程序會太複雜而無法作業。

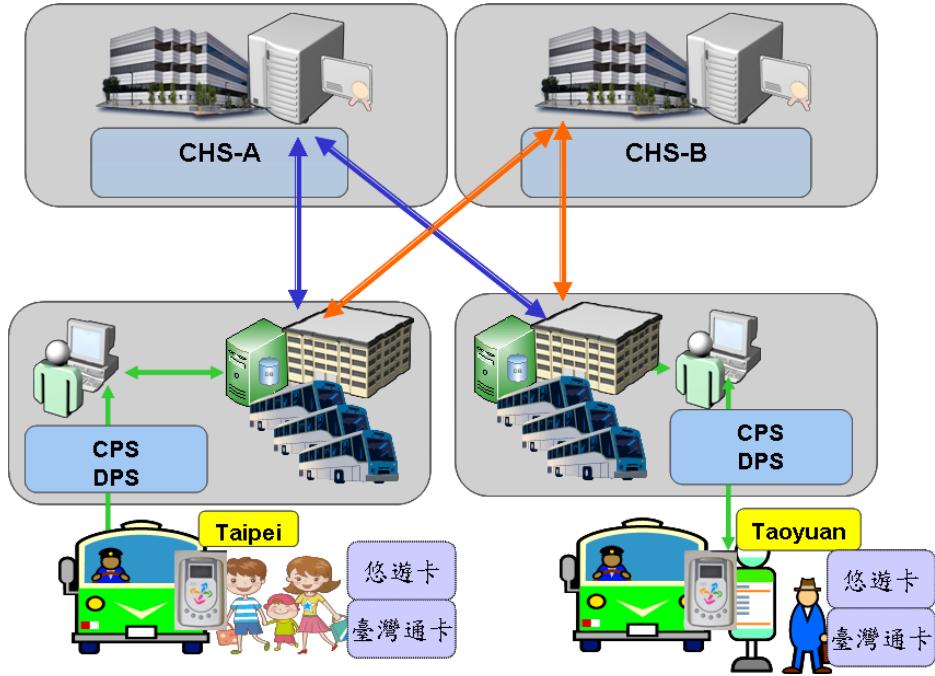


圖 3-12 一機多卡短期整合策略：交易分流

二、中期策略：管線共構

有別於前項之交易分流方式，「管線共構模式」不須更動或整合既有各票證業者各自獨立之清分清算系統，但透過「統一作業介面機制」，將所有清分之交易資料傳輸需求，匯合至此一平台，而由此一清分前處理平台將交易資料檔傳輸到各個票證業者。執行重點說明如下：

1. 策略目的：不須更動或整合既有各票證業者之清分清算系統，透過「統一作業介面機制」，提高硬體投資與維運作業上的效率。
2. 整合主體：前端驗票機、後端交易資訊流。
3. 整合介面：讀卡機驗證流程、驗票機(含應用軟體)、場站管理系統(DPS)、運輸業者管理系統(CPS)採共通標準格式、建立清分前作業平台(CHS Pre-processing Platform)。

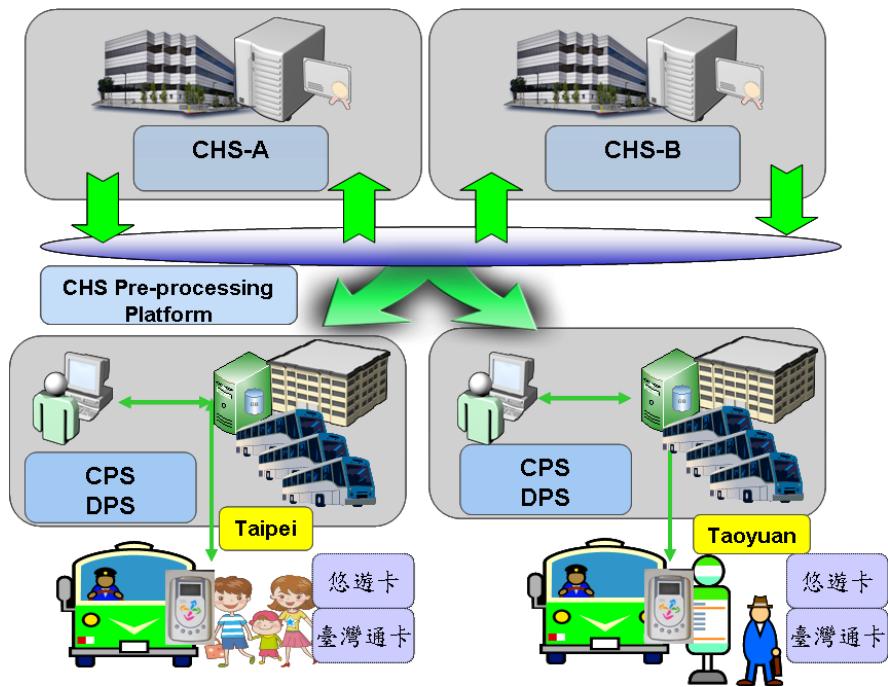


圖 3-13 一機多卡中期整合策略：管線共構

三、長期策略：聯合處理

長期策略可參考建置類似信用卡聯合清算中心的組織，提供各運輸業者代收其它票證業者之卡片，透過聯合處理之方式，可節省各票證業者重複作業及硬體投資。執行重點說明如下：

1. 策略目的：透過類似信用卡聯合清算中心之組織，運用聯合清分中心機制，可節省各票證業者重複作業及投資。
2. 整合主體：前端驗票機、後端交易流、資安驗證平台。
3. 整合介面：讀卡機驗證流程、驗票機(含應用軟體)、場站管理系統(DPS)、運輸業者管理系統(CPS)採共通標準格式、建立資安驗證中心及聯合清分處理中心(United HS Processing Center)。

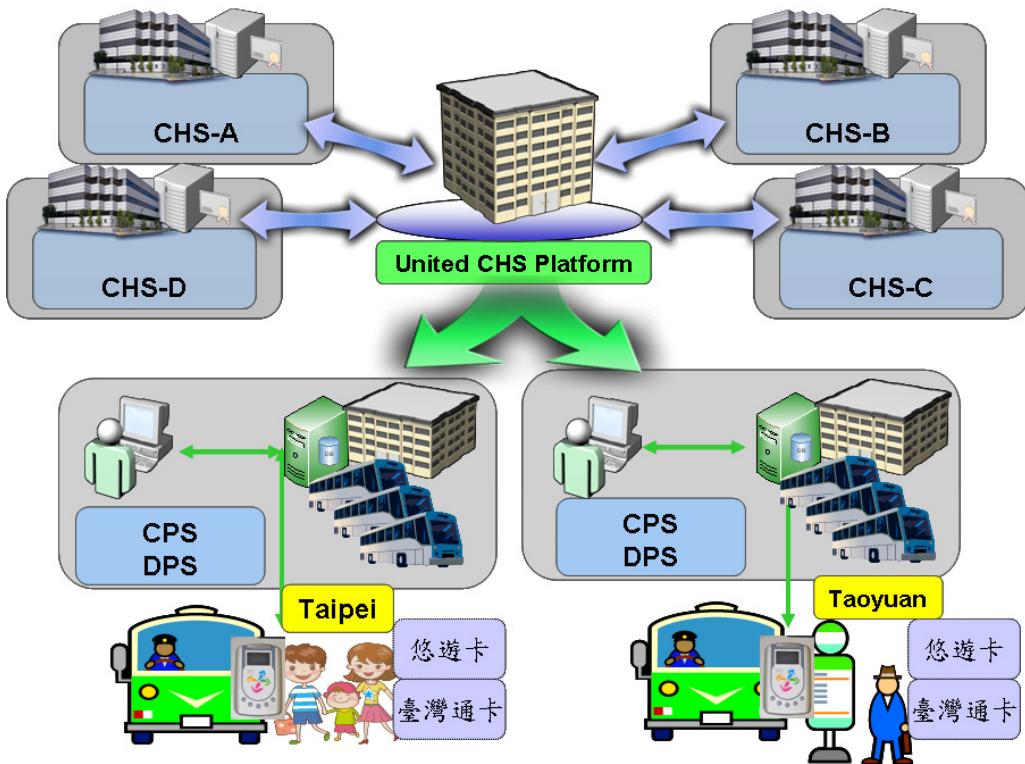


圖 3-14 一機多卡長期整合策略：聯合處理

第四章 一機多卡整合模式影響因素實例探討

本期研究從第三章技術解決實例來看，不論以硬體平行作業或以提升韌體效能及最佳化的作法，二者均可解決一機多卡交易速度的問題。故本研究認為，以國內資訊產業的研發能力，無論是應用硬體效能或韌體開發來解決一機多卡整合交易並不困難，但是非屬技術層面的問題則更複雜。

本研究以一機雙卡整合實例(說明如 4.1 節)進行個案分析，說明一機多卡票證整合模式對權益關係人的影響及因應作法建議。本個案僅為整合雙卡，持卡人等待扣款時間不長，故未採用同詢法之技術，但個案所衍生之商業技術問題同樣具有參考價值。

4.1 一機多卡整合模式實作案例

4.1.1 背景說明

桃園客運與台北客運於民國 99 年聯營桃園往返台北的國道客運路線，並邀請台北悠遊卡公司(悠遊卡)與台灣智慧卡公司(臺灣通)共同合作，建置該路線一機多卡電子票證整合系統，希望達成民眾無論持悠遊卡或是臺灣通均可於該兩家客運之特定路線公車上支付費用之目標。

此計畫為國內運輸業者首次整合兩家票證業者之應用，此應用將大為提升民眾使用電子票證之便利性，民眾不必因跨系統而再多買一張 IC 卡，客運公司也可以減少硬體設備之投資。然而一機多卡涉及多個層面之整合議題，包含需求整合、營運邏輯、資安驗證流程、系統整合、清算作業等層面，本研究擬從實務面所發現的問題提出可能解決之方向建議。

4.1.2 整合架構

由於台北客運之原有營運區域多使用悠遊卡，而桃園客運原有之營運區域則多使用臺灣通卡，因此，桃園往返台北公車上的驗票機必須具備可兼容兩種票卡之使用功能，避免造成民眾持有多卡之困擾。

此一機多卡個案之整合架構可就「設備層面」與「權益關係人層面」分別

說明，如圖 4-1 所示：

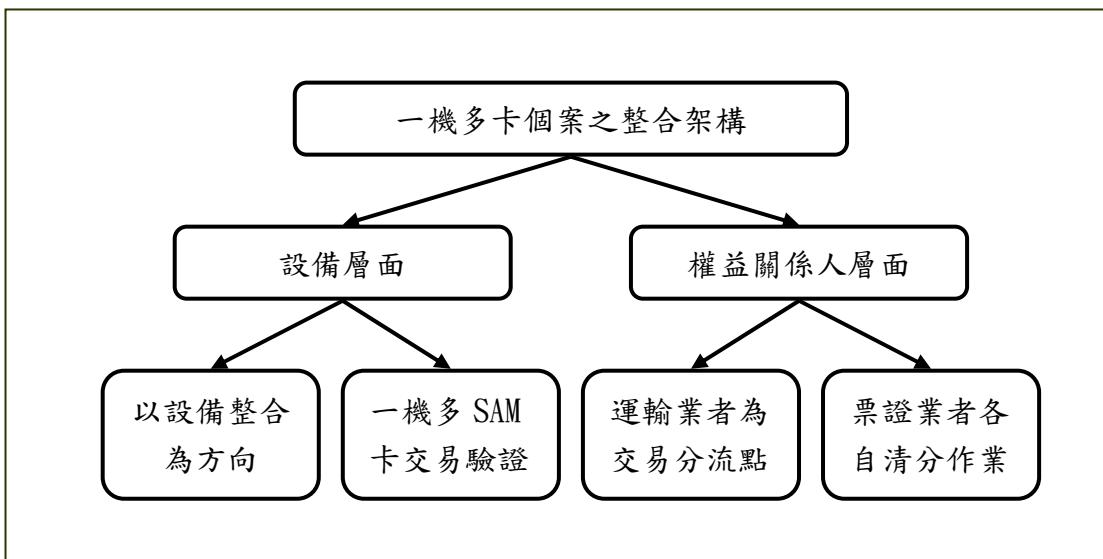


圖 4-1 一機多卡整合架構示意圖

一、設備層面

1. 以設備整合為方向：

電子票證整合有兩個主要方向，一種方式為規範統一的卡片資料定義、欄位格式屬性以及驗證流程等，如本研究前期所規劃之「交三版（草案）」；另一種方式為透過驗票機軟硬體技術以兼容不同票證業者之卡片（包含營運邏輯），本案例屬於後者之整合模式。

2. 一機多 SAM 卡交易驗證：

本作法是以「一機多卡」驗票機作為票證整合之主體，每一台驗票機同時插入兩家以上票證業者所提供之 SAM 卡，以作為交易安全驗證之用。

二、權益關係人層面

1 以運輸業者為交易分流點

本案例以運輸業者管理系統為傳輸介面，驗票機所產生之各票證業者交易檔，先傳送至運輸業者管理系統，再由該系統將交易檔依照所屬之票證業者分流上傳至各清算中心。

2 票證業者各自清分作業

透過運輸業者管理系統，各票證業者僅會取得所屬之交易檔，該

交易檔依循各票證業者之清分清算系統作業原則，自行與運輸業者進行清分，故運輸業者必須同時面對兩家以上票證業者之清分作業，即所謂清分分流機制，相關對帳與調整作業亦分別進行，並無實質資訊流或金流整合的問題。

以上的層次關係如圖 4-2。

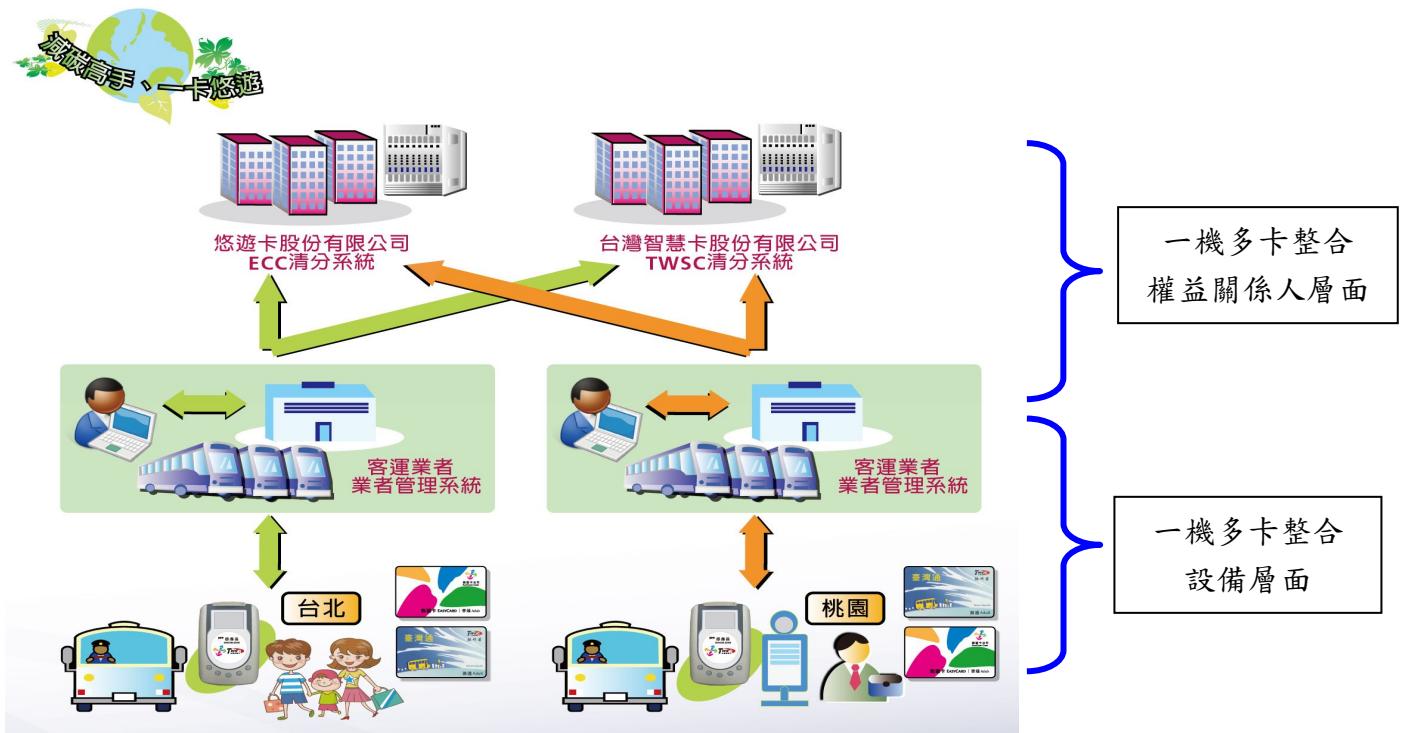


圖 4-2 一機多卡整合模式示意圖

4.1.3 整合的前提條件與執行步驟

本研究針對本個案整合之經驗，歸納出以下票證整合的前提條件及執行步驟。

一、本票證整合案例之載具分屬不同運輸業者但營運相同路線，整合的前提條件如下：

1. 驗票機的韌體須具備不同票證業者之營運邏輯。
2. 驗票機之讀寫模組(Reader Module)須能兼容不同票證業者之 SAM 卡驗證機制。
3. 驗票機上傳至運輸業者管理系統的營運資料，必須能滿足各運輸業者對

交易資料格式的需求。

4. 運輸業者管理系統必須具備多介面功能，用以上傳分屬不同票證系統之交易檔。

二、本票證整合案例歷經以下五項執行步驟，如圖 4-3 之流程圖所示：

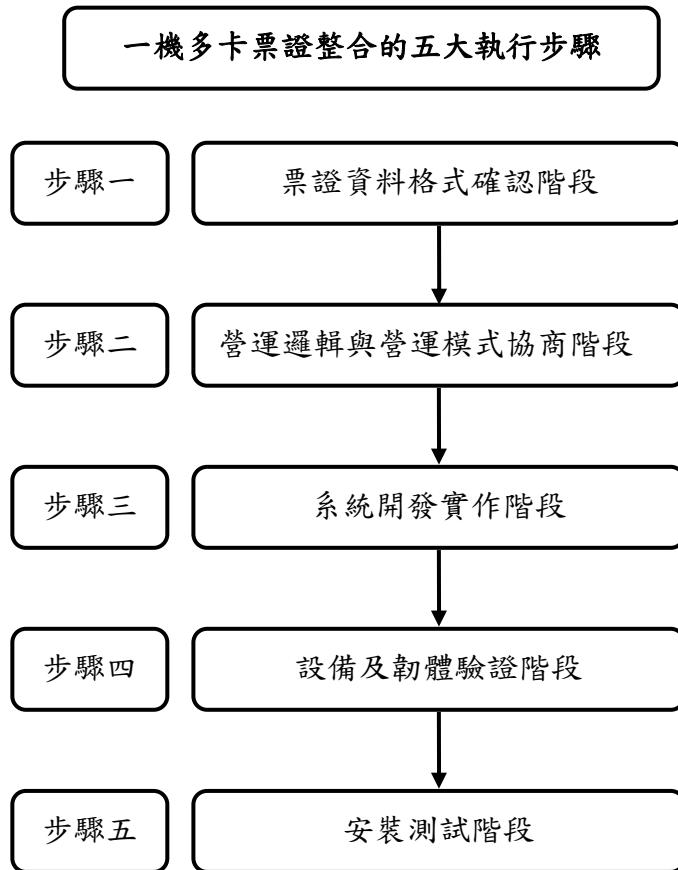


圖 4-3 一機多卡整合模式之執行步驟

步驟一：票證資料格式確認階段

透過正式授權管道，取得各家票證業者之票卡資料格式與營運邏輯，進一步比對各家票證業者之差異，作為下一階段協商調整之基礎。

步驟二：營運邏輯與營運模式協商階段

各票證業者與各運輸業者都必須面對彼此不同之營運邏輯與營運模式而相互調整，否則將導致整合作業流程之衝突。

步驟三：系統開發實作階段

依據上一階段已達成共識之營運邏輯與營運模式進行系統開發，分成三部分進行：

(1) 讀寫模組之程式開發：

驗票機讀寫模組必須同時讀取各家票證業者之 SAM 卡，作為安全交易與金鑰驗證之用。

(2) 驗票機之程式開發：

驗票機必須依據已達成共識之營運邏輯與票卡格式產出各票證業者之交易檔作為清分清算作業之用。

(3) 運輸業者管理系統開發：

運輸業者管理系統必須整合為統一之傳輸介面，以彙整所有驗票機之交易檔分別上傳至各票證業者清分系統。

步驟四：設備及韌體驗證階段

依據各家票證業者對減值設備作業之要求，各家系統整合廠商均須將讀寫模組、設備韌體與系統版本，提供給票證業者進行驗票機之驗證。

因為各家票證業者均有各自所屬之驗證作業規範與測試要求，在國內目前無統一驗證中心與驗證平台之狀況下，驗票機之驗證作業必須由各票證業者各自進行。

步驟五：安裝測試階段

完成上一階段之驗證流程後，各票證業者才能依據各自作業流程，提供正式上線用之 SAM 卡給各家系統整合廠商，以作為後續實機運作之用。車上驗票機與運輸業者管理系統亦須同步安裝測試，於確認無誤後方可正式營運。

4.2 一機多卡整合模式之影響分析與因應作法

4.1.3 節五項的整合步驟中，後面三步驟(系統開發實作階段、設備及韌體驗證階段、安裝測試階段)均是電子票證整合之標準流程。本研究認為，步驟一(票證資料格式確認階段)與步驟二(營運邏輯與營運模式協商階段)係整合困難度與共識分歧度最高的部分。其主要原因是：各票證業者當初成立時，均以各區域之交通票證需求為主，其系統架構與設計均以滿足各區域之運輸業者營運特性，因此，各票證業者之系統功能提供個別客製化的設計與當地區性的服務，

以致各票證業者之卡片資料格式與營運邏輯欠缺共通性架構。

因此，就系統技術開發角度而言，票證業者在卡片資料格式與營運邏輯的差異是影響系統整合最大的因素，此項工作是本個案一機多卡整合最困難突破的瓶頸所在。

4.2.1 一機多卡整合模式之影響因素

本研究分析 4.1 節「一機多卡整合模式實作案例」，將影響票證整合的因素分為營運邏輯類、應用代碼類、資安控管類、設定環境類、清分作業類、優惠補助類等六類，並針對各類整理共 19 項影響因素，如表 4-1：

此 19 項影響因素多為各票證業者營運邏輯的差異，以下為受影響之營運邏輯：

表 4-1 一機多卡整合模式受影響之營運邏輯

項目	受影響之營運邏輯
段次計費	費率計算採分段計費，依據乘客搭乘之起訖站段次區間，分一段、兩段、三段、甚至多段次計費。
里程計費	費率計算以乘客搭乘起訖站之站位，以三角費率表為計費依據。
交易紀錄	驗票機運用票證業者所提供之 SAM 卡，依據票證業者規範之紀錄格式、紀錄內容，將該次交易之資料產生交易檔，於結班時彙整當日交易檔作為上傳之交易紀錄。
轉乘優惠	持卡人於公路客運或市區公車下車後特定時間內，再搭乘特定區域內之交通載具時，可享有一次優惠，可以為同載具轉乘(公車轉乘公車或捷運轉乘捷運)，亦可為不同載具轉乘(公車轉乘捷運或捷運轉乘公車)
逃票作業	持卡人可能因某種原因導致有上車但無下車記錄之異常狀態時，驗票機於驗證時會拒絕此一卡片交易，該持卡人需至場站或指定地點進行解除程序後方可再度正常使用。
路故作業	路故作業為車輛發生故障，無法完成當次路線營運時，由駕駛員所執行的作業。
機故作業	車輛行進間驗票機因某種原因故障，無法提供驗票服務，導致原刷卡上車者無法以刷卡模式下車之情況。
票卡代墊額度	當持卡人下車時，若票卡餘額不足，票證業者代墊該一旅次不足之車資之金額限制。
錄押碼作業	在資安規範下，要求讀寫模組(Reader Module)在系統上線前，需將送至票證業者進行錄押碼之作業。
卡種類別	票證業者為因應運輸業者營運需求所提供之各種卡種，例如：學生卡、福利卡、認同卡、旅遊卡等。

針對「營運規則」一詞，主要源自運輸業者之營運規定，例如台灣鐵路局電子票證乘車之營運規則，包括車票種類、電子票卡種類、票價計算、票卡之使用規定、車上查驗規定、票卡加值服務等內容。

運輸業者中，以里程計費之公路客運的營運規則最複雜，主要原因為公路客運具地域性，每一地區的人口結構不同，形成不同屬性的客群，加上各地方政府因地制宜的大眾運輸政策，經過長期經營之後，幾乎沒有營運規則完全相同的公路客運業者。故本研究以下所稱之「營運規則」整合，係以里程計費之公路客運業者為主，不包括單次計費之市區公車及軌道運輸業者。

票證業者為了服務所轄區域之運輸業者，對各運輸業者之營運規則加以整合，以進一步歸納整合為票證業者之營運規則。

除了整合轄區內各家運輸業者之運務營運規則外，票證業者之營運規則同時包含票證運作所需之票證營運規則，例如：司機開班結班規則、路線管理規則、標準扣款作業、路線卡功能規則、點數優惠處理、問題票卡處理、餘額不足處理、機故處理規範、路故處理規範、特許管制規範、特種票規範、轉乘管理規範等。故所謂「營運規則」應該是包含「運務營運規則」與「票證營運規則」兩大類，其內容項目大致如表 4-2 所示。

表 4-2 營運規則的分類與內容

	運務營運規則	票證營運規則
細目參考	1. 乘車票種類 2. 電子票卡種類 3. 票價計算 4. 票卡之使用規定 5. 車上查驗規定 6. 票卡加值服務	1. 司機開班結班規則 2. 路線管理規則 3. 標準扣款作業 4. 路線卡功能規則 5. 點數優惠處理 6. 問題票卡處理 7. 餘額不足處理 8. 機故處理規範 9. 路故處理規範 10. 特許管制規範 11. 特種票規範 12. 轉乘管理規範

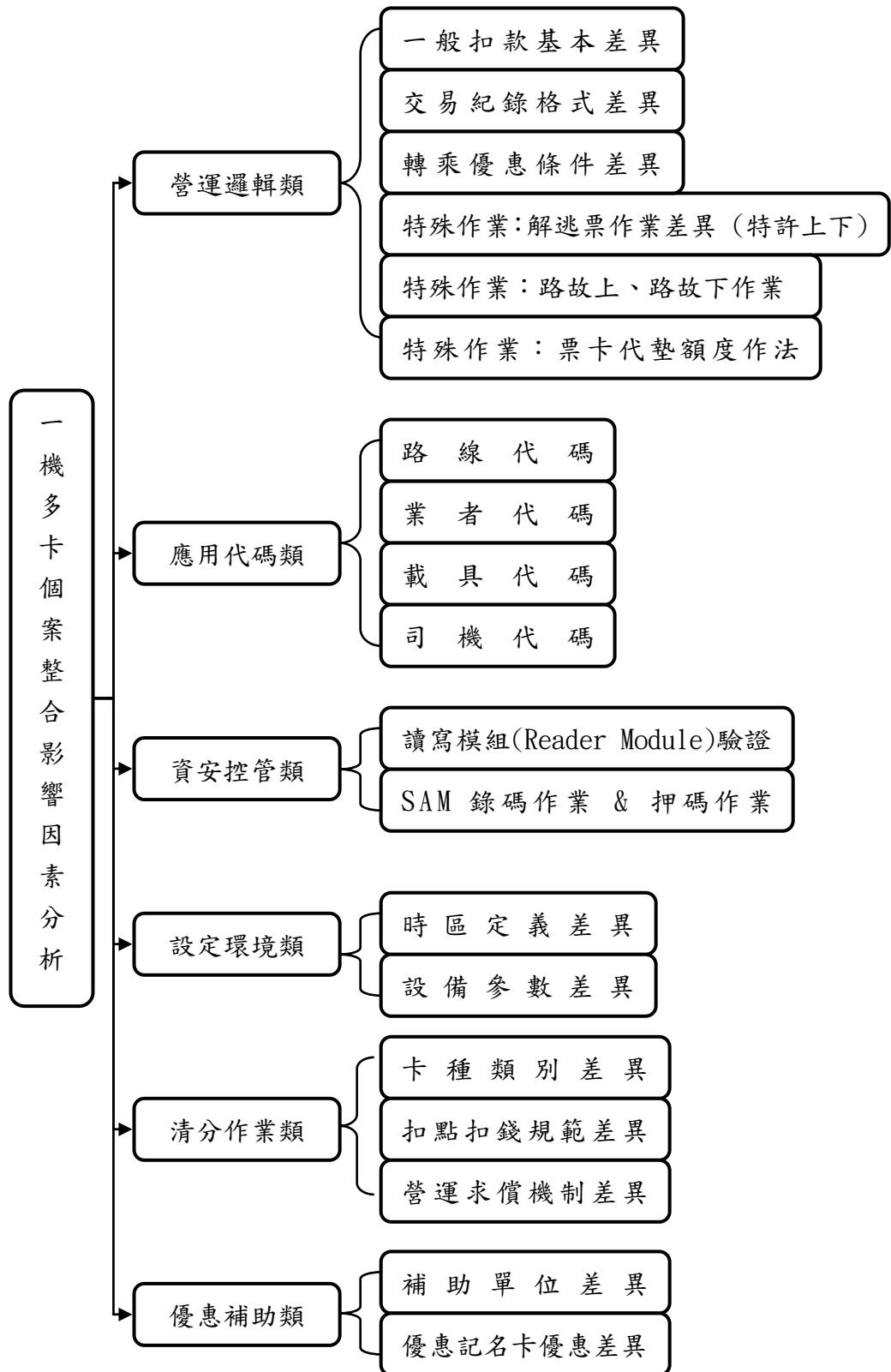


圖 4-4 一機多卡整合模式影響因素分析

圖 4-4 繞本實作案例「一機多卡整合模式」之影響因素分析圖，各類型之影響因素詳細說明如下：

一、營運邏輯類

1. 一般扣款基本差異：

票證業者針對不同營運區域的運輸業者，均有其客制化之營運邏輯，例如，悠遊卡對北縣市公路客運者有段次計費與里程計費兩種扣款機制，但因桃園地區的公路客運並不使用段次計費，故臺灣通規劃營運邏輯時並未考慮段次計費，本實作案例便須開發同時提供該路線可以段次計費以及里程計費之功能。

2. 交易紀錄格式差異：

一機多卡於交易所產生之交易檔，必須依據各票證業者所要求之交易檔產生原則進行設計，故交易檔格式、記錄方式與檔案位置均各自獨立而未統一，因此必須將兩造交易紀錄方式與檔案位置加以區隔。

3. 轉乘優惠條件差異：

各票證業者因為區域的營運條件不同，對於轉乘優惠的營運邏輯也會有所差異。例如，臺灣通持卡人於公路客運或市區公車下車後特定時間內，再搭乘同區域內所有客運公司之公路客運或市區公車時，可享有一次優惠；然而悠遊卡持卡人於公車或捷運下車後，在轉乘群組限定條件下(甚至可設定至路線別)可享受轉乘優惠，兩者之轉乘優惠營運邏輯不同。

4. 特殊作業：解除逃票作業差異(特許上下車)

臺灣通的逃票作業主要採取自動特許機制，即除了扣除當次上車時之基本車資外，並須補扣前次下車未驗卡時應支付之車資；而悠遊卡對解/逃票則需到指定場站進行處理方能恢復正常交易，但又有以下兩點例外：

- (1) 一般特許下車之處理：司機為因應上下車模式錯亂情況而對驗票機進行狀態修正，則可對此一車內之持卡人特許其下車。
- (2) 一般特許上車之處理：在里程計費狀況下，持卡人無論任何理由而導致有上車但無下車記錄之異常狀態時，除非是同客運業者同路線或是特許之設定，否則，系統將拒絕卡片交易，乘客需至指定場站進行罰款及解除逃票後，方可再度正常使用里程計費系統。

5. 特殊作業：路故上、路故下作業

所謂路故作業為駕駛員於車輛發生故障，無法完成當次路線營運時所執行的作業，不同票證業者對路故上、路故下之作業方式亦有所差異。例如，臺灣通之驗票機只對同家客運公司車輛發生路故下所註記之IC卡，可提供路故上免基本車資之自動驗卡服務，不同客運公司的車輛則回復一般正常扣款；悠遊卡路故上之條件為上次搭乘狀態是路故下，且限定在某一時間內由同公司同路線或聯營路線班車接駁。故驗票機對同一狀況(路故)，須針對不同票證業者的作業規定設計不同的作業流程。

6. 特殊作業：機故上、機故下作業

機故之狀況在於車子行進間驗票機因某種原因故障，無法提供驗票刷卡服務。臺灣通對於機故狀況，由駕駛員以人工計算車資。悠遊卡對於機故下車由司機手開憑證，尾款是否投現由各運輸業者自行決定；機故上車則乘客於下次搭乘時出具憑證，不需罰款。因兩家票證業者對機故上下特殊作業之差異，勢必要有統一的規定，否則司機須處理各種不同票卡之特殊作業需求，徒增行駛過程中額外的負擔，不利駕駛安全。

7. 特殊作業：票卡代墊額度作法

當持卡人下車時若票卡餘額不足，臺灣通將代墊該旅次不足之車資(目前無金額上限的規定)；而悠遊卡針對不足額票卡，其代墊額度有金額限制(目前代墊金額上限為60元)，超過限制之不足金額需由持卡人以現金支付。

二、應用代碼類

各家票證業者在票卡資料格式與營運邏輯相關欄位中，所需之營運參數需有一致性的規定，以避免交易資料代碼衝突或重複之狀況。目前整理已經統一或建議應儘速統一之應用代碼如下：

1. 路線代碼：由公路總局統一規定的的公路客運路線編碼是4碼，如將市區公車納入，將有效整合票證整合之公車路線代碼。
2. 業者代碼：建議應統一業者代碼，以避免清分作業之困擾。
3. 載具代碼：建議全國各種可能應用電子票證之交通載具統一載具代碼。

4. 司機代碼：目前悠遊卡之司機代碼為 4 碼，臺灣通之司機代碼為 6 碼，建議應統一司機代碼。

三、資安控管類

在資安驗證程序上，電子票證發行管理條例通過後，悠遊卡對於資安規範與讀寫模組(Reader Module)驗證，均依照金管會之要求與規範執行，特別在 SAM 卡控管作業以及 SAM 錄押碼作業之方式，均與臺灣通有所差異。此外，對於 SAM 卡與讀寫模組(Reader Module)通訊加密要求方面，悠遊卡均採用金融等級之規範，每筆交易均需要進行押碼作業。類似此種基於金融安全而考量之作業流程，其它尚未受金管會監管之票證業者，是否也能達到與悠遊卡同級之資安控管水準尚不可知，故此點也是電子票證整合過程中必須突破的重要議題。

四、設定環境類

目前一機多卡整合在環境設定方面，主要面臨以下兩項差異：

1. 時區定義差異：各家票證業者對於時區定義不同，在特殊狀況下對交易檔之資訊內容會造成差異，因此，對於時區校時必須有一致的定義。
2. 設備參數差異：各家票證業者對於設備參數之欄位與定義各自不同。針對 GPS 模組與電子票證計費模組整合所可能產生之票價誤差問題，必須考量里程計費係透過 GPS 定位作為計費的依據，若 GPS 模組已整合於電子票證設備中，一旦將 GPS 模組自電子票證設備中分離，可能會造成定位資訊非原始資訊而發生計費誤差，屆時電子票證模組所產出之報表可能與實際狀況有所誤差，也將造成計費誤差責任歸屬的問題(可能為電子票證模組，亦可能為 GPS 模組)，此並非票證整合所產生之問題，而是設備系統組件不同所產生之差異。因此，未來如果將電子票證設備之模組介接其它車載設備，如由不同設備供應商組合時，建議應建立檢驗機制。

五、清分作業類

由於各家票證業者之清分清算作業差異頗大，建議可採取清分清算分流模式，透過運輸業者管理系統將各自票證系統所需之交易檔，分別依據各票證業者所要求之格式傳送到所屬後台主機，進行交易驗證與清分清算作業，再將結果回傳給運輸業者管理系統，以進行對帳作業。雖然各票證

業者的清分清算作業各自獨立，但仍有以下幾項差異會影響一機多卡之整合：

1. 卡種類別差異：目前悠遊卡約有 30 餘種卡種，針對不同卡種之交易扣款運算邏輯均有所不同；臺灣通為配合客製化的需求，也提供各縣市業者近 90 餘種卡種，發展出許多複雜之交易邏輯與設計需求。建議可透過協商方式整合主流卡種來解決此項差異。
2. 扣點扣錢規範差異：臺灣通為滿足各運輸業者特殊的營運需求，因此發展出由各客運公司自己販售、推廣之多款認同卡及學生專車定期卡，並具備儲值金額或/及儲點餘額優惠折扣；悠遊卡除社福卡以外，無所謂儲點之優惠折扣。類似各家票證業者自行發展之優惠扣點營運規則，將會造成對帳時因各種交易方式與點數換算比率不同產生極大的困擾。
3. 營運求償機制差異：悠遊卡的求償機制以司機發車時之系統正常寫入為判斷依據；臺灣通則無此種機制。因此，如果一機多卡發生機故狀況，所衍生之賠償問題，將會造成各票證業者與運輸業者間認知上的差異而產生困擾。

六、優惠補助類

為鼓勵公共運輸與實施社會福利政策，地方政府往往會為特定持卡人提供相關優惠與補助，然而因為持卡人持有不同票證業者之卡片，在一機多卡整合模式中，可能造成優惠無法同步整合的情況，說明如下：

1. 補助單位差異：各家票證業者雖都可發行優惠記名卡，但是各補助單位對資訊內容的需求不同，因此，不同報表之產製將增加運輸業者請款作業的複雜度。
2. 優惠記名卡優惠差異：各家票證業者雖都可發行敬老卡，但是各縣市優惠上限不同，扣點或扣錢之規定與額度也不同，一來造成駕駛員判斷的困擾，二來民眾也會對於不同持卡人的優惠差異而產生認知上的落差。

4.2.2 一機多卡整合模式影響之權益關係人

本研究針對 4.2.1 節「一機多卡整合模式影響因素」之探討，除將影響一機多卡整合的因素歸納為六大類型之外，也依據影響類型的屬性分別歸屬不同的權益關係人，包括票證業者營運、運輸業者、系統整合商與持卡者使用認知等，

三者的關係彙整如表 4-3 及圖 4-5。本研究認為，一機多卡整合模式雖然可以透過驗票機軟硬體技術達到多卡一機整合的目的，但仍然無法避免不同票證業者在票證資料格式與營運邏輯上整合之困難。

表 4-3 一機多卡整合模式影響因素、所屬類型與權益關係人之關係

項次	影響因素類型	影響因素	權益關係人
1	營運邏輯類		
1.1		一般扣款基本差異	運輸業者
1.2		交易紀錄格式差異	系統整合商
1.3		轉乘優惠條件差異	運輸業者、持卡者使用認知
1.4		特殊作業：解逃票作業差異(特許上下)	運輸業者、持卡者使用認知
1.5		特殊作業：路故上、路故下作業	運輸業者、持卡者使用認知
1.6		特殊作業：機故上、機故下作業	運輸業者、持卡者使用認知
1.7		特殊作業：票卡代墊額度作法	票證業者營運、運輸業者、持卡者使用認知
2	應用代碼類		
2.1		路線代碼	票證業者營運、運輸業者
2.2		業者代碼	票證業者營運、運輸業者
2.3		載具代碼	票證業者營運、運輸業者
2.4		司機代碼	票證業者營運、運輸業者
3	資安控管類		
3.1		讀寫模組(Reader Module)驗證	票證業者營運、系統整合商
3.2		SAM 錄碼作業 & 押碼作業	票證業者營運、系統整合商
4	設定環境類		
4.1		時區定義差異	票證業者營運、系統整合商
4.2		設備參數差異	票證業者營運、系統整合商
5	清分作業類		
5.1		卡種類別差異	票證業者營運、運輸業者、持卡者使用認知
5.2		扣點扣錢規範差異	票證業者營運、運輸業者、持卡者使用認知
5.3		營運求償機制差異	票證業者營運、運輸業者
6	優惠補助類		
6.1		補助單位差異	票證業者營運、運輸業者
6.2		優惠記名卡優惠差異	票證業者營運、運輸業者

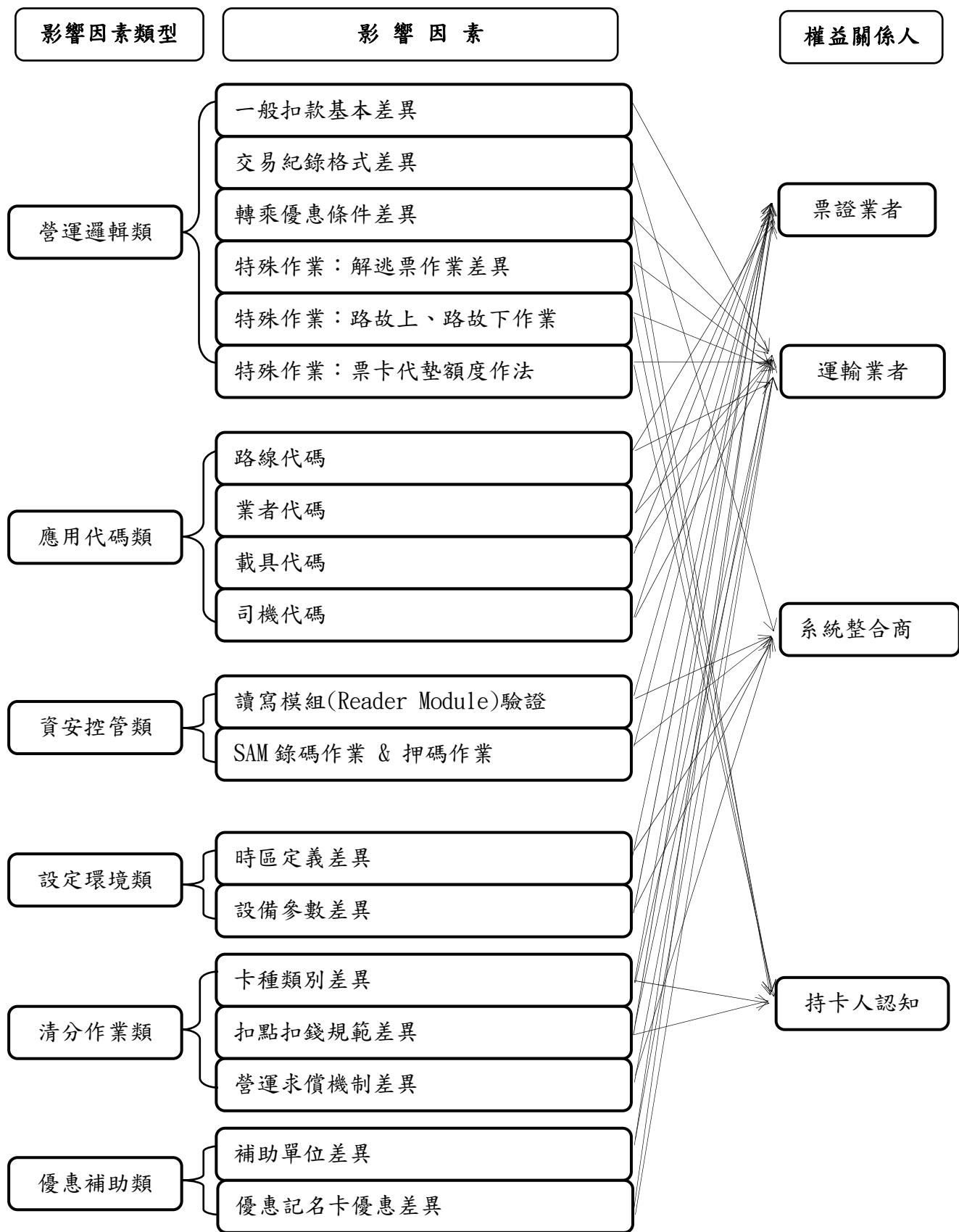


圖 4-5 一機多卡整合模式影響因素、所屬類型與權益關係人之對照圖

4.2.3 一機多卡整合模式跨區優惠對不同角色之權益關係人的影響

票證業者成立初期均有區域性，例如悠遊卡主要使用地區為大台北，台灣智慧卡則為中彰投、桃竹苗等地。本研究對交通票證「區域」的定義，係指該區域之行政機關，為滿足轄區特定民眾交通付費的需求，與某票證業者約定，針對指定之公車路線，提供特定民眾各種優惠或折扣。因此，所謂某「區域」的交通電子票證形式之社會福利卡須具備三項要素：一、僅發行給該「區域」行政機關所轄之特定民眾；二、該行政區機關須與特定票證業者簽約；三、僅能使用於指定之公車路線。故本研究以下所稱之「區域優惠」須符合以上三項要素。

例如，桃園縣之居民持台灣智慧卡公司所發行「桃園縣社會福利卡」搭乘桃園客運享有優惠，其前提是該居民為桃園縣政府所轄之居民、桃園縣政府與台灣智慧卡公司簽約、該居民僅能搭乘指定之桃園客運營運路線。

在「一機多卡整合模式」下，於沒有完整配套措施之前，本研究不建議票證業者對具有「區域優惠」票卡提供跨區使用，原因如下：

- 一、各地方政府對優惠之補助方式差異甚大，容易造成民眾與運輸業者之混淆。
- 二、社會福利補助對象以設籍居民為主，對跨區使用的優惠票卡如何計價有執行上的困難。

表 4-4 列出具「區域優惠」票卡跨區使用對民眾、運輸業者與政府三種不同角色之權益關係人之影響。

表 4-4 具「區域優惠」票卡跨區使用對各方權益關係人的影響

不同角色之 權益關係人	影響的內容
民眾認知	優惠卡種跨區使用時因補助單位計價方式不同，會造成民眾困惑。
運輸業者	民眾詢問的頻率增加，會加重司機及站務員的負擔。
政府角色	民眾申訴的案件增加，對施政滿意度有負面的影響。

本研究建議於在「一機多卡整合模式」導入初期，優惠票卡之「區域優惠」宜以「屬地主義」為主，「屬票證業者」為輔。所謂「屬地主義」以該優惠票卡核發之行政機關所管轄之區域為判定依據，當優惠票卡跨區使用時，則原「區域優惠」所享有之優惠將無法執行；所謂「屬票證業者」則是以票證業者所提供之折扣優惠辦法為依據，與「區域優惠」無關。

以下為本研究對「一機多卡整合模式」導入初期所建議的作法：

- 一、於跨區使用時，以「一般票卡(全票)」為限，並以扣錢為主，不支援扣點，以避免”一點”是否等同”一元”的困擾。
- 二、社會福利卡等優惠票卡不可跨區使用，以避免引發社福單位補助用途錯置之爭議。
- 三、不提供跨區票卡之轉乘優惠，以避免補助單位請款認定之困擾。
- 四、搭配優惠票卡跨區使用辦法之宣導，以避免民眾因為認知之差異而引發民怨。

將表 4-3「一機多卡整合模式影響因素、所屬類型與權益關係人之關係」對照因應作法以矩陣排列，如表 4-5「一機多卡整合模式影響因素與因應作法之矩陣表」。

表 4-5 一機多卡整合模式影響因素與因應作法之矩陣表

影響因素的類型 影響因素 因應作法	營運邏輯類 營運邏輯類	應用代碼類 資安控管類	設定環境類 清分作業類	優惠補助類
	<ul style="list-style-type: none"> ◆ 一般扣款基本 ◆ 差異 ◆ 轉乘優惠條件 ◆ 差異 ◆ 特殊作業：解逃票 ◆ 差異 ◆ (特許上下) ◆ 特殊作業：路故上、路故下作業 ◆ 上、路故下作業 ◆ 特殊作業：機故上、機故下作業 ◆ 上、機故下作業 ◆ 特殊作業：票卡代墊額度作法 ◆ 代墊額度作法 	<ul style="list-style-type: none"> --- --- --- --- --- 	<ul style="list-style-type: none"> ◆ 營運求償機制 ◆ 差異 	<ul style="list-style-type: none"> ---
驗證流程整合		<ul style="list-style-type: none"> --- 	<ul style="list-style-type: none"> ◆ 讀寫模組 (Reader Module)驗證 ◆ SAM 錄碼作業 及押碼作業 	<ul style="list-style-type: none"> ---

表 4-5 一機多卡整合模式影響因素與因應作法之矩陣表(續)

影響因素的類型 影響因素 因應作法	營運邏輯類 營運邏輯類	應用代碼類 資安控管類	設定環境類 清分作業類	優惠補助類
交易邏輯整合	<ul style="list-style-type: none"> ◆ 一般扣款基本差異 ◆ 轉乘優惠條件差異 ◆ 特殊作業：解逃票作業差異（特許上下） ◆ 特殊作業：路故障上、路故障下作業 ◆ 特殊作業：機故障上、機故障下作業 ◆ 特殊作業：票卡代墊額度作法 	<ul style="list-style-type: none"> ◆ 卡種類別差異 ◆ 扣點扣錢規範差異 ◆ 営運求償機制差異 	<ul style="list-style-type: none"> ◆ 補助單位差異 ◆ 優惠記名卡優惠差異 	
交易資訊整合	<ul style="list-style-type: none"> ◆ 交易紀錄格式差異 	<ul style="list-style-type: none"> ◆ 司機代碼 	<ul style="list-style-type: none"> ◆ 時區定義差異 ◆ 設備參數差異 	<ul style="list-style-type: none"> ---
運輸代碼整合	<ul style="list-style-type: none"> --- 	<ul style="list-style-type: none"> ◆ 路線代碼 ◆ 業者代碼 ◆ 載具代碼 	<ul style="list-style-type: none"> --- 	<ul style="list-style-type: none"> ---
區域特性宣導	<ul style="list-style-type: none"> --- 		<ul style="list-style-type: none"> ◆ 卡種類別差異 ◆ 扣點扣錢規範差異 	<ul style="list-style-type: none"> ◆ 補助單位差異 ◆ 優惠記名卡優惠差異

針對上述六項之整合因應作法，電子票證產業中各個不同角色之權益關係人，在不同的整合作法中，角色將會所轉換。例如，營運規則的整合應以運輸業者為核心，透過運輸業者間的溝通擬定一致性之營運規則，讓票證業者與系統整合商有已整合之營運規則可依循，票證業者在一機整合多卡作法上，可以主導之空間反而有限。

一機多卡整合模式各項因應作法與各層級權益關係人之關係如表 4-6，由該表可以進一步理解，電子票證整合所涉及之因素，以商業技術議題佔絕大部分。

表 4-6 一機多卡整合模式因應作法與各層級權益關係人之關係

項次	因應作法	主要權益關係人	次要權益關係人	技術性問題歸屬
1.	運輸規範整合	運輸業者	系統整合商、票證業者	商業技術問題
2	交易邏輯整合	運輸業者、票證業者	系統整合商	商業技術問題
3	交易資訊整合	票證業者	系統整合商、運輸業者	票證技術問題
4	驗證流程整合	票證業者	系統整合商	商業技術問題
5	運輸代碼整合	政府單位、票證業者	運輸業者	商業技術問題
6	區域特性宣導	政府單位、運輸業者	票證業者	商業技術問題

4.2.4 一機多卡整合模式對產業生態的影響

「一機多卡整合模式」可能對電子票證產業生態發生關係轉換的結果。因為若是由運輸業者自行採購驗票設備，則運輸業者將成為具有決策權的一方，現存由票證業者主導的關係，以及各方權益人及營運作業將產生明顯變化。票證業者對於其區域內之運輸業者將由一對多關係(一家票證業者對多家運輸公司)轉化為多對多關係(多家票證業者對多家運輸公司)；電子票證的作業流程與責任角色也必須面臨轉變。本研究認為此議題大致可以分為以下三種轉變：

一、主導權的轉變：由票證業者主導轉變為運輸業者主導

針對主導權之轉變，原本由票證業者主導之作業型態，將轉變為運輸

業者主導，影響之項目容包：票證前台系統建置、票證資訊系統需求、驗票設備採購者、設備維修保固責任與營運邏輯整合與版本更新等事宜，其轉變前後之各項目對照表如表 4-7。

表 4-7 一機多卡整合模式對作業流程與責任角色之影響

項目	轉變前建置方式	轉變後建置方式
資訊作業模式	電子票證委外	運輸業者主導
關係架構	一對多關係結構	多對多關係結構
設備提供	票證業者負責	運輸業者負責
設備維護	票證業者負責	運輸業者負責
系統需求確認	票證業者確認	運輸業者確認
營運邏輯	各區域由票證業者進行整合	各運輸業者將針對各自需求增加

以台北悠遊卡為例，目前由台北悠遊卡公司提供相關驗票設備(包含車上驗票設備，場站管理系統與業者管理系統)給運輸業者，對運輸業者而言，乃將電子票證業務委外。在「一機多卡整合模式」之下，若是由運輸業者自行採購驗票設備，則設備維護之主導權將由台北悠遊卡公司負責，轉變由運輸業者自行負責。

另外，對於賠償責任之主體而言，若由票證業者提供驗票機，一旦驗票設備經過司機開班確認後(完成設備善良管理人之必要檢測操作)，出車途中若發生驗票機故障導致營收短收，其損失由票證業者負責賠償；若驗票設備由業者自行負責，則由運輸業者自行負責。然而即便由運輸業者自行負責，由於驗票設備包含 SAM、Reader Module、GPS 定位、BV 軟體等設備均會交互影響，屆時如何釐清故障的權責，將會是實際運作的灰色地帶，仍需視實務狀況進一步輔以配套措施。

二、營運面的轉變：系統委外夥伴關係轉變為商業談判關係

在票證營運責任與風險分擔方面，若由票證業者來主導，運輸業者僅是票證業者之服務使用者，因此，彼此的關係類似系統委外夥伴關係。

但是票證整合勢必涉及跨區使用，對現在各票證業者具有地域區隔之營運特性勢將有所衝擊，因此，若運輸業者可自行承擔資訊系統及設備管理等風險，將具備與票證業者的談判能力，雙方的關係將由系統委外夥伴

關係轉變為商業談判關係。

三、關係面的轉變：一對多關係轉化為多對多關係票證業者

在「一機多卡整合模式」之下，票證業者與運輸業者的關係，將由目前的一對一關係(一家票證業者對一家運輸公司)轉變為多對多關係(多家票證業者對多家運輸公司)。

由於票證系統結合金流與資訊流，運輸業者之營運調度與運輸管理均與帳務作業息息相關，若票證業者對運輸業者為一對一的關係，其清分作業相對單純；若雙方的關係轉變為多對多，則運輸業者之清分作業與資訊管理負荷均會加重，需要有其它因應配套方案，以利票證整合後之帳務運作。

4.2.5 一機多卡整合模式影響因素之因應作法

針對各項一機多卡整合時所面對之影響因素，本研究進一步提出以下六個因應作法：運輸規範整合、驗證流程整合、交易邏輯整合、交易資訊整合、運輸代碼整合與區域特性宣導。前五項因應作法主要以簡化營運規則與整合作業為方向，而這些簡化營運差異之整合應同時配合宣導，讓民眾了解一機多卡、跨區使用會造成區域性優惠等之差異，以避免民眾誤解而產生民怨。

茲針對以上六項整合因應作法進行說明：

- 一、運輸規範整合：針對運輸業者的營運規範進行整合，彙整出一致性的作業規定與流程，以作為電子票證應用程式開發之依據。公路客運業者由於營運規則具地域性且最複雜，建議可由「中華民國公共汽車客運商業同業公會全國聯合會」(簡稱「全國聯合會」)主導整合，以凝聚客運業者之共識。
- 二、驗證流程整合：針對各家票證業者之驗證流程、SAM 卡存取流程，讀寫模組(Reader Module)等差異進行協商，以期取得最大的共識，確保日後驗證作業之效率與系統開發之效益。
- 三、交易邏輯整合：針對各票證業者營運邏輯差異的部分，建議透過協商進行整合，以減少票證整合之複雜度。
- 四、交易資訊整合：針對各票證業者之資訊格式與通訊規格，建議制定統一之交易資訊架構，並統一相關資訊流與環境設定的參數，如此可大幅減少票證業者與運輸業者維運管理之困擾。

五、運輸代碼整合：針對路線代碼、業者代碼、載具代碼，建議由主管機關統一規定，將有利票證業者、運輸業者資料交換與管理。

六、區域特性宣導：由於目前各地方政府均運用電子票證作為其社會福利政策與獎勵之工具，因此，造成同為優惠票卡，各地方政府補助機制不盡相同。建議透過各票證業者與運輸業者的宣導說明，避免具優惠身分之持卡人跨區使用產生認知差異，徒增民怨。

本研究整理第 4.1 節一機多卡整合的實作案例，對各個影響因素提出以下的建議因應作法，如表 4-8。

表 4-8 一機多卡整合模式影響因素之因應作法

項次	影響因素類型	影響因素	因應作法
1	營運邏輯類		
1.1		一般扣款基本差異	運輸規範整合、交易邏輯整合
1.2		交易紀錄格式差異	交易資訊整合
1.3		轉乘優惠條件差異	運輸規範整合、交易邏輯整合
1.4		特殊作業：解逃票作業差異（特許上下）	運輸規範整合、交易邏輯整合
1.5		特殊作業：路故上、路故下作業	運輸規範整合、交易邏輯整合
1.6		特殊作業：機故上、機故下作業	運輸規範整合、交易邏輯整合
1.7		特殊作業：票卡代墊額度作法	運輸規範整合、交易邏輯整合
2	應用代碼類		
2.1		路線代碼	運輸代碼整合
2.2		業者代碼	運輸代碼整合
2.3		載具代碼	運輸代碼整合
2.4		司機代碼	運輸代碼整合
3	資安控管類		
3.1		讀寫模組(Reader Module)驗證	驗證流程整合
3.2		SAM 錄碼作業 & 押碼作業	驗證流程整合
4	設定環境類		
4.1		時區定義差異	交易資訊整合
4.2		設備參數差異	交易資訊整合

表 4-8 一機多卡整合模式影響因素之因應作法(續)

項次	影響因素類型	影響因素	因應作法
5	清分作業類		
5.1		卡種類別差異	交易邏輯整合、區域特性宣導
5.2		扣點扣錢規範差異	交易邏輯整合、區域特性宣導
5.3		營運求償機制差異	運輸規範整合、交易邏輯整合
6	優惠補助類		
6.1		補助單位差異	交易邏輯整合、區域特性宣導
6.2		優惠記名卡優惠差異	交易邏輯整合、區域特性宣導

依據宏碁公司執行「高雄捷運一卡通與 Taiwan Money Card 一機雙卡整合個案」及「桃園客運與台北客運聯營桃園往返台北國道客運路線一機雙卡整合個案」之案例經驗，不同票證系統跨區使用時，本研究建議票證業者與運輸業者於「營運邏輯與營運模式協商階段」應對以下議題進行協商或談判：

- 一、卡種類別：於跨區使用時，以一般卡種(全票)為原則。
- 二、扣點扣錢規範：於跨區使用時，以扣錢為主，不支援扣點。
- 三、營運求償機制：各運輸業者與票證業者協商。
- 四、優惠卡優惠：社會福利卡等優惠票卡不可跨區使用。
- 五、交易紀錄格式：各運輸業者與票證業者協商。
- 六、轉乘優惠條件：不提供跨區票卡之轉乘優惠。
- 七、解逃票作業：於跨區使用時開放驗票機「自動特許上」功能。
- 八、路故上、路故下作業：不同運輸業者於限定時間內可接受「路故上」。
- 九、機故上、機故下作業：驗票機「機故」時由運輸業者自行規範司機以人工處理方式。
- 十、票卡代墊額度作法：統一代墊額度。

有鑑於以往各票證業者之營運，多以區域性發展為主，各票證業者當初成立時，亦以各區域之交通票證需求為主要目標，其系統架構與設計開發均以滿足各區域之交通發展特性，因此，各票證業者其營運規則及系統功能均為滿足各自服務對象之需求，提供許多客製化設計與區域性服務，造成各票證業者之票卡資料格式與營運邏輯彼此欠缺共通性架構。本研究所提出之因應作法有助於一機多卡整合模式之推動更為順利。

4.2.6 一機多卡整合模式實作案例之實證說明

本研究針對 4.2.1 節「一機多卡整合模式影響因素」探討後，可以發現一機多卡整合的因素，除影響不同層面外，亦涉及不同角色之運作。因此，包括票證業者、運輸業者、系統服務廠商與持卡人使用認知等不同角色之思维，均有所差異。

本研究案假設以運輸業者為票證設備採購主體，分析上述影響因素，可以發現，須透過票證業者間與運輸業者相互合作，方能解決許多衝突與分歧。以下就本研究 4.2.1 節「一機多卡整合模式影響因素」中各項之解決方向，透過 4.1 節實作案例的實際探討，提出各項影響因素之解決作法，如表 4-9。

表 4-9 一機多卡整合模式實作案例影響因素之解決作法

項次	影響因素類型	影響因素	實作案例的解決作法
1	營運邏輯類		
1.1		一般扣款基本差異	運輸業者僅使用里程計費交易，段次計費模式僅支援悠遊卡。
1.2		交易紀錄格式差異	確認彼此之交易紀錄格式與檔案位置並加以區隔，透過系統轉檔，將兩家票證業者所產生之交易檔，分送兩家票證業者後台。
1.3		轉乘優惠條件差異	聯營路線不提供轉乘優惠。
1.4		特殊作業：解逃票作業差異（特許上下）	以臺灣通規範為基礎，使用自動特許上功能。
1.5		特殊作業：路故上、路故下作業	於限定時間內可接受不同運輸業者持卡人路故上。
1.6		特殊作業：機故上、機故下作業	確認機故時不需處理，由運輸業者自行規範司機以人工處理。
1.7		特殊作業：票卡代墊額度作法	透過運輸業者協商，再與兩家票整公司溝通，統一代墊額度。
2	應用代碼類		
2.1		路線代碼	路線代碼由交通部公路總局統一規定。
2.2		業者代碼	兩家票證業者統一業者代碼
2.3		載具代碼	目前無轉乘需求，故不討論載具代碼問題
2.4		司機代碼	固定使用 4 碼。
3	資安控管類		

表 4-9 一機多卡整合模式實作案例影響因素之解決作法(續)

項次	影響因素類型	影響因素	實作案例的解決作法
3.1		讀寫模組(Reader Module)驗證	設備商依據票證業者要求分別進行驗證。
3.2		SAM 錄碼作業 & 押碼作業	悠遊卡為目前唯一經金管會核准之小額付款之票證業者，因此，各版本驗證流程最後均以悠遊卡為最後押碼之單位。
4	設定環境類		
4.1		時區定義差異	暫定統一時區為格林威治時區--台灣時間。
4.2		設備參數差異	各自參數檔分別讀取，透過系統整合成一份整合性之參數，供一機多卡驗票機進行設備參數下載。
5	清分作業類		
5.1		卡種類別差異	扣款邏輯比照一般卡種扣款。
5.2		扣點扣錢規範差異	設備商依據新的營運邏輯開發設計
5.3		營運求償機制差異	運輸業者自行與票證業者討論。
6	優惠補助類		
6.1		補助單位差異	設備商依據新的營運邏輯開發設計。
6.2		優惠記名卡優惠差異	設備商依據新的營運邏輯開發設計。

未來如果新增一個票證系統(即新公司設立)，本研究將其可能發生之概估成本試算項目列出如表 4-10 所示。然必須注意的是，概估成本試算有以下前提：

- 一、估算前提：本成本之估算，係以新加入的票證業者已具備功能完整之清算系統及營運能力為前提，估算其加入運輸業者現行營運中票證設備時，運輸業者應配合修改之相關軟、硬體成本。
- 二、分攤推估原則：運輸業者管理系統(CPS)與場站管理系統(DPS)係以新增一套新的票證業者所需開發之應用系統，其實際之成本分攤應視導入之運輸業者與場站數目而定，數目愈多，所分攤之費用愈低。例如新增一家票證業者管理系統(CPS)之成本為 1,500 萬元，若由十家運輸業者分攤，每套業者管理系統(CPS)分攤費用為 150 萬元；場站管理系統(DPS)之成本為 1,500 萬元，若由五十個場站分攤，每套場站管理系統(DPS)分攤費用為 30 萬元。
- 三、除外費用：業者管理系統(CPS)與場站管理系統(DPS)不包含硬體伺服主機

與作業系統等費用，亦不包含網路傳輸費用與設備保固費用。

四、項目範圍：本成本試算之範圍僅包含各運輸業者之場站設備與車上驗票機，不包含各票證業者針對特定之運輸業者需求，所進行之軟、硬體修改或建置。

五、計價金額：成本概算表以下之計價金額為新台幣，單位「元」。

六、參考資料來源：宏碁公司「高雄捷運一卡通與 Taiwan Money Card 一機雙卡整合個案」及「桃園客運與台北客運聯營桃園往返台北國道客運路線一機雙卡整合個案」。

表 4-10 一機多卡驗票機新增票證系統所需成本概算

成本項目	說明	備註
場站管理系統(DPS)	場站管理系統開發建置，其數量依據場站數量而定，每套新設系統約 1,500 萬元，每個場站實際費用依據分攤數目而定。	1. 如與既有票證業者系統共用硬體，則須增加相容性測試成本。 2. 本估算不包含硬體設備與網路頻寬費用。
業者管理系統(CPS)	業者管理系統開發建置，每套新設系統約 1,500 萬元，每家業者實際費用依據分攤數目而定。	1. 如與既有票證業者系統共用硬體，則須增加相容性測試成本。 2. 本估算不包含硬體設備與網路頻寬費用。
驗票設備應用軟體修改	驗票設備軟體為符合新增票證系統之營運邏輯，所需之開發修改成本，為一次性成本，實際成本依據實際修改需求而定。	修改後之讀寫設備需重新驗證所可能衍生之驗證成本，包括既有之票證系統重新驗證，視修改幅度而定。
讀寫模組應用韌軟體修改	讀寫設備韌體為符合新增票證系統之卡片資料格式，所需之開發修改成本，為一次性成本，實際成本依據實際修改需求而定。	修改後之讀寫設備需重新驗證所可能衍生之驗證成本，包括既有之票證系統重新驗證，視修改幅度而定。
驗票設備與讀寫模組安裝/測試費用	每台每次約 5,000 元	---

表 4-10 一機多卡驗票機新增票證系統所需成本概算(續)

成本項目	說明	備註
SAM 卡購置成本	票證系統 SAM 卡購置成本，實際成本依據各票證系統售價而定。	依據運輸業者與票證業者合約中關於成本分擔規定辦理。
管理成本	運輸業者之管理成本以及導入新的票證系統作業所衍生之成本	運輸業者針對新的票證業者之營運規則、作業流程、對帳作業所需要投入的人力成本。

註：本成本之概算係依據研究期間訪查所得資料，係為編列預算之概估參考，實際建置成本仍須視個案當時實際發生成本而定。

第五章 交通電子票證應用 CPU 卡之探討

非接觸式邏輯加密卡(CSC 記憶卡)憑藉其良好的性能和較低的價格，廣泛應用於交通、醫療、校園一卡通及門禁等領域。由於非接觸式邏輯加密卡晶片採用的是流密碼技術¹，密鑰長度也不是很長(比較典型的密碼長度是 MIFARE 的 48 bit)，因此邏輯加密卡晶片普遍存在著一定的安全隱憂，有被駭客破解的可能。因此在金融、身份識別、電子護照等對安全要求比較高的領域，目前較傾向於使用內嵌微處理器的非接觸式 CPU 卡晶片。依據 2010 年高鐵局桃園國際機場捷運線對非接觸式晶片卡讀寫機的招標規範規定：「...驗票機在設計上，考量日後其中部份票證公司將 CSC 記憶卡改為 CPU 卡後之混搭情形下，仍能運作正常且不影響各種功能與效能」，此亦宣告 CPU 卡將正式跨入交通電子票證的應用領域。

5.1 邏輯加密卡驗票機升級為 CPU 卡驗票機之技術探討

5.1.1 邏輯加密卡升級為 CPU 卡之趨勢與優勢

以下針對邏輯加密卡升級為 CPU 卡之趨勢與與 CPU 卡的優勢，分別說明如下。

一、邏輯加密卡升級為 CPU 卡之趨勢

2008 年曾有德國及美國的學者聯手透過逆向工程的方式，破解 NXP 的 MIFARE 晶片卡特有之 Crypto1 加密演算法；2010 舉辦的第六屆臺灣駭客年會(HIT 2010)中，臺灣大學電機系教授鄭振牟團隊則實作出 MIFARE 的破解方式。臺大團隊使用改進過 Sniffer-Based(監聽封包)的攻擊手法攻擊 MIFARE 卡。其方法是透過 Sniffer 監聽設備，在悠遊卡與加值機進行資料讀取時，透過監聽封包取得相關的卡片資料，將一張實際的悠遊卡，從餘

¹流密碼又稱為序列密碼。在流密碼中，將明文訊息按一定長度分組(長度較小)，然後對各組用相關但不同的密鑰進行加密，產生相應的密文，相同的明文分組會因在明文序列中的位置不同而對應於不同的密文分組。在分組密碼中，明文訊息也是按一定長度分組(長度較大的)，每組都使用完全相同的密鑰進加密，產生相應的密文，相同的明文分組不管處在明文序列的什麼位置，總是對應相同的密文分組。相對分組密碼而言，流密碼主要有以下優點：第一，在硬體實施上，流密碼的速度一般要比分組密碼快，而且不需要有很複雜的硬體電路；第二，在某些情況下(例如對某些電信上的應用)，當緩衝不足或必須對收到的字元進行逐一處理時，流密碼就顯得更加必要和恰當；第三，流密碼有較理想的數學分析工具，如頻譜理論和技術、代數方法等；第四，流密碼能較好地隱藏明文的統計特徵。

額為正 100 多元，更改為負五百多元。

雖然這種攻擊手法只能是單張卡片資料竄改，對於捷運公司而言，防護的方式很簡單，只要能夠在系統後端設備進行防堵措施，例如偵測卡片是否有異常；資料讀取過程中，不要洩露足夠的資訊可供人利用竄改等防護方式。就 MIFARE 卡片作為全世界各國交通票證之主要載體而言，卡片之不容偽造以及其資料之正確性是為其根本考量之一。尤其目前世界各國對於交通票證之應用有擴展至一般小額消費之趨勢，故其卡片本身之安全性更為各國交通票證業者之考量重點。

CPU 卡內含 CPU 與記憶體，可執行動態運算的主動式安全管理，具有無法盜製優點的卡片，亦即其含有一個 CPU 做為資料處理和安全功能，有 RAM 來儲存內部計算，有 ROM 來儲存程式和操作指令，EPROM 或 EEPROM 來儲存卡片的特殊資料的一種卡片。

每張 CPU 卡於出廠時，每個晶片都會有一組獨一無二的序號，所以具有不可複製的獨特性。此外 CPU 卡可提供電子簽章、加解密及儲存憑證等功能。

由於 CPU 卡具有動態運算之能力，因此對於卡片與讀卡設備之間的身份驗證以及資料傳輸，具有動態產生相對驗證碼之能力。也就是說，卡片與設備間之驗證乃是由一方依據其內部儲存之金鑰、動態產生之亂數及其它相對應之資料，進而產生出一組驗證碼。被檢驗方傳輸驗證碼至另外一方，由另一方依據事先定義好之驗算規範，來驗證對方之正確性。如此，所有之金鑰資料將不會出現於兩造溝通之通訊介面，因而外界無法由此而破解其金鑰內容。因此 CPU 卡比 MIFARE 卡片更具有不容易被破解的安全性。

本研究依據各國採用 CPU 卡片來取代 MIFARE 卡片之趨勢，探討我國電子票證應用若採用 CPU 卡來取代現有之 MIFARE 卡片，其技術規範之建議及票證系統的因應做法。

二、CPU 卡的優勢

CPU 卡晶片內部都有雙重安全機制，第一重是晶片本身的加密演算法模組，晶片設計公司通常都會將最安全的幾種加密演算法植入晶片，目前比較常見的安全演算法有 RSA，3-DES 等。中國大陸另開發國密算法

(SSF33，SCB2，SM2，SM3 等)來加強晶片的安全性。國密算法是不對外公開的，比其他公開算法的加密算法具有更高的安全性。第二重保護則是 CPU 卡晶片特有的 COS(Card Operation System)系統，COS 可以為晶片設立多個相互獨立的密碼，密鑰以目錄為單位存放，每個目錄下的密鑰相互之間獨立，並且有防火牆功能(不同目錄下密鑰不會互相影響)。同時 COS 內部還設立密碼最大重試次數以防止惡意攻擊。由此可見，非接觸式 CPU 卡比非接觸式邏輯加密卡具有更高的安全性。

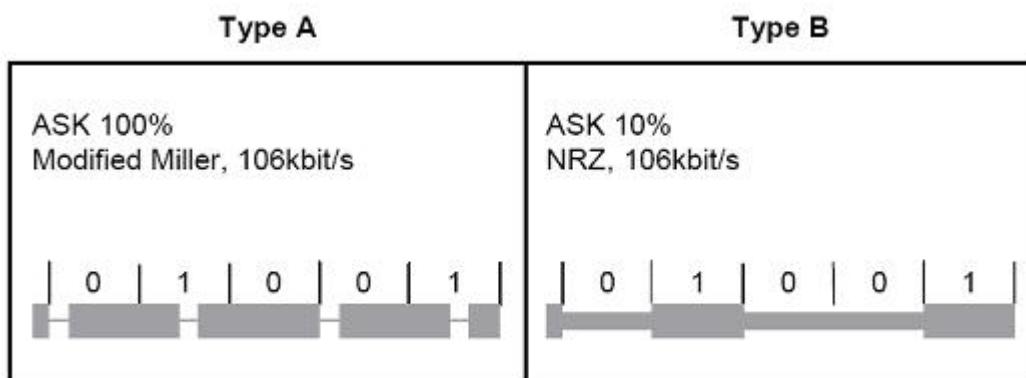
除此以外，CPU 卡可以實現真正意義上的「一卡多用」，每個應用相互獨立並受控於各自的密鑰管理系統。不同應用可以共用一個「錢包」，也可以分別擁有各自的「錢包」。服務商可以透過使用 CPU 卡，進行更加靈活有效的管理，用戶也能使用 CPU 卡實現多功能應用的需求。

5.1.2 CPU 卡的傳輸標準與技術發展

以下針對 CPU 卡的傳輸標準與 CPU 卡之技術發展，分別說明如下。

一、CPU 卡的傳輸標準

目前非接觸式 IC 卡的傳輸標準主要有 ISO/IEC 14443 Type A 和 ISO/IEC 14443 Type B 兩種。Type A 和 Type B 都是 ISO/IEC 14443 規定的標準，都使用 13.56MHz 的載波頻率，最高通訊速率均為 424kbit/s。它們之間最主要的差別在於讀寫器發送射頻信號的載波調製深度不同，Type A 是 100%ASK(Amplitude Shift Keying)調製，而 Type B 是 10%ASK 調製，如圖 5-1 所示：



資料來源：張綱；淺談非接觸式 IC 卡晶片技術的發展趨勢；2010 年 4 月

圖 5-1 TypeA 和 TypeB 載波調製深度

在通訊過程中，Type A 讀寫器發送給卡的能量傳遞是不連續的，會在短時間內中斷，而 Type B 讀寫器發出的能量傳輸是連續的。這種通訊方式會造成 Type A 卡所能接收到的能量較 Type B 少，因此 Type A 晶片電路的設計難度較 Type B 要高，週邊電路也要複雜一些。但是在另一方面，100% ASK 調製發送的信號間區別明顯，抗干擾能力強；而 10% ASK 調製，信號間區別很小，抗干擾能力弱，容易接收錯誤。實際應用中，Type A 類型卡片因其較強的抗干擾能力而在交通、地鐵等領域被廣泛的使用。

Type A 的防衝突機制²是基於 BIT 衝突檢測協議，而 Type B 是通過位元組、幀³及命令來完成防衝突。這兩種防衝突機制在實際使用中都能很好的工作。

TypeA 的防衝突機制為 NXP(原飛利浦半導體)獨家制定，所以標準規則比較明確，各卡廠生產 Type A 類型卡的性能一致性比較高，產品相互間的操作性和相容性比較好。而 Type B 的標準由多家制定，各家的產品可能有所不同，因此相對來說相容性可能不是特別好。此外 Type A 的專利權由 NXP 一家擁有，專利權人比較明確，而 Type B 的專利權則由多家公司擁有，專利權人相對不是很明確。

目前在非接觸式邏輯加密卡市場中，Type A 標準佔有明顯的優勢，在國內市場非接觸式 IC 卡基本上都是用 Type A 技術。因此，目前主流卡廠所生產的非接觸式 CPU 卡傳輸標準還是以 Type A 和 Type B 為主，但展望未來，發展抗干擾能力強，綜合使用環境好，相互操作性和相容性比較好的非接觸式傳輸標準，則更能符合 CPU 卡多用途的設計需求。

二、CPU 卡之技術發展

目前大多數非接觸式 CPU 卡晶片都採用 EEPROM⁴作為資料記憶體，

²所謂「防衝突機制」係指兩張以上非接觸式 IC 卡同時進行讀寫時，防止彼此之間出現資料干擾的機制，使讀寫器可以“同時”處理多張非接觸式 IC 卡。TYPE A 的防衝突機制需要在卡片和讀寫器中分別加入更多的硬體，以擁有處理較精確的時序能力；其防衝突機制係遵循協議的內容，使用標準禎用於資料交換，並由一定的順序組成；TYPE B 的防衝突機制使用位元組、幀和命令的格式，通過字元來發送和接收，具有使用更少的命令，更快的回應速度來實現防衝突和選擇卡片的能力，相較於 TYPE A，而 TYPE B 的防衝突更容易實現。

³在計算機網路和通信領域，幀是一個數字數據傳輸單元，可能包括幀同步序列。幀同步序列的意義在於接收器通過一串特定的連續比特或符號連續來確定一幀的開始和結束。如果接收器在數據傳輸的過程中接入到系統中，它會忽視接收的數據直到它檢測到一個幀同步序列。

⁴ EEPROM 中文稱「電子抹除式可複寫唯讀記憶體(Electronically Erasable Programmable Read-Only Memory)」，EEPROM 不需要用紫外線照射，也不需要取下，就可以用特定的電壓，來抹除晶片上的資訊，以便寫入新的數據。

Mask ROM⁵作為程式記憶體的結構。這樣做的優點是程式讀取速度比較快，也比較穩定，但由於 EEPROM 面積較大，因此晶片成本也較高。

IC 卡發展到非接觸式 CPU 卡階段以後，用戶對非接觸式 IC 卡的多功能應用的要求也越來越高，用戶希望 IC 卡擁有更多的功能，而每個功能都要有足夠的儲存空間來儲存資料。過去那種「EEPROM + Mask ROM」的記憶體結構，不能再滿足未來的應用需求，採用 Flash Memory⁵(快閃記憶體)作為資料記憶體和程式記憶體的儲存介質，將會是未來非接觸式 IC 卡技術的發展趨勢。

Flash Memory 相對於 EEPROM 最大的優勢是面積小，同樣的晶片面積，Flash Memory 擁有更多的儲存空間，這滿足低成本晶片的需要。同時 Flash Memory 比 EEPROM 更容易把容量擴大，這也滿足用戶對大容量儲存的需要。

Flash Memory 相對於 Mask ROM 最大的優勢是可讀寫。由於未來對非接觸式 IC 卡多功能應用的要求越來越高，因此用戶往往會希望 CPU 卡晶片中的程式可以根據具體應用靈活更新，如果使用 Mask ROM 作為儲存介質，必然無法滿足這一需求。而 Flash Memory 則可以儲存隨時下載的程式，以滿足用戶對新功能的需求。

目前 Flash Memory 技術已經被接觸式 CPU 卡晶片所採用，但因為 Flash Memory 在功耗、可靠性、讀寫速度等方面與 EEPROM 相比，仍存在一定的差距，所以目前在非接觸式 CPU 卡中應用的並不多。現在 Flash Memory 技術有向低功耗、高可靠性以及高讀寫速度方向發展的趨勢。隨著 Flash Memory 技術的提升，未來 Flash Memory 應該能夠滿足非接觸式 CPU 卡的需求，並逐步取代現在「EEPROM + Mask ROM」的儲存方式。

5.1.3 邏輯加密卡升級為 CPU 卡之問題探討與因應策略

中國大陸由於經濟快速發展，對於城市公用事業 IC 卡的應用也相對積極，加上 CPU 卡已經有相當成熟的技術，因此，中國大陸住房和城鄉建設部曾提出邏輯加密卡升級為 CPU 卡之問題與解決方案供業界參考，茲說明如下。

⁵非揮發性記憶體又分為兩種，一種是罩幕式唯讀記憶體〈Mask ROM〉，其資料在寫入後便不能修改，最有名的用途就是在任天堂 Nintendo 64 遊戲機軟體的應用上。另一種則是快閃記憶體〈Flash Memory〉，其寫入的資料可以隨意修改，目前最主要的用途就在於手機上的晶片。

一、邏輯加密卡升級為 CPU 卡問題之探討

針對邏輯加密卡升級為 CPU 卡的問題，可以從資料、清算、系統、應用與實施等五個角度來進行問題探討，分述如下：

1. 資料的角度

將邏輯加密卡的資料和 CPU 卡的資料進行區分是一個可行的解決方法。它既兼顧了資料的獨立性與安全性，同時為未來取消邏輯加密卡後，卡片資料的維護奠定基礎。

2. 清算的角度

將邏輯加密卡的資料和 CPU 卡的資料進行區分，將有助於資料的明確劃分和對帳，也便於對問題資料的定位。

3. 系統的角度

同時進行系統軟體和硬體中嵌入式軟體的開發，並且在系統正式使用前進行充分的測試，將可有效的避免邏輯加密卡和 CPU 卡共存的情況下，系統發生衝突的問題。

4. 應用的角度

儘量維持原有操作介面，將大部份的代碼轉換藉由程式完成，以避免重覆作業的問題。

5. 實施的角度

先執行硬體設備的軟體更新，再升級系統軟體，如此有助於轉換期間系統的穩定。

二、邏輯加密卡升級為 CPU 卡的解決方案之探討

在技術上，要將邏輯加密卡驗票機升級為可讀寫 CPU 卡是可行的，但仍必須經過實作及驗證的過程，方能確認是否符合商業運轉的條件。以下為就理論架構上之升級作法，必須考量之重點加以證明。

1. 生產驗票機時，須預估未來足夠將邏輯加密卡驗票機升級為可讀寫 CPU 卡時重新分配所需的記憶體儲存空間，根據原有邏輯加密卡和 CPU 兩種卡的消費流程，進行優化程式結構，確保驗票機的程式空間能滿足升級需要。

2. 更換/升級所有的 ISAM 卡/PSAM 卡，新的 ISAM/PSAM 卡必須保留支援原先邏輯加密卡金鑰的所有功能，同時由票證公司在 ISAM 卡中加入非接觸式 CPU 卡金鑰，逐步發行非接觸式 CPU 卡來替換現有的邏輯加密卡，在一定時期內保持非接觸式 CPU 卡和邏輯加密卡雙軌並行，並在邏輯加密卡的金鑰失效期前完成非接觸式 CPU 卡的轉換。也可在驗票機內保留原先支援邏輯加密卡的 PSAM 卡，並加裝支援非接觸式 CPU 卡的 PSAM 卡，票證公司新發行的卡片只限定為非接觸式 CPU 卡，然後逐步將邏輯加密卡升級為 CPU 卡，待時機成熟時，逐步淘汰邏輯加密卡。
3. 驗票機的韌體必須確保能使邏輯加密卡和 CPU 卡完全相容，並須注意刷卡速度，避免因相容二種卡而產生的交易時間遞增的現象。
4. 重新規劃通訊協定，提高驗票機上下傳資料及黑名單下載速度，使下載速度提高二倍以上。

此外，由於既有卡片與設備均須配套升級，因此在卡片與讀卡機的相容性測試、多用途設計和開放平臺與安全性與交易速度的權衡三方面，均需要有完整規劃，以下分此三方面說明如下：

1. 卡片與讀卡機的相容性測試

雖然 ISO 和眾多規範已經定義非接觸式 CPU 卡和讀卡機之間的電氣特性和通訊協定，但是同一種讀卡機，可能會無法支援不同卡片廠商的卡片；同一個卡片廠商的卡片，可能在這台讀卡機上能正常交易，在另一台讀卡機上卻無法使用。甚至，同一張卡片，和同一台讀卡機，做某一種交易能成功，做另一種交易卻失敗。究其原因，乃因驗票設備提供商對卡片規範的理解有差異，也與個別廠商的技術能力有關。因此，要成功實施非接觸式 CPU 卡轉換，大量、深入、全面的現場壓力測試，是克服卡片和讀卡機相容性問題的不二法門。

2. 多用途設計和開放平臺

採用非接觸式 CPU 卡的一個很重要的原因，就是可以支援很多的應用，並可定義不同應用的交易流程。在多用途的設計階段，如何儘量符合已有的規範，更開放地適應不同供應商，是非接觸式 CPU 卡專案能否長期順利的推廣的重要因素。

3. 安全性與交易速度的權衡

安全性和交易速度是非接觸式 CPU 卡應用上無法兼顧的問題。快捷的交易速度是採用非接觸式 IC 卡的一個重要原因。但是，為追求交易速度而犧牲安全性卻是一個不明智的作法。而提高安全性往往又必然須要耗費一定的交易時間，降低交易的速度。因此，為兼顧安全性和交易速度，系統的設計者必須根據實際的業務需要，取得最佳的平衡點。在考慮安全性和交易速度的同時，尤其在進行交易速度優化之後，特別需要進行全面的流程測試和異常交易測試，確保交易速度的優化不會影響各個交易階段的安全性。

三、MIFARE Plus 之升級方案之探討

為因應中國大陸之市場需求，NXP(原飛利浦半導體)對中國大陸城市公用事業 IC 卡提出以 MIFARE Plus 作為 CPU 卡升級的解決方案，MIFARE Plus 可輕易升級現有卡片的安全級別。在升級到新的安全級別之前，MIFARE Plus 是唯一相容 MIFARE 4K(MF1ICS70)，MIFARE 1K(MF1ICS50) 和 MIFARE Mini(MF1ICS20)的主流產品。安全性升級後，MIFARE Plus 使用 AES 進行認證、資料完整性和資料加密操作。MIFARE Plus 的介面和加密方式是基於安全級別最高的全球開放式標準，目前 MIFARE Plus 有可用兩個版本：MIFARE Plus S(MF1SPLUSx0y1)和 MIFARE Plus X(MF1PLUSx0y1)。MIFARE Plus S 是 MIFARE Classic 系統直接向前相容的標準版本。MIFARE Plus X 可以更靈活地優化速度和保密性。MIFARE Plus 與 MIFARE Classic 卡片性能對比如表 5-1。

表 5-1 MIFARE Classic 與 MIFARE Plus 卡片性能對比

技術指標	MIFARE Classic	MIFARE Plus
執行標準	ISO14443-3 TYPE A	ISO14443(所有協定，1~4 層)
工作頻率	13.56MHz	13.56MHz
卡片類型	邏輯加密卡	CPU 卡
卡片容量	1 Kbyte 或 4 Kbyte	2 Kbyte 或 4 Kbyte
CPU/作業系統	沒有	有
UID 號	4 位元組	4/7 位元組可設
硬體加密	Crypto1	Crypto1，AES
國際安全認證	---	CC/EAL 4+
特性	---	與 Classic 卡片儲存結構相容
升級級別	---	支援 0~3 安全等級

表 5-1 MIFARE Classic 與 MIFARE Plus 卡片性能對比(續)

技術指標	MIFARE Classic	MIFARE Plus
資料結構	Sector (Block)	Sector (Block)
是否破解	已破解	未破解
成本	較低	較高

以下為 MIFARE Plus 之特性與優點之重點說明。

1. MIFARE Plus 之特性

- (1) 2 或 4KB EEPROM；
- (2) 簡單的固定儲器結構，與 MIFARE Mini，MIFARE 1K，MIFARE 4K 相容；
- (3) 記憶體結構與 MIFARE 4K 相同；
- (4) 可隨意配置驗證條件；
- (5) 支援 ISO/IEC 14443-A 唯一序列號(4 或 7 位元組)，支援任意隨機 ID；
- (6) 多磁區認證，多塊讀和寫；
- (7) AES 用於認證、加密和驗證資料完整性；
- (8) 防撕裂保護；
- (9) 密鑰可儲存為 MIFARE CRYPTO1 密鑰(2×48 位元/磁區)或 AES 密鑰(2×128 位/磁區)；
- (10) 完全虛擬卡概念；
- (11) 中繼攻擊檢查；
- (12) 通信速率可達 848 Kbit/s；
- (13) 單獨寫操作次數：通常為 200,000；
- (14) 通過 CC(Common Criteria) EAL4+。

2. MIFARE Plus 之優點：

- (1) 卡片相容：向下相容 MIFARE Classic S50、S70 卡；
- (2) 升級模式：具備 4 級安全級別模式，可靈活升級；
- (3) 加密演算法：採用 AES 強加密身份驗證；

- (4) SAM 卡片：可擴展 SAM 卡加強安全等級；
- (5) 安全性：通過 EAL 4+認證；
- (6) 序列號：4 或 7 位元組可設，支援隨機識別模式；

四、中國大陸邏輯加密卡(M1)卡升級方案探討

中國大陸住房和城鄉建設部對城市公用事業 IC 卡如何由邏輯加密卡(M1)卡升級為 CPU 卡提出三種解決方案建議，分別是：(1)加強 M1 卡安全應用系統方案；(2)CPU 卡兼容 M1 卡應用系統方案；(3)CPU 卡替換 M1 卡應用系統方案，說明如下。

1. 強化 M1 卡片安全應用系統方案

MIFARE Classic (俗稱 M1 卡，為 MIFARE S50 和 MIFARE S70 卡) 是 NXP (前身是飛利浦半導體)提供的邏輯加密卡晶片。此類卡片以其較低的價格、較靈活的應用等優勢，使其在小額消費、身份識別領域具有高度的市占率，全球的發卡量在 10 億張以上。

(1) M1 卡加密法被破解後的可能出現的風險

M1 卡的加密過程被破解，是由於其採用過於簡單的加密演算法、過於短的金鑰位數(48bit)和可被控制的亂數發生機制。因此，在 M1 卡之安全產生問題後可能出現的風險如下：

A. 偽造卡的出現：

M1 卡晶片被攻破後，製作偽卡的技術也被公開。在目前全球技術快速流通的情況下，能夠生產各個類型偽卡的群體將不可忽視。簡言之此類風險是持卡人複製自有的卡，在卡片離線狀態使用的情況下，持卡人將可能重複使用。

B. 盜用卡的出現

由於 M1 卡採用非接觸方式，在操作過程中，資料可在傳輸中被輕易獲取。同時，由於加密演算法的攻破，即可獲得資料的明文。不法分子可以通過在驗票設備的周圍安裝裝置，在持卡人不知情的情況下獲得所持卡片的資料，再製作偽卡。此類風險是不法分子非法複製正常持卡人的卡片，並持卡消費。

C. 重複交易

由於 M1 卡產生亂數機制的缺陷，可以在使用環節中控制亂數的產生。持卡人可以在正常使用卡片之後，透過事後重演亂數的技術，將交易資料再次傳送給卡片，完成卡片的重複加值或恢復卡使用前的狀態，透過專用設備，可能得以重複使用合法的交易資料，以進行重複交易。

D. 偽造身份

由於偽卡的出現，原本依賴於 UID 序號進行身份識別的方式將不再可靠。由於偽卡的出現，UID 序號將不再唯一，製作、複製相同 UID 序號的卡將較容易實現。

(2) 建設事業 IC 卡金鑰管理系統的安全性

而中國大陸之金鑰管理規範由建設事業 IC 卡金鑰管理系統進行主導，其安全性說明如下：

A. 多層級金鑰管理機制

採用多層級金鑰管理，部會級金鑰和城市級金鑰間採用不可逆的分散演算法，分別由不同的機構管理。而寫入用戶卡的金鑰，是由城市金鑰對用戶卡的序號等每卡唯一的資料分別對應，即使用戶得到某張卡的金鑰，也不能得到系統密鑰，不能用於製作其它 UID 號的卡。

B. 基於 128bit 金鑰長度的 3DES 金鑰安全演算法

金鑰的分散和母金鑰產出採用 128bit 金鑰長度的 3DES 對稱演算法。3DES 的演算法是 DES 演算法的增強，DES 演算法是公開演算法，但其設計原理並未公佈。

C. 消費金鑰和儲值金鑰的分離

對於中國大陸一卡通系統而言，消費和儲值是最主要的二類業務。通常消費金鑰由住房和城鄉建設部發出，而儲值金鑰則由各城市自己產出。在消費環節中一般只出現消費金鑰，而儲值環節往往有較嚴格的安全控制，儲值金鑰在儲值環節被暴露的可能性，主要來自於儲值環節安全管理的疏漏。

D. 一卡一密

對於城市一卡通系統，寫入使用者卡的金鑰是分散後的，分散的資料包含每張卡的 UID 序號。在 UID 號被複製的偽卡出現前，用戶一般只能透過攻擊一張用戶卡，得到對一張卡的控制，而不能影響整個系統的安全。

E. 採用 PSAM 和認證碼的安全控制

建設系統消費環境中，使用者卡金鑰的取得，依賴於 PSAM 對金鑰的計算。PSAM 在計算金鑰時，透過驗證機制驗證卡片認證碼的安全。而卡片認證碼的產生，依賴 UID 號的唯一性。

採用 PSAM 的驗票設備，在計算用戶卡金鑰的過程中，驗票設備內部可以取得被操作用戶卡的金鑰，所以在取得含有 PSAM 的驗票設備的控制之後，可以取得某張用戶卡或一系列使用者卡的金鑰資料。在 UID 號可被複製的情況下，透過對含有 PSAM 的驗票設備的控制，可以製作出被系統接受的使用者卡。

(3) 應用系統應有的防範機制及控制方案

中國大陸卡片交易安全體系中對於未來的潛在性威脅，認為安全體系並不僅僅依賴於卡的安全性高低，而是應定義一套卡片驗證策略，用於驗證卡片的前一筆操作，並將本次操作的摘要資訊寫入卡中。若卡片驗證失敗，立即停止對卡片操作。卡片驗證策略的構成，由指定驗證因數、提供產出規則、卡片商提供摘要載體等三方組成。驗證策略強制部署在系統內部的所有機具和驗票設備，且可以連線更新。

A. 應有的防範機制

- a. 系統監控機制：目前系統中保留半年和最近 20 筆的交易資料，能夠判斷卡片交易重複性和合法性。
- b. 黑名單管理：監控偽卡的使用，對於有異常交易的帳戶，透過下載黑名單對非法卡進行攔截，同時由發卡公司配合對偽卡的持有人進行記錄。
- c. 交易模式：提供連線模式，要求持卡人輸入連線交易密碼，

能夠有效彌補離線交易在終端環節安全的不足。

B. 應用安全的建議措施

- a. 為防止非法卡進行惡意消費，建議限制離線大額消費。
- b. 為防止離線退卡非法獲利，建議退卡等儲值類業務採用連線模式。
- c. 加強消費和儲值場所的監控，建議在一些重要的場所安裝攝影機，作為捕獲偽卡的輔助追蹤工具。
- d. 建議卡內增加加密資料，在交易完成後對交易的結果，用SAM卡進行加密保存在卡內。除可以防範複製卡以外，並可降低卡片金鑰被攻破可能對單張卡造成的風險。

C. 應用安全的防範措施

a. 帳戶管理及跟蹤

IC 卡片的帳戶管理及有效跟蹤，包含與清算系統的資料一致處理、黑名單產出和下載。對於異常卡交易(非法儲值、偽造卡片和複製卡片等)，將該卡設定為可疑狀態，同時通過人工審核，確認是否將該卡納入為黑名單。系統會將黑名單傳送到驗票設備中，驗票設備對黑名單進行保存。當有卡片消費時，消費機具會根據驗票設備中的黑名單，對卡片進行篩選，若發現正在消費的卡片在黑名單中，則對卡片進行鎖卡操作，使之不能再次使用。

b. IC 卡的生命週期管理

IC 卡生命週期係指由原始自發卡狀態-使用狀態-回收狀態時的資料對應和物流管理。票證公司會透過制定卡片有效期的方式進行管理。當卡片的有效期屆滿後，卡片將不能在消費機具上進行消費，必須到票證公司指定的儲值網點進行儲值或年檢，使卡片有效期順延。票證公司可以透過卡片的儲值或年檢，對卡片進行再次的檢查和管理。縮短卡片有效期，可一定程度上彌補卡片被非法複製的行為。

D. 強化卡片安全應用系統方案之重點

- a. 改善消費記錄 TAC 的驗算能力
 - b. 改善即時線上的儲值環境
 - c. 較大額消費的連線驗證能力
- E. 強化卡片安全應用系統方案之缺點

此一方案會影響持卡人使用，如上車刷卡時間延長等。不能百分百的杜絕複製卡片的行為。

2. CPU 卡片兼容 M1 卡應用系統方案

中國大陸在 CPU 卡升級議題上，同樣有討論到兼容既有 M1 卡之方案，針對既有 M1 之產品兼容並同時逐步升級，希望可以減輕升級之不便，此一方案將非接觸式 CPU 卡逐步取代系統已發行並正在使用的非接觸式邏輯加密卡，逐步完成從現有的邏輯加密卡到 CPU 卡的升級。升級過程允許邏輯加密卡與 CPU 卡共同存在、共同使用，轉換期間內，可以結合交通卡的日常工作逐步改造儲值和消費機具。在不影響邏輯加密卡應用的情況下完成改造。完成改造後的卡系統，將完全使用 CPU 卡介面儲值和消費，並可視情況停止現有邏輯加密卡的發行而專門發行 CPU 卡。

此一方案需要確保升級過程的平順，不能因改造過程而影響已發行卡片的使用，必須能夠在支援 CPU 卡操作的驗票設備進行操作，並且確保升級過程中不影響現有系統的正常清分和結算。升級過程避免要求隔天完成所有驗票設備升級工作。具體過程可以遵循驗票設備生命週期，或者結合交通卡的業務，採用逐步改造的方式，在更換新驗票設備或者因業務需要調整驗票設備功能時，加入 CPU 卡操作功能並且不影響現有邏輯加密卡使用。

本 CPU 卡系統升級改造方案擬採用一次發卡，驗票設備逐步改造的方式。升級改造以兼容邏輯加密卡的 CPU 為基礎，在發卡階段關閉 CPU 卡介面(將 CPU 應用鎖定)。待儲值驗票設備完成升級後，經由後臺開啟或時間設定等方式，開啟卡片的 CPU 部分，此時 CPU 卡自動關閉邏輯加密部分儲值許可權，邏輯加密部分只擁有消費許可權。扣款設備優先使用 CPU 介面進行扣款。待各種驗票設備升級完成後，再關閉 CPU 卡邏輯加密介面，逐步廢除邏輯加密卡後升級工作即告完成。

本系統升級技術可分成以下八個步驟說明：

- (1) 以 CPU 卡為基礎，更改發卡系統，使其能夠發行帶有邏輯加密卡功能的 CPU 卡。發行的同時暫時鎖住 CPU 應用(此時卡片作為普通邏輯加密卡使用)。
- (2) 改造儲值系統，增加 CPU 卡線上啟動功能和 CPU 卡儲值功能。
- (3) 在完成第二步的基礎上，卡片 CPU 部分啟動以後，對於 CPU 卡僅支援可從 CPU 介面進行儲值操作，並可以同時支援 CPU 卡介面消費和現有的邏輯加密卡消費設備交易。此時，卡片的儲值安全等級提高到 CPU 卡層級。
- (4) 在上一個步驟完成後發行的 CPU 卡，無需鎖定 CPU 卡應用，並直接關閉其邏輯加密、部分的儲值功能。
- (5) 試運行成功後，將不再發行邏輯加密卡並逐步將其回收。
- (6) 逐步改造所有前端設備，支援 CPU 卡操作功能。
- (7) 在完成上述步驟(6)的基礎上，前端設備可線上關閉 CPU 卡的邏輯加密卡部分。此後，相容邏輯加密卡的 CPU 卡作為純 CPU 卡使用，新發行的 CPU 卡不必再具備邏輯加密卡功能。
- (8) 在完成邏輯加密卡回收的工作之後，停止邏輯加密卡的使用，在必要時可刪除驗票設備邏輯加密卡操作功能。

以下說明 CPU 卡兼容 M1 卡應用系統方案的作業重點：

- (1) 制訂相容邏輯加密卡的 CPU 卡技術規範和應用規範。
- (2) 制訂 CPU 卡應用結構和交易流程規範。
- (3) 建設符合上述流程和規範的 CPU 卡模擬測試系統。
- (4) 完成發卡系統的升級改造。
- (5) 先試辦發行相容邏輯加密卡的 CPU 卡。

3. CPU 卡替換 M1 卡應用系統方案

IC 卡整合的最終目標，是以一卡通的非接觸式 CPU 卡替換掉現有的 M1 卡。整合工作採用並存移轉、逐步替代的實施策略，確保在轉換

期間內不會對持卡人造成較大影響。

(1) 系統改造原則

針對 CPU 卡替換 M1 卡應用系統方案之改造原則說明如下：

- A. 保障 IC 卡持卡人的權益，確保可在系統轉換期間正常使用。
- B. 確保改造中新舊系統順利轉換，改造後系統安全可靠運行。
- C. 改造方案在財務面必須可行，以保障原有系統投資者的權益，盡可能充分利用原有設備。
- D. 改造後系統具有開放性、標準性、先進性、實用性等技術特點。
- E. 提供良好的系統可擴展性，便於系統升級擴展。

(2) 系統改造實施策略

為了將原有 IC 卡系統平穩轉換到 CPU 卡系統，在遵循系統改造原則前提下，改造實施策略基本概括為：業務平穩、技術可行、成本最少、風險最低等四項。

(3) 系統改造的技術措施

技術措施是系統改造目標實現、改造原則保障、改造策略落實的關鍵。系統改造的具體技術措施包括：

- A. 兩卡一機：透過驗票設備的改造，允許在一定時間的轉換期間內，CPU 卡和 M1 卡同時在車載驗票設備上使用。
- B. 逐步替換：在轉換期間內，透過 M1 卡退卡和 CPU 卡發售兩個步驟，逐步將 M1 卡替換為 CPU 卡。
- C. 雙系統並行：在轉換期間內，新的票證結算系統(簡稱 CPU 卡結算系統)和現有的結算系統(簡稱 M1 卡結算系統)並行運轉，分別處理 CPU 卡交易資料和 M1 卡的交易資料，轉換期結束後，關閉現有的結算系統。

建議票證連線儲值前端設備採用參數控制，系統可根據 CPU 卡發行業務狀況，於適當時間逐步關閉 M1 卡的儲值功能。如此可避免更換 M1 卡時可能出現的業務壓力，又可靈活地控制轉換期間的週期，避免 M1 卡不安全因素在系統中的長期存在。

以下說明 CPU 卡替換 M1 卡應用系統方案的作業重點：

(1) CPU 卡替換 M1 卡方案之技術實施內容包括：

- A. 車載驗票設備的改造。
- B. CPU 卡結算系統的建置。
- C. CPU 卡應用的開發。
- D. 現有 M1 卡的處理。

(2) CPU 卡替換 M1 卡方案於轉換期間內，系統的組成部分及主要功能如下：

- A. 車載驗票設備：同時支援 CPU 卡和 M1 卡刷卡乘車。
- B. 業者管理系統：營收資料收集系統可以同時收集 M1 卡資料和 CPU 卡資料，業者管理系統能區分 M1 卡資料和 CPU 卡資料，分別傳輸到 M1 卡結算系統和 CPU 卡結算系統；
- C. 黑名單：下載 CPU 卡和 M1 卡兩種黑名單。
- D. 結算系統：保留目前既有系統，以處理 M1 卡交易資料，不再發售及儲值 M1 卡。處理 CPU 卡的系統交易資料並與清算中心對帳。

(3) CPU 卡替換 M1 卡方案轉換期間結束後，主要功能如下

- A. 車載驗票設備：只接受 CPU 卡。
- B. 業者管理系統：營收資料收集系統收集驗票設備交易資料(只存在 CPU 卡資料)，傳輸到 CPU 卡結算系統，下載 CPU 卡黑名單。
- C. CPU 卡結算系統：處理 M1 卡的系統交易資料並與清算中心對帳。
- D. CPU 卡服務網點系統：受理 CPU 卡特殊卡種的乘客業務服務，包括發售、退卡、掛失、換卡等。

(4) CPU 卡替換 M1 卡方案對車載驗票設備的改造工作，主要事項包括：

- A. 在驗票設備中安裝 PSAM 卡。
- B. 升級部分既有驗票設備的硬體，使之可以同時支援對 CPU 卡和 M1 卡的讀寫。

C. 對車載驗票設備程式進行修改，使之可以處理 CPU 卡的扣款消費，並與 M1 卡資料進行區分。

(5) CPU 卡替換 M1 卡方案對業者管理系統的改造工作，主要事項包括：

- A. 修改營收資料收集程式，使之可以從驗票設備中區分並讀取 CPU 卡和 M1 卡資料數據。
- B. 修改業者管理系統程式，能夠對 CPU 卡資料和 M1 卡資料分別封裝，並分別傳輸到 CPU 卡結算系統和 M1 卡結算系統。
- C. 業者管理系統能夠接收 CPU 卡黑名單和 M1 卡黑名單，並在收集營收資料時下載到伺服器中。

(6) CPU 卡替換 M1 卡方案系統轉換作業重點如下：

- A. M1 卡系統資料移轉：現有生產系統有大量的關鍵資料及參數資料，在資料轉換過程中，必須確保上述資料能準確的轉換到清算系統，避免出現資料遺漏、重複。
- B. CPU 卡系統與 M1 卡系統的轉換。
- C. M1 卡的更換。
- D. 確保系統的連續性：在確保資料一致性的同時，還須保證系統業務營運在新舊應用系統改造轉換實施過程的連續性，不會發生任何因環境改變而使生產的連續性被中斷。

(7) CPU 卡替換 M1 卡方案系統轉換過程中應注意的問題如下：

- A. 方案可行性問題。
- B. 相容性問題。
- C. 轉換平順性問題。
- D. 各業務一致性問題。

5.2 交通 CPU 卡技術規範發展與現況之探討

5.2.1 國際金融/信用卡的主要技術標準--EMV

EMV 規範是由 Europay、MasterCard、VISA 三大國際信用卡組織聯合制定的金融集成電路(IC)卡的金融支付標準，目的是為金融 IC 卡、金融終端、支付系統及金融機構建立一個統一的標準平臺。在此國際標準規範中，對於晶片卡的介面標準，則有相當比例係根據ISO 7816所完成。

Europay國際公司於 2002 年併入萬事達卡。JCB(前身為日本信用局)於 2004 年 12 月加入 EMV 組織。EMV 規格原為 EMV96 Version 3.1.1，EMVCo 組織於 2000 年 12 月公告 EMV 2000 Version 4.0，2004 年 5 月公告 4.1 版。故目前正式發布的版本有 EMV96 和 EMV2000。

EMV2000 標準是國際上金融 IC 卡借記/貸記應用的統一技術標準，主要內容包括借/貸記應用交易流程、借記/貸記應用規範和安全認證機制等。EMV 導入是指按照 EMV2000 標準，在發卡、業務流程、安全控管、受理市場、訊息轉接等多個環節，實施銀行磁條卡向集成電路(IC)卡的技術升級，利用安全性更高的智慧 IC 卡，來有效防範諸如製作和使用假信用卡、信用卡欺詐、跨國金融詐騙等高科技金融犯罪。

EMV2000 的規範分成四冊，分別是：

第一冊 應用獨立 ICC 到終端介面的要求(Book 1 Application Independent ICC to Terminal Interface Requirements)；

第二冊 安全和密鑰管理(Book 2 Security and Key Management)；

第三冊 應用規格(Book 3 Application Specification)；

第四冊 持卡人、服務員和取得介面的要求(Book 4 Cardholder, Attendant, and Acquirer Interface Requirements)。

各冊內容大綱請參閱附錄三。

5.2.2 中國大陸交通電子票證 CPU 卡規範發展與產業現況

2009 年中國大陸無論是城市公共交通 IC 卡的建設，還是城市一卡通都已蓬勃的發展，截至 2009 年 10 月為止，全國共有 224 個城市建立不同規模的 IC 卡

系統，發卡量近 1.7 億張，並以 10%的速度遞增。全國直轄市以及絕大部分省會城市均建立 IC 卡一卡通系統，地方級城市 IC 卡覆蓋率近 60%。據統計，在全國 224 個應用 IC 卡系統的城市中，有 90%的城市使用的是邏輯加密卡。但隨著邏輯加密卡的安全問題越來越引起各地 IC 卡主管部門及營運單位的高度重視，在住房和城鄉建設部 IC 卡應用服務中心(以下簡稱「部 IC 卡服務中心」)指導之下，先後有上海、合肥、西安、銀川、昆山、江陰等城市完成 IC 卡系統升級改造。為全面推動城市公用事業 CPU 卡的應用奠定基礎，目前，全國 CPU 卡發卡總量已近 2500 萬張。

一、中國大陸交通電子票證 CPU 卡技術規範發展

中國大陸政府對推動 CPU 卡之規劃由「部 IC 卡服務中心」推動，其工作重點方針為：(一)規範標準先行；(二)各項流程一致；(三)金鑰管理統一；(四)城市互聯互通。根據以上的方針，「部 IC 卡服務中心」制定適合城市公用事業 IC 卡應用要求的積體電路卡片、晶片、設備、技術及應用的國家產業標準，緊密圍繞安全核心，內容涉及卡片、驗票設備和系統設計等 IC 卡產業鏈的各個環節，確實解決城市公用事業 IC 卡跨行業、跨城市、跨區域的應用問題，建立完善的標準體系，有效的確保整個城市公用事業 IC 卡的發展。各發展階段制定的標準如下：

1 2009 年之規範標準發布如下：

- (1) 《建設事業 CPU 卡作業系統技術要求》(標準號：CJ/T 304—2008)

該標準自 2009 年 6 月 1 日起正式實施。該標準規定建設事業 CPU 卡機電特性、邏輯介面與傳輸協定、檔和命令、應用選擇、安全機制及安全要求、電子存摺/電子錢包應用和相應的定義符號等。

- (2) 《建設事業非接觸式 CPU 卡晶片技術要求》(標準號：CJ/T 306-2009)

該標準規定了建設事業非接觸式 CPU 卡晶片相容性要求(主要是與 ISO/IEC 14443-3 TypeA 的相容性要求)、防衝突指令、晶片基本性能、晶片微處理器要求、加密演算法、記憶體要求、安全特性、建設事業非接觸式 CPU 卡安全認證碼等。

2. 2010 年 10 月之規範標準發布如下：

- (1) 《城市公用事業互聯互通卡通用技術要求》(標準號：CJ/T331-2010)
- (2) 《城市公用事業互聯互通卡清分清算技術要求》(標準號：

CJ/T332-2010)

(3) 《城市公用事業互聯互通卡密鑰及安全技術要求》(標準號：CJ/T333-2010)

透過以上標準之訂立，「部 IC 卡應用服務中心」進一步提出城市公用事業 IC 卡的互聯互通，並作為國家金卡工程之具體目標。從 2009 年 1 月 1 日起，對於新建 IC 卡系統城市、改造升級城市和互聯互通城市，均要求採用符合住房和城鄉建設部標準的 CPU 卡以及採用互聯互通密鑰；凡進行城市公用事業 CPU 卡升級的城市，必須要到住房和城鄉建設部進行備案和登記。

同時，自 2009 年 10 月 1 日起，對 CPU 卡晶片安全初始化費用大幅下調，各廠商提供的 CPU 卡成本價格也隨之調降，為 CPU 卡在城市公用事業領域大範圍推廣奠定基礎。

二、中國大陸交通 CPU 卡與 EMV 規範的關聯性

中國大陸住房和城鄉建設部於 2009 年頒佈《建設事業非接觸式 CPU 卡 COS 技術要求》，建議交通運輸業者應用 CPU 卡為扣款載具時，能共同遵循此一標準，以利全國票證技術統一、擴大建立經濟規模以降低使用成本。

《建設事業非接觸式 CPU 卡 COS 技術要求》的規範重點如下，各項重點大綱請參閱附錄七。

1. CPU 卡 COS 範圍；
2. 規範性引用檔；
3. CPU 卡 COS 定義；
4. CPU 卡 COS 縮略語和符號表示；
5. CPU 卡 COS 機電特性、邏輯介面與傳輸協定；
6. CPU 卡 COS 資料元和命令；
7. CPU 卡 COS 應用選擇；
8. CPU 卡 COS 安全機制；
9. CPU 卡 COS 電子存摺/電子錢包應用。

中國大陸人民銀行頒布的《PBOCv2.0 規範》是以 EMV 的規範為制定基準，自稱為繼 VISA 標準、MASTER 標準、JCB 標準之後世界上第四部銀行卡產業標準規範。該標準不僅適用於中國大陸有關銀行和金融機構，也可在全球適用。該規範符合 EMV 新的資料加密技術和安全演算法，卡內的 CPU 具有獨立運算、加解密和儲存等能力，晶片內的作業系統具有極高的安全性，在保證 IC 卡與外界進行資訊交換的同時，也保證了卡內資料的安全。在離線交易方面，透過驗票設備讀取卡片資訊，即可以驗證卡片的真偽，也可以與收單行系統進行連線認證，大幅提高銀行卡支付的安全性，減少詐欺行為。同時，考慮到中國大陸國情的特殊需求，該新規範在身份認證等方面不同於 VISA、MASTER，而擁有自己的特色。

《PBOCv2.0 規範》的規範重點如下，其各重點大綱請參閱附錄七。

第 1 部分：電子錢包/電子存摺應用卡片規範；

第 2 部分：電子錢包/電子存摺應用規範；

第 3 部分：與應用無關的 IC 卡與終端介面規範；

第 4 部分：借記/貸記應用規範；

第 5 部分：借記/貸記應用卡片規範；

第 6 部分：借記/貸記應用終端規範；

第 7 部分：借記/貸記應用安全規範；

第 8 部分：與應用無關的非接觸式規範；

第 9 部分：電子錢包擴展應用指南；

第 10 部分：借記/貸記應用個人化指南；

第 11 部分：非接觸式 IC 卡通訊規範；

第 12 部分：非接觸式 IC 卡支付規範；

第 13 部分：基於借記/貸記應用的小額消費規範。

《PBOCv2.0 規範》中將小額消費工具分為電子錢包(第一、二、九部分)及電子現金(第十三部分)，此二者雖然對持卡人而言幾乎沒有區別，但是就卡片技術而言卻不相同。《PBOCv 2.0 規範》的電子現金規範於第十

三部份「基於借記/貸記應用的小額消費規範」裡，電子現金是 PBOC 裡的一個應用。電子現金的卡片有如下幾個特點：

1. 由銀行發行。
2. 卡片只有一個應用，也就是一個 AID。從卡片的角度而言，實現多應用不成問題，但是，如果卡片支援多應用，還需要終端機(包括圈存終端機和消費終端機)以及銀行後台的相應配合，所以目前暫時以單應用為主。
3. 一般使用於小額消費，消費無需密碼，且是離線交易。
4. 目前尚無法應用於公共事業中(如交通用途)，因為這些行業是中國大陸住房和城鄉建設部管轄，有很多非技術的原因導致銀行與住房和城鄉建設部難以協商。

電子現金的應用是圈存交易，所謂電子現金圈存是指把用戶在銀行帳戶裡的錢先轉到卡片，電子現金應用是借記/貸記，每一筆交易所執行的流程就是簡化版的借記/貸記流程，以電子現金儲值為例，說明卡片交易流程如下：

第一步驟：先讀取支付系統目錄，再建立應用列表，然後選擇應用，所用命令是 select，參數是 AID(Application Identifier，應用標識符)。應用選擇後，卡片傳回一串資訊—PDOL (Processing Options Data Object List，處理選項數據對象列表)，這是一個交易初始化的列表，卡片透過這個列表告訴終端機，它需要哪些資料？這些資料用來給卡片做應用初始化，例如，卡片可能會需要授權金額(就是圈存的金額)、貨幣代碼等資料。終端機程式解析 PDOL，按照一定的規則解析資料，進入第二步驟。

第二步驟：應用初始化，命令是 GPO⁶，參數就是前一步根據 PDOL 所組的資料封包。該步驟表示終端機通知卡片開始交易，卡片會返回 AIP⁷ 和 AFL⁸兩個資料，AIP 告訴終端機卡片支援的功能，例如卡片是否支援離線資料認證、是否支援發卡行認證等；AFL 是要告訴終

⁶ GPO : GPO(Get Processing Option，取得處理選項)，為中國大陸金融積體電路(IC)卡規範中，IC 卡程式命令的縮寫。

⁷ AIP (Application Interchange Profile，應用交互特徵)，為列出了交易在處理過程中執行的功能。

⁸ AFL (Application File Locator，應用文件定位器)，為列出交易需要讀出的資料存放的短文件識別字、記錄號、記錄個數以及脫機資料認證需要的靜態簽名資料的存放位。

端機，如果要完成這筆交易，終端機該從卡上讀什麼資料。AFL 包含這些資料的位置和名稱，如交易序號、卡號等。

第三步驟：讀數據，命令是 read record，參數是前一步得到的終端機所需卡片資料的位置和名稱。終端機把 AFL 指定的所有資料讀出，並保存到終端機供下面的流程所用，每次讀到的資料是包含在卡片的返回資訊中，終端機解析返回資訊，提取相關的資料。

第四步驟：產生應用密文，命令是 GAC⁹，參數是密文類型和產生密文所需的資料。密文類型有三種，分別是交易證書 TC(Transaction Certificate，接受交易時由 IC 卡送出)、應用認證密文 AAC(Application Authentication Cryptogram，用於拒絕交易)，授權請求密文 ARQC(Authorization Request Cryptogram，終端機請求用)。因為這一步驟是為下一步驟連線處理做準備，所以終端機應用請求卡片產生的密文類型應該是授權 ARQC，查看卡片是否允許連線處理，卡片收到產生密文類型後，傳回的資訊有兩個重要的資料，第一個就是密文類型，該資料指示卡片是否願意做連線處理，如果願意，傳回的是 ARQC，與終端機一致，否則傳回 AAC，表示拒絕連線；第二個是終端機判斷卡片傳回的是否是 ARQC，如果是，終端機要讀取卡片返回的另一個重要的資料--應用密文 AC(Application Cryptogram)，該密文是卡片用存放在卡裡的密鑰，對終端機發過來的明文資料用 3DES 演算法產生。

第五步驟：連線驗證卡片。此步驟卡片本身沒有操作，終端機把前一步得到的應用密文，產生應用密文的一些資料，還有其它的資訊(如交易日期、交易時間等)，封包送到發卡行後台，通信方式一般是用 TCP/IP。後台透過驗證 ARQC 密文認證卡片，如果認證成功會傳回授權回應密文 ARPC(Authorisation Response Cryptogram，收單行用)，ARPC 是後台透過 3DES 演算法，對 ARQC 密文和二個位元組的授權回應碼加密產生。

第六步驟：此步驟是卡片驗證發卡行是否是一個有效的發卡行，命令是 External Authentication(外部認證)，參數是上一步連線處理回應的

⁹ GAC：GAC (Generate AC，產生應用密文)，為中國大陸金融積體電路(IC)卡規範中 IC 卡程式命令的縮寫。

ARPC 和授權回應碼。卡片收到命令後會用自己的密鑰，對 ARQC 和授權回應碼產生 ARPC，然後與終端機傳來的 ARPC 比較，若相同，就認為此 ARPC 是來自一個有效的發卡行後台。

第七步驟：連線圈存報文。驗證卡片和發卡行的合法性之後，終端機向發卡行後台請求圈存，上傳的資料包括儲值金額、卡內原來的餘額等資訊。發卡行後台傳回一個寫入卡片的命令，終端機解析這個命令是否合法，直接發給卡片，卡片儲值成功。

第八步驟：此步驟要發送第二請求密文命令(GAC2)，告訴卡片交易結束。與第四步驟 GAC1 不同的是，GAC2 的參數裡面多授權回應碼，並且請求的密文類型是 TC，也就是希望卡片接受交易。如果卡片傳回的也是 TC，表示接受交易。

第九步驟：讀交易日誌。在整個流程執行的過程中，卡片會以一定的格式記錄當前這筆交易的資訊，比如授權金額、卡號、交易時間等，終端機只需透過一個命令就可以把該資訊讀出，然後提取出有用的資訊，以便日後結算。

從持卡人應用的角度而言，電子現金所應用的功能跟電子錢包相似，都是最基本的三個交易功能：圈存、消費、查詢餘額，但是就卡片的交易流程、APDU、安全管理等技術卻不相同：

1. 交易流程上的差別：

電子現金因為是基於供借記/貸記，從讀取卡片支付系統目錄，到終端風險管理，一直到交易結束，每一步驟都必須完全遵守借記/貸記規範；而電子錢包本身是獨立於借記/貸記的，或者說它不同於 EMV 的規範。在安全管理上，電子錢包在風險控管方面並沒有那樣嚴格。

2. APDU 的差異：

電子錢包雖然有一些基本的應用協定資料單元 APDU(Application Protocol Data Unit，由報文結構組成)，跟電子現金借記/貸記是共用，但因為它有應用上的特殊性，自己也定義一套專門的 APDU 比如針對圈存，有 initialize for load(初始化圈存)、credit for load(圈存)等 APDU 指令，而電子現金是基於借記/貸記的，與電子錢包的 APDU 相容。

3. 在安全管理方面：

電子現金是基於借記/貸記，故在安全規範方面要符合借記/貸記的標準，安全的要求高過電子錢包。

例如一張電子錢包的 IC 卡要做圈存，首先向卡片發初始化圈存指令，卡片會產出一個 MAC1，這個 MAC1 是卡片用本身的密鑰，把一些必要的輸入資料(比如圈存金額)，用 3DES 演算法產生一個報文認證碼，這個 MAC1 隨後被送往後台，後台解密這個 MAC1，從而驗證卡片的合法性。如果驗證成功，後台產出一個 MAC2 送回給終端機，當終端機對 IC 卡發圈存指令時，要把這個 MAC2 一起發給 IC 卡，卡片以同樣的原理驗證後台的合法性，如果驗證成功，才更新卡上的金額，圈存成功。

又如，一張電子現金的 IC 卡要做圈存，讀取應用資料成功後，終端機向卡片發出密文指令，卡片收到該命令，以 3DES 演算法產生應用密文 ARQC，終端機連線將 ARQC 送到後台，後台用 ARQC 驗證卡片的合法性，如果驗證成功，會產一個授權回應密文 ARPC 給終端機，終端機用 ARPC 對卡片發出外部認證命令，卡片就可以驗證後台的合法性，驗證成功後終端機才會向後台申請卡片金額圈存指令，後台驗證透過才會發出圈存指令到終端機。

從以上流程可以看出，在圈存的方式上，電子錢包與電子現金合法性驗證的原理基本上是相同的。不過電子錢包的圈存指令是由驗票設備發起，而電子現金的圈存指令則是後台驗證合法性後傳來指令，驗票設備僅做解析，然後轉發到 IC 卡。

就目前的情況來看，無論是金融機構(比如銀行)，還是一些非金融的行業機構，在推廣金融 IC 卡小額消費的應用時，都是優先選擇電子錢包。因為無論是卡片，或是終端設備(驗票設備、圈存機等)，開發電子現金的應用，其複雜度都大於電子錢包。例如，電子現金的驗票設備機要求具有離線認證能力，必須同時具備 SDA 和 DDA，而這種認證的原理是基於非對稱的 RSA 加密技術，而電子錢包的驗票設備就沒有這個限制，可以用傳統的 DES 加密技術就可以解決。

《建設事業非接觸式 CPU 卡 COS 技術要求》和《PBOCv2.0 規範》電

子錢包相關規範(PBOC2.0 第一、第二、第八、第九部分)幾乎完全相同，和 PBOC 電子錢包的區別只有三處¹⁰：

1. 增加一條 APDU 命令，用來讀取晶片的唯一驗證碼。

根據《建設事業非接觸式 CPU 卡 COS 技術要求》的規範，每個晶片都必須有一個唯一的 9 位元組驗證碼，這個驗證碼由住房和城鄉建設部提供；而住房和城鄉建設部按照每個認證碼直接向晶片廠收取 RMB 1 元的費用。

2. 在電子錢包消費交易過程中，計算 Debit For Purchase 的 MAC1 時，在原來資料元的基礎上增加了前面提到的 9 位元組認證碼，一起參與 MAC1 的計算。
3. 在離線交易計數器和聯線交易計數器達到最大值 0xFFFF 之後，不再像標準 PBOC 電子錢包定義的那樣重新置 1，而是直接報錯終止交易。

但是中國大陸住房和城鄉建設部頒佈的《建設事業非接觸式 CPU 卡 COS 技術要求》與中國大陸人民銀行頒佈的基於 EMV2000 標準的《PBOCv2.0 規範》中電子錢包相關規範相同，加上遵循《建設事業非接觸式 CPU 卡 COS 技術要求》的每一個晶片都必須收取 RMB 1 元的驗證碼費用，故發卡量達經濟規模的地區，例如北京、上海、深圳等反而都按照自己的模式發行公交卡，以規避被收取 RMB 1 元的驗證碼費用。

三、中國大陸交通電子票證 CPU 卡發展現況

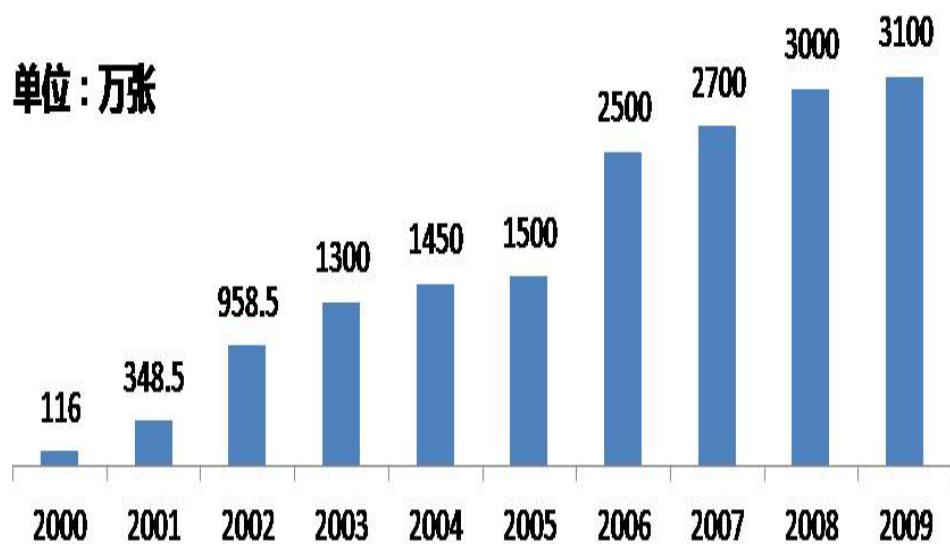
根據中國大陸移動研究院於 2010 年 9 月所做的調查¹¹，目前中國公交一卡通市場現況如下：

1. 公交一卡通發卡量近兩億，CPU 卡升級換代正在進行

從下圖可以看出，2000 年至今中國大陸城市交通領域一卡通累計發卡量突破 1.8 億張，2006 年之後每年增加量穩定在 200 萬張~400 萬張之間。

¹⁰引用 <http://smarticcard.blog.sohu.com/144743726.html>《建設事業非接觸式 CPU 卡 COS 技術要求》和 PBOC 电子钱包的区别

¹¹引用中國大陸移動研究院產業市場所；產業市場觀察王惠儀；國內公交一卡通市場現狀掃描；2010 年 9 月。



資料來源：中國大陸移動研究院

圖 5-2 2000~2009 年中國大陸城市交通領域「一卡通」年發卡量成長圖

另一方面，2008 年 M1 卡的加密方式被破解，讓人們擔憂一卡通的安全性。自 2009 年起中國大陸採用的 M1 卡開始升級為 CPU 卡，截至 2009 年 10 月，中國大陸 CPU 卡發卡總量已近 2500 萬張。根據握奇預計，從 2009 年到 2013 年中國大陸交通產業的 CPU 卡發行量，將從 1,300 萬張增長至 5,500 萬張。目前北京、上海、深圳、廣州等超大城市的交通卡營運公司，均正由 M1 卡升級到 CPU 卡，並開始測試等工作，由此預測在未來 3-5 年 CPU 卡會與 M1 卡形成均分市場的局面。

2. 一級城市覆蓋過半，佈署集中於經濟發達區域

從中國大陸已有公交一卡通業務佈署的城市營運資料來看，業務開展集中於長三角與珠三角等經濟發達區域，前十大城市的累計發卡量占全國的 50%(如圖 5-3)，在部分城市已經成功實現普及與規模化營運。以北京市為例，2009 年總發卡量約 3,000 萬張，49.3 億筆的年刷卡交易量為全國第一，而公交刷卡比例達 90%，地鐵刷卡比例達 78%，普及率已經非常高。

城市	运营主体	发卡量	应用领域	(拟)互通城市	卡片类型
北京	北京市政交通一卡通公司	3000万	公交、地铁、出租、高速路、停车场、小额消费	天津	M1 (type A)+CPU卡
上海	上海公共交通卡股份公司	2400万	公交、地铁、出租、轮渡	无锡、常熟、阜阳	M1 (type A)+CPU卡
广州	广州羊城通有限公司	1200万	公共交通、小额消费、企业及小区一卡通	佛山	CPU卡
深圳	深圳市深圳通有限公司	700万	公共交通、小额消费	香港、珠三角	M1 (type A)+CPU卡
南京	南京市民卡公司	500万	公交、出租、地铁、轮渡及购物、餐饮等近30个领域	芜湖、淮安、扬州和杭州	CPU卡
沈阳	沈阳城市通有限公司	368万	公交、小额消费	辽宁中部七城市	CPU卡
武汉	湖北鄂通卡系统有限公司	320万	公交、轻轨、轮渡及部分小额消费	武汉8+1城市圈	M1 (type A)+CPU卡
西安	西安城市一卡通有限公司	>300万	正由公交IC卡转向城市通卡，向全领域拓展	咸阳	CPU卡
重庆	重庆城市通卡有限公司	约300万	公交、索道、BRT、超市、公园、影院	-	M1 (type A)+CPU卡
杭州	杭州市城市通卡有限公司	230万	公交、出租、停车、小额消费、加油	萧山、余杭、上海、南京	CPU卡

来源：产业市场所，累计发卡量以2009年底为准

資料來源：中國大陸移動研究院

圖 5-3 中國大陸公交「一卡通」業務規模前十大城市發展情況彙整表

3. 向小額消費領域甚至城市一卡通拓展升級

公交一卡通主要應用於公交、地鐵、計程車三大領域，部分城市還將其拓展到高速公路、停車場、加油站等交通領域。但部分公交一卡通公司認為若侷限於單一領域應用，最終將面臨被吞併的危機，於是開始由單一公交應用向其他領域甚至城市一卡通主動升級。

2009年底由「部 IC 卡服務中心」展開的「行業 IC 卡應用情況調查」中發現，近 90%的公交/城市一卡通公司 IC 卡應用已經拓展到小額消費領域的商場、超市、便利店、餐飲、健身、電影院，以及自來水、燃氣、供熱等公用事業及交通方面的繳費，同時數位社區中門禁、停車場的管理以及園林景點門票應用也有涉及，涵蓋近 40 個非交通領域的應用。

同時，中國大陸部分城市公交 IC 卡已經開始向城市一卡通直接升

級，中國已啟動或計畫啟動城市一卡通的城市總量達到 367 個，例如南京於 2009 年底開始由現有的金陵卡通向城市一卡通升級、西安於 2009 年底開始在現有公交 IC 卡基礎上逐步實現城市一卡通功能、青島於 2009 年底組建青島市青島通卡股份有限公司，於 2010 年 3 月正式發行城市一卡通青島通卡，開始對原有公交 IC 卡進行升級替換等。

4. 區域互聯互通正在推進

長三角及珠三角地區早已實施區域內互聯互通，也在部分城市間推動單向或雙向互通，但由於利益分配矛盾、技術標準不統一等問題，一直推動緩慢。目前部 IC 卡服務中心作為住房城鄉建設領域 IC 卡 /RFID 應用的行業管理機構，正積極推動公交/城市一卡通的區域互聯互通。2008 年住建部就已經開始建設全國性建設事業 IC 卡資料處理中心，負責城市間公交 IC 卡互聯互通異地交易的資料處理和清算。

而其於 2010 年頒佈《城市公用事業互聯互通卡通用技術要求》在內的三項互聯互通國家產業標準，並於 10 月 1 日正式實施。山東省互聯互通一卡通專案成為首個試點專案，目前已開通濟南和臨濟互通，預計在兩年內將山東全省的城市一卡通全部互通。與此同時，在浙江(包括寧波，嘉興，紹興，台州)一卡通互聯互通進入籌備階段，系統升級方面已做好互聯互通基礎，計畫 2010 年底前實現這五個城市的互聯互通。

未來隨著城市間經濟活動的區域聯動特性加強、城際高速鐵路的大力興建，必將帶動公共交通領域跨區域的交易量與交易金額增長。

5. 一卡通公司已在特大型城市獲利

公交一卡通業務的營運實體是各地公共交通一卡通公司，其以交易手續費、清算服務費以及卡片押金及預付金所構成的呆滯款利息為三大主要收入來源。以上海為例，其年收入已超過億元，年淨利潤預估超過千萬元。而北京儘管至今與公交系統仍未達成結算協定，但呆滯款帶來的利息收入與北京市政府針對結算部分的補貼資金，仍使得北京公交一卡通公司能夠維持盈利狀態。

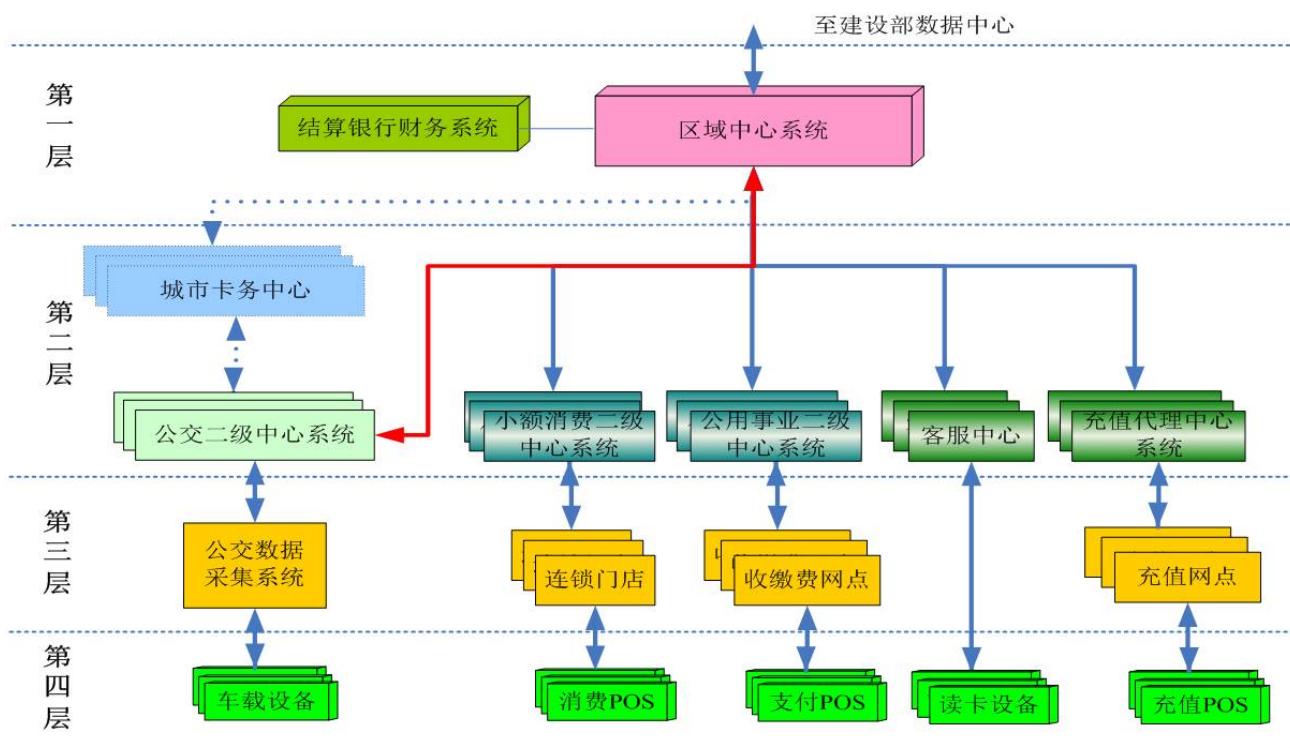
四、已實施 CPU 卡產業標準的城市概況

1. 銀川市「城市一卡通」

銀川市「城市一卡通」系統遵循「部 IC 卡服務中心」「統一規劃、統一標準、統一管理、統一發卡、統一清算」的指導原則，避免各行業、各單位重複投資、自行發卡，以減輕發卡單位的建置及營運成本。

按照寧夏經濟發展和沿線城市帶經濟發展規劃，銀川市「城市一卡通」定位區域中心營運管理平台建設，先行在銀川市應用「城市一卡通」，待時機成熟時再隨著沿線城市帶建設，逐步拓展到區內其他四個市區相關行業，從而建設起一個以銀川市為中心，輻射全區的城市一卡通區域中心營運平台。

銀川市「城市一卡通」系統的區域中心系統是整個系統的資訊交換樞紐以及業務資料處理核心，向上連接到住建部公用事業 IC 卡建設中心交換系統，實現未來同其它城市一通卡系統的互連互通目標，滿足城市一通卡在異地使用需要；橫向與郵政儲蓄銀行系統，由郵政儲蓄銀行系統根據區域中心系統的資金清算、結算需要，執行對相關單位資金安全快速的結算業務；向下連接各城市的卡務管理中心、各行業應用二級管理系統、各小額消費二級管理系統、各客服中心系統及加值代理點，其應用系統架構示意圖如下：



資料來源：<http://www.icfw.com.cn>

圖 5-4 銀川市「城市一卡通」應用系統架構圖

2. 鎮江「市民卡」

鎮江「市民卡」是鎮江市民辦理各項保障事務、享受政府公共服務的電子憑證，也是市政府各部門為市民提供社會保障和社會公共服務的工具，集接觸式 CPU 卡、非接觸式 CPU 卡與銀行卡為一體的多功能複合卡，同時作為小額消費的支付工具和銀行的借記卡或貸記卡使用。該卡的功能包括：

- (1) 公交卡：能在本地及跨區(如南京、上海等地)刷卡坐公車及計程車；
- (2) 健保卡：能實現醫保看病支付，可到本地及異地各大醫院及社區醫院就診；
- (3) 社會福利卡：能領取養老保險等各類社會保障資金；
- (4) 圈存卡：能在各大商場輸入密碼消費購物；
- (5) 小額消費卡：能當做電子錢包支付小額消費；
- (6) 銀行卡：能通過銀聯安全地在各銀行使用；
- (7) 借書卡：能辦圖書借閱證；
- (8) 公共事業繳費卡：能繳納水電氣等費用。

根據鎮江市市民卡工程建設目標，鎮江「市民卡」工程分三期建設：第一期為試營運期；2010 年 10 月份發放首批市民卡，實現社保、醫保、公交、園林、新行政中心門禁等應用；第二期為功能拓展期；2011 年將拓展市民卡應用範圍，逐步融合衛生、公積金、小額消費(公共事業繳費)、計程車等功能，同時具有城際鐵路、高鐵、輪渡互聯互通的功能，到 2011 年底實現鎮江市民卡發卡總量達 100 萬張；第三期為區域拓展期；2012 年將部分應用擴展到長三角地區乃至全國的互聯互通，爭取到 2012 年底，發卡總量達到近 300 萬張，發行區域全覆蓋全城鄉。

3. 無錫「市民卡」

無錫市 2010 年新辦理社會保險卡的用戶直接就能拿到整合社保、交通、醫療等多功能的「市民卡」，該卡是載入生物指紋資訊和二維識別碼的「雙核多介面」CPU 卡，卡內具有社會保險密鑰、城市密鑰和銀行密鑰，可以靈活地根據不同應用的特性，投入不同的應用管理區域。

2010 年內該卡將逐步整合市民中心公務卡、診療卡、選民卡、居住證、園林卡、體育一卡通、自行車租賃、駕駛人資訊卡、圖書卡、兒童免疫金卡、旅遊一卡通、遠端教育卡等。預計 2010 年底至少可發行 50 萬張，目標是 100 萬張，並與江陰互聯互通。

2011 年計畫著手拓展手機市民卡、社區一卡通、校園卡、水電通信等社會事業繳費、計生卡、社會停車卡、公積金卡以及商業消費等多領域。

4. 瀋陽「城市一卡通」

瀋陽地鐵一號線已於 2010 年 10 月 1 日正式營運，在票證營運上將與瀋陽「城市一卡通」整合，瀋陽「城市一卡通」同時轉換成符合中國產業標準要求的 CPU 卡。

瀋陽市原發行可以乘坐公車的「城市一卡通」，是屬於 TYPE B 的 CPU 卡，不符合最新頒佈的《建設事業 CPU 卡作業系統技術要求》(CJ/T 304-2008)以及《建設事業非接觸式 CPU 卡晶片技術要求》(CJ/T 306-2009)之中國大陸產業標準要求，同時也不具備未來全國城市一卡通互聯互通應用條件。因此，按照住房和城鄉建設部相關標準以及瀋陽市政府要求，瀋陽地鐵此次發行符合標準並具備互聯互通之 CPU 卡，並且在未來兩年時間內與現有的瀋陽城市一卡通卡進行逐步整合，最終實現二卡合一，預計發行 52 萬張 CPU 儲值票卡。

目前瀋陽地鐵正與撫順、鐵嶺洽談互聯互通事宜，預計 2011 年內將實現三城市間區域互通。另外，包括上述三個城市在內的遼寧中部城市群八城市，也可望在不久的將來實現互聯互通。在城市一卡通統一的安全體系管理下，瀋陽將在 3~5 年內達到全國一卡通的互聯互通，屆時瀋陽市民到上海、寧波、濟南等城市將可以使用瀋陽一卡通，擁有與當地市民同樣的刷卡便利。

5. 貴陽公交 IC 卡

2010 年 3 月，貴陽市公交系統 IC 卡系統已全面技術升級採用 CPU 卡。原貴陽公交 IC 卡發行量約萬張，市區 99 條公交線路，約 1,800 輛無人售票市區公車，全部採用 IC 卡電子收費。系統技術升級後乘客仍然可以持原貴陽公交 IC 卡乘車刷卡，不受影響。兩種卡都能在公車上

進行消費，現行乘車票價保持不變。普通票的持卡人則可在原公交 IC 卡的各個加值點進行加值、驗卡或補卡任何一項操作後，系統便會對卡內的原有餘額自動進行轉換。成人季票、學生季票、老年人卡、殘疾人卡的加值方式以及規定、刷卡乘車扣款方式暫時不變。

透過以上之說明，我們可以了解到中國大陸一方面在交通票證之發展規範上面，逐步由原本交通與建設部門規範主導，移轉為人民銀行之金融監理單位主導，另一方面，也因為應用層次擴展到小額消費，中國大陸對於交通票證之 CPU 卡應用十分積極，也發展出許多實務經驗可供其他國家參考。

5.2.3 日本 SONY FeliCa 技術規範發展與現況

FeliCa 是 Sony 所開發出來的非接觸式 CPU IC 卡技術。名稱由英語中代表「幸福」的 "Felicity" 和 "Card"(卡片)組合而成，是 Sony 的註冊商標。FeliCa 最初被提案為 ISO 14443 type C，但未被採納之後，FeliCa 和其向後相容方式被標準化為 ISO 18092(Near Field Communication, NFC, 近距離通信)。在日本國內，被當作 JICSAP IC 卡規格 V2.0 「第四部份 高速處理用 IC 卡」和日本鐵道サイバネティクス協議會的 IC 卡規格而予以標準化。

FeliCa 和一般的 IC 卡同樣有適用於現金卡或識別卡的技術，但為了要求高速處理特性(自動儲值設備、大樓進出管制等)或結帳(便利商店)等的應用，將指令集加以特殊化。因此和 ISO 7816-3 的基本指令並不相容，且 IC 晶片內部的記憶體固定為 16 位元組長的紀錄，因此和 ISO 7816-3 規定的檔案結構亦不相容。加密處理方面，相互認證使用 Triple DES，通訊使用 DES 或 Triple DES。沒有公開密鑰加密的規格。雙模型式(接觸／非接觸)雖然可以有公開密鑰加密，但只在接觸通訊時使用。相互認證時，退縮碼被作為加解的密碼來使用。不是說每一個項目個別認證、它是透過複數的驗證碼加密產出的鍵稱為退縮碼，這個退縮碼最多可供 16 個項目使用。退縮碼無法產生原來的密碼。如此，在不降低安全級別的情況下實現高速化處理。

一、日本 SONY FeliCa 技術規範發展

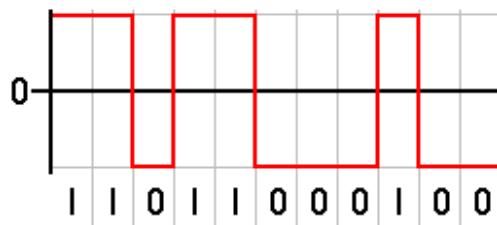
FeliCa 是 SONY 為了非接觸式 IC 卡而開發出來的通訊技術，IC 卡於讀寫時送出的載波，引導由驗票機供給電力，由載波的調變與卡片讀寫溝通。例如 ISO/I 電子現金/I 電子現金 14443 type B，使用 ASK 10% 調變，及

NRZ 編碼¹²，FeliCa 的調變同樣是 ASK10%，但不同的是採用曼徹斯特編碼¹³。

FeliCa 為符合快速交易處理的應用，將指令集加以特殊化，因此和 ISO/IEC/IEC 7816-3 的基本指令並不相容。且 IC 晶片內部的記憶體固定為 16 位元組的紀錄，因此和 ISO/IEC/IEC 7816-3 規定的檔案結構亦不相容。SONY 曾申請將 FeliCa 列為 ISO/IEC/IEC 14443 Type C，但未被採納。之後，SONY 為了讓 FeliCa 能與符合 ISO/IEC/IEC 國際標準的 IC 卡整合，於是在 2002 年與 PHILIPS 簽屬協定，聯合開發一種全新的 NFC(Near Field Communications)技術，該技術的 NFCIP-1 標準已於 2003 年 12 月成為 ISO/IEC/IEC 18092 國際標準。¹⁴

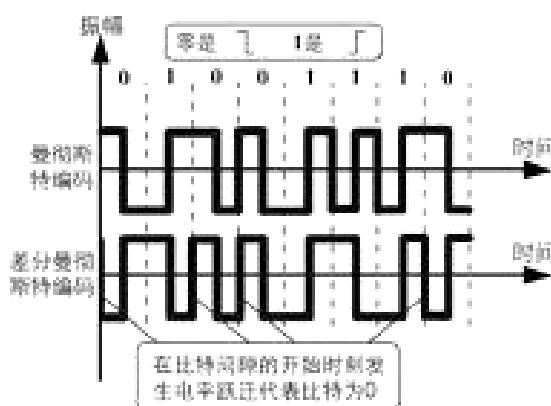
NFCIP-1 由 FeliCa 無線通訊協定、ISO/IEC/IEC 18092 無線通訊協定和設備間通訊協定三部份組成，可實現 FeliCa 和 ISO/IEC/IEC 14443A 相容通訊(通訊速率為 106kbps，212 kbps 和 424 kbps)以及多個設備間的通用數據

¹² NRZ 編碼 (Non-Return-to-Zero line code，不歸零編碼) 指的是一種二進位的訊號代碼，在這種傳輸方式中，假定邏輯值”1”為高位階(High Level)，邏輯值”0”為低位階(Low Level)，該狀態將保持到下次邏輯值改變為止，故頻率或相位也會保持到下次邏輯值改變。



資料來源：維基百科網站

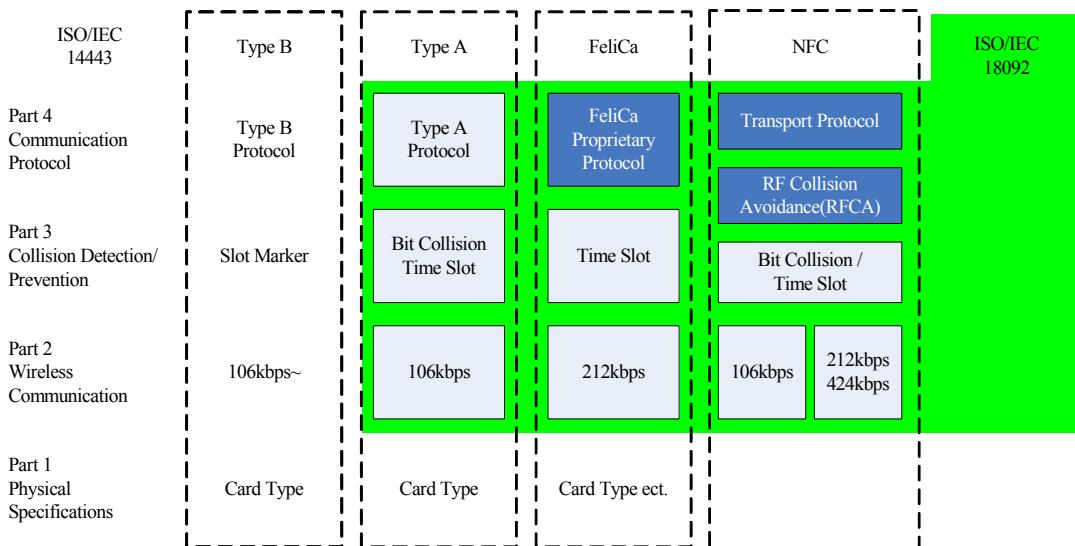
¹³ 曼徹斯特編碼 (Manchester Encoding) 係表示位元的兩種物理狀態，若邏輯值”1”以位元見隔的中央為準在負方向變化，則邏輯值”0”同樣以中央為準卻在正方向變化。無論邏輯值”1”或”0”一定會在位元中央變化，所以在其位元時間內的電壓平均值為 0。既使”1”或”0”連續，但平均值仍為 0，因此無直流電壓的重疊。



資料來源：百度百科網站

¹⁴ 資料來源：維基百科網站，<http://zh.wikipedia.org>

收發。圖 5-5 為 NFCIP-1(即 ISO/IEC/IEC 18092)與 FeliCa 及 ISO/IEC/IEC 14443 Type A 和 Type B 標準的對應關係。¹⁵



資料來源：電子工業出版社(北京)，非接觸式 IC 卡原理與應用，陸永寧編著，2006。

圖 5-5 NFCIP-1 與 FeliCa 及 ISO/IEC/IEC14443 的對應關係

2004 年 3 月，SONY、PHILIPS、NOKIA 三家公司聯合成立「NFC 論壇」，僅僅一年的時間就有 VISA、MasterCard、JCB、SIEMENS、SAMSUNG、PANASONIC、NEC、INFINEON、MOTOROLA、TI、GEMPLUS 等近 50 家世界知名的企業加入，迅速成為全球短距通訊研發的重要基地。同年，NFCIP-1 進一步發展為 NFCIP-2，成為 ISO/IEC/IEC DIS(Draft International Standard)21481 國際標準。NFCIP-2 除具備 NFCIP-1 的功能外，可同時與 ISO/IEC/IEC 18092、ISO/IEC/IEC 14443、ISO/IEC/IEC 15693 的 13.56MHz 頻率非接觸短距離通訊協定相容，也可與 ISO/IEC/IEC 14443 Type B 卡片及 ISO/IEC/IEC 15693 電子標籤相容。¹⁵

日本 SONY FeliCa 技術在交通應用方面，1997 年 9 月由香港的「八達通」首先採用。之後，2001 年 11 月日本的「Suica」，2002 年 4 月新加坡的「易通卡」等陸續採用。以下分別說明其應用現況如下。

二、香港八達通卡應用現況

八達通使用 Sony 的 13.56MHz Felica RFID 晶片及其他相關技術，應用於香港大眾運輸工具收費系統。最初只應用在公車、小巴、地鐵、輕軌、機場捷運、鐵路、渡輪、停車場等交通工具上，後來陸續擴展至其他產業，

¹⁵ 資料來源：電子工業出版社(北京)，非接觸式 IC 卡原理與應用，陸永寧編著，2006

包括商店、餐廳、停車場、收費電話、販賣機、休閒育樂等業務，也用作學校、辦公室和住所的通行卡。加值的方法也由最初的車站加值機，擴展至商店付款處和以信用卡、銀行帳戶自動轉帳。

八達通在香港地鐵和九廣鐵路各車站及機場均有販售，前端設備包括讀寫器(因應使用場所分大型及小型)、自動加值機、人工加值機、餘額查詢機，購買時需要繳付港幣 50 元的押金和 20 至 100 元的預付票值，押金於退還八達通卡時退回。一般八達通是無記名性質，毋須身份證明文件即可購買。使用者遺失八達通時，只會遺失卡內的儲值金額，並不會遺失其他個人資料。

除了三種為不同身份的人士而設的一般八達通外，八達通公司亦有發行個人八達通(記名卡)，八達通之卡片種類如表 5-2。個人八達通卡可用於進入住宅及商業大廈等設施，以及使用在學校點名及圖書館借書等用途。

表 5-2 八達通卡種類

種類	售價	面值	使用規則
小童	HK\$70	HK\$20	適用於年齡介於 3 至 11 歲的兒童。使用小童八達通搭乘大部分公共交通工具可以有半價優惠。
成人	HK\$150	HK\$100	適合於任何年齡的人士使用。
長者	HK\$70	HK\$20	適用年齡視不同業者的規定(城巴的適用年齡是 60 歲以上、九巴的適用年齡是 65)。長者優惠不適用時會作成人收費。
個人	不適用	不適用	個人八達通需要註冊，上面可以印有使用者的照片。多用於進入大廈門禁系統等設施。

資料來源：八達通卡有限公司網站(www.octopuscards.com)

每張八達通卡最多可儲值 HK\$1000 元。另外，若儲值金額不足支付交易金額，只要扣款後儲值金額不小於 HK\$-35，仍可進行交易，容許在儲值金額不足的情況下，仍能搭乘香港大部份交通工具或購買小額商品。八達通持卡人可利用銀行或信用卡帳戶為八達通卡自動加值。當八達通卡的剩餘儲值金額低於 HK\$0 時，便會自動加值 HK\$250 或 HK\$500，一般及個人八達通卡均具有自動加值功能。

三、日本 Suica 卡應用現況

Suica 是 JR 東日本為使用在自己路線而開發的非接觸式智慧卡系統的乘車票證。取代原本在自動售票機發行的儲值磁卡(2005 年 3 月 31 日停止發售)，Suica 與儲值磁卡一樣，可以在大部分的售票機購買，也可利用自動補票機(自動精算機)補票、加值；也有定期車票的機能，並能夠在車站商店街中的部份商店用來購買商品。



圖 5-6 Suica 卡區間定期票

Suica 卡卡片種類分為：

1. 一般之儲值卡

購買時必須支付 500 円的保證金，保證金無法折抵車資，售價 2,000 円中能實際使用的金額為 1,500 円，保證金在退還 Suica 時將會全額歸還。Suica 可以在有「Suica」標誌的「自動售票機」「卡片發售機」「自動補票機」，用現金來進行儲值。每次可儲值金額的單位是 1,000 円、2,000 円、3,000 冪、4,000 冪、5,000 冪、10,000 冪等 6 種，若不指定搭乘期限及路線，卡片可儲值的上限是 20,000 冪。

2. 記名卡(My Suica)

登錄個人基本資訊，遺失後能夠補發，使用 Suica 儲值卡或記名卡搭乘 JR 列車與購買單程票相較並沒有任何折扣。

3. 除具有一般儲值卡功能外，尚具備固定區間之定期票功能。

購買限定期限與指定路線的「定期區間通勤票」，則不受儲值上限 20,000 冪的限制。依照「JR 東日本旅客營運規則」第 35 條規定，通勤票有效期限通常是 1 個月，但如果所指定搭乘的區間超過 100 公里，則

可選擇 3 個月或 6 個月；另第 130 條規定，特種車輛共分 6 個收費區間（如表 5-3），最高收費區間為 7440 円，若購買 3 個月或 6 個月「定期區間通勤票」所須金額將遠超過 20,000 円上限，如表 5-4，圖 5-7 顯示以 Suica 購買東京至國立 JR 中央線最高可購買金額為 6 個月通勤定期票 77,100 冪。

表 5-3 JR 東日本特種車收費標準

營運公里 區間	100 公里	200 公里	400 公里	600 公里	800 公里	800 公里 以上
收費金額	1240 冪	2670 冪	4000 冪	5150 冪	6300 冪	7440 冪

資料來源：<http://www.jreast.co.jp/ryokaku/index.html> JR 東日本營運規則

表 5-4 JR 東日本「定期區間」通勤、通學票收費標準超過 5 萬円例舉

東北新幹線

區 間		通勤票		通學票	
		1 個月	3 個月	1 個月	3 個月
東京	福島	192,390	548,310	131,020	373,450
上野	福島	187,350	533,950	126,410	360,300
大宮	福島	176,510	503,080	120,450	343,330
大宮	白石藏王	190,320	542,400	127,970	364,770
小山	仙台	188,170	536,290	126,850	361,600
宇都宮	仙台	176,510	503,080	120,450	343,330
宇都宮	古川	198,910	566,900	132,350	377,230
那須塩原	古川	177,960	507,210	121,410	346,050
那須塩原	くりこま高原	182,540	520,220	123,940	353,270
那須塩原	一ノ関	195,450	557,050	130,640	372,360
新白河	水沢江刺	194,150	553,320	129,940	370,380
郡山	北上	183,350	522,560	124,240	354,130
郡山	新花巻	192,310	548,110	129,040	367,810
福島	盛岡	184,220	525,040	124,800	355,730
福島	いわて沼宮内	198,040	564,410	131,850	375,830
白石藏王	いわて沼宮内	182,980	521,490	124,170	353,930
白石藏王	二戸	198,420	565,500	132,160	376,700
仙台	二戸	178,550	508,890	121,920	347,520
仙台	八戸	192,310	548,110	129,040	367,810
古川	八戸	177,960	507,210	121,410	346,050

資料來源：https://www.calc.eki-net.com/TCalcWEB_Frex.asp#tohoku

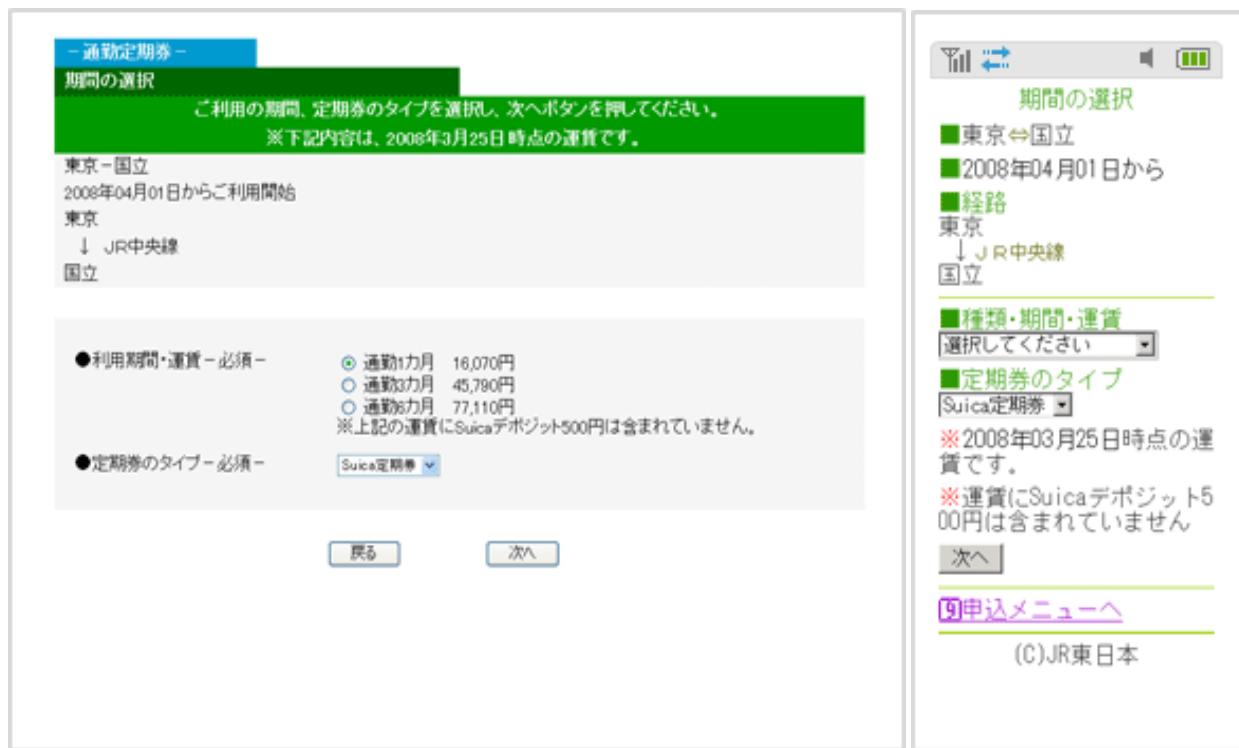


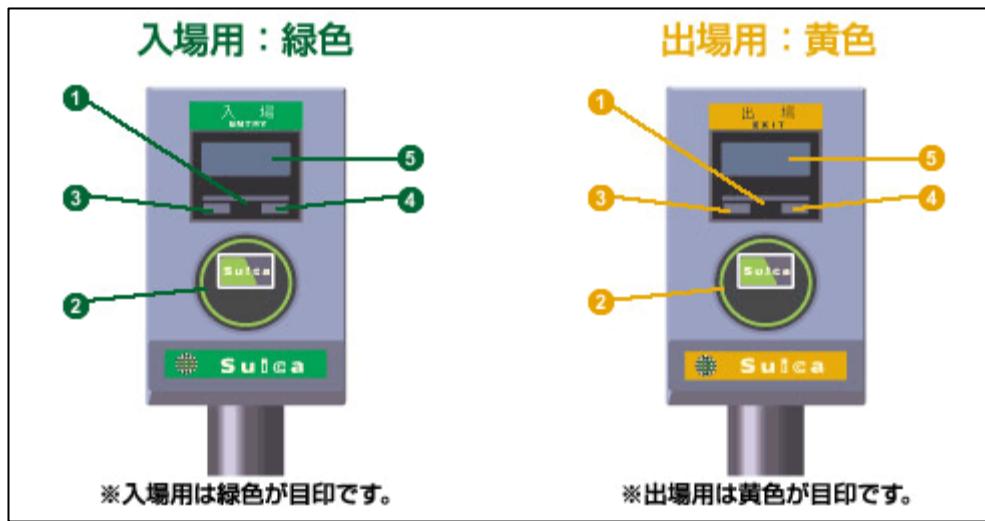
圖 5-7 以 Suica 購買 JR 東日本定期票畫面

4. 結合信用卡功能的 View Suica。

Suica 可使用在 JR East 公司所屬鐵路之部分車站(包括東京、仙台及新瀉等三個都會地區)、東京地區新幹線車站、東京地區其他巴士與軌道系統等，在 JR East 東京地區路線部分，往西可達靜岡縣(伊東市)，往北可達橋木縣(那須郡)、往東可達滋城縣(日立市)、往南可達千葉縣(君津市)，最遠範圍約距東京市中心 150 公里遠。

由於 JR 路線行經許多偏遠地區，在許多較小型的車站中布設 Suica 專用之簡易驗票機(稱為簡易 Suica 改札機，如圖 5-8 所示)，該驗票機區分為進站與出站兩種，不設自動閘門設備，以降低設置成本。

JR 鐵路的車票種類，除了基本票價外，特急列車、寢台車(臥鋪車)、綠色車廂(頭等車廂)、指定席等都需另外付費，例如搭乘特急列車綠色車廂指定席的票價，包含基本券、指定席特急券、綠色車廂券，不過在購買時僅會列出一張票券。使用 Suica 儲值卡的乘客，僅能使用一般列車(包含普通、區間快速及快速列車)普通車廂的自由席，若要搭乘特急列車、寢台車、指定席或綠色車廂時必須再額外購票。



資料來源：JR 東日本網站(<http://www.jreast.co.jp/suica/index.html>)

圖 5-8 Suica 簡易驗票機

四、新加坡 CPU 卡應用現況

新加坡之交通票證主要為 Ez-Link 卡片，其在 2009 年 8 月也首發交通、銀行聯名 CPU 卡，該卡因為合成新加坡現在的交通一卡通 Ez-Link 卡功能，符合新加坡現在通用的非接觸電子支付標準 CEPAS(Contactless e-Purse Application System)。CEPAS 標準為新加坡政府為解決複雜之電子付款環境，打造新加坡新一代的電子支付系統，由新加坡資訊通訊發展局(IDA)、SPRING Singapore 公司、陸路交通局(LTA)、卡片認證技術委員會(CPTIC)、電子轉帳體系公司(NETS)，以及 Ez-Link 公司共同合作，於 2006 年 6 月發表 SS 518 CEPAS (Contactless ePurse Application Specification 非接觸電子支付應用標準)。

另外，該卡符合現有智慧卡安全最高標準，持卡人僅在距非接觸驗票設備非常近的情況下，發起的交易才會被認證和完成。持卡人可以透過 ATM 機進行交易，可以在大型商場刷卡消費，亦可以在出外時刷卡乘車。因為同時實現了銀行卡接觸式、非接觸式功能以及交通一卡通三種功能，所以該卡也被稱作「三合一」卡。它也是全球第一張將銀行卡功能和交通一卡通功能融合起來的雙介面 CPU 卡。

新 Ez-Link 卡已經於 2009 年陸續發行並全面試用，根據 LTA 的計畫，新加坡政府將在未來的 12-18 個月內，將舊的 Ez-Link 卡逐步淘汰，全部替換成新版 Ez-Link 卡。新 Ez-Link 卡除原有大眾運輸工具用途以外，還可以

用於 ERP(公路電子收費)、EPS(停車場電子收費)、購物付款、支付圖書館罰款等其他符合 CEPAS 標準的電子付費系統以及額外功能。

5.3 以 CPU 卡為交通電子票證可能衍生之議題探討

針對 CPU 卡未來取代交通電子票證之可能衍生議題，除了影響目前已經大量發行之邏輯加密卡外，也讓國內交通電子票證公司面對新的變化而有所因應，特別是交通電子票證採用 CPU 卡後，未來可在一卡多用、小額付費、多功能應用等方面展現 CPU 卡強大之功能，然而其衍生之問題與衝擊勢必與單一交通用途之卡片有所差異，因此，本研究以下將針對以 CPU 卡為交通電子票證可能衍生之議題，分為交通營運面與交易安全面來說明。

一、交通營運面之可能衍生議題

1. 票證轉換運作部分

目前邏輯加密卡之發行數量，於交通票證領域佔絕大多數，因此，面對二千萬多張之邏輯加密卡未來之轉換，勢必牽動許多部門之配合，而在成本、效益、卡片規模、技術成熟度等影響層面下，進行不同之卡片轉換模式選擇，各家票證公司之採行作法亦可能有所不同。因此，對於卡片轉換策略內容有必要進一步加以研析，以往研究多為各廠商之產品升級說明，缺乏卡片升級作業實務經驗，因此，建議未來針對實務面之 CPU 卡升級轉換策略、配套措施、平行作業移轉程序、投入人力、物力、資源、時程等予以規劃探討，以利此一議題之進一步了解。

2. 交通營運邏輯整合部分

針對未來卡片可能由邏輯加密卡升級為 CPU 卡片，除了代表單一用途之交通票證卡片應用，將逐漸擴展為多功能智慧卡之趨勢外，也代表著一卡在手，處處通行的跨區使用情況將日漸普及，因此，除了在交通票證領域跨區使用規範需要整合外，對於卡片之優惠與紅利積點管理，也需進一步釐清與探討。

3. CPU 卡片規格整合部分

在邏輯加密卡片方面，卡片之格式因僅應用於單一交通票證領域，其均有基本底層架構之規劃。因此，票證公司於發卡規劃時，僅需要針對卡片應用上層欄位格式予以規劃即可。然而，CPU 卡片之應用

型態較為多樣化，因此，底層之基本架構規劃目前付之闕如，導致 CPU 卡應用上遠較先前卡片規劃之複雜度更高、考量因素更多，也導致各家票證公司所規劃之 CPU 卡片缺乏共通性基礎。

面對未來交通領域應用，CPU 卡片需要在基本底層架構有統一欄位之規劃，以成為未來多家票證公司整合之共通介面基礎，透過一個參考性的規範文件，讓 CPU 卡片更加具備互連互通之彈性。此外，面對未來無縫隙大眾運輸系統之需求，如何提供多元載具，以及訂定卡片格式規範，也將是未來值得探討之議題之一。

二、交易安全面之可能衍生議題

1 交易安全與金鑰管控部分

針對未來 CPU 卡導入之後，除了持卡人卡片差異外，由於邏輯加密卡之資訊安全管控模式與 CPU 卡片金鑰管理機制差異很大，可能導致目前既有之前後台系統需要面臨大幅修改。而 CPU 卡在交易正確性與不可否認性上面的提升，也同樣需要針對各票證公司既有營運規章、營運流程、作業準則上加以重新檢視，以適應未來 CPU 卡之交易認證實務需求，諸如此類實務面之影響與評估，未來應進一步探討與分析。

2. 多對多清分清算架構部分

目前國內已有多家票證公司上線運作，面對電子票證未來應用範圍日益廣泛，對於多對多之清分作業需求，亦將日漸增加，而如何有效建構一套低成本、高效率之清分清算架構，實需進一步加以探討。面對交通票證與小額消費應用層面日益廣泛之際，不同之支付方式與交易邏輯，除了交通業者進一步整合營運邏輯外，更需要針對未來多對多清分清算之作業流程進一步加以研究。

第六章 電子票證發行管理條例之衝擊與影響分析

近年來在電子票證業者及民意代表之推動下，立法院於民國 98 年 1 月正式通過「電子票證發行管理條例」，成為我國電子票證可跨業消費的重要法源依據。「電子票證發行管理條例」公告後，金管會分別公告相關施行細則，包括「電子票證發行機構業務管理規則」、「電子票證應用安全強度準則」、「電子票證發行機構負責人兼職限制及應遵行事項準則」、「非銀行發行機構發行電子票證預收款項準備金繳存及查核辦法」等。

本章則主要針對母法「電子票證發行管理條例」及相關實施辦法施行後，對國內電子票證市場的衝擊及影響進行初步分析。

6.1 電子票證營運資格及專營規定對票證公司之影響

一、對發行機構之經營採取核准制

以往交通部對於交通電子票證業者缺乏實質監督的法源，本法則因涉及金融市場吸收存款業務，可能對影響貨幣政策產生擴張的乘數影響，故電子票證主管機關為行政院金融監督管理委員會(以下簡稱”金管會”)，且採取核准制，即發行機構經主管機關核准後始得辦理發行電子票證、簽訂特約機構及其他經主管機關核准之業務。此乃由於電子票證服務具有吸收存款之性質，故宜由金管會透過適度管制，以避免對金融秩序及貨幣政策產生不利的影響。

原已營運中的票證公司須在半年內申請核准，但為避免對現有交通電子票證發行業者衝擊過大，對於非多用途支付之電子票證發行業者(即僅應用於交通工具付費之電子票證)，交通部於民國 98 年 7 月制定「非多用途支付使用交通電子票證核准基準」，其中第四條規定：「本部依本基準所為核准，以五年為上限，發行機構最遲應於核准期限屆滿前六個月內，依電子票證發行管理條例向行政院金融監督管理委員會申請並完成設立許可或業務核准」，現有電子票證業者若為非多用途支付使用，可依該基準向交通部申請核准，惟五年之後仍需回歸「電子票證發行管理條例」向金管會申請核准，這項規定對於現有電子票證業者有五年的緩衝期，讓現有電子票

證業者不致因無法符合「電子票證發行管理條例」要求，而面臨違法營運之困境。

依本條例之規定，電子票證之發行機構，其最低實收資本額為新臺幣三億元，應由發起人於發起時一次認足，並以股份有限公司組織為限。三億元的資本額限制對於較大型的企業而言，並不構成進入門檻，但已足以排除許多為電子商務業者提供金流服務的中小型廠商，因此，電子商務業者若希望採用跨平台、產業的電子票證付款機制時，可能只有尋求與大型的電子商務平台業者或其他發行實體電子票證業者的合作。

二、須專業經營電子票證業務

發行機構須專業經營電子票證業務，主要的目的是為避免主管機關監理範圍擴及發行機構其他兼營之非金融業務；而本法公布前已經金管會核准發行電子票證之金融機構，其原即屬金管會監理範圍，故特別規定其不受專業經營之限制。

然而，對於其他發行單一用途儲值卡的廠商而言，若欲將其發行之儲值卡轉為多用途使用，限制發行機構必須專業經營電子票證業務就會造成相當大的困難。以發行 icash 卡的統一超商股份有限公司為例，由於其並非在本條例公布施行前業經金管會核准發行電子票證之金融機構，故無法適用前述「不受專業經營之限制」之例外規定，若其欲跨企業使用，則須「重新」申請核准發行，如此即會受到專業經營之限制，可能就必須另外將 icash 卡業務移轉予新設立專門從事電子票證發行之公司來經營。亦即，發行電子票證之機構，原則上不會是提供商品或服務的企業。

6.2 電子票證發行管理條例對於持卡人的保障

一、持卡人預付款項之保障

目前國內電子票證業者發卡總量多 2 千萬張以上，持卡人的預付款項十分可觀，以國內最高發卡量的悠遊卡公司為例，其資本額為 5 億元，發卡量已高達 1800 萬張，若以每張悠遊卡餘額平均 200 元計算，其預付款總額已高達 36 億元，次高的高雄捷運公司發卡量已達 150 萬張，預付款總額亦已達 3 億元，若上述電子票證公司對於持卡人預付款沒有善加保管，將可能嚴重影響金融秩序以及民眾對電子票證的信賴。

為確保持卡人權益，本條例第 18、19、20 條明定，若非屬銀行之發行機構，其發行電子票證所收取款項達一定金額以上時，須繳存足額準備金，並應就其餘金額全部交付信託或取得銀行十足履約保證，並將該金額用途限制於支付特約機構商品對價、持卡人要求返還餘額、信託財產運用及運用信託財產所生孳息之分配，始可動用信託財產；同時，依本條例第 29 條第 2 項規定，「銀行發行電子票證所預先收取之款項，應依銀行法提列準備金，且為存款保險條例所稱之存款保險標的。」另持卡人對存放於信託業者之信託財產，就因電子票證產生之債權有優先於發行機構其他債權人及股東受償之權利，透過這些規定保障持卡人預付款項之權利。

如有違反前開繳存準備金或全額信託或擔保之規定者，其行為負責人處七年以下有期徒刑且得併科新臺幣一億元以下罰金，刑責非常嚴厲，故擔任發卡機構之負責人須特別留意。同時，如信託契約或履約保證契約期限屆至而未續約或訂新契約者，不得再發行新卡及接受持卡人儲存金額，違反者將處以六十萬元以上三百萬元以下罰鍰。

惟依本條例前開規定，銀行以外之發行機構除須提撥準備金外，尚須將全額預收款項交付信託或全額履約保障，是否對過於嚴苛，而導致發卡機構資金運用之過度限制，反而阻礙服務品質的提昇，而銀行並不適用此一規定，可能形成與可發行多功能電子票證之銀行間不公平競爭，確有再加以探討的空間。

二、持卡人個人資料與安全性之保障

本條例第 21 條規定，「I：發行機構及特約機構，對於申請人申請或持卡人使用電子票證之個人資料，除其他法律或主管機關另有規定者外，應保守秘密。II：發行機構不得利用持卡人資料為第三人從事行銷行為。」；第 26 條規定，「發行機構應確保交易資料之隱密性及安全性，並負責資料傳輸、交換或處理之正確性。」

由於電子票證無論是記名或無記名，其所可支付之商品或服務愈多，紀錄持卡人生活型態或消費習慣之訊息即愈多，如何避免相關訊息之不當洩漏或利用，以維護持卡人之隱私，亦是應該關切之議題。

相較於前述預付款項相當具體化的保障，本條例對於因電子票證使用所蒐集、產出或累積之資訊，除限制發行機構為得利用持卡人資料為第三人從事行銷行為外，僅規定就「個人資料」應保密，就交易資料應確保隱

密性及安全性，而違反者亦僅有行政罰鍰。事實上，電子票證發行機構所取得持卡人之資料，並不限於個人資料，非屬個人資料的部分，發行機構除自行利用外，亦可與他人合作或提供予他人利用，顯然超出持卡人合理預期，可再探討是否有必要給予一定程度的規範。

至於交易資料隱密性及安全性的問題，電子票證的發行機構若無法有效保護這些資訊，勢將造成更嚴重的社會問題，主管機關應儘速依本條例第17條第2項：「發行機構之業務、財務與其他應遵循事項之管理規則，由主管機關定之。」參酌銀行有關資訊安全管制之規範，定出電子票證發行機構有關個人資料及交易資料保密及安全性應遵循事項之管理規則。

6.3 電子票證發行管理條例對票證整合之影響

就電子票證與icash類型的電子儲值卡相較，由於交通電子票證牽涉不同票種(如全票、兒童票、敬老票)、依距離收費、轉乘優惠等營運規則，其收費機制較為複雜，而電子儲值卡僅為電子錢及忠誠點數等之紀錄，其機制相對而言較為單純。因此，純就技術而言，由交通電子票證轉應用在小額消費的困難度較低，而由電子儲值卡轉應用在交通付費的困難度較高，所以較可能的整合方式是由交通電子票證業者協調超商業者，將交通電子票證讀卡機裝設在超商內，而非將電子儲值卡讀卡機裝設在交通工具內。

電子票證的整合涉及法規、市場、技術等多面向的因素，當然不是本條例通過即可解決。國內現行各廠商所發行的儲值卡、電子錢包、禮券等，許多發行量都已達到一定的市場規模，從電子票證是否能被民眾所接受的角度來觀察，顯然市場已相當成熟，但若由整合成為「一卡通」的目的來觀察，綜觀我國電子票證發行現狀，交通電子票證已因交通部推動之「交通電子票證一卡通計畫」，整合簡化成北、中、南三區交通電子票證系統，朝全區一卡通目標邁進；而小額消費現金儲值卡則以icash卡發卡量最大且通路最多。但現有龐大的各種行業的儲值卡發行量，因為不同系統所採用的讀卡機及卡片結算機制的不同，反而可能成為彼此整合的一種障礙。

本條例僅為非銀行業者發行多支付用途電子票證提供法律依據，並未更積極於條例中鼓勵既有儲值卡發行業者彼此間的整合，亦未排除可能整合上法規適用的困難。因此，電子票證系統業者整合的方向，恐怕並不是既有的儲值卡業者彼此共榮共存、交互結算的整合，而是電子票證發行機構須逐步協調其它

單一用途的儲值卡發行業者接受其電子票證，進而放棄自行發行的儲值卡。

舉例而言，悠遊卡與 icash 卡的整合，因為悠遊卡和 icash 卡的讀卡機不同，若要整合此二系統，讓消費者持有悠遊卡或 icash 卡，都可以任意搭乘捷運或在 7-11 消費，預估雙方所付出的系統軟、硬體置換成本，將無法從所能獲得的利益中回收，故可行的作法應是悠遊卡公司說服 7-11 置換為可讀取悠遊卡的讀卡機，逐步說服 7-11 採取悠遊聯名卡的方式，由悠遊卡公司代為發行 icash 卡或讓 icash 卡直接消失。其主要原因在於悠遊卡背後的機制過於複雜，包括：社會福利(免費搭乘)、區段票價、不同交通工具折扣等，既有的 icash 機制較難直接進行系統整合，而 icash 除了紅利機制之外，僅作為支付工具使用較為單純，將其系統納入悠遊卡的子系統內相對容易且成本較低。

由這個例子也可以發現，本條例雖然沒有特別偏向由某一發行機構整合其它儲值卡發行機構的立意，但既有的交通電子票證已與交通設施整合建置，且系統功能與運輸業者的營運規則密切關連，不可能為整合其它行業的票證系統而予以更換，故交通票證業者在整合方面顯然較銀行或其它儲值卡發行機構更為有利。然而，若未鼓勵或強制業者間的整合，則既有的單一用途儲值卡業者可能因為發行多支付用途之電子票證管制太嚴格，經營成本過高，反而傾向於維持既有的儲值卡發行現況，對於多用途「一卡通」目標的追求反而形成阻力。

因此，本研究建議電子票證產業應該有類似「公協會」的組織，以討論各票證業者整合時可能面臨的各項問題，包括安全強度認定、卡片資料格式、金鑰認證方式等技術性議題；也必須處理各應用系統中交易邏輯、金流、資訊流等營運面的問題。惟金管會對其管轄之產業公協會的組成有監理的責任，若電子票證產業公協會的類似組織係以研究電子票技術或營運管理等為成立宗旨，與金管會管轄業務無關，則金管會基本上不會介入；但若成立的目的若涉及金管會管轄業務，則參加公協會的成員必須是經金管會核准成立之電子票證專業公司，必須比照銀行公會的成立條件及資格。依照目前電子票證產業僅有悠遊卡公司業經金管會核准成立為電子票證公司之外，尚無第二家，因此金管會此立場將使電子票證產業公會的成立倍增困難。

另外，若合法之電子票證專業公司擬將清算業務委外，且接受委外的公司也是金管會核准成立之電子票證專業公司，則金管會可以個案審查是否同意，但不一定核准；反之，則一定不行。

由於電子票證公協會組織可能無法在短期內成立，若未來二、三年電子票

證業者無法像手機業者透過市場力量制定出一套電子票證的整合機制時，建議應由國家透過立法及行政力量介入，訂定電子票證系統間整合所應共同遵循的規範或參考文件，以利電子票證之整合更順利、成本更低廉，都是未來推動電子票證整合所可考慮的方向。

6.4 電子票證發行管理條例對與現行電子票證業者的影響

「電子票證發行管理條例」正式實施之後，目前僅有台北悠遊卡公司於民國 99 年 1 月 28 日取得金管會核准，成為國內第一家可執行小額消費業務的電子票證專業發行機構。本法的頒布實施，對國內目前營運中之電子票證公司分別產生不同的影響，概述如下。

一、台北悠遊卡公司

悠遊卡公司於民國 98 年 6 月與 icash 策略聯盟發行「icash 悠遊卡」，並於民國 99 年 4 月 1 日正式上線，超過一萬個通路店面可同時使用悠遊卡、悠遊聯名卡及 icash 悠遊卡。icash 悠遊卡之卡片格式、功能均與現有悠遊卡相同，只是具有 icash 忠誠優惠記點功能，因此 icash 僅有一個晶片，由悠遊卡公司進行後台清算。

同時為拓展中南部市場，台中市及高雄市客服據點也於 4 月開張營運，可服務持卡人卡務處理及通路商故障設備報修等。

在卡片資料格式上，小額消費與計程車、動物園門票、掛號費、學校福利社等均共同使用「小額消費」的欄位進行使用記錄，在查詢機查詢歷史紀錄時，僅能顯示，「小額消費」，無法顯示使用通路或商店名稱，詳細使用通路或商店須向悠遊卡客服中心查詢。

悠遊 CPU 卡目前已進入 CC(Common Criteria 國際認證)階段，正式上市時間尚不明確。

二、遠通電子收費公司

遠通電子收費公司係於民國 93 年 3 月獲得高速公路局「民間參與高速公路電子收費系統建置及營運」BOT 案最優申請人資格，而取得 ETC 之經營特許權。遠通電收「e 通卡」目前仍無法跨業使用，係依據「電子票證發行管理條例」規定，電子票證專營公司虧損不得超過資本額 1/3，與 BOT 案初期呈現虧損之正常情況有所衝突所致，因此，目前金管會尚在審議中。

三、高雄捷運公司

高雄捷運所發行之「一卡通」係以高雄捷運公司之名義發行，依本法規定，本法落日條款屆臨前，高雄捷運公司必須成立一家「專業經營電子票證業務」之公司接管其電子票證業務，或將其「一卡通」委由可合法經營電子票證業務之公司發行及營運，否則「一卡通」僅能使用於高雄捷運本身營運之載具上，不得再支付其它運輸公司之交通載具及其它支付用途。

由於高雄捷運目前的載客量尚未達成損益兩平，董事會是否同意投資成立「專業經營電子票證業務」之公司或將其票證業務委外營運，則尚未定論。

四、台灣智慧卡公司

由於公路汽車客運業者除北部業者之外，其餘地區的業者幾乎處於損益兩平，甚至虧損的狀態，對於以公路汽車客運業者為股東主體的台灣智慧卡公司而言，要募集三億元的資本額確實會有實質上的困難。

據了解，該公司仍積極拓展發卡業務，包括金門地區及台鐵新竹-基隆-瑞芳路段，對於如何因應「電子票證發行管理條例」的落日條款，該公司董事會則尚未達成共識。

第七章 結論與建議

7.1 結論

- 一、就國內廠商的 IT 技術能力而言，對一機多卡驗票機的研發並不困難，然多卡整合後所衍生的營運規則差異、商業利益的衝突、重覆投資後台以及因清分所增加的成本等，有必要經由協商機制，以降低因多卡整合反而增加營運成本。同時也必須考量卡片新技術演化的速度，對前端設備建置成本的衝擊，以及各運輸業者(尤其是公路汽車客運業者)營運規則差異化對電子票證整合的影響。
- 二、在一機多卡整合的五個執行階段中，第一階段(票證資料格式確認階段)與第二階段(營運邏輯與營運模式協商階段)是整合困難度與共識分歧度最高的階段。
- 三、一機多卡整合模式雖然可以透過軟硬體技術達到一機整合多卡的目的，但仍然無法避免不同票證公司在票證資料格式與營運邏輯上整合之基本困難。
- 四、一機多卡整合模式對不同角色之權益關係人的影響(包括持卡人、運輸業者及政府)，以不同縣市具有優惠身分之持卡人跨區使用時，所產生之優惠折扣差異，最容易使民眾困擾。
- 五、一機多卡整合模式對電子票證產業生態，可能發生關係轉換的結果，大致可以分為主導權的轉變、營運面的轉變以及關係面的轉變等三種變化。
- 六、一機多卡整合時所面對之影響因素，包括：運輸規範整合、驗證流程整合、交易邏輯整合、交易資訊整合、運輸代碼整合與區域特性宣導等。
- 七、因為邏輯加密卡加密過程被破解，加上 IC 卡的多功能應用逐漸普及，CPU 卡已成為未來電子票證的主流載具。
- 八、中國大陸邏輯加密卡(M1)卡升級方案包括：1.強化 M1 卡片安全應用系統方案、2.CPU 卡片兼容 M1 卡應用系統方案及 3.CPU 卡替換 M1 卡應用系統方案三種。

九、中國大陸人民銀行頒布的《PBOCv2.0 規範》是以 EMV 的規範為制定基準，《建設事業非接觸式 CPU 卡 COS 技術要求》和《PBOCv 2.0 規範》電子錢包相關規範幾乎完全相同，此顯示在全球化的趨勢之下，制定電子票證規範應考慮參考國際共通規範。

十、我國「電子票證發行管理條例」頒布之後，對於票證公司的經營、持卡人的保障、票證整合的條件等，均產生明顯的影響。其中以落日條款、票證公司資本額的限制以及專營規定等，對現行的票證公司的影響最鉅。

十一、電子票證發行管理條例對現行電子票證業者的影響如下：(1)台北悠遊卡公司於 99 年 1 月 28 日取得金管會核准，成為國內第一家可執行小額消費業務的電子票證專業發行機構；(2)遠通電子收費公司囿於與高公局合約的限制，是否可以跨業營運非屬高速公路收費範圍之業務，目前尚無法確定；(3)高雄捷運「一卡通」係以高雄捷運公司之名義發行，依本法規定，落日條款屆臨前，高雄捷運公司必須成立一家「專業經營電子票證業務」之公司接管其電子票證業務，或將其「一卡通」委由可合法經營電子票證業務之公司承接發行及營運，否則「一卡通」僅能使用於高雄捷運公司本身營運之載具上。由於高雄捷運目前的載客量尚未達成損益兩平，董事會是否同意投資成立「專業經營電子票證業務」之公司，或將其票證業務委外營運，則尚未定論；(4)台灣智慧卡公司以公路客運業者為股東主體，對於如何因應「電子票證發行管理條例」的落日條款，該公司董事會則尚未達成共識。

7.2 建議

一、「一機多卡驗票機」乃一概念性的說法，其系統架構及元件規格將因廠商所採用的技術而異，故建議不宜訂定設備規格，否則將限制廠商研發新技術的能力，然訂定必要的功能規範則有其必要性。

二、根據本研究的訪談及觀察，以國內資訊產業的研發能力，應用一機多卡整合模式交易並不困難，但是：(一)如何因應卡片晶片技術的快速發展？(二)如何整合運輸業者差異頗大的營運規則？前者為票證業者的營運風險；後者則建議透過政府輔導、協助以達成共識，公路汽車客運業者可由「中華民國公共汽車客運商業同業公會全國聯合會」先行凝聚全省客運業者之共識後再考量是否由政府輔導。

三、建議一機多卡整合模式策略期程分短、中、長期三階段，短期採交易分流策略，中期採管線共構策略，長期採聯合處理策略。

四、採用一機多卡整合模式時，為減少不同票證系統跨區使用時，增加建置系統的複雜度，建議運輸業者之應用代碼應由主管機關加以統一，包括：路線代碼、業者代碼、載具代碼、司機代碼等。

五、採用一機多卡整合模式時，由於各家票證公司之清分清算作業差異頗大，建議採取清分清算分流模式，透過運輸業者管理系統將各票證系統所需之清分清算資料交易檔，分別依據各票證公司清分清算系統介面所要求之格式傳送到各票證公司後台主機，以進行交易驗證與清分清算作業。

六、在「一機多卡整合模式」下，具備優惠身分之持卡人跨區使用時，將產生不同地方政府補貼的優惠措施不同，而造成優惠折扣不同的情形，建議應有相關配套措施與規劃。

七、考量不同票證系統的持卡人跨區使用時，可能發生與各地區票證系統營運規則不符的情形，而導致民眾的不便與誤解。建議採「屬地主義」為主，「屬票證公司」為輔的原則，透過商業談判建立相關的配套措施。

八、綜觀國際 CPU 卡的發展歷程，皆先訂定共同規範以供相關設備及系統供應商遵循，如國際金融/信用卡的主要技術標準—EMV；中國《建設事業 CPU 卡作業系統技術要求》、《建設事業非接觸式 CPU 卡晶片技術要求》；中國人民銀行所頒布的《PBOCv2.0 規範》則以 EMV 的規範為制定基準，建議未來金管會可作為制定相關標準之參考。

九、SONY 為讓 FeliCa 能與符合 ISO/IEC/IEC 國際標準的 IC 卡整合，與 PFILIPS 聯合開發 NFC(Near Field Communications)技術，並成為 ISO/IEC/IEC 18092 國際標準。故建議我國發展 CPU 卡亦應先制定與國際接軌之規範，以降低建置成本及增加開拓應用市場之可能。

十、由於電子票證公協會組織必須接受金管會的監理，若在短期內無法成立，則建議應由國家透過立法及行政力量介入，訂定電子票證系統間整合所應共同遵循的規範或參考文件，以利電子票證之整合及創造規模經濟的條件。

參考文獻

1. <http://zh.wikipedia.org>；維基百科
2. <http://www.icfw.com.cn>；”城市一卡通應用與發展”網站
3. <http://www.nxp.com>；NXP_MIFARE_Plus_leaflet
4. <http://smarticcard.blog.sohu.com/144743726.html>；《建設事業非接觸式CPU卡 COS 技術要求》和 PBOC 電子錢包的區別。。
5. <http://www.jreast.co.jp/suica/index.html>；JR 東日本網站
6. 陸永寧，非接觸式 IC 卡原理與應用，電子工業出版社(北京)，2006 年。
7. 廣州周立功單片機發展有限公司，快速易用的主流非接觸式智能 IC 卡，2008 年。
8. 住房與城鄉建設部，關於發布行業產品標準「建設事業 CPU 卡操作系統技術要求」，2008 年 12 月。
9. 住房與城鄉建設部，關於發布行業產品標準「建設事業非接觸式 CPU 卡晶片技術要求」，2008 年 12 月。
10. 鄭菀瓊，簡評「電子票證發行管理條例」，科技法律透析，2009 年 3 月。
11. 賴文智、彭珮瑄，，「電子票證發行管理條例」實務議題研究，2009 年 5 月。
12. 廣州致遠電子有限公司，MIFARE S50/S70 到 PLUS CPU 卡升級方案，2009 年 7 月。
13. 住房和城鄉建設部 IC 卡應用服務中心，城市公用事業 IC 卡應用方案介紹，2009 年度城市公用事業 IC 卡應用和技術發展研討會會刊論文集，2009 年 11 月。
14. 住房和城鄉建設部 IC 卡應用服務中心，城市事業 IC 卡密鑰管理系統介紹，2009 年度城市公用事業 IC 卡應用和技術發展研討會會刊論文集，2009 年 11 月。
15. 恩智浦半導體，讓您的想像力自由馳騁--恩智浦智能識別技術讓您到達

夢想之地，2009 年度城市公用事業 IC 卡應用和技術發展研討會會刊論文集，2009 年 11 月。

16. 張轉輝，建設部標準公用事業 IC 卡項目方案研究，2009 年度城市公用事業 IC 卡應用和技術發展研討會會刊論文集，2009 年 11 月。
17. 袁育博，方便快捷的 M1 卡升級 CPU 卡改造方案，2009 年度城市公用事業 IC 卡應用和技術發展研討會會刊論文集，2009 年 11 月。
18. 張一鋒，如何成功實施非接觸 CPU 卡項目，2010 年 1 月。
19. 張綱，淺談非接觸式 IC 卡晶片技術的發展趨勢，2010 年 4 月。
20. 吳昊，城市 IC 卡收費系統升級為 CPU 卡的典型問題研究，2010 年 8 月。
21. 黃彥棻，臺大電機教授示範無線竄改悠遊卡金額，2010 年 9 月。
22. 王惠儀，國內公交一卡通市場現狀掃描，中國移動研究院，產業市場所，2010 年 9 月。

附錄 1

期中報告審查意見回覆表

附錄 1 期中報告審查意見回覆表

一、開會時間：99 年 7 月 22 日下午 2 時

二、開會地點：運研所五樓會議室

三、主持人：王組長穆衡

紀錄 黃立欽

四、出席單位及人員：(略)。

五、主席致詞：(略)。

六、簡報：(略)。

七、討論：

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
遠通電收公司	1. 請問簡報中提及採用「輪詢法」及「同詢法」的兩家實作廠商，是否能在相同的條件下作交易時間多寡之比較？	簡報所提「輪詢法」及「同詢法」的數據係參考實作廠商，在不含營運規則下之交易時間參考資料，主要係讓外界了解其作法。而實際交易時間必須包含營運規則才算完整交易，亦將隨程式優化程度不同而有所差異，在此不另作交易時間之估計。	同意研究單位處理情形。
	2. CPU 卡的安全性固然較高，但是交易速度會較慢，研究團隊是否能探討 CPU 卡在一機多卡下對交易時間的影響？	CPU 卡交易時間會較 Mifare 卡長，是因為其金鑰驗證的流程較為複雜，此可透過勒體程式優化加以改善。 TaiwanMoney 卡是 CPU 卡，目前在南區交通 IC 卡的應用上與 Mifare 卡整合時，其單筆交易時間可在 0.6 秒以內完成。而目前市面上之多卡通讀卡機尚未進入實作階段，因此，無法針對 CPU 卡在一機多卡下來做交易時間的影響分析。	同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
萬碁公司	1. 請問票證整合後，運輸業者如何將清分資料送到清算後台？	基本流程請參考本研究期末報告 4.1.2 節之圖 4-2，至於實際的清分流程可能因每家票證公司的清算交易方式不同而有所差異。	同意研究單位處理情形。
臺灣智慧卡公司	1. 請問 CPU 卡之交易時間，是否會因一機多卡交易而呈現交易速度較慢的問題？是否能提出解決之道？	請參閱遠通電收審查意見 2 之回覆辦理情形。	同意研究單位處理情形。
	2. 請問簡報第 10 頁中所規定的 0.6 秒交易時間是否包含完整的交易時間？而目前交通部科技顧問室提出的一機八卡的交易時間規範為 0.6 秒請問是如何定義？	一般而言，實際的採購規範上所定義之「交易時間」是指包含完整的交易流程所需的時間。據了解，交通部科技顧問室對於交易時間的規範為最低要求，因此，其規範之時間 0.6 秒並不包含「營運規則」在內。	同意研究單位處理情形。
	3. 請問「輪詢法」及「同詢法」完成個別交易程序分別之耗費時間為何？	就廠商之宣稱(本研究無法驗證)未含營運規則均可於 0.6 秒內完成，惟耗費時間多寡，將視各個廠商對驗票機及卡片韌體撰寫的技術能力而定。	同意研究單位處理情形。
	4. 簡報第 20 及 21 頁所建議的後台清分流程交由第三者執行的規劃似乎與金管會的規定不符，是否可加以說明？	目前本研究並未獲悉金管會有類似的相關規定，有關金管會對「公協會」類似組織的意見請參閱期末報告 6.3 節第 6 段「因此，本研究主張電子票證產業應該有類似「公協會」的組織....」。	同意研究單位處理情形。
悠遊卡公司	1. 臺鐵局的自動驗票閘門目前正在建置一機多卡的整合工程，有關交易資料整合規範將不涉及各公司的清分作業之機制，本公司認為設計理念不錯，建議研究團隊可進一步了解。	敬悉。	同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
中華電信研究所	<p>1. 多卡交易最重要的關鍵是營運模式，如何從一(票證公司)對多(運輸業者)，轉變成多(票證公司)對多(運輸業者)的模式？</p> <p>2. 另外，開發成本由誰分擔之問題應該要先加以釐清，例如當多卡交易的系統全部都建置完成後，如新增一個票證系統要加入整合，其所衍生出來的成本應如何分攤？</p> <p>3. 建議多卡交易所使用的驗票機盡量簡單，只要負責 I/O 的 security 部分，交易邏輯層的運算不要放在驗票機中，如此才能簡化驗票機的設計。</p> <p>4. 採用「輪詢法」時，若加入黑名單的比對，對交易時間會產生明顯的影響，建議研究團隊將此因素納入考量。</p> <p>5. 請問現在欲進行之「卡卡通」的策略與過去「一卡通」的策略，在政府部門係如何考量？</p>	<p>請參閱本研究期末報告 4.2 節。</p> <p>開發成本分攤之計算涉及各系統使用者的需求及後續衍生之商業利益，請參閱期末報告 4.2.6 節第 3 段「未來如果新增一個票證系統…」及表 4-10。</p> <p>敬悉。</p> <p>無論是採用「輪詢法」或「同詢法」，在判別出卡片發行單位後，仍然均必須進行黑名單比對之程序。</p> <p>「一卡通」當時之環境係以最小經費及最短時間做為整合之考量，惟因當時之整合係以票證公司為主導，因其中有票證公司對於卡片整合有所疑慮，因而改由市場來引導整合。今年度交通部因爭取到公路公共運輸發展之經費，欲以一機多卡之設備進行整合，並由運輸業者擔任主導者，希望以此為開端，開啟另一個整合之契機，對於民眾而言，仍是以其持有之交通電子票證，在不另購其他電子票證情況下，可以搭乘裝置多卡通讀卡機之運輸工具。</p>	<p>同意研究單位處理情形。</p> <p>同意研究單位處理情形。</p> <p>同意研究單位處理情形。</p> <p>同意研究單位處理情形。</p> <p>同意研究單位處理情形。</p>

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
高雄捷運公司 (書面意見)	1. 依據報告書 3.4 節一、指出邏輯加密卡已逐漸被 CPU 卡取代，若既有票證公司已發行 CPU 卡(如 TaiwanMoney 卡)，目前業界整合的技術而言，驗票機是否仍可同時驗證多種類型卡片？	邏輯加密卡與 CPU 卡的金鑰驗證方式不同，但是卡片與驗票機的通訊協定可以一致，因此驗票機是否可同時讀取兩種卡片則視讀卡機的韌體與硬體設計而定。	同意研究單位處理情形。
	2. 對於將發行 CPU 卡之票證公司而言，其系統重置或修改之成本為何？	此將視票證公司所採用的 CPU 卡與是否有向下與 Mifare 卡相容而定，例如 CPU 卡採用 Mifare Plus，因具備與 Mifare Classic 往下相容的能力，故系統重置或修改之成本會比其它卡廠的 CPU 卡低。請參閱本研究第三期期末報告 4.3 節、4.4 節。	同意研究單位處理情形。
	3. 依報告書 7.2 節，研究單位提供成立電子票證公協會組織之建議，本公司樂觀其成，惟請問交通部是否將接續訂定規範並促成相關組織產生？抑或相關工作係由金管會繼續辦理？	電子票證管理條例通過施行後，主管機關為行政院金管會，後續公協會組織之成立，建議由主管機關協助推動辦理。	同意研究單位處理情形。
交通部臺灣鐵路管理局	1. 目前本局所進行的自動閘門多卡整合作業，係已規定前端設備所有的票證資料先送到本局的伺服器，再依照各票卡的清算後台進行清分。	敬悉。	同意研究單位處理情形。
	2. 各業別是否需要一機多卡設備，應視其提供的服務內容而定，有些服務(例如醫院掛號費、路外停車場停車費)僅侷限在某些特定的族群，似乎無裝設必要；至於一機需要容納幾卡應該由業務單位自行決定。	敬悉。	同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
交通部高速鐵路工程局	1. 在一機多卡的情況下，由驗票機送到各票證公司清算後台的營運資料是由誰負責安全認證？	若一機多卡的運作模式採取交易分流機制，則由各票證公司自行認證。	同意研究單位處理情形。
	2. 請問 TaiwanMoney 卡及 Mifare 卡的 Reader Module 有何差異性？	在硬體層面，只要支援 ISO14443 Type A 的所有 Reader module 皆可讀取 TM 卡，因此可以讀取 Mifare 卡片之 Reader 模組理論上也應該可以讀取 TM 卡，其主要差異點在於金鑰驗證之流程以及交易處理流程，此乃屬於 Reader 模組之韌體程式的差異。	同意研究單位處理情形。
	3. 採用「輪詢法」或「同詢法」對現有設備的衝擊如何？	「輪詢法」是指 SAM 與讀卡機主控制單元為單工模式，目前的驗票機以採此種模式為主；「同詢法」則是 SAM 與讀卡機主控制單元為多工模式，二者的硬體設計不同。就廠商所提之「同詢法」而言，均必須更換現有設備。	同意研究單位處理情形。
交通部公路總局	1. 簡報提及本局目前建置的公車動態資訊系統的路線編碼應是 4 碼而非 5 碼，請予以更正。	已修改。	同意研究單位處理情形。
	2. 請問「一機多卡」與科顧室所提出的「多卡通讀卡機」意義是否相同？	「一機多卡」係本研究對「設備整合」方式之驗票機的通稱，並未涉及功能規範制定；而科顧室所提之「多卡通讀卡機」則係市面上新型的驗票機，並制定其功能規範，二者在意義上並不能劃為等號。	同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	3. 請問簡報第 8 頁，遠通 ETC 卡與其它票卡整合時，其 OBU 如何讀取其他票證公司的卡片？	就本研究的了解，目前的 OBU 只能讀遠通 ETC 卡。	同意研究單位處理情形。
	4. 簡報第 24 頁，桃園客運與台北客運並非「共同經營」，應係「聯營」。	已修改。	同意研究單位處理情形。
	5. 簡報第 30 頁，路線代碼是由本局統一規定，不是由客運業者自行協商決定。	已修改。	同意研究單位處理情形。
	6. 簡報第 36 頁，在既有模式下，設備提供的責任是票證公司，似乎與現況不符，請研究單位進一步加以說明。	請參閱期末報告 4.2.4 節「一、主導權的轉變：...」。	同意研究單位處理情形。
	7. 簡報第 36 頁，請研究團隊再補充說明，賠償責任在既有模式下由票證公司負舉證責任，而未來將改由運輸業者負舉證責任的理由。	此部分肇因於不同營運模式下，主導權轉變後，運輸業者對設備管理責任與運作風險之變化，請參閱期末報告 4.2.4 節「一、主導權的轉變....」。	同意研究單位處理情形。
交通部路政司	1. 期中報告所謂「營運規則」的定義是什麼？需要簡化的範圍是什麼？建議以全票及法定優待票為主，其餘部分可以分階段予以簡化。	期中報告所謂「營運規則」源自各票證公司之驗票設備驗證規範準則，詳細內容請參閱期末報告 4.2.1 節第 3~6 段「針對「營運規則」一詞，..」及表 4-2。	同意研究單位處理情形。
	2. 如依照金管會電子票證發行管理條例的規定，簡報第 21 頁管線共構型的建議及其他章節所提的電子票證公協會組織的成立都將有困難。	1. 期中報告所謂「管線共構型的建議」為中期發展可能模式，類似台鐵自動閘門多卡整合作業，將前端設備所有的票證資料先送到共用之伺服器，再依照各票卡的清算後台進行清分，惟各票證公司之資料是否涉及交易資料安全與隱私性資料，仍須視法令是否允許而定。	同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
		2. 有關金管會對「公協會」類似組織的意見請參閱期末報告 6.3 節第 6 段：「因此，本研究主張電子票證產業應該有類似「公協會」的組織....」。	
國立成功大學交通管理科學研究所林佐鼎教授	<p>1. 本研究中「台灣通」與「悠遊卡」利用前端設備整合的案例是否也可以複製到其它票證系統？是否還會衍生出額外的問題？</p> <p>2. 國外應用 CPU 卡(如香港八達通、日本 Suica 等)似乎沒有所謂交易時間延遲的問題，為何國內會有此種疑慮？</p>	<p>本研究案例架構上，可以推論到其他一機雙卡相關模式可行，但因不同票證公司之規範與作業亦不相同，一機三卡與一機四卡所產生之問題更加複雜，亦可能衍生其他問題，因此可能無法直接複製適用。</p> <p>國外 CPU 卡應用於交通電子票證的案例都是單一電子票證系統，驗票機對卡片的安全認證均已於事前規劃妥適，並未有跨系統整合的情形，故不會造成交易時間延遲問題。</p>	同意研究單位處理情形。
高雄市政府捷運工程局施嬌嬌總工程司	<p>1. 請研究團隊說明本研究執行已將屆滿四年，所面臨的關鍵課題為何？相關策略之建議為何？</p> <p>2. 本研究權益關係人包括營運主體(業者)、票證公司、系統商及持卡人等，彼此間之利益顯有衝突，就技術面而言應可克服，惟計畫付諸實施尚待商業談判或公權力介</p>	<p>本研究認為各種電子票證系統的整合關鍵是在制定卡片共同規範以供前端設備供應商遵循量產，如此才能簡化整合的複雜度及降低前端設備的製造成本。此策略觀點可由國內金融卡在可在各 ATM 進行跨行轉帳、提款，以及手機業者門號可互通的實例中獲得證實。</p> <p>針對權益關係人在一機多卡交易模式運作後，可能產生主導權與角色責任變化，請參閱期末報告 4.2.4 節。</p>	同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	入，就此，研究團隊是否提供未來發展方向供主辦單位參考？		
	3.一機多卡整合涉及 6 個類型、20 個影響因素，研究團隊是否參考現有案例，收斂影響因素，俾使研究計畫具體可行。	針對權益關係人在一機多卡交易模式運作後，可能產生主導權與角色責任變化，請參閱期末報告 4.2.4 節	同意研究單位處理情形。
本所王穆衡組長	1. 簡報第 8 頁所提 TaiwanMoney 卡將於明年 6 月 8 日終止營運，而萬事達國際組織在路政司召開的會議中表示目前尚未定案；另簡報第 10 頁「...，若 SAM 卡在插槽的位置愈後面，卡片交易所花費的時間為線性關係遞增」，此處所謂「線性關係」需要更嚴謹的證明，應該只有「遞增」的事實，上述內容均請一併修正。 2. 請研究團隊再進一步探討一機多卡整合對權益關係人的角色產生何種轉變，例如客運業者對票證的主導權是否會由整合前的被動角色改為主動等議題。 3. 請研究團隊探討將 GPS 模組與電子票證計費模組整合所可能造成的票價計算誤差，其責任的歸屬問題。 4. 請研究團隊進一步探討電子票證發行管理條例中，釐清有關禁止產業相關業者成立「產業組織」的相關議題。	已修訂，請參閱期末報告 2.2 節之表 2-2；第三章第 1 段「本研究第三期以模擬驗票機實機測試證實....」。 針對權益關係人在一機多卡交易模式運作後，可能產生主導權與角色責任變化，請參閱期末報告 4.2.4 節。 請參閱期末報告 4.2.1 節「四、設定環境類..... 2. 設備參數差異....」。 有關金管會對「公協會」類似組織的意見請參閱期末報告 6.3 節第 6 段：「因此，本研究主張電子票證產業應該有類似「公協會」的組織....」。	同意研究單位處理情形。 同意研究單位處理情形。 同意研究單位處理情形。 同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	5. 請研究團隊探討營運規則的定義，並就簡報第 28 頁的「營運邏輯與營運模式協商階段」，運輸業者要與票證業者談判的議題為何？一併予以深入探討。	在一機多卡交易模式運作後，運輸業者要與票證業者談判的議題，請參閱期末報告 4.2.5 節第 4 段「依據宏碁公司執行....」。	同意研究單位處理情形。
本所運管組	1. 本案進度經檢視符合合約規定。	敬悉。	同意研究單位處理情形。
	2. 有關 P2-6 提及六、設備整合多卡交易速度之測試與影響評估部分，請補充說明該測試係採用「輪詢法」方式進行測試。	已補充。	同意研究單位處理情形。
	3. 有關 P3-4 提及一機多卡整合模式整體架構分析，請先將票證整合技術之演進予以說明，例如本研究前期採用「輪詢法」方式進行測試，為何當時不採用廠商宣稱「同詢法」測試，其背景因素為何？請再予補充說明。	請參閱期末報告 3.2 節第 1 段「本研究前期採用「輪詢法」方式進行測試，...」。	同意研究單位處理情形。
	4. 有關 P3-4 提及本研究應用「層級分析法」將電子票證產業分成五個產業部分，請說明分成此五個產業之理論依據為何？係學理依據、文獻引用抑或為自創？請補充加以說明。	層級分析法(AHP, Analytical Hierarchy Process)是一種分析工具，本研究引用「層級分析法」分析電子票證產業則是引用本研究研究員許安慶之碩士論文：「以複雜性科學論析智慧卡產業之發展及策略模式--以建置「墾丁 e 卡」為例」，P3-19，2002 年，中山大學企業管理學系碩士班」	層級分析法是專有名詞
	5. 有關 P3-8 以一機多卡驗票機整合模式而言，若政府「將以政策補助地方建置電子票證，則應考慮影響票證整合	請參閱期末報告 3.2 節第 8 段「以一機多卡驗票機整合模式而言，則應考慮票證整合議題下，各種因素的影響	同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	之相關因素，其中可能包括.....」，請將文義加以修正。 6. P3-9 影響一機多卡整合因素中之六、優惠補助類似乎遺漏，請加以補充說明。	分析，包括.....」。 請參閱期末報告報告 3.2 節第 8 段「六、優惠補助類...」。	
本所運管組	7. 有關 P3-12 倒數第四行「一方面驗票機需要知道所接觸卡片是哪一家票證公司所發行，進而才可呼叫該家票證公司的 SAM 來產生衍生金鑰並存取卡片；另一方面則必須由卡片中儲存內容來研判卡片屬於哪一個票證業者發行？」此兩者就文義內容來看，驗票機都是想知道卡片為何種票證公司發行，但其差別為何？請予以說明。	此兩段敘述文義相同，期末報告已一併修改。	同意研究單位處理情形。
	8. 有關 P3-13 三、卡片歸屬判斷迴圈最佔時間的處理乃在於卡片的金鑰衍生作業中，對於卡片歸屬之判別過程並未加以說明，是否係圖 3.3.2-1 所示之流程，請予以補充說明。	卡片歸屬之判斷迴圈包含於圖 3-7，補充說明請參閱期末報告 3.3.1 節「三、卡片歸屬判斷迴圈最佔時間的處理乃在於卡片的金鑰衍生作業...」	同意研究單位處理情形。
	9. 有關 P3-18 表 3.3.3-2 富譽公司一機多卡驗票機實機測試結果中，並未就 SAM 卡增加後，完整交易時間為何？加以說明，請予以補充。	已請富譽公司協助提供檢測數據，補充說明請參閱期末報告 3.3.2 節之表 3-5~7。	同意研究單位處理情形。
	10. 有關 P3-24 二、中期策略：管線共構之定義為何？請補充說明。	期末報告所謂「管線共構型的建議」為中期發展模式，主要目的乃希望透過一個前處理平台，提供業者營收資料處理與後端多個票證公司	同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
		資料傳遞，類似台鐵自動閘門多卡整合作業，將前端設備所有的票證資料先送到共用之伺服器，再依照各票卡傳遞到清算後台進行清分。	
本所運管組	11.請研究單位一併說明所提出短、中、長期建議策略之分析基礎為何？	有關短、中、長期建議策略主要分析基礎為信用卡發展模式與交易型資訊系統架構為基礎。	同意研究單位處理情形。
	12.有關 P4-15 一機多卡整合模式影響層面分析部分，請增加影響因素與影響層面關係間之舉例說明。	請參閱期末報告 4.2.3 節之表 4-6。	同意研究單位處理情形。
	13.有關 P4-20 有關整合因應方向部分，究竟係五種或六種？請予以釐清。	有關整合因應作法共六項，請參閱期末報告 4.2.3 節之表 4-5。	同意研究單位處理情形。
	14.有關 P5-1 第五行，由於非接觸式邏輯加密卡晶片採用的是「流密碼技術」？請予以補充說明何謂「流密碼技術」。	流密碼相對於區塊加密，是製造一段任意長的金鑰元素，與明文依位元或字元結合，輸出的串流根據加密時的內部狀態而定。請參閱期末報告第五章註釋 1。	同意研究單位處理情形。
	15.有關 P5-1 邏輯加密卡升級為 CPU 卡之趨勢說明部分，請再加強兩卡之技術演進、成本、計算能力及廠商選用之考量等比較說明。	邏輯加密卡與 CPU 卡兩種卡片類種的總稱，各卡種有不同的製造廠商及所屬型號，每種卡片所應用的技術各不相同，本研究選擇具有市場代表性之卡種補充說明，請參閱期末報告 5.1.3 節「三、MIFARE Plus 之升級方案之探討...」	同意研究單位處理情形。
	16.有關 P5-2 CPU 卡的傳輸標準以讀寫器發送射頻信號的載波調製深度，為何以 100% 及 10% 區分為 Type A 或 Type B 兩種標準？請予以補充說明。	請參閱期末報告 5.1.2 節「一、CPU 卡的傳輸標準...」	同意研究單位處理情形。

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	17.有關 P5-3 Type A 的防衝突機制係基於「BIT 衝突檢測協議」，而 Type B 是通過「位元組、幀及命令」來完成防衝突，請分別就「BIT 衝突檢測協議」及「位元組、幀及命令」加以補充說明。	請參閱期末報告第五章註釋 2、3。	同意研究單位處理情形。
	18.有關 P5-4 非接觸式 CPU 卡晶片記憶體的發展中，請就「EEPROM」、「Mask ROM」及「Flash Memory」予以加強名詞說明。	請參閱期末報告第五章註釋 4、5。	同意研究單位處理情形。
	19.請研究單位就期中報告初稿之文字及語意部分再予以檢視並改正。	已於期末報告一併修訂。	同意研究單位處理情形。
主席結論	1.經徵詢在場委員同意，台灣世曦工程顧問股份有限公司所提期中簡報內容審查通過，請研究單位依據相關程序辦理第二期款請款事宜。	敬悉。	同意研究單位處理情形。
	2.相關單位所提之口頭及書面意見，均請研究單位依據本所契約規定之意見回覆表格式妥為予以回覆。	敬悉。	同意研究單位處理情形。

附錄 2

期末報告審查意見回覆表

附錄 2 期末報告審查意見回覆表

一、開會時間：99 年 12 月 2 日上午 10 時

二、開會地點：運研所十樓會議室

三、主持人：王組長穆衡

紀錄 黃立欽

四、出席單位及人員：略

五、主席致詞：(略)。

六、簡報：(略)。

七、討論：

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
遠通電收公司	1.研究團隊建議公路客運的營運規則可透過各區同業公會加以整合，但如何從各區同業公會所整合之區域性營運規則，過渡到全國性營運規則之整合？ 2.請問目前公路總局或路政司對於客運業者多卡通驗票機的補助，是否已考量未來與 CPU 卡相容或預留可擴充之空間？ 3.本研究所提之票價補貼原則可採「屬地主義為主，屬票證公司為輔」，然而，票證整合之後應沒有「屬地主義」的概念，請再補充說明「屬地主義」的定義。 4.遠通電收「e 卡通」無法跨業使用與高公局之契約無關，係電子票證發行管理條例規定，電子票證專營公司虧損	本研究建議公路客運運輸業者之營運規則可透過「中華民國公共汽車客運商業同業公會全國聯合會」進行整合。 據本研究了解，該補助計畫已針對未來之 CPU 卡預留可擴充之空間。 已補充說明，請參閱期末報告 4.2.3 節第 5 段「本研究建議於在「一機多卡整合模式」導入初期....」。 已修正，請參閱期末報告 6.4 節「二、遠通電子收費公司...」。	同意研究單位處理 同意研究單位處理 同意研究單位處理 同意研究單位處理

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	不得超過資本額 1/3，與 BOT 案初期呈現虧損之正常情況有所衝突所致，因此，目前金管會尚在審議中。		
宏碁公司	1. 本研究凸顯「商業技術」的整合議題才是交通電子票證整合的問題核心，可供後續研究單位參考。	敬悉。	同意研究單位處理
臺灣智慧卡公司	1. 交二版對於段次、里程計費、逃票等營運規則的規範不夠明確，以本公司為例，在票證整合的過程中的確造成票證公司及運輸業者之間很大的困擾。	相關營運規則之規範並非交二版之設計重點，應屬運輸業者與票證公司談判之範圍；且其設計亦非針對票證整合，因此，本研究才提出交三版(草案)之建議。	同意研究單位處理
悠遊卡公司	1. 目前在營運規則的整合部分以「特許上」最複雜，因為此規定會影響各客運公司對逃票的認定及營收的短缺，故很難達成共識。	敬悉。	同意研究單位處理
	2. 研究團隊對邏輯加密卡升級為 CPU 卡的解決方案可供本公司未來發行 CPU 卡時參考。	敬悉。	同意研究單位處理
交通部臺灣鐵路管理局	1. 一機多卡整合的議題中，關於營運規則的整合部分，應視運輸業者的經營特性而異，因此不應強制規範。	本研究所謂「營運規則」之議題主要係指公路汽車客運部分，不包括台鐵、捷運等大型軌道運輸業者。補充說明請參閱期末報告 4.2.1 節第 3、4 段「針對「營運規則」一詞，...」。	同意研究單位處理
	1. 目前本局進行一機四卡的閘門整合作業中，從 SAM 卡的取得直到實際進行驗證作業，過程中花費相當長的時間，故未來國內若欲推廣 CPU 卡，若沒有統一的規範，至少也要有卡片版本、	敬悉。	同意研究單位處理

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	資料格式等相關規定，以減少整合之困難。		
交通部高速鐵路工程局	1. 目前本局對驗票機的規劃為一機八卡，研究團隊對多卡整合的建議可供本局參考。	敬悉。	同意研究單位處理
	1. 「桃園機場捷運線」未來是否可使用 CPU 卡，與台北悠遊卡公司推出 CPU 卡的時程有關，請台北悠遊卡公司盡可能提早提供悠遊 CPU 卡的規範供本局參考。	敬悉。	同意研究單位處理
	1. 面對「電子票證管理條例」之落日條款規定，台灣智慧卡公司及遠通電收公司將如何作為，也請提早告知本局以便予以因應。	敬悉。	同意研究單位處理
交通部科顧室	1. 有關交通電子票證之整合，建議可如同信用卡(VISA、MasterCard)或金融卡一樣，有第三方認證機構對前端設備、卡片技術演進等進行認證，以減少運輸業者及票證公司的困擾。	敬悉。	同意研究單位處理
交通部公路總局(書面)	1. 目前乘客搭乘公路客運車輛(里程計費)，若於下車後忘記刷卡或驗票機異常等情形，將會造成乘客刷出產生異常，因而未完成付費交易，致該票證遭鎖卡，以致於下次再搭乘公路汽車客運車輛時，即無法刷卡付費乘車，此時民眾則必須回該客運公司之總站進行解卡，才能繼續使用，如此亦將會影響該民眾無法搭乘其他公路汽車客運公司之車輛。現階段於區域範圍內此一問題即已影	有關”鎖卡”及”解卡”係應用電子票證系統的參數予以設定及解除，係屬運輸業者間營運服務之議題，必須透過商業互助或商業談判解決，並非票證技術之問題。	同意研究單位處理

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	影響民眾之權益，倘未來票證之推動達全區多卡通後，民眾由高雄到台北觀光旅遊後，因上述情形而必須回高雄進行解卡者，勢必將造成民眾之反彈及影響電子票證之推動成效，爰此一議題，研究團隊可否於契約內，於期末報告書中提供相關可行之解決方案。		
國立成功大學 交通管理科學 研究所林佐鼎 教授	1.本研究對 CPU 卡的探討似乎太偏重中國的作法，至於其它歐美地區是否也有票證整合的作法可供參考？	相較於歐美地區，中國近年來對於交通 CPU 卡的技術投資及應用研究相對積極，故本研究以中國為主要的探討對象。至於歐美地區 CPU 卡的應用，主是金融 (EMV 即為 CPU 卡的規範之一) 及通訊(如手機及 RFID 設備)，且各主要產業均有其所屬的規範可供遵循，比較沒有同業整合的問題。	同意研究單 位處理
	1.一機多卡驗票機新增票證系統成本概算，是否可依據實際的案例作為計算基礎？若無，是否可能會與實際狀況差異太大？	已補充說明，請參閱期末報告 4.2.6 節第 3 段「未來如果新增一個票證系統...」及表 4-10。	同意研究單 位處理
	2.本研究認為運輸業者與票證公司於「營運邏輯與營運模式協商階段」會面臨各種談判議題，以目前公路客運對 IC 卡技術的了解，是否有能力與專業的票證公司在資訊不對稱的情況之下進行談判，研究團隊的建議為何？	建議公路汽車客運可透過全國聯合會的力量，挑選各客運業者優秀的資訊人才加以訓練，搭配其善於談判之業務主管，便可匯集力量與票證公司進行商業談判。	同意研究單 位處理
	3.悠遊卡公司的 CPU 卡即將進入發卡的階段，而國內 IC 卡的規範仍停留在民國 92 年頒	由於電子票證之主管機關為金管會，建議可將本研究之成果移交金管會卓參。	同意研究單 位處理

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	布的交二版，是否能夠符合現況的需求？研究團隊的具體建議為何？		
高雄市政府捷運工程局施嫩嫩總工程司	<p>1.有關運輸業者與票證公司於「營運邏輯與營運模式協商階段」之談判議題：</p> <p>(1)建議不對跨區優惠票提供優惠，請問何謂跨區優惠？</p> <p>(2)建議一般卡種(全票)扣款，則敬老卡、博愛卡(已編預算優惠補貼)，如何扣款並享優惠？</p> <p>2.一機多卡驗票機新增票證系統概算每套總成本多少？是否可能成為業者無法協商整合之關鍵？</p> <p>3.票證一卡通整合涉技術性、成本面等議題，而權益關係人包含運輸業者、票證公司、系統廠商，技術性不是問題，非技術面影響因子影響廣泛且較鉅，建議交通部自政策面著手，由交通部成立票證公司，由各權益關係人投資入股，以收整合之效。</p>	<p>請參閱期末報告 4.2.3 節第 1 段「票證公司成立初期均有區域性...」。</p> <p>請參閱期末報告 4.2.3 節第 3 段「在「一機多卡整合模式」下...」</p> <p>已補充說明，請參閱期末報告 4.2.6 節第 3 段「未來如果新增一個票證系統...」及表 4-10。</p> <p>本研究之成果可供相關決策部門進一步探討。</p>	<p>同意研究單位處理</p> <p>同意研究單位處理</p> <p>同意研究單位處理</p>
本所王穆衡組長	<p>1.本研究將營運面的問題歸納為「非技術問題」，建議改為「商業技術問題」，「技術問題」改為「票證技術問題」，以免前者被誤解為不重要。</p> <p>2.富譽公司所提供之輪詢法多卡交易時間可能係各 SAM 卡最終累加之結果，為何 SAM3 排序第三順位時交易時間總反而縮短，請研究團隊再確認。</p>	<p>遵照辦理，已於期末報告中修正。</p> <p>已請富譽公司重新提供測試數據，修訂及補充說明請參閱期末報告 3.3.2 節「作法一：富譽公司最佳化「判斷卡片歸屬」流程...」及表 3-5~7。</p>	<p>同意研究單位處理</p> <p>同意研究單位處理</p>

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	3.有關「屬地主義」的議題，請研究團隊再補充說明。	請參閱期末報告 4.2.3 節第 5 段「本研究建議於在「一機多卡整合模式」導入初期....」。	同意研究單位處理
	4.有關一機多卡所衍生之整合成本，其計算單位、施工範圍、參考資料來源等，請研究團隊再補充說明。	已補充說明，請參閱期末報告 4.2.6 節第 3 段「未來如果新增一個票證系統...」及表 4-10。	同意研究單位處理
本所運管組	1. p4-20 有關 4.2.3 節係僅就優惠折扣情形對不同權益關係人的影響進行分析，因此，章節題目應予修正。同時建議內容應分別先就優惠折扣情形(包括法定優惠、公司或路線優惠等)先予探討後，再就整合後跨區部分採原區域之身分別折扣方式或整合後跨區部分不予優惠分別做優、缺點比較方為妥適。	已補充說明，請參閱期末報告 4.2.3 節。	同意研究單位處理
	2. 表 4.2.3-1 「一機多卡整合模式對不同角色之權益關係人影響」中，亦係僅針對權益關係人優惠折扣部分予以探討，因此，表之名稱及內容亦請予以適度修正。	已修訂，請參閱期末報告 4.2.3 節之表 4-4。	同意研究單位處理
	3. p4-24 表 4.2.3-3 「一機多卡整合模式因應作法與各層級權益關係人之關係」中，其中次要權益關係人應為「系統整合商」，請予以修正。	已修訂，請參閱期末報告 4.2.3 節之表 4-6。	同意研究單位處理
	4. p4-28 最後一段文字在敘述完後，應加上「因此，本研究所提出之因應作法有助於一機多卡整合模式之推動更為順利」語意較為完整。	已補充說明，請參閱期末報告 4.2.5 節。	同意研究單位處理

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	5.p4-31 有關表 4.2.6-2「一機多卡驗票機新增票證系統所需成本概算」應先將基本前提予以確立，例如此估算基礎是否係以新加入的票證公司已具備其建置基礎下，而在多卡通讀卡機及其附屬相關設備中(DPS、CPS)，估算其他票證公司、運輸業者等應配合修改之相關軟、硬體設備成本項目。	已補充說明，請參閱期末報告 4.2.6 節第 3 段「未來如果新增一個票證系統...」及表 4-10。	同意研究單位處理
	6.p5-23 有關卡片交易流程中所提及之專有名詞，例如 PBOC、GPO、PDOL、AIP、AFL 等，請將其英文完整名稱列出，並增加中文名詞解釋。	已補充說明，請參閱期末報告 5.2.2 節「二、中國交通 CPU 卡與 EMV 規範的關聯性... 第 6 段：電子現金的應用是圈存交易...」頁尾註釋 6~9。	同意研究單位處理
	7.p5-34 第一段部分，請增加註解解釋何謂 NRZ 編碼?何謂曼徹斯特編碼?其意義為何?	已補充說明，請參閱期末報告第五章註釋 12、13。	同意研究單位處理
	8.p6-6 有關台北悠遊卡公司部分之第二行說明，應不只 icash 悠遊卡可於一萬個以上通路店面使用，一般悠遊卡或銀行發行之悠遊聯名卡也可進行一般小額消費使用，請予以補充修正。	已於期末報告中修正。	同意研究單位處理
	9.請研究單位就期末報告初稿之文字及語意部分再予以重新檢視並改正。	已檢視及修正。	同意研究單位處理
主席結論	1.本所運輸資訊組「智慧財產權之研究案」所委託之查核機構發現，一機多卡驗票機已有國內廠商申請部份技術專利，請各採購單位進行採購時注意智慧財產權的查核。	敬悉。	同意研究單位處理

與會代表 (依發言順序)	審查意見	回覆辦理情形	主辦單位 查核意見
	2.在一機多卡的情況下，運輸業者對票證公司的選擇將擁有主導的力量，公路客運運輸業者應透過全國聯合會凝聚共識，與票證公司進行各項商業談判。	敬悉。	同意研究單位處理
	3.本研究前期成果「交三版」對於卡片資料格式的統一，以及如何應用於整合營運規則等都已提出完整的建議，研究團隊可於本期期末報告中摘錄重點提示，供後續研究者參考。	已補充說明，請參閱期末報告 2.1 節「三、交三版草案卡片規格與交易流程...」。	同意研究單位處理
	4.本案之期末審查原則性通過，請研究團隊依據委員及各單位之意見填寫審查意見回覆表，並於 99 年 12 月 20 日前提送期末報告定稿。	遵照辦理。	同意研究單位處理

附錄 3

專家學者座談會會議紀錄

附錄 3 交通電子票證系統共通技術規範研究與票證

一卡通推動計畫 專家學者座談會會議紀錄

一、開會時間：九十九年十月十四日(星期四)上午十時

二、開會地點：運研所五樓會議室

三、主持人：吳榮煌 資深協理

紀錄 許安慶

四、出席單位及人員：

交通電子票證系統共通技術規範研究與票證—一卡通推動計畫(1/4)

公路總局

專家學者座談會—交通電子票證CPU卡發展趨勢

吳善樞

與會人員簽到表

(素食者請於簽名後面註明「素」字)

與談人

中華電信研究所 謝嘉新 博士

成功大學交通管理科學系 李威勳 助理教授

萬事達卡國際組織 王純鍵 資深經理

公部門與會代表

行政院金管會

臺灣鐵路管理局

交通部運研所

票證業者與會代表(依筆畫排序)

台灣高鐵股份有限公司

高雄捷運公司

悠遊卡公司

科技顧問室

路政司

臺灣智慧卡公司

遠通電收公司

旅易股份有限公司

五、主席致詞：(略)。

六、簡報：(略)。

七、與會單位發言

1. 中華電信研究所繆嘉新博士

- (1) 目前所討論的交通 CPU 卡電子票證已非單純地應用於交通領域，在跨業消費的應用需求下，卡片交易的安全性當然是首要考量的因素，但還要同時考量卡片的效能及成本。
- (2) 在制定交通 CPU 卡卡片的技術及規範上，應該要參酌採用現有的國際標準標準，以便降低各應用系統間設計的複雜度。
- (3) 以 Mifare 做為非交通用途之跨業消費的卡片，因為交易型態及環境變得更複雜，無法再應用後台做為最後一道的安全防線，故採用安全性較佳之 CPU 卡為必然的趨勢，但是國內目前並沒有關於交通 CPU 卡的安全規範可供遵循，建議可考慮以悠遊卡正在規劃中的 CPU 卡安全規範為業界參考的依據。

2. 成功大學交通管理科學系李威勳助理教授

- (1) 由邏輯加密卡轉換為 CPU 卡已是必然的趨勢，但是轉換的過程不宜拖太久，以免新的 CUP 卡技術不斷翻新演化，甚至出現比 CPU 卡更完善的解決方案，如此有可能造成前、後期轉換的系統又面臨無法整合或相容的現象。
- (2) 多卡整合面臨的另一個難題可能是營運面的問題，包括各業者之間商業利益的衝突、卡片外觀的統一(如外碼及照片大小等)，此部份的困難度不亞於技術面的整合，建議公部門必要時應介入協調以便加速整合績效。
- (3) CPU 卡在應用上最有機會與 NFC 產品結合，例如手機，建議日後研究可探討台灣是否也有此趨勢及商機的存在。

3. 萬事達卡國際組織王純鍵資深經理

- (1) 萬事達卡國際組織當初即已提供目前仍屬先進技術的 CPU 卡給宏碁團隊建置「南區交通 IC 卡—TM 卡」，該卡之所以失敗的主要原因有二，一是高雄市的大眾運輸市場規模無法容許兩張交通 IC 卡同時營運，從資料顯示，TM 卡的使用量是在高雄捷運「一卡通」開始營運之後明顯

下滑；另一個原因是，TM 卡團隊並沒有成立票證公司，所以沒有營運主體可以吸收因提供票價折扣所產生的成本，導致持卡人使用意願低落，這是 TM 卡行銷上一直無法克服的問題。

- (2) 萬事達卡國際組織以 TM 卡相同的卡片技術在南非開普敦發卡，從今年五月迄今已發行將近一百萬張卡，南非政府看重的就是 TM 卡的安全技術，故從公車到計程車，在政策上都鼓勵使用 TM 卡。
- (3) 再看國內悠遊卡的成功也可證明，在同一區域內不宜有兩種以上相同類型的卡片任其競爭，因為競爭的結果必導致另一方的失敗，而失敗的代價包含社會成本在內。故交通 IC 卡的在一個區域的成敗，與當地的經營的環境及政策有極大的關連性。
- (4) 兩岸人民的交流愈來愈熱絡，國內的票證業者應該將眼光放在如何與中國所發行的電子票證整合應用，將市場的餅做大，這就必須訂定及遵守一些共同的技術規範，故本人贊成繆博士的看法，電子票證的卡片技術規範應該遵循國際標準規範，以方便與國際接軌。

4. 公路總局

- (1) 公路總局就對客運業者的了解，客運業者對 IC 卡電子票證最在乎的是交易速度及正確性。

5. 高鐵局

- (1) 本局建議研究的成果必須能趕上目前實際建置的進度，否則建置的範圍愈廣，日後升級的困難及成本會愈高。

6. 臺鐵局

- (1) 本局自兩年前開始導入電子票證及自動化收費系統，除北部都會區民眾因為已習慣使用悠遊卡而較順利之外，部份中南部的民眾對於自動化收費系統仍不習慣而徒增本局第一線工作人員的困擾。
- (2) 目前本局正在進行多卡驗票機的建置工程，除驗票機對於多卡的讀寫技術較沒問題之外，對於後端如何與各票證公司清算及對帳等作業模式仍有許多需要再探討及改善的地方。
- (3) 在與各票證公司的業務整合上，因為 IC 卡有安全管控等機制，與本局使用多年的票務作業習慣有諸多待協調的地方，故本局承商目前也花費許多的心力與各票證公司共同努力處理後端的金流作業流程，以及相關

配合設備的修改。

7. 台灣高鐵公司

- (1) 卡片技術係由發卡公司所掌握，對於提供扣款設備的運輸業者如何因應後續加入者卡片技術的修改及所需成本，以及如何預估 CPU 卡驗票機可支援多少的 Mifare 票證系統是一個可以再探討的議題。

8. 台北悠遊卡公司

- (1) 悠遊 CPU 卡目前已進入 CC(Common Criteria 國際認證)階段，對於正式上市時間尚不明確。
- (2) 本公司推出 CPU 卡有三個原因：
- A. 符合主管機關金管會對於小額消費 IC 卡加值上限安全準則的規定。
 - B. NXP 已宣佈 Mifare Classic 的 serial number 將於明年開始改為 7 byte，此措施將可能造成與悠遊卡目前使用的 4 byte serial number 卡片發生重覆號碼的問題。
 - C. 為因應目前使用中的 Mifare 驗票機無法在短期內全部支援 CPU 卡，所以悠遊 CPU 卡在第一階段可以往下與 Mifare 驗票機相容，第二階段視驗票機與卡片是否已全部完成升級再全面轉換為 CPU 卡系統。

9. 台灣智慧卡公司

- (1) 由於各種 CPU 卡有不同的技術，故驗票機在第一時間接觸到 CPU 卡時就可知道是屬於那一家票證公司，此種技術應該可以解決目前多卡同機時交易速度遞增的問題。
- (2) CPU 卡的安全性就加密技術而言是優於目前使用的 Mifare Classic，但是如何選用適合客運用途的加密技術是可以再討論。

10. 遠通電收公司

- (1) Mifare Classic 當初選擇卡種時即已隱約知道 Mifare Classic 的加密法則在國外似乎遭破解，但是當時 CPU 卡的技術無法滿足遠通電收對卡片扣款速度的要求，因此遠通電收 FETC 卡最後採用金資電子錢包的規格，再加上一個不公開的 API 做為 CPU 卡錢包與模擬 Mifare 通訊協定之間的溝通程式。
- (2) 基於安全的考慮，遠通電收 FETC 卡的 Mifare 只能應用於扣款，不能應用在加值上，加值必須透過 CPU 卡的接觸式介面。

(3) 建議政府相關部門能夠制定有關 IC 卡在卡片資料格式、交易流程等各方面的標準或參考文件，如此可減少票證公司在系統開發及整合應用上的困擾及成本。

11. 交通部科技顧問室卓訓榮主任

(1) 交通 IC 卡若要跨業使用在小額消費，使用 CPU 卡是必然的趨勢。

(2) 回應繆博士的說法，CPU 卡的標準應該遵循國際標準。

(3) CPU 卡的優點是安全性高，但是在交易速度方面因此增加，CPU 卡是否能滿足所有交通業者的需求是一個值得探討的議題。

(4) 交三版草案提出時因涉及票證業者可能需要全面換卡的成本考量故暫緩推動，但目前國內票證業者擬全面將目前的票卡換成 CPU 卡，是否可利用此時間點由政府相關部門制定一套標準供業者參考是有考量的空間。

12. 交通部運輸研究所王穆衡組長

(1) 本次座談會將應用 CPU 卡改量的因素歸納為安全、效能、成本、多功能是一個很好的方向，也是本研究案一直努力探討的重點。

(2) 由於「電子票證發行管理條例」已頒佈，交通電子票證各項規範的制定權責將由交通部移轉到金管會，本研究的各項研究成果可提送給金管會參考。

(3) 票證市場在本質上就是一種寡占市場，國內市場不具備多卡發行的容量，但是目前的寡占廠商也不意謂將一直擁有此市場地位，而必須不斷開創創新市場。

(4) TM 卡的營運經驗顯示，好的卡片技術要搭配合宜的應用市場方能成功，這是一個值得學習的經驗。

(5) 交通部在票證市場能著力的地方是在起始階段創造使用電子票證的環境，至於各票證業者之間的競合關係要靠業者彼此協商解決，共同合作努力將市場的餅做大才能進一步創造良好的市場契機。

八、主席結論

1. 本次座談會歸納出 IC 卡在需求面必須著重效能、安全、成本、營運四個層

面，可供日後相關研究參考。

2. 本次座談會除探討 IC 卡的技術、營運面的財務以及法令面等議題外，另外也初步探討 IC 卡跨國應用時可能另須考量政治面及政策等議題，可供後續研究單位持續探討。

附錄 4

專家學者座談會引言簡報

附錄4 專家學者座談會引言簡報

交通電子票證系統共通技術規範研究 與票證一卡通推動計畫(4/4)

專家學者座談會

「交通電子票證CPU卡發展趨勢之探討」



台灣世曦
工程顧問股份有限公司

民 國 9 9 年 1 0 月 1 4 日



簡報大綱

- 壹、計畫背景說明
- 貳、交通電子票證發展趨勢
- 叁、國外電子票證系統不同卡種間轉換
之技術探討
- 肆、以CPU卡為交通電子票證可能衍生之
議題
- 伍、國內交通電子票證CPU卡應用探討

壹、計畫背景說明

3

計畫背景說明

- 本計畫為四年期計畫的第四年期計畫，前三年期計畫已先後完成：
 - 國內電子票證系統營運現況與設備開發現況調查。
 - 交三版(草案)卡片規格與交易流程定義、交三版(草案)卡片驗證機制規劃與驗證系統開發。
 - 設備整合多卡交易速度測試與影響評估等工作項目。
- 本年期計畫擬蒐集國內、外CPU卡之技術規範及發展趨勢，提供國內交通電子票證CPU卡發展之參考。

4

貳、交通電子票證發展趨勢

一、交通CPU卡的使用趨勢及現況

二、MIFARE Classic 的安全危機

三、CPU卡取代邏輯加密卡發展趨勢 的主要原因

5

交通CPU卡的使用趨勢及現況 [1/2]

- 中國政府基於安全及一卡通整合上的必要，住房和城鄉建設部於2008年12月12日正式批准『建設事業CPU卡作業系統技術要求』(標準號：CJ/T 304—2008)
 - 北京公交一卡通於2009年將現在的MIFARE S70卡升級為CPU卡，升級後的系統可以兼容目前使用的MIFARE S70卡。
 - 上海公共交通卡也於2009年4月將原MIFARE晶片升級為CPU晶片。

6

交通CPU卡的使用趨勢及現況 [2/2]

- 韓國首爾已發行2000多萬張可支付交通及小額消費的非接觸式CPU卡--“T-Money”。
- 新加坡引進CPU卡為新版本的“EZLink”。
- 目前CPU交通卡跨業使用最多的行業是銀行與電信業者。



7

主要應用於交通用途的CPU卡 [1/2]

- 恩智浦半導體(NXP)：MIFARE Plus
 - MIFARE Plus在NXP目前的產品平台裏，處於MIFARE Classic和MIFARE DESFire中間。

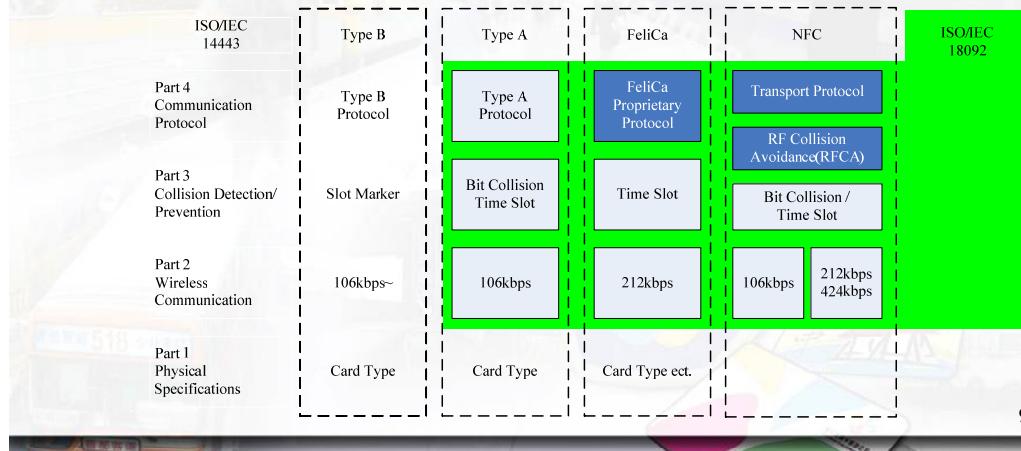
	Ultralight	Ultralight C	Classic	Plus	DESFire
硬體加密	--	3DES	Crypto 1	Crypto 1、AES	3DES、AES
EEPROM	512 Bits	1536 Bits	1K、4KBytes	2K、4K Bytes	2K、4K、6 K Bytes
特性	--	--	--	和 Classic 相容	
國際安全認證				CC EAL 4+	CC EAL 4+
非接觸通訊協定	ISO/IEC14443A-3	ISO/IEC14443A	ISO/IEC14443A	ISO/IEC14443A(-4)	ISO/IEC14443A(-4)
讀卡機晶片	Micore I Micore II				

8

主要應用於交通用途的CPU卡 [2/2]

■ 日本SONY：FeliCa

- ▶ SONY與PHILIPS聯合開發新的NFC技術--NFCIP-1，已成為ISO/IEC/IEC 18092國際標準，可和ISO/IEC/IEC 14443A相容。



9

貳、交通電子票證發展趨勢

一、CPU交通卡的使用趨勢及現況

二、MIFARE Classic 的安全危機

三、CPU卡取代邏輯加密卡發展趨勢

的主要原因

10

MIFARE Classic 晶片卡的加解密過程遭破解

- 在2008年荷蘭曾有論文以PCD-Based的攻擊手法破解NXP的Mifare Classic。
- 臺灣大學電機系教授鄭振牟團隊2010年則使用Sniffer-Based（監聽封包）的攻擊手法攻擊Mifare Classic。
 - 此種攻擊手法的前提是必須能夠監聽到卡片的資料，才能夠進行資料竄改。因此，只能是單張的卡片資料竄改。
 - 對於票證公司而言，只要能夠在系統後端設備進行防堵措施，例如，偵測卡片是否有異常，資料讀取過程中，不要流洩出足夠的資訊可供人利用竄改，便可以確保卡片的安全性。

11

貳、交通電子票證發展趨勢

- 一、CPU交通卡的使用趨勢及現況
- 二、MIFARE Classic 的安全危機
- 三、CPU卡取代邏輯加密卡發展趨勢的主要原因

12

CPU卡的安全性

■ CPU卡內部有雙重安全機制

- 第一重：晶片本身具備加密算法模組，目前比較常見的安全算法有RSA，3-DES等。
 - ✓ 中國另開發國密算法（SSF33，SCB2，SM2，SM3等）來加強晶片的安全性。國密算法是不對外公開的，比其他公開算法的加密算法具有更高的安全性。
- 第二重：CPU卡晶片有COS（Card Operation System）系統。
 - ✓ COS可以為晶片設立多個相互獨立的密鑰，密鑰以目錄為單位存放，每個目錄下的密鑰相互之間獨立，並且有防火牆功能。
 - ✓ 同時COS內部還設立密鑰最大重試次數以防止惡意攻擊。

13

CPU卡的多功能性

■ CPU卡可以實現真正的“一卡多用”

- “一卡多用”每個應用相互獨立並受控於各自的密鑰管理系統。
- 不同應用可以共享一個“錢包”，也可以分別擁有各自的“錢包”。
- 服務商可以通過使用CPU卡進行更加靈活有效的管理，用戶也能使用CPU卡實現多功能應用的需求。

14

叁、國外電子票證系統不同卡種間轉換/相容之技術

一、NXP卡種轉換方案

二、中國卡種轉換策略

15

NXP卡片解決方案-Key Features

- 2 or 4 kbyte EEPROM
- MIFARE Plus X with full feature set, or MIFARE Plus S with simplified feature set.
- Unique serial number: 7 byte (optional 4 byte during migration)
- Delivery types: Wafer or MOA4
- Simple fixed memory structure compatible with MIFARE Classic
- Access conditions free configurable
- Multi-sector authentication / Multi-block read & write
- Anti-tear function for writing AES keys
- Keys can be stored as MIFARE Classic keys (2 x 48 bit per sector) or AES keys (2 x 128 bit per sector)
- Privacy features
- Typical number of single write operations: 200.000



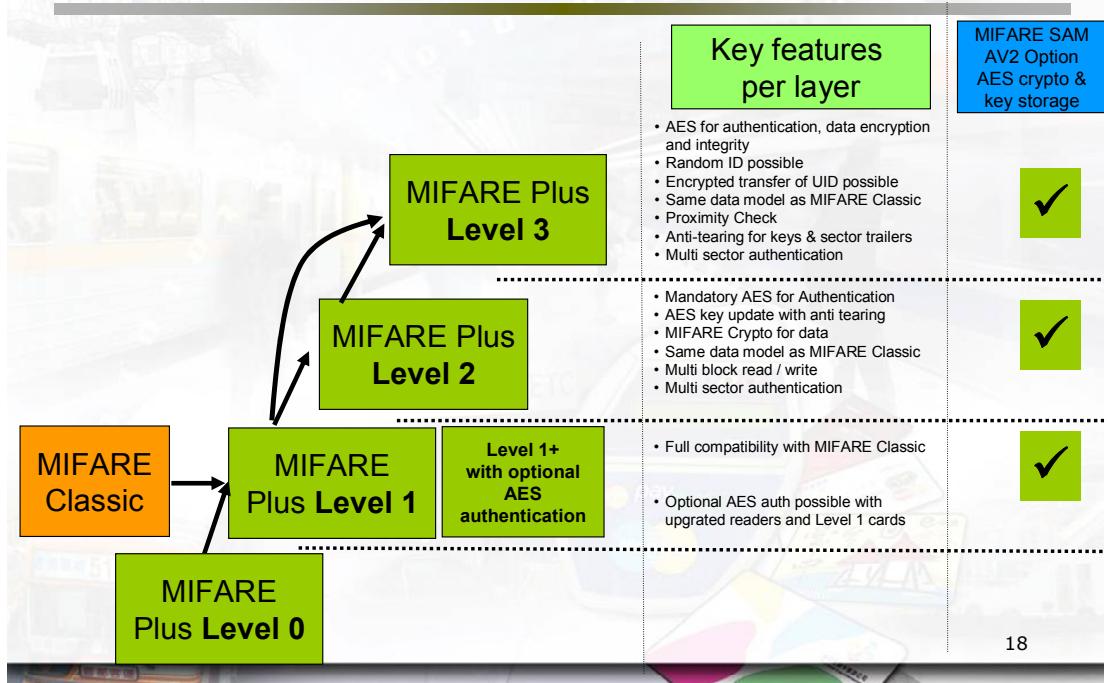
16

NXP卡片解決方案-高安全MIFARE Plus

- State of the art use of Advanced Encryption Standard (AES) instead of CRYPTO1
- AES is approved by the US government authorities for secret documents beyond 2030
- True Random Number Generator (TRNG) tested against AIS 20
- Composite Common Criteria EAL 4+ certification
- Anti tear function for consistent deployment of changing keys and access conditions
- State of the art transmission security using Cipher Message Authentication Code (CMAC) according to NIST Special Publication 800-38B
- Optional Random ID in anti-collision to protect privacy
- MIFARE SAM, for secure storage of AES keys and AES encryption on the reader side.
- Proximity detection as countermeasure against relay attacks.

17

NXP卡片解決方案- MIFARE Plus升級模式



18

叁、國外電子票證系統不同卡種間轉換/相容之技術

一、NXP卡種轉換解決方案

二、中國卡種轉換策略

19

中國卡片轉換策略-方案一

■ 加強M1卡安全應用系統方案

- 以不發行CPU卡為前提下，針對M1卡之弱點加強其全安性

■ 工作計劃及內容重點：

- 多級密鑰管理
- 消費密鑰和加值密鑰的分離
- 一卡一密
- 採用PSAM和認證碼的安全控制
- 黑名單管理
- 限制離線最大交易之金額
- 帳戶管理及審計跟蹤

20

中國卡片轉換策略-方案二

■ CPU卡兼容M1卡應用系統方案

- 以非接觸式CPU卡來逐步取代系統已發行邏輯加密卡，逐步完成現有的邏輯加密卡到CPU卡的升級。

■ 工作計劃及內容重點：

- 制定兼容邏輯加密卡的CPU卡規範和應用規範。
- 制定CPU卡應用結構和交易流程規範。
- 建設符合上述流程和規範的CPU卡模擬測試系統。
- 完成發卡系統的升級改造。
- 試辦發行兼容邏輯加密卡的CPU卡的地區。

21

中國卡片轉換策略-方案三

■ CPU卡替換M1卡應用系統方案

- IC卡整合的最終目標，以CPU卡替換掉現在之M1卡，在支付中停止使用M1卡。

■ 工作計劃及內容重點：

- 兩卡一機
 - ✓ 透過驗票機之改造，在過渡期間內，CPU卡及M1卡皆可以在車載驗票機上使用。
- 逐步替換
 - ✓ 在過渡期內，以行銷方式將M1卡替換為CPU卡。
- 雙系統並行
 - ✓ 過渡期M1卡及CPU卡兩結算系統並行，過渡期結束後，停止M1卡之結算系統。

22

肆、以CPU卡為交通電子票證 可能衍生之議題

23

交通營運面

一. 票證轉換運作議題

1. 卡片轉換做法策略之選擇
2. 平行移轉作業之程序

二. 交通營運邏輯整合

1. 跨區使用規範
2. 跨區優惠與紅利積點

三. CPU卡片規格整合

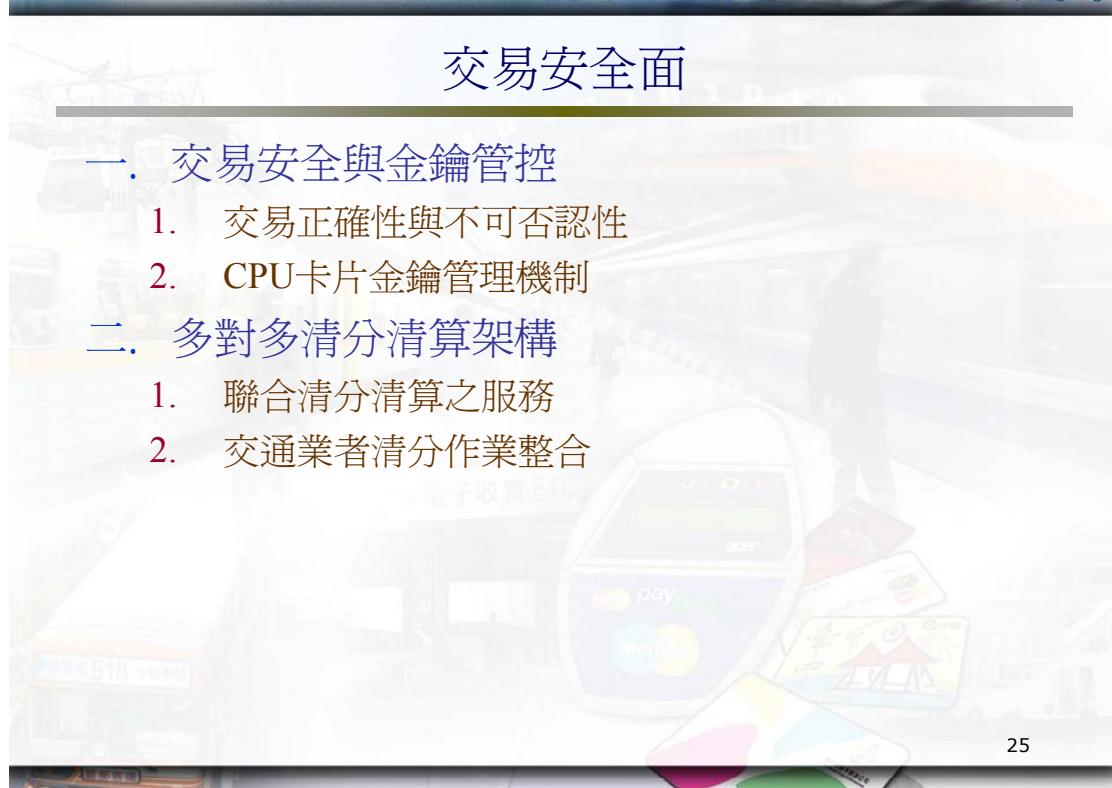
1. 多元載具卡片格式規範
2. 交通領域統一欄位格式之規範

24

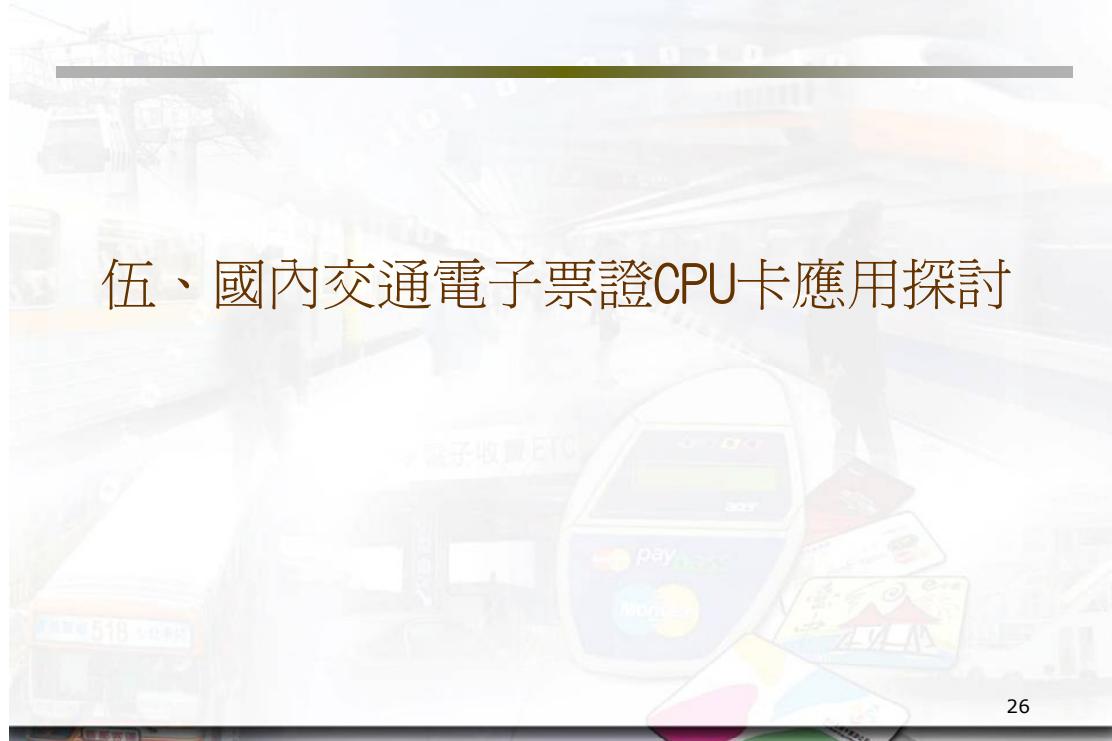
交易安全全面

- 一. 交易安全與金鑰管控
 - 1. 交易正確性與不可否認性
 - 2. CPU卡片金鑰管理機制
- 二. 多對多清分清算架構
 - 1. 聯合清分清算之服務
 - 2. 交通業者清分作業整合

25



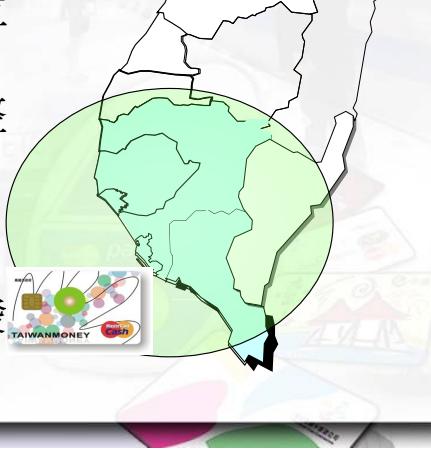
伍、國內交通電子票證CPU卡應用探討



26

Taiwan Money Card 背景介紹

- 於 2004 年開始營運
- 範圍遍及南台灣七縣市
- 營運於 11 家客運、44 個場站、500 家以上便利商店與 2000 輛以上公車與渡輪
- 目前與高雄捷運完成整合
- 採用 MasterCard Cash CPU 卡技術
- 由兩家銀行負責卡片發行作業



27

Taiwan Money Card 應用範圍

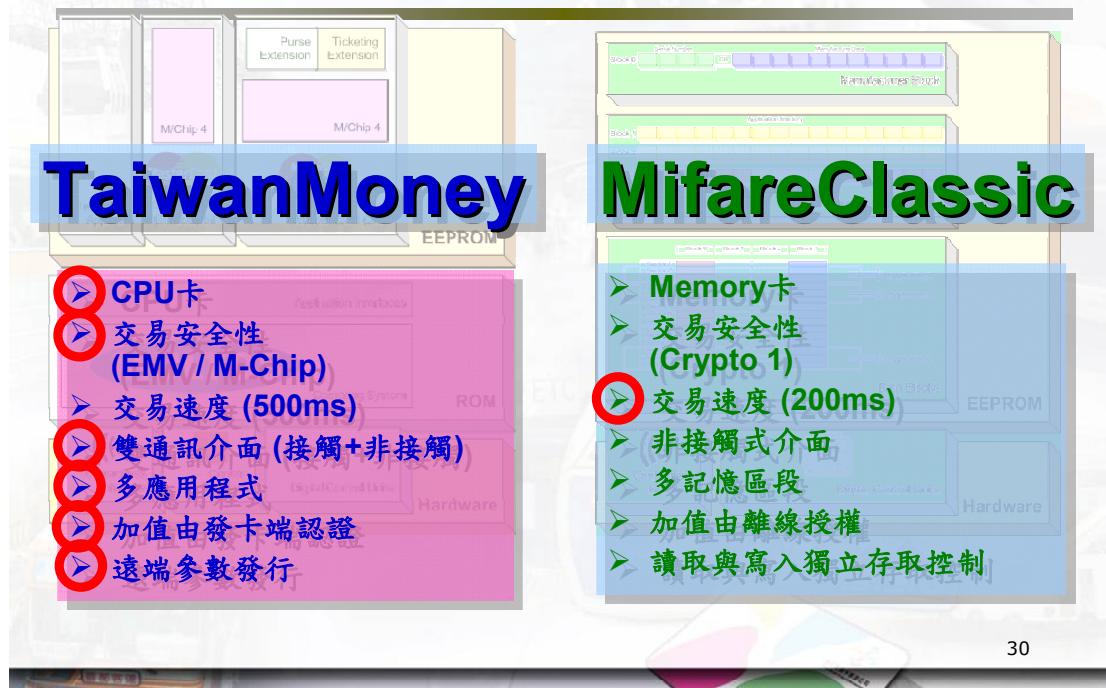


28

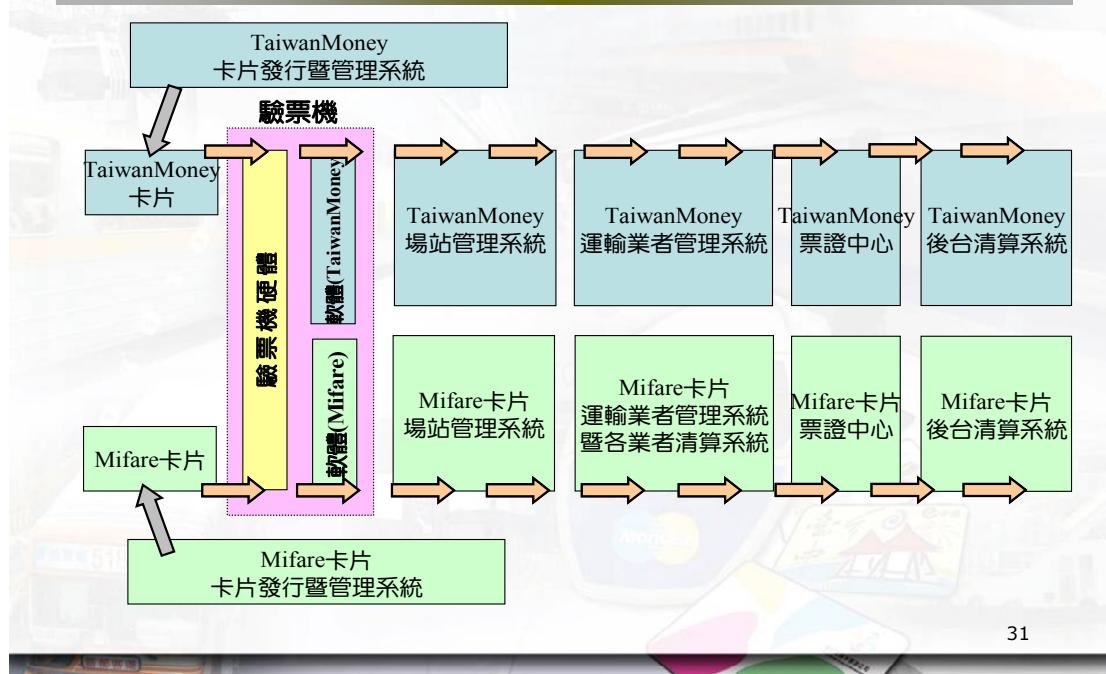
Taiwan Money Card 內部架構



Taiwan Money Card 與 MifareClassic 架構比較



Taiwan Money Card 與高捷卡片整合模式



31

Taiwan Money Card的市場挑戰

- 採用金融最高安全等級之CPU晶片卡，成本比一般記憶型卡片高出四到五倍。
- 電子價金受「銀行發行現金儲值卡許可及管理辦法」管制，銀行資金無法自由運用。
- 市場交易與加值手續費過低，銀行推廣普及困難
- 與信用卡整合之策略因雙卡風暴而失敗。
- 高雄捷運自行發行儲值票卡，造成同一都市有兩家卡片發行單位，未能從發行端即統合資源
- 南部地區之大眾運輸工具使用率過低。

32

簡報結束 敬請指教

附錄 5

期末報告簡報

附錄5 期末報告簡報



- 壹、計畫說明暨票證系統營運現況
- 貳、一機多卡整合模式之技術探討
- 參、一機多卡整合模式之影響因素vs. 權益關係人及因應作法
- 肆、交通電子票證應用CPU卡之探討
- 伍、電子票證發行管理條例之衝擊與影響分析
- 陸、結論與建議

壹、計畫說明暨票證系統營運現況

3/53

本研究前三期計畫成果

- 一. 國內電子票證系統及設備廠商開發現況。
- 二. 電子票證跨系統整合模式評估。
- 三. 交三版草案卡片規格與交易流程定義。
- 四. 交三版卡片驗證機制規劃與檢測系統開發。
- 五. 電子票證系統後台功能整合建議。
- 六. 設備整合多卡交易速度之測試與影響評估。
- 七. 對國內電子票證系統從記憶卡轉換為CPU卡的過程提出建議模式。
- 八. 提出在不同大眾運輸系統的經營環境及策略下，選擇不同票證整合方案的建議。

4/53

本期計畫目的

- 依據本研究案前三期研究的結果，探討政府與民間如何營造一個有利於票證整合與相關技術發展的基礎環境。



5/53

電子票證系統營運現況^[1/2]

統計時間：民國99年10月

系統別 營運現況	悠遊卡	臺灣通	TaiwanMoney	一卡通	金門電子票證	e通卡
營運單位	悠遊卡股份有限公司	台灣智慧卡股份有限公司	萬事達卡國際組織	高雄捷運股份有限公司	金門縣公共車船管理處	遠通電收股份有限公司
開始營運時間	民國91年	民國93年	民國95年	民國97年	民國88年	民國95年
交通應用範圍	台北捷運、聯營公車(台北縣市、基隆、宜蘭、馬祖)、國道客運、纜車、淡水河藍色公路、臺鐵、公有路邊及路外停車場、台北市公共自行車租賃、台中市快捷公車、計程車(敬老愛心車隊)	桃竹苗、中彰投、花東地區及雲林縣部分客運，共11縣市、21家業者；99年6月15日於新竹-基隆-瑞芳間計28站(暖暖站除外)全線售卡；金門縣公車處票證整合建置案進行中。	南部七縣市公車、高雄市輪船、高雄捷運、公有立體停車場	高雄捷運、高雄市輪船、公車(高雄市公車、東南客運、南台灣客運、高雄客運、義大客運及台南市公車)、高雄市立圖書館	公車、渡輪	高速公路(國1、3、5)
驗票機	約16,000部	3,600部	2,327部	2,100部	60部	115.6萬個OBU
累計發卡量	2200萬張	151萬張	28萬張	177萬張	10萬張	140萬張

6/53

電子票證系統營運現況[2/2]

統計時間：民國99年10月

系統別 營運現況	悠遊卡	臺灣通	TaiwanMoney	一卡通	金門電子票證	e通卡
其他應用範圍	小額錢包、學生證、圖書館借、動物園門票、醫院診療費	學生證、停車場	具有小額消費之電子錢包功能	圖書館借書學生證	無	無
今年營運大事紀	<ul style="list-style-type: none"> •民國99年1月成爲第一家經金管會核准發行電子票證之專業發行機構。 •民國99年4月1日悠遊卡小額消費全面上線；該月悠遊卡高雄及台中客服中心正式啓用。 •民國99年10月悠遊卡、7-ELEVEN和中華電信三方攜手合作，成立「悠遊卡紅利積點策略聯盟」。 	<ul style="list-style-type: none"> •民國99年6月15日於新竹-基隆-瑞芳間計28站（暖暖站除外）完成建置。 •民國99年9月1日，臺灣通發行鼎東客山線學生認同卡、通勤認同卡。 	<ul style="list-style-type: none"> •該系統維運服務將於民國100年6月8日屆滿，系統營運廠商必須與高雄市政府續約方能提供系統營運服務。 	<ul style="list-style-type: none"> •民國99年4月提供『一卡通手機貼』功能。 	<ul style="list-style-type: none"> •民國99年度5月辦理系統更新招標，由台灣智慧卡公司得標建置。 	<ul style="list-style-type: none"> •民國99年7月推出「全民體驗ETC」及「ETC成功扣款即享95折優惠」，鼓勵民眾裝置OBU。 •民國99年11月06日至100年12月31日止，推出「全民體驗ETC方案」。

貳、一機多卡整合模式之技術探討

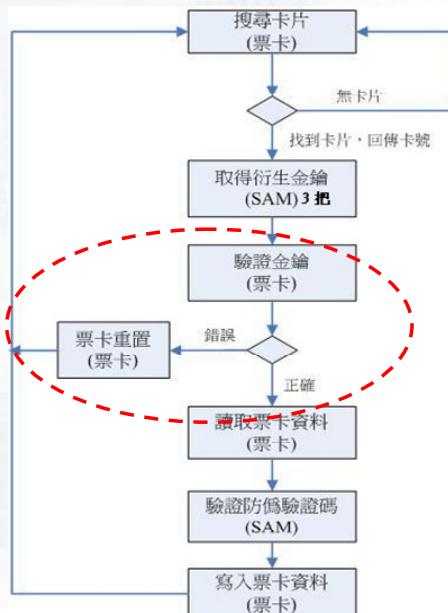
本研究前期「一機多卡驗票機」之交易流程

■ 輪詢法：判斷卡片歸屬之迴圈

- 衍生金鑰→驗證金鑰→票卡重置
- 「判斷卡片歸屬」可透過最佳化流程進行改善

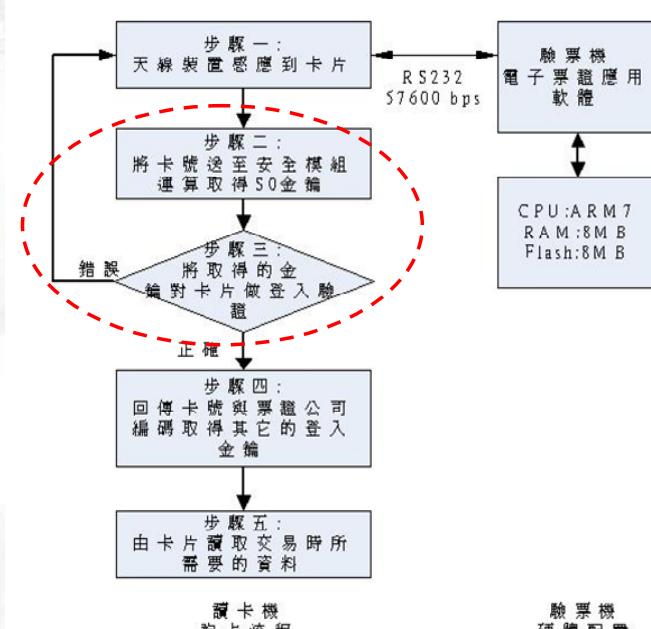
■ 其它技術方案

- 多卡平行驗證技術，即所謂「同詢法」



9/53

採用「判斷卡片歸屬」最佳化流程：富譽公司



10/53

富譽公司實機測試結果 [1/2]

SAM SLOT	SA 邏輯加密卡
JAVA CARD 廠牌	GemPlus T=1
Baud Rates	9600 bps~115200 bps
讀取票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API, Application Programming Interface) 讀取票卡資料
寫入票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API, Application Programming Interface) 寫入票卡資料
上車完整交易時間	0.593 秒
下車完整交易時間	0.593 秒

論詢順序	1	2
SAM SLOT	SA 邏輯加密卡	SAM2
JAVA CARD 廠牌	GemPlus T=1	Gemalto TOP_IS GX4 (GX4 36K Java Card) T=1
Baud Rates	9600 bps~115200 bps	9600~115200 bps
讀取票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API, Application Programming Interface) 讀取票卡資料	Value: S2、S7 Data: S1 B0、S1B1、S3、S6、S10 B0 S1~S5 以交二版標準欄位規劃
寫入票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API, Application Programming Interface) 寫入票卡資料	Value: S2 或 S7 Data: S3 B0、S3B1 或 S3B2、S4 或 S5、S6 B0、S6B2 S1~S5 以交二版標準欄位規劃
上車完整交易時間	0.621秒	0.580秒
下車完整交易時間	0.621秒	0.580秒

論詢順序	2	1
SAM SLOT	SA 邏輯加密卡	SAM2
JAVA CARD 廠牌	GemPlus T=1	Gemalto TOP_IS GX4 (GX4 36K Java Card) T=1
Baud Rates	9600 bps~115200 bps	9600~115200 bps
上車完整交易時間	0.638秒	0.515秒
下車完整交易時間	0.638秒	0.515秒

11/53

富譽公司實機測試結果 [2/2]

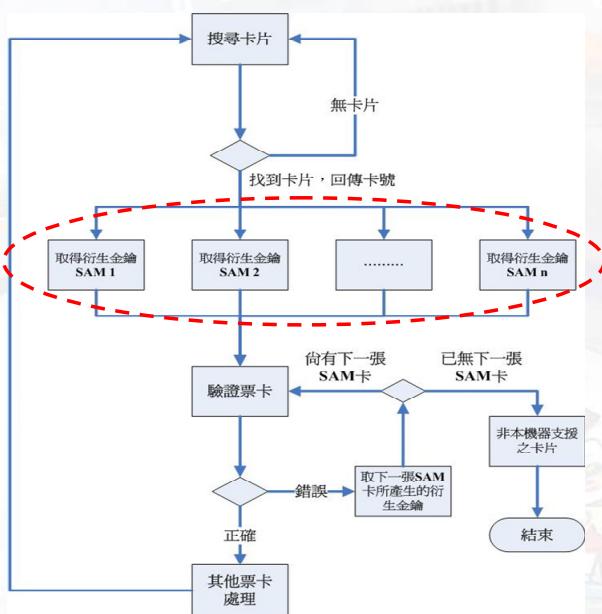
論詢順序	1	2	3
SAM SLOT	SA 邏輯加密卡	SAM2	SAM3
JAVA CARD 廠牌	GemPlus T=1	Gemalto TOP_IS GX4 (GX4 36K Java Card) T=1	OCS V7.0 T=1
Baud Rates	9600 bps~115200 bps	9600~614400bps	9600~614400bps
讀取票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API, Application Programming Interface) 讀取票卡資料	Value: S2、S7 Data: S1 B0、S1B1、S3、S6、S10 B0 S1~S5 以交二版標準欄位規劃	Value: S2 Data: S1B0、S1B1、S3
寫入票卡資料	以台灣通區域營運規則，結合里程計費程式函數庫 (API, Application Programming Interface) 寫入票卡資料	Value: S2 或 S7 Data: S3 B0、S3B1 或 S3B2、S4 或 S5、S6 B0、S6B2 S1~S5 以交二版標準欄位規劃	Value: S2 Data: S3 B0、S3B1
上車完整交易時間	0.671秒	0.671秒	0.450秒
下車完整交易時間	0.671秒	0.671秒	0.450秒

論詢順序	2	1	3
SAM SLOT	SA 邏輯加密卡	SAM2	SAM3
JAVA CARD 廠牌	GemPlus T=1	Gemalto TOP_IS GX4 (GX4 36K Java Card) T=1	OCS V7.0 T=1
Baud Rates	9600 bps~115200 bps	9600~115200 bps	9600~614400bps
上車完整交易時間	0.710秒	0.605秒	0.450秒
下車完整交易時間	0.710秒	0.605秒	0.450秒

論詢順序	2	3	1
SAM SLOT	SA 邏輯加密卡	SAM2	SAM3
JAVA CARD 廠牌	GemPlus T=1	Gemalto TOP_IS GX4 (GX4 36K Java Card) T=1	OCS V7.0 T=1
Baud Rates	9600 bps~115200 bps	9600~115200 bps	9600~614400bps
上車完整交易時間	0.710秒	0.691秒	0.400秒
下車完整交易時間	0.710秒	0.691秒	0.400秒

12/53

採用多卡平行驗證技術：寶錄公司

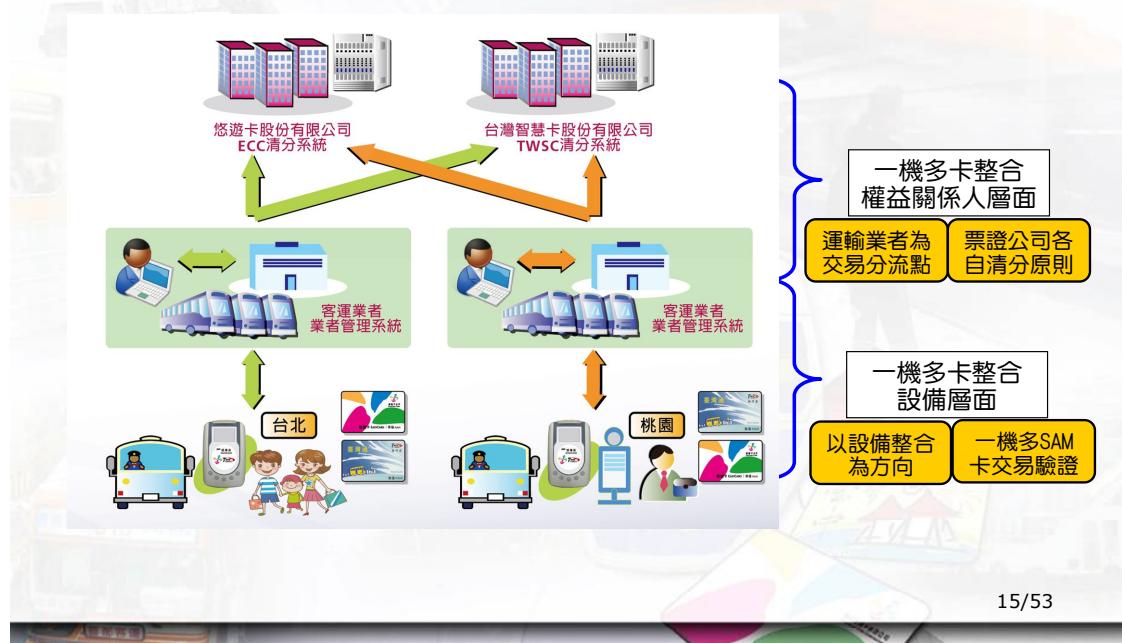


13/53

參、一機多卡整合模式之影響因素vs. 權益關係人及因應作法

14/53

一機多卡整合模式示意圖



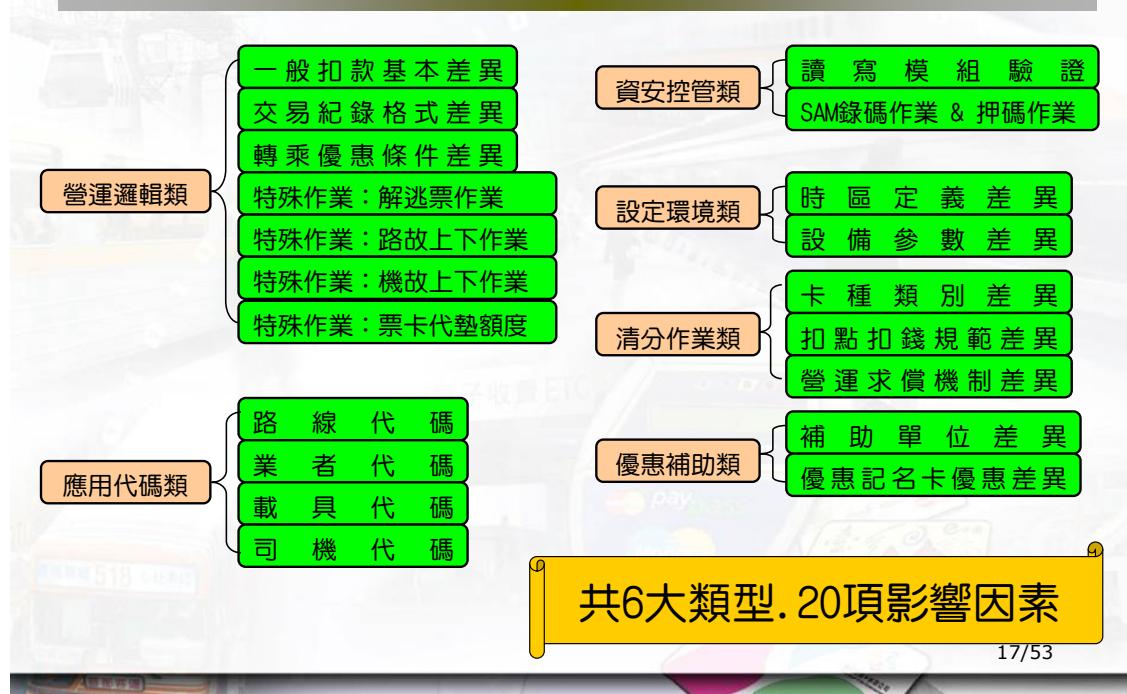
15/53

一機多卡整合模式「營運規則」之分類

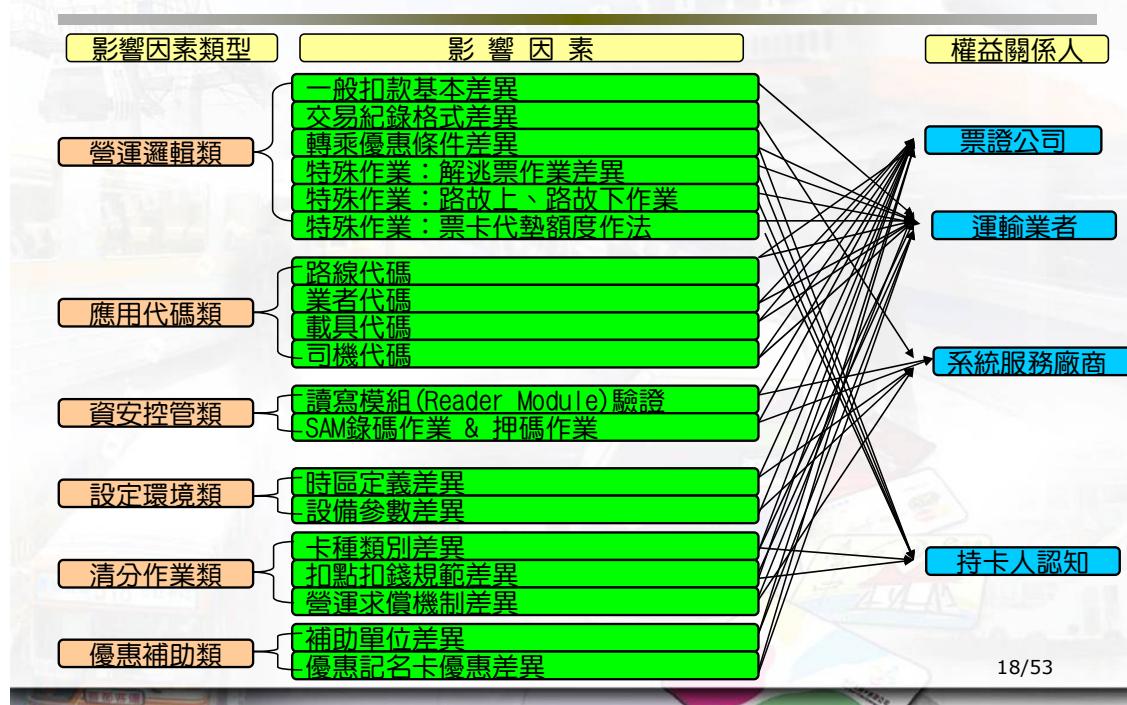
項目	運務營運規則	票證營運規則
細目參考	1. 乘車票種類 2. 電子票卡種類 3. 票價計算 4. 票卡之使用規定 5. 車上查驗規定 6. 票卡加值服務	1. 司機開班結班規則 2. 路線管理規則 3. 標準扣款作業 4. 路線卡功能規則 5. 點數優惠處理 6. 問題票卡處理 7. 餘額不足處理 8. 機故處理規範 9. 路故處理規範 10. 特許管制規範 11. 特種票規範 12. 轉乘管理規範

16/53

一機多卡整合模式之「影響因素」分析



影響因素 vs. 權益關係人



建議因應作法 vs. 各層級權益關係人

項次	建議因應作法	主要權益關係人	次要權益關係人	技術性問題歸屬
1	運輸規範整合	運輸業者	系統整合商 票證公司	非技術性
2	交易邏輯整合	運輸業者 票證公司	系統整合商	非技術性
3	交易資訊整合	票證公司	系統整合商 運輸業者	技術性
4	驗證流程整合	票證公司	系統整合商	非技術性
5	運輸代碼整合	政府單位 票證公司	運輸業者	非技術性
6	區域特性宣導	政府單位 運輸業者	票證公司	非技術性

19/53

建議因應作法與影響因素類型之矩陣表 [1/2]

影響因素的類型 影 響 因 素 應 付 作 法	營運邏輯類	應用代碼類	資安控管類	設定環境類	清分作業類	優惠補助類
運輸規範整合	<ul style="list-style-type: none"> ◆ 一般扣款基本差異 ◆ 轉乘優惠條件差異 ◆ 特殊作業：解逃票作業差異（特許上下） ◆ 特殊作業：路故上、路故下作業 ◆ 特殊作業：機故上、機故下作業 ◆ 特殊作業：票卡代墊額度作法 	--	--	--	◆ 營運求償機制差異	--
驗證流程整合	--	--	<ul style="list-style-type: none"> ◆ 讀寫模組驗證 ◆ SAM 錄碼作業及押碼作業 	--	--	--

20/53

建議因應作法與影響因素類型之矩陣表[2/2]

影響因素 因應作法	影響因素的 類型	營運邏輯類	應用代碼類	資安控管類	設定環境類	清分作業類	優惠補助類
交易邏輯整合	<ul style="list-style-type: none"> ◆ 一般扣款基本差異 ◆ 轉乘優惠條件差異 ◆ 特殊作業：解逃票作業差異（特許上下） ◆ 特殊作業：路故上、路故下作業 ◆ 特殊作業：機故上、機故下作業 ◆ 特殊作業：票卡代墊額度作法 	--	--	--	--	<ul style="list-style-type: none"> ◆ 卡種類別差異 ◆ 扣點扣錢規範差異 ◆ 營運求償機制差異 	<ul style="list-style-type: none"> ◆ 補助單位差異 ◆ 優惠記名卡優惠差異
交易資訊整合	<ul style="list-style-type: none"> ◆ 交易紀錄格式差異 	<ul style="list-style-type: none"> ◆ 司機代碼 	--	<ul style="list-style-type: none"> ◆ 時區定義差異 ◆ 設備參數差異 	--	--	--
運輸代碼整合	--	<ul style="list-style-type: none"> ◆ 路線代碼 ◆ 業者代碼 ◆ 載具代碼 	--	--	--	--	--
區域特性宣導	--	--	--	--	--	<ul style="list-style-type: none"> ◆ 卡種類別差異 ◆ 扣點扣錢規範差異 	<ul style="list-style-type: none"> ◆ 補助單位差異 ◆ 優惠記名卡優惠差異

21/53

運輸業者與票證公司於「營運邏輯與營運模式協商階段」之談判議題 [1/2]

議題項目	談判重點
卡種類別差異	建議以一般卡種(全票)為原則。
扣點扣錢規範差異	建議以扣錢為主，不支援扣點。
營運求償機制差異	建議各業者自行與票證公司討論。
補助單位差異	建議不開放跨區之社福票卡。
優惠卡優惠差異	建議不對跨區優惠票提供優惠。
一般扣款基本差異	建議以一般卡種(全票)及當地運輸業者自行提供之優待票為限。

22/53

運輸業者與票證公司於「營運邏輯與營運模式協商階段」之談判議題 [2/2]

議題項目	談判重點
交易紀錄格式差異	建議各業者自行與票證公司討論。
轉乘優惠條件差異	建議不提供跨區票卡之轉乘優惠。
解逃票作業差異	建議使用自動特許上功能。
路故上、路故下作業	不同公司限定時間內可接受路故上的方式。
機故上、機故下作業	透過運輸業者協商與溝通，確認機故時不需處理，由運輸業者自行規範司機人工處理方式。
票卡代墊額度作法	透過運輸業者協商，再與兩家票整公司溝通，統一代墊額度。

23/53

一機多卡整合模式對產業生態的影響 [1/2]

一、主導權的轉變：

票證公司主導轉變為運輸業者主導

項目	轉變前建置方式	轉變後建置方式
資訊作業模式	電子票證委外	運輸業者主導
關係架構	一對多關係結構	多對多關係結構
設備提供	票證公司負責	運輸業者負責
設備維護	票證公司負責	運輸業者負責
系統需求確認	票證公司確認	運輸業者確認
營運邏輯	各區域由票證公司進行整合	各運輸業者將針對各自需求增加

24/53

一機多卡整合模式對產業生態的影響 [2/2]

二、營運面的轉變：

系統委外夥伴關係轉變為清分費率商業談判關係

三、關係面的轉變：

一(票證公司)對多(運輸業者)轉變為多(票證公司)對多(運輸業者)

25/53

一機多卡驗票機新增票證系統成本概算 [1/2]

成本項目	說明	備 註
場站管理系統 (DPS)	每套系統約1,500萬元，實際費用依據分擔數目而定。	如與既有票證業者系統共用硬體，則須增加相容性測試成本。
業者管理系統 (CPS)	每套系統約1,500萬元，實際費用依據分擔數目而定。	同上
驗票設備應用 軟體修改	為一次性成本，實際成本依據實際修改需求而定。	修改後之驗票設備需重新驗證，可能衍生驗證成本，視修改幅度而定。
讀寫模組應用 韌軟體修改	為一次性成本，實際成本依據實際修改需求而定。	同上
驗票設備與讀 寫模組安裝/ 測試費用	每台每次約5,000元	

26/53

一機多卡驗票機新增票證系統成本概算 [2/2]

成本項目	說 明	備 註
SAM卡購置成本	票證系統SAM卡購置成本，實際成本依據各票證系統售價而定。	依據運輸業者與票證公司合約內關於成本分擔規定辦理。
管理成本	運輸業者之管理成本以及導入新的票證系統作業所衍生之成本	運輸業者針對新的票證公司之營運規範、作業流程、對帳作業均需導入作業、教育訓練等衍生之成本。

27/53

肆、交通電子票證應用CPU卡之探討

28/53

CPU卡的優勢一：安全性

■ CPU卡內部有雙重安全機制

- 第一重：晶片本身具備加密算法模組，目前比較常見的安全算法有RSA，3-DES等。
 - ✓ 中國另開發國密算法（SSF33，SCB2，SM2，SM3等）來加強晶片的安全性。國密算法是不對外公開的，比其他公開算法的加密算法具有更高的安全性。
- 第二重：CPU卡晶片有COS（Card Operation System）系統。
 - ✓ COS可以為晶片設立多個相互獨立的密碼，密鑰以目錄為單位存放，每個目錄下的密鑰相互之間獨立，並且有防火牆功能。
 - ✓ 同時COS內部還設立密碼最大重試次數以防止惡意攻擊。

29/53

CPU卡的優勢二：多功能性

■ CPU卡可以實現真正的“一卡多用”

- “一卡多用”每個應用相互獨立並受控於各自的密鑰管理系統。
- 不同應用可以共享一個“錢包”，也可以分別擁有各自的“錢包”。
- 服務商可以通過使用CPU卡進行更加靈活有效的管理，用戶也能使用CPU卡實現多功能應用的需求。

30/53

國際金融/信用卡的主要技術標準--EMV

- EMV2000標準是國際上金融IC卡借記/貸記應用的統一技術標準，主要內容包括借貸記應用交易流程、借記/貸記應用規範和安全認證機制等。
- EMV導入是指按照EMV2000標準，在發卡、業務流程、安全控管、受理市場、訊息轉接等多個環節的技術規範。

31/53

中國交通CPU卡與EMV規範的關聯性

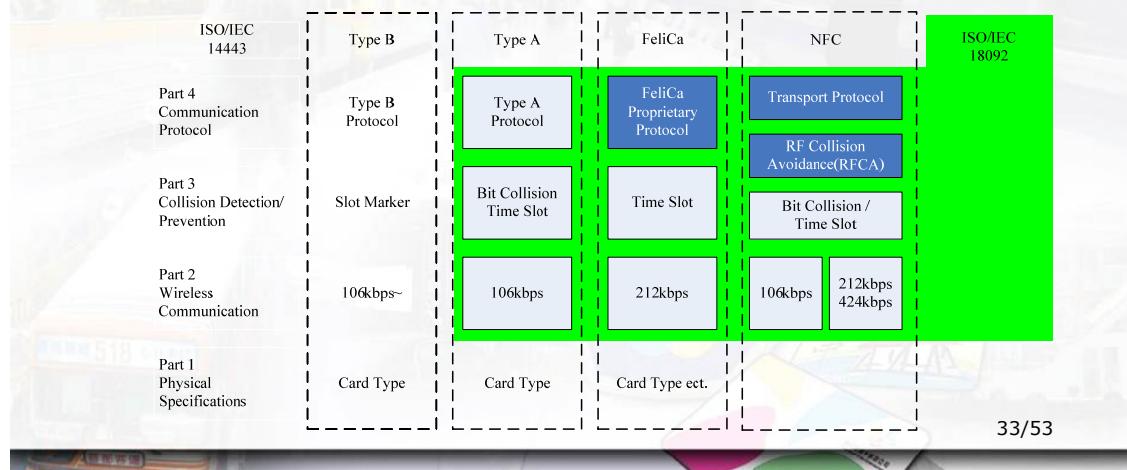
- 中國人民銀行頒布的《PBOCv2.0規範》是以EMV的規範為制定基準，自稱為繼VISA標準、MASTER標準、JCB標準之後世界上第四部銀行卡產業標準規範。
- 中國住房和城鄉建設部頒布的《建設事業非接觸式CPU卡COS技術要求》和《PBOCv2.0規範》電子錢包相關規範（PBOC2.0第一、第二、第八、第九部分）幾乎完全相同。

32/53

日本SONY FeliCa的技術規範

■ 日本SONY：FeliCa

- ▶ SONY與PHILIPS聯合開發新的NFC技術--NFCIP-1，已成為ISO/IEC/IEC 18092國際標準，可和ISO/IEC/IEC 14443A相容。



邏輯加密卡升級為CPU卡之問題探討與因應策略[1/2]

一. 邏輯加密卡升級為CPU卡問題之探討

1. 資料的角度：將二者的資料進行區分，既兼顧了資料的獨立性、安全性，同時為未來取消邏輯加密卡後，CPU卡片資料的維護奠定了基礎。
 2. 清算的角度：將二者的資料進行區分，將有助於資料的明確劃分和對賬。
 3. 系統的角度：同時進行系統軟體和硬體中嵌入式軟體的開發，將可有效的避免二卡共存的情況下，系統發生衝突的問題。
 4. 應用的角度：儘量維持原有操作介面，以避免重覆作業的問題。
 5. 實施的角度：先執行硬體設備的軟體更新，再升級系統軟體，如此有助於轉換期間系統的穩定。
- 34/53

邏輯加密卡升級為CPU卡之問題探討與因應策略 [2/2]

二. 邏輯加密卡驗票機升級為CPU卡的解決方案

1. 生產驗票機時須預估未來升級CPU卡時所需的記憶體儲存空間。
2. 新的ISAM/PSAM卡必須保留支援原先邏輯加密卡金鑰的所有功能，在一定時期內保持非接觸式CPU卡和邏輯加密卡雙軌並行。
3. 驗票機的韌體必須確保能使邏輯加密卡和CPU卡完全相容。
4. 重新規劃通訊協定。

35/53

中國邏輯加密卡(M1)卡升級方案探討 [1/3]

一. 強化M1卡片安全應用系統方案

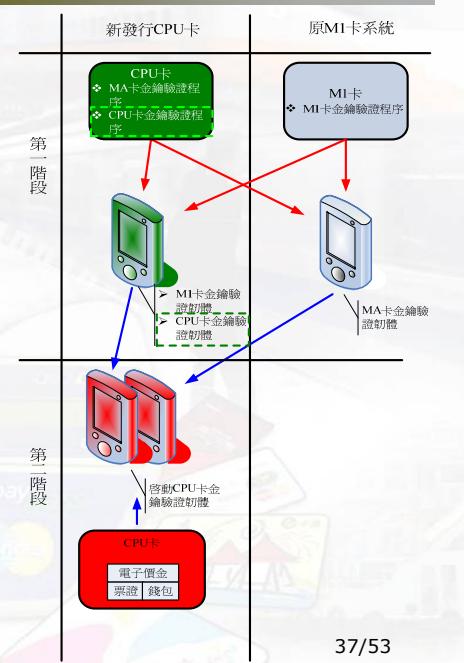
- 以不發行CPU卡為前提下，針對M1卡之弱點加強其全安性
- 工作計劃及內容重點：
 - ✓ 多級密鑰管理
 - ✓ 消費密鑰和加值密鑰的分離
 - ✓ 一卡一密
 - ✓ 採用PSAM和認證碼的安全控制
 - ✓ 黑名單管理
 - ✓ 限制離線最大交易之金額
 - ✓ 帳戶管理及審計跟蹤

36/53

中國邏輯加密卡(M1)卡升級方案探討 [2/3]

二. CPU卡兼容M1卡應用系統方案

- 以非接觸式CPU卡來逐步取代現有系統已發行邏輯加密卡，逐步完成現有的邏輯加密卡到CPU卡的升級。
- 工作計劃及內容重點：
 - ✓ 制定兼容邏輯加密卡的CPU卡規範和應用規範。
 - ✓ 制定CPU卡應用結構和交易流程規範。
 - ✓ 建設符合上述流程和規範的CPU卡模擬測試系統。
 - ✓ 完成發卡系統的升級改造。

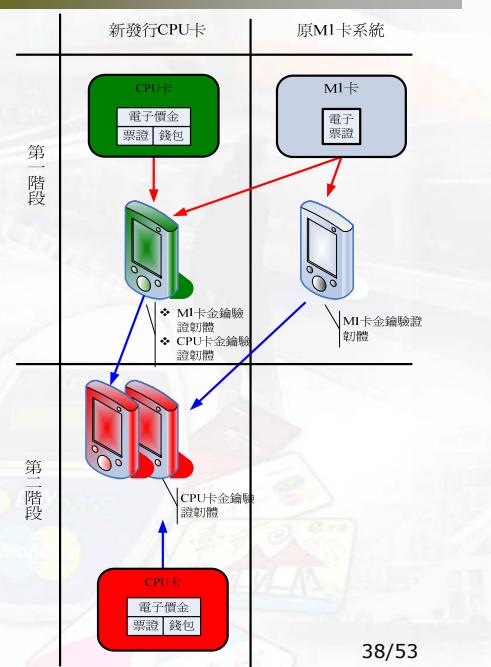


37/53

中國邏輯加密卡(M1)卡升級方案探討 [3/3]

三. CPU卡替換M1卡應用系統方案

- IC卡整合的最終目標，以CPU卡替換掉現在之M1卡，在支付中停止使用M1卡。
- 工作計劃及內容重點：
 - ✓ 兩卡一機
 - 透過驗票機之改造，在過渡期間內，CPU卡及M1卡皆可以在車載驗票機上使用。
 - ✓ 逐步替換
 - 在過渡期內，以行銷方式將M1卡替換為CPU卡。
 - ✓ 雙系統並行
 - 過渡期M1卡及CPU卡兩結算系統並行，過渡期結束後，停止M1卡之結算系統。



38/53

以CPU卡為交通電子票證可能衍生之議題

一. 交通營運面

1. 票證轉換運作議題
 - ① 卡片轉換策略之選擇
 - ② 平行移轉作業之程序
2. 交通營運邏輯整合
 - ① 跨區使用規範
 - ② 跨區優惠與紅利積點
3. CPU卡片規格整合
 - ① 多元載具卡片格式規範
 - ② 交通領域統一欄位格式之規範

二. 交易安全面

1. 交易安全與金鑰管控
 - ① 交易正確性與不可否認性
 - ② CPU卡片金鑰管理機制
2. 多對多清分清算架構
 - ① 聯合清分清算之服務
 - ② 交通業者清分作業整合

39/53

伍、電子票證發行管理條例之衝擊與影響分析

40/53

電子票證營運資格及專營規定對票證公司之影響

一. 對發行機構之經營採核准制

- 電子票證之發行機構，其最低實收資本額為新臺幣三億元，足以排除許多中小型廠商，對大型的電子商務平台業者或其他發行實體電子票證業者較有利。

二. 須專業經營電子票證業務

- 本法公布前已經金管會核准發行電子票證之金融機構，其原即屬金管會監理範圍，故特別規定其不受專業經營之限制。
- 對於非在本條例公布施行前業經金管會核准發行電子票證之金融機構，必須「重新」申請核准發行，如此即會受到專業經營之限制；此意謂發行電子票證之機構，原則上不會是提供商品或服務的企業。

41/53

對於持卡人的保障

一. 持卡人預付款項之保障

- 依本條例規定，銀行以外之發行機構除須提撥準備金外，尚須將全額預收款項交付信託或全額履約保障。

二. 持卡人個人資料與安全性之保障

- 本條例對於因電子票證使用所蒐集、產出或累積之資訊，除限制發行機構為得利用持卡人資料為第三人從事行銷行為外，僅規定就「個人資料」應保密。
- 應參照銀行有關資訊安全管制之規範，定出電子票證發行機構有關個人資料及交易資料保密及安全性應遵循事項之管理規則。

42/53

對票證整合之影響

- 一. 本條例並未鼓勵既有儲值卡發行業者彼此間的整合，亦未排除可能整合上法規適用的困難。
- 二. 本研究主張電子票證產業應該有類似「公協會」的組織，惟電子票證產業公協會成立的目的若涉及金管會管轄業務，則其成員必須是經金管會核准成立之電子票證專業公司，必須比照銀行公會的成立條件及資格。

43/53

對現行電子票證業者的影響 [1/2]

一. 台北悠遊卡公司

- 「icash悠遊卡」於民國99年4月正式上線，超過一萬個通路店面可使用icash悠遊卡。
- 台中市及高雄市客服據點於民國99年4月開張營運。
- 悠遊CPU卡目前已進入CC(Common Criteria 國際認證)階段，正式上市時間尚不明確。

二. 遠通電子收費公司

- 遠通電收是否可以跨業營運非屬高速公路收費範圍之業務，必須視其與高速公路局所立之契約而定，目前則尚不確定。

44/53

對現行電子票證業者的影響 [2/2]

三. 高雄捷運公司

- 高雄捷運公司董事會是否同意投資成立「專業經營電子票證業務」之公司或將其票證業務委外營運，尚未定論。

四. 台灣智慧卡公司

- 該公司仍積極拓展發卡業務，包括金門地區及台鐵新竹-基隆-瑞芳路段，對於如何因應「電子票證發行管理條例」的落日條款，該公司董事會則尚未達成共識。

45/53

陸、結論與建議

46/53

結 論 [1/3]

- 一. 就國內廠商的IT技術能力而言，一機多卡驗票機的研發並不困難，然多卡整合後所衍生的營運規則等差異則必須透過協商機制處理。
- 二. 在一機多卡整合階段中，「票證資料格式確認階段」與「營運邏輯與營運模式協商階段」是整合困難度與共識分歧度最高的階段。
- 三. 一機多卡整合模式仍然無法避免不同票證公司在票證資料格式與營運邏輯上整合之基本困難。

47/53

結 論 [2/3]

- 四. 一機多卡整合模式以不同縣市具有優惠身分之持卡人跨區使用時，所產生之優惠折扣差異，最容易使民眾困擾。
- 五. 一機多卡整合模式對電子票證產業生態的影響，大致可以分為主導權的轉變、營運面的轉變以及關係面的轉變等三種變化。
- 六. 一機多卡整合時所面對之影響因素，包括：運輸規範整合、驗證流程整合、交易邏輯整合、交易資訊整合、運輸代碼整合與區域特性宣導等。

48/53

結 論 [2/3]

- 七. 中國人民銀行頒布的《PBOCv2.0規範》是以EMV的規範為制定基準，《建設事業非接觸式CPU卡COS技術要求》和前者電子錢包相關規範幾乎完全相同，此顯示制定電子票證規範應考慮參考國際共通規範。
- 八. 「電子票證發行管理條例」以落日條款、票證公司資本額的限制以及專營規定等，對現行的票證公司的影響最鉅。

49/53

建 議 [1/3]

- 一. 「一機多卡驗票機」乃一概念性的說法，其系統架構及元件規格將因廠商所採用的技術而異，故不宜訂定設備規格，然訂定必要的功能規範則有其必要性。
- 二. 以國內資訊產業的研發能力，應用一機多卡整合模式交易並不困難，但是(一)、如何因應卡片晶片技術的快速發展？(二)、如何整合運輸業者差異頗大的營運規則？前者為票證業者的營運風險；後者則建議透過政府輔導、協助以達成共識。
- 三. 建議一機多卡整合模式之策略期程：短期採交易分流策略；中期採管線共構策略；長期採聯合處理策略。

50/53

建 議 [2/3]

- 四. 採用一機多卡整合模式時，為減少不同票證系統跨區使用時，增加建置系統的複雜度，建議運輸業者之應用代碼由主管機關加以統一。
- 五. 採用一機多卡整合模式時，由於各家票證公司之清分清算作業差異頗大，建議採取分流模式進行交易驗證與清分清算作業。
- 六. 在一機多卡整合模式下，具備優惠身分之持卡人跨區使用時，將產生不同地方政府補貼的優惠措施不同，而造成優惠折扣不同的情形，建議應有配套措施與規劃。

51/53

建 議 [3/3]

- 七. 考量不同票證系統的持卡人跨區使用時，因各地區票證系統營運規則不同，可能導至民眾的誤解，建議採「屬地主義」為主，「屬票證公司」為輔的原則，透過商業談判建立相關的配套措施。
- 八. 綜觀國際CPU卡的發展歷程，皆先訂定共同規範以供相關設備及系統供應商遵循，建議我國發展CPU卡亦應先制定與國際接軌之規範。
- 九. 電子票證公協會組織若在短期內無法成立，建議由國家訂定規範或參考文件，以利電子票證之整合及創造規模經濟的條件。

52/53

簡報結束
敬請指教

53/53

附錄 6

「第五章 交通電子票證應用 CPU 卡之探討」之 CPU 卡參考規範

附錄 6 「第五章 交通電子票證應用 CPU 卡之探討」之 CPU 卡參考規範

附 6.1 中國《建設事業非接觸式 CPU 卡 COS 技術要求》規範大綱

中國《建設事業非接觸式 CPU 卡 COS 技術要求》的規範大綱如下

1. 範圍
2. 規範性引用檔
3. 定義
4. 縮略語和符號表示
5. 機電特性、邏輯介面與傳輸協定
 - 5.1 接觸式 CPU 卡的機電特性、邏輯介面與傳輸協定
 - 5.2 非接觸式 CPU 卡機電特性、邏輯介面與傳輸協定
 - 5.3 CPU 卡的機械特性
6. 資料元和命令
 - 6.1 文件
 - 6.2 命令
7. 應用選擇
 - 7.1 應用識別字的編碼
 - 7.2 支付系統環境結構
 - 7.3 支付系統目錄編碼
 - 7.4 目錄入口中執行的命令的使用
 - 7.5 其他目錄的編碼
 - 7.6 終端的應用選擇
8. 安全機制
 - 8.1 基本安全要求

- 8.2 密鑰和個密碼的存放
- 8.3 安全報文傳送
- 8.4 認可的加密演算法
- 9. 電子存摺/電子錢包應用
 - 9.1 文件
 - 9.2 命令
 - 9.3 交易流程
 - 9.4 防拔
 - 9.5 交易處理性能.

附 6.2 中國《PBOC 2.0 規範》規範大綱

中國《PBOC 2.0 規範》的規範大綱如下：

第 1 部分：電子錢包/電子存摺應用卡片規範：

規定了電子錢包/電子存摺卡片方面的內容。

第 2 部分：電子錢包/電子存摺應用規範

規定了電子錢包/電子存摺應用所涉及的檔、命令、安全需求及交易流程，也描述了磁條卡功能的相關需求。

第 3 部分：與應用無關的 IC 卡與終端介面規範

規定了應用無關的 IC 卡與終端介面方面的內容，包括卡片的機電介面、卡片操作過程、字元的物理傳輸、重定應答、傳輸協議、文件、命令及應用選擇機制。

第 4 部分：借記/貸記應用規範

主要描述了借記/貸記應用卡片和終端之間處理的技術概要，提出了對基於 IC 卡借記/貸記項目的最低要求。

第 5 部分：借記/貸記應用卡片規範

從卡片的角度描述了借記/貸記交易流程，包括卡片內部的處理細節、卡片所使用的數據元、卡片所支援的指令集等。

第 6 部分：借記/貸記應用終端規範

從終端的角度描述了借記/貸記交易流程，包括終端的硬體需求、終端內部的處理細節、終端所使用的數據元、終端所支援的指令集等。

第 7 部分：借記/貸記應用安全規範

描述了借記/貸記應用安全功能方面的要求以及為實現這些安全功能所涉及的安全機制和獲准使用的加密演算法。

第 8 部分：與應用無關的非接觸式規範

規定了接觸式 IC 卡的物理特性、射頻功率和信號介面、初始化和防衝突、傳輸協議等內容。

第 9 部分：電子錢包擴展應用指南

描述了電子錢包複合應用、電子錢包灰鎖應用等內容。

第 10 部分：借記/貸記應用個人化指南

描述了 IC 卡借記/貸記應用特有的個人化指令、特有的數據分組標識的定義及個人化時有關安全方面的規定。

第 11 部分：非接觸式 IC 卡通訊規範

規定了非接觸式通訊所使用的符號編碼技術、數據幀格式等詳細內容。

第 12 部分：非接觸式 IC 卡支付規範

描述了非接觸式 IC 卡應用，在磁條非接觸式支付應用和快速借記/貸記非接觸式支付應用方面作出了相關要求和規定。

第 13 部分：基於借記/貸記應用的小額支付規範

描述了關於如何在借記/貸記卡上實現小額支付功能(即電子現金)的相關資訊，並提供了電子現金的功能。

附 6.3 《EMV2000》規範大綱

EMV2000 的規範分成四冊，各冊內容目大綱如下：

第一冊 應用獨立 ICC 到終端介面的要求(Book 1 Application Independent ICC to Terminal Interface Requirements)

Part I - General

1. Scope
2. Normative References
3. Definitions
4. Abbreviations, Notations, Conventions, and Terminology

Part II - Electromechanical Characteristics, Logical Interface, and Transmission Protocols

5. Electromechanical Interface
6. Card Session
7. Physical Transportation of Characters
8. Answer to Reset
9. Transmission Protocols

Part III - Files, Commands, and Application Selection

10. Files
11. Commands
12. Application Selection

Part IV - Annexes

Part V - Common Core Definitions

第二冊 安全和密鑰管理(Book 2 Security and Key Management)

Part I - General

1. Scope
2. Normative References
3. Definitions
4. Abbreviations, Notations, Conventions, and Terminology
5. Static Data Authentication (SDA)
6. Offline Dynamic Data Authentication
7. Personal Identification Number Encipherment

8. Application Cryptogram and Issuer Authentication
9. Secure Messaging
10. Certification Authority Public Key Management Principles and Policies
11. Terminal Security and Key Management Requirements

第三冊 應用規格(Book 3 Application Specification)

Part I - General

1. Scope
2. Normative References
3. Definitions
4. Abbreviations, Notations, Conventions, and Terminology

Part II - Data Elements and Commands

5. Data Elements and Files
6. Commands for Financial Transaction

Part III - Debit and Credit Application Specification

7. Files for Financial Transaction Interchange
8. Transaction Flow
9. GENERATE AC Command Coding
10. Functions Used in Transaction Processing

Part IV - Annexes

Part V - Common Core Definitions

第四冊 持卡人、服務員和取得介面的要求(Book 4 Cardholder, Attendant, and Acquirer Interface Requirements)

Part I - General

1. Scope
2. Normative References
3. Definitions

4. Abbreviations, Notations, Conventions, and Terminology

Part II - General Requirements

5. Terminal Types and Capabilities

6. Functional Requirements

7. Physical Characteristics

Part III - Software Architecture

8. Terminal Software Architecture

9. Software Management

10. Data Management

Part IV - Cardholder, Attendant, and Acquirer Interface

11. Cardholder and Attendant Interface

12. Acquirer Interface

Part V - Annexes