

98-109-4235

MOTC-IOT-97-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(2/4)

著者：林維信、許安慶、汪經堯、王穆衡、黃立欽

交通部運輸研究所

中華民國 98 年 11 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. (2/4) / 林維信等著. -- 初版.

-- 臺北市：交通部運研所，民98.11

面；公分

參考書目：面

ISBN 978-986-02-0680-7(平裝)

1. 交通管理 2. IC卡 3. 管理資訊系統

557.15029

98021147

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)

著者：林維信、許安慶、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 98 年 11 月

印刷者：九茹印刷有限公司

版(刷)次冊數：初版一刷 130 冊

本書同時登載於交通部運輸研究所網站

定價：100 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 臺北市中山區松江路 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：1009803044 ISBN：978-986-02-0680-7 (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(2/4)			
國際標準書號（或叢刊號） ISBN 978-986-02-0680-7(平裝)	政府出版品統一編號 1009803044	運輸研究所出版品編號 98-109-4235	計畫編號 97-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：林維信 研究人員：許安慶、汪經堯 地址：臺北市辛亥路2段185號28樓 聯絡電話：(02) 27363567		研究期間 自 97 年 2 月 至 97 年 12 月
關鍵詞：電子票證、智慧卡、驗證機制			
摘要： <p>國內電子票證系統的應用正處於快速發展階段，但在市場有限的情形下，後續維運、擴充與整合卻是各票證公司面臨的嚴峻課題，為了讓票證公司獲得足夠交易量以持續維運，並設法降低設備採購與維運成本，達成交通部「一卡通」目標。本計畫(4年期計畫)以交通部「電子票證系統之多功能卡片規劃書」第二版與「票證後台清算核心模組」研發成果為發展基礎，推動電子票證共通技術規範的研究。</p> <p>本期計畫(第2年期)研擬「電子票證系統之多功能卡片規劃書」第三版草案，規劃交三版卡片驗證機制，實際開發交三版卡片靜態資料測試系統，探討票證整合後台相關功能整合之議題以及票證整合配合事項，以加速國內票證整合的順利推動。本計畫效益包括可提升國內電子票證系統中下游相關技術產業之發展，促成產業技術之升級，同時將國外卡片之最新技術發展引進國內，使國內業界之技術與國外並駕齊驅，進而加速票證系統設備之更新，有助於交通部交通電子票證發展政策之推動；而本計畫成果可支援交通部交通電子票證發展政策之需要，適時提供技術與政策分析支援。</p>			
出版日期	頁數	定價	本 出 版 品 取 得 方 式
98 年 11 月	242	100	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。
機密等級： <input type="checkbox"/> 密 <input type="checkbox"/> 機密 <input type="checkbox"/> 極機密 <input type="checkbox"/> 絕對機密 （解密條件： <input type="checkbox"/> 年 <input type="checkbox"/> 月 <input type="checkbox"/> 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） <input checked="" type="checkbox"/> 普通			
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

TITLE: Universal Technical Specifications Research of Electronic Payment Systems and Universal Traffic Cards Promotion (Phase II)			
ISBN(OR ISSN) ISBN 978-986-02-0680-7 (pbk.)	GOVERNMENT PUBLICATIONS NUMBER 1009803044	IOT SERIAL NUMBER 98-109-4235	PROJECT NUMBER 97-MDB005
DIVISION: Operations and Management Division DIVISION DIRECTOR: Mu-Han Wang PRINCIPAL INVESTIGATOR: Mu-Han Wang PROJECT STAFF: Li-Chin Huang PHONE: (02) 2349-6837 FAX: (02) 2545-0431			PROJECT PERIOD FROM February 2008 TO December 2008
RESEARCH AGENCY: CECI Engineering Consultants, Inc. PRINCIPAL INVESTIGATOR: Wei-Hsin Lin PROJECT STAFF: An-ching Hsu, Joe Wang ADDRESS: 28F, 185 Hsinhai Road, Sec. 2, Taipei PHONE: (02) 2736-3567			
KEY WORDS: Electronic Payment, Smart Card, Validation Mechanism			
ABSTRACT: <p>Electronic payment systems (EPS) in Taiwan have been developing very fast. Due to a limited scale of the domestic market, however, EPS companies face the difficulties of system maintenance, expansion, and integration. To assure EPS companies with enough transaction volume and to cut the cost of purchase and maintenance, this project, based on the research results of two Ministry of Transportation and Communications (MOTC) projects- "The Planning Guide for EPS Multi-functional Cards, V2" and "EPS Clearing & Settlement Core Module", developed the interoperable standards for EPS.</p> <p>This project developed the V3 (draft) of "The Planning Guide for EPS Multi-functional Cards" and proposed a validation mechanism based on this specification. A static data validation system was developed. We also studied issues regarding the integration for backend systems and other related issues. The benefit of this project included upgrading the technology of the EPS industry and introducing the latest EPS technology in foreign countries which is helpful for Taiwan's EPS industry. The result also can give the suggestions for the need of government's policy decisions.</p>			
DATE OF PUBLICATION November 2009	NUMBER OF PAGES 242	PRICE 100	CLASSIFICATION <input type="checkbox"/> RESTRICTED <input type="checkbox"/> CONFIDENTIAL <input type="checkbox"/> SECRET <input type="checkbox"/> TOP SECRET <input checked="" type="checkbox"/> UNCLASSIFIED
The views expressed in this publication are not necessarily those of the Ministry of Transportation and Communications.			

目 錄

第一章	計畫背景分析.....	1-1
1.1	計畫背景與目的.....	1-1
1.2	研究範圍與對象.....	1-2
1.3	研究內容、項目與流程.....	1-2
第二章	現況分析.....	2-1
2.1	國內電子票證系統發展現況.....	2-1
2.2	國外電子票證整合發展現況.....	2-7
2.2.1	由主要交通營運商及電子票證組織發起整合.....	2-7
2.2.2	由政府出面主導交通電子票證整合.....	2-9
2.2.3	由系統整合商和私營企業聯合發起多用途交通卡.....	2-15
2.3	第一年期計畫成果回顧.....	2-16
第三章	交三版(草案)卡片內部功能規格與交易流程定義.....	3-1
3.1	修訂目的及範圍.....	3-1
3.2	檔案資料格式、內容及存取權限.....	3-3
3.3	編碼準則.....	3-6
3.4	交易流程設計規範及參考範例.....	3-9
3.4.1	非接觸式 IC 卡主要交易流程框架.....	3-9
3.4.2	雙介面複合式卡(Dual Interface Card)交易流程規劃參考範例.....	3-10
第四章	以交三版為基礎之票證整合驗證機制規劃.....	4-1
4.1	交三版卡片驗證機制規劃.....	4-1
4.1.1	驗證申請作業流程.....	4-1
4.1.2	驗證系統架構規劃.....	4-4
4.1.3	驗測流程設計.....	4-7
4.2	一階段卡片靜態資料驗證結果.....	4-19
4.3	跨系統票證整合試辦計畫.....	4-24
4.3.1	以交三版執行票證整合試辦計畫.....	4-24
4.3.2	以前端設備執行票證整合試辦計畫.....	4-29
第五章	電子票證跨系統整合相關配合事項研擬.....	5-1

5.1	跨系統整合之議題探討.....	5-1
5.2	成立「電子票證跨系統清算交換中心」之探討.....	5-3
5.3	相關法規研析.....	5-7
第六章	後台票證整合之問題探討.....	6-1
6.1	金鑰整合機制.....	6-1
6.1.1	交三版金鑰管理規範建議.....	6-1
6.1.2	減值金鑰演算法則選擇之建議.....	6-2
6.1.3	發卡流程建議.....	6-4
6.2	卡片真偽確認機制.....	6-6
6.2.1	遠通電收建議之防偽驗證碼產製及驗證流程.....	6-7
6.2.2	防偽驗證碼驗證機制討論之議題.....	6-9
6.2.3	防偽驗證碼產製及驗證流程之選擇及建議.....	6-11
6.3	交易真偽確認機制.....	6-12
6.4	後台交易/黑名單交換機制.....	6-13
第七章	結論與建議.....	7-1
7.1	結論.....	7-1
7.2	建議.....	7-3
參考文獻	參-1
附錄 1	歷次技術研討會紀錄	
附錄 2	期中報告審查意見回覆表	
附錄 3	期末報告審查意見回覆表	
附錄 4	期末簡報	
附錄 5	交三版(草案)與交二版資料欄位修訂前後比較	
附錄 6	減值主金鑰組電文檔	
附錄 7	廠商測試申請表	
附錄 8	靜態驗證程式之測試紀錄檔樣本	
附錄 9	卡片靜態資料顯示列印程式 操作手冊	
附錄 10	更換金鑰作業之標準作業流程建議	

圖目錄

圖 1-1	計畫研究流程圖.....	1-4
圖 2-1	TaiwanMoney 卡片系統結構圖.....	2-18
圖 3-1	不同收費模式情境之示意圖.....	3-2
圖 3-2	以電子票證收費模式規劃交易資料檔案格式.....	3-4
圖 3-3	非接觸式 IC 卡主要交易流程框架.....	3-10
圖 3-4	雙介面複合式卡與非接觸式 IC 卡之整體交易流程參考範例.....	3-11
圖 3-5	雙介面複合式卡主要交易流程參考範例.....	3-12
圖 4-1	交三版驗證申請作業流程.....	4-1
圖 4-2	交三版驗證系統架構.....	4-4
圖 4-3	驗測流程設計之主要程序.....	4-8
圖 4-4	靜態驗證程式主畫面.....	4-20
圖 4-5	靜態驗證程式匯入金鑰畫面.....	4-21
圖 4-6	靜態驗證程式金鑰存取權限驗證畫面.....	4-22
圖 4-7	靜態驗證程式卡片格式驗證畫面.....	4-23
圖 4-8	交三版卡片整合系統與清分架構.....	4-26
圖 5-1	中國建設事業 IC 卡密鑰管理系統結構圖.....	5-2
圖 5-2	統一清算交換中心進行清算架構圖.....	5-4
圖 5-3	系統分別各自進行清算架構圖.....	5-4
圖 5-4	電子票證跨系統清算交換中心建置參考時程.....	5-6
圖 6-1	交三版卡片發行架構.....	6-5
圖 6-2	遠通電收建議之防偽驗證碼產製流程.....	6-7
圖 6-3	遠通電收建議之防偽驗證流程.....	6-8
圖 6-4	本計畫討論過程之防偽驗證碼產製流程.....	6-10
圖 6-5	本計畫討論過程之防偽驗證流程.....	6-10
圖 6-6	本計畫建議之防偽驗證碼產製流程.....	6-11
圖 6-7	本計畫建議之防偽驗證流程.....	6-12

表目錄

表 2-1	國內電子票證系統營運現況彙整表	2-1
表 2-1	國內電子票證系統營運現況彙整表(續)	2-2
表 2-2	高雄捷運一卡通種類	2-5
表 2-2	高雄捷運一卡通種類(續)	2-6
表 2-3	國外電子票證系統營運現況彙整表	2-17
表 2-4	國內電子票證系統驗票機功能比較表	2-20
表 3-1	交三版資料欄位格式一覽表	3-4
表 3-1	交三版資料欄位格式一覽表(續)	3-5
表 4-1	使用金鑰存取測試模組進行檢測預期結果表	4-10
表 4-2	不同載具間相互搭乘可能發生之搭乘行為	4-15
表 4-3	交三版卡片整合第 1 期測試計畫分工項目	4-25
表 4-4	交三版卡片整合第 1 期測試計畫驗證項目	4-27
表 4-5	交三版卡片整合第 2 期計畫驗證項目	4-28
表 4-6	交三版卡片整合第 3 期計畫驗證項目	4-29

第一章 計畫背景分析

1.1 計畫背景與目的

非接觸式智慧卡交通票證之應用在國內正處於快速發展的階段，目前已有臺北悠遊卡、基隆交通卡、桃竹苗臺灣通、中彰投臺灣通、南部地區 IC 智慧卡、高速公路電子收費系統、高雄捷運一卡通、馬祖悠遊卡及金門公共車船等 9 個電子票證系統上線營運，許多公民營停車場、路邊停車、計程車亦逐漸採用電子票證做為收費媒介，高鐵與臺鐵間之票證系統亦朝向服務與技術之整合，電子票證在其他非交通領域的應用亦逐漸拓展，如學生證、圖書館借書證、政府規費收費、社區門禁卡等。交通電子票證的應用對於吸引民眾搭乘大眾運輸、改善民眾行的便利以及提升運輸業者營運績效等層面已具有顯著效能並獲得民眾認同，未來在整體運輸經營效率與管理層面的潛在應用將是有待積極開發的新領域。

各地方票證系統雖在政府補助下陸續開通，使國內交通票證電子化邁出重要的第一步，但在國內市場有限的情形下，系統後續的維運、擴充與票證整合將是各票證公司必須立即面對的嚴峻課題，為了能讓客運市場最大佔有率之公路及市區客運運輸業者確實轉換票務處理模式，使票證公司能夠獲得足夠的交易量以持續維運，並且擴大交通電子票證應用範圍，降低各種設備採購與維運成本，進而發揮其潛在效能，達成交通部「一卡通用、多卡相容」之政策目標，政府與民間必須合作營造一個利於票證整合與相關技術發展的基礎環境。

為了達到此一目的，實有必要推動交通電子票證共通技術規範之研究，以交通部既有的「電子票證系統之多功能卡片規劃書」與「票證後台清算核心模組」研發成果為發展基礎，進一步研訂交通部卡片規格及交易流程規範，並開發符合交通部規範之卡片驗證機制與測試系統，推動策略上則結合票證公司、運輸業者、金融機構及設備供應商等民間力量成立相關公協會，以中立的角度確認相關規範的適用性，並且擔負規範的維護與更新工作。整體而言，本計畫的目的有三：

- 推動交通電子票證共通技術規範之研究，營造一個利於票證整合與技術發展的基礎環境

- 擴大交通票證應用範圍，使票證公司獲得足夠交易量，並降低票證公司成本
- 達成民眾於城際、都會、不同運具間「跨系統整合」之目標

1.2 研究範圍與對象

本計畫為 4 年期計畫，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，本期計畫為第 2 年期，依據第 1 年期計畫提出之交通部第三版「電子票證系統多功能卡片規劃書」(以下簡稱交三版)草案，詳細定義交三版草案之卡片規格及交易流程，協助交通部進行交三版草案的審查與公告頒布，規劃交三版卡片之驗證機制與開發測試系統，並協助各票證公司進行後台功能的研討與協商，以及參與國內電子票證公司之交三版卡片票證整合模擬驗證。在票證整合相關配套措施方面，本年期計畫提出以交三版卡片規格為基礎跨系統整合模式之相關配合事項，以利後續交三版卡片的發行與推廣使用。

1.3 研究內容、項目與流程

本計畫的研究流程如圖 1-1 所示，完成的工作內容與項目如下：

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、交三版之卡片規格與交易流程定義

本計畫將根據第 1 年期計畫的分析結果，以交二版卡片規格為基礎，規劃交三版檔案資料格式與交易流程，本計畫將採用技術討論座談方式，邀請票證相關業者與單位規劃交三版格式，凝聚各界共識以減少未來推動的阻礙。

三、交三版卡片驗證機制之規劃與測試系統開發

建立一套公正且為各票證公司接受之交三版驗證機制，乃是確保各票證業者卡片能夠互通的一項重要工作，本計畫規劃交三版驗證作業的流程與作法，並進行第一階段(靜態卡片欄位格式)檢測系統設計與開發。

四、協助電子票證公司進行後台功能整合研討協商

由本計畫協調各票證業者進行後台功能整合與運作機制，由各票證業者自行遵行，主要包含金鑰整合、卡片真偽確認、交易真偽確認及後台交易/黑名單交換等機制。

五、電子票證跨系統整合模式相關配合事項研擬

本工作項目主要為研擬相關配套措施，如補助電子票證整合設備建置之機制、補助大眾運輸轉乘、電子票證公協會組織之建立等，以促進國內交通電子票證進行跨系統整合。

六、交通票證整合相關法規研訂與配套措施研擬

本工作在探討政府單位於運輸業者在面臨運輸票證發行、整合時所可能面對的管理機制問題，並檢討目前法令之不足，提出政府制定電子票證監督管理機制時，相對應的建議與作法。

七、未來年期工作計畫研擬

研擬本計畫後續年期之研究範圍、工作項目及預期成果等計畫構想。

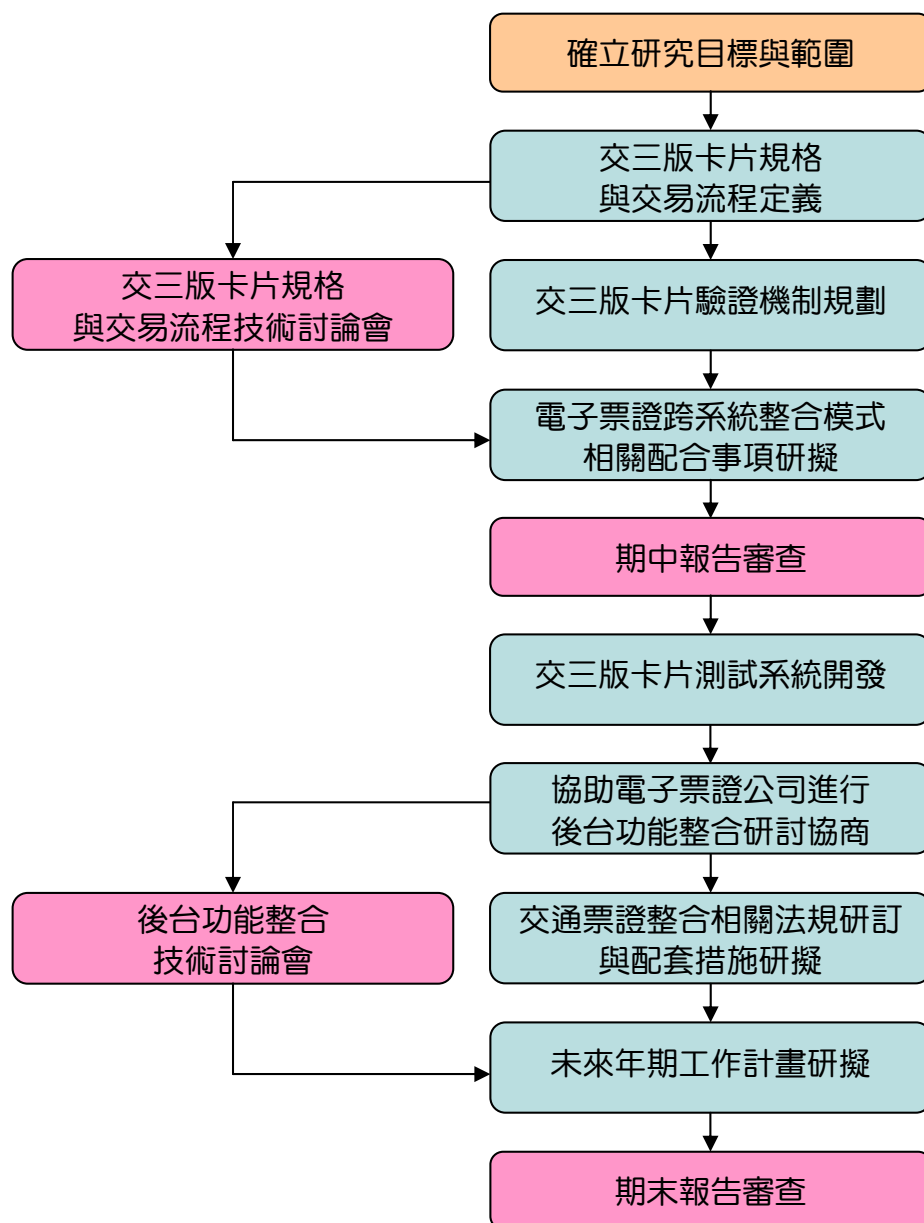


圖 1-1 計畫研究流程圖

第二章 現況分析

2.1 國內電子票證系統發展現況

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 年完成建置之大眾運輸電子票證系統，之後臺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，其他包括臺北悠遊卡、中彰投公車、南部七縣市公車、桃竹苗公車、高雄捷運、馬祖悠遊卡等電子票證系統亦陸續營運，其中悠遊卡系統憑藉著大臺北地區大眾運輸系統高使用量，以及積極擴充非交通運輸應用範圍如數位借書證及數位學生證之大力推廣等，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，國內各地方政府也積極發展相關的應用，國內目前電子票證系統營運現況整理如表 2-1：

表 2-1 國內電子票證系統營運現況彙整表

統計時間：97 年 12 月

系統別 營運現況	悠遊卡 ¹	臺灣通 ²	南部地區 TaiwanMoney 卡	高雄捷運一卡 通	高速公路電子 收費 e 通卡
營運單位	悠遊卡股份有限公司	臺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	遠通電收股份有限公司
開始營運時間	91 年	93 年	95 年	97 年	95 年
交通應用範圍	公車(臺北縣市、基隆、宜蘭、馬祖)、國道客運、捷運、纜車、淡水河藍色公路、臺鐵、公有路邊及路外停車場	桃竹苗中彰投等七縣市公車、花東公車(98 年度完成)	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、南臺灣客運、高雄客運、臺南市公車)	高速公路(國一、國三)
驗票機	約 12,000 部	3014 部	2010 部	2100 部	66.3 萬個 OBU 23 個收費站， 130 個車道

表 2-1 國內電子票證系統營運現況彙整表(續)

統計時間：97 年 12 月

系統別 營運現況	悠遊卡 ¹	臺灣通 ²	南部地區 TaiwanMoney 卡	高雄捷運一卡通	高速公路電子 收費 e 通卡
累計發卡量	1480 萬張	80 萬張	25.7 萬張	95 萬張	92 萬張(一般卡 79.4 萬、聯名卡 12.6 萬)
平均日交易量	320 萬次	30 萬次	1.1 萬次	12 萬次	40 萬次
其他應用範圍	學生證、圖書館借書證、動物園門票、醫院醫療費	無	具有小額消費之電子錢包功能	無	無
備註	<ul style="list-style-type: none"> 96.9 與基隆交通卡完成整合 97.8 完成臺鐵基隆—中壢間 19 個車站之悠遊卡建置計畫 	桃竹苗與中彰投系統於 97.4 完成整合	可使用在高雄捷運，每日交易量約 300 次	可使用在裝設 TM 系統之公車，每日交易量約 1.8 萬次	正進行與臺灣智慧卡公司的整合互通計畫

註 1：自 96 年 9 月 1 日起，基隆交通卡整併至悠遊卡系統。

註 2：臺灣智慧卡公司發行之桃竹苗與中彰投臺灣通已於 97 年 4 月整合完成，兩者卡片可在對方系統任一車輛上使用。

一、悠遊卡票證系統

悠遊卡(EasyCard)是通用於大臺北地區之非接觸式交通電子票證系統智慧卡，於 91 年始正式營運，由悠遊卡股份有限公司(原臺北智慧卡票證公司)發行，可用於搭乘臺北、基隆、宜蘭、馬祖地區之捷運、市區公車、公路客運、纜車等，並可搭乘許多國道客運班車，至 97 年 12 月之累計發卡量已達 1480 萬張，成為國內最大之交通電子票證系統。

悠遊卡公司不屬於銀行業，依照「銀行發行現金儲值卡許可及管理辦法」的規定不得發行具小額消費用途的現金儲值卡，為擴大悠遊卡的應用範圍，該公司於 95 年 7 月與國泰世華、臺北富邦、中信銀及臺新等四家銀行共同推出「悠遊聯名卡」，使悠遊聯名卡可使用在小額消費用途。悠遊聯名卡包含四種功能：信用卡、悠遊卡、悠遊電子錢包、與非接觸式小額感應支付功能(亦即 VISA 的 VISAWAVE 與 MasterCard 的 PayPass)，「悠遊電子錢包」使用在貼有「悠遊錢包」的商店(包括便利商店、連鎖咖啡店、電影院、加油站、照相館等)，與悠遊卡的餘額彼此不能互通。

此外，臺鐵局正積極推動「再生計畫」，IC 卡電子票證因具有票種、身分辨識、快速驗票、減少逃票及機動調整費率之功能，因此有利於推動臺鐵捷運化、票種簡化與票價合理化等政策。由於臺北都會區與鄰近縣市通勤頻繁，且臺北與基隆間大多數之大眾運輸系統已整合在悠遊卡系統內，因此，臺鐵局與悠遊卡公司合作試辦基隆—中壢間 19 個臺鐵車站使用悠遊卡扣款，於各試辦車站每一出入口設置一進一出之里程計價驗票機設備，並於各車站設置場站系統及站務員處理設備，提供民眾現金充值、票卡分析、資料傳輸等功能。試辦期間採用悠遊卡原有之充值及售票系統，臺鐵車站則新增人工充值窗口提供持卡者充值功能，本試辦計畫分為兩階段，第一階段試辦區間為樹林—松山 4 個車站，本階段於 97 年 6 月啟用，第二階段為基隆—中壢間其他 15 個車站，已於 97 年 8 月開始營運。

臺北縣政府於 96 年底接受公路總局的補助，於部分地區的市區公車及公路客運加裝悠遊卡驗票及充值設備，包括臺北縣轄公車及公路客運、臺北市短程國道客運、宜蘭縣轄公車及公路客運等，共計 1328 部驗票機及 221 部人工充值機，已於 98 年初完成建置。

悠遊卡公司正推動與臺灣高鐵及高雄捷運之票證整合計畫，在高鐵部份，將以無需劃位、營運規則較單純的自由席為優先整合之票種，規劃在高鐵車站公務門裝設里程計價之悠遊卡驗票設備，以及站務員處理設備、場站電腦、中央處理系統、查詢機等相關設備，整合範圍包括高鐵全線八個車站，原預計 97 年底完成，惟因雙方談判對於部分條件仍未達成共識，以致時程延宕；在高雄捷運部份，規劃以 SAM¹卡方式進行設備整合，於高雄捷運公務門裝設悠遊卡驗票設備，並於臺北捷運公務門驗票機安插高雄捷運 SAM 卡進行整合，使雙方卡片可在對方驗票機刷卡使用，整合範圍包括高捷全線 37 個車站及北捷全線 67 個車站，原預計 98 年 3 月完成整合，惟因雙方談判對於部分條件仍未達成共識，以致時程延宕。

二、臺灣通票證系統

臺灣通由臺灣智慧卡公司營運的兩大系統所組成，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臺中縣、市、彰化縣與南投縣內之 10 家客運業者(包括 5 家市區汽車客運—臺中客

¹ SAM 是(Secure Access Module, 安全存取模組)的簡稱，安裝在電子票證前台設備的稱為 ISAM，安裝在卡片內的稱為 PSAM，通稱為 SAM，SAM 通常以卡片形式安裝在前台設備上，其與卡片的 SAM 互相作用以驗證卡片的真偽。

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 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，客運業者包括桃園客運、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。

中彰投之臺灣通原與桃竹苗之臺灣通並不相通，96 年在交通部的票證整合政策的推動與經費補助下，兩者已於 97 年 4 月整合完成，兩者卡片可在對方系統任一車輛上使用。目前臺灣通的公車驗票機約有 3000 餘部，人工加值機約 1500 餘部，累計發卡量達 80 萬餘張。

公路總局於 96 年度補助花蓮及臺東地區建置公路客運 IC 卡票證系統，補助 209 台驗票機與 96 台人工加值機，採用臺灣智慧卡公司的臺灣通票證系統，預定於 98 年度完工啟用。

三、南部地區 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，結合南臺灣及全國之交通運輸工具，建置具有結合交通票證、金融儲值與消費等付款機制之 TaiwanMoney 卡，該計畫之建置與營運團隊由宏碁公司、萬事達卡國際組織、國泰世華銀行、玉山銀行、萬基公司及臺灣世曦工程顧問公司所組成。

現行之 TaiwanMoney 卡種類可分為兩種，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。迄 97 年 12 月為止發卡量 25.7 萬張，平均日交易 1.1 萬次，營運中之驗票機 2010 台，TaiwanMoney 卡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 發展團隊與高雄捷運公司依據交通部與高雄市政府交通局的要求，進行高雄捷運一卡通與 TaiwanMoney 卡的整合計畫，於高雄市公車及渡輪驗票機改裝成具有讀寫高捷一卡通的功能，至 97 年 12 月止，高捷一卡通在 TaiwanMoney 系統的使用量約為每日 1.8 萬人次，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，未來將視發展狀況提供兩者更為密切的整合功

能，由於目前的使用方式受到公務門位置、現場有無服務人員、問題卡片處理、卡片加值等之多方面限制條件，至 97 年 12 月止，TaiwanMoney 在高捷系統的使用量僅約每日 300 人次。

四、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電子票證，於 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」之電子票證。

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 2-2)，未來還將結合銀行發行聯名卡、結合電信業者提供聯名手機服務、結合保全業者保全系統及門禁系統使用之保全卡、結合中華電信推行校園數位學生證以及與 NFC 手機之 Gift Card(具備小額消費功能)等。至 97 年 12 月止，一卡通累計發行量已達 95 萬張，平均每日交易量約 12 萬次。

表 2-2 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	捷運轉乘高雄市公車 2 小時內公車一段票免費，公車轉乘捷運，捷運減免 12 元優惠(優惠至 98 年 3 月止)
一日卡	200 元，押金 70 元	否	—	一日內無限搭乘高雄捷運
暢遊卡	200 元，賣斷制	否	—	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	捷運轉乘高雄市公車 2 小時內公車一段票免費，公車轉乘捷運，捷運減免 10 元優惠(優惠至 98 年 3 月止)
敬老卡	免費	是	半票	65 歲以上之高雄市民 <ul style="list-style-type: none"> ● 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 <ul style="list-style-type: none"> ● 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

表 2-2 高雄捷運一卡通種類(續)

種類	售價	記名	計費方式	使用說明/優惠方法
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)。

五、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 95 年 2 月正式開始服務。

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(Venicle 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)，以提供短距、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，將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。

高速公路電子收費服務自 95 年 2 月上線至 97 年 12 月為止，已有 66.3 萬個 OBU 用戶，發卡量為 92 萬張，包含一般卡 79.4 萬張及聯名卡 12.6 萬張，平均日交易量 40 萬次，OBU 申裝與卡片加值地點包括高速公路休息站、汽車保養廠、便利商店、加油站、遠傳門市等。

2.2 國外電子票證整合發展現況

2.2.1 由主要交通營運商及電子票證組織發起整合

一、中國珠江三角洲

珠江三角洲目前有多個票證系統在進行整合，如香港的八達通卡與深圳通卡，以及廣洲羊城通與週圍城市交通 IC 卡的整合，最終的目的係期望達到「一卡通十城」之目標。

目前各票證系統整合的方向有兩種，其一是「互聯互通」，另一則是「一卡通」，二者是係不同的整合概念。所謂「互聯互通」是各地自建城市智慧交通卡系統，如深圳的交通卡(深圳通)在廣州、佛山等城市的讀寫器上可被使用；「一卡通」是一張交通卡內置多個城市的交通信息，統一採用一個數據，同一種資料格式，如此可以避免重複建設、投資浪費，但需要各城市的配合。

最近幾年來，香港有關部門一直與深圳磋商，以探討兩卡在深圳-香港通用的可行性。八達通卡其實已於 2006 年前已開始在深圳某些零售點使用，但只限於深圳兩家位於羅湖商業城和火車站內的「大快活」快餐廳消費，屬於試範點使用。且八達通卡深圳使用時不能自動增值，港幣與人民幣的匯率兌換由商戶自行確定。八達通卡公司正持續探討八達通卡與深圳通卡在兩地通用的可行性，主要考量商業、操作及技術層面的因素。早在 2004 年深圳地鐵完成時已有票證整合的構想，但因兩地採用的技術標準不統一，涉及設備改造、銀行匯率、利益分配等問題，整合的進程一直很緩慢。2008 年 4 月深圳市長在《政府工作報告》中提出，要推動深圳通與香港八達通互聯互通。目前已由深圳市交通局成立了一個推動深圳通、八達通互通的協調小組，從各方面論證如何加快互通。

為了能與八達通卡整合，深圳通在開發初期就與 SONY 公司、香港八達通公司接觸，並使用了相同的 SONY 卡讀寫模組，為兩卡互聯互通建立基本的技術平台。然而在實際建置時才發現，SONY 卡讀寫模組無法兼容兩地的密鑰信息，必須開發新的讀卡器。為此，深圳通研發了新的讀卡器，克服互聯互通的技術問題，並更換了原有的 SONY 設備。但由於香港仍使用 SONY 系統，並不符合中國國家標準、國際標準甚至日本標準，所以無

法與中國內地系統互通。而八達通讀卡器有近 5 萬台，改造費用高達 2 億元人民幣，短期內暫難與深圳通互聯互通。

其中最主要的技術關鍵是八達通卡採用 SONY 的 FeliCa 不符合 ISO 非接觸 IC 卡 TYPE A 的通訊協定等標準，故其早期建置的驗票機無法讀取屬於 TYPE A 非接觸 IC 卡系列的深圳通卡，而深圳通系統屬於後開發的驗票機，故可以事先於驗票機加設可讀取八達通卡的 SAM 卡，以至於造成八達通卡可至深圳地區使用，而深圳通卡無法於香港地區使用的結果。

八達通卡公司會繼續探討八達通卡和深圳通互通的可行性，包括在商業、運作、技術及法規上的考慮，現階段無法確定整合的時程表。八達通公司將邀請深圳有關機構入股，或是考慮與深圳通公司合併。深圳-香港交通互聯互通除了技術層面的問題外，金融層面也存在障礙。八達通採取港幣結算，深圳通採取人民幣結算，而匯率總是不斷變化，這需要政府相關部門在政策上予以支持。

珠江三角洲另一個整合的票證系統為廣州羊城通，與深圳-香港間互聯互通的進展相比，目前羊城通在廣佛地區的整合要快得多。廣州羊城通公司將羊城通系統直接應用於其他城市，採用當地項目建設權、營運權、發卡增值利益歸當地項目公司所有的模式，於 2003 年 12 月與南海市合作，並於 2006 年 11 月與佛山地區合作。廣佛市民可以異地消費、異地充值，甚至進行異地客服。2008 年每月互相刷卡消費已超過 30 萬人次，實現無縫整合。

這種模式適用於推動建設交通卡系統中的城市。由廣州羊城通公司統一提供密鑰管理與票卡初始化作業，中央清算服務則僅收取象徵性的服務費用，遠低於當地自建的成本，可以有效優化整合資源、降低投資、經營、技術和政策風險，也能降低市場開發難度。羊城通目前已與廣東省內多個城市協商過互通事宜，如東莞、湛江、肇慶、中山、江門、惠州等。羊城通系統仍有幾百萬交通卡的剩餘容量，如果將其他城市的交通卡信息納入其中，尚不需要增加額外的系統設置投資成本。

除廣佛等待各市協商外，珠江三角還有東莞將實現跨城東莞一卡通。從 2006 年 7 月開始已在城巴上啟用 IC 卡，逐漸推廣至旅遊巴士、區間巴士，最後是涵蓋到東莞的整個公交系統。東莞城巴在技術上已能與羊城通和深圳通整合，但由於剛剛施行交通 IC 卡服務，有待營運穩定後，再和兩

個城市進行協商。

實現城市一卡通之間的互聯互通，有協作和對等兩種模式，模式不同清算方式也不一樣，其方式說明如下。

1. 協作模式：中心城市建設完整的一卡通系統，衛星城市直接建置加值和消費系統，並通過數據交換系統與中心城市進行數據交換，通過結算系統與中心城市進行結算對帳。用戶卡可在兩地任意消費。廣佛目前採取的是協作模式，目前廣佛軌道交通由 IC 卡營運方結算。
2. 對等模式：即兩個城市各自建設完整、獨立的一卡通系統，利用中國建設部之消費密鑰全國統一的特點，用戶卡可在對方城市消費，兩個城市間互相交換跨區域消費數據及名單數據。

從區域發展來講，協作模式是比較理想的作法，可以節省大量的資源，避免重複建設，關鍵是各票證系統商之間能不能談得攏。阻礙珠江三角城市間公交一卡通進程最關鍵的是城市間本位思想，各城市發展交通 IC 卡各自為政，有先有後，應用範圍也不同，如廣州羊城通已經發行近 1000 萬張，因此在整合時有的城市就會有地域觀念。有的城市認為，外市的交通 IC 卡比自己先進，自己要升級匹配，或許會認為自己被別人併吞而難以接受。有些城市認為要花大筆投資改造系統不值得。因此，只有將區域共同利益置於地方利益之上，才能打破成見，真正構築一體化的區域共同市場。

2.2.2 由政府出面主導交通電子票證整合

一、曼谷大眾運輸電子票證整合

曼谷地區目前有兩條捷運路線，分別由 BTSC (Bangkok Mass Transit System Company Ltd.)及 BMCL(Bangkok Metro Public Company Ltd.)兩家公司營運，由於政府欠缺一套電子票證標準，目前兩家捷運公司各自發行電子票證，彼此電子票證系統間無法互通，轉乘旅客除了必須準備兩張卡片外，兩家公司收取的基本運價(Flag-fall)總和也十分可觀。有鑒於此，泰國政府正進行一項共通票證系統計畫(Common Ticketing Smart Card System)，將制定一套捷運系統之共通票證標準，該標準涵蓋卡片規格、前台設備及後台系統等，未來將要求新成立的捷運公司採用該套標準，僅能使用新的共通票證，既有捷運票證系統初期則採用兩套系統並行方式，讓

既有票證及共通票證均能在既有捷運票證系統中運作，再逐漸淘汰既有票證系統而完全採用共通票證。

除了票證規格統一外，泰國政府未來將主導並出資成立票證公司，該公司將負責建置票證清算平台並發行捷運共通票證，初期由政府擁有 100% 股權，當清算平台建立後，逐步將部份股份釋放給既有及新成立之捷運公司，使捷運公司亦能參與新票證公司的營運，但政府最後仍將保有該公司 40%~60% 的股份，使政府能主導該公司的電子票證策略以確保社會利益，此外，為使該票證公司能夠順利成立，並使後續清算平台的建置與營運能夠滿足捷運票證整合需求，政府將另委外招標一個計畫管理團隊，協助政府成立票證公司及監督票證清算系統的建置與營運，目前該共通票證系統之規格仍在規劃中，預計 2009 年中完成。

二、瀋陽「城市一卡通」

瀋陽「城市一卡通」的營運單位是瀋陽城市通有限公司(原瀋陽天龍金卡有限公司)，是中國國家金卡工程的試點城市。瀋陽城市通有限公司是市政府授予的瀋陽市唯一發卡單位，採用 CPU 卡技術，於 2003 年 7 月開始籌備，並於 2004 年 8 月正式營運，迄 2008 年 7 月發卡量已達到 300 萬張，瀋陽市已成為中國國內城市一卡通領域首例大規模成功使用 CPU 卡的城市，也是 CPU 卡發卡量最大的城市。

瀋陽市「城市一卡通」的建設目標是實現跨行業一卡多用途，建構的基礎是 IC 卡技術的城市信息化平台，該系統採用先進、成熟的計算機技術和 IC 卡技術，是一個高效率、多應用的城市一卡通應用信息平台和電子支付收費系統。

卡片規劃的應用範圍包括公交、地鐵、出租、水、煤氣、熱力、加油、有線電視、旅遊、社區管理、停車收費、餐飲、超市等以電子支付為核心的小額消費領域，從公交入手，逐步向其他小額消費領域拓展。迄 2008 年 7 月已應用的領域有：公交、加油、小額消費、公用事業繳費試辦點，正在建設的領域主要是應用於小額消費的拓展，包括出租車、餐飲、藥店、超市、電影院等。

在城市一卡通系統技術因素中，卡片類型的選擇是成功的基礎，整合應用平台是成功的關鍵，密鑰管理系統是實現一卡多用途和城市互聯的前提，說明如下：

1. 雙界面 CPU 卡

卡片類型的選擇符合中國建設部積極倡導「優先採用符合行業標準的 CPU 卡」的精神，採用雙界面 CPU 卡，是一種支持接觸式與非接觸兩種通訊方式的智慧卡，具有高安全性、高擴展性、高運算能力、高應用承載能力、大儲存量、便於攜帶、不易磨損等特性，適合於金融與非金融的各類應用，符合《中國金融集成電路 IC 卡規範》和《中國金融集成電路 IC 卡應用規範》。

2. 跨行業及一卡多用途的城市一卡通平台

瀋陽「城市一卡通」所採用的跨行業及一卡多用的城市一卡通平台，具有安全性、穩定性及可擴展性的特性。該平台包括三個主要應用系統，包括高安全規格、功能完善的清分清算系統；卡片發行系統；信息交換和信息管理系統。該系統安全、穩定的運行是實現跨行業一卡多用、城際間互聯互通的重要基礎。

3. 建設部密鑰管理系統

瀋陽「城市一卡通」項目採用中國建設部的密鑰管理系統和機具安全模組，採取必要的安全管理機制，能夠確保瀋陽「城市一卡通」系統發卡、充值、消費、清算、資金劃撥等環節高度的安全性，方便城市一卡通進行行業拓展和城際間的互通互聯。

綜合瀋陽「城市一卡通」成功的關鍵因素，包括以下幾個方面：

1. 體制創新

瀋陽「城市一卡通」採用「市場化運作」的模式進行營運管理，提出「政府主導、市場運作」的理念，以股份制的型式成立了瀋陽天龍金卡有限公司(瀋陽城市通有限公司的前身)。透過資金入股，使各入股的企業在共同利益下共同努力。體制的創新，既解決了系統建設的資金問題，又使一卡通系統營運管理工作真正做到市場化。

瀋陽市市政府在建設的過程中只進行宏觀管理與導向，制定有關政策法規，而各系統建設的技術方案、管理方法、經營模式等方面均由企業自主決定，加快了建置的進程。

2. 機制創新

一卡通系統涉及範圍廣、影響大，需要參與建設的各企業共同努力，共同承擔營運管理和服務的責任，瀋陽城市通有限公司與各入股的企業共同承擔風險，共享利益，把各參與的企業結合在一起，確定共同的目標和彼此的權責利害關係，相互制約，使得各方獲取利益最大化。

3. 技術創新

瀋陽城市通有限公司與系統供應商共同進行總體規劃，充分了解各行業需求，對於關鍵技術充分掌握，選擇先進、實用的技術，對於大量數據、關鍵業務充分做好壓力測試工作。

4. 管理創新

(1) 制定各項管理規定

瀋陽城市通有限公司依法立規，為服務制定各種方案和管理規定，分別制定了《一卡通運營管理方案》、《瀋陽市「城市一卡通」系統 IC 卡使用管理規定》、《瀋陽市「城市一卡通」系統清算管理規定》、《瀋陽市「城市一卡通」系統 IC 卡發行管理規定》等規定來規範一卡通系統的營運管理。

(2) 分級管理

為了使建設和營運管理得以順利進行，瀋陽城市通有限公司建立了分級管理制度，分別定期召開各項例會，即時商討、協調、解決系統營運管理和行業拓展中出現的問題。

(3) 以消費者為中心，提高服務理念

瀋陽城市通有限公司把自己定位為「服務型」公司，以提高服務質量為宗旨，在提高人員素質、創造良好的卡片使用環境、建立熱線諮詢電話、處理市民投訴和建議等方面予以改善，取得顯著成效。

隨著中國國內許多地區經濟的快速發展，各地區間交流頻繁，公共交通 IC 卡互通趨勢逐漸明朗。最突出的特點就是許多跨省的中、大城市已經形成了聯絡緊密的城市群落，因而公共交通 IC 卡在城市間的互通互用，方便地區人員的往來方面的需求越來越迫切。

2008 年 12 月，中國住房和城鄉建設部標準定額研究所在北京召開《城市互聯互通卡通用技術要求》等系列行業標準編寫工作會議。「城市互聯互通卡系列行業標準」包括《城市互聯互通卡通用技術要求》、《城市互聯互通卡清分清算技術要求》及《城市互聯互通卡密鑰及安全技術要求》，是由中國住房和城鄉建設部於 2008 年 6 月批准編制的國家行業標準，IC 卡應用服務中心為主編單位。該會議確定標準的制定工作須遵循「一致性、先進性、可行性」三個基本原則，參編單位就卡片技術要求、終端機具技術要求、密鑰系統安全要求、互聯互通密鑰應用要求、應用系統安全技術要求、卡片及終端安全、安全機制、區域界定、清分清算規則等問題加以探討，確定了前述三項技術需求之編寫大綱。

三、巴黎多用途交通卡

1960 年代磁卡付費就已成為巴黎公共交通系統的主流支付方式，但是隨著乘客數量的不斷增加，偽造磁卡的不斷出現以及磁卡讀卡機昂貴的維修費用，使磁卡付費系統已經無法符合市場發展的需要。1990 年，巴黎公交總公司與 INNOVATRON 公司合作開發一套新的票務系統，後來隨著 SNCF 公司和一些參與過歐盟 ICARE 和 CALYPSO 框架計劃的歐洲公司的加盟，使得該項目的科技研發能力逐漸提升。

目前巴黎多用途交通卡已經開發出了一系列的產品，這些新產品可以應用於公共交通支付、電子支付、緊急救援服務等領域，並根據不同用戶的需求，分別應用了達到國際標準的接觸或非接觸式技術，某些技術甚至同步推動了國際標準的發展。

由於此系統具有強大的功能，乘客可根據自己的需求選擇不同的交通卡，其類型分述如下：

1. 小型卡：

可供偶爾乘坐公交車之乘客使用，面值較小，為一次性的非接觸式 IC 卡。

2. 普通卡：

係帶有微處理器的 CPU 卡，可供經常乘坐公交車的乘客使用，可分為接觸式和非接觸式兩種 IC 卡。

3. 大型卡：

一種配有小型鍵盤和顯示幕的 CPU 卡。這種卡可根據用戶的設定接收和查閱地鐵信息和各種快速鐵路信息，還可加裝緊急救援系統，以便救援人員能迅速的確定持卡人所處的位置。

在多用途交通卡的推廣方面，目前共發行了四種主要卡種：

1 單一用途交通卡

法國尼斯和亞眠市早在 1999 年就已經使用了非接觸式交通 IC 卡，其他城市對推廣這一系統也表示支持，並決定在更廣的領域內對該系統進行測試和應用。巴黎大區在 125 座公交車站成功安裝並使用該系統後，於 1999 年 7 月決定正式使用該系統，並於 2000 年年中簽署了在 800 座車站安裝非接觸式交通卡系統的合約，成為世界上最大的非接觸票務系統。到 2001 年秋天，巴黎大區已有超過 100 萬人次使用非接觸式交通 IC 卡年卡。到 2003 年非接觸式交通卡的種類將擴展到月卡、星期卡和一次性卡。而最終這種非接觸式交通 IC 卡將完全取代一次性磁卡成為公交付費的主要方式。

2. 多用途交通卡

多用途交通卡除了可作為日常公交支付的票卡外，其快速、安全的特點，還可應用於電子支付和發展緊急救援服務等用途。在多用途交通卡上有一塊專門負責電子支付的資料儲存區，可紀錄持卡人的各項小額購物，包括：購買報紙、咖啡、支付自動販賣機、打公共電話等；在市區的交通設施中可用於支付停車費、過路費、乘坐計程車等。

3. 旅遊卡

在歐洲，可在非接觸交通卡中裝入票款和一些預付費服務的功能，以便遊客在其他城市使用。

4 巴黎公交公司內部使用之交通卡

這種多用途交通卡主要用於公交公司內部，可應用在日常生活中的各個領域，例如：考勤、出入通行卡、支付午餐等等。

2.2.3 由系統整合商和私營企業聯合發起多用途交通卡

一、SONY 與飛利浦的合作方案

SONY 與飛利浦於 2008 年合資成立 Moversa 公司，共同推廣手機作為虛擬錢包來購物和購買火車票的應用。這項技術是開發一種包含了兩家公司非接觸晶片卡格式：Mifare 和 FeliCa 的晶片，來促進智慧卡在手機中的應用。

飛利浦開發的 Mifare 和 SONY 開發的 FeliCa 是目前安全非接觸晶片領域應用最為廣泛的兩種格式，它們被嵌入到大樓、公交系統中，或被嵌入到手機中作為電子錢包。這項技術及相關服務在亞洲已經相當普及，尤其是在日本使用更為廣泛。相關技術供應商和服務供應商都積極在全球推廣它們的應用。

SONY 和飛利浦宣稱這種安全晶片的首個樣品已於 2008 年中期推出，以作為嵌入到手機中的解決方案。雙方的目標是於 2009 年底進行商業部署。

二、NFC 手機於交通的應用與多用途整合

NFC(Near Field Communication，近距離無線通信)是由飛利浦公司發起，由諾基亞、SONY 等著名廠商聯合主推的一項無線技術，NFC 設備可以用作非接觸式智慧卡、智慧卡的讀寫器終端以及設備對設備的數據傳輸通路。

2008 年開發的 NFCIP-1 晶片已符合 ISO/IEC 18092，能讓手機代替人們身上各種各樣的「卡」，使手機從通信層面跳躍到了支付層面，讓手機成為真正的「一卡通」。諾基亞應用 NFC 讓手機成為電子錢包，把銀行卡、交通卡、門卡、VIP 卡均予以涵括，還可以利用 NFC 的讀卡功能，實現商品的防偽驗證。

諾基亞 6131iNFC 手機已於 2008 年 9 月底正式在北京進行商業應用，用戶買了手機以後，可以充值電子票證，和普通一卡通是一樣的，所以，可用一卡通的地方，NFC 手機也一樣可以使用。NFC 手機也會隨著北京市政交通一卡通的應用擴大而拓展使用範圍。

由於 NFC 要把不同的卡置入同一個晶片中，使得 NFC 產業鏈需要有不同的角色共同組成，通訊運營商、芯片製造商、服務提供商、應用提供商等。以營運商為例，SIM 卡一直被通訊營運商視為重要資產，目前主要

用於基礎網絡連接，只有營運商找到有效的獲利模式，NFC 服務才能夠大規模推行，但是對於產業鏈上每個環節都缺一不可的 NFC 移動支付而言，其他行業的利益同樣需要平衡由於涉及多個行業的合作，主導權的爭奪十分微妙。

為此，諾基亞與德國捷德(G&D)成立合資公司，研發空中發卡等新的服務應用，關注更多的增值服務和商機。預計 2009 年，NFC 論壇會聯合 GSMA、ETSI 定義 NFC 標準，將 NFC 技術規範化，促進 NFC 產業鏈的發展²。

2.3 第一年期計畫成果回顧

第一年期計畫主要工作項目共有四大項，其工作內容與重要成果分述如下：

一、國內外電子票證系統之最新應用狀況與發展趨勢調查

該計畫蒐集國內外票證系統最新應用狀況與發展趨勢，並統計最新營運統計資料，國內部份調查成果如 2.1 節，國外部份調查成果彙整如表 2-3 所示。

²本節資料來源：

1. 金卡網(<http://www.goldencard.com.cn/>)。
2. 巴黎多功能城市交通 IC 卡，中國公交網(<http://www.cupta.net.cn>)，2008-8-19。
3. 技術和理論層面無障礙珠三角何時一卡通十城，南方日報網路版(www.nanfangdaily.com.cn)，2008-4-21。

表 2-3 國外電子票證系統營運現況彙整表

系統別 營運現況	香港八達通卡 Octopus Card	倫敦牡蠣卡 Oyster Card	日本西瓜卡 Suica	北京市政交通 一卡通	上海公共 交通卡
正式營運 時間	1997	2001	2001	2003	2000
發卡量	1400 萬張(2007)	700 萬張(2006)	2200 萬張(2007)	1400 萬張(2007)	1200 萬張(2006)
日交易量	1000 萬次(2007)	343 萬次(2006)	1600 萬次(2007)	1200 萬次(2007)	260 萬次(2006)
卡片種類	FeliCa	Mifare	FeliCa	Mifare	Mifare
發行單位	八達通公司	TranSys 公司	JR 東日本	北京市政交通 一卡通公司	上海公共交通 卡公司
交通票證 範圍	地鐵、巴士、渡 輪、停車場、停 車表、計程車(試 辦)	地鐵、巴士、輕 軌、渡輪、國家 鐵路	JR 東日本、新幹 線、地鐵、停車 場	地鐵、巴士、計 程車、高速公路 收費	地鐵、磁浮、輪 渡、巴士、停車 場、高速公路收 費、旅遊交通、 計程車
其他用途 範圍	零售業、自動販 賣機(含電話 亭)、自助影印 機、圖書館、休 閒娛樂業、圖書 館、門禁系統	無	零售業	電影院、連鎖藥 房、美髮店、連 鎖餐廳、便利商 店	社區門禁、汽車 修理、汽車租 賃、加油站、快 遞
其他	該公司由金管 局認定為「接受 存款公司」，解 除其應用在小 額消費之限制	民間參與方 式，由倫敦交通 局委託 TranSys 建置與營運	與關西 ICOCA 及東京 PASMO 互通，卡片可在 對方系統中使用		與無錫、蘇州、 阜陽等地公車 互通

資料來源：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)－電子票證與驗票機介面規範及票證一卡通論壇推動之規劃，交通部運輸研究所，民國 97 年。

二、國內電子票證系統及設備廠商開發現況調查

調查國內系統及設備廠商已開發各類電子票證卡片、設備及系統之功能及規格，分析與比較不同票證系統間的異同處。在卡片方面，國內各票證系統除南部地區 TaiwanMoney 系統外，其餘系統均使用飛利浦 Mifare 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、老殘票、學生票等。

4. IC 卡須能記錄最近一筆交易資料，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 格式卡片的資料儲存於內部所提供的記憶體空間，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)，其結構圖如表 2.3-1，其中 AC(Access control)為每一個扇區的存取權限控制設定資料，包括存取控制用認證金鑰(Key)及存取條件(Access condition)設定資料。

南區交通 IC(TaiwanMoney 系統)卡屬於複合式卡(Combi-Card)，為一 CPU 卡，採用 PayPass 應用程式處理卡片資料，晶片檔案資料結構與 Mifare 不同，其晶片檔案資料結構圖如圖 2-1。

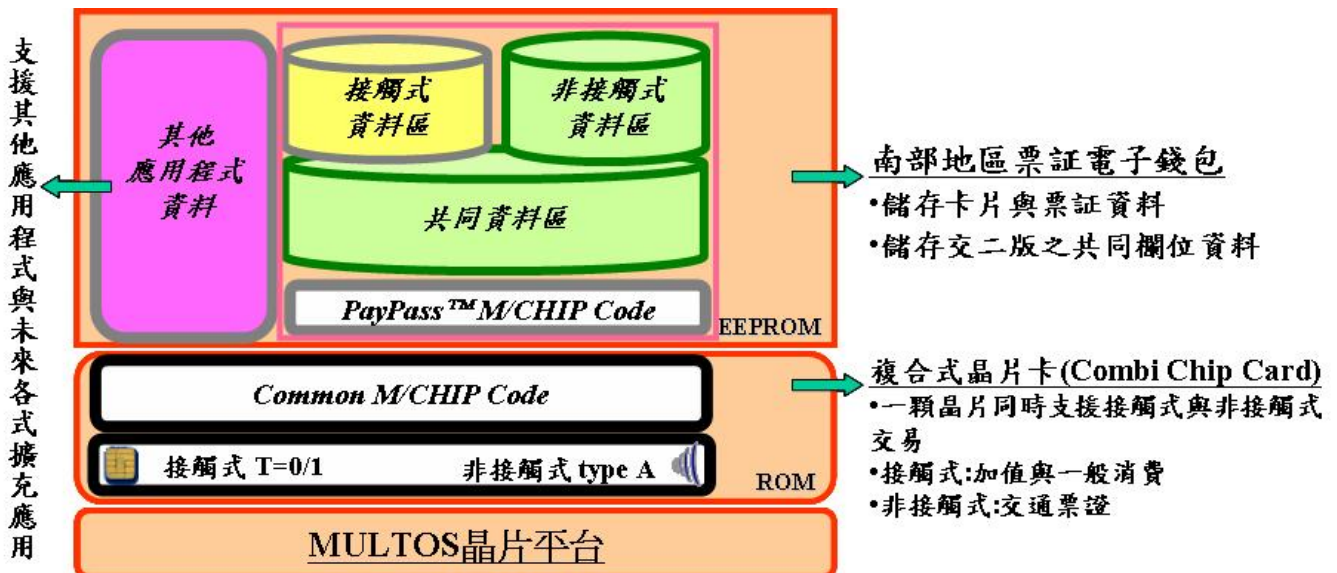


圖 2-1 TaiwanMoney 卡片系統結構圖

資料來源：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)－電子票證與驗票機介面規範及票證一卡通論壇推動之規劃，交通部運輸研究所，民國 97 年。

在驗票機部份，國內除南部地區 TaiwanMoney 系統同時支援 Mifare 及 PayPass 卡片規格外，其餘系統均支援 Mifare 卡片規格，TaiwanMoney 驗票機之加密算法採用 RSA 外，Mifare 系統驗票機均採用 3 DES 演算法，Mifare 系統驗票機若需讀取 TaiwanMoney 卡片，驗票機必須經過 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 SAM 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)，少部份驗票機(RC531)則具有 4 個插槽，因此若採用 SAM 卡進行票證整合，需更新驗票機設施，其整合代價較高，其餘票證公司驗票機的 SAM 卡插槽則在 4 個以上，各電子票證系統之驗票機主要功能比較如表 2-4。

表 2-4 國內電子票證系統驗票機功能比較表

系統別 驗票機比較項目	悠遊卡系統		臺灣通系統		南部地區電子票證 (TaiwanMoney卡)	高速公路電子收費 系統
設備形式	場站驗票機(捷運、纜車、停車場)	公車驗票機	公車驗票機	公車驗票機	公車驗票機	OBU (車上設備單元)
支援卡片規格	Mifare Type A	Mifare Type A	Mifare Type A	Mifare Type A	Mifare Type A + PayPass	Mifare Type A
交易速度	0.3sec 以下	0.6sec 以下	0.3sec 以下	0.3sec 以下	0.6sec 以下	0.3sec 以下
交易距離	5cm 以上	6cm 以上	5cm 以上	5cm 以上	5-10cm	1 cm 以內
計費模式	段數計費	里程/段次計費雙模式	里程/段數計費雙模式	里程/段數計費雙模式	里程/段數計費雙模式	計次收費
GPS 定位功能	無	內建 GPS	GPS+手動定位	GPS+手動定位	GPS+手動定位	無
營收資料傳輸方式	PDA 下載	無線傳輸+ 備用記憶裝置手動傳輸	無線傳輸 + 備用記憶裝置手動傳輸	無線傳輸 + 備用記憶裝置手動傳輸	無線傳輸 + 備用記憶裝置手動傳輸	經收費車道主動傳輸至後端系統
備用記憶裝置		USB 介面+RS232 介面	CF 插槽+RS232 插槽	CF 插槽+RS232 插槽	CF 插槽+RS232 插槽	電子收費車道系統
加密演算法	3 DES	3 DES	3 DES	3 DES	RSA	3 DES
交易資料儲存數量	2,000 筆以上	3,000 筆以下	3,000 筆以上	3,000 筆以上	10,000 筆以上	即時傳送電子收費車道儲存, 次日回傳後端系統
操作盤	無	具備	具備	具備	具備	餘額讀取鍵
卡種識別模式	警聲	具警聲、語音及 LED 顯示燈	具警聲及語音	具警聲及語音	具警聲及語音	警聲
SAM 卡插槽	RC531 具備 4 組, RC171 具備 1 組測試用插槽		RC531 具備 6 組, RC171 具備 4 組	RC531 具備 6 組, RC171 具備 4 組	6 組(1 組金融、5 組交通運輸)	無
車輛故障處理機制	無		路故上、路故下	路故上、路故下	特許上、路故上、路故下	執法系統+人工判案
印表機		具備列印介面, 可搭配印表機列印乘車收據等	可外接列印中英文及數字之印表機			無

資料來源：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)－電子票證與驗票機介面規範及票證一卡通論壇推動之規劃，交通部運輸研究所，民國 97 年。

三、臺鐵電子票證系統整合規範需求分析

為配合鐵路捷運化的實施，臺鐵局已正進行車種簡化計畫，在西部幹線僅區分為城際列車與區間列車兩種。區間列車的發車密度高，如同捷運一般，民眾對於可快速通關的電子票證需求將會大幅提高，故臺鐵局實施電子票證有其必要性，在短期階段以應用在區間列車之儲值式 IC 卡為發展對象，中長期階段則建議擴充在城際對號列車及定期票兩類票種。

臺鐵局與聯外運輸系統的轉乘非常重要，大部份的民眾必須透過轉乘系統才能完成旅程，故本計畫在分析臺鐵局的電子票證與其它交通 IC 卡互通的模式之後，提出互通雙方必須遵循共同介面規範的必要性。其中，驗票機將資料傳送所屬內部系統的過程屬於內部網路介面，不需制定共同的介面規範，但是交易資料送達清算中心之後，各票證系統的資料檔案必須交換，故臺鐵局的電子票證若欲與其他票證系統的卡片互通，必須制定最前端卡片與驗票機之間，以及最終端清算中心之間的介面規範。

四、電子票證跨系統整合模式評估

該計畫評估三種跨票證系統整合技術方案，分別是以 SAM 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認為第三方案(發行交三版卡片整合不同發卡組織前端設備)具有「一次到位」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卡片規格，並利用方案一的 SAM 卡整合技術，修改各系統既有驗票機使其讀取交三版卡片。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無法容納多個 SAM 以及多個 SAM 可能影響驗票機交易速度的問題。

發行交三版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。

第三章 交三版(草案)卡片內部功能規格與交易流程定義

本計畫延續前期計畫之規劃成果，以交二版卡片規格為基礎，規劃交三版檔案資料格式、內容及交易流程，並邀集各電子票證公司、運輸業者及相關主管機關，歷經 16 次技術討論會議，歸納各界共識後規劃出下列草案內容，並已提送交通部，以進行後續之審查作業程序。

3.1 修訂目的及範圍

本版卡片格式規劃之目的係期透過發行可跨系統交易營運之「電子票證系統多功能卡片規劃書(第三版)」(以下簡稱「交三版」)之卡片，與目前各票證發卡公司所發行的「交二版」或「在地票證卡」採用併行過渡的方式，逐步達到票證整合的目的。營運中之票證發卡公司仍然繼續使用現行的票卡資料格式，若欲發行與其他票證發卡公司整合互通的票卡，則必須遵照「交三版」規劃的卡片資料格式及交易流程，並於驗票機安裝符合「交三版」規範的 SAM 卡，以達到新、舊卡皆可在同一台驗票機交易的目的。

本計畫主要以作為交通運輸系統使用之非接觸式 IC 卡(Contactless IC Card)及雙介面複合式卡(Dual Interface Card)為修訂標的，其規格訂定的範圍包括卡片實體規格、卡片及其介面設備之介面規格、卡片內部功能規格(檔案結構及檔案資料格式、內容及存取權限)、卡片資料安全功能需求、編碼準則及交易流程設計等。

有鑑於交二版在卡片檔案資料格式及交易流程的規劃上未能滿足國內多卡整合的需要，因此，交三版增加以下規劃內容：

一、彙整並精簡卡片交易資料所需的欄位

交三版以「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接繼連續性封閉性系統」最常應用，例如下列之情境一：

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」，各情境示意如圖 3-1。

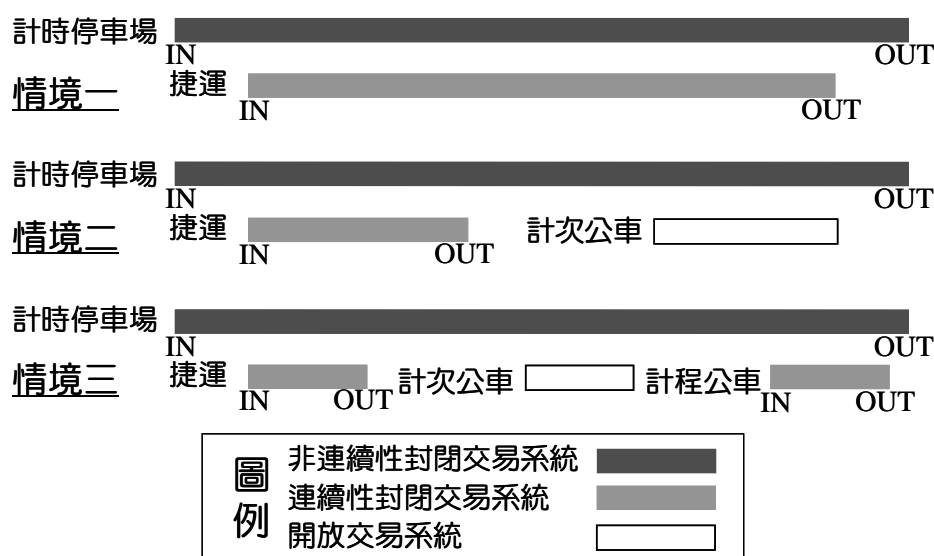


圖 3-1 不同收費模式情境之示意圖

交三版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，例如公路計程客運，二者的交易流程略有不同。

根據以上分析，交三版以三個扇區，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」包含所有交通電子票證交易所需的檔案存放欄位，請詳見 3.2 節。

二、明確規範交易流程

交二版未規範明確的交易流程，使得每一家發卡單位¹皆有自己的交易

¹發卡單位：指擁有金鑰管理系統，能對卡片所有欄位進行錄製的單位，例如：悠遊卡公司(0x02)、

流程。交三版則規劃各發卡單位皆必須遵守的交易主流程以及參考交易流程，透過交三版的統一規範之後，各發卡單位的驗票機才能彼此讀寫卡片資料，請詳見 3.4 節。

三、增加雙介面複合式卡(Dual Interface Card)的參考規範

雙介面複合式卡其資料檔案結構應符合 ISO/IEC 7816 之規定，管理儲存記憶體可不需以固定的扇區作存取限制，檔案結構建議以標籤(Tag)資料記錄模式。本版以已發行營運中之「南部地區交通電子票證」-TaiwanMoney 卡為參考規範，供非使用 Mifare 卡片系列的發卡單位參考。

在非接觸式 IC 卡(Contactless IC Card)方面，交三版基本上沿用交二版的規格，因此在卡片實體規格、卡片與卡片介面設備之介面規格、卡片資料安全功能需求以遵照交二版規劃為原則；在雙介面複合式卡(Dual Interface Card)方面，因各卡種技術上的差異頗大，在能與非接觸式 IC 卡讀寫相容的前提下，本版以 TaiwanMoney 卡為參考規範，由各發卡單位自行參考規劃。

為使卡片交易於跨系統時能彼此整合，交三版於卡片內部功能規格(檔案資料格式、內容及存取權限)、編碼準則、交易流程設計參考等均有大幅度的修訂，茲於後續各節中詳細說明，另有關交三版(草案)與交二版差異比較表如附錄 5。

3.2 檔案資料格式、內容及存取權限

交三版交易資料檔案欄位可概分為二大類，分別是封閉交易系統及開放交易系統。封閉交易系統(進/出或上/下均需讀卡以完成扣款程序)可再分為「連續型」及「非連續型」兩類。

「連續型封閉交易系統」指交易流程中不中斷，進/出或上/下必須連續發生，中途不會插入其它交易，例如：軌道運輸、客運運輸；因軌道運輸進/出的扣款設備並不相同，但是客運運輸上/下的扣款設備係同一設備，故「連續型封閉交易系統」又再細分為「異機進出連續型封閉交易系統」及「同機進出連續型封閉交易系統」。

「非連續型封閉交易系統」指交易流程中有可能插入其它交易，例如：路外停車場收費系統。

「開放交易系統」係指「一次扣款行為」，故直接由「主要票值」欄位中扣除，不再單獨規劃應用欄位。

遠通電收公司(0x08)、臺灣智慧卡公司(0x05)、高雄捷運公司(0x06)等。

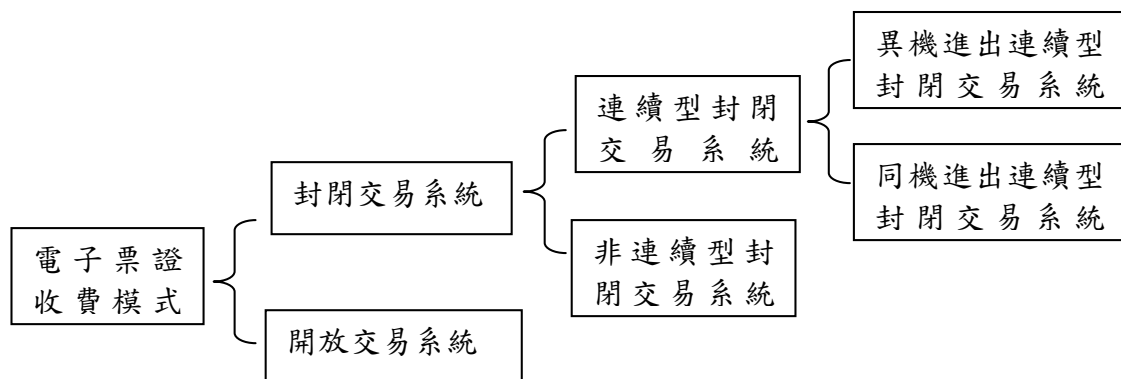


圖 3-2 以電子票證收費模式規劃交易資料檔案格式

據此交三版在卡片內部功能規格上新增交三版資料應用區間(Sector 9~11)，用以記載連續型封閉交易系統及非連續型封閉交易系統的卡片交易資料；目錄服務區及共同資料區仍沿用交二版的規劃精神，僅於部份欄位新增內容及修訂定義。

在存取權限方面，交三版目錄服務區(Sector 0)的金鑰讀取權限規劃為固定的 Key Value，以便應用系統都能快速讀取卡片出廠資料及目錄服務指標，方便卡片搜尋交易所須的欄位；共同資料區(Sector 1~5)基本上遵循交二版的規劃；交三版應用資料區(Sector 9~11)則規劃應用系統²的金鑰權限僅可「讀取」，交易系統³則可「寫入」。

交三版資料欄位格式規劃如表 3-1。

表 3-1 交三版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	卡片管理	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	

²應用系統：提供持卡人運輸服務或其它服務的前端設備系統，包括減值系統及查詢系統等，但不包括加值系統。

³交易系統：提供持卡人運輸服務或其它服務的減值或加值系統。例如：臺北大眾捷運系統(0x02)、臺灣汽車客運系統(0x07)等。

表 3-1 交三版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
	電子票值	2	主要票值	寫：發卡單位 加值單位 讀：應用系統 減值：交易系統
			票值備份	
			票值加值記錄	
	共用資料	3	卡片交易狀態資料	寫：交易系統 讀：應用系統
			最近兩筆交易記錄(1)	
			最近兩筆交易記錄(2)	
		4	最近六筆交易記錄(1)	寫：交易系統 讀：應用系統
			最近六筆交易記錄(2)	
			最近六筆交易記錄(3)	
		5	最近六筆交易記錄(4)	寫：交易系統 讀：應用系統
			最近六筆交易記錄(5)	
			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	連續型封閉交易系統	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	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(1)	
			同機進出連續型封閉交易系統最近兩筆交易記錄(2)	
	非連續型封閉交易系統	11	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

3.3 編碼準則

為達票證整合目的，本節所規範之編碼準則係所有應用「交三版」發行票卡之單位皆必須遵守，包括：

一、交易(應用)系統 AID 編碼

交易(應用)系統 AID 編碼的原則是依交易(應用)系統提出申請並經審核完成後的先後順序給予該系統編碼。

AID 編碼主要是做為跨交易(應用)系統時讀寫資料的索引，因為 AID 欄位有限，為使欄位有效使用，本規劃建議交三版 AID 申請及編碼準則如下：

1. 新申請 AID 的交易(應用)系統必須有跨系統之需要，不與其他交易(應用)系統整合或缺乏整合之規模與能力者，AID 編碼一律為 0xFF，不須申請及列管，若他日欲與其他交易(應用)系統整合時再提出申請。
2. 新申請 AID 的交易(應用)系統必須具有基本的驗票機台數及預估發卡量之規模，並經主管機關認定具備與其它交易(應用)系統整合之能力；或經主管機關專案核可認為有必要新增 AID 者。建議基本驗票機台數最少 2,000 台，預估發卡量 30 萬張，以上數量應隨市場發展每年調整之。
3. 屬於卡片應用資料區的 AID 編碼一律為 0xFF，X=1~F 為申請序號。交三版新增三個卡片應用資料區的 AID 如下：

交三版異機進出連續性封閉系統	0xF1
交三版同機進出連續性封閉系統	0xF2
交三版非連續性封閉系統	0xF3

二、發卡單位編碼

發卡單位編碼的原則是依發卡單位提出申請並審核完成後的先後順序給予該單位編碼。申請發卡單位編碼必須先取得 AID 編碼，並經主管機關認定具備發卡之專業能力者。

三、卡片規格版本編碼

發行格式定義如下：

high nibble：主版本

0x2X：交二版

0x3X：交三版

low nibble：次版本

X=0：標準版本

X=1~F：各發卡單位自行規劃交三版衍生應用版本順序

四、卡片狀態編碼

記錄卡片經發行單位⁴所做的最新狀態，目前包括以下四種狀態項目：

狀態項目	記錄內容	說 明
尚未啟始化	0x00	卡片尚未被發行單位執行啟始化工作
已完成啟始化	0x01	卡片已被發行單位完成啟始化工作
已完成個人化	0x02	卡片已被發行單位完成個人化工作
黑名單指標	0xFE	卡片已被發行單位設定為黑名單

五、基本身分別編碼

記錄卡片持卡人的使用身分別，編碼格式定義如下：

0x00：一般民眾

0x01：老人(>70 歲)

0x02：老人(65-70 歲)

0x03：殘障(愛心)

0x04：陪伴

0x05：學生

0x06：軍人

0x07：警察

0x08：兒童

六、基本身分區碼編碼

基本身分區碼以各縣市中華電信長途電話區域識別碼第 1 碼為 high

⁴發行單位：指發行定期卡或社福卡的單位，須對持卡人負法律責任，例如基隆市公車處發行「學生定期票」，但是使用悠遊卡公司(0x02)的系統，則基隆市公車處為發行單位，悠遊卡公司為發卡單位。

nibble；相同的 high nibble 再依照順序編列 low nibble，日後各地區若有擴編需求則以此類推，編碼準則如下：

1. 0x00~0x0F、0x10~0x1F：保留，供主管機關統籌應用。
2. 0xFF：由發卡(行)單位彈性應用，不需列管也不與其他票證系統相通。

七、優惠補助身分別編碼

優惠補助身分別編碼記錄特殊身分隸屬於那一補助單位。代碼格式定義如下：

預設值為”0x00”

high nibble：補助單位

0x1X：社會處/局/課

0x2X：民政處/局/課

0x3X：教育處/局/課

low nibble：特殊身分

X=1：敬老

X=2：愛心

X=3：博愛

X=4：學生

X=5：特定居民(如：高雄市旗津區居民)

八、交易類別編碼

交易類別編碼使用一個位元組長度，記錄交易操作行為之類別。一般交易編碼準則如下說明，若有特殊交易類別編碼則由發卡單位依照其營運需要自行規劃。

0x0X 進站/進場

X=0 不扣款/不扣點

X=1 電子票值扣款

X=2 電子票卡扣點

X=3 電子票卡定期票查核

0x1X 出站/出場

X=0 不扣款/不扣點

X=1 電子票值扣款

X=2 電子票卡扣點

X=3 電子票卡定期票查核

0x2X 一次扣款

X=0 電子票值扣款交易

0x3X 人工加值

X=0 現金

X=1 金融卡轉帳

X=2 信用卡轉帳

X=3 記帳式

X=4 優惠積點轉換為電子票值

0x4X 自動加值

X=0 金融卡轉帳

X=1 信用卡轉帳

X=2 記帳式

3.4 交易流程設計規範及參考範例

3.4.1 非接觸式 IC 卡主要交易流程框架

為達到跨系統可相互讀取的目的，交三版規劃每一筆必須寫入共同資料區及交三版應用資料區之欄位資料必須依照圖 3-3 主要交易流程框架之順序完成交易。主要交易流程框架之外的交易流程則由各發卡單位自行規劃。

主要交易流程框架實線的步驟為必須執行且交易順序不可變動，虛線的步驟則列為選項，由各發卡單位視營運需要而調整。

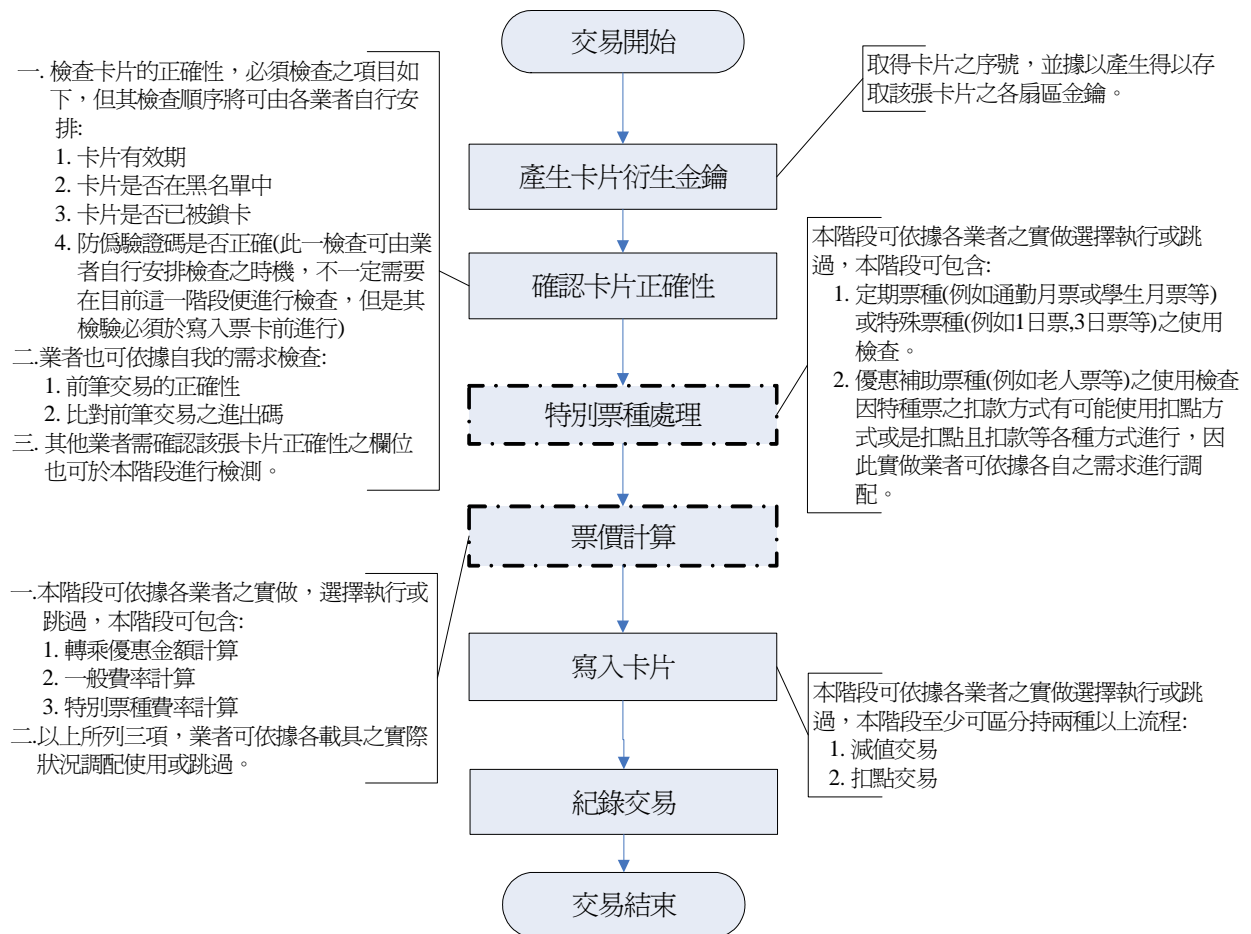


圖 3-3 非接觸式 IC 卡主要交易流程框架

3.4.2 雙介面複合式卡(Dual Interface Card)交易流程規劃參考範例

雙介面複合式卡(Dual Interface Card)因各卡種技術迥異的因素，交易流程的規劃可較有彈性，但仍須與符合交三版之非接觸式 IC 卡在資料讀取及儲存方面相容。雙介面複合式卡之交易流程分為兩部份說明，第一部份是雙介面複合式卡與非接觸式 IC 卡之交易流程的整體共同說明，其整體交易參考流程如圖 3-4；另一部份是雙介面複合式卡的主要交易流程，參考流程如圖 3-5。

以下說明雙介面複合式卡與非接觸式 IC 卡整體交易流程各步驟之行為：

步驟 1：驗票機搜尋卡片是否在感應區範圍內。

步驟 2：檢查所讀取的卡片是否符合 ISO 14443-4 規範。

步驟 3：讀取 ISO 14443-4 卡片資料內容，做為驗票機票價計算之來源。

步驟 4：卡片讀取失敗，將卡片取消選擇，使卡片進入”已搜尋到卡片”之狀態。

步驟 5：讀取非 ISO 14443-4 之卡片資料，進行卡片處理。

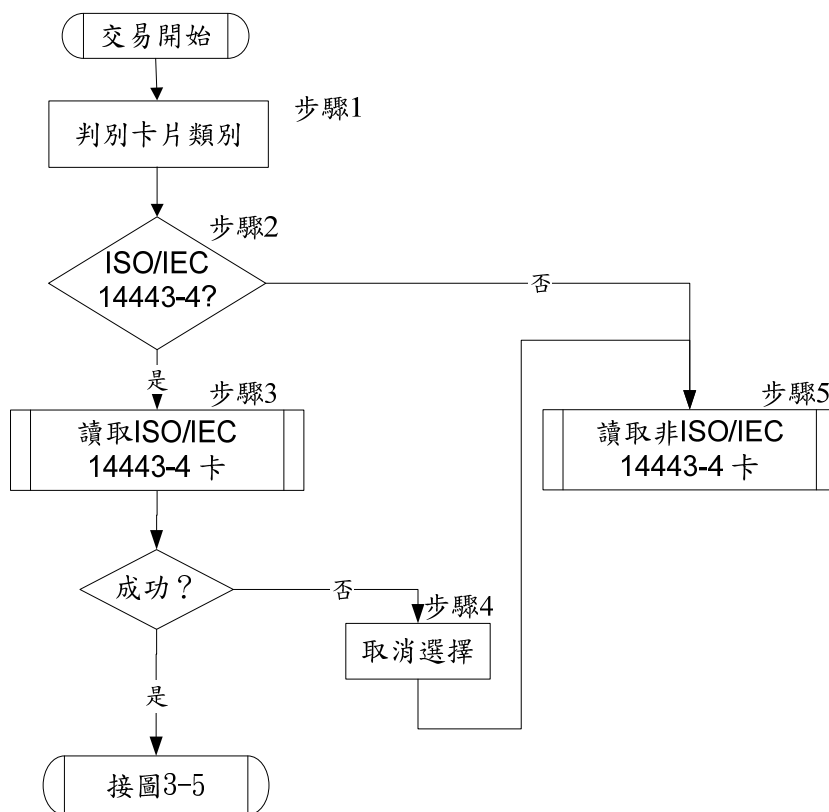


圖 3-4 雙介面複合式卡與非接觸式 IC 卡之整體交易流程參考範例

為使雙介面複合式卡之交易流程的規劃較有彈性，其主要交易流程如下：

步驟 1：讀取卡片內之應用程式。

步驟 2：若指定之應用程式不存在，則交易結束；若存在，則進行後續交易。

步驟 3：應用程式讀取最後確認並回覆票證系統 ID 標籤。

步驟 4：讀取卡片內容，包含交易所需之資料欄位集。

步驟 5：讀取卡片內容，包含交易所需之資料欄位。

步驟 6：讀取卡片內其它資料欄位集。

步驟 7：進行各種票種運算處理。

步驟 8：進行計算票價處理。

步驟 9：進行風險管理檢核。

步驟 10：進行交易接受或拒絕判別。

步驟 11：產生卡片之付款憑證(認證簽章)。

步驟 12：動態驗證付款憑證，檢查是否為偽卡交易。

步驟 13：檢查驗證付款憑證是否成功。

步驟 14：交易完成，讀卡機將交易資料寫入卡片中。

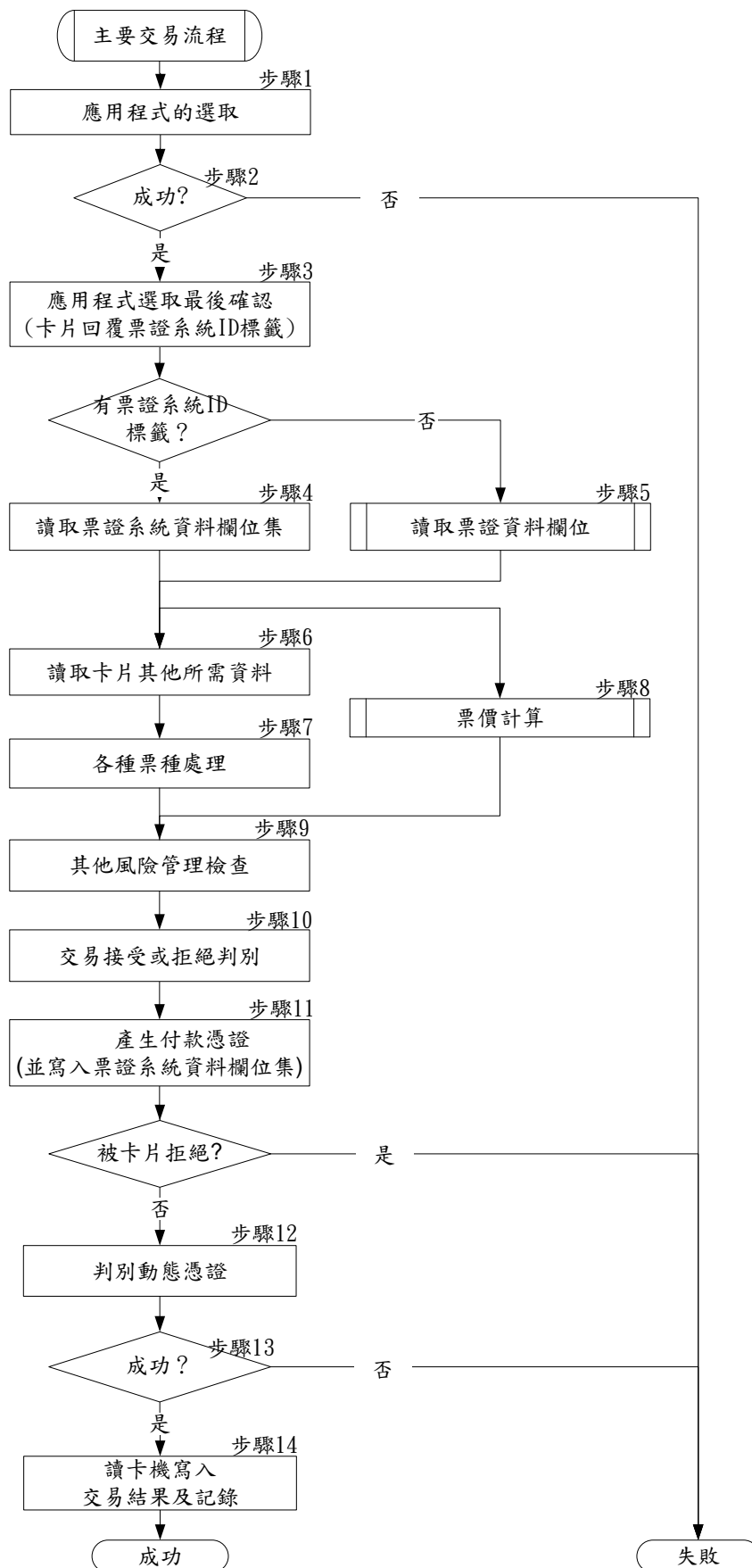


圖 3-5 雙介面複合式卡主要交易流程參考範例

第四章 以交三版為基礎之票證整合驗證機制規劃

4.1 交三版卡片驗證機制規劃

本驗證機制規劃的目的在於建立一套公正的交三版卡片格式及互通交易流程的檢驗機制，驗證各家票證業者發行的卡片能夠依照交三版所規劃的卡片格式及建議的交易流程相互通用，以確保各家票證系統能夠依照交三版卡片格式進行整合互通。另為確認卡片的格式以及減值/查詢機之交易流程確實符合交三版的規劃，本節進一步針對各家票證業者所發行的交三版卡片以及減值機的驗證機制進行規劃。

有關交三版卡片驗證機制規劃部分，本期計畫完成(1)完整交三版驗證機制規劃設計及(2)靜態卡片欄位格式檢測系統設計製作等兩部份。4.1 節係前項完整交三版驗證機制規劃設計之說明，並據此接續完成後項靜態卡片欄位格式檢測系統設計製作。

為開發靜態卡片欄位格式檢測系統，必須先訂定統一之共同減值金鑰衍生邏輯，以供申請驗證的發卡公司參用，若無此統一減值金鑰衍生邏輯，則該驗證系統將無法真實驗證不同發卡公司間的卡片是否能夠達成扣款整合的目的。

4.1.1 驗證申請作業流程

為求明確定義交三版驗證作業規範，需要有一個各家票證業者得以遵循之驗證申請作業流程規劃，圖 4-1 說明交三版驗證申請作業流程：

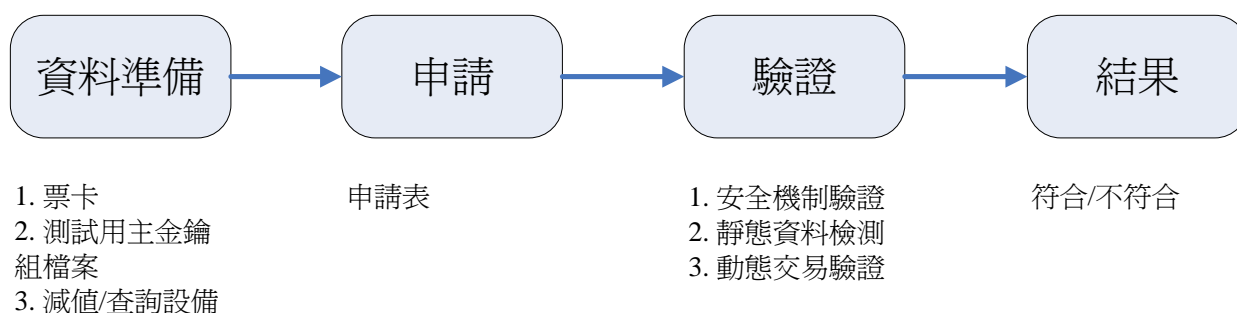


圖 4-1 交三版驗證申請作業流程

一、資料準備

為使申請驗證之票證業者(以下稱送測單位)得以順利開始進行驗證，在申請驗證之前，送測單位需先準備相關的資料以利驗證之進行。所需準備之相關資料應該包含驗證用之減值主金鑰組，及以驗證主金鑰組產製之交三版卡片。若欲對減值設備或查詢設備進行驗證，則該減值/查詢設備需能針對驗測用之卡片進行減值及查詢的動作。以下分別對所需準備之項目詳細說明：

1. 驗證用之減值主金鑰組電文檔

為使送測單位確保其減值主金鑰組之安全性，且不需進行驗證而須另行修改發卡作業系統，驗證用之減值主金鑰組應由送測單位提供。如此，於驗證環境中將不會牽涉任何保密問題，而送測之卡片也因是使用驗證用之測試主金鑰組所產製，將不會與票證業者實際環境或測試環境中使用之卡片混淆而導致安全上之漏洞。此外，因驗證用主金鑰組乃是由送測單位自行提供，而送測單位可遵循其原有製卡流程產製出可供驗證用之卡片，而不需進行發卡系統的任何修改。有關驗證用之減值主金鑰組(key set)電文檔的格式及範例請參考附錄 6。

2. 票卡

送測單位於送測前需準備各式票種三套，其票種名稱及定義需符合交三版之定義，其交三版之編碼格式定義如下：

0x00：一般民眾

0x01：老人(>70 歲)

0x02：老人(65-70 歲)

0x03：殘障(愛心)

0x04：陪伴

0x05：學生

0x06：軍人

0x07：警察

0x08：兒童

送測單位所提供之三套送測卡片，皆須由驗證用減值主金鑰組依照各業者統一定義之交三版金鑰衍生規範所衍生之個別卡片金鑰所加密。因此驗證系統可於輸入送測單位所提供之驗證用減值主金鑰組後，存取該張卡片之減值相關扇區。此外，送測卡片中每張卡片至少需存入5000 元的『虛擬』電子票值，以供驗證流程進行各種減值測試，且若於測試中電子票值減扣完畢，則送測單位需再針對送測卡片進行儲值動作。

此一作法之主要目的，不僅因為交三版之驗證乃是著重於減值設備之交易流程處理，處理加值相關之流程事宜則是由各家票證業者自行規範，且交三版定義之減值金鑰組並不包含任何足以加值之相關金鑰，因此驗證系統中也無法幫送測單位進行送測卡片之加值動作。

3. 減值設備或查詢設備

送測單位若欲對其減值設備或查詢設備進行驗證，則須備妥相關之減值或查詢設備，且該減值或查詢設備必須可以對送測卡片進行減值或查詢，亦即，該減值或查詢設備必須內含驗證用之減值主金鑰組以及各業者統一定義出之交三版金鑰衍生規範。

二、申請

送測單位需填寫「交三版卡片/設備驗證申請書」，送交驗測單位後進行驗證程序安排及相關作業。交三版驗證申請書請參考附錄 7。

三、驗證

驗證單位於接受送測單位之申請後，依據驗證項目進行卡片或減值/查詢設備之驗證作業。

四、結果

驗證完成後，驗證單位將對於送測單位所提供之卡片以及減值/查詢設備出具驗證報告。驗證報告中將包含送測卡片及送測減值/查詢設備之是否相容於交三版定義之安全性/各規定欄位及交互檢測結果進行說明。若有不相容或有疑義之地方，送測單位可依據驗證報告進行修改後再次送至驗證單位進行再次驗證。

4.1.2 驗證系統架構規劃

交三版驗證系統架構是整個驗證機制規劃的骨幹，有了明確且完整的驗證系統，不僅可使整個驗證流程易於執行，也得以讓各送測單位信任其系統之公正性。整個驗證系統包含標準非接觸式 IC 卡、標準非接觸式讀卡機、驗證系統程式、標準接觸式讀卡機、接觸式 IC 卡等設備。除此之外，驗證系統也包含送測單位所提供之受檢卡片以及受檢減值/查詢設備等。驗證系統架構如圖 4.2，以下分項說明各項設備之功能用途。

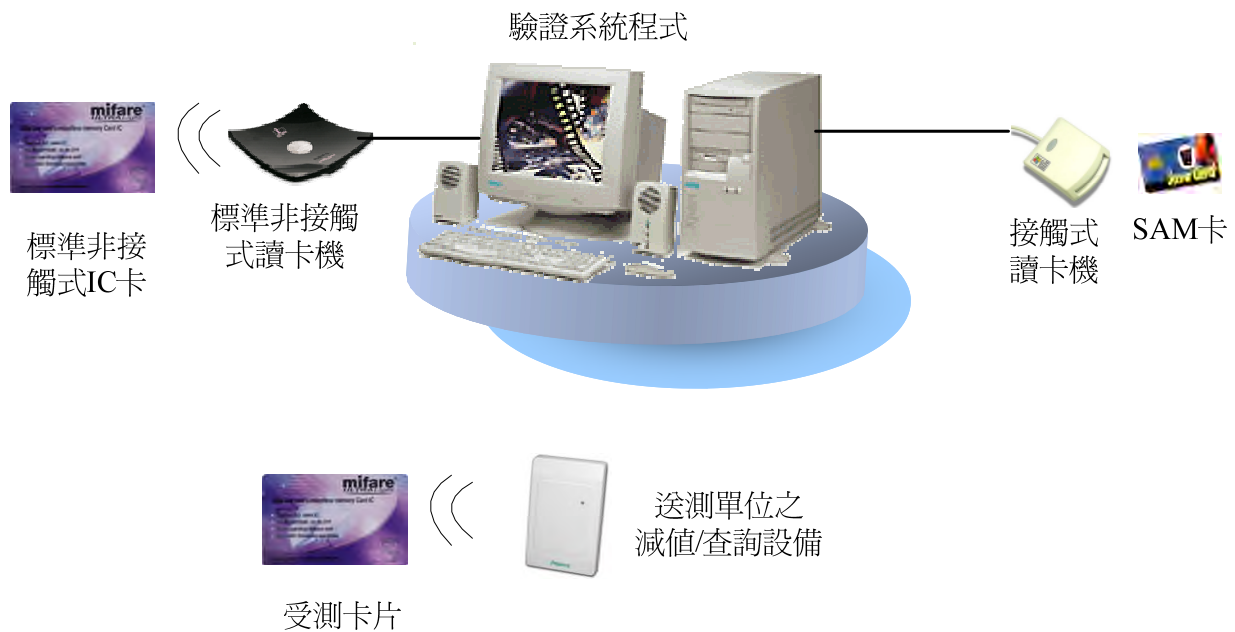


圖 4-2 交三版驗證系統架構

一、標準非接觸式 IC 卡

標準非接觸式 IC 卡之使用時機係在於卡片動態資料驗證時，用以檢測各送測單位之減值/查詢設備對於非屬送測單位之標準交三版卡片之操作行為測試。此卡片由驗測單位提供，並依據送測單位檢附之驗證用減值主金鑰組進行製卡而成。

本計畫使用飛利浦公司發行之 Mifare 1K 卡片來作為驗證系統中之標準非接觸式 IC 卡，主要因為為此種卡片亦為各票證公司現行發行之卡片類別，符合運行中大多數系統之卡片規格。

二、標準非接觸式讀卡機

標準非接觸式讀卡機乃是使用於卡片靜態及動態資料驗證時，用以讀

取/寫入送測卡片以及標準非接觸式 IC 卡之各扇區資料。

為力求能提供公正的檢驗，建議使用飛利浦公司所生產的標準讀卡模組，如此將不需牽涉各票證公司讀卡設備之差異性，且可令各受測業者信服驗證系統所產製出來之結果。

因此本驗證系統之非接觸式讀卡設備為飛利浦公司所出產之標準 Mifare Pegoda 讀卡機。

三、驗證系統程式

驗證系統程式分為兩大類別，其一為卡片靜態資料顯示列印程式，另一類則為卡片動態資料驗證程式，卡片靜態資料顯示列印程式之目的在於檢查卡片資料之內容是否符合交三版之格式定義，包含欄位編碼方式、資料型態及金鑰存取權限檢查等。卡片動態資料驗證即為跨系統交易交叉測試，驗證目的為測試票證公司送測之受測卡片及受測設備能符合交三版定義之交易流程，達到跨系統使用之目的。

1. 卡片靜態資料顯示列印程式

卡片靜態資料顯示列印程式之功能包含下列幾個模組：

(1) 各送測單位之驗證用減值主金鑰匯入 SAM 卡模組

輸入送測單位提供之減值主金鑰組，並透過標準接觸式讀卡機將金鑰資料置放至 SAM 卡中。

(2) 卡片資料讀取模組

驅動標準非接觸式讀卡機讀取卡片序號，並送至 SAM 卡中產生衍生金鑰，並據此讀取送測卡片或標準非接觸式 IC 卡中相關於減值交易所需使用之各扇區資料。

(3) 金鑰存取測試模組

依據送測單位提供之減值主金鑰組，逐一檢測各扇區讀取權限，以供進行卡片安全機制驗證。

(4) 交三版欄位定義解譯模組

讀取各扇區資料後，解譯交三版所定義之各欄位資料，並顯示於介面中，必要時可列印出各欄位資料詳細內容。當解譯交三版定義之各扇區欄位資料時，若發生無法解譯之狀況，則表示該欄位不

相容於交三版之定義，因此該欄位將被標記為”不相容”。據此，將可產出交三版靜態資料驗證報告，於驗測完畢後，交付各送測單位進行修正。

2. 卡片動態資料驗證程式

卡片動態資料驗證程式之功能包含下列幾個模組：

(1) 標準非接觸式 IC 卡之製作模組

依據各送測單位提供之驗證用減值主金鑰組及驗證系統預設之加值主金鑰組製作檢測用之標準非接觸式 IC 卡片。

(2) 開放型減值交易產生模組

可針對送測卡片或標準非接觸式 IC 卡片進行開放型減值交易之扣款，並依據交三版定義之欄位格式進行卡片資料寫入。

(3) 異機進出連續型封閉交易產生模組

可針對送測卡片或標準非接觸式 IC 卡片進行異機進出連續型封閉交易之扣款，並依據交三版定義之欄位格式進行卡片資料寫入。

(4) 同機進出連續型封閉交易產生模組

可針對送測卡片或標準非接觸式 IC 卡片進行同機進出連續型封閉交易之扣款，並依據交三版定義之欄位格式進行卡片資料寫入。

(5) 非連續型封閉交易產生模組

可針對送測卡片或標準非接觸式 IC 卡片進行非連續型封閉交易之扣款，並依據交三版定義之欄位格式進行卡片資料寫入。

四、標準接觸式讀卡機

標準接觸式讀卡機乃是用於放置安全模組卡，以供驗證系統程式與置放於安全模組卡中之程式交談，據以產生對應的衍生金鑰。讀卡機模組建議符合現行業界通用之 PC/SC(Personal Computer/Smart Card)規格，此規格為國際資訊大廠提出之讀卡機驅動規範，遵循此規範才能讓安全模組卡與讀卡機與驗證系統程式相容運作。

五、安全模組卡(SAM 卡)

安全模組卡中將放置依據各業者統一定義出之交三版金鑰衍生規範所製作成之金鑰衍生程序(須待各業者定義出統一之金鑰衍生規範後才可進行此程序開發)。此一程序將可安全地儲存送測單位所提供之驗證用減值主金鑰組，並依據每張卡片之卡片序號以及相關資料產生各張卡片之衍生金鑰(其實際所需之資料內容須待各業者統一定義出金鑰衍生規範後才得以確認)。

六、送測單位之減值/查詢設備

送測單位驗票設備依照各單位的需求可包含各種減值設備或查詢設備，這些設備應已具備讀取或處理交三版卡片之能力，並依照交三版建議之交易流程進行卡片讀寫之處理(可依照各業者實際應用上之需求，增加交三版建議交易流程，但不應少於交三版建議之內容)。因使用之送測卡片使用驗證用之減值主金鑰，因此送測單位所提供之送測設備必須可以處理送測卡片之交易處理。

4.1.3 驗測流程設計

驗測流程設計包含四個步驟：清點交付設備及文件、安全機制驗證、靜態卡欄位格式檢測及卡片動態資料驗證。每一步驟完成後才能進行下一步驟，當所有程序完成後表示交付測試之卡片及設備符合交三版規劃定義之規範，圖 4-3 為驗測流程設計之主要程序。

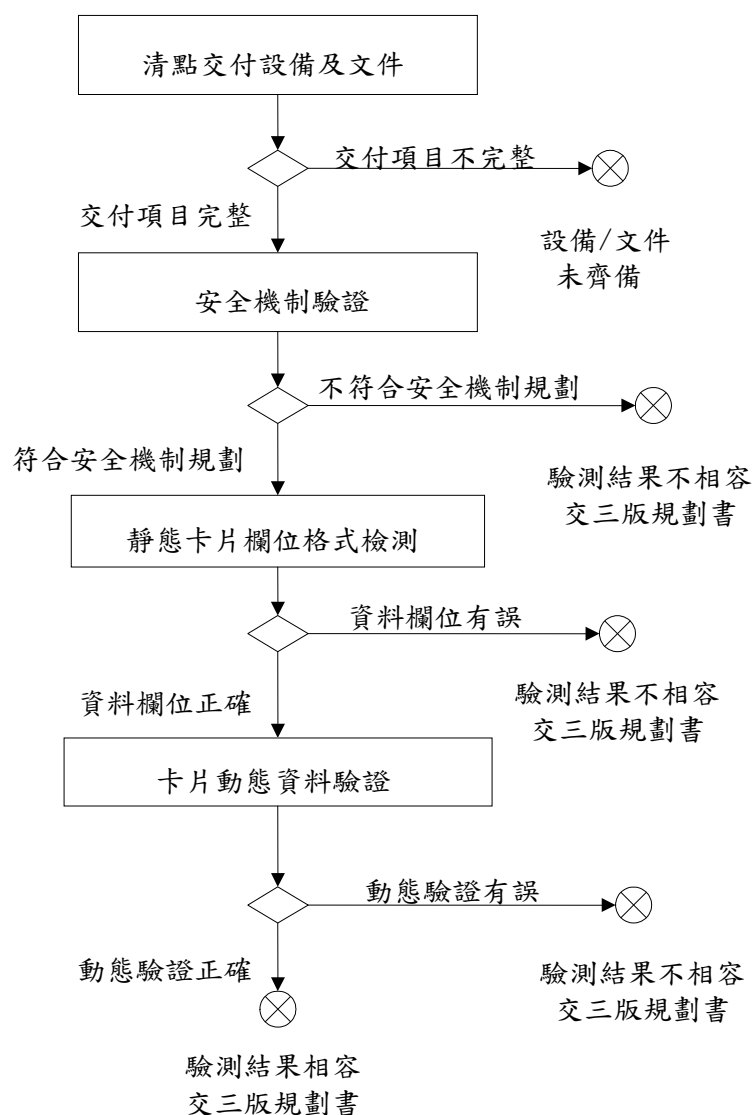


圖 4-3 驗測流程設計之主要程序

一、清点交付設備及文件

送測單位依據申請程序填寫申請表及交付驗測卡片及設備，所有項目(包含文件)待詳細點交及確認後，即可進行安全機制驗證步驟。

二、安全機制驗證

安全機制驗證主要在驗測卡片讀取及寫入時安全機制是否符合交三版規劃書之規範，使卡片在跨系統使用時能正確被應用系統使用，在安全的狀況下進行交易之減值扣款。

此安全機制驗證包含下列兩大部份：

1. 減值主金鑰組匯入作業驗測

送測單位需提供減值主金鑰組電文檔，由驗證單位提供之驗證系統程式讀入後，將主金鑰值置入 SAM 卡中，驗證系統程式將檢查電文檔內容是否提供足夠之主金鑰數量及金鑰型態，故電文檔中至少需供下列表格之資料：

資料類別		使用扇區位置	金鑰種類	金鑰值
目錄服務區		0	A	送測單位提供
共同資料區	卡片管理	1	A	送測單位提供
	電子票值	2	A	送測單位提供
	共用資料	3	B	送測單位提供
		4	B	送測單位提供
		5	B	送測單位提供
交三版應用資料區	連續型封閉交易系統	9	B	送測單位提供
		10	B	送測單位提供
	非連續型封閉交易系統	11	B	送測單位提供

註：在卡片規範中，至少需包含 16 個扇區，每一個扇區皆使用不同的金鑰保護，而且每一扇區皆包含兩把金鑰，分別為 Key A 及 Key B，在一般票證系統規劃中，Key A 的權限為讀取，Key B 的權限為讀取/寫入，做為票卡之安全控管機制之基礎。

驗證系統程式讀入電文檔後，依序檢查下列條件：

- (1) 電文檔格式(包含 Header, Data, Trailer 格式檢查)
- (2) 金鑰個數檢查
- (3) 扇區位置(編號)正確性檢查
- (4) 扇區對應之金鑰種類檢查(Key A 或 Key B)

上述檢查條件需全部合格即表示驗證系統程式可正確匯入電文檔，即符合交三版規劃書之規範。

2. 卡片讀取權限驗測

依據交三版金鑰管理規範並完成電文檔匯入作業，SAM 卡可使用主金鑰值、各票證公司認可之演算法則及卡號，進行單張卡片之多樣化處理程序並取得卡片金鑰值，來進行卡片讀取權限驗測作業。測試方式

為使用金鑰存取測試模組進行檢測，預期結果如下表 4-1：

表 4-1 使用金鑰存取測試模組進行檢測預期結果表

扇區位置	讀取	減值	寫入	加值
0	成功	失敗	失敗	失敗
1	成功	失敗	失敗	失敗
2	成功	成功	失敗	失敗
3	成功	失敗	成功	失敗
4	成功	失敗	成功	失敗
5	成功	失敗	成功	失敗
9	成功	失敗	成功	失敗
10	成功	失敗	成功	失敗
11	成功	失敗	成功	失敗

此項卡片讀取權限驗測係指所有多樣化之金鑰值皆需能依存取權限讀寫卡片，即符合交三版規劃書之規範。

三、靜態卡片欄位格式檢測

此項目之檢測範圍為確認送測單位送交之卡片內容符合交三版規格書之規範，檢測內容包含卡片內各欄位之型態及資料。

1. 卡片製卡完成後初始化資料檢查

(1) 目錄服務區(S0B1~B2)

交三版新增三版應用資料區 AID，說明如下：

應用系統名稱	交易系統編號	扇區編號
交三版異機進出連續型封閉交易系統	0xF1	0x09
交三版同機進出連續型封閉交易系統	0xF2	0x0A
交三版非連續型封閉交易系統	0xF3	0x0B

驗證系統程式檢查此三種交易系統編碼是否記錄於卡片的目錄服務區中。

(2) 發行管理資料(S1B0)

序號	資料項目	必要項目	預期結果
1	發卡單位編碼	Y	需符合交三版編碼準則
2	發卡設備編碼		
3	發行批號		
4	發行日期	Y	
5	有效日期	Y	
6	卡片規格版本	Y	0x3X

7	卡片狀態	Y	0x01
8	檢查碼		

(3) 票值管理資料(S1B1)

序號	資料項目	必要項目	預期結果
1	自動加值設定		
2	自動加值票值數額		
3	儲存最大票值數額		
4	每筆可扣減最大票值數額		
5	自動加值銀行代碼		
6	基本身分別	Y	0x00 – 0x08
7	基本身分區碼	Y	需符合交三版編碼準則
8	優惠補助身分別		
9	優惠補助身分有效日		
10	優惠補助最大次數		
11	檢查碼		

(4) 電子票值資料(S2B0~B1)

序號	資料項目	必要項目	預期結果
1	主要票值	Y	需符合數值資料格式
2	備份票值	Y	需符合數值資料格式

2. 共用資料區資料檢查

(1) 卡片交易狀態資料(S3B0)

序號	資料項目	必要項目	預期結果
1	卡片交易序號	Y	每次交易完成後加一
2	交易記錄檔指標	Y	0x00 – 0x05
3	優惠積點數		
4	優惠積點交易序號		
5	鎖卡旗標	Y	0x01 或 0x02
6	每日優惠累計轉乘點數		
7	轉乘優惠日期		
8	特殊身分優惠累計次數		
9	加值累計點數		

(2) 最近兩筆交易記錄(S3B1~B2)

序號	資料項目	必要項目	預期結果
1	交易序號	Y	為 S3B0 卡片交易序號之 LSB
2	交易時間		
3	交易類別	Y	需符合交三版編碼準則
4	交易票值/票點		
5	交易後票值/票點		
6	交易系統編碼	Y	需符合交三版編碼準則
7	交易地點/RSU 編碼/ 交易票價站		
8	交易機器/OBU 編碼/ 轉乘優惠指標		

(3) 最近六筆交易記錄(S4B0~B2, S5B0~B2)

序號	資料項目	必要項目	預期結果
1	交易序號	Y	為 S3B0 卡片交易序號之 LSB
2	交易時間		
3	交易類別	Y	需符合交三版編碼準則
4	交易票值/票點		
5	交易後票值/票點		
6	交易系統編碼	Y	需符合交三版編碼準則
7	交易地點/RSU 編碼/ 交易票價站		
8	交易機器/OBU 編碼/ 轉乘優惠指標		

3. 異機進出連續型封閉交易系統應用資料區

(1) 定期票卡管理資料(S9B0)

序號	資料項目	必要項目	預期結果
1	發卡單位編碼	Y	需符合交三版編碼準則
2	交易系統編碼/ 發行單位代碼	Y	需符合交三版編碼準則
3	票卡種類	Y	0x1X：定期票
4	有效起始日		
5	有效到期日		
6	進出站代碼 1		
7	進出站代碼 2		
8	最大可使用次數		
9	售出票價		
10	保留		

(2) 異機進出連續型封閉交易系統最近兩筆交易記錄(S9B1~B2)

序號	資料項目	必要項目	預期結果
1	已使用次數		
2	首次交易日期		
3	交易系統編碼	Y	需符合交三版編碼準則
4	交易單位代碼		
5	交易類別	Y	需符合交三版編碼準則
6	進出站代碼		
7	交易時間		
8	交易機器流水號/ OBU 編碼		
9	實扣交易票值 (預收/尾款)		

4. 同機進出連續型封閉交易系統應用資料區

(1) 定期票票卡管理資料(S10B0)

序號	資料項目	必要項目	預期結果
1	發卡單位編碼	Y	需符合交三版編碼準則
2	交易系統編碼/ 發行單位代碼	Y	需符合交三版編碼準則
3	票卡種類	Y	0x1X：定期票
4	有效起始日		
5	有效到期日		
6	進出站代碼 1		
7	進出站代碼 2		
8	最大可使用次數		
9	可用路線/路線群組代碼		
10	售出票價		

(2) 同機進出連續型封閉交易系統最近兩筆交易記錄(S10B1~B2)

序號	資料項目	必要項目	預期結果
1	已使用次數		
2	首次交易日期		
3	交易系統編碼	Y	需符合交三版編碼準則
4	交易單位代碼		
5	交易類別	Y	需符合交三版編碼準則
6	上/下站序號		
7	交易時間		
8	路線代碼		
9	交易機器流水號/		

	OBV 編碼		
10	實扣交易票值 (預收/尾款)		

5. 非連續型封閉交易系統應用資料區

(1) 定期票卡管理資料(S11B0)

序號	資料項目	必要項目	預期結果
1	交易系統編碼 A	Y	需符合交三版編碼準則
2	發行單位代碼 A		
3	票卡種類+延伸使用碼 A		
4	有效起始日 A		
5	有效到期日 A		
6	可使用之場站/ 場站群組代碼 A		
7	交易系統編碼 B	Y	需符合交三版編碼準則
8	發行單位代碼 B		
9	票卡種類+延伸使用碼 B		
10	有效起始日 B		
11	有效到期日 B		
12	可使用之場站/ 場站群組代碼 B		

註：A、B 代表不同的發行單位區塊

(2) 非連續型封閉交易系統最近兩筆交易記錄(S11B1~B2)

序號	資料項目	必要項目	預期結果
1	P1：交易系統編碼	Y	需符合交三版編碼準則
2	P1：交易單位代碼		
3	P1：交易類別	Y	需符合交三版編碼準則
4	P1：交易時間		
5	P1：場站代碼		
6	P2：交易系統編碼	Y	需符合交三版編碼準則
7	P2：交易單位代碼		
8	P2：交易類別	Y	需符合交三版編碼準則
9	P2：交易時間		
10	P2：場站代碼		

註：P1、P2 代表兩個不同的交易地點。

驗證系統程式待搜尋到卡片後，先完成安全機制驗證，並讀取卡片中需要檢查之扇區資料，最後將欄位資料顯示於畫面中，並提供報表列印之功能，使驗證單位及送測單位能充份了解驗證狀況。

四、卡片動態資料驗證

卡片動態資料驗證即為跨系統交易交叉測試，故此驗證程序需包含交三版定義的四種交易型態：開放交易系統、非連續型封閉交易、異機進出連續型封閉交易系統、同機進出連續型封閉交易系統，此四種交易型態在卡片中使用不同的扇區儲存交易資料，故此部份的驗證即在檢核在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。為確認跨系統交易或驗票設備間是否正確，需使用靜態卡片欄位格式檢測功能進行資料內容驗證，使驗證能有效進行。

依照交三版定義之基本票種及基本減值流程功能，卡片動態資料驗證需包含各種不同載具間的相互搭乘，表 4-2 表示載具間可能發生之搭乘行為(表格中搭乘運具為舉例說明，例如高速公路 ETC 系統即歸類為開放型交易系統)：

表 4-2 不同載具間相互搭乘可能發生之搭乘行為

	開放型交易	非連續型封閉交易	異機進出連續型封閉交易	同機進出連續型封閉交易
開放型交易	段次公車→ 段次公車	段次公車→ 停車場	段次公車→ 捷運	段次公車→ 里程公車
非連續型封閉交易	停車場→ 段次公車	停車場→ 停車場	停車場→捷運	停車場→ 里程公車
異機進出連續型封閉交易	捷運→ 段次公車	捷運→ 停車場	捷運→捷運	捷運→ 里程公車
同機進出連續型封閉交易	里程公車→ 段次公車	里程公車→ 停車場	里程公車→ 捷運	里程公車→ 里程公車

1. 開放型交易動態資料驗證

開放型交易系指一次扣款行為，直接由主要票值欄位中扣除，無應用欄位之規劃，故此型態之交易僅需在交易完成後將交易記錄寫入共同資料區中，做為交易查詢或下筆交易進行之參考。

區塊位置	資料項目	驗測項目	前次交易卡片記錄	本次交易完成後卡片寫入記錄
S3B0	卡片交易序號	Y	0x6400	0x6500
	交易記錄檔指標	Y	0x01	0x02(表示該次記錄於 S4B1)
	優惠積點數			
	優惠積點交易序號			

區塊位置	資料項目	驗測項目	前次交易 卡片記錄	本次交易完成後卡片寫入記錄
	鎖卡旗標	Y	0x01	0x01(表卡片狀態正常)
	每日優惠累計轉乘點數			
	轉乘優惠日期			
	特殊身分優惠累計次數			
	加值累計點數			
S4B1	交易序號	Y		0x65
	交易時間	Y		驗票設備之系統時間
	交易類別	Y		需符合交三版編碼準則
	交易票值/票點	Y		本次交易票值/票點
	交易後票值/票點	Y		交易後票值/票點
	交易系統編碼	Y		需符合交三版編碼準則
	交易地點/RSU 編碼/ 交易票價站	Y		驗票設備之 RSU 碼
	交易機器/OBU 編碼/ 轉乘優惠指標	Y		驗票設備之交易機器碼

2. 非連續型封閉交易動態資料驗證

非連續型封閉交易應用於停車場時交易不連續之設備，除共用資料區之外，需將交易資料記錄於 Sector 11 中，做為進站/出站之交易判斷之用。

區塊位置	資料項目	驗測項目	前次交易 卡片記錄	本次交易完成後卡片寫入記錄
S3B0	卡片交易序號	Y	0x6400	0x6500
	交易記錄檔指標	Y	0x01	0x02(表示該次記錄於 S4B1)
	優惠積點數			
	優惠積點交易序號			
	鎖卡旗標	Y	0x01	0x01(表卡片狀態正常)
	每日優惠累計轉乘點數			
	轉乘優惠日期			
	特殊身分優惠累計次數			
	加值累計點數			
S4B1	交易序號	Y		0x65
	交易時間	Y		驗票設備之系統時間
	交易類別	Y		需符合交三版編碼準則
	交易票值/票點	Y		本次交易票值/票點
	交易後票值/票點	Y		交易後票值/票點
	交易系統編碼	Y		需符合交三版編碼準則
	交易地點/RSU 編碼/ 交易票價站	Y		驗票設備之 RSU 碼

區塊位置	資料項目	驗測項目	前次交易 卡片記錄	本次交易完成後卡片寫入記錄
	交易機器/OBU 編碼/ 轉乘優惠指標	Y		驗票設備之交易機器碼
S11B1 或 S11B2	P1：交易系統編碼	Y		需符合交三版編碼準則
	P1：交易單位代碼			
	P1：交易類別	Y		需符合交三版編碼準則
	P1：交易時間	Y		驗票設備之系統時間
	P1：場站代碼	Y		驗票設備之場站代碼
	P2：交易系統編碼			
	P2：交易單位代碼			
	P2：交易類別			
	P2：交易時間			
	P2：場站代碼			

3. 異機進出連續型封閉交易系統動態資料驗證

異機進出連續型封閉交易系統應用於捷運等運具設備，除共用資料區之外，需將交易資料記錄於 Sector 9 中，做為進站/出站之交易判斷之用。

區塊位置	資料項目	驗測項目	前次交易 卡片記錄	本次交易完成後卡片寫入記錄
S3B0	卡片交易序號	Y	0x6400	0x6500
	交易記錄檔指標	Y	0x01	0x02(表示該次記錄於 S4B1)
	優惠積點數			
	優惠積點交易序號			
	鎖卡旗標	Y	0x01	0x01(表卡片狀態正常)
	每日優惠累計轉乘點數			
	轉乘優惠日期			
	特殊身分優惠累計次數			
	加值累計點數			
S4B1	交易序號	Y		0x65
	交易時間	Y		驗票設備之系統時間
	交易類別	Y		需符合交三版編碼準則
	交易票值/票點	Y		本次交易票值/票點
	交易後票值/票點	Y		交易後票值/票點
	交易系統編碼	Y		需符合交三版編碼準則
	交易地點/RSU 編碼/ 交易票價站	Y		驗票設備之 RSU 碼
	交易機器/OBU 編碼/ 轉乘優惠指標	Y		驗票設備之交易機器碼
S9B1	已使用次數			

區塊位置	資料項目	驗測項目	前次交易卡片記錄	本次交易完成後卡片寫入記錄
或 S9B2	首次交易日期			
	交易系統編碼	Y		需符合交三版編碼準則
	交易單位代碼			
	交易類別	Y		需符合交三版編碼準則
	進出站代碼	Y		驗票機之站點代碼
	交易時間	Y		驗票設備之系統時間
	交易機器流水號/ OBU 編碼	Y		驗票機編號
	實扣交易票值 (預收/尾款)	Y		本次交易之實扣金額

4. 同機進出連續型封閉交易系統動態資料驗證

同機進出連續型封閉交易系統應用於公車等設備，除共用資料區之外，需將交易資料記錄於 Sector 10 中，做為上車或下車之交易判斷之用。

區塊位置	資料項目	驗測項目	前次交易卡片記錄	本次交易完成後卡片寫入記錄
S3B0	卡片交易序號	Y	0x6400	0x6500
	交易記錄檔指標	Y	0x01	0x02(表示該次記錄於 S4B1)
	優惠積點數			
	優惠積點交易序號			
	鎖卡旗標	Y	0x01	0x01(表卡片狀態正常)
	每日優惠累計轉乘點數			
	轉乘優惠日期			
	特殊身分優惠累計次數			
	加值累計點數			
S4B1	交易序號	Y		0x65
	交易時間	Y		驗票設備之系統時間
	交易類別	Y		需符合交三版編碼準則
	交易票值/票點	Y		本次交易票值/票點
	交易後票值/票點	Y		交易後票值/票點
	交易系統編碼	Y		需符合交三版編碼準則
	交易地點/RSU 編碼/ 交易票價站	Y		驗票設備之 RSU 碼
	交易機器/OBU 編碼/ 轉乘優惠指標	Y		驗票設備之交易機器碼
S10B1 或 S10B2	已使用次數			
	首次交易日期			
	交易系統編碼	Y		需符合交三版編碼準則

區塊位置	資料項目	驗測項目	前次交易卡片記錄	本次交易完成後卡片寫入記錄
	交易單位代碼			
	交易類別	Y		需符合交三版編碼準則
	上/下站序號	Y		站點代號
	交易時間	Y		驗票設備之系統時間
	路線代碼	Y		本次交易路編代碼
	交易機器流水號/ OBU 編碼	Y		驗票機編號
	實扣交易票值 (預收/尾款)	Y		本次交易之實扣金額

卡片動態資料驗證作業中，為使交易流程的各個環節於票證業者的減值設備中正確的被製作進去，必須編撰大量的測試驗證案例來配合整個驗證程序。而驗證程序中將包含這些測試案例的執行。

驗測案例之編撰將參考本章節之驗證機制規劃內容，其主要內容將包含：

1. 一般交易案例：包含封閉式及非封閉式交易的各種票卡案例。
2. 交易查詢案例：包含一般業者查詢時需能顯示出來的所有交易案例。
3. 交易例外案例：包含所有故意導致的錯誤狀況，用以觀察業者提供的減值設備的例外處理能力。

4.2 第一階段卡片靜態資料驗證結果

靜態驗證程式主要功能為讀取卡片資料進行欄位資料檢查，目的為檢查資料是否符合交三版規劃書之定義，包含欄位型態、編碼格式等，並產生驗證結果報表，驗證結果可分為通過與不通過，做為卡片資料是否相容於交三版之依據。

一、靜態驗證程式主要功能說明

1. 主畫面：

靜態驗證程式主要分為四個部份，分別為執行步驟區、卡資資料輸入區、測試結果記錄檔區及交三版欄位解釋區等，畫面如圖 4-4 所示：

The screenshot shows a Windows-style application window titled "交三版卡片靜態資料顯示列印程式". The interface is divided into four main panes:

- 執行步驟 (Execution Steps):** Contains two steps. Step 1 is "卡片金鑰存取權限驗證" (Card Key Access Permission Verification). Step 2 is "卡片格式驗證" (Card Format Verification).
- 卡片資料 (Card Information):** Contains input fields for "公司名稱" (Company Name), "卡別" (Card Type) with a dropdown menu currently showing "一般民眾" (General Public), and "驗證次數" (Verification Count) with a dropdown menu currently showing "1".
- 測試結果記錄檔 (Test Result Log):** A list box showing a single entry: "acer_一般民眾_1.rpt".
- 交三版欄位解釋 (Jiao San Ban Field Explanation):** A large, empty text area for displaying the explanation of the Jiao San Ban fields.

圖 4-4 靜態驗證程式主畫面

2. 匯入金鑰：

選擇選單中的”匯入金鑰檔”選項，進行金鑰輸入作業。檔案格式必須符合驗證程序之要求，且金鑰組必須包含交三版規劃書所提之相關主金鑰，若不包含則會產生錯誤訊息，畫面如圖 4-5 所示。

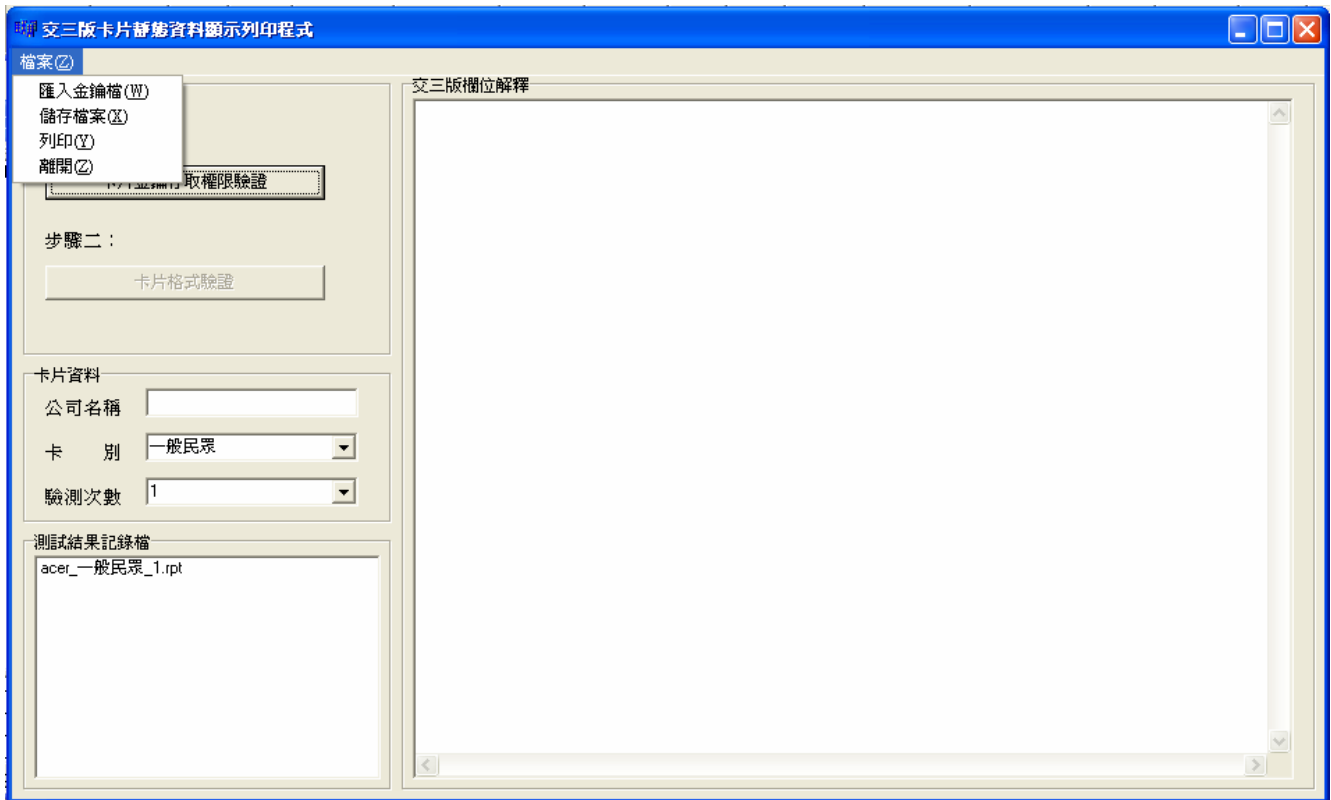


圖 4-5 靜態驗證程式匯入金鑰畫面

3. 卡片金鑰存取權限驗證：

按下主畫面中之”卡片金鑰存取權限驗證”按鍵，進行此驗證作業。金鑰存取權限作業依交三版規範之存取權限進行檢驗，畫面如圖4-6所示。

交三版卡片靜態資料顯示列印程式

檔案(F)

執行步驟

步驟一：

卡片金鑰存取權限驗證

步驟二：

卡片格式驗證

卡片資料

公司名稱：acer

卡別：一般民眾

驗證次數：1

測試結果記錄檔

acer_一般民眾_1.rpt

交三版權位解釋

驗證基本資料：

公司名稱：acer

卡別：一般民眾

驗證次數：1

驗證時間：2008/10/6 10:37:59

驗證項目：卡片金鑰存取驗證

扇區位置	金鑰種類	認證測試	讀取測試	寫入測試	驗證結果
0	A	成功	成功	失敗	通過
1	A	成功	成功	失敗	通過
2	A	成功	成功	失敗	通過
3	B	成功	成功	成功	通過
4	B	成功	成功	成功	通過
5	B	成功	成功	成功	通過
9	B	成功	成功	成功	通過
10	B	成功	成功	成功	通過
11	B	成功	成功	成功	通過

圖 4-6 靜態驗證程式金鑰存取權限驗證畫面

4. 卡片格式驗證：

按下主畫面中的”卡片格式驗證”按鍵，進行卡片格式驗證作業。卡片格式將依據交三版定義中註明必要項目的各欄位內容進行檢測，若為自行使用欄位，則不會進行研判，畫面如圖 4-7 所示。

欄位位置	欄位內容	資料項目	資料內容	驗證結果
S0	卡片序號	94C533A6		通過
B0	廠商批號	C488040047C11E3685004705		通過

欄位位置	欄位內容	資料項目	資料內容	驗證結果
S0	檢查碼	F008		通過
B1, B2	AID01	F109		通過
	AID02	F210		通過
	AID03	F311		通過
	AID04	0000		通過
	AID05	0000		通過
	AID06	0000		通過
	AID07	0000		通過
	AID08	0000		通過
	AID09	0000		通過
	AID10	0000		通過
	AID11	0000		通過
	AID12	0000		通過
	AID13	0000		通過
	AID14	0000		通過
	AID15	0000		通過

欄位位置	欄位內容	資料項目	資料內容	驗證結果
S1	發卡單位編碼	02		通過
B0	發卡設備編碼	0102		通過
	發行批號	3333		通過

圖 4-7 靜態驗證程式卡片格式驗證畫面

二、靜態驗證程式實證結果

靜態驗證程式提供儲存測試結果記錄檔功能，做為日後查詢及製作驗證報告之用，驗證證果可分為三狀態：

1. 通過：表示該欄位為交三版規劃書之必要項目，且檢測結果符合規劃書之定義。
2. 不通過：表示該欄位為交三版規劃書之必要項目，且檢測結果不符合規劃書之定義。
3. ----：表示該欄位為票證公司可自定之欄位，不做資料內容檢查。

附錄 8 為靜態驗證程式之測試記錄檔樣本，做為驗證結果之參考依據。本驗證程式完成後，利用遠通電收公司所提供的交三版規格卡片進行卡片靜態資料驗證，測試結果符合交三版草案的相關規定。

4.3 跨系統票證整合試辦計畫

為配合交通部推動我國電子票證跨系統整合政策，目前國內電子票證公司提出兩個試辦計畫，分別以交三版(草案)及前端設備整合的方式執行，詳述於以下各小節。

4.3.1 以交三版執行票證整合試辦計畫

臺灣智慧卡公司(TWSC)與遠通電收公司(FETC)的票證整合試辦計畫將採用以交三版(草案)為規格的卡片進行整合，兩家公司將各自發行符合交三版(草案)規格的卡片，協助交通部驗證交三版(草案)卡片規格及交易流程的可行性。該計畫可分為 3 個階段：

一、第 1 期試辦計畫

1. 計畫範圍

- (1) 國道高速公路電子收費
- (2) 桃竹苗公車 15 條路線以上

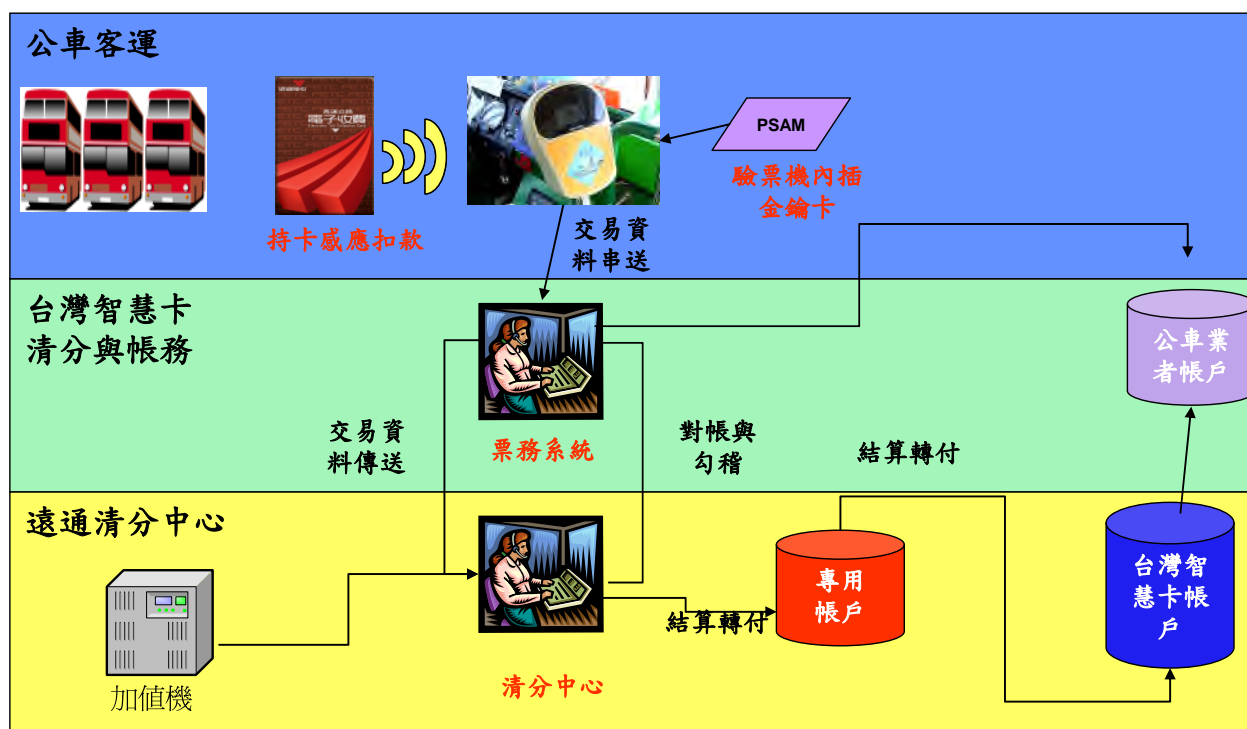
2. 測試方式

- (1) 預計總發行 500 張 -1000 張符合交三版(草案)卡片
- (2) FETC 與 TWSC 各發行 250 張-500 張卡片，彼此卡片可在對方系統扣款使用
- (3) 卡片免費，每張卡片皆有儲值，民眾可再加值使用
- (4) 新購 50 台公車驗票機，修改 200 台既有公車驗票機
- (5) 參與測試的使用者需填寫同意書，同意追蹤其使用情況，並提供測試問卷調查
- (6) 跨系統清算平台設置於遠通清分中心
- (7) FETC 與 TWSC 將匯整相關數據清分並提供相關報表
- (8) ETC 與 TWSC 依清分相關數據進行撥付款作業
- (9) FETC 與 TWSC 雙方的分工項目詳如表 4-3，系統與清分架構如圖

4-8

表 4-3 交三版卡片整合第期測試計畫分工項目

類別	遠通電收(FETC)	臺灣智慧卡(TWSC)	備註
全區卡製 Key	<ul style="list-style-type: none"> ● 提供製 Key 環境 ● 共同製交三版 Key ● 金鑰共管、共同持有 	<ul style="list-style-type: none"> ● 共同製交三版 Key ● 金鑰共管、共同持有 	● 機房設備與環境由遠通提供
製卡/發卡/售卡	<ul style="list-style-type: none"> ● 製卡/發卡 ● 門市及通路售卡 	<ul style="list-style-type: none"> ● 製卡/發卡 ● 門市及通路售卡 	
加值點	● FETC 加值點	● TWSC 加值點	
加值帳戶	● FETC 專用帳戶	● TWSC 專用帳戶	
讀卡機/ 扣款	<ul style="list-style-type: none"> ● OBU 設定 ● 車道系統更新及測試 	<ul style="list-style-type: none"> ● 桃竹苗/中彰投公車讀卡機 (SAM)更新 & 測試 	● 扣款共通
清分	● FETC 清分系統進行前置處理(大清分)	● TWSC 清分系統進行交易清分(小清分)	



公車扣款部分

ETC 扣款部分

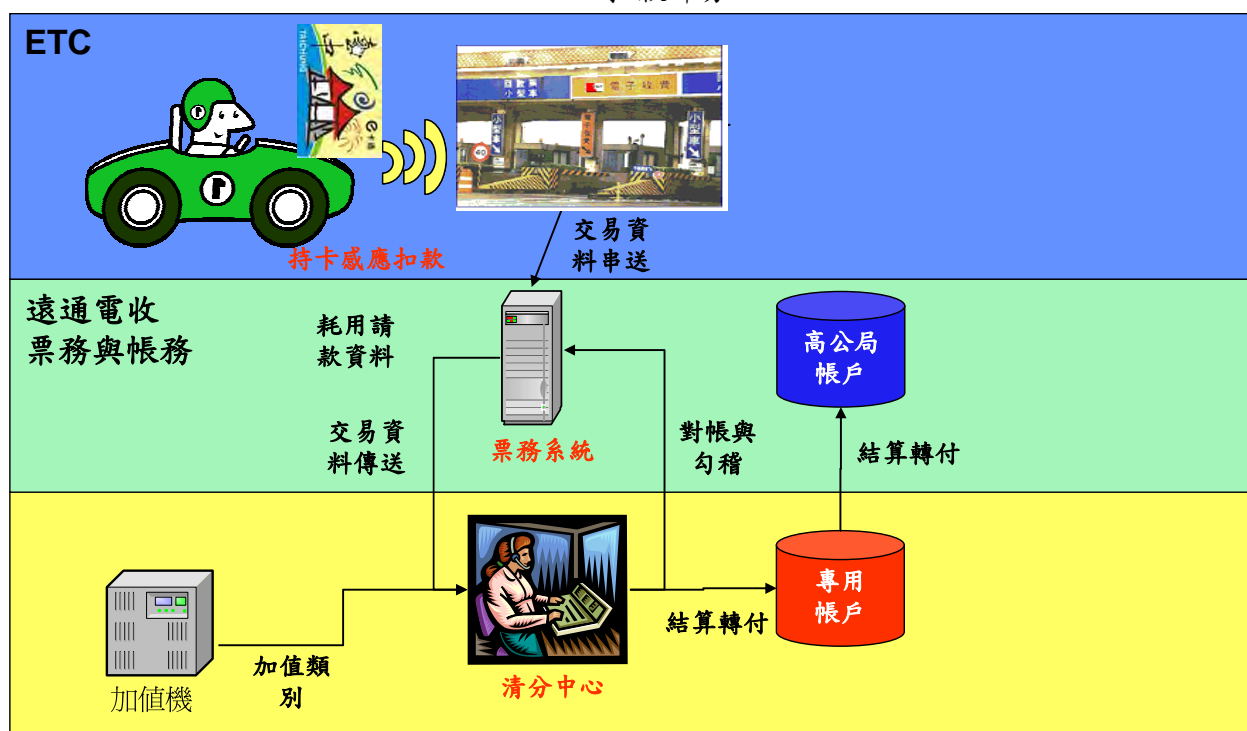


圖 4-8 交三版卡片整合系統與清分架構

3. 驗證項目

- (1) 驗證交三版卡片格式、一致的通訊協定、票卡與讀卡機介面溝通之作業規範及程序等相關機制之可行性。

(2) 配合本計畫進行「交三版靜態存取資料驗證」

- 減值主金鑰匯入 SAM 卡模組
- 卡片資料讀取模組
- 公鑰存取測試模組
- 交三版欄位定義解譯模組

遠通電收公司於 97 年 11 月初將該公司製作符合交三版規格之卡片送交本計畫團隊進行初步測試，初步測試結果並未發現異常或不符合交三版草案之處，建議未來應待本計畫驗證系統完成後，再由相關主管單位進行正式驗證工作。

(3) 驗證交三版規劃欄位可滿足同機進出連續性封閉交易系公路客運里程計費與開放型交易系統高速公路電子收費功能，如表 4-4。

表 4-4 交三版卡片整合第 1 期測試計畫驗證項目

系統類型	驗證項目
同機進出連續性封閉交易系統	公路客運里程計費、計日旅遊卡、定期學生月票 <ul style="list-style-type: none">● 上車刷卡註記上車站代號● 下車刷卡註記下車站代號● 依里程計費● 依有效日無限使用● 依有效日及里程計費
開放型交易系統	國道高速公路電子收費 <ul style="list-style-type: none">● 電子票值欄位計次扣款

二、第 2 期計畫

1. 計畫範圍

- (1) 國道高速公路電子收費
- (2) 桃竹苗公車全部路線約 633 條
- (3) 桃園私有停車場

2. 測試方式

- (1) 預計總發行 5000 張 -10000 張符合交三版(草案)卡片

- (2) FETC 與 TWSC 各發行 2500 張-5000 張卡片
- (3) 卡片付費但每張卡片皆有儲值，民眾可再加值使用
- (4) 新購 450 台公車驗票機，修改 1000 台既有公車驗票機。
- (5) FETC 與 TWSC 將匯整相關數據清分並提供相關報表
- (6) ETC 與 TWSC 依清分相關數據進行撥付款作業

3. 驗證項目

驗證交三版規劃欄位可滿足同機進出連續性封閉交易系公路客運里程計費、開放型交易系統高速公路電子收費功能及非連續型封閉交易系統，如表 4-5。

表 4-5 交三版卡片整合第 2 期計畫驗證項目

系統類型	驗證項目
同機進出連續性封閉交易系統	公路客運里程計費、計日旅遊卡、定期學生月票 <ul style="list-style-type: none"> ● 上車刷卡註記上車站代號 ● 下車刷卡註記下車站代號 ● 依里程計費 ● 依有效日無限使用 ● 依有效日及里程計費
開放型交易系統	國道高速公路電子收費 <ul style="list-style-type: none"> ● 電子票值欄位計次扣款
非連續型封閉交易系統	桃園停車場 <ul style="list-style-type: none"> ● 進站刷卡註記停車進入時間 ● 出站刷卡註記停車離開時間 ● 依使用時間計費

三、第 3 期計畫

1. 計畫範圍

- (1) 國道高速公路電子收費
- (2) 桃竹苗公車全部路線約 633 條
- (3) 桃園私有停車場
- (4) 中彰投公車路線約 364 條
- (5) 臺中停車場(大誠停車場)

2. 測試方式

- (1) 全面發行交三版卡片
- (2) 卡片購買與加值依正常程序進行
- (3) 新購 2000 台公車驗票機。
- (4) FETC 與 TWSC 將匯整相關數據清分並提供相關報表
- (5) ETC 與 TWSC 依清分相關數據進行撥付款作業

3. 驗證項目

驗證交三版規劃欄位可滿足同機進出連續性封閉交易系公路客運里程計費、開放型交易系統高速公路電子收費功能及非連續型封閉交易系統，如表 4-6。

表 4-6 交三版卡片整合第 3 期計畫驗證項目

系統類型	驗證項目
非連續型封閉交易系統	臺中停車場 ● 進站刷卡註記停車進入時間 ● 出站刷卡註記停車離開時間 ● 依使用時間計費 ● 轉乘市區公車

4.3.2 以前端設備執行票證整合試辦計畫

高雄捷運公司自紅、橘兩線通車後，至 97 年 12 月之發卡量已達 95 萬張，有鑑於高雄與臺北兩地旅客往來頻繁，再加上高鐵快速的運輸服務，兩地電子票證的互通需求日益增加，因此悠遊卡公司計畫與高雄捷運公司合作，於臺北與高雄捷運車站公務門之驗票設備，以 SAM 卡方式進行設備整合，使悠遊卡與一卡通不需換卡即能在對方車站使用。

本試辦計畫整合範圍包括高雄捷運 37 個車站與臺北捷運 67 個車站，預定建置之驗票設備 220 組，加值設備為 200 組，本計畫合作雙方仍在洽談中，開始提供服務之時程仍未確定。

而本節所述之票證整合試辦計畫，因 97 年度交通部公路總局已無經費補助，須視 98 年度經費額度及審查結果再予核定，因此，上述計畫內容仍屬規劃階段。

第五章 電子票證跨系統整合相關配合事項研擬

5.1 跨系統整合之議題探討

目前國內已實際進入跨系統電子票證整合各項業務討論的票證組織為遠通電收公司及臺灣智慧卡公司，該二家公司並提出具體的整合試辦內容，本研究綜合國內電子票證跨系統整合所面臨的各種問題，分就政策指導、技術規範及營運面議題說明如下：

一、政策指導

檢視 2.2 節國外交通電子票證整合以及多用途交通卡發展現況可以發現，成功的案例皆有政府強力的政策指導，例如中國珠江三角洲的八達通卡、深圳通、廣洲羊城通、東莞一卡通的票證整合，中國政府提出「一卡通十城」的政策目標，並制定中國國家標準要求各票證營運組織逐年調整現有系統，以達最終整合的目的；在瀋陽市則由政府成立票證公司，直接進行多用途交通卡的建置，各項系統規範及卡片資料格式則遵照國家標準，成為中國國內城市一卡通領域之首例大規模成功使用 CPU 卡的城市，也是 CPU 卡發卡量最大的城市；曼谷捷運的電子票證整合政策，則是由政府制定共通卡相關標準，並出資成立票證公司建立清算後台及發行共通卡，以整合捷運系統的電子票證。

國內目前電子票證公司的主管機關已由交通部移轉至行政院金管會，電子票證管理條例已於 98 年 1 月 13 日三讀通過，主管機關的改變對於交通電子票證的使用範圍及存款準備金等之規定勢必會影響營運中的票證組織，致使電子票證業者原訂的整合進度產生觀望的遲延現象，本研究將持續探討本議題對後續電子票證整合的影響程度及範圍。

二、技術規範

目前中國建設部已完成交通電子票證的規範，各級地方政府所管轄的交通電子票證系統皆必須遵守國家技術規範逐年逐項修改，由小區域的整合擴大到大區域，最後達成國家一卡通的目的。以金鑰管理為例，中國建設事業 IC 卡密鑰管理系統結構圖如圖 5-1，各級地方政府的城市主密鑰卡

皆須由建設部的總控密鑰卡及部級主密鑰卡共同產生，如此各地方所電子票證系統未來整合時，在金鑰存取上便可建立共通的管道。

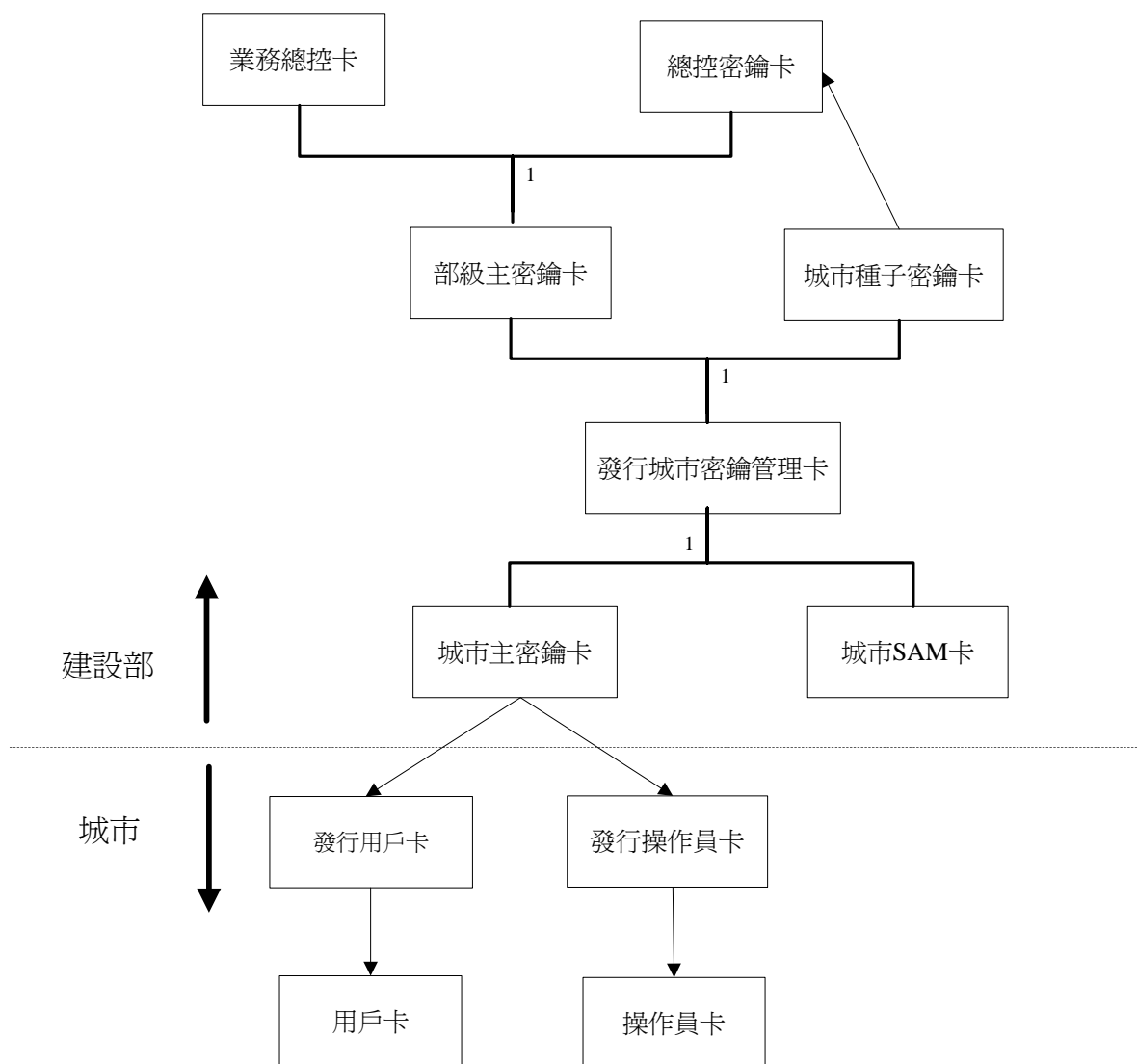


圖 5-1 中國建設事業 IC 卡密鑰管理系統結構圖

本研究已完成「交三版草案」，若公布實施之後即屬國家級的規範，但是除卡片資料格式的頒定外，尚包括金鑰管理、資料交換、資料傳輸安全等議題，以中國目前已發布的電子票證(收費)標準化文件為例，相關標準包括：

1. 電子收費專用短程通信物理層(20020249-T-348)
2. 電子收費專用短程通信數據鏈路層(20020250-T-348)
3. 電子收費專用短程通信應用層(20020251-T-348)

4. 電子收費專用短程通信設備應用規範(20020252-T-348)
5. 智能運輸系統電子收費系統框架模型(GB/T 20135-2006)

由於國內電子票證的各項標準尚未完整建立，故當多家電子票證組織進行跨系統整合時，將會面臨整合過程過度複雜的問題。例如遠通電收與臺灣智慧卡公司進行跨系統整合時，除遵照「交三版草案」的卡片資料格式外，對於金鑰管理為加速整合的進度，所採取的作法如下：

1. 遠通電收與臺灣智慧卡公司之交三版卡片交易基碼(金鑰)分獨立基碼與共管基碼。
2. 獨立基碼為發卡單位獨立擁有之基碼(如加值基碼)。
3. 共管基碼為全區共用基碼(如減值基碼)。
4. 共管金鑰為公協會管理，目前為遠通電收與臺灣智慧卡公司共管之方式，並保管於遠通電收電信安全機房。
5. 依據遠通電收之「基碼管理辦法」以及「HSM 管理辦法」等規定之作業程序，建置交易基碼。

以遠通電收與臺灣智慧卡公司的整合而言，目前的權宜作法是由兩家共管，但是當有第三家票證組織加入時，共管的複雜度及風險將大幅提高，因此，必須盡快成立共管金鑰的公協會組織。

三、營運面

以目前遠通電收與臺灣智慧卡公司的整合過程所衍生的相關議題包括：客戶服務流程、對帳作業流程、金流作業流程、營運管理資料流程、共同行銷、利益分配等。但營運面的部份議題會隨著各家的經營條件以及相對規模等因素而有所差異，且其中涉及部份的業務機密以及智慧財產權的認定，故此部份應為個案探討的範圍，由各家票證業者於實際進行整合時再具體研議。

5.2 成立「電子票證跨系統清算交換中心」之探討

未來國內各電子票證系統採用交三版卡片進行整合後，有關跨系統交易之清算主要有兩種方式進行：一種為建立統一清算交換中心進行清算，架構圖如 5-2；另一種為系統分別各自清算，架構圖如圖 5-3。

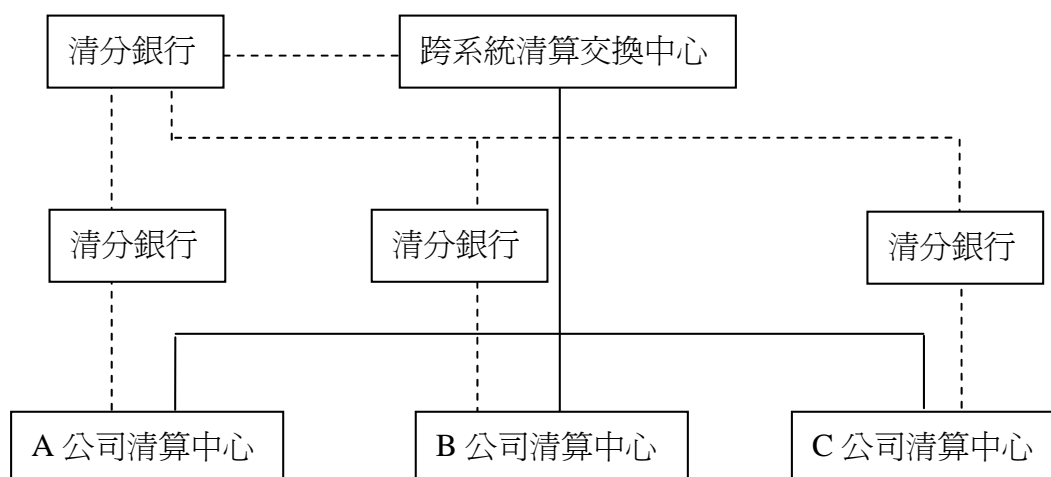


圖 5-2 統一清算交換中心進行清算架構圖

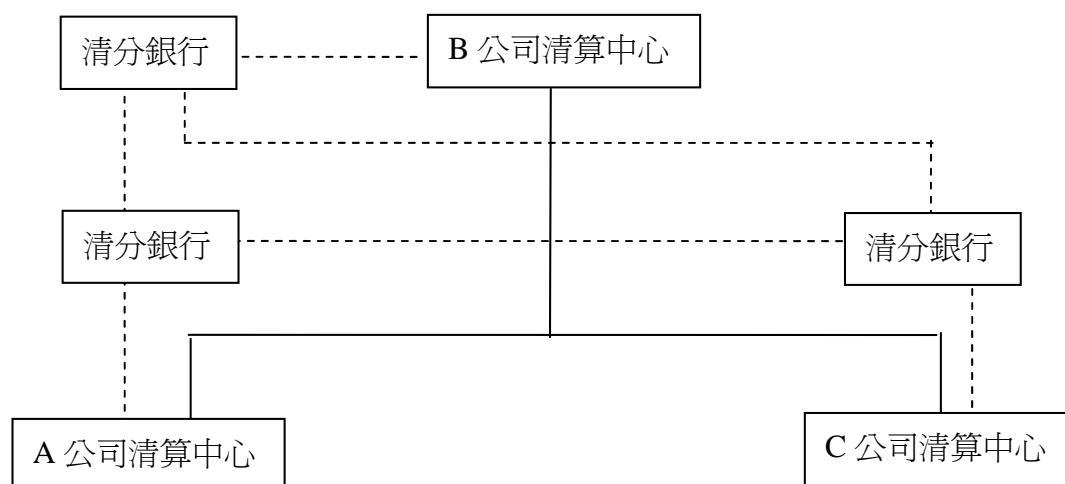


圖 5-3 系統分別各自進行清算架構圖

統一清算的方式對於現有各家票證營運組織之系統修改程度比分別各自清算低很多，因此建議成立「電子票證跨系統清算交換中心」，串接各家票證業者之後台清算系統，以進行每日交易交換及結算作業，並提供交三版共同減值金鑰組之金鑰管理作業，以及協助各票證組織發行交三版共同減值 SAM 卡。

「電子票證跨系統清算交換中心」為國內票證整合是否能夠實踐之重要關鍵，該中心之長遠發展，應由國內交通電子票證產業共同成立與監管，因為依照國內已營運的電子票證組織建置清算後台的經驗，建置單一的清算後台所需時間至少 9 個月以上，若是建置跨系統的清算後台所需時間至少 12 個月以上。建置跨系統的清算後台之工作流程大致分為以下三個階段：

第一階段：針對目前營運中票證相關系統進行了解，並進行需求訪談。

第二階段：完成需求分析與系統整合分析、系統分析(SA)與系統設計(SD)文件、系統軟體開發。

第三階段：完成各系統之功能驗證測試。

建置規劃參考時程如圖 5-4。

	工作項目 \ 工作週		1	2	3	4	5	6	...	10	17	28	...	41	48	時間 預估	備註
第一階段	系統現況分析																					6週	
	需求訪談																					10週	
第二階段	需求分析與系統整合分析																					15週	
	系統 SA 與 SD																					25週	
	系統軟體開發																					35週	
第三階段	系統功能驗證測試																					8週	
	商業運轉開始																					0週	

圖 5-4 電子票證跨系統清算交換中心建置參考時程

長期而言，「電子票證跨系統清算交換中心」將為一獨立於各家交通電子票證公司之機構，但是在短期內本計畫建議由目前已具有票證清算能力之公司(如悠遊卡公司、遠通電收公司等)取得同業共識後，以擴充現有設備代管之方式進行，如此可降低初期的建置經費與時程，並於獨立的「電子票證跨系統清算交換中心」成立之後，將營運資料及業務依照事前規劃的方式予以移轉。

短期內若國內各交通電子票證公司仍無法達成共識，建議未來臺鐵局於建置電子票證系統時可依照政府採購法及「電子票證發行管理條例」相關規定，將臺鐵局電子票證建置與管理專案計畫委由專業廠商承攬，並將「電子票證跨系統清算中心」納入委託服務範圍。其著眼點在於，無論短期內是否建立臺灣地區交通電子票證之共同「電子票證跨系統清算中心」，當臺鐵交通電子票證系統推出服務後，勢必面臨該票證與銜接各地方之交通電子票證整合之課題。因此，臺鐵未來之交通電子票證受委託單位，本身即必須提供臺鐵與銜接各地區之交通電子票證清算與交換之功能。

換言之，如果能全力協助臺鐵加速完成通勤列車票證電子化計畫，同步搭配交通部輔導各區交通電子票證系統符合交三版規範之轉換輔導計畫，則可以讓臺鐵之新電子票證可以達到跨系統交易全國一卡通之目的，而各區之交三版交通電子票證亦可跨系統於臺鐵站上使用，如此臺灣交通電子票證一卡通之雛型可以實現。至於各區交通電子票證如果可以同步達成共識，亦可暫時利用臺鐵電子票證建置與管理專案計畫內所建立之「電子票證跨系統清算交換中心」功能，作為短期內彼此跨系統交易產生之資料運算管理中心。

5.3 相關法規研析

一、政府監理運輸票證之法源與相關規定

目前地方政府制訂運輸票證監理自治條例之法源為憲法、地方制度法，規定各地方交通之規劃、營運管理，係屬地方政府之自治事項，地方政府自得依據地方制度法規定，制定運輸票證監理自治條例；另外各運輸事業體依據主管機關之不同，有其不同之票證監理規定，公路客運之票證監理規範為公路法第七十九條訂定之「汽車運輸業管理規則」，內容多屬對於乘客乘車使用車票之相關規定，較少關於業者票務管理之規定，關於票務人員、儲值票之製作發行、交易記錄保存、異常狀況處理及乘客申訴等並未加以規定，因此完整性仍有所不足；捷運票證部份，有關票證之監理

制度規定甚少，主要法源為「大眾捷運法」，但僅有規定大眾捷運系統之旅客運價及聯運運價受主管機關之監督；停車場票證部份則無明確法令之規定，亦無與其他大眾運輸工具間之票證整合監理規範。

二、電子票證相關規定之限制

根據「銀行法」第四十二條之一規定，「銀行發行現金儲值卡應經主管機關許可，並依中央銀行之規定提列準備金；其許可及管理辦法，由主管機關洽商中央銀行定之。前項所稱現金儲值卡，謂發卡人以電子、磁力或光學形式儲存金錢價值，持卡人得以所儲存金錢價值之全部或一部交換貨物或勞務，並得作為多用途之支付使用者。」；「銀行發行現金儲值卡許可及管理辦法」第三條規定，「前項所稱多用途係指現金儲值卡之使用，可跨越不同營運系統間使用，或應用於不同之商業體系。非銀行不得發行現金儲值卡。」非銀行不得發行儲值卡，原根據金管會的解釋，票證公司所發行的電子票證若用途超過單一用途者便視為現金儲值卡，即便在不同運輸系統中使用(如捷運與公車)亦屬於跨營運系統之現金儲值卡，因此若未來進行票證整合在多系統共用，除非由銀行發行卡片或由銀行與票證公司發行聯名卡才得實現。目前國內對於電子票證之管理規定有以下兩項法規：

1. 預付型交通電子票證定型化契約應記載及不得記載事項

交通部於 96 年研擬「預付型交通電子票證定型化契約應記載及不得記載事項」，該案已於 97 年 4 月 1 日正式頒布施行，該案明確定義預付型交通電子票證的應用範圍，包括公路客運、市區客運、大眾捷運、鐵路、纜車、渡輪等運輸服務之支付及高速公路通行費、停車場使用費等，該案除定義電子票證應用範圍外，為降低發行人和消費者間所存在之資訊不對稱性，預防消費糾紛，該案規定下列重點以保障消費者權益：

- (1) 電子票證中應記載或顯示發行人名稱、服務電話、票種、識別標識等。
- (2) 發行人對其所收取之金額，應辦理履約保證，例如已經○○金融機構提供足額履約保證，或存入信託專戶，專款專用。
- (3) 預付型交通電子票證之儲值金額上限不得超過新臺幣 1 萬元。
- (4) 除經主管機關核准者外，不得記載逾期或未使用完之票證餘額不得退費。

- (5) 不得記載記名式預付型交通電子票證票證不得辦理掛失。
- (6) 不得記載使用期限或污損無效等不合理之使用限制。

2. 「電子票證發行管理條例」

有鑒於「銀行發行現金儲值卡許可及管理辦法」第三條規定「非銀行不得發行現金儲值卡。」，而目前悠遊卡公司因非屬銀行，因此無法將應用範圍推動到便利商店、自動販賣機、速食店...等等之小額消費，有賴相關法令予以放寬。該條例係為建構我國完善之小額消費體系，以保護消費者權益及維護市場交易秩序，須對於發行電子票證機構採取適當之管理機制，對交易體系建立有效監控機制。「電子票證發行管理條例」已於 98 年 1 月 13 日三讀通過，該條例之重點如下：

- (1) 本條例之主管單位為行政院金管會。
- (2) 以非銀行之發行機構規範對象，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。另外，針對多用途支付使用部分，但僅用於支付交通運輸使用並經交通目的事業主管機關核准者，不視為多用途支付使用。
- (3) 發行機構之實施資本額須達新臺幣三億元。
- (4) 發行機構應採取下列方式之一以確保電子票證發行之履約能力：
 - A. 設置結算信託專戶
 - B. 繳存結算保證金
 - C. 取得銀行履約保證
 - D. 其他經主管機關許可之履約保證方式
- (5) 電子票證之儲存金額不得超過新臺幣一萬元。
- (6) 規定結算及清算方式
 - A. 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。
 - B. 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。

該條例實施後，預料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由交通部移轉至金管會，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；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侷限於交通電子票證，還能應用於其他商業體系，使得交通電子票證可應用於其他小額消費，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有相當大助益；另外，該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。而因應該條例第三條第四款有關多用途支付使用但書之規定，交通部於 98 年 7 月 30 日發布「非多用途支付使用交通電子票證核准基準」，其中訂定 5 年之落日條款，如主管機關認定其為僅用於支付交通運輸使用並核准者，得暫不適用該條例，未來該等公司在 5 年限期內必須致力於調整公司體質，以符合該條例之規定。

第六章 後台票證整合之課題探討

交三版制定精神係著重於訂定前台設備的共通基準，然而對於實際運行的整體系統而言，此標準只是整個大架構中的一環。為了真正達到某票證業者發行之交三版卡片確實可以為他家業者的系統所接受，並可享受跨系統業者所提供的服務，則尚有數項工作必須由各家業者持續透過技術討論進行協商，確認出來一套大家都同意的作法機制，由各票證業者共同遵行。為推動各電子票證系統之作業面實質整合，本章針對後台票證整合之關聯課題如金鑰整合機制、卡片真偽確認機制、交易真偽確認機制及後台交易/黑名單交換機制等進行探討。

6.1 金鑰整合機制

在交三版規劃書(草案)中已對卡片欄位、資料型態、交易流程等提出建議，但對於減值金鑰的實際做法及卡片真偽辨認則需要各家票證公司統一協商出共同的做法，使交三版卡片能在安全的金鑰管控流程中相互使用於各家票證公司之減值設備。

針對防偽驗證而言，交三版定義之共通技術規範係在於每一業者產製出來的交三版卡片皆可於其他業者的減值設備上使用。若無一致的驗證機制，將導致票證業者無法檢驗或確認其他業者的卡片真偽。若其他業者的卡片是一張偽卡，而前台設備將無法於服務提供時進行檢驗，將可能導致這張卡片所做的任何交易都無法取得原卡片發行業者的款項。若統一訂定此一卡片檢驗的機制，則對於各發行業者的卡片安全機制產生一定程度的衝擊，因此需要業者自行討論出一個解決的方法。就技術面而言，可由業者評估統一防偽碼產製的作法，對於其本身發卡安全性的衝擊，最後協調出各家票證業者皆同意之防偽驗證作法。

為使交三版卡片能跨票證系統使用，各業者的減值主金鑰組以及卡片減值相關扇區的衍生演算法需要一致，使各設備在進行減值時有一致的規範。

6.1.1 交三版金鑰管理規範建議

為使交三版規劃之共同減值主金鑰組能被各參與業者所信任，其金鑰管理作業至少必須符合下列建議之相關規範：

一、交三版全區卡之卡片金鑰(基碼)，應分個別管理主金鑰組與共同管理主金

鑰組。

- 二、個別管理主金鑰組為發卡單位個別擁有之主金鑰組(如：加值主金鑰組...)。
- 三、共同管理主金鑰組為全區共用之主金鑰組(如：減值主金鑰組，防偽驗證碼主金鑰等...)。
- 四、共同管理主金鑰組應由公信單位(如公協會)管理並保管於各方可信賴的安全機房。
- 五、依據各方同意之「基碼管理辦法」以及「機房管理辦法」等辦法規定之作業程序，以共同管理主金鑰組。
- 六、基碼管理辦法中須包含金鑰之安全管理存取權限管控、金鑰備份及回復作業、金鑰安全傳輸作法，並應規範主金鑰之明碼不得儲存於非 HSM、IC 智慧卡外之其他儲存媒體中。若欲進行主金鑰組資料傳輸時，則可使用多張 IC 智慧卡搭配存取密碼的方式進行。
- 七、欲加入發卡單位之金鑰管理機制，必須經由公信單位中各家已加入之發卡單位認可後才得以加入組織，此一作為乃在於確保各發卡單位之金鑰管理機制確可提供安全且保密之運作發卡環境，而不至於發生單位人員盜用金鑰之狀況。
- 八、公信單位須規範各發卡單位進行定期之安全控管檢查，用以防堵不肖員工可能造成之安全漏洞。
- 九、若因發卡單位之內控發生問題，導致共同金鑰內容發生洩密，致使他家發卡單位蒙受損失，則該發生內控問題之發卡單位應賠償其損失。

6.1.2 減值金鑰演算法則選擇之建議

為使交三版規劃之減值金鑰及演算法則能取得票證公司實務上之適用性，且能保障各票證公司之安全性要求，以下將說明交三版減值金鑰及演算法則：

一、減值金鑰演算法種類

1. AES 演算法

AES 演算法為新式之加密技術，演算法則如下：

Input：

Diversification ID (ID)

Master Key (M) (128 bit AES Key)

Output :

Diversified Key (D)

Algorithm :

O = AES_ENC(M, ID|| 0128-[ID]) 不足 128bit 的補足 128bits

D = [D] leftmost bits of O 取最左的[D] left bits

PS : Mifare Key is 6 bytes

2. Triple-DES 演算法

Triple-DES 為目前國內大部份的票證公司及一般加密使用之技術規格，演算法則如下：

Input :

Diversification ID (ID)

Master Key (M) (16 bytes Triple-DES Key)

Output :

Diversified Key (D)

Algorithm:

O = Triple-DES(M, ID|| 0128-[ID]) 不足 128bit 的補足 128bits

D = [D] leftmost bits of O 取最左的[D] left bits

PS: Mifare Key is 6 bytes

3. DES 演算法

DES 為早期系使用之加密機制，演算法則如下：

Input :

Diversification ID (ID)

Master Key (M) (8 bytes DES Key)

Output :

Diversified Key (D)

Algorithm :

O = DES(M, ID|| 0128-[ID]) 不足 128bit 的補足 128bits

D = [D] leftmost bits of O

取最左的[D] left bits

PS: Mifare Key is 6 bytes

二、演算法則之比較

針對金鑰衍生機制，上述三種為常用之演算法，分別依金鑰演算速度、保密性以及演算法的新穎性進行演算機制之討論及選擇：

1. AES 演算法

(1) 演算速度：快

(2) 保密性：不易破解，用來替代原先的 DES 演算法，亦比 Triple-DES 安全性高

(3) 新穎性：2002 年為美國國家標準，目前為主流之對稱金鑰加密技術

2. Triple-DES 演算法

(1) 演算速度：慢

(2) 保密性：較 DES 演算法安全

(3) 新穎性：為 DES 演算之變型，在 AES 演算法未正式公佈前，美國國家標準局將 Triple-DES 視為過渡之加密標準

3. DES 演算法

(1) 演算速度：慢

(2) 保密性：演算法易破解

(3) 新穎性：1977 年為美國國家標準

三、演算法則之建議

建議使用較新穎之 AES 演算法。

6.1.3 發卡流程建議

定義演算法則可律定前端設備金鑰存取驗證之一致性方法，但各票證公司之發卡流程需定義出共同之介面及流程，如此才能確保不同票證公司發行之交三版卡片能跨系統進行減值作業。

一、發卡架構說明

交三版卡片發行包含公協會、票證公司及持卡人三種角色，如圖 6-1，說明如下：

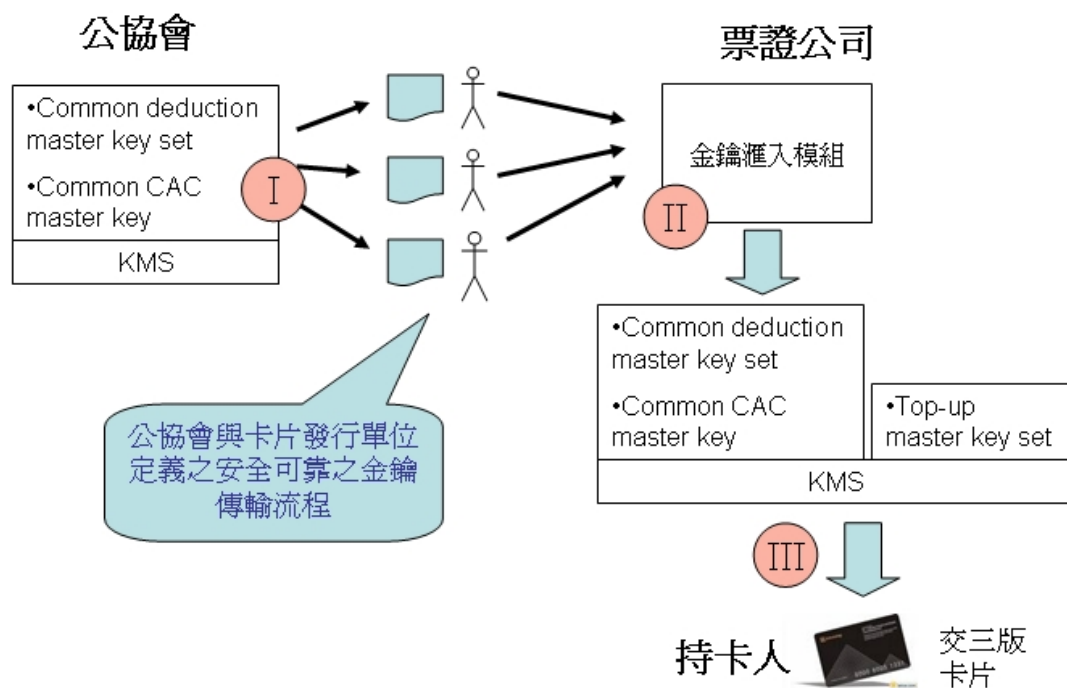


圖 6-1 交三版卡片發行架構

1. 公協會

為票證系統執行及管理之公證單位，負責管理交三版減值母金鑰組，提供給各票證公司做為減值之金鑰驗證之用，如此，交三版卡片皆有相同之母金鑰組做為減值之依據，即可進行跨票證系統之交易扣款。公協會管理之金鑰包含兩種金鑰值：

- (1) 減值主金鑰組(Common deduction master key set)
- (2) 防偽驗證碼母金鑰(Common CAC master key)

2. 票證公司

票證公司為獨立發行交三版卡片之營運單位，除使用公協會提供之減值母金鑰之外，個別票證公司管理該公司之加值母金鑰組，使交三版卡片在發卡時，即可進行跨票證系統之交易扣款及個別票證公司之加值服務交易。票證公司管理之金鑰則為加值主金鑰組(Top-up master key set)。

3. 持卡人

持卡人購卡(或開卡)完成後，即表示該卡片已完成加值金鑰、減值金鑰及防偽驗證碼之製卡作業，故可使用於支援交三版交易之驗票設備進行交易扣款。

二、發卡流程說明

為使交三版卡片在製/發卡時能以統一及安全的方式進行，以下說明製/發卡建議之流程：

步驟一：

以公協會與發卡單位共同規範之金鑰傳輸流程進行金鑰滙出作業，此作業需在安全之機制下進行，需要滙出之金鑰包含 Common deduction master key set 及 Common CAC master key。

步驟二：

以公協會與發卡單位共同規範之金鑰傳輸流程進行金鑰滙入作業，此作業需在安全之機制下進行，完成滙入後，共同金鑰即儲存於票證公司之金鑰管理系統中(KMS)，每一發卡單位僅需進行一次滙入作業。

步驟三：

發卡時需使用交三版共同金鑰及票證公司管理之加值金鑰完成製卡流程，完成發卡之卡片即可在支援交三版交易之驗票設備進行交易扣款。

6.2 卡片真偽確認機制

交二版的定義中，在第一扇區的第三個區塊中放置了卡片的防偽驗證資料，此一資料針對每一家票證業者而言，不僅每張卡片的內容都不同，且每家業者的產製邏輯以及金鑰也都不同。然而，交三版定義的主要目標乃在於每一家業者產製出來的交三版卡片皆可於其他家業者的減值設備上使用。如此將導致其他家業者將無法檢驗或確認他家業者的卡片真偽的問題。若該張他家業者的卡片是一張偽卡，則前台設備將無法於服務提供時進行檢驗，而有可能導致這張卡片的所有交易都無法向他家業者申請款項。若統一訂定此一卡片檢驗的機制，則對於各家發行業者的卡片安全性產生一定程度的衝擊。因此需要業者自行討論出一個解決的方法，可由技術面或是營業面上來提出解決方案。技術面上，可由業者評估統一防偽碼產製的作法對於其本身發卡安全性的衝擊，到底有多大來取決是否可以按照大家統一的演算法以及金鑰來進行驗證，如此將不會有各家金鑰交換以及演算法互相交換的問題。

6.2.1 遠通電收建議之防偽驗證碼產製及驗證流程

防偽驗證碼由票證公司在發卡時即寫入卡片中，在持卡人進行刷卡交易時，由驗票設備進行卡片防偽驗證碼之檢查。

以下為遠通電收所提供之卡片防偽驗證碼之產生以及驗證機制，其建議各家票證業者於前台驗票設備中皆使用同一把金鑰透過 AES 演算法進而產生卡片之防偽驗證碼，進行前端卡片驗證，而後傳回卡片防偽資料再由後台使用另一把各自不同之金鑰進行再次驗證。

一、產生防偽驗證碼流程(如圖 6-2)

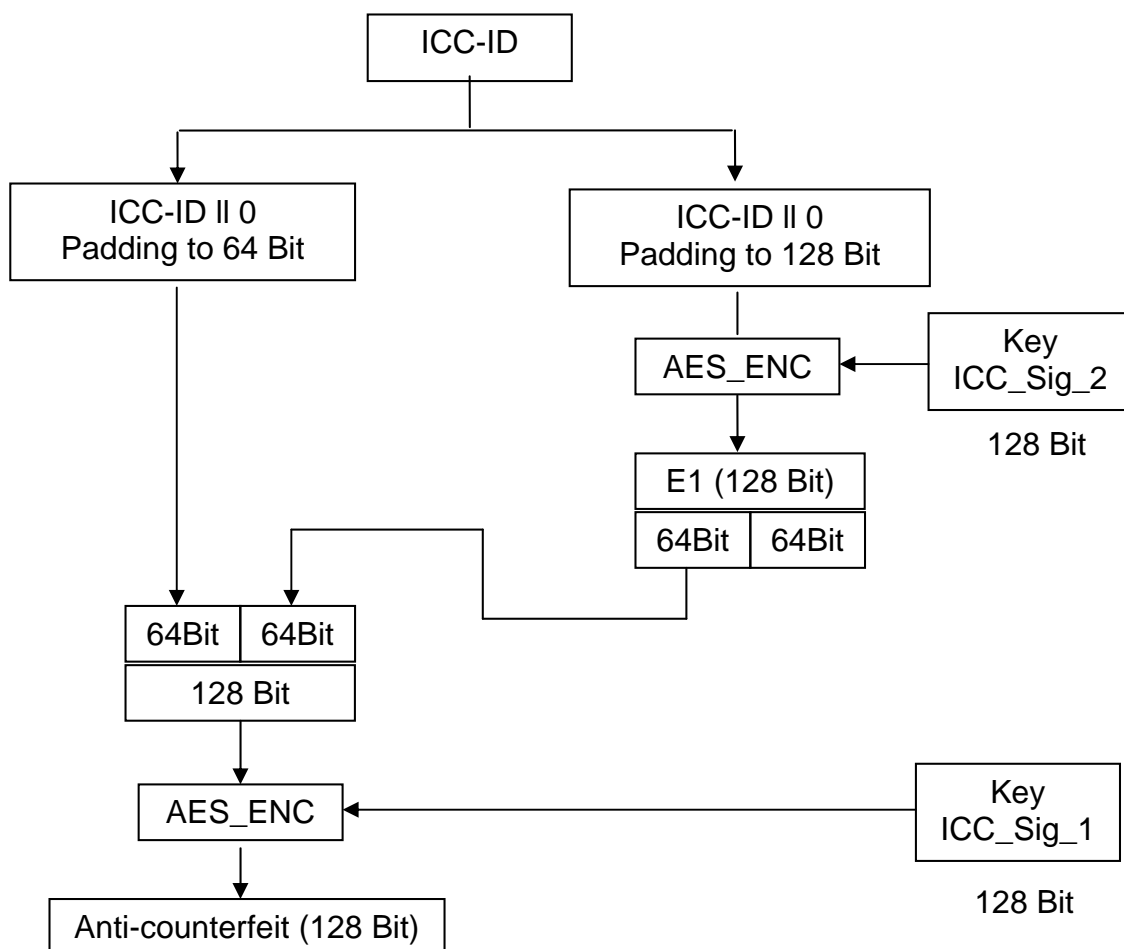


圖 6-2 遠通電收建議之防偽驗證碼產製流程

二、驗證防偽驗證碼(如圖 6-3)

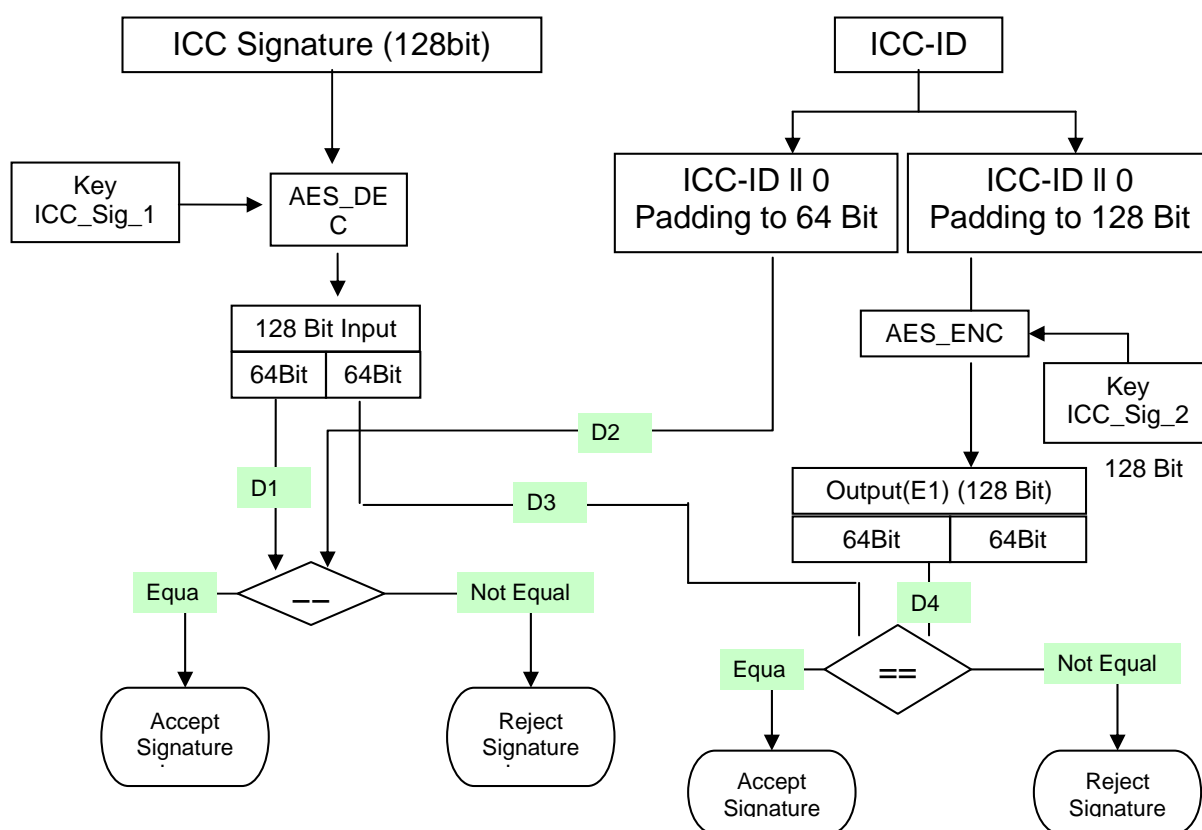


圖 6-3 遠通電收建議之防偽驗證流程

三、安全性考量事項

此一作法於技術上乃屬可行之建議，然而尚有一些安全性上之考量需進行修改：

1. 當前台驗票設備已驗證該卡片為"真"，且以提供相對應之服務，但是如果後台使用另一把金鑰驗證出為"偽"時，則後台要撥款或不撥款都會是一個問題，因為驗出是"偽"所以應該不撥款，但是前台服務已經提供，若不撥款則會受到業者的質疑，因此將會造成營運上的困擾。
2. 若欲於後台再行驗證防偽驗證碼，則每張卡片之防偽驗證碼將會隨著交易紀錄回傳後台，以供驗證然而此將會造成系統安全性上的極大漏洞，因每張卡片之防偽驗證碼將會透過交易紀錄回傳的機制透通的傳回後台，而回傳機制的每一個環節皆有可能因此而攔截其資料，造成系統洩密的問題。
3. 若每家票證業者皆使用同一把金鑰產製防偽驗證碼，則有可能一家票證業者可輕易複製他家票証業者之卡片，因此有可能會造成系統性問題。

6.2.2 防偽驗證碼驗證機制討論之議題

為使防偽驗證碼之產製及驗證能安全及快速進行，各票證公司於技術會議中提出相關之做法，議題整理如下：

一、演算法則之選擇：

使用較新穎之 AES 演算法進行防偽驗證碼驗證，可提高安全及速度之要求。

二、每家業者皆使用不同之防偽驗證碼產生金鑰：

1. 唯採用此建議將有以下缺點。若已有 A、B 兩家已發行交三版卡片的票證業者完成票證整合，當第三家 C 票證業者要加入時，所有 A、B 兩家業者的驗票設備皆需更換原來已完成票證整合的交三版 SAM 卡，以加入第三家 C 業者之防偽驗證碼產製金鑰，故新加入票證整合的 C 票證業者需考慮 SAM 卡置換之成本。
2. 為使每家票證業者皆使用不同之防偽驗證碼產生金鑰，SAM 卡在進行防偽驗證碼檢查時，須得知卡片之發行公司，故建議交三版之減值設備傳給 SAM 卡之輸入參數須加上發行公司代碼(issue code)，以利快速驗證。
3. 建議每家票證業者皆使用不同之防偽驗證碼產生金鑰，以保護票證業者之發卡權利及可能發生之偽卡問題處理。
4. 防偽驗證碼之檢驗，只須於前台驗票設備中進行檢驗，而不應回傳至後台，也不能開放各家後台選擇須驗或不需驗。

三、產生防偽驗證碼建議流程(如圖 6-4)

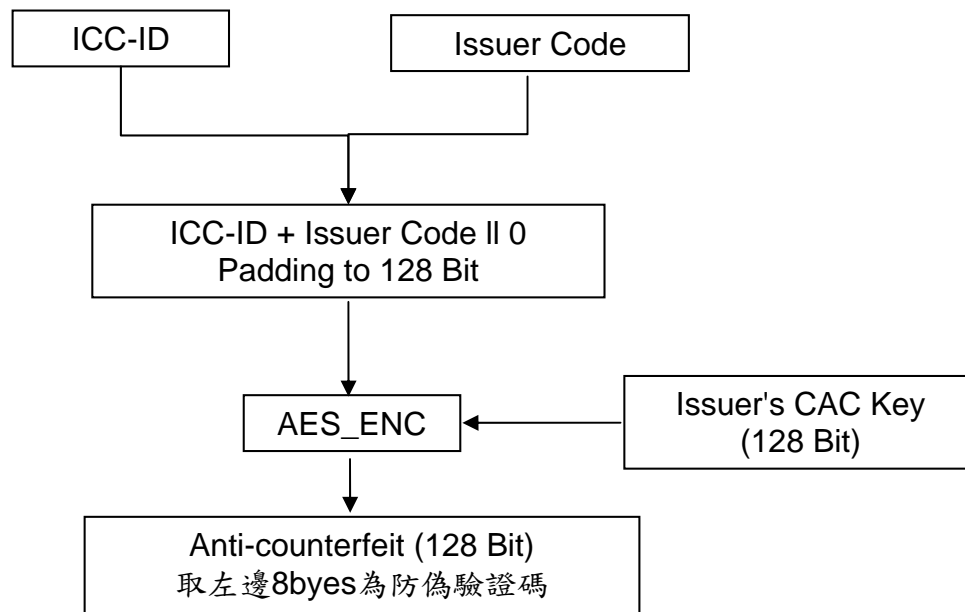


圖 6-4 本計畫討論過程之防偽驗證碼產製流程

四、驗證防偽驗證碼建議流程

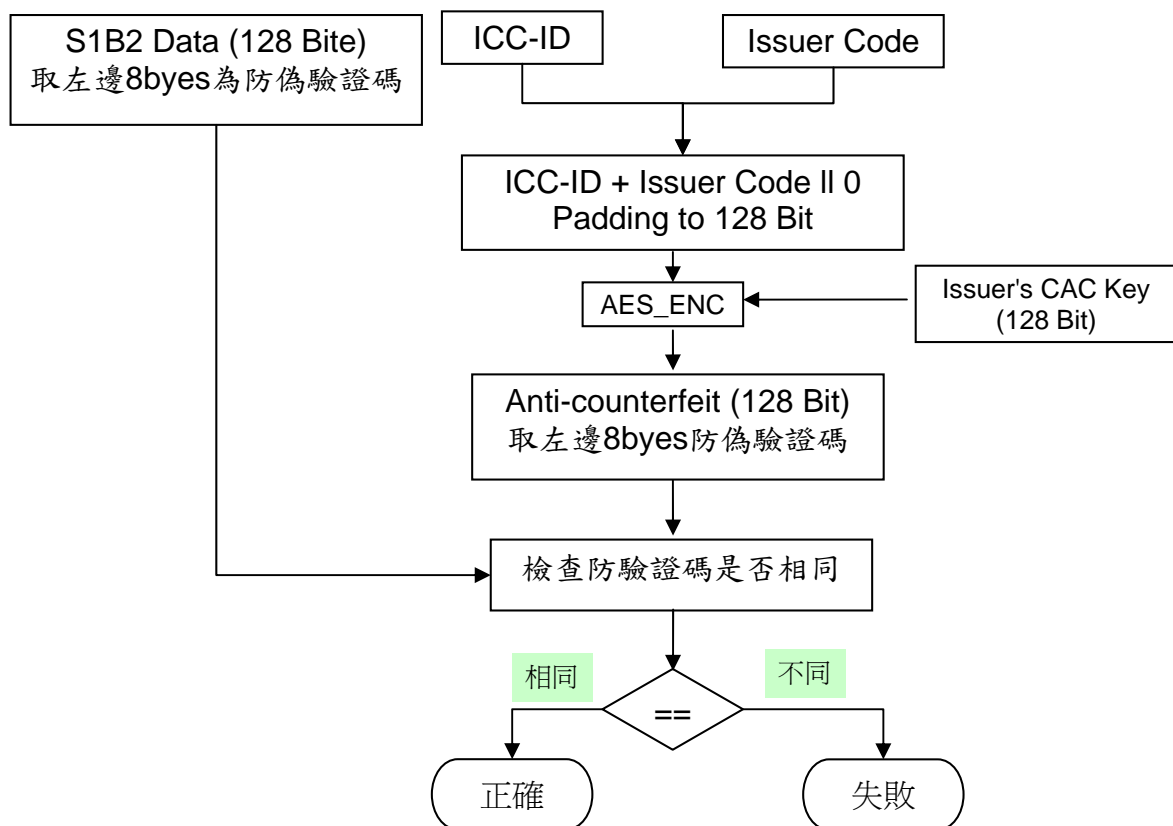


圖 6-5 本計畫討論過程之防偽驗證流程

6.2.3 防偽驗證碼產製及驗證流程之選擇及建議

一、演算法則之選擇：

建議使用遠通電收提出之 AES 演算法。

二、防偽驗證碼產製流程之建議：

1. 本計畫提出防偽驗證碼產製流程之建議，待各家票證公司試行確認可行後，由公協會制定此防偽驗證碼產製標準流程。
2. 在此流程中，各家票證公司使用之防偽驗證碼之母金鑰皆相同，則有可能一家票證業者可輕易複製他家票證業者之卡片，因此有可能會造成系統性問題，建議公協會訂定票證公司認可之稽核流程及做法，以確保票證公司發卡之權利。
3. 在此流程中，各家票證公司使用之防偽驗證碼之母金鑰皆相同，若有新票證公司加入發行交三版卡片時，不會影響現有票證公司之發卡流程，並且卡片可直接跨系統使用，驗票設備無需修改。
4. 此產製流程之選擇，避免新加入票證整合之票證業者時需考慮 SAM 卡置換之成本及系統維護之複雜度，故建議使用本方案。
4. 其流程如下圖 6-6：

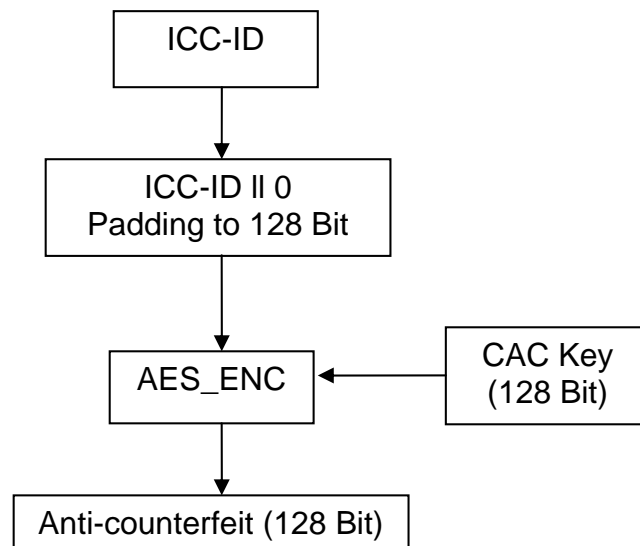


圖 6-6 本計畫建議之防偽驗證碼產製流程

三、防偽驗證碼驗證流程之建議：

1. 本計劃提出防偽驗證碼產製流程之建議，待各家票證公司試行確認可行後，由公協會制定此防偽驗證碼驗證標準流程。
2. 防偽驗證碼之檢驗，只須於前台驗票設備中進行檢驗，而不應回傳至後台，也不能開放各家後台選擇須驗或不需驗。
3. 在此流程中，前台扣款設備可直接讀取不同票證公司之卡片，並進行扣款交易，驗票設備無需修改，也不需更新 SAM 卡。
4. 此驗證流程之選擇，避免新加入票證整合之票證業者時需考慮 SAM 卡置換之成本及系統維護之複雜度，故建議使用本方案。
5. 其流程如下圖 6-7：

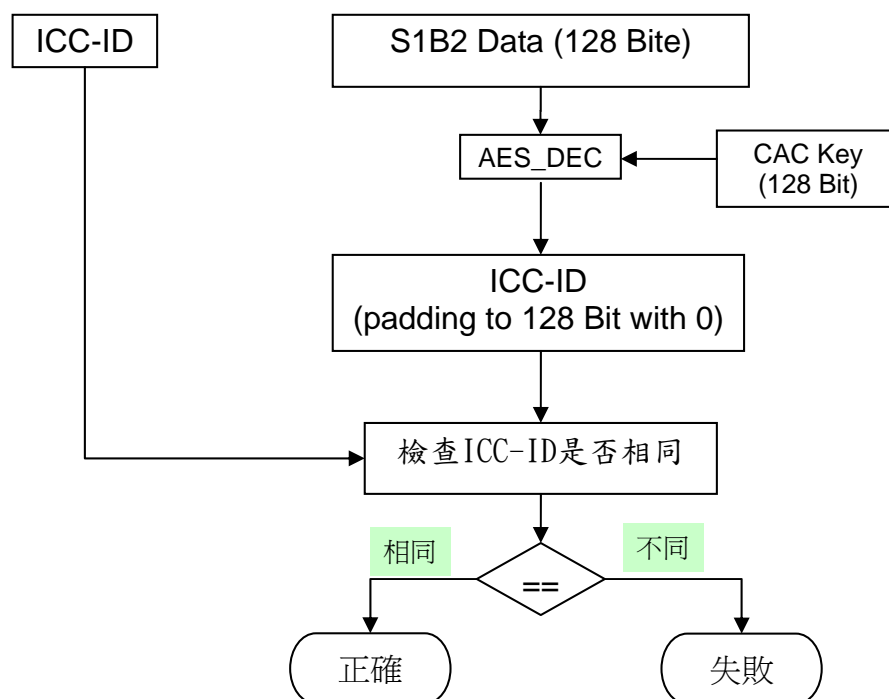


圖 6-7 本計畫建議之防偽驗證流程

6.3 交易真偽確認機制

交易真偽確認機制乃在於確保每一家業者產製出來的交三版卡片皆可於其他家業者的減值設備上使用並且得以順利撥款，因此提供減值設備之業者不僅須於減值的當時確認卡片之真偽以外，並需於減值設備中產生一組交易壓碼資料以供後台確認。此一交易壓碼之主要目的在於由後台確認該減值設備已完成卡片減值之程序(亦即該交易卡片中之餘額確實已經被扣除了該交易所應支付之

金額)進而確認該交易之完成。後台系統確認該交易之確實完成，便可逕行撥付款項於該減值設備之安裝業者。

本計畫依據一般金融信用卡代收代付之作業慣例，減值設備所收具之電子票價由鋪設減值設備之業者代付所有款項，則減值設備本身乃至於減值設備到清算後台之安全機制應由鋪設減值設備之業者負責。因此本計畫建議交易真偽之確認機制應秉持各參與交三版票卡共通之各家業者互信原則，交由各減值設備鋪設業者自行定義並負責確保該交易之確實產生。故本計畫並不另行規劃交易真偽確認機制。

6.4 後台交易/黑名單交換機制

後台交易/黑名單交換機制之實施必須由所有參與交三版票卡共通的各家業者所組成之公信單位進行統籌運作。所有各家業者所產生之黑名單以及減值設備收取之非該家業者之所有交易，皆須傳送至該公信單位之交換中心，並將黑名單彙總後轉送至各家業者，且將所有傳入之交易轉送至該交易卡片之所屬業者。所有相關之黑名單檔案格式以及交換交易檔格式應由各家業者以及公信單位研議並確定，本計畫將不另行規劃。

第七章 結論與建議

經過歷年來交通部與地方政府的推動與輔導，國內交通電子票證的發展已逐漸應用到各種大眾運輸工具，包含悠遊卡(臺北、基隆、宜蘭、馬祖等地區及臺鐵基隆—中壢區間)、臺灣通(桃、竹、苗、中、彰、投、花、東等縣市公車)、TaiwanMoney(嘉、南、高、屏等縣市公車)、高雄捷運一卡通、金門電子票證及高速公路 ETC 等系統，電子票證在其他非交通領域的應用亦逐漸擴展，如學生證、借書證、社區門禁、政府規費收費等，迄 97 年 12 月底為止，各系統累計發卡量的總和已超過 1770 萬張。

為促進各系統間的互通使用，本計畫提出以交三版卡片規格為基礎的整合方式，研擬交三版規格與交易流程規範之草案，並規劃交三版卡片驗證機制，開發第一階段之靜態資料驗證系統。整體而言，本計畫獲致的重要結論歸納如下：

7.1 結論

- 一、本計畫蒐集國外電子票證整合發展的案例，包括中國珠江三角洲、瀋陽一卡通、曼谷捷運共通卡、巴黎多用途交通卡等，其中以曼谷捷運共通卡與我國電子票證所面臨的挑戰與現實環境最為類似，泰國政府將研擬共通卡規格及相關系統之規範，做為整合既有及未來捷運公司電子票證系統的基礎，與國內目前各電子票證系統彼此不相容，政府將發展交三版卡片規範作為整合的基礎相同，不同之處在於泰國政府將積極主導整合計畫，計畫籌資成立電子票證公司，發行捷運共通卡，並逐漸淘汰既有的捷運電子票證，相關做法值得交通部參考借鏡。
- 二、本計畫研擬完成交三版草案，該草案以交二版為基礎，交通電子票證使用之非接觸式 IC 卡及雙介面複合式卡為修訂標的，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，交三版以「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及增加交易速度。
 2. 明確規範交易流程，規劃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 卡片系列的發卡單位參考。

三、為了建立一套公正的交三版卡片格式及交易流程的檢驗機制，驗證各家票證系統的卡片能夠依照交三版定義的卡片格式及交易流程而相互通用，本計畫規劃完成交三版驗證機制，包括驗證申請作業流程、驗證系統架構及驗證流程，其中驗證流程包含第一階段卡片靜態資料驗證及第二階段卡片動態資料驗證，本計畫今年度開發完成卡片靜態資料驗證系統，可以檢視送測之卡片資料內容是否符合交三版之格式定義，包括欄位編碼方式、資料型態及金鑰存取權限檢查等。

四、為利於國內電子票證的管理，「電子票證發行管理條例」已於 98 年 1 月 13 日經立法院三讀通過，該法案未來可能對國內電子票證市場產生重大變革，首先，電子票證發行將採核准制，未來需經金管會核准才得辦理電子票證業務；其次，發行電子票證機構的設立門檻提高，資本額須達新臺幣三億元，且規範發行機構的履約能力，部分既有票證公司需大幅調整公司體質才能符合該法案的規定；最後，對於非銀行體系機構所發行的電子票證未來能夠應用於小額消費，鬆綁過去電子票證不得跨領域應用的限制，對於票證公司的發展遠景有相當大的助益。而因應該條例第三條第四款有關多用途支付使用但書之規定，交通部於 98 年 7 月 30 日發布「非多用途支付使用交通電子票證核准基準」，其中訂定 5 年之落日條款，如主管機關認定其為僅用於支付交通運輸使用並核准者，得暫不適用該條例，未來該等公司在 5 年期限內必須致力於調整公司體質，以符合該條例之規定。

五、本計畫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的整合機制，其中在金鑰整合方面，本計畫規劃的交三版卡片發卡流程，係由電子票證公協會負責管理交三版減值主金鑰組及防偽驗證碼母金鑰，各票證公司負責管理加值主金鑰組。

本計畫效益包括可提升國內電子票證系統中下游相關技術產業之發展，促成產業技術之升級，同時將國外卡片之最新技術發展引進國內，使國內業界之技術與國外並駕齊驅，進而加速票證系統設備之更新，有助於交通部交通電子票證發展政策之推動；而本計畫成果可支援交通部交通電子票證發展政策之需要，適時提供技術與政策分析支援。

7.2 建議

一、建置共通的電子票證跨系統清算平台

本研究探討國外電子票證整合最積極的國家是中國，其原因是中國電子票證系統早期建置時尚未有國家標準，而中國的高速公路大部份採 BOT 方式建設，故高速公路電子票證系統均由建置廠商各自規劃，不同的 BOT 廠商的電子票證並不相通。目前因為中國高速公路網已成型，故中國政府要求各電子票證組織，包括公交系統均必須遵照建設部所頒定的電子票證各種規範逐年整合，故建置跨系統的清算平台成為電子票證業者必須面臨的問題。

目前中國所建置的跨系統的清算平台可分為 2 種模式：

1. 協作模式：以一個清算中心為主要系統，其它系統依附在主要系統直接建置加值和消費系統，並通過數據交換系統與中心系統進行數據交換，通過結算系統與中心系統進行結算對帳。
2. 對等模式：即 2 個電子票證系統各自建置獨立的系統，利用建設部密鑰統一的規格，2 個系統間互相交換跨區域消費數據及名單數據。

以臺灣目前電子票證的市場規模狀況，從經濟效益而言，參考中國清算平台的協作模式是比較理想的作法，可以節省大量的資源，避免重複建設，關鍵是各票證系統間必須能夠取得共識，共同參與清算平台的建立與營運，評估國內目前狀況，該清算平台由業者自行成立的可能性不高，故本研究建議由政府主導並建置一共通的電子票證清算平台。

二、探討以 CPU 卡作為國內交通電子票證載體之可行性

2008 年 4 月位於德國漢堡的 ChaosComputerClub 已經破解了 NXP 的熱門 Mifare Classic RFID 晶片的加密方法，同年倫敦大眾運輸電子票證用的 Mifare 也被成功破解。Mifare 因交易速度快，目前是世界應用在交通電子票證的主流卡片，但是其安全機制也一直備受質疑。

至於 CPU 卡則可執行較複雜的邏輯運算，其安全性相對較高，金融卡大部份也以 CPU 卡為主，就交通卡多用途的發展趨勢而言，若要將交通應用擴展到小額消費，交通卡已具有電子錢的功能，屬於「準貨幣」型態，若被破解後所遭受到的損失遠大於交通票證的損失程度，因此卡片的安全防護勢必要提高，故建議本計畫下一階段應探討 CPU 交通卡之可行性研究。

三、接續開發卡片動態資料驗證系統

本計畫已完成交三版第一階段卡片靜態資料驗證系統，建議本計畫之下一階段開發卡片動態資料驗證系統，如此方能驗證交三版各資料欄位格式之完整性及正確性。

卡片動態資料驗證即為跨系統交易交叉測試，一套完整的動態資料驗證程序需包含交三版定義的 4 種交易型態：開放交易系統、非連續型封閉交易、異機進出連續型封閉交易系統、同機進出連續型封閉交易系統，此 4 種交易型態在卡片中使用不同的扇區儲存交易資料，故此部份的驗證目的即在檢核不同之驗票設備間是否能正確進行減值交易，確保卡片交叉使用於不同載具時，其資料格式及交易流程皆符合交三版的相關定義。建議本研究未來應視計畫經費的多寡選擇全部或部分的交易型態進行動態資料驗證系統的開發。

四、本計畫提出的票證整合方案以交三版卡片規格及交易流程作為整合的基礎，除交三版的規範外，仍有許多機制必須加以制定與執行，包括交三版卡片的金鑰管理規範、卡片防偽驗證流程的制定，以及交三版卡片規格驗證的執行與減值主金鑰的管理等，上述工作需要協調各票證公司的運作並取得各票證公司的信任，因此需要由一個公信單位加以執行，此公信單位建議由政府協調既有票證公司及相關單位共同組成電子票證公協會，由該公協會統籌運作票證整合的相關事宜。

參考文獻

一、國內部份

1. 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(1/4)－電子票證與驗票機介面規範及票證一卡通論壇推動之規劃，民國 97 年。
2. 交通部，全國交通票證 IC 智慧卡清算後台標準核心模組發展研究計畫(二)，民國 95 年。
3. 交通部，全國交通票證 IC 智慧卡清算後台標準核心模組發展研究計畫(一)，民國 94 年。
4. 宏基股份有限公司，南部地區 IC 智慧卡電子票證系統整合建置案細部設計書，民國 94 年。
5. 交通部，大眾運輸智慧卡功能整合與推廣示範計畫(二)，民國 93 年。
6. 交通部，大眾運輸智慧卡功能整合與推廣示範計畫(一)，民國 92 年。
7. 交通部運輸研究所，高鐵、臺鐵票證系統整合規劃之研究，民國 92 年 12 月。
8. 交通部，電子票證系統之多功能卡片規劃書(第二版)，民國 92 年。
9. 臺灣鐵路管理局，第三代票務整合系統委外規劃，民國 91 年。
10. 遠通電收公司網頁(<http://www.fetc.net.tw/>)。
11. 財金公司網頁(<http://www.fisc.com.tw/FISCWeb/FISCBimonthly>)。
12. 高雄捷運公司網頁(www.krtco.com.tw)。
13. 金卡網(<http://www.goldencard.com.cn/>)。

二、國外部份

1. ITSO 網站(www.itso.org.uk)。
2. JR 東日本網站(<http://www.jreast.co.jp/>)。
3. 香港八達通卡有限公司網站(www.octopuscards.com)。

附錄 1

歷次技術研討會紀錄

「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」

第七次技術討論會紀錄

一、開會時間：九十七年一月十四日(星期一)下午二時

二、開會地點：運輸研究所十樓會議室

三、主持人：王穆衡組長

記錄 許安慶

四、出席單位及人員：略

五、簡報：略

六、結論：如下表

案號	提案單位	Sector/Block	討論議題	會議結論
S0B0-01	TSCC	S0/B0~2	建議： 1. Sector 0 Key A = 0x A0~A5 2. AC Value = 0x78778800(KeyA/B Read KeyB Write) 3. Sector 0 Key B 保留各票證自行權限控管	本議題屬於各扇區 AC 的規劃，將於扇區存取權限規劃工作會議時一併討論。
S0B1-01	KRTC	S0/B1、2	建議若交易系統編號定義不足時，能使用 0xFF 來表示「未定義交易系統編號」。	此為 KRTC 目前與 TaiwanMoney 卡整合時暫時性的權宜作法，不列入交三版規劃。
S0B1-02	TSCC	S0/B1、2	建議： 1. AID1 0x1100、0x1201、0x1302（依交易系統編號--使用扇區編號）	1. FETC 已向交通部申請 0x12、0x13、0x14、0x15 等四個交易系統編號，故交三版應用資料區交易系統編號仍維持原規劃。 2. 因為 1 Byte 僅可規劃 256 組交易系統編號，為有效應用此欄位，對於未來各使用單位申請交易系統編號的處理原則，請臺灣世曦列入規劃。

案號	提案單位	Sector/Block	討論議題	會議結論
S1B0-01	KRTC	S1/B0	票證整合使用之票卡、交易記錄檔等文件格式中的所有日期時間格式欄位建議統一採用標準 Unix Time Format 記錄，避免不同發卡單位使用不同的定義，造成無法正確判讀。	1. 交三版統一規劃所有日期時間格式採用臺灣時間的 UNIX Time 格式。 2. 時間位元格式採用 LSB(最低有效位元，least significant bit)。
S1B0-02	FETC	S1/B0	雖已定義為 UNIX Time，但尚無確認各票證業者之 UNIX 的基準為何	
S1B0-03	KRTC	S1/B0	1. 卡片規格版本依照原文定義應有兩者：0x20 與 0x30。 2. 對於 high nibble: main no.與 low nibble: minor no.，建議採用統一規格。	與交三版原規劃相同。
S1B0-04	FETC	S1/B0	建議增加『黑名單指標』 0xFE：黑名單	納入交三版規劃，對於黑名單指標的存取權限將於各扇區存取權限規劃工作會議時再檢視其合理性，
S2B0-01	KRTC	S2/B0~1	電子票值的主要票值與備份票值，建議統一採用標準 Mifare Value Block Format，避免不同發卡單位使用不同的定義，造成卡片無法通用扣值。	納入交三版規劃，電子票值資料長度＝16 個 Byte。
S3B0-01	FETC	S3/B0	此部份 FETC 已使用如下： 鎖卡旗標 Blocked Flag (RM3)：1 進出閘口編號 Entry/Exit ID (RM4)：2 進出閘口時間 Entry/Exit Time：4 保留(Reserve)：2	1. 採納 TSCC 建議，將保留的 9 個 Byte 規劃如下： 鎖卡旗標(黑名單、防偽驗證碼錯誤..)：1 Byte 每日優惠累計轉乘點數：2 Byte 轉乘優惠日期：2 Byte 特種票轉乘優惠點數：2 Byte 加值累計點數：1 Byte 請 TSCC 提供以上欄位規劃的資料，供納入交三版規劃內，並於各扇區存取權限規劃討論時再檢視其合理性。 2. 對於交三版保留欄位的使用必須制定規範，避免各單位各自使用而造成無法整合的結果。

案號	提案單位	Sector/Block	討論議題	會議結論
S3B1-02	TSCC	S3/B1、2	建議： 1. 最近兩筆轉乘群組交易記錄 (1)、(2) 2. <u>轉乘交易序號、交易時間、交易方式代碼、轉乘金額、餘額、轉乘群組、交易場站代碼、設備編號</u>	1. 基於交三版跨區使用的特性，保留最近兩筆交易資料作為前端設備故障時追索的指標有其必要性，故 S3/B1、2 採納 FETC 的建議規劃為「最近兩筆交易記錄」。 2. TSCC 建議的欄位規劃比較適合地區轉乘的用途，可於各票證系統的個別應用區內規劃。 3. 跨區轉乘若有其必要性，可在交三版應用區的「跨系統營運規則控制碼」中再進一步規劃。
S3B1-03	FETC	S3/B1、2	1. Sector 3 Block 1,2 交二版規劃為"最近兩筆封閉系統交易記錄"，因交三版為跨業者之規格，無論是封閉性或非封閉系統皆已在 Sector9~11 已規劃且欄位格式皆相同，無需再重複寫入資料。 2. 考量未來跨業交易時，遺失交易的檢核是一重要問題，此兩欄位應定義為『最近兩筆交易記錄』，無論是加值或扣款記錄皆需寫入交易資料。 3. 在每次交易時，也需將此最近兩筆交易記錄讀出並傳送回後端系統，以做為跨系統遺失交易之檢核。	
S3B1-04	KRTC	S3/B1、2	扇區 3 的最近兩筆封閉交易系統交易記錄與扇區 9、10 的封閉交易系統交易記錄使用定義不明確，建議明確區分定義扇區 3、9、10 各個封閉交易系統交易記錄的使用方式。	
S4B0-01	KRTC	S4B0~3	交易記錄之交易地點，目前長度 1 Bytes，依一般設計邏輯，可以記錄 256 個地點，是否可考量一個跨系統交易時，不同系統間所記錄之交易地點皆適用的方式。	由於各業者的交易地點編碼邏輯不同，若由欄位統一規劃將不敷使用，將於交易系統流程討論時再進一步探討如何透過交易流程的設計來解決此問題。

依本次會議結論增修交三版草案的前後比較如附錄：交三版草案增修前後比較表。

附錄：交三版草案增修前後比較表(依據 97.1.14 會議結論修改)

Sector/ Block	原交三版草案內容	交三版草案增修後內容																																																						
S1/B0	<p>一、發行管理資料：</p> <table border="1"> <thead> <tr> <th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr> </thead> <tbody> <tr> <td>發卡單位編號</td><td>1</td><td>BIN</td></tr> <tr> <td>發卡設備編號</td><td>2</td><td>BIN</td></tr> <tr> <td>發行批號</td><td>2</td><td>BIN</td></tr> <tr> <td>發行日期</td><td>4</td><td>UNIX</td></tr> <tr> <td>有效日期</td><td>4</td><td>UNIX</td></tr> <tr> <td>卡片規格版本</td><td>1</td><td>BIN</td></tr> <tr> <td>卡片狀態</td><td>1</td><td>BIN</td></tr> <tr> <td>檢查碼</td><td>1</td><td>BIN</td></tr> </tbody> </table> <p>1. 發卡單位編號：編號準則請參閱交二版 6.1 節。</p> <p>2. 發卡設備編號：由發卡單位給予其每一個發卡設備的編號。</p> <p>3. 發行批號：由發卡單位對於其發行的每一批卡片所設定的編號。</p> <p>4. 發行日期：卡片發行日期，以卡片發行當天 23 點 59 分 59 秒之時間做記錄。</p> <p>5. 有效日期：卡片有效日期，以卡片有效終止日當天 23 點 59 分 59 秒之時間做記錄。</p>	資料項目	長度 (Byte)	屬性	發卡單位編號	1	BIN	發卡設備編號	2	BIN	發行批號	2	BIN	發行日期	4	UNIX	有效日期	4	UNIX	卡片規格版本	1	BIN	卡片狀態	1	BIN	檢查碼	1	BIN	<p>一、發行管理資料：</p> <table border="1"> <thead> <tr> <th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr> </thead> <tbody> <tr> <td>發卡單位編號</td><td>1</td><td>BIN</td></tr> <tr> <td>發卡設備編號</td><td>2</td><td>BIN</td></tr> <tr> <td>發行批號</td><td>2</td><td>BIN</td></tr> <tr> <td>發行日期</td><td>4</td><td>UNIX</td></tr> <tr> <td>有效日期</td><td>4</td><td>UNIX</td></tr> <tr> <td>卡片規格版本</td><td>1</td><td>BIN</td></tr> <tr> <td>卡片狀態</td><td>1</td><td>BIN</td></tr> <tr> <td>檢查碼</td><td>1</td><td>BIN</td></tr> </tbody> </table> <p>1. 發卡單位編號：編號準則請參閱交二版 6.1 節。</p> <p>2. 發卡設備編號：由發卡單位給予其每一個發卡設備的編號。</p> <p>3. 發行批號：由發卡單位對於其發行的每一批卡片所設定的編號。</p> <p>4. 發行日期：卡片發行日期，以卡片發行當天 23 點 59 分 59 秒之時間做記錄，採用臺灣時間的 UNIX Time 及 LSB(最低有效位元，least significant bit)時間格式。</p> <p>5. 有效日期：卡片有效日期，以卡片有效終止日當天 23</p>	資料項目	長度 (Byte)	屬性	發卡單位編號	1	BIN	發卡設備編號	2	BIN	發行批號	2	BIN	發行日期	4	UNIX	有效日期	4	UNIX	卡片規格版本	1	BIN	卡片狀態	1	BIN	檢查碼	1	BIN
資料項目	長度 (Byte)	屬性																																																						
發卡單位編號	1	BIN																																																						
發卡設備編號	2	BIN																																																						
發行批號	2	BIN																																																						
發行日期	4	UNIX																																																						
有效日期	4	UNIX																																																						
卡片規格版本	1	BIN																																																						
卡片狀態	1	BIN																																																						
檢查碼	1	BIN																																																						
資料項目	長度 (Byte)	屬性																																																						
發卡單位編號	1	BIN																																																						
發卡設備編號	2	BIN																																																						
發行批號	2	BIN																																																						
發行日期	4	UNIX																																																						
有效日期	4	UNIX																																																						
卡片規格版本	1	BIN																																																						
卡片狀態	1	BIN																																																						
檢查碼	1	BIN																																																						

Sector/ Block	原交三版草案內容	交三版草案增修後內容																																	
	<p>6. 卡片規格版本：因加入交三版功能，卡片發行格式化建議明確定義如下。</p> <p>init = 0x20</p> <p>high nibble: main no.</p> <p>low nibble: minor no.</p> <p>交三版 = 0x30</p> <p>7. 卡片狀態：記錄卡片經發卡單位所做的最新發行狀態。</p> <table border="1"> <thead> <tr> <th>狀態項目</th><th>記錄內容</th><th>說明</th></tr> </thead> <tbody> <tr> <td>尚未啟始化</td><td>0x00</td><td>卡片尚未被發卡單位執行啟始化工作</td></tr> <tr> <td>已完成啟始化</td><td>0x01</td><td>卡片已被發卡單位完成啟始化工作</td></tr> <tr> <td>已完成個人化</td><td>0x02</td><td>卡片已被發卡單位完成個人化工作</td></tr> <tr> <td>暫停使用</td><td>0xFF</td><td>卡片已被發卡單位設定為暫停使用</td></tr> </tbody> </table> <p>8. 檢查碼：由發卡單位編號、發卡設備編號、發行批號、發行日期、有效日期、卡片規格版本、卡片狀態資料的每一個位元組做 XOR 的計算後所得到的碼值。</p>	狀態項目	記錄內容	說明	尚未啟始化	0x00	卡片尚未被發卡單位執行啟始化工作	已完成啟始化	0x01	卡片已被發卡單位完成啟始化工作	已完成個人化	0x02	卡片已被發卡單位完成個人化工作	暫停使用	0xFF	卡片已被發卡單位設定為暫停使用	<p>點 59 分 59 秒之時間做記錄，採用 臺灣時間的 UNIX Time 及 LSB(最低有效位元，least significant bit)時間格式。</p> <p>6. 卡片規格版本：因加入交三版功能，卡片發行格式化建議明確定義如下。</p> <p>init = 0x20</p> <p>high nibble: main no.</p> <p>low nibble: minor no.</p> <p>交三版 = 0x30</p> <p>7. 卡片狀態：記錄卡片經發卡單位所做的最新發行狀態。</p> <table border="1"> <thead> <tr> <th>狀態項目</th><th>記錄內容</th><th>說明</th></tr> </thead> <tbody> <tr> <td>尚未啟始化</td><td>0x00</td><td>卡片尚未被發卡單位執行啟始化工作</td></tr> <tr> <td>已完成啟始化</td><td>0x01</td><td>卡片已被發卡單位完成啟始化工作</td></tr> <tr> <td>已完成個人化</td><td>0x02</td><td>卡片已被發卡單位完成個人化工作</td></tr> <tr> <td>暫停使用</td><td>0xFF</td><td>卡片已被發卡單位設定為暫停使用</td></tr> <tr> <td>黑名單指標</td><td>0xFFE</td><td>卡片已被發卡單位設定為黑名單</td></tr> </tbody> </table> <p>8. 檢查碼：由發卡單位編號、發卡設備編號、發行批號、發行日期、有效日期、卡片規格版本、卡片狀態資料的每一個位元組做 XOR 的計算後所得到的碼值。</p>	狀態項目	記錄內容	說明	尚未啟始化	0x00	卡片尚未被發卡單位執行啟始化工作	已完成啟始化	0x01	卡片已被發卡單位完成啟始化工作	已完成個人化	0x02	卡片已被發卡單位完成個人化工作	暫停使用	0xFF	卡片已被發卡單位設定為暫停使用	黑名單指標	0xFFE	卡片已被發卡單位設定為黑名單
狀態項目	記錄內容	說明																																	
尚未啟始化	0x00	卡片尚未被發卡單位執行啟始化工作																																	
已完成啟始化	0x01	卡片已被發卡單位完成啟始化工作																																	
已完成個人化	0x02	卡片已被發卡單位完成個人化工作																																	
暫停使用	0xFF	卡片已被發卡單位設定為暫停使用																																	
狀態項目	記錄內容	說明																																	
尚未啟始化	0x00	卡片尚未被發卡單位執行啟始化工作																																	
已完成啟始化	0x01	卡片已被發卡單位完成啟始化工作																																	
已完成個人化	0x02	卡片已被發卡單位完成個人化工作																																	
暫停使用	0xFF	卡片已被發卡單位設定為暫停使用																																	
黑名單指標	0xFFE	卡片已被發卡單位設定為黑名單																																	

S2/B0~1

一、主要票值：

資料項目	長度 (Byte)	屬性
電子票值	=16	BIN

電子票值：至少可提供 2 Bytes(含)以上的長度記錄電子票值的數額，票值應可提供以加值(Increase)、減值(Decrease)或由票值備份之備份電子票值移轉(Transfer)的方式來做交易處理。

二、票值備份：

資料項目	長度 (Byte)	屬性
備份電子票值	=16	BIN

一、主要票值：

資料項目	長度 (Byte)	屬性
電子票值	≥2	BIN

電子票值：至少可提供 2 Bytes(含)以上的長度記錄電子票值的數額，票值應可提供以加值(Increase)、減值(Decrease)或由票值備份之備份電子票值移轉(Transfer)的方式來做交易處理。

二、票值備份：

資料項目	長度 (Byte)	屬性
備份電子票值	≥2	BIN

S3/B0	<p>一、卡片交易狀態資料：</p> <p>卡片交易狀態資料內容記錄卡片歷次的累積交易狀態資料。</p> <table> <tr> <th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr> <tr> <td>卡片交易序號</td><td>2</td><td>BIN</td></tr> <tr> <td>交易記錄檔指標</td><td>1</td><td>BIN</td></tr> <tr> <td>優惠積點數</td><td>2</td><td>BIN</td></tr> <tr> <td>優惠積點交易序號</td><td>2</td><td>BIN</td></tr> <tr> <td>鎖卡旗標</td><td>1</td><td>BIN</td></tr> <tr> <td>每日優惠累計轉乘點數</td><td>2</td><td>BIN</td></tr> <tr> <td>轉乘優惠日期</td><td>2</td><td>UNIX</td></tr> <tr> <td>特種票轉乘優惠點數</td><td>2</td><td>BIN</td></tr> <tr> <td>加值累計點數</td><td>1</td><td>BIN</td></tr> <tr> <td>保留</td><td>1</td><td>BIN</td></tr> </table>	資料項目	長度 (Byte)	屬性	卡片交易序號	2	BIN	交易記錄檔指標	1	BIN	優惠積點數	2	BIN	優惠積點交易序號	2	BIN	鎖卡旗標	1	BIN	每日優惠累計轉乘點數	2	BIN	轉乘優惠日期	2	UNIX	特種票轉乘優惠點數	2	BIN	加值累計點數	1	BIN	保留	1	BIN	<p>一、卡片交易狀態資料：</p> <p>卡片交易狀態資料內容記錄卡片歷次的累積交易狀態資料。</p> <table> <tr> <th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr> <tr> <td>卡片交易序號</td><td>2</td><td>BIN</td></tr> <tr> <td>交易記錄檔指標</td><td>1</td><td>BIN</td></tr> <tr> <td>優惠積點數</td><td>2</td><td>BIN</td></tr> <tr> <td>優惠積點交易序號</td><td>2</td><td>BIN</td></tr> <tr> <td>保留</td><td>9</td><td>BIN</td></tr> </table>	資料項目	長度 (Byte)	屬性	卡片交易序號	2	BIN	交易記錄檔指標	1	BIN	優惠積點數	2	BIN	優惠積點交易序號	2	BIN	保留	9	BIN
資料項目	長度 (Byte)	屬性																																																			
卡片交易序號	2	BIN																																																			
交易記錄檔指標	1	BIN																																																			
優惠積點數	2	BIN																																																			
優惠積點交易序號	2	BIN																																																			
鎖卡旗標	1	BIN																																																			
每日優惠累計轉乘點數	2	BIN																																																			
轉乘優惠日期	2	UNIX																																																			
特種票轉乘優惠點數	2	BIN																																																			
加值累計點數	1	BIN																																																			
保留	1	BIN																																																			
資料項目	長度 (Byte)	屬性																																																			
卡片交易序號	2	BIN																																																			
交易記錄檔指標	1	BIN																																																			
優惠積點數	2	BIN																																																			
優惠積點交易序號	2	BIN																																																			
保留	9	BIN																																																			

S3/B1、2	<div>二、最近兩筆封閉系統交易記錄：</div> <div>記錄最近兩筆持卡人搭乘交通運輸載具的卡片交易記錄，可作為封閉式系統“IN”的交易操作記錄，以作為“OUT”的交易參考，並且“IN”“OUT”的交易操作記錄也可作為不同應用系統間連續交易行為“轉乘優惠”的參考依據。該最近兩筆封閉系統交易記錄不包括票值加值的記錄。</div> <div>最近兩筆封閉系統交易記錄每筆交易的記錄內容如下：</div> <table><tr><th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr><tr><td>交易序號</td><td>1</td><td>BIN</td></tr><tr><td>交易時間</td><td>4</td><td>UNIX</td></tr><tr><td>交易類別</td><td>1</td><td>BIN</td></tr><tr><td>交易票值/票點</td><td>2</td><td>BIN</td></tr><tr><td>交易後票值/票點</td><td>2</td><td>BIN</td></tr><tr><td>交易系統編號</td><td>1</td><td>BIN</td></tr><tr><td>交易地點/RSU編號</td><td>1</td><td>BIN</td></tr><tr><td>交易機器/OBU編號</td><td>4</td><td>BIN</td></tr></table>	資料項目	長度 (Byte)	屬性	交易序號	1	BIN	交易時間	4	UNIX	交易類別	1	BIN	交易票值/票點	2	BIN	交易後票值/票點	2	BIN	交易系統編號	1	BIN	交易地點/RSU編號	1	BIN	交易機器/OBU編號	4	BIN
資料項目	長度 (Byte)	屬性																										
交易序號	1	BIN																										
交易時間	4	UNIX																										
交易類別	1	BIN																										
交易票值/票點	2	BIN																										
交易後票值/票點	2	BIN																										
交易系統編號	1	BIN																										
交易地點/RSU編號	1	BIN																										
交易機器/OBU編號	4	BIN																										
	<div>二、最近兩筆交易記錄：</div> <div>記錄最近兩筆持卡人搭乘交通運輸載具的卡片交易及加值記錄，在每次交易時，需將此最近兩筆交易記錄讀出並傳送回後端系統，以做為跨系統遺失交易資料之檢核。</div> <div>最近兩筆交易記錄每筆交易的記錄內容如下：</div> <table><tr><th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr><tr><td>交易序號</td><td>1</td><td>BIN</td></tr><tr><td>交易時間</td><td>4</td><td>UNIX</td></tr><tr><td>交易類別</td><td>1</td><td>BIN</td></tr><tr><td>交易票值/票點</td><td>2</td><td>BIN</td></tr><tr><td>交易後票值/票點</td><td>2</td><td>BIN</td></tr><tr><td>交易系統編號</td><td>1</td><td>BIN</td></tr><tr><td>交易地點/RSU編號</td><td>1</td><td>BIN</td></tr><tr><td>交易機器/OBU編號</td><td>4</td><td>BIN</td></tr></table>	資料項目	長度 (Byte)	屬性	交易序號	1	BIN	交易時間	4	UNIX	交易類別	1	BIN	交易票值/票點	2	BIN	交易後票值/票點	2	BIN	交易系統編號	1	BIN	交易地點/RSU編號	1	BIN	交易機器/OBU編號	4	BIN
資料項目	長度 (Byte)	屬性																										
交易序號	1	BIN																										
交易時間	4	UNIX																										
交易類別	1	BIN																										
交易票值/票點	2	BIN																										
交易後票值/票點	2	BIN																										
交易系統編號	1	BIN																										
交易地點/RSU編號	1	BIN																										
交易機器/OBU編號	4	BIN																										

「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」

第八次技術討論會紀錄

一、開會時間：九十七年一月三十一日(星期四)上午十時

二、開會地點：臺灣世曦公司百世大樓二十四樓會議室

三、主持人：王穆衡組長

記錄 許安慶

四、出席單位及人員：略

五、簡報：略

六、結論：

1. 議題一：交三版草案增修前後比較(依據 97.1.14 會議結論修改)

決議：與會代表若對 CECI 前次會議紀錄及修訂前後之內容認為有修改之必要，請會後知會 CECI 修訂。

2. 議題二：交三版應用資料區討論

決議：對於臺灣智慧卡公司所提出之交三版應用資料區規劃建議(如附錄)，因為會議時間有限，各與會代表恐無法當場詳細研讀及回應，請各與會代表攜回研討後，於下次開會之前將意見送達 CECI 彙整，並列為下次工作會議的討論重點。

3. 議題三：交三版各扇區存取權限討論

決議：本次會議討論重點為共同資料區 Sector 0~ Sector 5，其中

- (1) Sector 2 KeyB2' 的存取權限經討論修改後如下：

Sector	Block	KeyA2'				KeyB2'			
		R	W	I	D	R	W	I	D
2	0 主要票值	V			V	V		V	V
	1 票值備份	V			V	V		V	V
	2 票值加值記錄	V			V	V	V		
	3 KeyA2' AC KeyB2'								

- (2) Sector 2/Block 0「卡片交易狀態資料」的第7個資料項目「轉乘優惠日期」的屬性修改為「DOS」。

「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」

第九次技術討論會紀錄

一、開會時間：九十七年二月二十日(星期三)下午二時

二、開會地點：運輸研究所十樓會議室

三、主持人：王穆衡組長

記錄 許安慶

四、出席單位及人員：略

五、簡報：略

六、結論：

議題一：票種/票卡欄位規劃

決議：請 CECI 在「特殊身分」欄位規劃上，要應用樹狀型分析法，將各縣市政府(包含所轄鄉鎮公所)的補助單位代碼，有系統地予統一分類及彙整，供未來各票證發卡組織遵循。

議題二：交三版應用資料區兩個封閉系統應分別對應至「連續性封閉系統」以及「非連續性封閉系統」

決議：若將 S9 改為「連續性封閉系統」，S10 改為「非連續性封閉系統」，在規劃上仍應在「連續性封閉系統」及「非連續性封閉系統」的區塊上各保留兩筆 IN 及 OUT 的交易記錄欄位，以作為各封閉系統與開放系統間交織使用之需。

議題三：減少重複的個別應用交易資料記錄。

決議：此部份將於交易流程規劃時逐項檢視各區塊可再精簡的欄位。

議題四：建議建立錯誤回復機制

決議：錯誤回復機制有其存在之必要性，TSCC 對於此部份的規劃及應用有豐富的經驗，請 CECI 了解是否能在不影響 TSCC 商業機密的情況下，參用 TSCC 此部份機制之可行性。

議題五：減值設備將前二筆交易送至後台之規畫重新檢討。(最近兩筆交易紀錄，S3/B1、2)

決議：請 CECI 先研究此二欄位存在之必要性，及其他欄位可替代的可行性，再進一步決定應放什麼資料。。

臨時動議：

第八次工作會議紀錄議題三，因筆誤將(1)「票值加值記錄」KeyA2' "D" 誤植打"V"；(2) Sector 3誤植為Sector 2。

修改後如下：

(3) Sector 2 KeyB2'的存取權限經討論修改後如下：

Sector		Block			KeyA2'				KeyB2'			
					R	W	I	D	R	W	I	D
2	電子票值	0	主要票值		V			V	V		V	V
		1	票值備份		V			V	V		V	V
		2	票值加值記錄		V			.	V	V		
		3	KeyA2'	AC	KeyB2'							

(4) Sector 3/Block 0「卡片交易狀態資料」的第7個資料項目「轉乘優惠日期」的屬性修改為「DOS」。

「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」

第十次技術討論會紀錄

一、開會時間：九十七年三月十日(星期一)上午十時

二、開會地點：運輸研究所十樓會議室

三、主持人：王穆衡組長

記錄 許安慶

四、出席單位及人員：略

五、簡報：略

六、結論：

1. 因大部份票證公司目前均已自行規劃使用錯誤回復機制，為使交三版規格能達到共通的目的，交三版應統一錯誤回復機制。
2. 對於 CECI 所提之錯誤回復機制，因 TSCC 於營運上有實際的案例顯示，系統有可能因為 bug 而將整個 BLOCK 覆蓋為 0 值，故應將(S3B0)的"上筆卡片交易狀態資料"及"上上筆卡片交易狀態資料"以及配對指標(S11B0)的"上筆備份配對記錄指標"及"上上筆備份配對記錄指標"分別置放在不同的 BLOCK。
3. 交三版的欄位規劃討論預計於下次會議後告一段落，若各票證公司對於 CECI 目前所規劃的內容有所建議，請於 3 月 20 日前提供意見供 CECI 參考。
4. 請 CECI 下次會議提出交三版的交易流程及各種編碼的統一編寫格式。

「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」

第十一次技術討論會紀錄

一、開會時間：九十七年四月一日(星期二)上午十時

二、開會地點：運輸研究所十樓會議室

三、主持人：王穆衡組長

記錄 許安慶

四、出席單位及人員：略

五、簡報：略

六、討論事項

1. 交三版(草案)與交二版修訂前後比較

- (1) S9 及 S10 區分為「軌道型連續性封閉交易系統」及「公路型連續性封閉交易系統」會造成未來系統適用性的限制，應依照「進出相同驗票機」及「進出不同驗票機」的規劃本意重新思考合適的名稱。
- (2) S9~S11 有關旅遊票的規劃，因該票種屬於行銷或臨時性的卡種，應由各票證公司自行規劃，不宜納入交三版規範內。
- (3) S1B0「黑名單指標」與 S3B0「鎖卡旗標」的區別及如何搭配使用請 CECI 再補充說明。
- (4) S1B2「防偽驗證碼」第一段由共通金鑰認證，因目前尚未討論共通金鑰的做法，建議先行刪除此規劃，待共通金鑰的處理機制確定後再行規劃，或由票證公司依照其安全機制規定自行規劃。
- (5) S10B0「上/下站代碼」為 2 個 Byte，S10B1~2 則為 1 個 Byte，請 CECI 再補充說明其用法。
- (6) S11B0 規劃為「A」、「B」兩個部份的目的及使用方法請 CECI 再補充說明。

(二) 交易流程設計參考

- (1) 主要流程中各個步驟應再區分「不可變更」及「可變更」兩部份，「不可變更」係指一旦變更此流程就無法達成票證整合的目的，

「可變動」則可由各票證公司自行規劃。

(2) 主要流程中「是否使用優惠補助票種」及「優惠補助票種作業」的相關流程在邏輯上似不夠明確，請 CECI 再補充必要的流程。

(3) 卡片寫入流程的部份說明不夠明確，請 CECI 再補充說明。

(三) 編碼準則

(1) 請 CECI 提出編碼的邏輯，才能有效率地使用有限的欄位。

(四) 臨時動議(TSCC 建議事項)

(1) 為顧及原持卡人的權益，票證整合方案仍建議將「設備整合」方案一併納入考量。

(2) 交三版相關配套「執行作業」及「方式」宜先進行討論及研議並經驗證其「技術可行性」後再行公佈。

(3) 交三版之內容如有涉及智慧財產權或機密之資料，應先釐清後再行納入。

七、主席結論：

1. 交三版與交二版的延續性及差異比較請 CECI 以現有的版本為基礎再補充說明。

2. 交三版規劃的是卡片共通所必要的規範及功能，對於必須要政策配合才能執行的部份應區隔不列入，屬於必須再協商或有爭議的規劃內容，則請 CECI 再斟酌列為建議事項或删除。

3. 交三版在規劃上要有層次，所有票證公司必須共同遵守才能票卡互通的規範要明確定義，屬於參考性質的規範則可模糊化以避免不必要的爭議。

4. 有關退卡票別的規劃請 CECI 確認是否抵觸「電子票證定型化契約」的相關規定，不能影響民眾的權益。

5. 針對 TSCC 的建議事項，主席結論如下：

(1) 交三版規劃是經過與會代表多次討論之後的結果，內容若有涉及侵犯與會廠商的智慧財產權或機密，請事先提出以免規劃單位在不知覺的情況下誤觸法令，也避免在公告之後才發生法律爭議。

- (2) 交三版規劃是否經過驗證的程序以認定可行才發佈，由交通部決定。
 - (3) 票證整合所需的經費補助及配套措施，運研所與 CECI 已研擬推動計畫及構想，並奉部指示陳報作業中。
6. 各與會單位若對交三版草案的內容還有建議，請在會後一星期內送 CECI 彙整檢討。

「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」

第十二次技術討論會紀錄

一、開會時間：九十七年五月七日(星期三)上午十時

二、開會地點：運輸研究所十樓會議室

三、主持人：王穆衡組長

記錄 許安慶

四、出席單位及人員：略

五、簡報：略

六、討論事項

1. 票證整合預算概估

- (1) 若交三版頒定過程順利，遠通電收及臺灣智慧卡公司應可在今年底完成票證整合；高雄捷運表示在與其建置廠商簽約後估計一年應可完成軟硬體系統修改，至於與廠商協商確認所需時間另計；臺灣高鐵公司因須與國外建置廠商討論修改內容，由於討論內容尚未確定，目前期程與經費無法評估。
- (2) 本次會議各單位所提出的票證整合預算為一概括的估算金額，係提供交通部決策參考，部份公司因現有設備設計限制多，因此初估整合經費龐大，未來是否能足額對應支持，將由交通部綜合考量決定，惟後續若能編列預算執行補貼，補貼的方式將一視同仁，各單位的做法可自行規劃提出，經本部審查確認後執行。
- (3) 臺北智慧卡公司建議本年度補助的票證整合經費，不應僅限於採用交三版整合方案的計畫，對於各票證公司自行採用其他整合方式的計畫亦請考量予以補助。

2. 交三版草案內容修訂

- (1) 交三版中複合式雙介面卡的資料欄位規劃將以符合交二版的「南區交通 IC 卡—TaiwanMoney 卡」為參考範例，各發卡組織可自行參酌規劃。
- (2) 遠通電收建議「票值管理資料(S1B1#11)」中「退卡票別」的欄位

恢復為交二版原先規劃的「檢查碼」，以增加票卡資料的安全性，「退卡票別」因各發卡組織營運規則不同，由發卡組織自行規劃，以上建議經討論後同意修改。

3. 票證整合方案討論

- (1) 臺北智慧卡公司提出票證整合涉及營運整合及技術整合等層面，智慧卡首重「安全」問題，若採交三版方案整合，每家營運業者共用共管部份的扣款金鑰，此可能衍生「偽卡」發生之疑慮，如管理機制不當，可能進而導致無法確認其原因及稽核之重大安全問題。
- (2) 臺北智慧卡公司提出票證整合短期如採用「設備整合」方案，將較有機會達成年底一卡通之目標，該公司已完成悠遊卡、TAIWAN MONEY 卡和高捷 I PASS 於同一設備之技術整合驗證工作，「設備整合」方案希望一併納入票證整合方案中。
- (3) 臺北智慧卡公司建議一卡通整合應尊重市場機制，交通部不宜強制代為指定方案，及指定期限完成，因此，對採用交三版的票證整合方案仍持保留意見。
- (4) 會中對於臺北智慧卡公司所提建議，基本予以尊重，惟設備整合仍將涉及各公司保密系統互置，安全顧慮與卡片格式整合模式類似，另該構想由各公司自行配對整合，仍無法實現一卡通環境，且後續每增加一系統納入整合，則系統更新必須重覆投入，可能導致投資浪費，因此各有其利弊得失。

七、主席結論：

1. 票證整合的金鑰及資訊安全等議題並非目前制定交三版資料欄位格式的範圍，本部分牽涉各營運系統內部作業，應由營運業者另闢會議再進一步討論。
2. 交三版草案內容經多次討論後各單位意見已趨一致，將於本次會議後由運研所與 CECI 就草案內容做最後檢核後報部。
3. 由於目前部分業者對於交三版票證整合方案仍有疑慮，故建議交通部本年度先進行交三版方案 pilot test 的補助計畫，目前已有遠通電收公司與臺灣智慧卡公司的交三版票證整合方案提出規劃，未來實際推動

與執行時，鼓勵其他票證公司亦可加入測試，本測試計畫至少需完成或測試以下項目：

- (1) 發行符合交三版規格之卡片
 - (2) 跨公司合作在安全機制上的可行方式
 - (3) 跨公司合作的營運作業規章訂定
4. 因應臺北智慧卡公司所提出的前端設備整合方案未來或可與本部目前推動之交三版卡片整合模式整合，即建議交通部未來在補助新的驗票設備建置時，SAM 卡插槽除考量交三版 SAM 之執行為必要外，必須預留足夠插槽供其他票證系統互置 SAM 卡整合使用，以保留卡片整合與設備整合兩種方案供參考選擇之空間。
 5. 請 CECI 就遠通公司及高雄捷運公司所提出的票證整合方案，摘要納入提送給交通部之一卡通計畫短期分案與作業預算初估報告，並將本會議各公司(含臺北智慧卡公司)的提報內容作為報告附件統一提送。

「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」

第十三次技術討論會紀錄

一、開會時間：九十七年七月十七日(星期四)上午十時

二、開會地點：臺灣世曦工程顧問公司智慧運輸部五樓會議室

三、主持人：許安慶正工程師

記錄 許安慶

四、出席單位及人員：略

五、簡報：略

六、討論事項

1. 遠通電收所提金鑰衍生機制、防偽驗證碼產生機制，主要考量三個重點，金鑰長度要夠長、演算速度要夠快、演算法則要夠新夠強，因此採用 AES 演算法則。
2. 遠通電收所建議之卡片防偽驗證碼產生以及驗證機制，可為兩階段認證模式，即前端及後端皆可進行卡片驗證。
 - (1) 前端驗證：各家票證業者於前台驗票設備中，使用演算法則及相同金鑰進行前端卡片驗證，當新增其他票證業者卡片時，可達不召回設備之目的。
 - (2) 後端驗證：傳回之卡片防偽資料，再由發卡單位之後台使用另一把金鑰進行驗證。
3. 上述防偽驗證碼驗證機制，於技術上乃屬可行之建議，然而尚有一些安全性上之考量需進行修改：
 - (1) 當前台驗票設備已驗證該卡片為"真"，且已提供相對應之服務，但是如果發卡單位後台驗證為"偽"時，則發卡單位與收單位易有資料判定問題。
 - (2) 防偽驗證碼隨著交易紀錄回傳回後台以供驗證，將會造成系統安全性上的問題，因回傳機制的每一個環節皆有可能被攔截資料，造成防偽驗證碼洩漏的風險。
4. 遠通電收所提金鑰衍生機制建議使用 AES 演算機制搭配卡片卡號以

及 128bit 金鑰來進行，此一作法考量金鑰演算速度、保密性以及演算法的新穎性來做建議，實務上確實可行。

5. 目前各票證業者金鑰及防偽驗證碼之演算法有多種，故建議可列舉一些常使用之演算法，讓各家票証業者選擇，待大家決定一種後再進行確認。
6. 下次工作會議討論議題
 - (1) 若每家業者皆使用不同之防偽驗證碼產生金鑰，將導致若已發行交三版卡片的業者於第三家業者要加入時，所有的驗票設備皆需更換新的交三版 SAM 卡,用以產生新加入新第三家業者之防偽驗證碼產製金鑰，故防偽驗證碼是否應統一？
 - (2) 防偽驗證碼之檢驗只需於前台驗票設備中進行檢驗，是否有必要回傳至後台？可否建立開放各家後台選擇需驗或不需驗的機制？
 - (3) 針對目前常用的三種金鑰衍生演算法(DES 演算法、AES 演算法、Triple-DES 演算法)加以討論，以確認交三版建議應採用的演算法。

「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」

第十四次技術討論會紀錄

一、開會時間：九十七年八月二十一日(星期四)上午十時

二、開會地點：交通部運輸研究所十樓會議室

三、主持人：王穆衡組長

記錄 許安慶

四、出席單位及人員：略

五、簡報：略

六、決議事項

1. 請 CECI 對於全國票證整合的技術策略做全盤的考量，規劃短中長期應完成的階段任務，及與前後階段的銜接性。
2. 減值金鑰及防偽驗證碼是否應統一，除考慮安全性之外，亦應一併考量置換 SAM 卡的經費及作業的困難度，例如防範的對象是內部員工，則應考慮是否藉由建立嚴密的內部控管機制加以防範，如此就可免除新加入票證整合者必須重覆換置 SAM 卡的問題，請 CECI 於下次工作會議中提出具體的建議方案。
3. 防偽驗證碼之檢驗只需於前台驗票設備中進行檢驗，是否回傳至後台驗證開放由各票證公司自行決定。
4. 交三版金鑰衍生演算法經與會代表討論後，建議採用 AES 演算法。
5. 「產生防偽驗證碼建議流程」及「驗證防偽驗證碼建議流程」中的 Issuer Code 經與會代表討論後建議可不列入流程參數內。
6. 本年度因為預算編列的問題，在無政府預算支援的情況下，請 CECI 彙整交三版票證整合試辦計畫在年底前可達到的成果，並於期末報告說明詳細作法與初步測試成果。
7. 請 CECI 收集國外不同交通電子票證系統整合的技術方案及適用環境以供本研究參考。

「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」

第十五次技術討論會紀錄

一、開會時間：九十七年九月十一日(星期四)上午十時

二、開會地點：交通部運輸研究所十樓會議室

三、主持人：黃立欽研究員代理

記錄 許安慶

四、出席單位及人員：略

五、簡報：略

六、決議事項

1. 議題一第七點：「為提供未來可能發生的洩密事件，故建議仍需事先規劃完整的換 Key 作業。」，請 CECI 提出具體的標準作業流程(SOP)建議以供相關業者參考。
2. 請萬事達卡國際組織提供 Dual Interface Card 對於卡片安全機制內部控管建議供 CECI 作為本研究之參考。
3. 議題二：「交三版驗證系統卡片安全機制規劃與討論」，與會代表沒有異議，請 CECI 依照規劃內容持續開發交三版驗證系統。該系統預計於 10 月中旬完成，屆時將邀請有意參與驗證測試的廠商開始進行模擬測試。
4. 有關交通部請運研所協調遠通電收公司與臺灣智慧卡公司 97 年度交三版卡片小規模實做及測試計畫經費部分，請上述業者於一星期內提出修正計畫交由 CECI 彙整後，轉請 運研所報部辦理。
5. 遠通電收建議交通部能對其主管機關高速公路局說明一卡通之政策，以請其主管機關本於權責協助辦理推動乙案，請 CECI 於下次技術工作會議時邀請高速公路局出席，俾使其充分了解工作進度並配合交通部政策辦理。
6. 有關後台清算模組部分，運研所將協助了解科顧室委請資策會開發的清算平台模組如何提供給票證整合的業者使用，以節省業者的整合成本。

7. 請 CECI 於下次會議提出交三版驗證系統的 SOP 及測試個案內容，以讓有意參與驗證的廠商提早準備配合。
8. 遠通電收提出參與交三版驗證時 S1B0「交三版版本定義」將暫時以 0x02 代替 0x3X；以及建議將 S3B0 的「0x01：卡片可合法使用」改為「0x00：卡片可合法使用」，「0x02：卡片因某種因素暫時無法使用」改為「0x01：卡片因某種因素暫時無法使用」，因上述變更並不違背交三版的精神與邏輯，與會代表均無反對意見，請 CECI 先行將修正版本 mail 給各票證公司確認後，再列入下次工作會議報告正式確認。

「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」

第十六次技術討論會紀錄

一、開會時間：九十七年十月二十日(星期四)上午十時

二、開會地點：交通部運輸研究所十樓會議室

三、主持人：黃立欽研究員代理

記錄 許安慶

四、出席單位及人員：如簽到表

五、簡報：略

六、決議事項

1. 交三版靜態資料驗證軟體已完成實體測試，請有意參與測試的票證組織，於本年度研究計畫期末報告完成前與 CECI 聯絡，以便安排靜態資料驗證作業。
2. 明年度的研究計畫重點為交三版卡片測試計畫，但不包括設備建置之補助。請 CECI 與有意參與交三版卡片測試之實質營運票證組織組成合作團隊並於 11 月中旬前提出明年度之工作計畫書。
3. 請 CECI 參考臺灣智慧卡公司的建議，於明年度計畫中研討制定電子票證驗票機硬體規範之可行性。
4. 一卡通政策是否持續推動仍將視部裡的政策而定，本研究計畫將配合政策彈性調整未來工作項目。
5. 「電子票證發行管理條例(草案)」刻正由行政院金管會審議中，雖條文中主管機關明訂為行政院金管會，交通部如認為「交通電子票證一卡通」為既定之政策目標，仍會編列相關預算並透過地方政府補助相關票證公司或營運組織配合辦理，不因主管機關非為交通部而有所變動，未來仍應視政策走向而定。

附錄 2

期中報告審查意見回覆表

期中報告審查意見回覆表

一、開會時間：九十七年七月十四日上午十時

二、開會地點：運研所五樓會議室

三、主持人：王組長穆衡

記錄 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
萬事達卡國際 組織	期中報告中所提及驗證機制，在 Dual interface Card 部分應如何驗證？	本期礙於技術及經費之考量，先以目前電子票證主流 Mifare 卡片為驗證標的，明年度將再視 Dual Interface 的技術是否足以形成產業共同規範並考量經費之後再研究如何驗證。	同意研究單位處理情形
	有關票證整合之現況說明，並未具體反映 TaiwanMoney 卡與高捷卡整合後之相關數據，請予以更新。	已補充於 2.1 節(P2-4)。	同意研究單位處理情形
高雄捷運	高雄捷運一卡通之資料尚未更新，請研究單位予以修正。	已更新於 2.1 節(P2-5)。	同意研究單位處理情形
	本公司自今年八月起將開始發行校園卡及聯名卡，以擴大卡片使用範圍。	敬悉	同意研究單位處理情形
遠通電收	本公司與臺灣智慧卡公司正積極以交三版卡片格式進行票證整合工作，預計應可於年底前完成。	敬悉	同意研究單位處理情形
	在進行整合過程中，對於交三版的部份規範及參數定義等有須部分修改之建議，在小規模實作計畫完成後，再提送給臺灣世曦公司參考修訂。	將待遠通公司實作計畫完成、提送修改建議後再行修訂相關規範與參數。	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
	對於交三版卡片之驗證方法部分，本公司未來亦可提供相關實務經驗供參。	敬悉	同意研究單位處理情形
臺灣智慧卡公司	請研究單位更新本公司發卡數量及營運現況資料。	已更新於 2.1 節(P2-4)。	同意研究單位處理情形
	建議電子票證整合作業應由上級主管機關政策引導推動才能較有成效，並可縮短整合時程。	有關政府應協助事項已建議於 6.1 及 6.2 節。	同意研究單位處理情形
臺北智慧卡公司	請研究單位更新本公司營運現況資料。	已更新於 2.1 節(P2-2~3)。	同意研究單位處理情形
	有關本公司對於交三版草案之意見，在前幾次會議中均已充分表達，本公司於本次會議中不再表示意見。	敬悉	同意研究單位處理情形
宏碁公司	本公司今年度已與臺灣世曦公司合作，有關本計畫技術支援之部分，將配合該公司辦理。	敬悉	同意研究單位處理情形
高鐵公司	對於初期以驗票閘門進行設備整合之方式，對本公司而言尚有困難，且本公司尚未正式發卡，因此，與臺北智慧卡公司的整合方式，將以獨立驗票機裝置於人工閘門並佐以人員輔助方式進行。	敬悉	同意研究單位處理情形
臺鐵局	本局與臺北智慧卡公司試辦之悠遊卡於臺鐵北部 4 站使用計畫，自 97 年 6 月 20 日至 7 月 13 日為止，初步估計每天使用人次約有 5,000 人次。	敬悉	同意研究單位處理情形
	有關基隆至中壢間之試辦計畫，預訂於 8 月上旬即可於臺鐵 19 個站間使用，此區間每天使用之人次約 14 萬。預期未來悠遊卡使用量應會大幅成長。	臺鐵之悠遊卡試辦計畫說明於 P2-3。	同意研究單位處理情形
高鐵局	請問設備整合的定義為何？例如臺北智慧卡公司即將與臺灣高鐵公司試辦於公務門(或人工閘門)設置獨立驗票機之計畫，是否係	設備整合之定義及模式已於本研究計畫前期期末報告第四章中說明。	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
	屬設備整合？請研究單位說明。		
王瑞民教授	建議臺灣高鐵公司除與臺北智慧卡公司合作外，應與臺灣智慧卡公司及遠通電收公司合作，使各地區使用電子票證之民眾均能於高鐵站使用。	敬悉	同意研究單位處理情形
	扣款金鑰衍生邏輯的完成期限為何？與票證整合計畫之密切性請再予說明。	(1).依照本研究規劃之期程必須於8月中旬之前確定，預計7月下旬及8月上旬召開第13、14次工作會議定案。 (2).扣款金鑰衍生邏輯對ISAM的發行有密切的關係，若無法確認扣款金鑰衍生邏輯，意謂交三版的卡片無法順利發行及驗證。	同意研究單位處理情形
	跨系統的清算後台如交由臺鐵局建置，未來公告時如何訂出資格條件，使各票證公司均能夠參與而不被排除？請研究單位再予說明。	建議臺鐵局可依照政府採購法及審議中之金管會「電子票證發行管理條例」相關規定訂定資格條件。	同意研究單位處理情形
	有關記名卡是否納入交三版規範可再研究，究竟交通卡與校園卡之使用，是否有隱私或個人資料外洩之問題，請再加以說明。	(1).交三版草案第一扇區第一區塊(S1B1)「票值管理資料」已規劃記名卡所需之識別欄位。 (2).是否有隱私或個人資料外洩之問題將於期末報告提出說明及建議。	同意研究單位處理情形
施嫩嫩副總工程師	高雄捷運已通車營運，捷運一卡通並已發行，P2-2表2.1-1及P2-16表2.2-2部分請增列一卡通相關資料。	已更新於2.1節。	同意研究單位處理情形
	P2-11僅略述高雄捷運一卡通，並未敘述發行張數，請予以補列。	已補充於2.1節(P2-5)。	同意研究單位處理情形
	2.1節資料請研究單位更新，如P2-8至P2-10均採96年7月資料；P3-9圖3.4.1-1特別票種處理，於高雄捷運統稱優惠記名卡，含	已更新於2.1節。	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
	敬老卡、博愛卡(身心障礙人士)、博愛陪伴卡，後續將推出仁愛卡(低收入戶)。		
	為期本計畫獲致實質效益，建請研訂短期達成票證整合之具體作為，以為中、長期推動之基石，而本報告 P4-20 表 4.2-1 可作為短期試辦計畫，並建議訂定完成時程。	目前國內正推動的票證整合實作計畫有二，一為遠通電收與臺灣智慧卡合作的交三版整合試辦計畫，一為悠遊卡與高雄捷運的前端設備整合試辦計畫，詳見第五章。	同意研究單位處理情形
	P4-21，4.2 節「四、成立電子票證跨系統清算交換中心」說明「該中心為票證整合能否實踐之關鍵，預期短期(一年)內成立與運作並不樂觀」，建請規劃單位研擬該中心成立之相關流程，並於各步驟中估列期程，俾供了解全貌。	說明如 6.2 節。	同意研究單位處理情形
	P4-21，4.2 節「四、成立電子票證跨系統清算交換中心」說明「該中心將為一獨立於各家交通電子票證公司之機構，短期建議由目前已具有票證清算能力之公司進行」，請規劃單位了解目前已具有票證清算能力之公司有幾家？另未來如何由目前已具有票證清算能力之公司，轉為一獨立於各家交通電子票證公司之機構，請一併提出建議。	說明如 6.2 節。	同意研究單位處理情形
林佐鼎教授	交三版中最近兩筆與最近六筆資料與異機進出、同機進出的記錄是否有重覆的問題？請再予說明。	最近兩筆交易資料主要供電子票值演算參數之用；最近六筆交易資料主要供持卡人查詢之用。詳細說明如交三版草案第三~五扇區。	同意研究單位處理情形
	在卡片格式規劃中，發卡單位重覆出現在不同的欄位，是否有必要？	發卡單位出現在不同欄位係為縮短交易流程，若只規劃在一個欄位，交易的檢核流程反而會更複雜。	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
	最近兩筆交易記錄中第 7、8 欄位的資料如何遞補？請再予說明。	此二欄位採先進先出方式覆蓋，不斷更新最新資料。	同意研究單位處理情形
本所王穆衡組長	雖然部份公司對於交三版仍有顧慮，但是交通部推動交三版卡片之方向已確定不變，未來將先推動小規模實做計畫予以驗證，再就交三版卡片格式部分內容予以修正，並召開會議討論頒布事宜。	敬悉	同意研究單位處理情形
	交通部已訂於 7 月 22 日召開電子票證整合協調會議，以確定後續推動期程，請有意參與票證整合小規模實做計畫的票證公司提出具體的計畫內容，以及可於本年度內完成之時程規劃與經費概算，並請於近日內交由臺灣世曦公司彙整。	本公司已於 7 月 30 日交通部召開之電子票證整合協調會議中，提出各公司本年度之票證整合試辦計畫。	同意研究單位處理情形
運輸研究所運輸經營管理組	有關第二章現況分析部份，請增加國外有關卡片技術規範之最新現況及整合應用情形，另有關 4K 卡與 1K 卡是否相容使用之資訊亦請一併蒐集。	(1) 說明如 2.2 節。 (2) 另本研究所蒐集之案例尚無以 4K 卡與 1K 卡同時應用於同一交通卡系統之情形。	同意研究單位處理情形
	有關 P3-12 註 1 部份，其中「遠東電收」請修正為「遠通電收」。	已修正。	同意研究單位處理情形
	有關 P4-2 一、資料準備之 2.票卡部份，其中老人為何區分成 70 歲以上及 65-70 歲兩種類別，請加以說明。	因各地方政府或客運公司對老人乘車優惠的年齡規定不同，有些規定為 65 歲以上，有些則為 70 歲以上，故必須於票卡標記中予以區格以利辨別。	同意研究單位處理情形
	有關 P4-1 交三版卡片驗證機制之規劃，應將驗證之目的、驗證程序中相關金鑰可能涉及公司業務機密部分等可能面臨之關鍵性問題予以述明，俾便未來驗證程序之執行。	驗證機制之目的敘述於 P4-1，金鑰的管理問題說明於 P7-2。	同意研究單位處理情形
	有關 P4-1 圖 4.1.1-1 交三版驗證申請作業流程，請將各階段應備文件及程序納入重新繪製流程圖，	已更新流程圖。	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
	俾能清楚了解。		
	有關 p4-3 第 6 行「5000 元的電子票值」應修正為「5000 元的『虛擬』電子票值」。	已修正。	同意研究單位處理情形
	有關 p4-4 中倒數第 3 行，「建議使用飛利浦公司發行之 Mifare 1k 卡片作為驗證系統中之標準非接觸式 IC 卡」之原因應予述明，另 P4-5 第 3 行及第 6 行情形亦應同時予以說明。	已補充說明於 P4-4 及 4-5。	同意研究單位處理情形
	有關 p4-5 中第 8 行，三、驗證系統程式可分為卡片靜態資料及卡片動態資料兩部份，請補充說明兩部份驗證之目的及差異性。	已補充說明於 P4-5。	同意研究單位處理情形
	P4-6 倒數第 4 行，PCSC 接觸式讀卡模組意義為何？請補充說明。	已補充說明於 P4-7。	同意研究單位處理情形
	P5-3 倒數第 5 行，交通部於 96 年研擬「預付型交通電子票證定型化契約應記載及不得記載事項」(草案)，該案已於 97 年 4 月 1 日正式頒布施行，請予修正。	已修正，詳見 6.2 節。	同意研究單位處理情形
	P5-4 之「五、法規研擬建議與配套措施」，目前金管會正就丁守中立法委員所提之「電子票證發行管理條例」版本進行審查討論中，請研究單位注意該條例審查進度予以更新資料。	已更新，詳見 6.2 節。	同意研究單位處理情形
主席結論	請研究單位更新各票證公司的營運現況資料。	已更新，詳見 2.1 節。	同意研究單位處理情形
	短期可見到票證整合成果的試辦計畫，可由公部門資源支應，請研究單位於本週確認各票證系統所需試辦經費。	已將試辦經費需求提送交通部。	同意研究單位處理情形
	具小額消費功能的電子票證權責機關已移轉至金管會，請研究單位注意電子票證管理辦法等法規的演變。	遵照辦理。	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
	報告原則審查通過，各審查委員及與會代表之意見請參考納入研究報告，並請將審查意見逐項回覆後，送交本所審核。	遵照辦理。	同意研究單位處理情形

附錄 3

期末報告審查意見回覆表

期末報告審查意見回覆表

一、開會時間：九十七年十一月二十五日上午十時

二、開會地點：運研所五樓會議室

三、主持人：吳副所長玉珍

記錄 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
本所吳副所長 玉珍	期末報告中的專有名詞應清楚說明並予統一(如 SAM 及 PSAM 卡)，以免讀者混淆。	SAM 是(Secure Access Module, 安全存取模組)的簡稱，安裝在電子票證前台設備的稱為 ISAM，安裝在卡片內的稱為 PSAM，通稱為 SAM，上述說明已補充在 P2-3，為避免讀者混淆，本報告一致採用 SAM。	同意研究單位處理情形。
悠遊卡股份有限公司	請更新期末報告中有關本公司最新的營運資料。	已更新如表 2.1-1 及 2.1 節內容。	同意研究單位處理情形。
	本公司對於交三版的看法仍持保留態度，建議以前端設備之「設備整合」方式進行票證整合。	電子票證跨系統整合模式的評估為第一年期計畫的工作項目(詳見第一年期計畫報告書 4.4 節)，研究團隊尊重悠遊卡公司的看法，目前國內將有「設備整合」及「卡片整合」兩種模式的試辦計畫，試辦過程中將可更進一步瞭解兩種方式的優缺點。	同意研究單位處理情形。
	建議票證整合應考量目前的市場營運狀況，尋找最佳的解決方案。	本計畫已召開多次技術討論會議，並考量市場現況及多數共識進行規劃與建議。	同意研究單位處理情形。
臺灣智慧卡票證公司	期末報告中對於本公司營運資料之「交易次數」，係以「刷卡次數」或「人次」定義，請重新予以確	本計畫係以「人旅次」為「交易次數」的計算基礎。	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
	認。		
	票證整合需要考慮前端設備的規範，並且需要時間驗證，建議下一期的研究應納入制定前端設備規範的議題。	本計畫著重在卡片規格的統一，以利票證系統間的互通，前端設備的技術進步甚快，似不宜由政府制定規範。	同意研究單位處理情形。
遠通電收公司	遠通電收與臺灣智慧卡公司已共同合作完成交三版的靜態資料存取測試，建議將測試結果納入本研究報告中。	已將測試結果敘述於 P4-23。	同意研究單位處理情形。
	就本團隊實際的整合經驗分享，如採用「各自加值金鑰，共同減值金鑰」的模式進行整合，其清算平台並不複雜。本團隊目前兩家公司就是以公協會的模式進行前、後台整合，如有第三家票證業者加入營運也不會複雜。	敬悉。	同意研究單位處理情形。
	對票證整合目標而言，金鑰管理是一個重要議題，本公司建議將共同清算平台納入明年度的研究。	本計畫在研擬明年度工作計畫時將納入考量。	同意研究單位處理情形。
	對於將 CPU 卡的可行性研究納入明年度的工作，本公司也抱持正面的看法。	本計畫在研擬明年度工作計畫時將納入考量。	同意研究單位處理情形。
	本團隊將積極配合本研究進行明年度動態資料的存取驗證，若將驗證擴大為試辦計畫，建議政府能夠編列預算，補助試辦計畫範圍內所需的驗票機建置經費。	本計畫在研擬明年度工作計畫時將納入考量。	同意研究單位處理情形。
	若交通電子票證發行管理條例三讀通過，目前所規劃的交三版格式是否需要修訂，以及是否可應用於跨業消費等議題，建議納入明年度的研究計畫中。	本計畫在研擬明年度工作計畫時將納入考量。	同意研究單位處理情形。
	請更新報告中本公司的營運資料。	已更新如表 2.1-1 及 2.1 節內容。	同意研究單位處理情形。
萬事達卡國際組織	在馬來西亞已有雙介面卡片的應用案例，可供本研究參考。	雙介面卡是明年度的研究重點之一，本研究將請萬事達卡國	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
		際組織提供相關資料進行深入的了解。	
	TM 卡在本研究中著墨太少，建議應再深入探討。	TM 卡是 CPU 卡的一種，屬於明年度的研究範圍，本研究明年將會對 TM 卡的營運狀況及與其它票卡整合等議題深入探討。	同意研究單位處理情形。
交通部臺灣鐵路管理局	由政府介入公協會的成立或清算平台的建置，本局認為是一個可以探討的方向。	公協會組織之成立仍應由業界發起，政府可站在正面的角度鼓勵業者參與；至於清算平台的建置在研擬明年度工作計畫時將納入考量。。	同意研究單位處理情形。
	未來本局若建置電子票證，是否就是以交三版為招標的規範？	是否採用交三版仍須依提出招標規範當時是否已公告而定，若交通部正式公告交三版規範，建議臺鐵局應採用該規範。	同意研究單位處理情形。
	本局實施電子票證之後，對於清算中心的各種替代方案及其他業者是否可加入營運或應用等細節應再研議後確認。	建議臺鐵局應就建置電子票證之方式及清算中心等相關議題進一步尋求局內共識後，以開顧問標方式尋求專業顧問公司協助辦理。	同意研究單位處理情形。
臺灣高鐵公司	本公司將先行了解政府的政策，未來執行時會遵守各項規定。	敬悉。	同意研究單位處理情形。
交通部國道高速公路局	對於目前金管會送審的電子票證發行管理條例對遠通電收公司的影響，本局將遵守原訂之契約規範，避免產生爭議。	敬悉。	同意研究單位處理情形。
交通部公路總局	電子票證的營運資料可以應用於 APTS，供本局作為客運補貼之參考資料，建議對於資料的格式應該予以統一。	電子票證相關營運資料均可依主管機關需要提供，目前並未產生格式差異而無法提供之問題。	同意研究單位處理情形。
交通部高速鐵路工程局	簡報所提交三版試辦計畫提到可應用於桃園的私有停車場，是否也可應用於公有停車場？	交三版卡片均可適用在公有及私有停車場，試辦計畫需視業者合作意願而定。	同意研究單位處理情形。
	悠遊卡公司與高鐵公司的試辦計畫因為商業談判尚未完成，因此目前工作進度停頓中。	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	未來公路總局的補助原則是否將以採用交三版為限？	未來若交三版成為交通部的建議規格，建議相關電子票證之補助仍應以交三版為規範。	同意研究單位處理情形。
	對於前端設備的規範，建議納入未來之研究。	本計畫著重在卡片規格的統一，以利票證系統間的互通，前端設備的技術進步甚快，似不宜由政府制定規範。	同意研究單位處理情形。
	桃園機場捷運機電標 AFC 系統即將招標，建議交三版應儘快定案，俾便有所依循。	交三版已呈報交通部辦理後續頒佈事宜，至於頒佈與否涉及政策走向，應由交通部綜合考量加以決定。	同意研究單位處理情形。
交通部郵電司	對於票證整合的前端設備規範建議納入未來之研究範圍。	本計畫著重在卡片規格的統一，以利票證系統間的互通，前端設備的技術進步甚快，似不宜由政府制定規範。	同意研究單位處理情形。
	業者的參與意願似乎與報告的成果不符，例如合作團隊是否已經成立？分期試辦計畫的具體成果等，報告中應再說明。	報告中所提的試辦計畫並非本計畫成立的試辦計畫，該等計畫係由票證業者自行整合提出的試辦計畫，本計畫則扮演協助的角色，提供各業者在整合作業上一個討論平台。	同意研究單位處理情形。
	本研究歷經 16 次技術討論會議，請加強討論會議之溝通平台，落實會議討論內容，有效反應於報告內。	本報告已將技術討論會議的結論納入報告書內容。	同意研究單位處理情形。
	跨系統票證整合試辦計畫，臚列分期試辦計畫，各期試辦計畫之實際進度如何？可能影響試辦之關鍵因素為何？	試辦計畫主要問題有二，關鍵一在於財務問題，由於今年度政府未能編列經費補助試辦計畫，因此如 FETC 與 TWSC 試辦計畫的進度已有落後，關鍵二在於商業談判問題，如悠遊卡與臺灣高鐵及高雄捷運的試辦計畫，因雙方尚未談妥合作條件，因此系統整合的實際開發作業並未積極進行。	同意研究單位處理情形。
國立高雄大學 都市發展與建	建議制定電子票證前端設備的規範，例如交易時間的長短等。	本計畫著重在卡片規格的統一，以利票證系統間的互通，	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
築研究所王瑞 民教授		前端設備的技術進步甚快，似不宜由政府制定規範。	
	公協會的成立有其必要性，建議臺鐵局若實施電子票證，可仿照悠遊卡公司，邀集相關業者成立電子票證公司。	臺鐵局是否可以成立獨立的票證公司或仿照悠遊卡公司邀集相關業者成立電子票證公司，應由臺鐵局內部討論後，並視營運狀況需要加以決定。	同意研究單位處理情形。
	對於使用電子票證的運輸業者是否願意接受金管會監管，可視其電子票證的應用範圍而定，若未跨業或多用途，即可不須由金管會監管。	敬悉。	同意研究單位處理情形。
國立成功大學 交通管理科學 研究所林佐鼎 教授	試辦計畫提到卡片可應用於轉乘的紀錄，卡片的資料格式是否會因為轉乘家數的增減而必須更新？	轉乘紀錄的資料格式已於交三版有所規劃，不會因為轉乘家數的增減而必須更新卡片的資料格式。	同意研究單位處理情形。
	兩種不同的卡種技術透過前端整合國內已有高雄市的 TM 卡與高雄捷運一卡通整合的成功案例，為何八達通卡(SONY 的 Felica)與周邊地區的電子票證(Mifare 卡)的整合會有金鑰互通的問題而無法整合？曼谷的票證是否也是透過前端整合技術？到底透過前端整合是不是一個可行的解決方案？	<ol style="list-style-type: none"> 1. 八達通卡與周邊地區的電子票證無法整合之因素已補充說明於 P2-7。 2. 曼谷電子票證整合係制定卡片的標準，並由單一票證公司發卡，因此屬於卡片整合方式。 3. 不同系統的電子票證透過前端整合會因為加入的家數增加而以幾何級數方式增加驗票機的交易時間，相關的研究請參照本研究第一期報告第四章。 	同意研究單位處理情形。
	交三版的共同金鑰須透過公信組織發行，若公信組織一直無法成立，是否意謂交三版無法落實執行？	交三版是規範卡片統一的資料格式與交易流程，若公信組織一直無法成立，會增加各業者利用交三版整合的困難度，是否能落實執行則可透過商業談判來達成。	同意研究單位處理情形。
	若交通電子票證採用 CPU 卡，目前送審中的「交三版」資料格式	交三版是規範卡片的資料格式與交易流程，採用更高階的	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
	還適用嗎？是否須要重新規劃？	CPU 卡可利用卡片軟體來達成讀寫交三版卡片的目的，除安全規範必須更嚴謹之外，卡片資料格式仍可適用不必修改。	
本所王穆衡組 長	本研究期末報告內容符合工作計畫書之執行項目。	敬悉。	同意研究單位處理情形。
	訂定下一期的工作計畫範圍時將考慮各單位的建議事項。	遵照辦理。	同意研究單位處理情形。
	電子票證發行管理條例的立法勢必對於電子票證業者造成衝擊，但衝擊的層面目前看來限於公司治理方面、金融安定與民眾權益保障，有關交通應用之推廣及有關政策應仍由交通部主導。	敬悉。	同意研究單位處理情形。
	對於前端設備的規範，因為科技的日益更新，無法作有效的定義，本研究仍著重在卡片資料欄位的規劃。	敬悉。	同意研究單位處理情形。
	臺鐵局若擁有電子票證清算平台，因使用範圍涵蓋全臺各地，勢必有跨系統交易的需求，而該平台是否能使用在其他系統則必須視系統容量而定。	敬悉。	同意研究單位處理情形。
	APTS 及 IC 卡的整合應用是本研究的研究方向，下一期的工作計畫將持續加以探討。	研擬下年度工作計畫時將納入考量。	同意研究單位處理情形。
本所書面審查 意見	本案進度符合合約書規定。	敬悉。	同意研究單位處理情形。
	依據 2008-11-10 射頻快報訊息，大陸建設部建標【2008】103 號文批准了《城市互聯互通卡通用技術要求》、《城市互聯互通卡清分清算技術要求》、《城市互聯互通卡密鑰及安全技術要求》國家行業標準的制訂工作，請貴研究團隊進一步蒐集上述資料，俾供未來後續研究制定相關標準參考。	相關訊息已補充說明於 P2-12，本團隊將於明年度計畫收集中國建設部有關 IC 卡的各種規範進行進一步的研究。	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
本所書面審查 意見	有關 P2-9「曼谷大眾運輸電子票證整合」之內容說明，僅係兩家公司分別經營兩條捷運路線，是否有其他大眾運輸工具(如公車)加入？如無，僅能稱其為「大眾捷運電子票證整合」，其整合困難度亦有所差異，請再予釐清。	泰國政府的整合目標，第一階段為捷運電子票證，除現有兩家既有捷運公司票證外，亦將包含未來捷運公司票證的整合，公車部分則列為未來階段的整合範圍，目前共通卡的功 能與標準的規劃將考量公車票證的需求，因此應可稱之為大眾運輸電子票證整合。	同意研究單位處理情形。
	有關 P2-11 所介紹「八達通卡」與「深圳通」之整合，請再與予清楚述明兩者所採用技術之差異，以及其遭遇之整合技術關鍵問題為何？俾供本研究參考。	已補充說明於 P2-7。	同意研究單位處理情形。
	有關跨系統整合試辦計畫部分，請於計畫後附註說明，因 97 年度交通部公路總局已無經費補助，須視 98 年度經費額度及審查結果再予核定，請加以補充。	已補充於 P5-6。	同意研究單位處理情形。
	有關 p6-1 倒數第 12 行，國內目前電子票證主管機關擬由交通部移轉至「財政部」金管會，請修正為「行政院」金管會。	已修正。	同意研究單位處理情形。
	P6-7 第 2 行，在短期內本計畫建議由目前已具有票證清算能力之公司(如「臺北智慧卡」公司、遠通電收等)，請修正為「悠遊卡」公司。	已修正。	同意研究單位處理情形。
	P7-4 二、「衍算」法則比較與建議，請修正為「演算法則之比較」；三、「衍算」法則比較與建議，請修正為「演算法則之建議」。	已修正。	同意研究單位處理情形。
	有關 P7-12 防偽驗證碼產製及驗證流程之選擇及建議部分，請貴研究團隊加強說明其產製說明及流程之優缺點，及選擇之原因為	相關優缺點及選擇原因已補充於 P7-12 及 P7-13。	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
	何？		
	P8-1TaiwanMoney 未包含雲林地區，請予以修正。	已修正。	同意研究單位處理情形。
	有關各次技術工作會議結論所提及應提供之 SOP 及相關資料，請再予檢視彙整後置於報告書附錄。	有關工作會議結論所提之 SOP 已補充於附錄十：更換金鑰作業之標準作業流程建議。	同意研究單位處理情形。
	各章節均有錯漏字，請再予檢視修正。	已全部檢視與修正完畢。	同意研究單位處理情形。
主席結論	期末報告原則審查通過，各審查委員及與會代表之意見請參考納入研究報告，並請將審查意見逐項回覆後，送交本所審核。	遵照辦理。	同意研究單位處理情形。

附錄 4

期末簡報



簡報大綱

- 壹、計畫背景與現況分析
- 貳、交三版(草案)卡片內部功能規格與交易流程定義
- 參、交三版票證整合驗證機制規劃與實作
- 肆、跨系統票證整合試辦計畫
- 伍、電子票證跨系統整合相關配合事項
- 陸、後台票證整合問題探討
- 柒、結論與建議
- 捌、交三版驗證程式展示

壹、計畫背景與現況分析

3

計畫背景

- 國內電子票證系統已有台北悠遊卡等九個系統上線營運，臺鐵亦開始其北部路段之悠遊卡試辦計畫
- 上述系統中有三區的票證系統已可雙向互通
 - 台北悠遊卡、基隆交通卡及馬祖電子票證
 - 桃竹苗及中彰投台灣通
 - 南部地區IC智慧卡及高雄捷運一卡通
- 交通部已發布「**預付型交通電子票證定型化契約應記載及不得記載事項**」，電子票證持卡者權益已獲得基本的保障，立法院正審查金管會提出之「**電子票證發行管理條例**」草案，將加強國內之電子票證管理機制
- 本計畫為四年期計畫的第二年期，以第一年期的規劃結果為基礎，詳細定義交三版草案之卡片規格及交易流程，規劃交三版卡片之驗證機制與開發測試系統，並探討票證公司進行後台功能整合的問題

4

國內電子票證系統營運現況彙整表

統計時間：97.8

系統別 營運現況	悠遊卡	臺灣通	南部地區 TaiwanMoney卡	高雄捷運一卡通	高速公路電子 收費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	遠通電收股份有限公司
開始營運時間	91年	93年	95年	97年	95年
交通應用範圍	公車(台北縣市、基隆、宜蘭、馬祖)、國道客運、捷運、纜車、淡水河藍色公路、臺鐵、公有路邊及路外停車場	桃竹苗中彰投等七縣市公車	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、公車(高雄、屏東、台南)	高速公路
驗票機	約11,000部	2831部	1911部	442部	23個收費站 130個車道
累計發卡量	1390萬張	66.7萬張	24萬張	80萬張	59萬個OBU
平均日交易量	290萬次	13萬次	2.3萬次	12萬次	37萬次
其他應用範圍	學生證、圖書館借書證、動物園門票、醫院醫療費	無	具有小額消費之電子錢包功能	無	無
備註	<ul style="list-style-type: none"> 96.9與基隆交通卡完成整合 97.8完成臺鐵基隆－中壢間19個車站之悠遊卡建置計畫 正進行與高鐵及高雄捷運之互通使用計畫 	桃竹苗與中彰投系統於97.4完成整合	可使用在高雄捷運，每日交易量約400次	可使用在裝設TM系統之公車，每日交易量約1.5萬次	正進行與台灣智慧卡公司的整合互通計畫

國外電子票證整合現況回顧

■ 香港八達通卡與深圳通

- 深圳通於建置時即採用與八達通卡相同的驗票機讀寫模組(Felica產品)，但兩者因金鑰問題仍無法互通
- 八達通卡標準與中國國家標準不同，全面換發驗票機模組至少需花費2億人民幣，目前仍在評估其可行性
- 現階段並無明確的整合時間表
- 珠江三角洲地區尚有其他兩家既有票證系統－廣州羊城通及東莞一卡通，有待後續協商技術與商業上整合議題

國外電子票證整合現況回顧

■ 曼谷地區電子票證

- 現有捷運系統由兩家捷運公司營運，分別發行不同電子票卡，彼此間不能互通
- 未來五年內將有五條新捷運路線陸續營運，若票證系統仍採目前發包方式運作，將面臨乘客需持多張捷運票卡轉乘、每轉乘一次就要多收一次基本票價的困境
- 曼谷捷運共通票證計畫(Common Ticketing Project)
 - ✓ 政府將制定捷運**共通卡標準**，涵蓋卡片規格、前台設備與後台系統等
 - ✓ 政府考慮主導建置成立**票證公司**，初期由政府擁有100%股份，開始營運後，政府逐步釋放股份給予捷運公司參與
 - ✓ 共通票證公司負責前後台系統的建置，並發行共通卡，捷運公司僅負責卡片的銷售
 - ✓ 將委外招商票證整合**計畫管理團隊**，負責監督前後台整合、協助政府成立票證公司、監督票證公司營運等工作

7

貳、交三版(草案)卡片內部功能 規格與交易流程定義

8

修訂目的及過程

■ 修訂目的

- 透過發行可跨交易系統營運之「電子票證系統多功能卡片規劃書(第三版)」(簡稱「交三版」，可視為「全區卡」)卡片，與目前各票證發卡公司所發行的「交二版」卡片(可視為「在地票證卡」)，採用**併行使用及逐漸汰換**的方式，逐步達到票證整合的目的

■ 修訂過程

- 本計畫延續去年期計畫的規劃成果，以交二版卡片規格為基礎，邀集各家電子票證公司、運輸業者及相關主管單位，歷經十餘次技術討論會議後完成交三版草案之研擬，目前已將草案提送交通部等待後續審查程序

9

修訂範圍

- 以交通運輸系統使用之非接觸式IC卡(Contactless IC Card)及雙介面複合式卡(Dual Interface Card) 為修訂標的

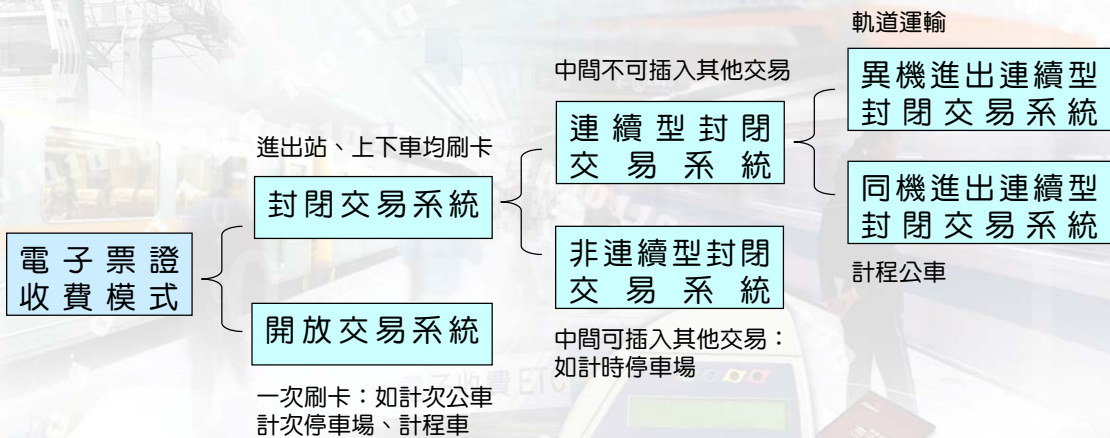
■ 規格訂定的範圍包括

- 卡片實體規格
- 卡片與卡片介面設備之介面規格
- 卡片內部功能規格(檔案結構及檔案資料格式、內容及存取權限)
- 卡片資料安全功能需求
- 編碼準則
- 交易流程設計

10

交三版(草案)與交二版差異

■ 以電子票證收費模式規劃交易資料檔案格式



- 彙整並精簡卡片交易資料所需的欄位
- 明確規範交易流程
- 增加雙介面複合式卡的參考規範

11

參、交三版票證整合驗證機制規劃與實作

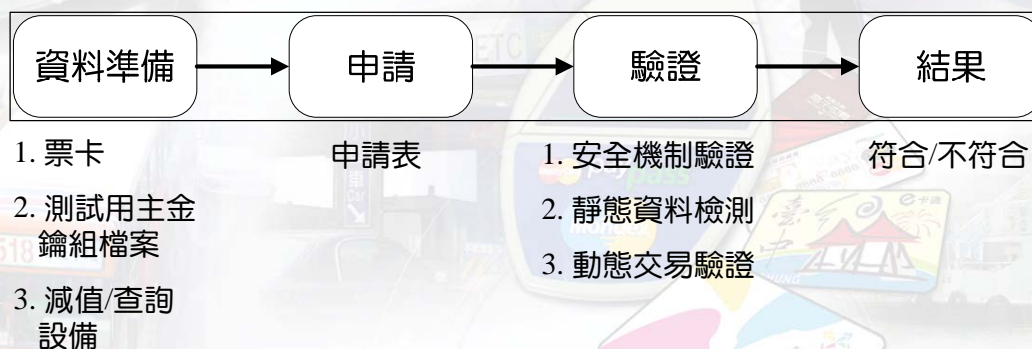
12

規劃目的與申請作業流程

■ 規劃目的

- 規劃票證業者所發行的交三版卡片及減值設備驗證機制，供未來電子票證公信組織(如公協會)使用
- 建立一套公正的交三版卡片格式及互通交易流程的驗證機制，驗證票證業者發行的卡片能夠依照交三版規劃的卡片格式及交易流程互相通用

■ 交三版驗證申請作業流程



13

交三版卡片驗證機制規劃

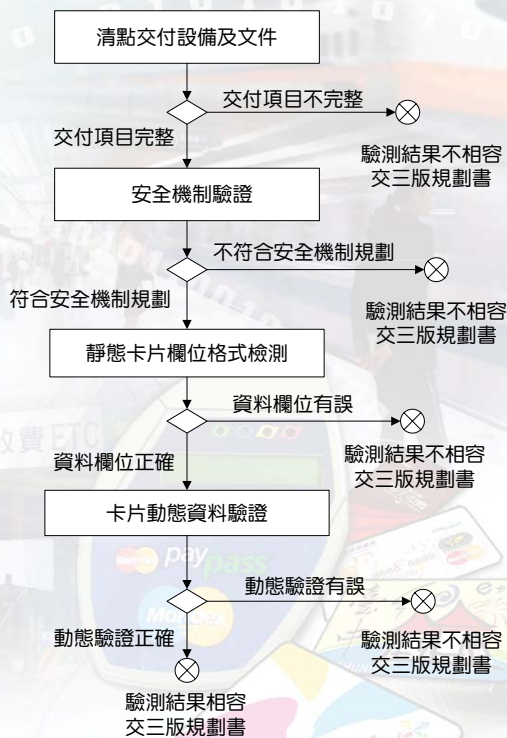
■ 驗證系統架構



14

交三版卡片驗證機制規劃

■ 驗測流程設計



15

交三版卡片驗證機制規劃

■ 驗證系統程式

➤ 卡片靜態資料顯示列印程式(本期計畫實作)

- ✓ 減值主金鑰匯入SAM卡模組
- ✓ 卡片資料讀取模組
- ✓ 公鑰存取測試模組
- ✓ 交三版欄位定義解譯模組

➤ 卡片動態資料驗證程式

- ✓ 標準非接觸式IC卡之製作模組
- ✓ 開放型減值交易產生模組
- ✓ 異機進出連續型封閉交易產生模組
- ✓ 同機進出連續型封閉交易產生模組
- ✓ 非連續型封閉交易產生模組

16

靜態驗證程式

交三版卡片靜態資料顯示列印程式

檔案(F)

執行步驟

步驟一：

卡片金鑰存取權限驗證

步驟二：

卡片格式驗證

卡片資料

公司名稱：

卡別：一般民眾

驗證次數：1

測試結果記錄檔

acer_一般民眾_1.rpt

交三版權位解釋

17

驗證程序－輸入減值主金鑰組檔

- 選擇選單中的"匯入金鑰檔"選項，進行金鑰輸入
- 檔案格式必須符合驗證程序之要求，且金鑰組必須包含交三版規範之主金鑰數量及金鑰型態

交三版卡片靜態資料顯示列印程式

檔案(F)

匯入金鑰檔(V)

儲存檔案(S)

列印(P)

離開(E)

執行步驟

步驟一：

卡片金鑰存取權限驗證

步驟二：

卡片格式驗證

卡片資料

公司名稱：

卡別：一般民眾

驗證次數：1

測試結果記錄檔

acer_一般民眾_1.rpt

交三版權位解釋

18

驗證程序－輸入檢測基本資料

- 輸入此次檢測之相關基本資料
 - 受測公司名稱、受測卡片別、以及此卡別之第幾次檢測

19

驗證程序－金鑰存取驗證

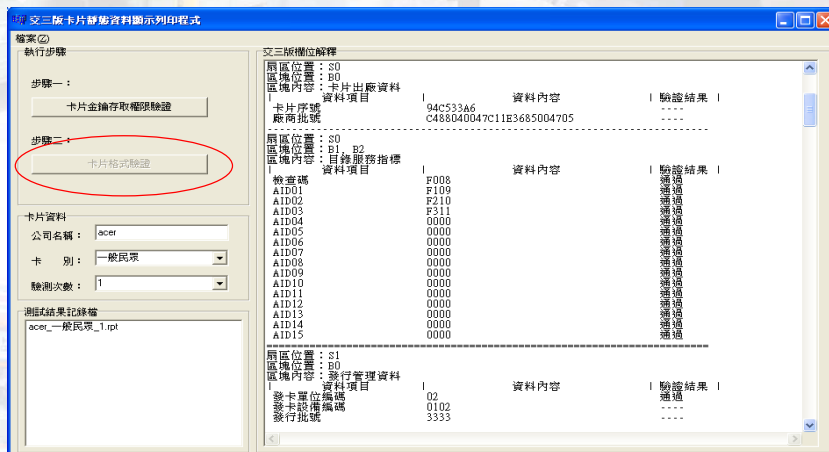
- 按下主畫面中之”卡片金鑰存取權限驗證”按鍵，進行此驗證作業
- 金鑰存取權限將以交三版規範之存取權限進行檢驗

扇區位置	金鑰種類	認證測試	讀取測試	寫入測試	驗證結果
0	A	成功	成功	無權限	通過
1	A	成功	成功	無權限	通過
2	A	成功	成功	無權限	通過
3	B	成功	成功	成功	通過
4	B	成功	成功	成功	通過
5	B	成功	成功	成功	通過
9	B	成功	成功	成功	通過
10	B	成功	成功	成功	通過
11	B	成功	成功	成功	通過

20

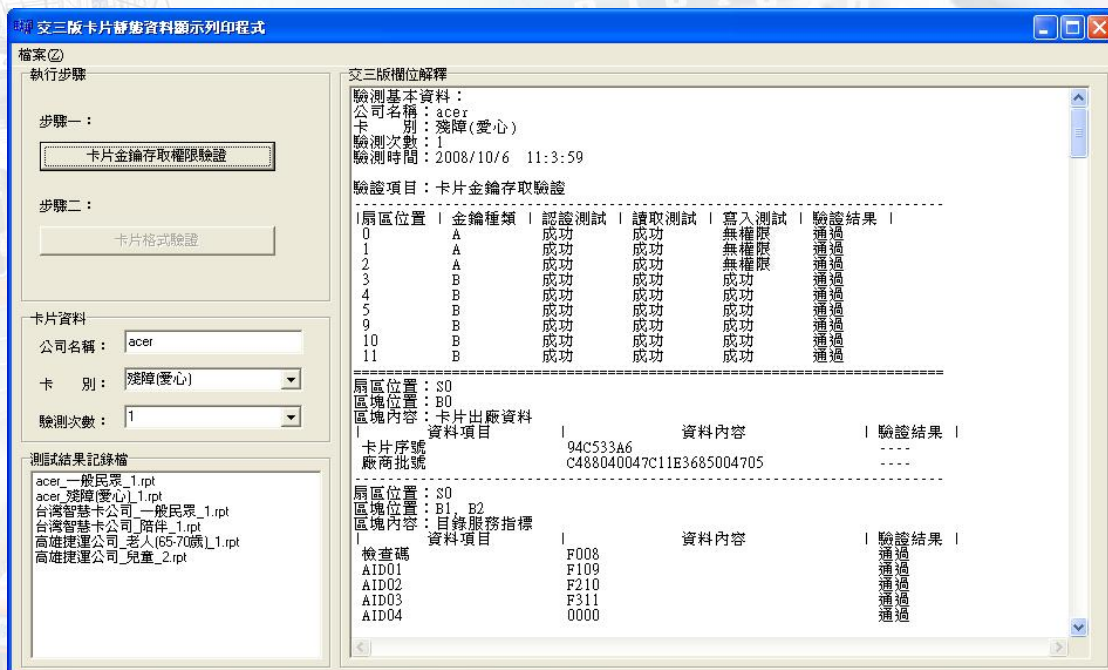
驗證程序－卡片格式驗證

- 按下主畫面中的”卡片格式驗證”按鍵，進行卡片格式驗證作業
- 卡片格式將依據交三版定義中註明必要項目的各欄位內容進行檢測，若為自行使用欄位，則不會進行研判



21

檢測結果顯示



22

肆、跨系統票證整合試辦計畫

23

跨系統票證整合試辦計畫

- 以**交三版**執行票證整合試辦計畫
 - 由遠通電收公司(FETC)與台灣智慧卡公司(TWSC)進行整合
- 以**前端設備**執行票證整合試辦計畫
 - 由悠遊卡公司與高雄捷運公司進行整合
- 試辦結果將作為交通部擬定電子票證整合未來發展政策的重要參考依據

24

以交三版執行票證整合試辦計畫

- 台灣智慧卡公司(TWSC)與遠通電收公司(FETC)各自發行符合交三版(草案)規格的卡片，協助交通部驗證交三版卡片規格及交易流程的可行性
- 共同產製**交三版卡片金鑰**，並共同保管與持有
- 由FETC設置**跨系統清算平台**
- 第一期試辦計畫(預定97年底完成)
 - 計畫範圍：高速公路電子收費及桃竹苗公車15條路線
 - 試辦方式
 - ✓ FETC與TWSC各發行250~500張符合交三版卡片，卡片可在對方系統扣款使用
 - ✓ 修改200台既有公車驗票機，新增50台公車驗票機
 - ✓ 主要進行**同機進出連續性封閉交易**(里程計費公車)及**開放型交易**(高速公路ETC)兩種系統的驗證

25

以交三版執行票證整合試辦計畫

- 第二期試辦計畫(預定98年6月完成)
 - 計畫範圍：高速公路電子收費、桃竹苗公車所有路線及桃園私有停車場
 - 試辦方式
 - ✓ FETC與TWSC各發行2500~5000張符合交三版卡片，卡片可在對方系統扣款使用
 - ✓ 修改1000台既有公車驗票機，新增450台公車驗票機
 - ✓ 主要進行**同機進出連續性封閉交易**(里程計費公車)、**開放型交易**(高速公路ETC)及**非連續型封閉交易**(停車場)等三種系統驗證
- 第三期試辦計畫(預定98年年底完成)
 - 計畫範圍：高速公路電子收費、桃竹苗中彰投公車所有路線及桃園與台中私有停車場
 - 試辦方式
 - ✓ 主要進行**同機進出連續性封閉交易**(里程計費公車)、**開放型交易**(高速公路ETC)及**非連續型封閉交易**(停車場)等三種系統驗證

26

以前端設備執行票證整合試辦計畫

- 悠遊卡、台北捷運與高雄捷運公司合作進行票證整合，驗證以前端設備進行整合的可行性
- 將於台北與高雄捷運車站公務門之驗票設備，以SAM卡方式進行設備整合，使悠遊卡與高捷一卡通**不需換卡**即能在對方車站使用
- 計畫範圍
 - 高雄捷運37個車站與台北捷運67個車站
 - 預定修改220組驗票設備及200組加值設備

27

伍、電子票證跨系統整合相關配合事項

28

跨系統整合之議題探討

- 本研究綜合國內電子票證跨系統整合所面臨的各種問題，可分為三個面向：

一、政策指導

- 檢視國外交通電子票證整合以及多用途交通卡發展現況可以發現，成功的案例皆有政府強力的政策指導
 - ✓ 中國珠江三角洲由中國政府提出「一卡通十城」的政策目標，並制定中國國家標準要求各票證營運組織逐年調整現有系統，以達最終整合的目的
 - ✓ 瀋陽市由政府成立票證公司，直接進行多用途交通卡的建置，各項系統規範及卡片資料格式則遵照國家標準
 - ✓ 曼谷捷運的電子票證整合政策，則是由政府制定共通卡相關標準，並出資成立票證公司建立清算後台及發行共通卡，以整合捷運系統的電子票證

29

跨系統整合之議題探討

二、技術規範

- 以中國為例，目前中國建設部已完成交通電子票證的規範，各級地方政府所管轄的交通電子票證系統皆必須遵守國家技術規範逐年逐項修改，由小區域的整合擴大到大區域，最後達成國家一卡通的目的
- 本計畫已完成「交三版草案」，若公布實施之後即屬國家級的規範，但是除卡片資料格式的頒定外，尚包括金鑰管理、資料交換、資料傳輸安全等議題，需要後續加以規範
- 共同金鑰管理的前提是電子票證公信單位(如公協會)的設立，目前FETC與TWSC整合案的權宜作法是兩家共管，未來如第三家以上之票證組織加入時，共管的複雜與風險性將大幅提高

30

跨系統整合之議題探討

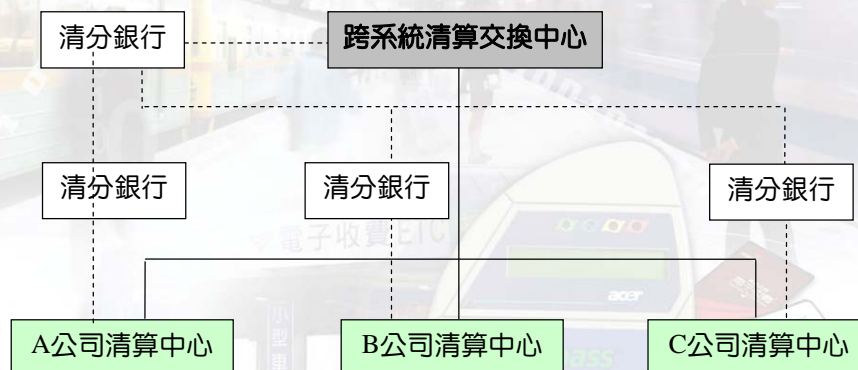
三、營運面

- 以目前FETC與TWSC整合過程中所衍生的議題包括：客戶服務流程、對帳作業流程、金流作業流程、營運管理資料流程、共同行銷、利益分配等
- 營運面的議題會因為各家的經營條件以及相對規模等因素而不同，且其中尚涉及部份的業務機密以及智慧財產權的認定，故此部份應為個案探討的範圍，由各票證業者於實際進行整合時再具體研議

31

成立「電子票證跨系統清算交換中心」之探討

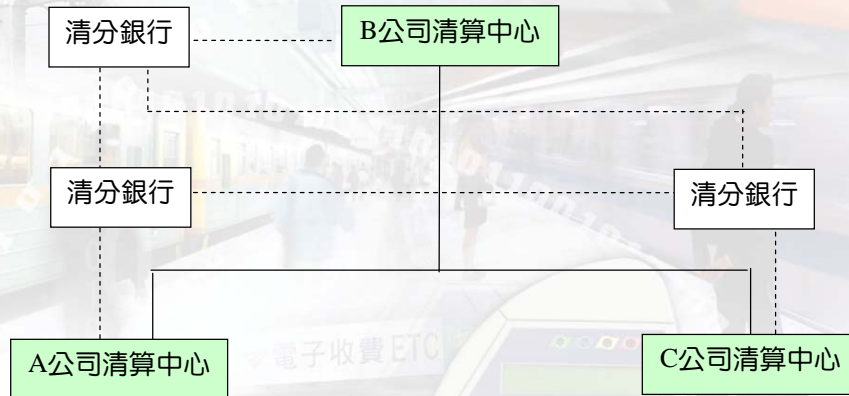
- 未來國內各電子票證系統採用交三版卡片進行整合後，有關跨系統交易之清算主要有兩種方式進行：
一. 建立統一清算交換中心進行清算



32

成立「電子票證跨系統清算交換中心」之探討

二. 兩兩系統各自清算



33

成立「電子票證跨系統清算交換中心」之探討

- **統一清算**的方式對於現有各家票證營運組織之系統修改程度比**兩兩各自清算**單純
- 建議成立「電子票證跨系統清算交換中心」，串接各家票證業者之後台清算系統，以進行每日交易交換及結算作業，並提供交三版共同減值金鑰組之金鑰管理作業，以及協助各票證組織發行交三版共同減值SAM卡

34

成立「電子票證跨系統清算交換中心」之探討

- 「電子票證跨系統清算交換中心」為一獨立於各家交通電子票證公司之機構，應由電子票證公信組織(如公協會)建置與營運，其為國內票證整合是否能夠成功的重要關鍵
- 短期內建議由目前已具有票證清算能力之公司(如台北智慧卡公司、遠通電收等)取得同業共識後，以擴充現有設備代管之方式進行
- 短期內若國內各交通電子票證公司仍無法達成共識，建議未來台鐵局於建置電子票證系統時，可依照政府採購法及審議中之金管會「電子票證發行管理條例」相關規定，將台鐵局電子票證建置與管理專案計畫委由專業廠商承攬，並將「電子票證跨系統清算中心」納入委託服務範圍

35

電子票證相關法規分析

- 銀行相關法規
 - 銀行法第42條之1：銀行發行現金儲值卡應經主管單位許可，並依中央銀行之規定提列準備金
 - 銀行發行現金儲值卡許可及管理辦法第3條：...多用途現金儲值卡之使用，可跨越不同營運系統間使用，或應用於不同之商業體系。非銀行不得發行現金儲值卡。
 - 電子票證使用於跨不同營運系統，應屬於上述法規所規定的多用途現金儲值卡範圍
- 預付型交通電子票證定型化契約應記載及不得記載事項
 - 由交通部97.4.1頒布施行
 - 規定基本事項以保障消費者權益：預付款應辦理履約保證或存入信託專戶、儲值金額上限、不得記載使用期限及餘額不得退費

36

電子票證相關法規分析

■ 電子票證發行管理條例(草案)

- 由**金管會**擬定，本草案已於97.11.6初審通過
- 將採用**核准制**，需經金管會核准才得辦理電子票證業務
- 放寬非銀行體系的電子票證發行公司的電子票證應用範圍能夠應用在其他商業體系，例如小額消費
- 對於電子票證發行公司的**設立門檻**訂定標準，如公司資本額及履約能力，對於現行規模較小之電子票證公司影響較大

37

陸、後台票證整合問題探討

- 金鑰整合機制
- 卡片真偽確認機制
- 交易真偽確認機制
- 後台交易/黑名單交換機制

38

交三版金鑰管理規範建議

- 交三版之卡片金鑰(基碼)，分為**個別管理主金鑰組**與**共同管理主金鑰組**
- 個別管理主金鑰組為**發卡單位個別擁有之主金鑰組**(如：加值主金鑰組...)
- 共同管理主金鑰組為**全區共用之主金鑰組**(如：減值主金鑰組，防偽驗證碼主金鑰等...)
- 建議須先成立**電子票證公信單位(如公協會)**，共同管理主金鑰組應由公信單位管理並保管於各方可信賴的安全機房
- 依據各方同意之**基碼管理辦法**以及**機房管理辦法**規定之作業程序，管理共同管理主金鑰組
- **基碼管理辦法**中須包含金鑰存取權限管控、金鑰備份及回復作業、金鑰安全傳輸作法，並應規範主金鑰之明碼不得儲存於非HSM(Hardware Security Module)、IC智慧卡外之其他儲存媒體中

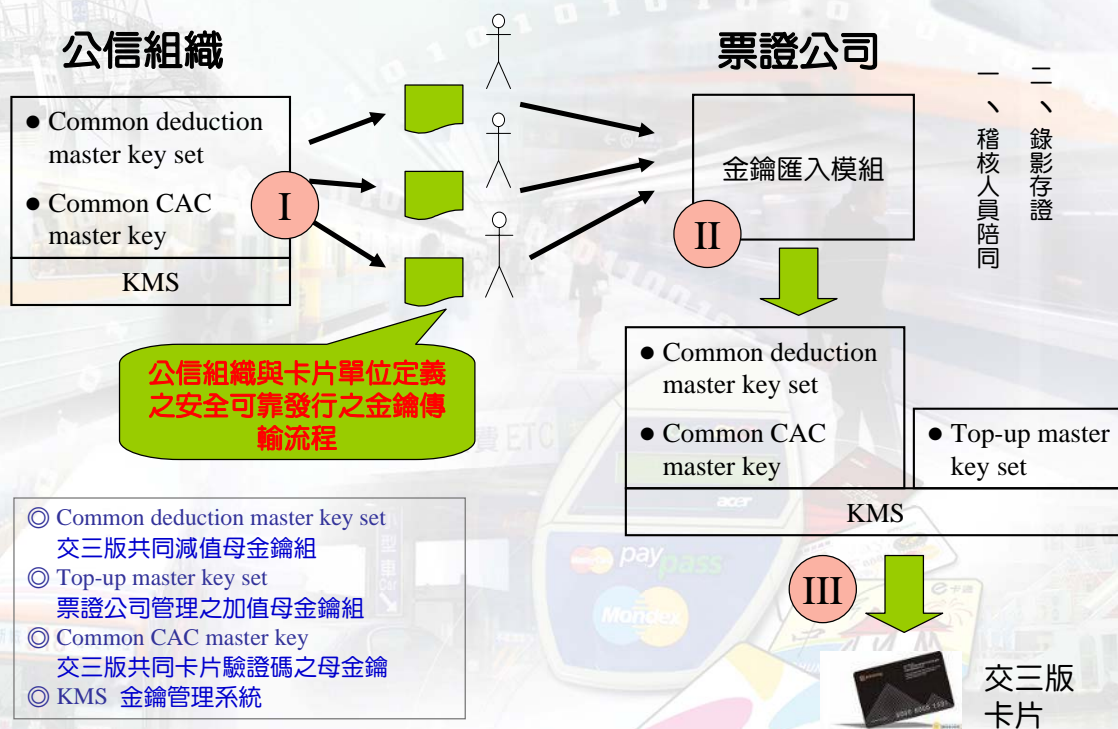
39

交三版金鑰管理規範建議

- 為提供未來可能發生洩密事件之準備，需事先規劃完整的**換Key作業**
- 各欲加入之發卡單位之**金鑰管理机制**必須經由公信單位中各家已加入之發卡單位認可後才得以加入組織
 - 確保各發卡單位之金鑰管理机制確可提供安全且保密之運作發卡環境，而不至於發生單位人員盜用金鑰之狀況
- 規範各家發卡單位必須進行定期之**安全控管檢查**
 - 防堵不肖員工可能造成之安全漏洞
- 若因發卡單位之內控發生問題，導致共同金鑰內容發生洩密，致使他家發卡單位蒙受損失，則該發生內控問題之發卡單位應賠償其損失

40

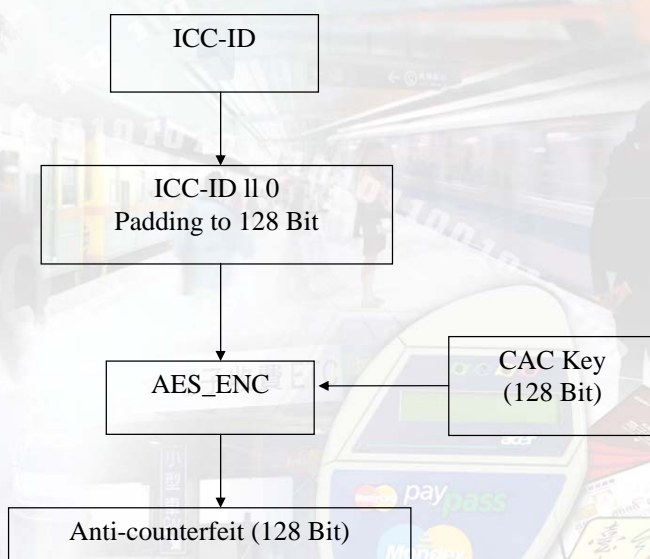
交三版共同金鑰之發卡流程建議



41

卡片真偽確認機制建議

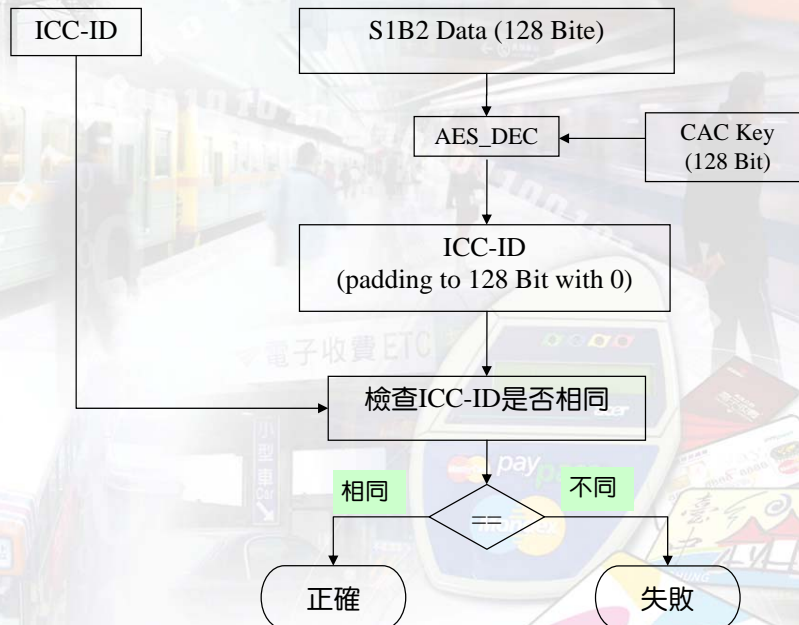
產生防驗證碼



42

卡片真偽確認機制建議

■ 驗證防偽驗證碼



43

卡片真偽確認機制建議

■ 演算法則之選擇

- 建議使用較新穎之**AES演算法**，以提高安全性與速度

■ 安全性議題

- 卡片真偽確認機制待各家票證公司試行確認可行後，由**公協會**制定此防偽驗證碼驗證標準流程
- 各家票證公司使用之防偽驗證碼之母金鑰皆相同，則有可能一家票證業者可輕易複製他家票證業者之卡片，因此有可能會造成系統性問題，建議公協會訂定票證公司**認可之稽核流程及做法**，以確保票證公司發卡之權利
- 防偽驗證碼之檢驗，只須於**前台驗票設備**中進行檢驗，而不應回傳至後台，也不能開放各家後台選擇需驗或不需驗

44

交易真偽確認機制

- 減值設備於交易完成後即產生一組**交易壓碼資料**以供後台確認
- 後台系統確認該交易之確實完成(卡片之餘額確實已被扣除該交易所應支付之金額)，便可逕行撥付款項予該減值設備之安裝業者
- 建議交易真偽之確認機制應秉持各參與交三版票卡共通之各家業者互信原則，交由**各減值設備鋪設業者**自行定義並負責確保該交易之確實產生(依據一般金融信用卡代收代付之作業慣例)

45

後台交易/黑名單交換機制

- 須由所有參與交三版票卡共通的各家業者所組成之公信單位進行統籌運作
- 所有業者所產生之黑名單以及減值設備收取之非該家業者之所有交易，皆須傳送至該公信單位之交換中心
- 交換中心將黑名單彙總後轉送至各家業者，且將所有傳入之交易轉送至該交易卡片之所屬業者
- 相關之黑名單檔案格式以及交換交易檔格式應由各家業者以及公信單位研議並確定

46

柒、結論與建議

47

結論

- 本計畫蒐集國外電子票證整合發展的案例，其中以曼谷捷運共通卡與我國電子票證所面臨的挑戰與現實環境最為類似，泰國政府將研擬**共通卡規格**及相關系統之規範，並計畫籌資成立**電子票證公司**，發行**捷運共通卡**，逐漸淘汰既有的捷運電子票證，相關做法值得交通部參考借鏡
- 本計畫邀集各票證公司及相關單位，歷經一年時間、共召開16次技術研討會，研擬完成**交三版草案**，並提送交通部進行後續審查作業
- 交三版草案以交通電子票證使用之非接觸式IC卡及雙介面複合式卡為修訂標的，其與交二版的主要不同處在於：
 - 交三版以「**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及增加交易速度
 - 明確規範**交易流程**，規劃主交易流程及參考交易流程
 - 增加**雙介面複合式卡**的參考規範，供非使用Mifare卡片系列的發卡單位參考

48

結論

- 本計畫規劃完成**交三版驗證機制**，包括驗證申請作業流程、驗證系統架構及驗證流程，其中驗證流程包含第一階段卡片靜態資料驗證及第二階段卡片動態資料驗證，本計畫今年度開發完成**卡片靜態資料驗證系統**，可以檢視送測之卡片資料內容是否符合交三版之格式定義
- 本計畫提出包括金鑰整合、卡片真偽確認、交易真偽確認、後台交易/黑名單交換等**後台系統整合機制**，其中在**金鑰整合**部份，所規劃的交三版卡片發卡流程，係由**電子票證公協會**負責管理交三版減值主金鑰組及防偽驗證碼母金鑰，各票證公司負責管理增值主金鑰組

49

建議事項

- 建置共通的電子票證跨系統清算平台
 - 本計畫提出電子票證跨系統清算平台的建置計畫，其建置期分為三階段，建置需時約一年，建議由政府依照採購法及金管會審議中之電子票證發行管理條例相關規定，委由專業廠商承攬建置
- 探討以CPU卡做為交通電子票證載體之可行性研究
 - 國內交通票證的主流－Mifare卡片近來在國外頻頻傳出被成功破解的案例
 - 未來交通票證在「電子票證發行管理條例」通過後將可使用在小額消費，其遭受攻擊的可能性更高，破解後所受到的損失亦更為嚴重
 - 建議下一期計畫可考量採用安全等級較高的CPU卡片之可行性分析，以提高未來電子票證之卡片防護機制

50

建議事項

■ 接續開發卡片動態資料驗證系統

- ▶ 本期計畫已完成卡片靜態資料驗證系統，僅能進行卡片的基本項目檢測
- ▶ 建議下一期計畫應進行卡片動態資料驗證系統開發，以測試受測卡片及設備能符合**交三版之交易流程定義**，受測卡片需可在驗證程式中進行減值交易，卡片回到業者的減值設備中亦可被正確處理
- ▶ 完整的動態資料驗證系統應包含以下模組
 - ✓ 開放型減值交易產生模組
 - ✓ 異機進出連續型封閉交易產生模組
 - ✓ 同機進出連續型封閉交易產生模組
 - ✓ 非連續型封閉交易產生模組

51

建議事項

- ▶ 上述四種模組皆需依照交三版定義之基本票種及基本減值流程功能來進行製作
- ▶ 卡片動態資料驗證依據各種不同載具間的相互搭乘行為來進行資料檢測，用以確定卡片於各種載具間之使用符合交三版的相關定義
- ▶ 此一檢測流程，可使用廠商提供之“受測減值設備”，用以檢測此設備是否符合交三版規範
- 制定其他交三版整合相關規範
 - ▶ 包括**共同金鑰管理規範**及**卡片防偽驗證流程**
 - ▶ 由政府協調各票證公司組成**電子票證公協會**，負責統籌票證整合相關事宜，包括相關規範的制定、交三版驗證機制的執行、共同金鑰的管理等工作

52

捌、交三版驗證程式展示

53

**簡報結束
敬請指教**

附錄 5

交三版(草案)與交二版 資料欄位修訂前後比較

交三版(草案)與交二版資料欄位修訂前後比較

Sector	Block	交二版	交三版草案
S0	B0	卡片出廠資料	卡片出廠資料(未更改)
	B1~B2	目錄服務指標	目錄服務指標(新增交三版應用區AID)
S1	B0	發行管理資料	發行管理資料(修改部份資料項目說明)
	B1	票值管理資料	票值管理資料(新增7個資料項目)
	B2	卡片防偽驗證資料	卡片防偽驗證資料(未更改)
S2	B0	主要票值	主要票值(更改主要票值Byte長度及資料屬性)
	B1	票值備份	票值備份(更改票值備份Byte長度及資料屬性)
	B2	票值加值記錄	票值加值記錄(未更改)
S3	B0	卡片交易狀態資料	卡片交易狀態資料(新增5個資料項目)
	B1~B2	最近兩筆閘門交易記錄	最近兩筆交易記錄(修改欄位及資料項目#8的定義)
S4~S5	B0~B2	最近六筆交易記錄資料	最近六筆交易記錄資料(未更改)
S6~S8		系統應用資料	個別應用區(未更改)
S9	B0	系統應用資料	異機進出連續型封閉交易系統定期票票卡管理資料(新增)
	B1	系統應用資料	異機進出連續型封閉交易系統交易記錄(1)(新增)
	B2	系統應用資料	異機進出連續型封閉交易系統交易記錄(2)(新增)
S10	B0	系統應用資料	同機進出連續型封閉交易系統定期票票卡管理資料(新增)
	B1	系統應用資料	同機進出連續型封閉交易系統交易記錄(1)(新增)
	B2	系統應用資料	同機進出連續型封閉交易系統交易記錄(2)(新增)
	B0	系統應用資料	非連續型封閉交易系統定期票票卡管理資料(新增)

Sector	Block	交二版	交三版草案
S11	B1	系統應用資料	非連續型封閉交易系統交易記錄(1)(新增)
	B2	系統應用資料	非連續型封閉交易系統交易記錄(2)(新增)
S12~S15		系統應用資料	保 留

Sector/ Block	交二版	交三版(草案)									
S0B0	<div>卡片出廠資料(S0B0)</div> <table><tr><td>資料項目</td><td>長度 (Byte)</td><td>屬性</td></tr><tr><td>卡片序號</td><td>4</td><td>BIN</td></tr><tr><td>廠商批號</td><td>12</td><td>BIN</td></tr></table>	資料項目	長度 (Byte)	屬性	卡片序號	4	BIN	廠商批號	12	BIN	未更改
資料項目	長度 (Byte)	屬性									
卡片序號	4	BIN									
廠商批號	12	BIN									
S0B1~2	目錄服務指標(S0B1~B2)	目錄服務指標(S0B1~B2) 新增交三版應用區 AID： <table><tr><td>交三版異機進出連續型封閉交易系統</td><td>0xF1</td></tr><tr><td>交三版同機進出連續型封閉交易系統</td><td>0xF2</td></tr><tr><td>交三版非連續型封閉交易系統</td><td>0xF3</td></tr></table>	交三版異機進出連續型封閉交易系統	0xF1	交三版同機進出連續型封閉交易系統	0xF2	交三版非連續型封閉交易系統	0xF3			
交三版異機進出連續型封閉交易系統	0xF1										
交三版同機進出連續型封閉交易系統	0xF2										
交三版非連續型封閉交易系統	0xF3										

Sector/ Block	交二版	交三版(草案)																																				
S1B0	發行管理資料(S1B0)	發行管理資料(S1B0) 修改部份資料項目說明如下： (4) 發行日期：卡片發行日期，以卡片發行當天 23 點 59 分 59 秒之時間作記錄，採用台灣時間的 UNIX Time。 (5) 有效日期：卡片有效日期，以卡片有效終止日當天 23 點 59 分 59 秒之時間作記錄，採用台灣時間的 UNIX Time。 (6) 卡片規格版本：發行格式定義如下。 high nibble：主版本 0x2X：交二版 0x3X：交三版 low nibble：次版本 X=0：標準版本 X=1~F：各發卡單位自行規劃交三版衍生應用版本順序 (7) 卡片狀態：記錄卡片經發行單位所做的最新發行狀態，目前包括以下四種狀態項目：																																				
	<table><tr><th>序號</th><th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr><tr><td>1</td><td>發卡單位編號</td><td>1</td><td>BIN</td></tr><tr><td>2</td><td>發卡設備編號</td><td>2</td><td>BIN</td></tr><tr><td>3</td><td>發行批號</td><td>2</td><td>BIN</td></tr><tr><td>4</td><td>發行日期</td><td>4</td><td>UNIX</td></tr><tr><td>5</td><td>有效日期</td><td>4</td><td>UNIX</td></tr><tr><td>6</td><td>卡片規格版本</td><td>1</td><td>BIN</td></tr><tr><td>7</td><td>卡片狀態</td><td>1</td><td>BIN</td></tr><tr><td>8</td><td>檢查碼</td><td>1</td><td>BIN</td></tr></table>	序號	資料項目	長度 (Byte)	屬性	1	發卡單位編號	1	BIN	2	發卡設備編號	2	BIN	3	發行批號	2	BIN	4	發行日期	4	UNIX	5	有效日期	4	UNIX	6	卡片規格版本	1	BIN	7	卡片狀態	1	BIN	8	檢查碼	1	BIN	
	序號	資料項目	長度 (Byte)	屬性																																		
	1	發卡單位編號	1	BIN																																		
	2	發卡設備編號	2	BIN																																		
	3	發行批號	2	BIN																																		
	4	發行日期	4	UNIX																																		
	5	有效日期	4	UNIX																																		
	6	卡片規格版本	1	BIN																																		
	7	卡片狀態	1	BIN																																		
8	檢查碼	1	BIN																																			

Sector/ Block	交二版	交三版(草案)																																																
S1B1	票值管理資料(S1B1)：																																																	
	<table><tr><th>序號</th><th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr><tr><td>1</td><td>自動加值設定</td><td>1</td><td>BIN</td></tr><tr><td>2</td><td>自動加值票值數額</td><td>2</td><td>BIN</td></tr><tr><td>3</td><td>儲存最大票值數額</td><td>2</td><td>BIN</td></tr><tr><td>4</td><td>每筆可扣減最大票值數額</td><td>2</td><td>BIN</td></tr><tr><td>5</td><td>自動加值銀行代碼</td><td>1</td><td>BIN</td></tr><tr><td>6</td><td>基本身分別</td><td>1</td><td>BIN</td></tr><tr><td>7</td><td>基本身分區碼</td><td>1</td><td>BIN</td></tr><tr><td>8</td><td>優惠補助身分分別</td><td>1</td><td>BIN</td></tr><tr><td>9</td><td>優惠補助身分有效日</td><td>2</td><td>DOSDate</td></tr><tr><td>10</td><td>特殊身分優惠最大次數</td><td>2</td><td>BIN</td></tr><tr><td>11</td><td>檢查碼</td><td>1</td><td>BIN</td></tr></table>	序號	資料項目	長度 (Byte)	屬性	1	自動加值設定	1	BIN	2	自動加值票值數額	2	BIN	3	儲存最大票值數額	2	BIN	4	每筆可扣減最大票值數額	2	BIN	5	自動加值銀行代碼	1	BIN	6	基本身分別	1	BIN	7	基本身分區碼	1	BIN	8	優惠補助身分分別	1	BIN	9	優惠補助身分有效日	2	DOSDate	10	特殊身分優惠最大次數	2	BIN	11	檢查碼	1	BIN	
	序號	資料項目	長度 (Byte)	屬性																																														
	1	自動加值設定	1	BIN																																														
	2	自動加值票值數額	2	BIN																																														
	3	儲存最大票值數額	2	BIN																																														
	4	每筆可扣減最大票值數額	2	BIN																																														
	5	自動加值銀行代碼	1	BIN																																														
	6	基本身分別	1	BIN																																														
	7	基本身分區碼	1	BIN																																														
8	優惠補助身分分別	1	BIN																																															
9	優惠補助身分有效日	2	DOSDate																																															
10	特殊身分優惠最大次數	2	BIN																																															
11	檢查碼	1	BIN																																															
S1B2	卡片防偽驗證資料(S1B2)																																																	
	<table><tr><th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr><tr><td>防偽驗證資料</td><td>16</td><td>BIN</td></tr></table>	資料項目	長度 (Byte)	屬性	防偽驗證資料	16	BIN	未更改																																										
	資料項目	長度 (Byte)	屬性																																															
防偽驗證資料	16	BIN																																																

Sector/ Block	交二版	交三版(草案)																											
S2B0	主要票值(S2B0) <table border="1"> <tr> <td>資料項目</td><td>長度 (Byte)</td><td>屬性</td></tr> <tr> <td>電子票值</td><td>≥2</td><td>BIN</td></tr> </table>	資料項目	長度 (Byte)	屬性	電子票值	≥2	BIN	主要票值(S2B0) <table border="1"> <tr> <td>資料項目</td><td>長度 (Byte)</td><td>屬性</td></tr> <tr> <td>電子票值</td><td>=16</td><td>Mifare Value</td></tr> </table>	資料項目	長度 (Byte)	屬性	電子票值	=16	Mifare Value															
資料項目	長度 (Byte)	屬性																											
電子票值	≥2	BIN																											
資料項目	長度 (Byte)	屬性																											
電子票值	=16	Mifare Value																											
S2B1	票值備份(S2B1) <table border="1"> <tr> <td>資料項目</td><td>長度 (Byte)</td><td>屬性</td></tr> <tr> <td>備份電子票值</td><td>≥2</td><td>BIN</td></tr> </table>	資料項目	長度 (Byte)	屬性	備份電子票值	≥2	BIN	票值備份(S2B1) <table border="1"> <tr> <td>資料項目</td><td>長度 (Byte)</td><td>屬性</td></tr> <tr> <td>備份電子票值</td><td>=16</td><td>Mifare Value</td></tr> </table>	資料項目	長度 (Byte)	屬性	備份電子票值	=16	Mifare Value															
資料項目	長度 (Byte)	屬性																											
備份電子票值	≥2	BIN																											
資料項目	長度 (Byte)	屬性																											
備份電子票值	=16	Mifare Value																											
S2B2	票值加值記錄(S2B2) <table border="1"> <tr> <td>資料項目</td><td>長度 (Byte)</td><td>屬性</td></tr> <tr> <td>交易序號</td><td>1</td><td>BIN</td></tr> <tr> <td>交易時間</td><td>4</td><td>UNIX</td></tr> <tr> <td>交易類別</td><td>1</td><td>BIN</td></tr> <tr> <td>交易票值</td><td>2</td><td>BIN</td></tr> <tr> <td>交易後票值</td><td>2</td><td>BIN</td></tr> <tr> <td>交易系統編號</td><td>1</td><td>BIN</td></tr> <tr> <td>交易地點/運輸業者/RSU 編號</td><td>1</td><td>BIN</td></tr> <tr> <td>交易機器/OBU 編號</td><td>4</td><td>BIN</td></tr> </table>	資料項目	長度 (Byte)	屬性	交易序號	1	BIN	交易時間	4	UNIX	交易類別	1	BIN	交易票值	2	BIN	交易後票值	2	BIN	交易系統編號	1	BIN	交易地點/運輸業者/RSU 編號	1	BIN	交易機器/OBU 編號	4	BIN	未更改
資料項目	長度 (Byte)	屬性																											
交易序號	1	BIN																											
交易時間	4	UNIX																											
交易類別	1	BIN																											
交易票值	2	BIN																											
交易後票值	2	BIN																											
交易系統編號	1	BIN																											
交易地點/運輸業者/RSU 編號	1	BIN																											
交易機器/OBU 編號	4	BIN																											

Sector/ Block	交二版	交三版(草案)																																																																
S3B0	卡片交易狀態資料(S3B0)																																																																	
	卡片交易狀態資料(S3B0)																																																																	
	<table><tr><th>序號</th><th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr><tr><td>1</td><td>卡片交易序號</td><td>2</td><td>BIN</td></tr><tr><td>2</td><td>交易記錄檔指標</td><td>1</td><td>BIN</td></tr><tr><td>3</td><td>優惠積點數</td><td>2</td><td>BIN</td></tr><tr><td>4</td><td>優惠積點交易序號</td><td>2</td><td>BIN</td></tr><tr><td>5</td><td>保留</td><td>9</td><td>BIN</td></tr></table>	序號	資料項目	長度 (Byte)	屬性	1	卡片交易序號	2	BIN	2	交易記錄檔指標	1	BIN	3	優惠積點數	2	BIN	4	優惠積點交易序號	2	BIN	5	保留	9	BIN	<table><tr><th>序號</th><th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr><tr><td>1</td><td>卡片交易序號</td><td>2</td><td>BIN</td></tr><tr><td>2</td><td>交易記錄檔指標</td><td>1</td><td>BIN</td></tr><tr><td>3</td><td>優惠積點數</td><td>2</td><td>BIN</td></tr><tr><td>4</td><td>優惠積點交易序號</td><td>2</td><td>BIN</td></tr><tr><td>5</td><td>鎖卡旗標</td><td>1</td><td>BIN</td></tr><tr><td>6</td><td>每日優惠累計轉乘點數</td><td>2</td><td>BIN</td></tr><tr><td>7</td><td>轉乘優惠日期</td><td>2</td><td>DOSDate</td></tr><tr><td>8</td><td>特殊身分優惠累計次數</td><td>2</td><td>BIN</td></tr><tr><td>9</td><td>加值累計點數</td><td>2</td><td>BIN</td></tr></table>	序號	資料項目	長度 (Byte)	屬性	1	卡片交易序號	2	BIN	2	交易記錄檔指標	1	BIN	3	優惠積點數	2	BIN	4	優惠積點交易序號	2	BIN	5	鎖卡旗標	1	BIN	6	每日優惠累計轉乘點數	2	BIN	7	轉乘優惠日期	2	DOSDate	8	特殊身分優惠累計次數	2	BIN	9	加值累計點數	2	BIN
	序號	資料項目	長度 (Byte)	屬性																																																														
	1	卡片交易序號	2	BIN																																																														
	2	交易記錄檔指標	1	BIN																																																														
	3	優惠積點數	2	BIN																																																														
	4	優惠積點交易序號	2	BIN																																																														
	5	保留	9	BIN																																																														
	序號	資料項目	長度 (Byte)	屬性																																																														
1	卡片交易序號	2	BIN																																																															
2	交易記錄檔指標	1	BIN																																																															
3	優惠積點數	2	BIN																																																															
4	優惠積點交易序號	2	BIN																																																															
5	鎖卡旗標	1	BIN																																																															
6	每日優惠累計轉乘點數	2	BIN																																																															
7	轉乘優惠日期	2	DOSDate																																																															
8	特殊身分優惠累計次數	2	BIN																																																															
9	加值累計點數	2	BIN																																																															

Sector/ Block	交二版	交三版(草案)
S3B1~2	最近兩筆開門交易記錄(S3B1~B2)	最近兩筆交易記錄(S3B1~B2)
	序號	資料項目
	1	交易序號
	2	交易時間
	3	交易類別
	4	交易票值/票點
	5	交易後票值/票點
	6	交易系統編號
	7	交易地點//RSU 編號/交易票價站
	8	交易機器/OBU 編號/ 轉乘優惠群組
	長度 (Byte)	長度 (Byte)
	1	1
	4	4
	1	1
	2	2
	1	1
	1	4
	BIN	BIN
	UNIX	UNIX
	BIN	BIN
	BIN	BIN
	BIN	BIN
	BIN	BIN
	BIN	BIN
	BIN	BIN

Sector/ Block	交二版	交三版(草案)
S4B0~2 S5B0~2	最近六筆交易記錄資料(S4B0~B2/S5B0~B2)	
	資料項目	長度 (Byte)
	交易序號	1
	交易時間	4
	交易類別	1
	交易票值/票點	2
	交易後票值/票點	2
	交易系統編號	1
	交易地點/RSU 編號	1
	交易機器/OBU 編號	4
		屬性
		BIN
		UNIX
		BIN
		BIN
		BIN
		BIN
		BIN
S6~S8	系統應用資料	
		未更改

未更改

未更改

Sector/ Block	交二版	交三版(草案)																																												
S9B0	系統應用資料	異機進出連續型封閉交易系統定期票卡管理資料(S9B0) <table><tr><th>序號</th><th>資料項目</th><th>長度(Byte)</th><th>屬性</th></tr><tr><td>1</td><td>發卡單位編碼</td><td>1</td><td>BIN</td></tr><tr><td>2</td><td>交易系統編號/ 發行公司代碼</td><td>1</td><td>BIN</td></tr><tr><td>3</td><td>票卡種類</td><td>1</td><td>BIN</td></tr><tr><td>4</td><td>有效起始日</td><td>2</td><td>DOSDate</td></tr><tr><td>5</td><td>有效到期日</td><td>2</td><td>DOSDate</td></tr><tr><td>6</td><td>進出站代碼 1</td><td>2</td><td>BIN</td></tr><tr><td>7</td><td>進出站代碼 2</td><td>2</td><td>BIN</td></tr><tr><td>8</td><td>最大可使用次數</td><td>1</td><td>BIN</td></tr><tr><td>9</td><td>售出票價</td><td>2</td><td>BIN</td></tr><tr><td>10</td><td>保留</td><td>2</td><td>BIN</td></tr></table>	序號	資料項目	長度(Byte)	屬性	1	發卡單位編碼	1	BIN	2	交易系統編號/ 發行公司代碼	1	BIN	3	票卡種類	1	BIN	4	有效起始日	2	DOSDate	5	有效到期日	2	DOSDate	6	進出站代碼 1	2	BIN	7	進出站代碼 2	2	BIN	8	最大可使用次數	1	BIN	9	售出票價	2	BIN	10	保留	2	BIN
序號	資料項目	長度(Byte)	屬性																																											
1	發卡單位編碼	1	BIN																																											
2	交易系統編號/ 發行公司代碼	1	BIN																																											
3	票卡種類	1	BIN																																											
4	有效起始日	2	DOSDate																																											
5	有效到期日	2	DOSDate																																											
6	進出站代碼 1	2	BIN																																											
7	進出站代碼 2	2	BIN																																											
8	最大可使用次數	1	BIN																																											
9	售出票價	2	BIN																																											
10	保留	2	BIN																																											

Sector/ Block	交二版	交三版(草案)																																								
S9/B1~2	系統應用資料	異機進出連續型封閉交易系統交易記錄 (1) (2) (S9B1/B9B2) <table><tr><th>序號</th><th>資料項目</th><th>長度(Byte)</th><th>屬性</th></tr><tr><td>1</td><td>已使用次數</td><td>1</td><td>BIN</td></tr><tr><td>2</td><td>首次交易日期</td><td>2</td><td>DOSDate</td></tr><tr><td>3</td><td>交易系統編號</td><td>1</td><td>BIN</td></tr><tr><td>4</td><td>交易單位代碼</td><td>1</td><td>BIN</td></tr><tr><td>5</td><td>交易類別</td><td>1</td><td>BIN</td></tr><tr><td>6</td><td>進出站代碼</td><td>2</td><td>BIN</td></tr><tr><td>7</td><td>交易時間</td><td>4</td><td>BIN</td></tr><tr><td>8</td><td>交易機器流水號/OBU 編號</td><td>2</td><td>BIN</td></tr><tr><td>9</td><td>實扣交易票值(預收/尾款)</td><td>2</td><td>BIN</td></tr></table>	序號	資料項目	長度(Byte)	屬性	1	已使用次數	1	BIN	2	首次交易日期	2	DOSDate	3	交易系統編號	1	BIN	4	交易單位代碼	1	BIN	5	交易類別	1	BIN	6	進出站代碼	2	BIN	7	交易時間	4	BIN	8	交易機器流水號/OBU 編號	2	BIN	9	實扣交易票值(預收/尾款)	2	BIN
序號	資料項目	長度(Byte)	屬性																																							
1	已使用次數	1	BIN																																							
2	首次交易日期	2	DOSDate																																							
3	交易系統編號	1	BIN																																							
4	交易單位代碼	1	BIN																																							
5	交易類別	1	BIN																																							
6	進出站代碼	2	BIN																																							
7	交易時間	4	BIN																																							
8	交易機器流水號/OBU 編號	2	BIN																																							
9	實扣交易票值(預收/尾款)	2	BIN																																							

Sector/ Block	交二版	交三版(草案)																																												
S10/B0	系統應用資料	同機進出連續型封閉交易系統定期票卡管理資料(S10B0)																																												
		<table><tr><th>序號</th><th>資料項目</th><th>長度(Byte)</th><th>屬性</th></tr><tr><td>1</td><td>發卡單位編碼</td><td>1</td><td>BIN</td></tr><tr><td>2</td><td>交易系統編號/ 發行公司代碼</td><td>1</td><td>BIN</td></tr><tr><td>3</td><td>票卡種類</td><td>1</td><td>BIN</td></tr><tr><td>4</td><td>有效起始日</td><td>2</td><td>DOSDate</td></tr><tr><td>5</td><td>有效到期日</td><td>2</td><td>DOSDate</td></tr><tr><td>6</td><td>上/下站代碼 1</td><td>2</td><td>BIN</td></tr><tr><td>7</td><td>上/下站代碼 2</td><td>2</td><td>BIN</td></tr><tr><td>8</td><td>最大可使用次數</td><td>1</td><td>BIN</td></tr><tr><td>9</td><td>可用路線/路線群組代碼</td><td>2</td><td>BIN</td></tr><tr><td>10</td><td>售出票價</td><td>2</td><td>BIN</td></tr></table>	序號	資料項目	長度(Byte)	屬性	1	發卡單位編碼	1	BIN	2	交易系統編號/ 發行公司代碼	1	BIN	3	票卡種類	1	BIN	4	有效起始日	2	DOSDate	5	有效到期日	2	DOSDate	6	上/下站代碼 1	2	BIN	7	上/下站代碼 2	2	BIN	8	最大可使用次數	1	BIN	9	可用路線/路線群組代碼	2	BIN	10	售出票價	2	BIN
		序號	資料項目	長度(Byte)	屬性																																									
		1	發卡單位編碼	1	BIN																																									
		2	交易系統編號/ 發行公司代碼	1	BIN																																									
		3	票卡種類	1	BIN																																									
		4	有效起始日	2	DOSDate																																									
		5	有效到期日	2	DOSDate																																									
		6	上/下站代碼 1	2	BIN																																									
		7	上/下站代碼 2	2	BIN																																									
		8	最大可使用次數	1	BIN																																									
		9	可用路線/路線群組代碼	2	BIN																																									
10	售出票價	2	BIN																																											

Sector/ Block	交二版	交三版(草案)																																												
S10/B1~2	系統應用資料	同機進出連續型封閉交易系統交易記錄(1)(2) (S10B1/B10B2)																																												
		<table><tr><th>序號</th><th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr><tr><td>1</td><td>已使用次數</td><td>1</td><td>BIN</td></tr><tr><td>2</td><td>首次交易日期</td><td>2</td><td>DOSDate</td></tr><tr><td>3</td><td>交易系統編號</td><td>1</td><td>BIN</td></tr><tr><td>4</td><td>交易單位代碼</td><td>1</td><td>BIN</td></tr><tr><td>5</td><td>交易類別</td><td>1</td><td>BIN</td></tr><tr><td>6</td><td>上/下站序號</td><td>1</td><td>BIN</td></tr><tr><td>7</td><td>交易時間</td><td>4</td><td>BIN</td></tr><tr><td>8</td><td>路線代碼</td><td>2</td><td>BIN</td></tr><tr><td>9</td><td>交易機器流水號/OBU 編號</td><td>1</td><td>BIN</td></tr><tr><td>10</td><td>實扣交易票值(預收/尾款)</td><td>2</td><td>BIN</td></tr></table>	序號	資料項目	長度 (Byte)	屬性	1	已使用次數	1	BIN	2	首次交易日期	2	DOSDate	3	交易系統編號	1	BIN	4	交易單位代碼	1	BIN	5	交易類別	1	BIN	6	上/下站序號	1	BIN	7	交易時間	4	BIN	8	路線代碼	2	BIN	9	交易機器流水號/OBU 編號	1	BIN	10	實扣交易票值(預收/尾款)	2	BIN
		序號	資料項目	長度 (Byte)	屬性																																									
		1	已使用次數	1	BIN																																									
		2	首次交易日期	2	DOSDate																																									
		3	交易系統編號	1	BIN																																									
		4	交易單位代碼	1	BIN																																									
		5	交易類別	1	BIN																																									
		6	上/下站序號	1	BIN																																									
		7	交易時間	4	BIN																																									
		8	路線代碼	2	BIN																																									
		9	交易機器流水號/OBU 編號	1	BIN																																									
10	實扣交易票值(預收/尾款)	2	BIN																																											

Sector/ Block	交二版	交三版(草案)																																																				
S11/B0	系統應用資料	非連續型封閉交易系統應用資料區(S11B0)																																																				
		<table><tr><th>序號</th><th>資料項目</th><th>長度 (Byte)</th><th>屬性</th></tr><tr><td>1</td><td>交易系統編號 A</td><td>1</td><td>BIN</td></tr><tr><td>2</td><td>發行單位代碼 A</td><td>1</td><td>BIN</td></tr><tr><td>3</td><td>票卡種類+延伸使用碼 A (1bit)</td><td>1</td><td>BIN</td></tr><tr><td>4</td><td>有效起始日 A</td><td>2</td><td>DOSDate</td></tr><tr><td>5</td><td>有效到期日 A</td><td>2</td><td>DOSDate</td></tr><tr><td>6</td><td>可使用之場站/場站群組代碼 A</td><td>1</td><td>BIN</td></tr><tr><td>7</td><td>交易系統編號 B</td><td>1</td><td>BIN</td></tr><tr><td>8</td><td>發行單位代碼 B</td><td>1</td><td>BIN</td></tr><tr><td>9</td><td>票卡種類+延伸使用碼 B (1bit)</td><td>1</td><td>BIN</td></tr><tr><td>10</td><td>有效起始日 B</td><td>2</td><td>DOSDate</td></tr><tr><td>11</td><td>有效到期日 B</td><td>2</td><td>DOSDate</td></tr><tr><td>12</td><td>可使用之場站/場站群組代碼 B</td><td>1</td><td>BIN</td></tr></table>	序號	資料項目	長度 (Byte)	屬性	1	交易系統編號 A	1	BIN	2	發行單位代碼 A	1	BIN	3	票卡種類+延伸使用碼 A (1bit)	1	BIN	4	有效起始日 A	2	DOSDate	5	有效到期日 A	2	DOSDate	6	可使用之場站/場站群組代碼 A	1	BIN	7	交易系統編號 B	1	BIN	8	發行單位代碼 B	1	BIN	9	票卡種類+延伸使用碼 B (1bit)	1	BIN	10	有效起始日 B	2	DOSDate	11	有效到期日 B	2	DOSDate	12	可使用之場站/場站群組代碼 B	1	BIN
		序號	資料項目	長度 (Byte)	屬性																																																	
		1	交易系統編號 A	1	BIN																																																	
		2	發行單位代碼 A	1	BIN																																																	
		3	票卡種類+延伸使用碼 A (1bit)	1	BIN																																																	
		4	有效起始日 A	2	DOSDate																																																	
		5	有效到期日 A	2	DOSDate																																																	
		6	可使用之場站/場站群組代碼 A	1	BIN																																																	
		7	交易系統編號 B	1	BIN																																																	
		8	發行單位代碼 B	1	BIN																																																	
		9	票卡種類+延伸使用碼 B (1bit)	1	BIN																																																	
		10	有效起始日 B	2	DOSDate																																																	
11	有效到期日 B	2	DOSDate																																																			
12	可使用之場站/場站群組代碼 B	1	BIN																																																			

Sector/ Block	交二版	交三版(草案)																																												
S11/B1~2	系統應用資料	非連續型封閉交易系統最近兩筆交易記錄(1)(2) (S11B1/B11B2) <table><tr><td>序號</td><td>資料項目</td><td>長度 (Byte)</td><td>屬性</td></tr><tr><td>1</td><td>P1：交易系統編號</td><td>1</td><td>BIN</td></tr><tr><td>2</td><td>P1：交易單位代碼</td><td>1</td><td>BIN</td></tr><tr><td>3</td><td>P1：交易類別</td><td>1</td><td>BIN</td></tr><tr><td>4</td><td>P1：交易時間</td><td>4</td><td>UNIX</td></tr><tr><td>5</td><td>P1：場站代碼</td><td>1</td><td>BIN</td></tr><tr><td>6</td><td>P2：交易系統編號</td><td>1</td><td>BIN</td></tr><tr><td>7</td><td>P2：交易單位代碼</td><td>1</td><td>BIN</td></tr><tr><td>8</td><td>P2：交易類別</td><td>1</td><td>BIN</td></tr><tr><td>9</td><td>P2：交易時間</td><td>4</td><td>UNIX</td></tr><tr><td>10</td><td>P2：場站代碼</td><td>1</td><td>BIN</td></tr></table>	序號	資料項目	長度 (Byte)	屬性	1	P1：交易系統編號	1	BIN	2	P1：交易單位代碼	1	BIN	3	P1：交易類別	1	BIN	4	P1：交易時間	4	UNIX	5	P1：場站代碼	1	BIN	6	P2：交易系統編號	1	BIN	7	P2：交易單位代碼	1	BIN	8	P2：交易類別	1	BIN	9	P2：交易時間	4	UNIX	10	P2：場站代碼	1	BIN
序號	資料項目	長度 (Byte)	屬性																																											
1	P1：交易系統編號	1	BIN																																											
2	P1：交易單位代碼	1	BIN																																											
3	P1：交易類別	1	BIN																																											
4	P1：交易時間	4	UNIX																																											
5	P1：場站代碼	1	BIN																																											
6	P2：交易系統編號	1	BIN																																											
7	P2：交易單位代碼	1	BIN																																											
8	P2：交易類別	1	BIN																																											
9	P2：交易時間	4	UNIX																																											
10	P2：場站代碼	1	BIN																																											
S12~S15	系統應用資料	保 留																																												

附錄 6

減值主金鑰組電文檔

減值主金鑰組電文檔

A.1 電文檔規格

Description: 減值主金鑰組電文檔規格

File Format: DKS_[yyyymmddvv].DAT

Sample: DKS_2004060701.DAT

Header Record

No.	Field Name	Length	Attribute	Description
1.	Rec_flag	1	a, MF	資料標誌 固定值='H'
2.	Separator	1	a, MF	“,”(always)
3.	Key_Counter	4	n,MF,RJ,L Z	金鑰總數
4.	Record Separator	2	h, MF	0x0d, 0x0a

Total Length **8**

Detail Record(1)

No.	Field Name	Length	Attribute	Description
1.	Rec_flag	1	a,MF	資料標誌 固定值='D'
2.	Separator	1	a, MF	“,”(always)
3.	Sector_Number	2	n,MF,RJ,LZ	扇區編號
4.	Separator	1	a, MF	“,”(always)
5.	Key_Type	1	a,MF	金鑰種類 ‘A’ : 表 Key A ‘B’ : 表 Key B
6.	Separator	1	a, MF	“,”(always)
7.	Key_Value	32	a,MF	金鑰值
8.	Reserved	6	a,FS	保留 固定值= space
9.	Record Separator	2	h, MF	0x0d, 0x0a

Total Length **47**

Detail Record(2)

No.	Field Name	Length	Attribute	Description
10.	Rec_flag	1	a,MF	資料標誌 固定值='M'
11.	Separator	1	a, MF	“,”(always)
12.	Reserved	2	a,FS	保留 固定值= space
13.	Separator	1	a, MF	“,”(always)
14.	Key_Type	1	a,MF	金鑰種類 ‘C’ : CAC Key
15.	Separator	1	a, MF	“,”(always)
16.	Key_Value	32	a,MF	金鑰值
17.	Reserved	6	a,FS	保留 固定值= space
18.	Record Separator	2	h, MF	0x0d, 0x0a

Total Length **47**

Trailer

No.	Field Name	Length	Attribute	Description
1.	Rec_flag	1	a, MF	資料標誌 固定值='T'
2.	Record Separator	2	h, MF	0x0d, 0x0a

Total Length **3**

Field Attributes:

MF: must be fill

LJ: left justify

TS: trailing space

RJ: right justify

LZ: leading zero

FS: fill space if not available

LS: leading space

A.2 電文檔範例

H, 0010

D, 00, A, A0A0A0A0A0A0A0A00000000000000000

D, 01, A, A1A1A1A1A1A1A1A1111111111111111

D, 02, A, A2A2A2A2A2A2A2A2222222222222222

D, 03, B, B3B3B3B3B3B3B3B3333333333333333

D, 04, B, B4B4B4B4B4B4B4B4444444444444444

D, 05, B, B5B5B5B5B5B5B5B5555555555555555

D, 09, B, B9B9B9B9B9B9B9B9999999999999999

D, 10, B, BABABABABABABABAAAAAAAAAAAAAAAAAA

D, 11, B, BBBB BBBB BBBB BBBB BBBB BBBB BBBB BBBB

M, , C, 33333333333333333333333333333333

T

附錄 7

廠商測試申請表

廠商測試申請表

申請日期： 年 月 日

廠 商 填 寫	公司名稱：	
	公司地址：	
	公司電話：	公司傳真：
	聯絡人：	行動電話：
	Email Address：	
	開發工程師：	
	公司電話：	行動電話：
	Email Address：	
	測試設備種類及其數量：	
	測試特別注意事項：	
	預計測試期間： 年 月 日 — 年 月 日	

廠商須檢附之相關文件

- ☐ 設備操作手冊
- ☐ 減值主金鑰組電文檔
- ☐ 測試用卡片三組及卡片種類說明文件

註：檢附之相關文件請打勾

附錄 8

靜態驗證程式之測試紀錄檔樣本

靜態驗證程式之測試紀錄檔樣本

驗測基本資料：

公司名稱：acer

卡 別：一般民眾

驗測次數：1

驗測時間：2008/11/7 15:39:24

驗證項目：卡片金鑰存取驗證

扇區位置	金鑰種類	認證測試	讀取測試	寫入測試	驗證結果
0	A	成功	成功	失敗	通過
1	A	成功	成功	失敗	通過
2	A	成功	成功	失敗	通過
3	B	成功	成功	成功	通過
4	B	成功	成功	成功	通過
5	B	成功	成功	成功	通過
9	B	成功	成功	成功	通過
10	B	成功	成功	成功	通過
11	B	成功	成功	成功	通過

扇區位置：S0

區塊位置：B0

區塊內容：卡片出廠資料

資料項目	資料內容	驗證結果
卡片序號	DAB91600	----
廠商批號	7588040047C12550E5002106	----

扇區位置：S0

區塊位置：B1, B2

區塊內容：目錄服務指標

資料項目	資料內容	驗證結果
檢查碼	F008	通過
AID01	F109	通過
AID02	F20A	通過
AID03	F30B	通過

AID04	0000	通過
AID05	0000	通過
AID06	0000	通過
AID07	0000	通過
AID08	0000	通過
AID09	0000	通過
AID10	0000	通過
AID11	0000	通過
AID12	0000	通過
AID13	0000	通過
AID14	0000	通過
AID15	0000	通過

扇區位置：S1

區塊位置：B0

區塊內容：發行管理資料

資料項目	資料內容	驗證結果
發卡單位編碼	02	通過
發卡設備編碼	0102	----
發行批號	3333	----
發行日期	662EC848	----
有效日期	E6DCBF5E	----
卡片規格版本	30	----
卡片狀態	01	通過
檢查碼	23	通過

扇區位置：S1

區塊位置：B1

區塊內容：票值管理資料

資料項目	資料內容	驗證結果
自動加值設定	FF	通過
自動加值票值數額	B80B	----
儲存最大票值數額	1027	----
每筆可扣減最大票值數額	F401	----
自動加值銀行代碼	13	----
基本身分別	00	通過
基本身分區碼	20	通過
優惠補助身分	11	通過
優惠補助身分有效日	392A	----

優惠補助最大次數	7800	----
檢查碼	C7	通過

扇區位置：S1

區塊位置：B2

區塊內容：卡片防偽驗證資料

資料項目	資料內容	驗證結果
防偽驗證資料	F655318F298C2F55D56B2E92F60B8D0F	通過

扇區位置：S2

區塊位置：B0

區塊內容：主要票值

資料項目	資料內容	驗證結果
電子票值	741200008BEDFFFF7412000008F708F7	通過

扇區位置：S2

區塊位置：B1

區塊內容：票值備份

資料項目	資料內容	驗證結果
備份電子票值	741200008BEDFFFF7412000008F708F7	通過

扇區位置：S3

區塊位置：B0

區塊內容：卡片交易狀態資料

資料項目	資料內容	驗證結果
卡片交易序號	6402	----
交易記錄檔指標	00	通過
優惠積點數	5000	----
優惠積點交易序號	AB22	----
鎖卡旗標	01	----
每日優惠累計轉乘點數	6400	----
轉乘優惠日期	392A	通過
特殊身分優惠累計次數	6400	----
加值累計點數		

扇區位置：S3

區塊位置：B1

區塊內容：最近兩筆交易記錄(一)

資料項目	資料內容	驗證結果
------	------	------

交易序號	23	通過
交易時間	662EC848	----
交易類別	01	通過
交易票值	6400	----
交易後票	ACOD	----
交易系統編碼	02	通過
交易地點	01	----
交易機器	31313131	----

扇區位置：S3

區塊位置：B2

區塊內容：最近兩筆交易記錄(二)

資料項目	資料內容	驗證結果
交易序號	23	通過
交易時間	272EC848	----
交易類別	01	通過
交易票值	6400	----
交易後票	ACOD	----
交易系統編碼	02	通過
交易地點	01	----
交易機器	32323232	----

扇區位置：S4

區塊位置：B0

區塊內容：最近六筆交易記錄資料(一)

資料項目	資料內容	驗證結果
交易序號	5F	通過
交易時間	A129C848	----
交易類別	01	通過
交易票值	6400	----
交易後票	ACOD	----
交易系統編碼	02	通過
交易地點	01	----
交易機器	40404040	----

扇區位置：S4

區塊位置：B1

區塊內容：最近六筆交易記錄資料(二)

資料項目	資料內容	驗證結果
------	------	------

交易序號	60	通過
交易時間	672AC848	----
交易類別	01	通過
交易票值	6400	----
交易後票	ACOD	----
交易系統編碼	02	通過
交易地點	01	----
交易機器	41414141	----

扇區位置：S4

區塊位置：B2

區塊內容：最近六筆交易記錄資料(三)

資料項目	資料內容	驗證結果
交易序號	61	通過
交易時間	232BC848	----
交易類別	01	通過
交易票值	6400	----
交易後票	ACOD	----
交易系統編碼	02	通過
交易地點	01	----
交易機器	42424242	----

扇區位置：S5

區塊位置：B0

區塊內容：最近六筆交易記錄資料(四)

資料項目	資料內容	驗證結果
交易序號	62	通過
交易時間	B62CC848	----
交易類別	01	通過
交易票值	6400	----
交易後票	ACOD	----
交易系統編碼	02	通過
交易地點	01	----
交易機器	50505050	----

扇區位置：S5

區塊位置：B1

區塊內容：最近六筆交易記錄資料(五)

資料項目	資料內容	驗證結果
------	------	------

交易序號	63	通過
交易時間	CD2DC848	----
交易類別	01	通過
交易票值	6400	----
交易後票	ACOD	----
交易系統編碼	02	通過
交易地點	01	----
交易機器	51515151	----

扇區位置：S5

區塊位置：B2

區塊內容：最近六筆交易記錄資料(六)

資料項目	資料內容	驗證結果
交易序號	64	通過
交易時間	362EC848	----
交易類別	01	通過
交易票值	6400	----
交易後票	ACOD	----
交易系統編碼	02	通過
交易地點	01	----
交易機器	52525252	----

扇區位置：S9

區塊位置：B0

區塊內容：定期票票卡管理資料

資料項目	資料內容	驗證結果
發卡單位編碼	02	通過
交易系統編碼	04	----
票卡種類	10	----
有效起始日	392A	通過
有效到期日	392A	通過
進出站代碼 1	0200	----
進出站代碼 2	0800	----
最大可使用次數	64	----
售出票價	6400	----

扇區位置：S9

區塊位置：B1

區塊內容：異機進出連續型封閉交易系統最近兩筆交易記錄(一)

資料項目	資料內容	驗證結果
已使用次數	23	----
首次交易日	392A	通過
交易系統編碼	02	通過
交易單位代碼	03	----
交易類別	01	通過
進出站代碼	6400	----
交易時間	662E	----
交易機器流水號	A1A2	----
實扣交易票值	AC0D	----

扇區位置：S9

區塊位置：B2

區塊內容：異機進出連續型封閉交易系統最近兩筆交易記錄(二)

資料項目	資料內容	驗證結果
已使用次數	23	----
首次交易日	392A	通過
交易系統編碼	02	通過
交易單位代碼	03	----
交易類別	01	通過
進出站代碼	6400	----
交易時間	662E	----
交易機器流水號	A1A2	----
實扣交易票值	AC0D	----

扇區位置：S10

區塊位置：B0

區塊內容：定期票票卡管理資料

資料項目	資料內容	驗證結果
發卡單位編碼	02	通過
交易系統編碼	04	----
票卡種類	10	----
有效起始日	392A	通過
有效到期日	392A	通過
上/下站代碼 1	0200	----
上/下站代碼 2	0800	----
最大可使用次數	64	----
可用路線	0300	----
售出票價	6400	----

扇區位置：S10

區塊位置：B1

區塊內容：同機進出連續型封閉交易系統最近兩筆交易記錄(一)

資料項目	資料內容	驗證結果
已使用次數	23	----
首次交易日	392A	通過
交易系統編碼	02	通過
交易單位代碼	03	----
交易類別	01	通過
上/下站序號	05	----
交易時間	662E	----
路線代碼	7800	----
交易機器流水號	A1	----
實扣交易票值	AC0D	----

扇區位置：S10

區塊位置：B2

區塊內容：同機進出連續型封閉交易系統最近兩筆交易記錄(二)

資料項目	資料內容	驗證結果
已使用次數	23	----
首次交易日	392A	通過
交易系統編碼	02	通過
交易單位代碼	03	----
交易類別	01	通過
上/下站序號	05	----
交易時間	662E	----
路線代碼	7800	----
交易機器流水號	A2	----
實扣交易票值	AC0D	----

扇區位置：S11

區塊位置：B0

區塊內容：定期票票卡管理資料

資料項目	資料內容	驗證結果
交易系統編碼 A	02	通過
發行單位代碼 A	03	----
票卡種類 A	04	----
有效起始日 A	392A	通過

有效到期日 A	392A	通過
可使用之場站 A	01	----
交易系統編碼 B	02	通過
發行單位代碼 B	03	----
票卡種類 B	04	----
有效起始日 B	392A	通過
有效到期日 B	392A	通過
可使用之場站 B	02	----

扇區位置：S11

區塊位置：B1

區塊內容：非連續型封閉交易系統最近兩筆交易記錄(一)

資料項目	資料內容	驗證結果
P1：交易系統編碼	02	通過
P1：交易單位代碼	03	----
P1：交易類別	01	通過
P1：交易時間	662EC848	----
P1：場站代碼	B1	----
P2：交易系統編碼	02	通過
P2：交易單位代碼	03	----
P2：交易類別	01	通過
P2：交易時間	662EC848	----
P2：場站代碼	B1	----

扇區位置：S11

區塊位置：B2

區塊內容：非連續型封閉交易系統最近兩筆交易記錄(二)

資料項目	資料內容	驗證結果
P1：交易系統編碼	02	通過
P1：交易單位代碼	03	----
P1：交易類別	01	通過
P1：交易時間	662EC848	----
P1：場站代碼	B2	----
P2：交易系統編碼	02	通過
P2：交易單位代碼	03	----
P2：交易類別	01	通過
P2：交易時間	662EC848	----
P2：場站代碼	B2	----

卡片靜態資料驗證結果：

總檢查欄位個數：85

通過個數：85

不通過個數：0

=====

附錄 9

卡片靜態資料顯示列印程式 操作 手冊

目 錄

第一章	前言	1
1.1	範圍.....	1
1.2	系統需求	1
第二章	系統安裝	2
2.1	安裝接觸式讀卡機	2
2.2	安裝 Pegoda 非接觸式讀卡機.....	4
2.3	安裝卡片靜態資料顯示列印程式	7
第三章	系統操作	11
3.1	匯入金鑰	11
3.2	卡片金鑰存取權限驗證與卡片格式驗證	12

第一章 前言

1.1 範圍

卡片靜態資料顯示列印程式之目的在於檢查卡片資料之內容是否符合交三版之格式定義，包含欄位編碼方式、資料型態及金鑰存取權限檢查等，驗證結果(通過或不通過)為資料是否相容於交三版之參考。

1.2 系統需求

一、硬體需求

- Pentium III 800 MHz (或更高)
- 128 MB RAM (建議 256 MB 或更高)
- 40 MB 硬碟空間 (建議 128 MB 或更高)
- USB 連接埠二個
- CD-ROM 或 DVD-ROM 光碟機一台

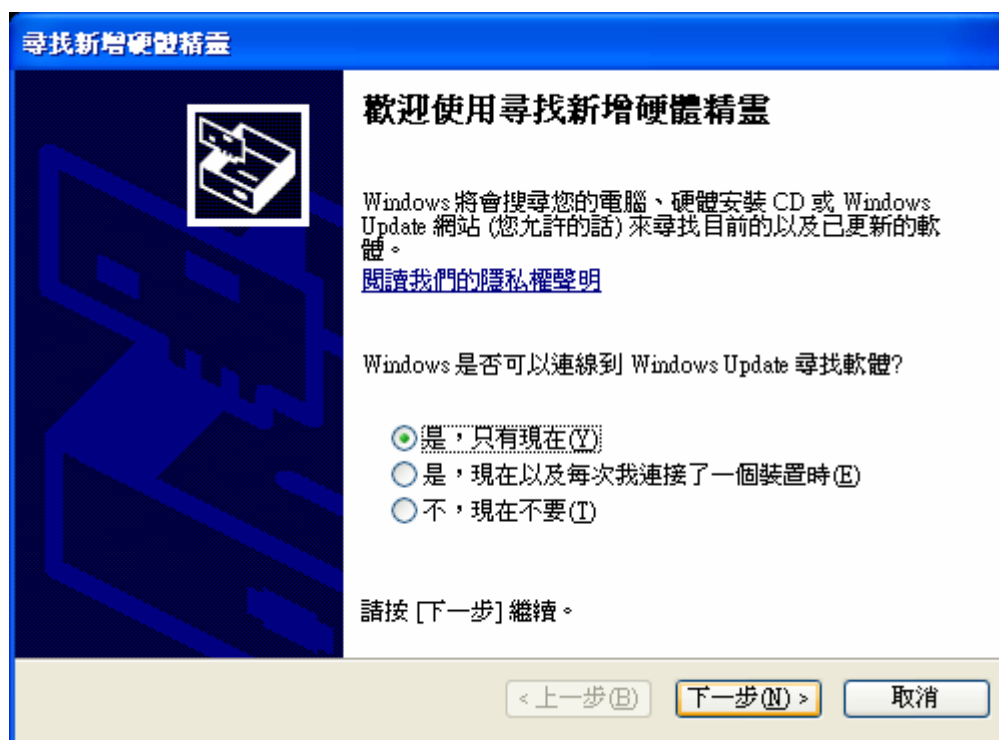
二、軟體需求

- Windows XP Service Pack 2

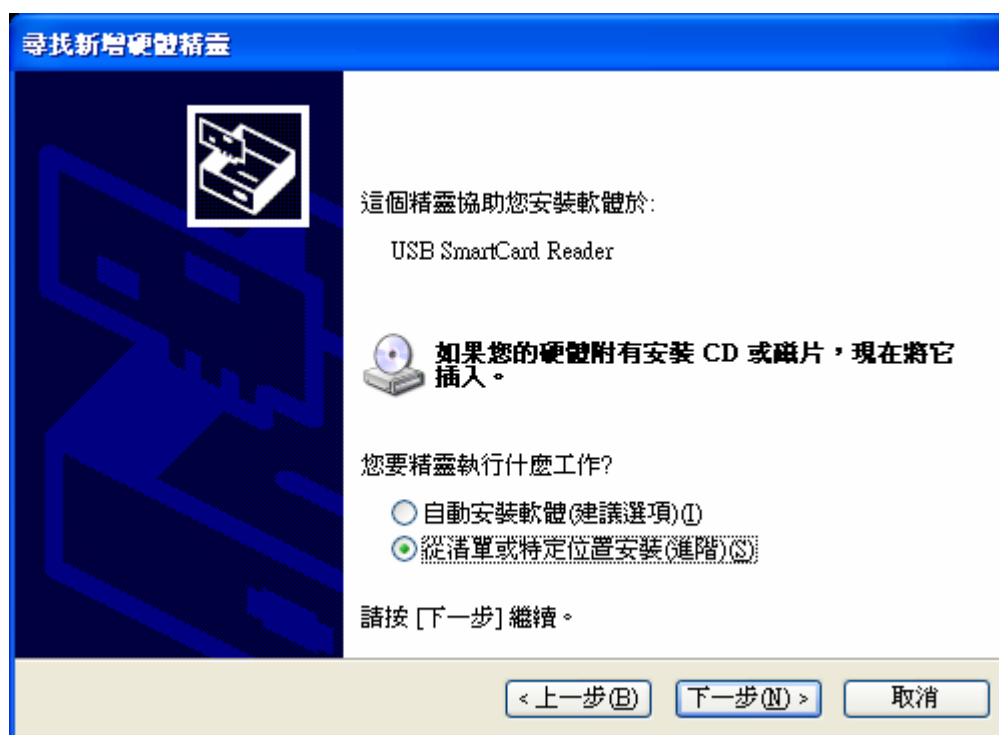
第二章 系統安裝

2.1 安裝接觸式讀卡機

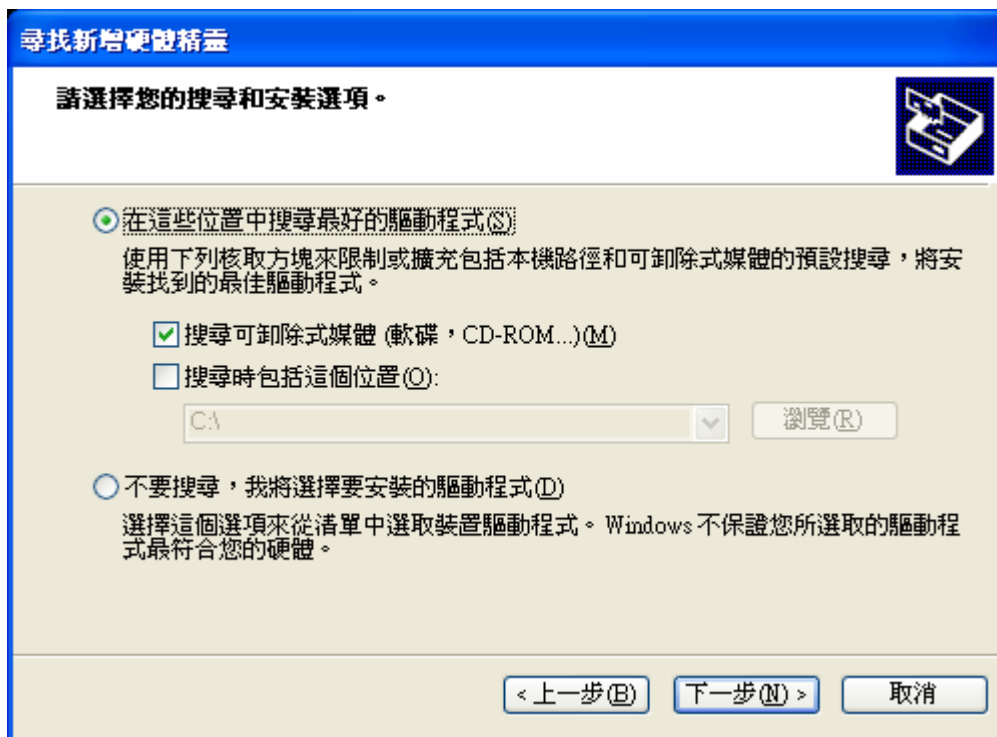
請將讀卡機 GemPC 透過 USB 介面接上電腦，出現安裝驅動程式畫面



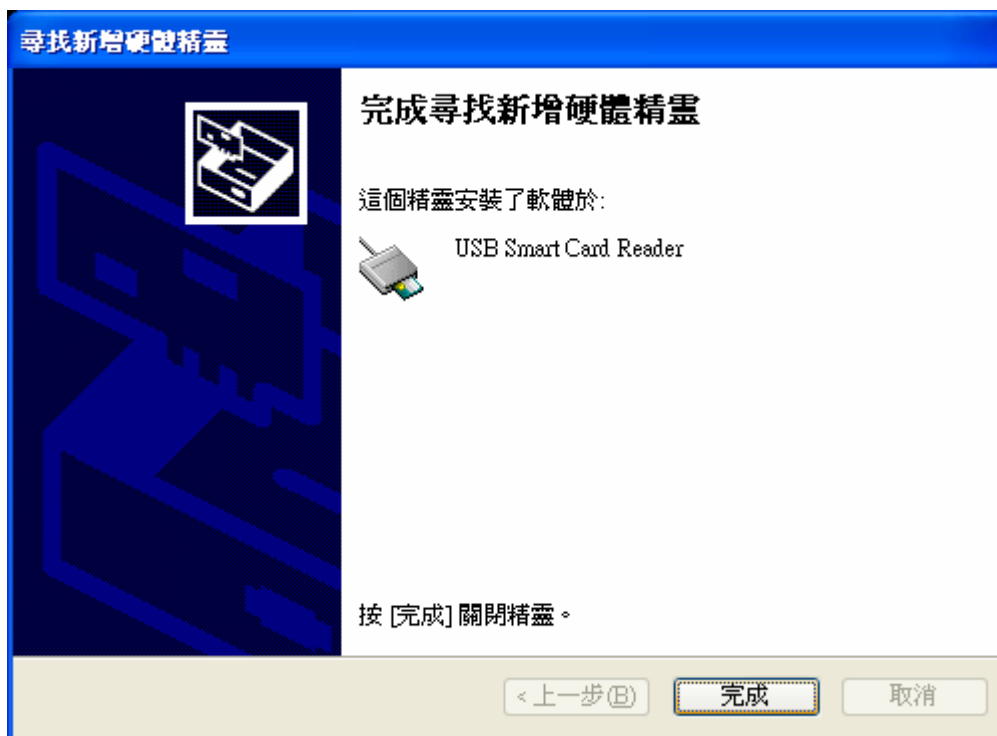
點選下一步



將驅動程式光碟放入光碟機後，點選從清單或特定位置安裝，點選下一步



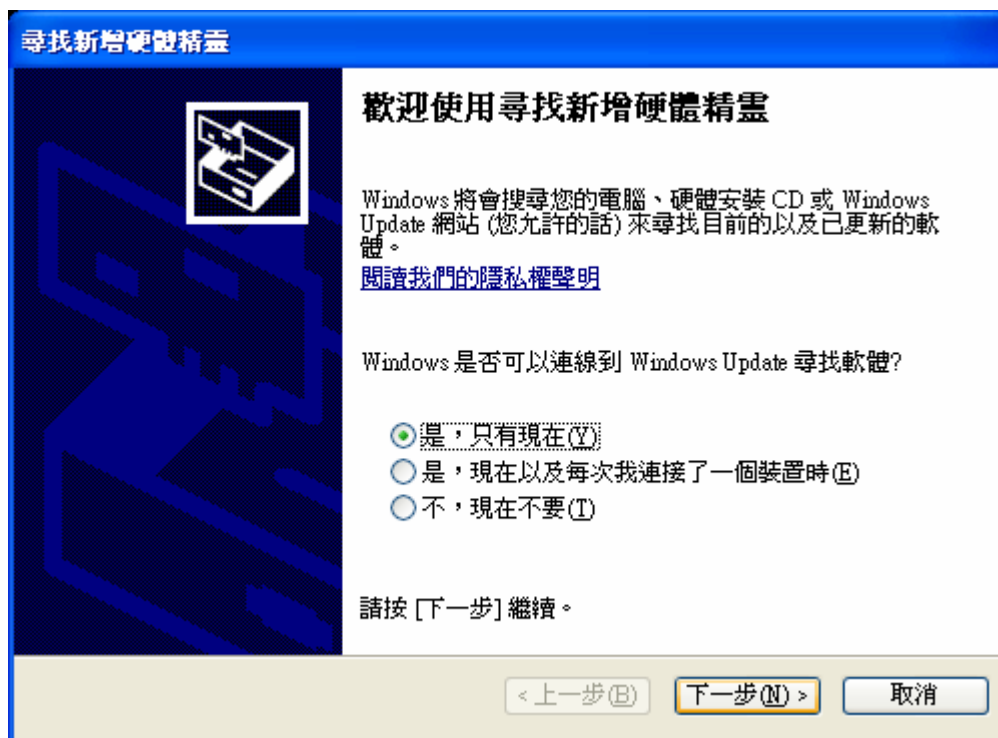
點選下一步



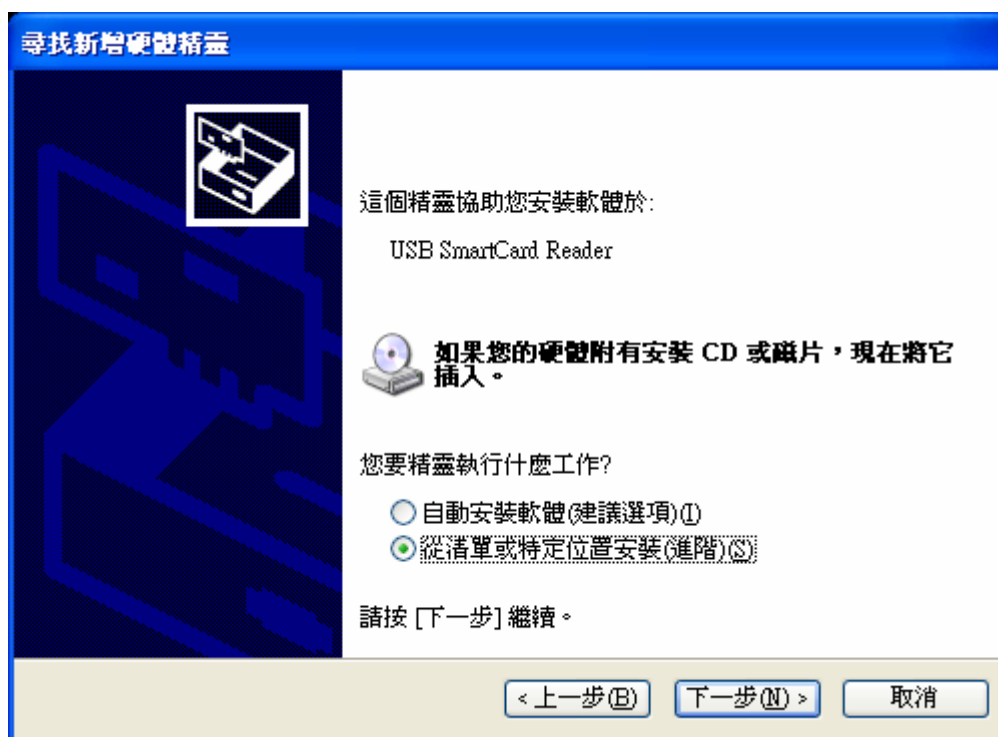
點選完成，USB Smart Card reader 即可使用。

2.2 安裝 Pegoda 非接觸式讀卡機

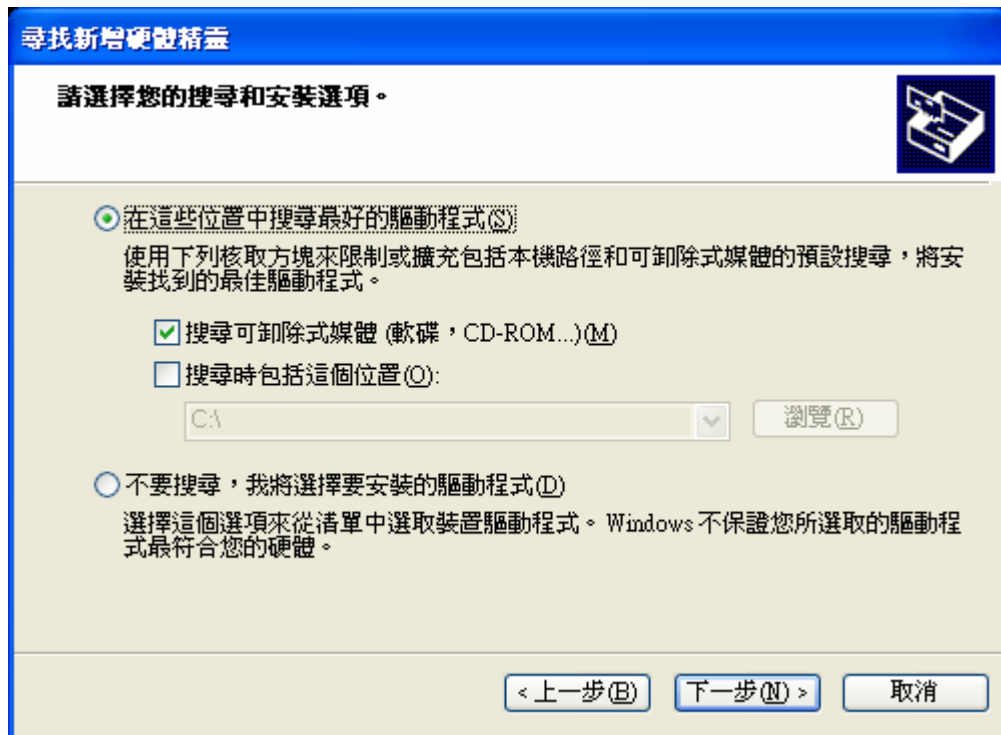
請將 Pegoda 非接觸式讀卡機透過 USB 介面接上電腦，出現安裝驅動程式畫面



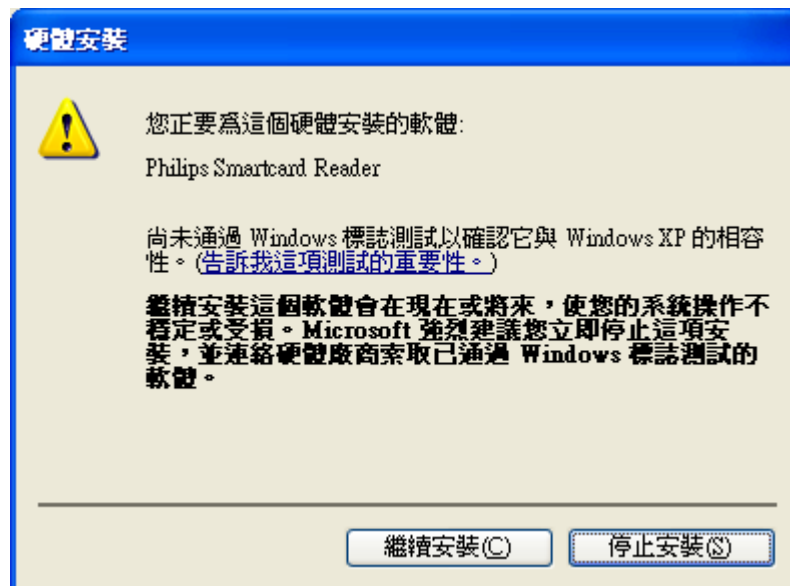
點選下一步



將驅動程式光碟放入光碟機後，點選從清單或特定位置安裝後，點選下一步



點選下一步



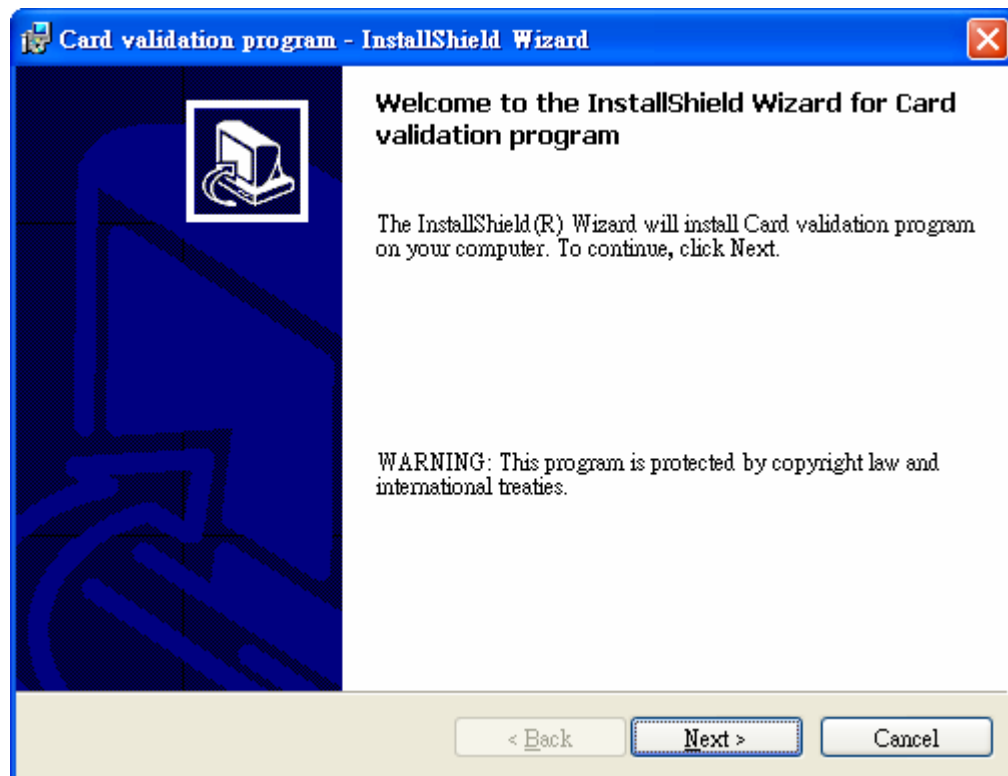
點選繼續安裝



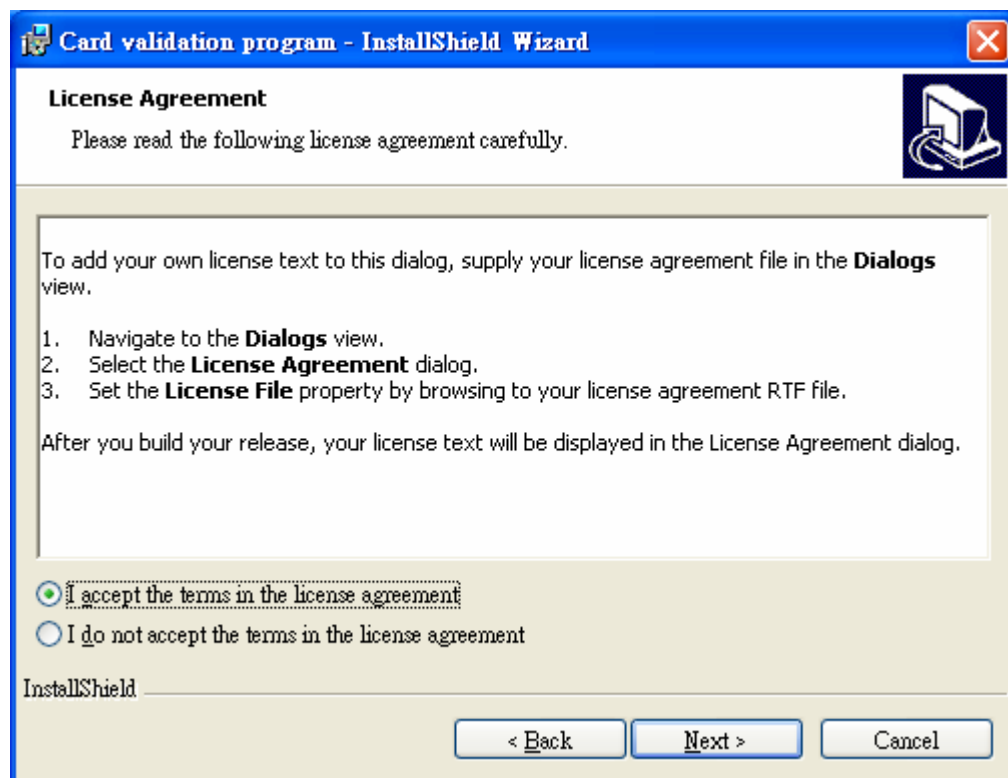
點選完成，即完成安裝 Pegoda 非接觸式讀卡機。

2.3 安裝卡片靜態資料顯示列印程式

安裝光碟中的 CD:\T3V_setup\T3VWnd_setup.exe



點選 next



勾選 I accept 後，點選 next

Card validation program - InstallShield Wizard

Customer Information
Please enter your information.

User Name:
acer

Organization:

Install this application for:

- ☒ Anyone who uses this computer (all users)
- ☐ Only for me (acer)

InstallShield

< Back Next > Cancel

點選 next

Card validation program - InstallShield Wizard

Ready to Install the Program
The wizard is ready to begin installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Current Settings:

Setup Type:

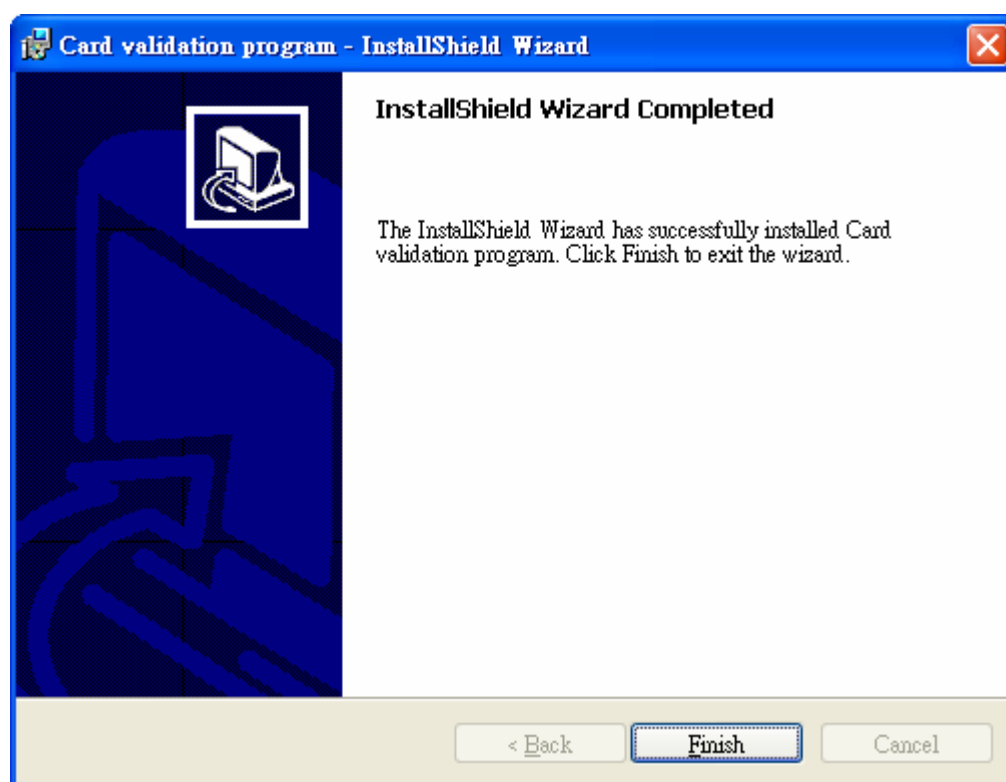
Destination Folder:
C:\T3V\Wnd\

User Information:
Name: acer
Company:

InstallShield

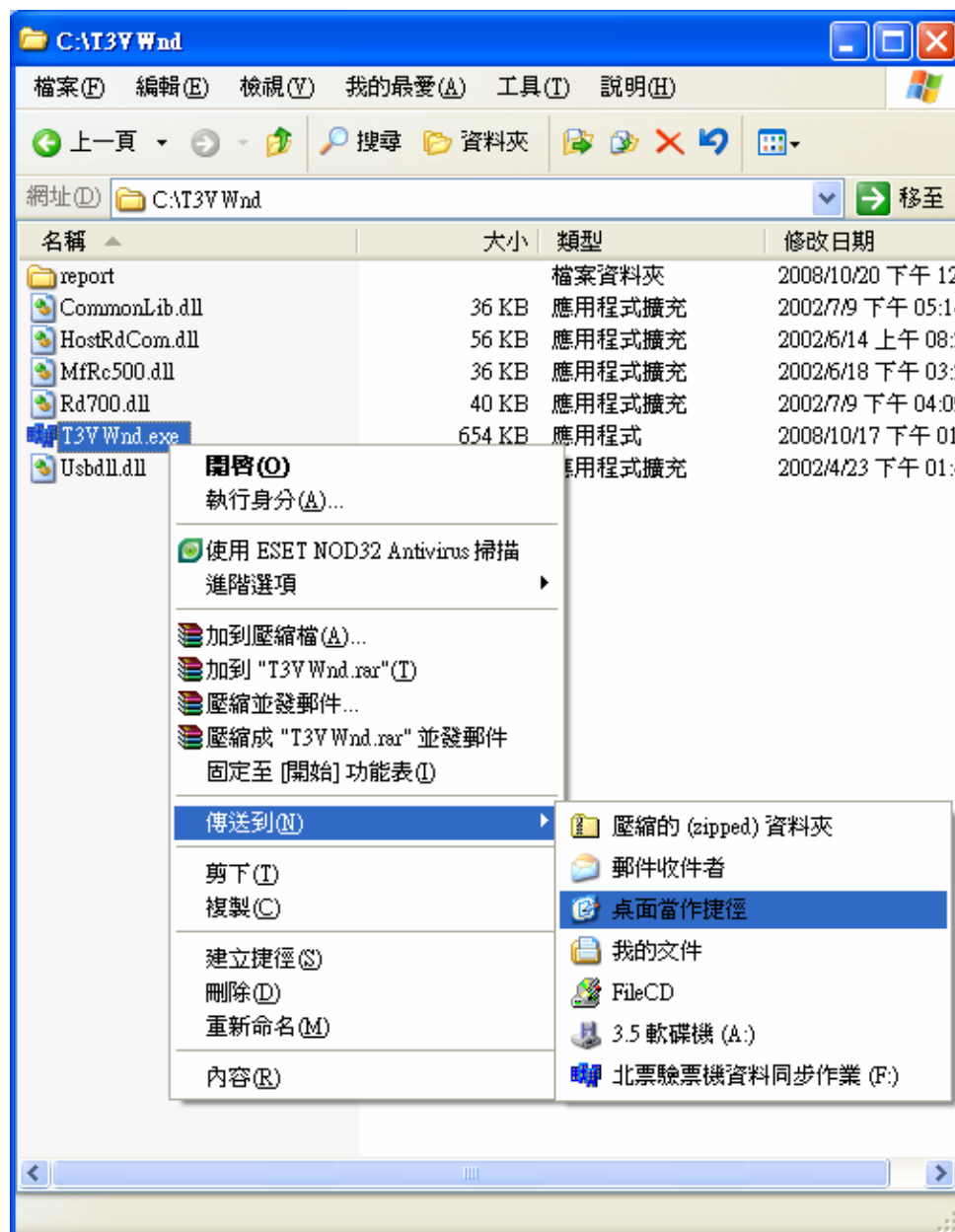
< Back Install Cancel

點選 Install



點選 Finish 完成安裝

主程式位於 C:\T3VWnd\T3VWnd.exe，可將此程式在桌面上建立捷徑

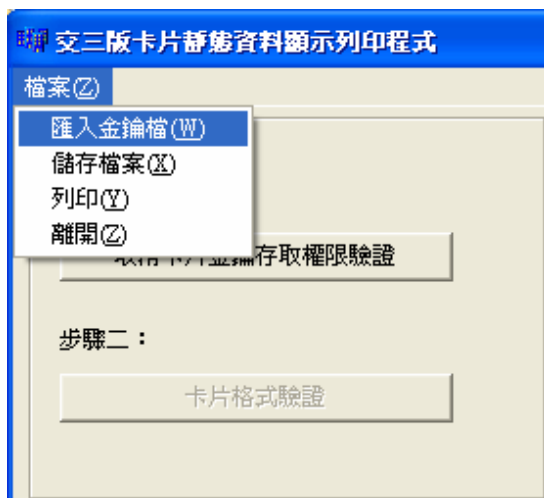


第三章 系統操作

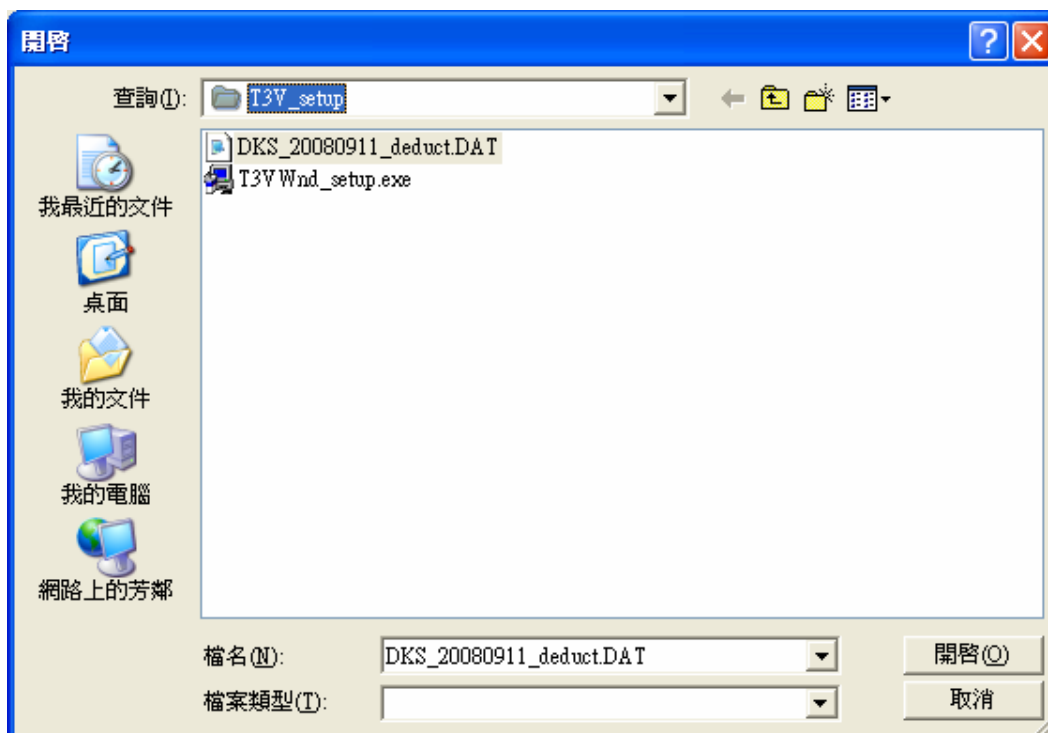
在執行系操作前，請先將安全模組卡片置入接觸式讀卡機中(IC 卡面朝上)，以利系統操作。

3.1 匯入金鑰

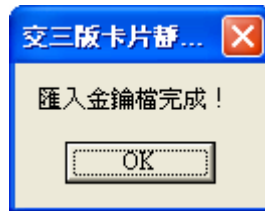
開啟桌面上的 T3VWnd.exe



點選檔案-匯入金鑰檔



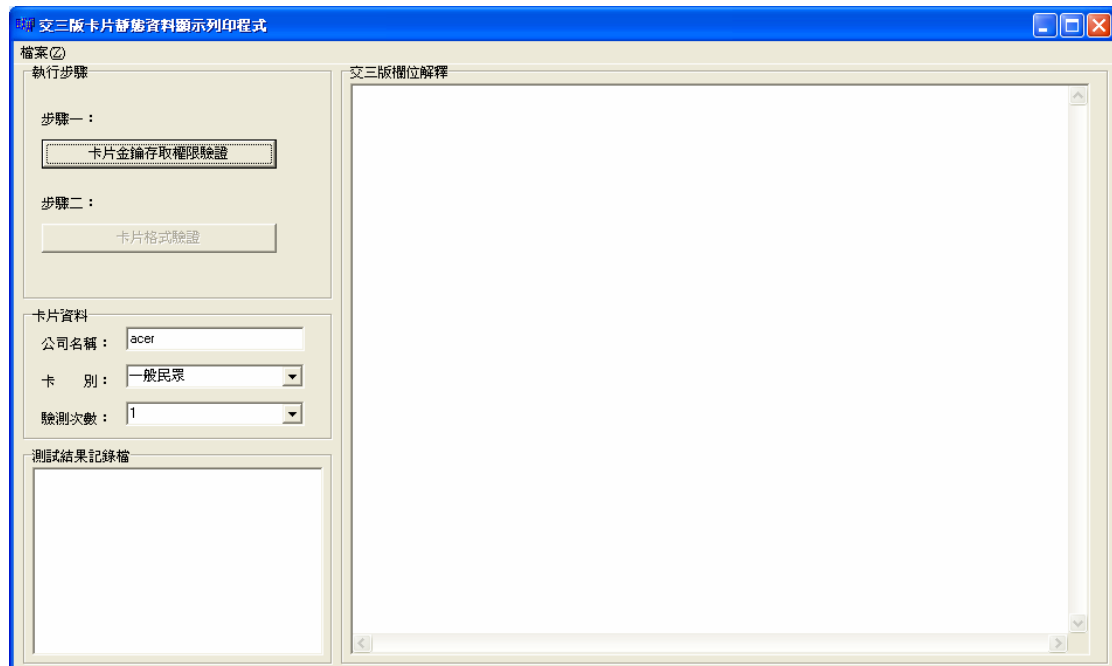
選擇待匯入的金鑰案，例如：如 CD:\T3V_setup\DKS_20080911_deduct.DAT



按下 OK 完成金鑰檔的匯入。

3.2 卡片金鑰存取權限驗證與卡片格式驗證

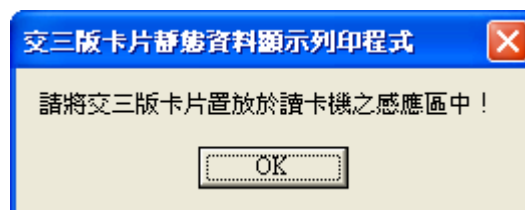
開啓桌面上的 T3VWnd.exe



將安全模組卡片置入 Gemplus 讀卡機，IC 卡片朝上

在公司名稱輸入相關資訊，如：acer

並點選 步驟一：卡片金鑰存取權限驗證



請將交三版卡片置放於 Pegoda 非接觸讀卡機之感應區，然後按 OK。

交三版卡片靜態資料顯示列印程式

檔案(F)

執行步驟

步驟一：

卡片金鑰存取權限驗證

步驟二：

卡片格式驗證

卡片資料

公司名稱：acer

卡別：一般民眾

驗證次數：1

測試結果記錄檔

交三版欄位解釋

驗證基本資料：

公司名稱：acer

卡別：一般民眾

驗證次數：1

驗證時間：2008/11/18 15:53:32

驗證項目：卡片金鑰存取驗證

扇區位置	金鑰種類	認證測試	讀取測試	寫入測試	驗證結果
0	A	成功	成功	無權限	通過
1	A	成功	成功	無權限	通過
2	A	成功	成功	無權限	通過
3	B	成功	成功	成功	通過
4	B	成功	成功	成功	通過
5	B	成功	成功	成功	通過
9	B	成功	成功	成功	通過
10	B	成功	成功	成功	通過
11	B	成功	成功	成功	通過

驗證金鑰存取權限功能後，在程式右方會出現卡片驗證之相關資訊

再按下步驟二：卡片格式驗證

訊息

驗證程序完成，請取回受測卡片！

確定

按下確定，完成驗證

交三版卡片靜態資料顯示列印程式

檔案(F)

執行步驟

步驟一：

卡片金鑰存取權限驗證

步驟二：

卡片格式驗證

卡片資料

公司名稱：acer

卡別：一般民眾

驗證次數：1

測試結果記錄檔

交三版欄位解釋

區塊位置：B1

區塊內容：非連續型封閉交易系統最近兩筆交易記錄(一)

資料項目	資料內容	驗證結果
P1：交易系統編碼	02	通過
P1：交易單位代碼	03	通過
P1：交易類別	01	通過
P1：交易時間	662EC848	通過
P1：場站代碼	B1	通過
P2：交易系統編碼	02	通過
P2：交易單位代碼	03	通過
P2：交易類別	01	通過
P2：交易時間	662EC848	通過
P2：場站代碼	B1	通過

區塊位置：S11

區塊內容：非連續型封閉交易系統最近兩筆交易記錄(二)

資料項目	資料內容	驗證結果
P1：交易系統編碼	02	通過
P1：交易單位代碼	03	通過
P1：交易類別	01	通過
P1：交易時間	662EC848	通過
P1：場站代碼	B2	通過
P2：交易系統編碼	02	通過
P2：交易單位代碼	03	通過
P2：交易類別	01	通過
P2：交易時間	662EC848	通過
P2：場站代碼	B2	通過

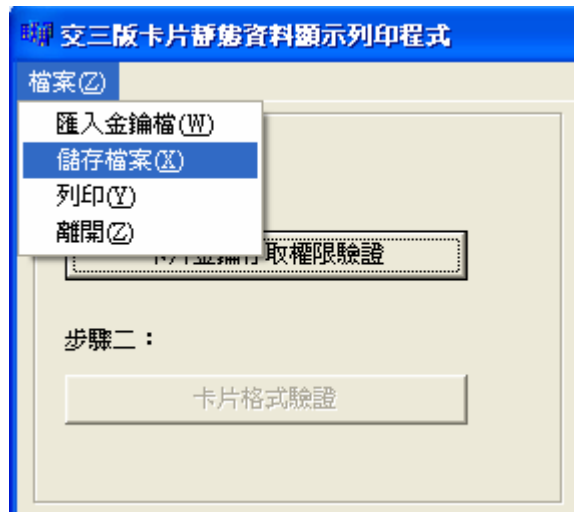
卡片靜態資料驗證結果：

總驗證個數：85

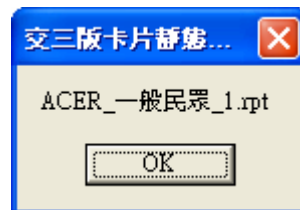
通過個數：85

不通過個數：0

右方欄位會秀出通過總數，與不通過總數，與各項明細



按下檔案-儲存檔案



按下 OK，完成儲存檔案，OK 鍵上的名稱即為存檔檔名
存放的路徑為 C:\T3VWnd\report

附錄 10

更換金鑰作業之標準作業 流程建議

更換金鑰作業之標準作業流程建議

一、準備階段

1. 製作新版加值用 SAM 卡，此 SAM 卡需包含新的主金鑰組。
2. 製作新版減值用 SAM 卡，此 SAM 卡需包含新的主金鑰組。
3. 修改加值機使其能依序操作兩張 SAM 卡進行交易加值及換 Key 作業。功能如下：
 - (1) 交三版卡片進行加值作業時，依序對兩張 SAM 卡(現有版及新版)進行金鑰驗證處理，當其中一張 SAM 卡驗證金鑰成功，則可進行加值作業，若兩張 SAM 卡皆無法完成金鑰驗證作業，則拒絕交易之進行。
 - (2) 當偵測卡片為舊版之卡片時，可執行換 Key 作業，將交三版卡片更新為新版金鑰。
4. 修改驗票機或查詢機使其能依序操作兩張 SAM 卡進行交易扣款。功能如下：
 - (1) 交三版卡片進行減值作業時，依序對兩張 SAM 卡(現有版及更新版)進行金鑰驗證處理，當其中一張 SAM 卡驗證金鑰成功，則可進行減值作業，若兩張 SAM 卡皆無法完成金鑰驗證作業，則拒絕交易之進行

二、設備換裝階段

1. 更新加值機軟體程式，使加值機具備操作兩張 SAM 卡進行交易加值及換 Key 作業。
2. 票證公司將具有新版金鑰組之加值用 SAM 卡加裝至加值機中，此時加值機中具備兩張 SAM 卡，可提供交三版卡片之換 Key 作業，並提供兩種金鑰組交三版卡片(現在版及更新版)進行加值作業。
3. 更新減值設備軟體程式，使減值設備具備操作兩張 SAM 卡進行交易扣款。
4. 票證公司加裝減值用之新金鑰 SAM 卡至驗票機或查詢機，此時減值設備中具備兩張 SAM 卡，提供兩種金鑰組交三版卡片(現在版及更新版)進行減值作業。。

當完成此階段之換裝作業，加值設備及減值設備皆包含兩張 SAM 卡，以利新舊版交三版卡片同時皆可使用。

三、過渡階段

1. 過渡階段為兩張 SAM 卡(現在版及更新版)皆同時存在於加值設備或減值設備之時期，建議期間為一年，以做為換 Key 之過渡階段。
2. 當過渡階段結束，票證公司取出加值設備或減值設備之舊版 SAM 卡(現在版)，交易之進行將以更新版之主金鑰進行金鑰驗證作業。
3. 當過渡階段結束後，未完成換 Key 之卡片將無法進行加值或減值之交易，此時持卡人需將卡片攜至發卡單位指定之服務窗口進行換 Key 後，方可進行交易。