金融監督管理委員會公告

中華民國 104 年 3 月 27 日
金管銀票字第 10440000670 號

主　　旨：預告修正「電子票證應用安全強度準則」部分條文草案。

依　　據：行政程序法第一百五十一條第二項準用第一百五十四條第一項。

公告事項：

一、修正機關：金融監督管理委員會。

二、修正依據：電子票證發行管理條例第四條第二項規定。

三、「電子票證應用安全強度準則」部分條文修正草案如附件。本案另載於「本會主管法規整合查詢系統」網站（網址：http://law.fsc.gov.tw）「法規草案預告論壇」網頁。

四、對於本公告內容有任何意見或修正建議者，請於本公告刊登公報翌日起七日內陳述意見或洽詢：

(一) 承辦單位：本會銀行局

(二) 地址：新北市板橋區縣民大道 2 段 7 號 7 樓

(三) 電話：02-8968-9780

(四) 傳真：02-8969-1357

主任委員　曾銘宗

電子票證應用安全強度準則部分條文修正草案總說明

「電子票證發行管理條例」（以下簡稱本條例）業經總統於九十八年一月二十三日公布施行，金融監督管理委員會依據本條例第四條第二項授權訂定「電子票證應用安全強度準則」（以下簡稱本準則），並於九十八年七月十六日公布施行。為利電子票證可更廣泛地於小規模商家運用，並協助持卡人於繳納政府部門相關款項時，有更多元之繳款方式，爰修正本準則相關條文。

本次計修正四條條文，修正要點如下：

一、 考量持卡人以電子票證繳納政府部門規費、稅捐、罰鍰或其他費用（簡稱政府部門款項）、電信服務費、支付捐贈金或至特約機構以電子票證繳納政府部門款項之交易風險較一般交易低，爰將屬第一類商品或服務性質之「政府部門規費」放寬為「繳納政府部門規費、稅捐、罰鍰或其他費用」，並將電信服務費、捐贈金及「特約機構受各級政府委託代徵收之規費、稅捐與罰鍰及受公用事業委託代收之服務費」納入第一類商品或服務性質範疇。（修正條文第五條）

二、 參酌現行信用卡組織對感應式電子票證交易之感應距離限制，增加電子票證於小規模特約機構交易之安全控管機制選項，以防杜不當扣款之情事。另實務上部分加盟店因自身實收資本額及年營業額規模較小，須適用前述防杜小規模特約機構不當扣款之機制，惟考量加盟關係之特殊經營型態，且業主可透過加盟契約控管其加盟店，爰增訂當發行機構於與加盟業主之特約機構契約中，已要求該業主對加盟店倘發生不當扣款情事，須對持卡人負同一責任；且發行機構亦訂定防止加盟店不當扣款之內部控制制度之兩種條件，則該情境下之加盟店可不適用前開防杜機制之規定。（修正條文第九條）

三、 為利條文內容更符合實務作業，酌作文字修正。（修正條文第十條及第十一條）

電子票證應用安全強度準則部分條文修正草案條文對照表

<table>
<tr><th>修正條文</th><th>現行條文</th><th>說明</th></tr>
<tr><td>第五條　發行機構對於電子票證各項交易類型，應依電子票證應用之範圍，考量商品或服務之性質與交易金額等因素，區分應用範圍等級（如下表），並依據本準則之規定辦理。
一、商品或服務之性質
<table><tr><th>商品或服務之性質</th><th>說明</th></tr><tr><td>第一類</td><td>(一)繳納政府部門規費、稅捐、罰鍰或其他費用及支付公用事業（依據民營公用事業監督條例第二條定義）服務費、電信服務費、學雜費、醫藥費、公共運輸（依據發展大眾運輸條例第二條定義及纜車、計程車、公共自行車）、停車等服務費用、依公益勸募條例辦理勸募活動之捐贈</td></tr></table></td><td>第五條　發行機構對於電子票證各項交易類型，應依電子票證應用之範圍，考量商品或服務之性質與交易金額等因素，區分應用範圍等級（如下表），並依據本準則之規定辦理。
一、商品或服務之性質
<table><tr><th>商品或服務之性質</th><th>說明</th></tr><tr><td>第一類</td><td>繳納政府部門規費及支付公用事業（依據民營公用事業監督條例第二條定義）服務費、學雜費、醫藥費、公共運輸（依據大眾運輸條例第二條定義及纜車、計程車、公共自行車）、停車等服務費用，或配合政府政策且具公共利益性質經主管機關核准者屬之。</td></tr><tr><td>第二類</td><td>支付各項商品或服務之費用。</td></tr></table>二、交易金額
<table><tr><th>交易金額</th><th>說明</th></tr><tr><td>小額</td><td>電子票證僅支付</td></tr></table></td><td>一、為協助持卡人於繳納政府部門相關款項，有更多元之繳款方式，且考量繳納政府部門款項之交易風險較低，交易金額應可不受限制，爰於第一項將屬第一類商品或服務性質之「政府部門規費」放寬為「政府部門規費、稅捐、罰鍰或其他費用」；另一〇二年十二月三十一日金管銀票字第一〇二〇〇三五八四九〇號函已開放電子票證亦得支付特約機構受政府委託代徵收之規費，又特約機構受公用事業委託代收之服務費與受政府委託代徵收之款項性質相似，兩者風險屬性相當，爰併將「支付特約機構受各級政府委託代徵收之規費、稅捐與罰鍰及受公用事業委託代收之服務費」納入第一類商品或服務性質範疇。
二、現行第一類商品或服務性質之「公用事業服務費」係包含「市內電話費」，不含行動電話費。鑒於目前行動電話普及程度甚高，且行動電話服務提供者「電信事業」依「電信法」須經主管</td></tr>
</table>

	金，或配合政府政策且具公共利益性質經主管機關核准者屬之。 (二)支付特約機構受各級政府委託代徵收之規費、稅捐與罰鍰及受公用事業委託代收之服務費。		
第二類	支付各項商品或服務之費用。		

二、交易金額

交易金額	說明
小額交易	電子票證僅支付於單筆消費金額新臺幣壹千元以下之交易。
不限金額交易	電子票證非僅支付於小額交易。

三、應用範圍等級

商品或服務之性質		第一類	第二類
交易金額	小額交易	第一級	第一級
	不限金額交易	第一級	第二級

交易	於單筆消費金額新臺幣壹千元以下之交易。		
不限金額交易	電子票證非僅支付於小額交易。		

三、應用範圍等級

商品或服務之性質		第一類	第二類
交易金額	小額交易	第一級	第一級
	不限金額交易	第一級	第二級

機關特許或許可，始得營業，屬高度監理行業，爰將電信事業之服務費用，即「電信服務費」納入第一類商品或服務性質範疇。

三、另考量現行持卡人可用信用卡進行公益捐款，為增加持卡人捐款方式，且捐款金額不受限制，爰將支付「依公益勸募條例辦理勸募活動之捐贈金」納入第一類商品或服務性質範疇。

第九條　前條發行機構管理面安全需求之安全設計應符合下列要求：	第九條　前條發行機構管理面安全需求之安全設計應符合下列要求：	一、修正第四款發行機構對小規模特約機構應制定防止不當扣款之安全控管機制，於現行防杜機
安全需 安全設計	安全需 安全設計	

求		求		
建立電腦資源存取控制機制與安全防護措施	應防範未經授權存取系統資源，並降低非法入侵之可能性。應以下列方式處理及管控： 一、建置安全防護軟硬體，如防火牆(Firewall)、安控軟體、偵測軟體等。 二、控制密碼錯誤次數。 三、電腦系統密碼檔加密。 四、留存交易紀錄(Transaction Log)及稽核追蹤紀錄(Audit Trail)。 五、設計存取權控制(Access Control)如使用密碼、晶片卡等。 六、簽入(Login)時間控制。 七、遠端存取	建立電腦資源存取控制機制與安全防護措施	應防範未經授權存取系統資源，並降低非法入侵之可能性。應以下列方式處理及管控： 一、建置安全防護軟硬體，如防火牆(Firewall)、安控軟體、偵測軟體等。 二、控制密碼錯誤次數。 三、電腦系統密碼檔加密。 四、留存交易紀錄(Transaction Log)及稽核追蹤紀錄(Audit Trail)。 五、設計存取權控制(Access Control)如使用密碼、晶片卡等。 六、簽入(Login)時間控制。 七、遠端存取	制外，新增其他安全設計：參酌現行信用卡組織對感應式電子票證交易之感應距離係限制不得超過（含）四公分之規定，爰增加「小規模特約機構之交易感應距離限縮至四公分（含）以下」之安全機制。 二、實務上部分加盟店因自身實收資本額及年營業額規模較小須適用第四款防止小規模特約機構不當扣款之安全設計，惟考量同屬特約機構之加盟店與其加盟業主所適用之安全設計宜有一致性規範，爰於第四款增訂如加盟店之加盟業主實收資本額高於新臺幣八千萬元或年營業額高於新臺幣六千萬元，該加盟店可不適用現行針對小規模特約機構之交易確認方式；且發行機構與前開加盟業主及加盟店應有特約機構契約關係，發行機構可按實務作業需求，選擇以三方合約或分別與加盟業主及加盟店簽訂特約機構契約；另增訂對該類加盟店之管理機制，以防杜發生不當扣款之情事。

	應使用虛擬私有網路(VPN)。 八、系統資源應依其重要性與敏感性分級管理。 九、強制更換應用軟體及網路作業系統之預設密碼。 十、系統提供各項服務功能時，應確保個人資料保護措施。		應使用虛擬私有網路(VPN)。 八、系統資源應依其重要性與敏感性分級管理。 九、強制更換應用軟體及網路作業系統之預設密碼。 十、系統提供各項服務功能時，應確保個人資料保護措施。	
交易必須可被追蹤	交易紀錄明細應包含下列資訊，並留存於發行機構主機備查： 一、用戶代號或卡號。 二、交易金額。 三、端末設備代號。 四、交易序號或交易日期、時間。	交易必須可被追蹤	交易紀錄明細應包含下列資訊，並留存於發行機構主機備查： 一、用戶代號或卡號。 二、交易金額。 三、端末設備代號。 四、交易序號或交易日期、時間。	
監控非法交易	發行機構應監控非法交易。	監控非法交易	發行機構應監控非法交易。	
須防止小規模之特約機構不	一、實收資本額低於新臺幣八千萬元且年營業額低	須防止小規模之特約機構不	實收資本額低於新臺幣八千萬元且年營業額低於新臺幣	

當扣款	於新臺幣六千萬元之特約機構應以下列任一方式進行交易： (一)刷卡或插卡。 (二)輸入密碼。 (三)任何由系統所提供予持卡人進行確認之設計。 (四)感應距離限縮至四公分(含)以下。	當扣款	六千萬元之特約機構應以下列任一方式進行持卡人交易確認，但提供第一類商品或服務者，不在此限： 一、刷卡或插卡。 二、輸入密碼。 三、任何由系統所提供予持卡人進行確認之設計。	
	二、特約機構符合下列情形之一者，得不適用前目規定： (一)提供第一類商品或服務。 (二)加盟經營關係中，加盟業主實收資本額高於新臺幣八千萬元或年營業額高於新臺幣六千萬元之加盟店。 三、發行機構與前目加盟業主及加盟店間應簽訂三方之特約機	完善之金鑰管理	金鑰管理應有下列之安全考量： 一、應確保金鑰品質(避免產生弱金鑰)。 二、金鑰之使用、儲存、傳送與銷毀，應確保金鑰之內容無洩露之虞。 三、金鑰應備份以確保其可用性。 四、保存金鑰之設備或媒體，於更新或報廢時，應具適	

	構契約，或分別與前目加盟業者及加盟店簽定特約機構契約，並應依下列規定辦理： (一)發行機構應訂定防止加盟店不當扣款之內部控制制度。 (二)發行機構應於三方契約中或與加盟業主之契約中，要求加盟業主對加盟店及其受僱人員因故意或過失致發生不當扣款情事，對持卡人負同一責任。		當之存取控管程序，以確保金鑰無洩露之虞。	
		提昇電腦系統之安全及可用性	應建立異地備援及故障預防措施，包含： 一、預備主機、伺服器、通訊設備、線路、週邊設備等備援裝置。 二、建置病毒偵測軟體(Virus Detection Software)，定期對網路節點及伺服器進行掃毒。 三、定期更新系統修補程式（Patch, Hotfix）。 四、確保伺服器、網路設備之實體安全。	
完善之金鑰管理	金鑰管理應有下列之安全考量： 一、應確保金鑰品質(避免產生弱金鑰)。 二、金鑰之使用、儲存、傳送與銷毀，應確保金鑰之內	制定作業管理規範	應確定發行機構、特約機構與加值機構內部之責任制度、核可程序及與持	

	容無洩露之虞。 三、金鑰應備份以確保其可用性。 四、保存金鑰之設備或媒體，於更新或報廢時，應具適當之存取控管程序，以確保金鑰無洩露之虞。		卡人之間之責任歸屬，應包含： 一、制定安全控管規章含設備規格。 二、安控機制說明、安控程序說明。 三、金鑰管理措施或辦法。 四、制定持卡人使用安全須知及完整合約。	
提昇電腦系統之安全及可用性	應建立異地備援及故障預防措施，包含： 一、預備主機、伺服器、通訊設備、線路、週邊設備等備援裝置。 二、建置病毒偵測軟體(Virus Detection Software)，定期對網路節點及伺服器進行掃毒。 三、定期更新系統修補程式（Patch,			

	Hotfix）。 四、確保伺服器、網路設備之實體安全。		
制定作業管理規範	應確定發行機構、特約機構與加值機構內部之責任制度、核可程序及與持卡人之間之責任歸屬，應包含： 一、制定安全控管規章含設備規格。 二、安控機制說明、安控程序說明。 三、金鑰管理措施或辦法。 四、制定持卡人使用安全須知及完整合約。		
第十條　發行機構於端末設備與環境面應採取下列防護措施：		第十條　發行機構於端末設備與環境面應採取下列防護措施：	有關本條第一款第六目之安全需求及安全設計規範係訂於第十一條第六款，依其規定內容，發行機構除應設置監視設備外，亦可採取其他必要措施，爰二者規定有不一致之處。為有一致性規範，爰調整本條第一款第六目文字，將「應設置監視設備」修正為「應採取降低偽卡交易之必要措施」。
防護措施	安全需求	防護措施	安全需求
建立安全防護策略	一、保持端末設備與環境之實體完整性 二、確保端末設備交易	建立安全防護策略	一、保持端末設備與環境之實體完整性 二、確保端末設備交易

	之安全性 三、建置有效或即時之管控名單管理機制 四、非接觸式電子票證應降低交易被意外觸發之機率 五、非線上即時加值應具有端末安全模組之設計 六、非線上即時交易，若採用應用範圍等級第一級之電子票證，且使用於提供第二類商品或服務之特約機構，應採取降低偽卡交易之必要措施 七、網際網路應用系統開發注意事項		之安全性 三、建置有效或即時之管控名單管理機制 四、非接觸式電子票證應降低交易被意外觸發之機率 五、非線上即時加值應具有端末安全模組之設計 六、非線上即時交易，若採用應用範圍等級第一級之電子票證，且使用於提供第二類商品或服務之特約機構，應設置監視設備 七、網際網路應用系統開發注意事項	
提高系統可用性之措	提高系統可用性之措施	提高系統可用性之措施	提高系統可用性之措施	
		制定作	制定作業管理	

施		業管理規範	規範：內部環境管理部分應落實管理規則之規範。	
制定作業管理規範	制定作業管理規範：內部環境管理部分應落實管理規則之規範。			
第十一條　前條發行機構端末設備與環境面安全需求之安全設計應符合下列要求：		第十一條　前條發行機構端末設備與環境面安全需求之安全設計應符合下列要求：		一、配合第十條第一款第六目「安全需求」之文字調整，修正本條第六款之「安全需求」文字。 二、本條第八款規定係以備援方式提高系統可用性，為保持系統設備之發展彈性，增訂發行機構可採用其他方式，提高系統可用性。
安全需求	安全設計	安全需求	安全設計	
保持端末設備與環境之實體完整性	應採用下列各項安全設計： 一、定期檢視是否有增減相關裝置： (一) 原始設施確實逐項編號。 (二) 比對現場相關設施及裝置是否與原始狀態一致。 (三) 建立檢視清單(Checklist)，並應定期覆核並追蹤考核。 二、應確定與端末設備合作廠商簽訂資料保密契約，並應將參與端末設備安裝、維	保持端末設備與環境之實體完整性	應採用下列各項安全設計： 一、定期檢視是否有增減相關裝置： (一) 原始設施確實逐項編號。 (二) 比對現場相關設施及裝置是否與原始狀態一致。 (三) 建立檢視清單(Checklist)，並應定期覆核並追蹤考核。 二、應確定與端末設備合作廠商簽訂資料保密契約，並應將參與端末設備安裝、維	

	護作業之人員名單交付造冊列管，如有異動，應隨時主動通知發行機構更新之。 三、端末設備合作廠商人員至現場作業時，均應出示經認可之識別證件。除安裝、維護作業外，並應配合隨時檢視端末設備硬體是否遭到不當外力入侵或遭裝置側錄設備。 四、發行機構應不定時派員抽檢安裝於特約機構或加值機構之端末設備，檢視該硬體是否遭到不當外力入侵，並檢視其軟體是否遭到不法竄改。		護作業之人員名單交付造冊列管，如有異動，應隨時主動通知發行機構更新之。 三、端末設備合作廠商人員至現場作業時，均應出示經認可之識別證件。除安裝、維護作業外，並應配合隨時檢視端末設備硬體是否遭到不當外力入侵或遭裝置側錄設備。 四、發行機構應不定時派員抽檢安裝於特約機構或加值機構之端末設備，檢視該硬體是否遭到不當外力入侵，並檢視其軟體是否遭到不法竄改。	
確保端末設備交易之	運用端末設備處理交易時，應符合下述規範：	確保端末設備交易之	運用端末設備處理交易時，應符合下述規範：	

安全性	一、電子票證內含錄碼及資料，除帳號、卡號、有效期限、交易序號及查證交易是否發生之相關必要資料外，其他資料一律不得儲存於端末設備。 二、應確保端末設備之合法性，另端末設備應有唯一之端末設備代號。 三、應用範圍屬第二級之交易，端末設備之安全模組應個別化(即每一端末設備之認證金鑰皆不相同)。	安全性	一、電子票證內含錄碼及資料，除帳號、卡號、有效期限、交易序號及查證交易是否發生之相關必要資料外，其他資料一律不得儲存於端末設備。 二、應確保端末設備之合法性，另端末設備應有唯一之端末設備代號。 三、應用範圍屬第二級之交易，端末設備之安全模組應個別化(即每一端末設備之認證金鑰皆不相同)。	
建置有效或即時之管控名單管理機制	為有效防範非法電子票證進行交易，發行機構應建置管控名單管理機制，對於線上即時交易應即時更新，非線上即時交易應每日更新。	建置有效或即時之管控名單管理機制	為有效防範非法電子票證進行交易，發行機構應建置管控名單管理機制，對於線上即時交易應即時更新，非線上即時交易應每日更新。	
非接觸	端末設備應包含	非接觸	端末設備應包含	

式電子票證應降低交易被意外觸發之機率	下列設計，以降低非接觸式電子票證在持卡人無交易之意願下，交易被意外觸發之機率： 一、感應距離限縮至六公分（含）以下。 二、交易過程應有聲音、燈號或圖像等之提示。	式電子票證應降低交易被意外觸發之機率	下列設計，以降低非接觸式電子票證在持卡人無交易之意願下，交易被意外觸發之機率： 一、感應距離限縮至六公分（含）以下。 二、交易過程應有聲音、燈號或圖像等之提示。	
非線上即時加值應具有端末安全模組之設計	非線上即時加值交易之端末設備應具有安全模組之設計，進行加值交易另應包含下列設計： 一、逐筆授權加值交易。 二、限制其單筆加值金額。 三、限制其加值總額（如：日限額），額度用罄應連線至發行機構重新授權可加值額度。 四、安全模組應進行妥善之管理，如製發卡與交貨控管流程、管制製卡作	非線上即時加值應具有端末安全模組之設計	非線上即時加值交易之端末設備應具有安全模組之設計，進行加值交易另應包含下列設計： 一、逐筆授權加值交易。 二、限制其單筆加值金額。 三、限制其加值總額（如：日限額），額度用罄應連線至發行機構重新授權可加值額度。 四、安全模組應進行妥善之管理，如製發卡與交貨控管流程、管制製卡作	

	業、落實安全模組之安全控管等。		業、落實安全模組之安全控管等。	
非線上即時交易，若採用應用範圍等級第一級之電子票證，且使用於提供第二類商品或服務之特約機構，應採取降低偽卡交易之必要措施	應用範圍等級第一級之電子票證，若使用於提供第二類商品或服務之特約機構進行非線上即時交易，發行機構應要求特約機構設置錄影監視設備且於營業時間內保持全時錄影，或採取其他必要之措施以降低偽卡交易。	非線上即時交易，若採用應用範圍等級第一級之電子票證，且使用於提供第二類商品或服務之特約機構，應設置監視設備，或採取其他必要之措施以降低偽卡交易	應用範圍等級第一級之電子票證，若使用於提供第二類商品或服務之特約機構進行非線上即時交易，發行機構應要求特約機構設置錄影監視設備且於營業時間內保持全時錄影，或採取其他必要之措施以降低偽卡交易。	
網際網路應用系統開發注意事項	若電子票證持卡人透過瀏覽器以網際網路進行交易，網路應用系統之開發應有下列設計： 一、網站應採用網頁安全傳輸協定（Secure Sockets Layer；簡稱SSL）加密或其他安全	網際網路應用系統開發注意事項	若電子票證持卡人透過瀏覽器以網際網路進行交易，網路應用系統之開發應有下列設計： 一、網站應採用網頁安全傳輸協定（Secure	

	強度不得低於第七條對訊息隱密性之規定(A)之方式加密傳輸資料。 二、系統應依每筆交易動態隨機變動端末設備查核碼或以亂碼化保護。 三、系統應設計具遮罩功能之圖形驗證碼(Graphic One Time Password；簡稱GOTP)或隨機按鈕等方式。 四、系統應設計動態頁面呈現或限制滑鼠點選，以防止模擬鍵盤控制（SendKey Control）攻擊。 五、系統應有連線(Session)控制及網頁逾時(Timeout)中斷機制。 六、若有多網頁		Sockets Layer；簡稱SSL）加密或其他安全強度不得低於第七條對訊息隱密性之規定(A)之方式加密傳輸資料。 二、系統應依每筆交易動態隨機變動端末設備查核碼或以亂碼化保護。 三、系統應設計具遮罩功能之圖形驗證碼(Graphic One Time Password；簡稱GOTP)或隨機按鈕等方式。 四、系統應設計動態頁面呈現或限制滑鼠點選，以防止模擬鍵盤控制（SendKey Control）攻擊。 五、系統應有連線(Session)控制及網頁	

	設計，系統應驗證前一網頁正確性。 七、客戶端元件應驗證網站正確性。 八、客戶端元件應具有防盜用機制，以驗證正確網站。 九、客戶端元件應具有作業系統認可之程式碼簽章憑證(CodeSign)。 十、客戶端元件應具存取卡片時限定為獨占模式之設計。 十一、客戶端元件應具有需經人工介入以完成交易之設計。 十二、如有駭客入侵時，發行機構應即關閉網路服務，以確保交易安全。		逾時(Timeout)中斷機制。 六、若有多網頁設計，系統應驗證前一網頁正確性。 七、客戶端元件應驗證網站正確性。 八、客戶端元件應具有防盜用機制，以驗證正確網站。 九、客戶端元件應具有作業系統認可之程式碼簽章憑證(CodeSign)。 十、客戶端元件應具存取卡片時限定為獨占模式之設計。 十一、客戶端元件應具有需經人工介入以完成交易之設計。 十二、如有駭客入侵時，發行機構應即關閉網路服	
提高系	應以下列方式處			

統可用性之措施	理及管控： 一、規劃備援線路或其他可確保提高系統可用性之措施。。 二、規劃備援電路或不斷電系統（Uninterruptible Power Supply；簡稱 UPS）。		務，以確保交易安全。	
		提高系統可用性之措施	應以下列方式處理及管控： 一、規劃備援線路。 二、規劃備援電路或不斷電系統（Uninterruptible Power Supply；簡稱 UPS）。	
制定作業管理規範	應制定端末設備管理規章，含設備規格、安控機制說明、安控程序說明、安全模組控管作業原則、管控名單管理機制、特約機構與加值機構簽約與管理辦法等。	制定作業管理規範	應制定端末設備管理規章，含設備規格、安控機制說明、安控程序說明、安全模組控管作業原則、管控名單管理機制、特約機構與加值機構簽約與管理辦法等。	