電子票證應用安全強度準則部分條文修正條文

第四條　本準則用詞定義如下：

一、加值機構：係指接受發行機構委託辦理加值作業之特定機構。

二、線上即時交易：係指透過各種網路型態，經由特約機構、加值機構或直接與發行機構即時連線進行交易，並將電子票證餘額及交易紀錄即時儲存於發行機構端者，包含特約機構與發行機構間、加值機構與發行機構間、加值機構或特約機構與其所屬之端末設備間之即時訊息傳輸。

三、前款所稱網路型態如下：

(一)專屬網路：指利用電子設備或通訊設備以撥接(Dial-Up)、專線(Leased-Line)或虛擬私有網路(Virtual Private Network，VPN)等連線方式進行訊息傳輸。

(二)網際網路：指利用電子設備或通訊設備，透過網際網路服務業者進行訊息傳輸。

(三)行動網路：指利用電子設備或通訊設備，透過電信服務業者進行訊息傳輸。

四、非線上即時交易：係指利用各種介面類型，於端末設備進行交易，並將電子票證餘額及交易紀錄即時儲存於電子票證端，而不需與發行機構即時連線者。

五、前款所稱介面類型如下：

(一)接觸式介面：利用磁性、光學或電子型式之電子票證，與端末設備以實際接觸方式進行訊息傳輸。

(二)非接觸式介面：利用無線射頻、紅外線或其他無線通訊技術實作之電子票證，與端末設備以非實際接觸方式進行訊息傳輸。

(三)網路及其他離線方式：利用電子票證，透過網路、通訊設備及其他方式，與遠端之特約機構或加值機構進行訊息傳輸，而不與發行機構即時連線進行驗證者。

六、交易類型：

(一)線上即時消費交易：係指消費交易發生時，其消費是否合法之驗證，必須透過連線，將相關資訊送回發行機構進行處理，並將電子票證餘額及交易紀錄即時儲存於發行機構端者。

(二)非線上即時消費交易：係指消費交易發生時，其消費是否合法之驗證，不需透過連線送回發行機構進行處理，並將電子票證餘額及交易紀錄即時儲存於電子票證端者。

(三)線上即時加值交易：係指加值交易發生時，其加值是否合法之驗證，必須透過連線，將相關資訊送回發行機構進行處理，並將電子票證餘額及交易紀錄即時儲存於發行機構端者。

(四)非線上即時加值交易：係指加值交易發生時，其加值是否合法之驗證，不需透過連線將相關訊息送回發行機構進行處理，並將電子票證餘額及交易紀錄即時儲存於電子票證端者。

(五)票證款項移轉交易：係指將具儲值功能之記名式電子票證款項移轉至同一持卡人電子支付帳戶，其款項移轉是否合法之驗證，必須透過連線，將相關訊息送回發行機構進行處理，並將電子票證餘額及交易紀錄即時儲存於電子票證端或即時儲存於發行機構端者。

(六)帳務清結算交易：包含特約機構或加值機構與其所屬端末設備間之批次帳務訊息、特約機構或加值機構與發行機構間之批次帳務訊息、加值機構與發行機構間之非線上即時加值額度授權請求訊息等。

七、常用密碼學演算法如下：

(一)對稱性加解密演算法：指資料加密標準(Data Encryption Standard；以下簡稱 DES)、三重資料加

密標準(Triple DES；以下簡稱3DES)、進階資料加密標準(Advanced Encryption Standard；以下簡稱AES)。

(二)非對稱性加解密演算法：指 RSA 加密演算法(Rivest, Shamir and Adleman Encryption Algorithm；以下簡稱 RSA)、橢圓曲線密碼學(Elliptic Curve Cryptography；以下簡稱 ECC)。

(三)雜湊函數：指安全雜湊演算法(Secure Hash Algorithm；以下簡稱 SHA)。

八、動態密碼：係運用動態密碼產生器或以其他方式運用一次性密碼(One Time Password；以下簡稱 OTP)原理，隨機產生限定一次使用之密碼者。

九、晶片卡：係指具有晶片功能之卡片或設備。

十、磁條卡：係指具有磁條功能之卡片或設備。

第七條　前條各項交易安全所稱訊息隱密性、訊息完整性、來源辨識性及不可重覆性之安全設計應符合下列要求：

一、訊息隱密性 A：應採用下列對稱性加解密系統或非對稱性加解密系統，針對訊息進行全文加密，以防止未經授權者取得訊息之明文。

(一)對稱性加解密系統應採用3DES 112bits、AES 128bits或其他安全強度相同(含)以上之演算法及金鑰進行加密運算。

(二)非對稱性加解密系統應採用 RSA 1024bits、ECC 256bits 或其他安全強度相同(含)以上之演算法及金鑰進行加密運算。自一〇六年一月一日起，新發行並應用於本項之電子票證不應採用低於 RSA 1024bits 之金鑰長度進行加密運算。

二、訊息完整性

(一)B1防護措施：應採用下列防止非惡意篡改訊息之檢核碼技術之一：

1、縱向冗餘校驗(Longitudinal Redundancy Check，LRC)。

2、循環冗餘校驗(Cyclic Redundancy Check，CRC)。

3、使用雜湊(Hash)演算法產生訊息摘要(Message Digest)。

(二)B2防護措施：應採用可防止蓄意篡改訊息之加解密技術，可採對稱性加解密系統進行押碼(Message Authentication Code, MAC)或非對稱性加解密系統產生數位簽章(Digital Signature)等機制。

1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。

2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。

(三)B3防護措施：除須符合本條第二款第二目 B2所要求之強度外，加值交易訊息之金額須參與訊息完整性之運算。

三、來源辨識性

(一)C1防護措施：應確保持卡人之正確性，可採用下列任一種持卡人認證方式；採用下列第1至第3方式者，其認證方式並應採用對稱性加解密系統或非對稱性加解密系統，由發行機構確認電子票證之合法性，以防範非法之電子票證。

1、具加解密運算能力之晶片卡。

2、記憶型晶片卡與固定密碼。

3、磁條卡與磁條卡密碼。

4、用戶代號與動態密碼(如簡訊 OTP)。

5、用戶代號與持卡人及發行機構所約定之資訊，且無第三人知悉(如固定密碼、圖形鎖或手勢)。

6、用戶代號與持卡人所持有之實體設備(如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑

證載具等)：發行機構應確認該設備為使用者與發行機構所約定持有之設備。

7、用戶代號與持卡人所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)：發行機構應直接或間接驗證該生物特徵並依據其風險承擔能力調整生物特徵之錯誤接受度，以有效識別持卡人身分，必要時應增加多項不同種類生物特徵;間接驗證由持卡人設備(如行動裝置)驗證，發行機構僅讀取驗證結果，必要時應增加驗證來源辨識；採用間接驗證者，應事先評估持卡人身分驗證機制之有效性。

(二)C2防護措施：應採用具訊息認證功能之晶片型電子票證或端末安全模組，確保訊息來源之正確性，可採對稱性加解密系統進行押碼或非對稱性加解密系統產生數位簽章等機制。

1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。

2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。

3、採用前目之5至7之二項(含)以上認證方式，並事先與持卡人約定交易通知方式(如簡訊、推播等)。

(三)C3防護措施：應採用知識詢問(如卡號、有效月年及檢查碼)，由發行機構確認電子票證之合法性，以防範非法之電子票證，並確保非用戶本人授權使用之交易於掛失後無需承擔遭冒用之損失，發行機構應於十四日內返還帳款，持卡人應配合協助發行機構之後續調查作業。

(四)D1防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由端末設備確認電子票證之合法性，以防範非法之電子票證。

(五)D2防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由端末設備確認電子票證之合法性，以防範非法之電子票證。

1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。

2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。

(六)E1防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由電子票證確認端末設備或發行機構之合法性，以防止未經授權之端末設備逕行交易。

(七)E2防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由電子票證確認端末設備或發行機構之合法性，以防止未經授權之端末設備逕行交易。

1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。

2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。

四、不可重覆性 F：應防止以先前成功之交易訊息完成另一筆交易，可採用序號、日期時間或時序或密碼學挑戰-回應(Challenge-Response)等機制。

第八條　發行機構於管理面應採取下列防護措施及其安全需求：

一、建立安全防護策略

(一)建立電腦資源存取控制機制與安全防護措施。

(二)交易必須可被追蹤。

(三)監控非法交易。

(四) 完善之金鑰管理。

二、提高系統安全之措施

(一)提昇電腦系統之安全及可用性。

(二)提昇應用系統之安全及可用性。

三、制定作業管理規範。

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、建立電腦資源存取控制機制與安全防護措施，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。

二、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。

三、發行機構應監控非法交易。

四、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) 金鑰應儲存於通過 FIPS 140-2 Level3(含)以上之硬

體安全模組內並限制金鑰明文匯出。

(四)金鑰應備份以確保其可用性。

(五)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。

五、提昇電腦系統之安全及可用性，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，並定期更新病毒碼。

(三)定期更新系統修補程式（Patch, Hotfix）。

(四)於對外網段建置入侵偵測機制並定期更新特徵碼。

(五)建置上網管制機制，限制連結非業務相關網站。

(六)每年針對系統維運人員進行郵件社交工程演練。

(七)每季進行弱點掃描，依據風險高低逐步改善。

(八)每半年針對異動程式進行程式碼掃描或黑箱測試，依據風險高低逐步改善。

(九)伺服器、網路設備等營運設備應集中於機房內，並應建立外圍門禁管制、內部空間監控及機櫃門禁管制等三道防護，以確保實體安全。

六、提昇應用系統之安全及可用性：

(一)提供網際網路之應用系統應符合下列安全設計：

1、載具密碼不應於網際網路上傳輸，機敏資料於網際網路傳輸時應全程加密。

2、應設計連線控制及網頁逾時中斷機制。持卡人超過十分鐘未使用應中斷其連線或採取其他保護措施，但持卡人以第七條第三款第一目之6所定持卡人所持有的實體設備進行交易，得延長至三十分鐘。

3、應辨識外部網站及其所傳送交易資料之訊息來源及交易資料正確性。

4、應辨識持卡人輸入與系統接收之支付指示一致性。

5、應設計於持卡人進行身分確認與交易機制時，須採用一次性亂數或時間戳記，以防止重送攻擊。

6、應設計於持卡人進行身分確認與交易機制時，如需使用亂數函數進行運算，須採用安全亂數函數產生所需亂數。

7、應設計於持卡人修改線上即時交易之約定時，須先經採用第七條第三款第一目之5至7之二項(含)以上認證方式進行身分確認。

8、應設計個人資料顯示之隱碼機制。

9、應設計個人資料檔案及資料庫之存取控制與保護監控措施。

10、應建置防偽冒與洗錢防制偵測系統，建立風險分析模組與指標，用以於異常交易行為發生時即時告警並妥善處理。風險分析模組與指標應定期檢討修訂。

(二) 提供持卡人端之程式應符合下列安全設計：

1、應採用被作業系統認可之數位憑證進行程式碼簽章。

2、執行時應先驗證網站正確性。

3、應避免儲存機敏資料，如有必要應採取加密或亂碼化等相關機制保護並妥善保護加密金鑰，且能有效防範相關資料被竊取。

(三)提供行動裝置之應用程式應符合下列安全設計：

1、於發布前檢視行動裝置應用程式所需權限應與提供服務相當；首次發布或權限變動，應經法遵部門或風控部門同意，以利綜合評估是否符合個人資料保護法之告知義務。

2、應於官網上提供行動裝置應用程式之名稱、版本與下載位置。

3、啟動行動裝置應用程式時，如偵測行動裝置疑似遭破解，應提示持卡人注意風險。

4、應於顯著位置(如行動裝置應用程式下載頁面等)提示持卡人於行動裝置上安裝防護軟體。

5、採用憑證技術進行傳輸加密時，行動裝置應用程式應建立可信任憑證清單並驗證完整憑證鏈及其憑證有效性。

6、採用 NFC 技術進行付款交易資料傳輸前，應經由持卡人人工確認。

7、行動裝置應用程式設計要求應符合中華民國銀行商業同業公會全國聯合會（以下簡稱銀行公會）所訂定之行動裝置應用程式相關自律規範。

(四)定期針對網際網路服務之系統或應用程式進行滲透測試，依據風險高低逐步改善。

(五)採用條碼掃描技術之設計要求，應符合銀行公會所訂定之條碼掃描應用安全相關自律規範。

七、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，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及其安全需求：

一、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)應用於非線上即時加值交易，端末設備應具有安全模組之設計。

(六)應用於非線上即時加值交易或非線上即時消費交易，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。

二、提高系統可用性之措施。

三、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：

一、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：

1、原始設施確實逐項編號。

2、比對現場相關設施及裝置是否與原始狀態一致。

3、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)端末設備安裝、維護作業人員至現場作業時，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。

二、確保端末設備交易之安全性，應符合下列規範：

(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)。

三、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驗證，非線上即時交易應每日更新管控名單。

四、發行機構應有效防止特約機構不當扣款，其端末設備應包含下列設計，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)感應距離限縮至十公分（含）以下。

(二)交易過程應有聲音、燈號或圖像等之提示。

五、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。

六、應用範圍等級第一級之電子票證於提供第二類商品或服務之特約機構之交易，如管控名單之驗證未送回發行機構進行即時驗證者，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。

七、端末設備若係持卡人個人持有之電子設備或通訊設備者（如晶片讀卡機、具備可模擬電子票證卡讀卡機模式(reader mode)之行動裝置等），可不適用第一款、第二款第二目、第三目及第五款之規定。

八、提高系統可用性之措施，如備用設備、備援線路、備援電路、不斷電系統(Uninterruptible Power Supply；簡稱 UPS)或其他可確保提高系統可用性之措施等措施。

九、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。

第十二條　發行機構應依據應用範圍等級選用下列適當型式之電子票證：

一、電子票證為下列類型之一者，得適用於第一級應用範圍：

(一)具加解密運算能力之晶片卡。

(二)記憶型晶片卡與固定密碼。

(三)磁條卡與固定密碼。

二、電子票證為安全認證之晶片卡者，得適用於第二級應用範圍。

前項所稱「安全認證」需經主管機關確認其安全等級通過國家通訊傳播委員會或共同準則相互承認協定(Common Criteria Recognition Arrangement；CCRA)認可之驗證機構進行第三方驗證，符合或等同於下列任一標準者：

一、共同準則（Common Criteria）ISO/IEC15408 v2.3 EAL4+（含增項 AVA_VLA.4及 ADV_IMP.2）。

二、共同準則（Common Criteria）ISO/IEC15408 v3.1 EAL4+（含增項 AVA_VAN.5）。

三、我國國家標準 CNS 15408 EAL4+（含增項

AVA_VLA.4及 ADV_IMP.2）。

四、其他經主管機關認可之驗證標準。

第十四條　前條發行機構電子票證安全需求之安全設計應符合下列要求：

一、電子票證須具有獨立且唯一之識別碼或具有認證之功能，以確保其合法性。

二、若採用戶代號及固定密碼者，應具有下列之安全設計：

(一)用戶代號如使用顯性資料(如商業統一編號、身分證統一編號、行動電話號碼、電子郵件帳號、電子票證編號等)作為唯一之識別，應另行增設持卡人代號以資識別。持卡人代號亦不得為上述顯性資料。

(二) 密碼不應少於六位。

(三)密碼不應與用戶代號相同，亦不得與持卡人代號相同。

(四)密碼不應訂為相同之英數字、連續英文字或連號數字，預設密碼不在此限。

(五)密碼建議採英數字混合使用，且宜包含大小寫英文字母或符號。

(六)密碼連續錯誤達五次時應限制使用，須重新申請密碼。

(七)變更後之密碼不得與變更前一次密碼相同。

(八)密碼超過一年未變更，發行機構應做妥善處理。

(九)持卡人註冊時係由發行機構發予預設密碼者，於持卡人首次登入時，應強制變更預設密碼。

三、儲存於電子票證之個資必須保護：若使用電子票證儲存個人資料，應設計存取控制或持卡人確認之機制，以限制其讀取。

四、制定電子票證交貨控管流程：發行機構應針對電子票證之生命週期進行妥善之管理，應制定電子票證製發卡與交貨控管流程、管制外包製卡作業及落實實體電

子票證之安全控管。