電子支付機構資訊系統標準及安全控管作業基準辦法部分修正條文

第五條　電子支付機構於使用者登入電子支付平臺時應進行身分確認，使用者應以帳號及第七條規定之 A 類、B 類、C 類或 D 類交易安全設計登入。

前項帳號及採用固定密碼之安全設計如下：

一、帳號如使用顯性資料(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、信用卡卡號等)作為唯一之識別，應另行增設使用者代號以資識別。使用者代號亦不得為上述顯性資料。

二、密碼不應少於六位。

三、密碼不應與帳號相同，亦不得與使用者代號相同。

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、密碼建議應採英數字混合使用，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，電子支付機構應做妥善處理。

九、使用者註冊時係由電子支付機構發予預設密碼者，於使用者首次登入時，應強制變更預設密碼。

第一項採用圖形鎖或手勢之安全設計，準用前項第六款及第七款規定。

第七條　電子支付機構執行前條所列交易安全設計，應符合下列要求：

一、A 類交易安全設計：指採用固定密碼、圖形鎖或手勢之安全設計，如為固定密碼，其安全設計應符合第五條第二項之規定；如為圖形鎖或手勢，其安全設計應符合第五條第三項之規定。

二、B 類交易安全設計：指採用簡訊傳送一次性密碼至使用

者行動裝置之安全設計，應設定密碼有效時間，並應避免簡訊遭竊取或轉發。

三、C類交易安全設計：指採用下列任一款之安全設計：

（一）採用晶片金融卡之安全設計，應依每筆交易動態產製不可預知之端末設備查核碼，每次需輸入卡片密碼產生交易驗證碼，並由原發卡銀行驗證交易驗證碼；應設計防止第三者存取。

（二）採用一次性密碼之安全設計，應採用實體設備且非同一執行交易之設備；設定密碼有效時間；設計密碼連續錯誤達三次時予以鎖定使用，經適當身分認證後才能解除。如實體設備與執行交易之設備為同一設備，則應於使用者端經由人工確認交易內容後才能完成交易。

（三）採用二項（含）以上技術（Two Factors Authentication），其安全設計應具有下列任二項以上技術：

1. 使用者與電子支付機構所約定之資訊，且無第三人知悉(如固定密碼、圖形鎖或手勢)。

2. 使用者所持有之實體設備(如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等)：電子支付機構應確認該設備為使用者與電子支付機構所約定持有之設備。

3. 使用者所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)：電子支付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，以有效識別使用者身分，必要時應增加其他身分確認機制(如密碼)。間接驗證由使用者端設備(如行動裝置)驗證，電子支付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，應事先評估使用者身分驗證機制

之有效性。

四、D類交易安全設計：指採用下列任一款之安全設計：

（一）臨櫃受理使用者交易，應核對身分證明文件及印鑑或簽名。

（二）採用符合電子簽章法之安全設計。

使用者依第五條規定以帳號及前項A類、B類、C類或D類交易安全設計登入電子支付平臺，於符合第十條第一款第二目規定之連線控制及網頁逾時中斷機制時限內，得直接進行該類交易安全設計及依前條第二項所定其得替代交易安全設計之交易。

第一項第四款第二目採用符合電子簽章法之安全設計得使用憑證機制，相關要求如下：

一、應遵循憑證機構之憑證作業辦法。

二、應確認憑證之合法性、正確性、有效性、保證等級及用途限制，該憑證應由憑證主管機關核定之第三方憑證機構所核發。

三、擔任憑證註冊中心，受理使用者憑證註冊或資料異動時，其臨櫃作業應額外增加具二項(含)以上技術之安全設計或經由另一位人員審核。

四、憑證線上更新時，須以原使用中有效私密金鑰對憑證更新訊息做成簽章傳送至註冊中心提出申請。

五、應用於交易不可否認之憑證，應選擇負賠償責任之憑證機構，且該憑證申請須由使用者自行產製私鑰。

六、政府機關核發之憑證限應用於註冊時之身分確認。

七、每筆交易須針對支付內容進行簽章並驗證該憑證之有效性。

八、應確認該憑證私鑰儲存於符合共同準則(Common Criteria) EAL 4+(至少包含增項AVA_VLA.4或AVA_VAN.5)或FIPS 140-2 Level 3(含)以上或其他相同安全強度之認證等晶片硬體內，以防止該私鑰被匯出或複製。如晶片硬體與產生支付指示為同一設備，則應於

使用者端經由人工確認交易內容後才完成交易；或於交易過程額外增加具二項(含)以上安全設計。

第九條　前條所稱訊息隱密性、訊息完整性、訊息來源辨識性、訊息不可重複性及訊息不可否認性之安全設計，應符合下列要求：

一、訊息隱密性：應採用3DES 112bits、AES 128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同(含)以上之演算法進行加密運算。

二、訊息完整性：應採用 SHA 160bits、3DES 112bits、AES 128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同(含)以上之演算法進行押碼或加密運算。

三、訊息來源辨識性：應採用 SHA 160bits、3DES 112bits、AES 128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同(含)以上之演算法進行押碼、加密運算或數位簽章。

四、訊息不可重複性：應採用序號、一次性亂數、時間戳記等機制產生。

五、訊息不可否認性：應採用 SHA256以上或其他安全強度相同(含)以上之演算法進行押碼，及採用 RSA 2048bits、ECC 256bits 以上或其他安全強度相同(含)以上之演算法進行數位簽章。

第十條　電子支付平臺之設計原則，應符合下列要求：

一、網際網路應用系統設計要求：

(一)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。

(二)應設計連線控制及網頁逾時中斷機制，使用者超過十分鐘未使用應中斷其連線。但使用者以第七條第一項第三款第三目之2所定使用者所持有之實體設備進行交易，得延長至三十分鐘。

(三)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。

(四)應辨識使用者輸入與系統接收之支付指示一致性。

(五)應設計於使用者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。

(六)應設計於使用者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。

(七)應設計於使用者修改個人資料、約定或變更提領電子支付帳戶款項之銀行存款帳戶時，須先經第七條第一項第二款至第四款任一類交易安全設計進行身分確認。

(八)應設計個人資料顯示之隱碼機制。

(九)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。

(十)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。該風險分析模組與指標應定期檢討修訂。

二、實體通路支付服務程式設計要求：

(一)電子支付機構應確認實體通路之設備及其所傳送或接收之訊息隱密性及完整性。

(二)電子支付機構辦理款項間移轉或支付實質交易款項時，如將支付指示記錄於圖片、條碼或檔案，應經使用者確認；如將上述媒體透過近距離無線通訊、藍芽、掃描、上傳等機制交付他人者，應視必要增加存取限制(如密碼)，防止第三人竊取或竄改。

三、使用者端程式設計要求：

(一)應採用被作業系統認可之數位憑證進行程式碼簽章。

(二)執行時應先驗證網站正確性。

(三)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。

四、行動裝置應用程式設計要求：

(一)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，應經法遵部門及風控部門同意，以利綜合評估是否符合個人資料保護法之告知義務。

(二)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。

(三)啟動行動裝置應用程式時，如偵測行動裝置疑似遭破解，應提示使用者注意風險。

(四)應於顯著位置(如行動裝置應用程式下載頁面等)提示使用者於行動裝置上安裝防護軟體。

(五)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。

(六)採用 NFC 技術進行付款交易資料傳輸前，應經由使用者人工確認。

(七)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。

五、再確認之設計要求：

(一)收到支付指示後，以信用卡線上刷卡、電子支付帳戶款項或約定連結存款帳戶付款進行支付者，應以事先與使用者同意之方式(如交易確認頁面、郵件、簡訊等)通知付款方再確認，經確認無誤後才進行交易。但實體通路支付服務，不適用之。

(二)非以前目方式辦理者，如透過其他方式進行付款者，可視為付款方之再確認。

六、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。但本條例及本條例授權訂定之命令另有規定者，依其規定。

第十條之一　約定連結存款帳戶付款之設計原則，應符合下列要求：

一、電子支付機構採用直接連結機制或間接連結機制，提供約定連結存款帳戶付款服務。

二、電子支付機構應向金融機構申請金融憑證，並與金融機構約定為執行約定連結存款帳戶付款作業之專屬憑證；應用時應以憑證簽章方式提出約定連結申請或扣款指示，雙方同意以憑證簽驗章機制作為交易不可否認。申請方式如下：

(一)直接連結機制：向使用者開戶金融機構申請。

(二)間接連結機制：向電子支付機構之專用存款帳戶銀行申請。

三、約定連結程序：

（一）使用者應向電子支付機構提出申請並同意委由電子支付機構代使用者辦理轉帳，使用者並依下列方式向開戶金融機構提出申請：

１、以臨櫃或電子銀行向開戶金融機構提出申請。

２、透過電子支付機構依前款所定方式，向開戶金融機構提出申請。

（二）使用者提出申請時，應提供其開戶金融機構存款帳戶帳號、電子支付帳戶帳號及其他約定資料，經開戶金融機構確認使用者身分後完成約定。

（三）電子支付機構應要求開戶金融機構依金融機構辦理電子銀行業務安全控管作業基準所規定之交易面之介面安全設計確認使用者身分，並依不同身分確認方式所適用之風險類別，限制轉帳交易額度。

（四）使用者利用同一電子支付機構之約定連結存款帳戶付款服務，每月付款金額以新臺幣三十萬元為限。

四、交易程序：

（一）直接連結機制：電子支付機構應依使用者支付指示，向開戶金融機構提出扣款指示，經開戶金融機構驗

證與電子支付機構約定之金融憑證及核對約定連結存款帳戶相關資料後撥付款項。

（二）間接連結機制：電子支付機構應依使用者支付指示，經由專用存款帳戶銀行介接金融資訊服務事業或票據交換所，向開戶金融機構提出扣款指示，經專用存款帳戶銀行驗證與電子支付機構約定之金融憑證，並由開戶金融機構核對約定連結存款帳戶相關資料及金融資訊服務事業或票據交換所傳送之相關訊息後撥付款項。

五、私鑰保護：憑證私鑰應儲存於符合共同準則（Common Criteria） EAL 4+（至少包含增項 AVA_VLA.4 或 AVA_VAN.5）或 FIPS 140-2 Level 3(含)以上或其他相同安全強度之硬體安全模組內並限制金鑰明文匯出。

六、存取控制：電子支付機構應建立管控機制，限制非授權人員或程式存取私鑰及約定連結存款帳戶付款作業之相關程式。

七、通知機制：電子支付機構應要求開戶金融機構建立通知機制，於完成轉帳交易後，通知使用者。

八、風險控管：電子支付機構應要求專用存款帳戶銀行或開戶金融機構建立合理交易流量管控機制。

九、終止約定連結申請：

（一）使用者應依第三款第一目方式或其他與電子支付機構或開戶金融機構約定之方式，提出終止約定連結申請。

（二）開戶金融機構於使用者直接向其申請終止約定連結時，應通知電子支付機構。

十、兼營電子支付機構簡化規定：

（一）兼營電子支付機構之銀行或中華郵政股份有限公司為開戶金融機構時，得依本辦法之規定確認使用者身分，完成約定連結程序及交易程序，不適用第二

款至第四款、第七款及第八款之規定。

（二）兼營電子支付機構之銀行或中華郵政股份有限公司非開戶金融機構，並採用間接連結機制時，得不適用第二款第二目、第三款第一目之2及第四款第二目有關與專用存款帳戶銀行約定及驗證金融憑證之規定。

第十四條　電子支付平臺之機敏資料隱密及金鑰管理，應符合下列要求：

一、如有下列情形者，應建立訊息隱密性機制：

(一)機敏資料儲存於使用者端操作環境。

(二)機敏資料於網際網路上傳輸。

(三)使用者身分識別資料(如密碼、個人化資料)儲存於系統內；如為生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)，應遵循銀行公會所訂定之生物特徵相關自律規範辦理。

二、使用者身分識別資料如為固定密碼者，於儲存時應先進行不可逆運算(如雜湊演算法)，另為防止透過預先產製雜湊值推測密碼，應進行加密保護或加入不可得知之資料運算；採用加密演算法者，其金鑰應儲存於硬體安全模組內並限制匯出功能。

三、採用硬體安全模組保護金鑰者，該金鑰應由非系統開發與維護單位(如客服、會計、業管等)之二個單位(含)以上產製並分持管理其產製之基碼單，另金鑰得以加密方式分持匯出至安全載具(如晶片卡)或備份至具存取權限控管之位置，供維護單位緊急使用。

四、應減少金鑰儲存之地點，並僅允許必要之管理人員存取金鑰，以利管理並降低金鑰外洩之可能性。

五、當金鑰使用期限將屆或有洩漏疑慮時，應進行金鑰替換。

第二十四條　本辦法自中華民國一百零四年五月三日施行。

本辦法修正條文除中華民國一百零六年十二月二十八日修正發布之條文自一百零七年一月一日施行外，自發布日施行。