電子支付機構資訊系統標準及安全控管作業基準

金融監督管理委員會 110 年 6 月 15 日
金管銀票字第 1100136807 號函同意照辦
金融監督管理委員會 112 年 3 月 20 日
金管銀票字第 1120133069 號函同意照辦

第一條　本基準依電子支付機構管理條例(以下簡稱本條例)第三十二條第二項規定訂定之。

第二條　電子支付機構辦理電子支付機構業務之資訊系統及安全控管作業，應依本基準規定辦理。

第三條　本基準用詞定義如下：

一、網路型態區分如下：

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

(二)網際網路(Internet)：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。

二、訊息防護措施區分如下：

(一)訊息隱密性(Confidentiality)：指訊息不會遭截取、窺竊而洩漏資料內容致損害其秘密性。

(二)訊息完整性（Integrity）：指訊息內容不會遭篡改而造成資料不正確，即訊息如遭篡改時，該筆訊息無效。

(三)訊息來源辨識性(Authentication)：指傳送方無法冒名傳送資料。

(四)訊息不可重複性(Non-duplication)：指訊息內容不得重複。

(五)訊息不可否認性(Non-repudiation)：指無法否認其傳送或接收訊息行為。

三、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)或其他對稱性加解密演算法。

(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）或其他非對稱性加解密演算法。

(三)雜湊函數：指安全雜湊演算法(Secure Hash Algorithm；以下簡稱 SHA)、縱向冗餘校驗(Longitudinal Redundancy Check；以下簡稱 LRC)、循環冗餘校驗(Cyclic Redundancy Check；以下簡稱 CRC)、訊息鑑別碼(Message Authentication Code；以下簡稱 MAC)。

四、安全元件(Secure Element)：指符合我國國家標準 CNS 15408 EAL 4+(含增項 AVA_VLA.4 及 ADV_IMP.2)、共通準則(Common Criteria) ISO/IEC 15408 v2.3 EAL 4+(含增項 AVA_VLA.4 及 ADV_IMP.2)、ITSEC level E4、FIPS 140-2 Level 3 以上或其他相同安全強度認證之設備。

五、行動裝置：指包含但不限於智慧型手機、平板電腦等具通信及連網功能之使用者可攜式設備。

六、儲值卡端末設備：指可讀取儲值卡內容資訊，並將資料

傳送至特約機構或電子支付機構後台進行帳務處理之設備。

七、實體通路支付服務（Online To Offline，O2O）：指電子支付機構就電子支付機構業務，利用行動支付或儲值卡端末設備於實體通路提供服務。

八、行動支付：指消費者使用智慧型行動載具，透過密碼或生物特徵等身分驗證、掃碼及近距離無線通訊(Near-field communication，NFC)感應或結合物聯網相關先進應用等驗證及傳輸技術，於實體商店結帳付款，取得商品或使用服務之實質交易支付方式。

九、限定性繳稅費：指使用者透過電子支付帳戶或使用者授權特約機構發動交易指示，由使用者之電子支付帳戶繳納政府機關、金融機構或事業單位事先指定稅費及款項，並匯入指定帳戶。

十、指定稅費：繳納政府部門規費、稅捐、罰鍰或其他費用及支付水費、電費、瓦斯費、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、公共汽機車）、停車等服務費用、依公益勸募條例辦理勸募活動之捐贈金、配合政府政策且具公共利益性質經主管機關核准者、支付特約機構受各級政府委託代徵收之規費、稅捐與罰鍰、或受政府部門委託代收之服務費。

十一、機敏資料：指包含但不限於密碼、個人資料、身分認證資料、信用卡卡號、信用卡驗證碼或個人化資料等。

十二、使用者端電腦應用程式：指電子支付機構所發行或提供，且運行於非行動裝置之應用程式，包含但不限於軟體開發套件（Software Development Kit, SDK）、外掛程式（plug-in）等。

十三、近距離無線通訊（Near Field Communication；以下簡稱 NFC）：指利用點對點功能，使行動裝置在近距離內與其他設備進行資料傳輸。

十四、條碼受理終端：指參與條碼解析及生成之終端裝置，包含但不限於行動、POS 及自動化服務設備等裝置，並依照條碼資訊以進行相關交易作業。

十五、交易資訊類：指該條碼用於取代人工輸入之行為，該條碼被掃描後，掃描之處理端應用程式顯示相關資訊，經使用者檢視條碼內容後，由使用者另啟動交易指示者。

十六、交易指示類：指該條碼被條碼受理終端掃描解析後，應用程式依所含指示內容進行交易，涉及資金轉移或直接影響使用者及特約機構權益者。

十七、條碼處理平臺：指提供條碼解析及生成、重要資料之加解密、加解密系統金鑰管理及交易訊息處理等功能之管理平臺。

十八、主掃模式：指電子支付機構、特約機構或收款使用者生成交易之條碼，付款使用者持行動裝置應用程式掃描以確認交易，傳輸至條碼處理平臺或其他支付系統，完成支付交易。

十九、被掃模式：指付款使用者持行動裝置應用程式生成條碼，提供特約機構或收款使用者掃描後，傳輸至條碼處理平臺或其他支付系統，完成支付交易。

二十、系統維運人員：指電子支付平臺之作業人員，其管理或操作營運環境之應用軟體、系統軟體、硬體、網路、資料庫、使用者服務、業務推廣、帳務管理或會計管理等作業。

二十一、電子支付平臺：指辦理電子支付機構業務相關之應用軟體、系統軟體及硬體設備。

二十二、電子支付作業環境：指電子支付平臺、網路、作業人員及與該電子支付平臺網路直接連結之應用軟體、系統軟體及硬體設備。

二十三、代碼化(Tokenization)：運用 EMVCo 組織技術，提供一組與原始資料具有相同格式的代碼，藉以替代原始的敏感性資料。

第四條　電子支付機構執行本基準所列交易安全設計，應符合下列要求：

一、使用加密押碼簽章，其安全設計應符合下列要求：

(一)訊息加密：應採用對稱性加解密系統或非對稱性加解密系統進行訊息加密；如為增強要求應採用符合第六條訊息隱密性之安全設計進行訊息加密。

(二)訊息押碼：應採用具安全認證之晶片型儲值卡或端末安全模組以對稱性加解密系統或非對稱性加解密系統進行訊息押碼；如為增強要求應採用符合第六條訊息完整性之安全設計進行訊息押碼。

(三)訊息簽章：應採用具安全認證之晶片卡、晶片型儲值卡或端末安全模組以非對稱性加解密系統進行訊息簽章；如為增強要求應採用符合第六條訊息不可否認性之安全設計進行憑證簽章，並符合本款第四目要求。

(四)憑證簽章

1、應符合下列要求：

(1)應遵循憑證機構之憑證實務作業基準。

(2)應確認憑證之合法性、正確性、有效性、保證等級及用途內容，該憑證應由我國憑證主管機關核定之第三方憑證機構所核發。

(3)應擔任憑證註冊中心，受理使用者憑證註冊或資料異動時，其註冊中心之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；臨櫃確認使用者身分應核驗國民身分證及具辨識力之第二身分證明文件（如健保卡等）；如為外籍人士應核驗本人之居留證及具辨識力之第二身分證明文件（如護照等）。

(4)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。

(5)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。

(6)政府機關核發之憑證(如自然人憑證、工商憑證)限應用於註冊時之身分確認。

(7)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。

2、如為金融憑證簽章，除符合前子目憑證簽章要求外，其憑證可應用於金融交易且經本會認可。

3、如為硬體金融憑證簽章，除符合前子目金融憑證簽章要求外，其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。

二、使用晶片金融卡，其安全設計應符合下列要求：

(一)應用於簽入作業時，應由原發卡行驗證交易驗證碼始得簽入(如：餘額查詢交易)。

(二)系統應依每筆交易動態產製不可預知之端末設備查核碼，並檢核網頁回傳資料之正確性及有效性。

(三)應用於辦理國內外小額匯兌時，系統應每次輸入卡片密碼產生交易驗證碼。

(四)元件於存取卡片時應設計防止第三者存取。

(五)應提示收回卡片妥善保管。

三、使用一次性密碼，係運用動態密碼產生器（Key Token）、晶片金融卡或以其他方式運用 OTP 原理，產生限定一次使用之密碼者，其安全設計應符合下列要求：

(一)所產生之一次性密碼，如應用於辦理國內外小額匯兌時，且該密碼之產生與交易內容無關者，應限定該密碼於產生時起 120 秒內有效。

(二)採用簡訊傳送OTP且應用於辦理國內外小額匯兌時，應符合下列要求：

1、電子支付機構發送OTP與發送行銷廣告之門號應有所區隔。

2、考量使用者交易使用之電腦或行動裝置，可能遭植入惡意程式竊取 OTP 等敏感資料，應加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP綁交易、語音OTP、SIM認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易內容等)。

四、使用兩項以上技術，其安全設計應具有下列三項之任兩項以上技術：

(一)使用者與電子支付機構所約定之資訊，且無第三人知悉（如密碼、圖形鎖、手勢等)。

(二)使用者所持有之設備，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)。

(三)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。如應用於辦理國內外小額匯兌時，應符合下列要求：

1、採用直接驗證生物特徵技術者，電子支付機構應確認真人(Liveness Detection)、本人(Biorecognition)辦理並符合「金融機構運用新興科技作業規範」有關生物特徵資料安全控管部分。又電子支付機構應依據其風險承擔能力調整生物特徵參數(如近似率、錯誤接受率、錯誤拒絕率)，以期有效識別使用者身分；若無法有效確認真人或本人時應加強防護機制(可評估前款第二目第 2 子目防護機制)。

2、採用間接驗證生物特徵技術者，電子支付機構應事先評估使用者端設備驗證機制之有效性，善盡告知使用者使用上之風險，並提供間接驗證機制關閉管道，必要時應加強防護機制(可評估前款第二目第 2 子目防護機制)。

五、使用視訊會議，其安全設計應符合下列要求：

(一)應確認真實視訊環境(如隨機問答)，以防止透過科技預先錄製影片、製作面具或模擬影像等機制偽冒身分。

(二)應依相關規定留存影像或照片，以利後續查證。

(三)若依規定須驗證留存證件者應核對確認。

六、使用知識詢問，其安全設計應利用使用者之其他資訊(如卡號、有效月年及檢查碼、學校教育、社群識別碼、交易紀錄等)，以利有效識別使用者身分。如為辦理收付實質交易業務並以儲值卡進行交易者，另應確保非本人授權使用之交易於掛失後無需承擔遭冒用之損失，電子支付機構應於十四日內返還帳款，持卡人應配合協助電子

支付機構之後續調查作業。

七、使用固定密碼，其安全設計應符合下列要求；使用圖形鎖或手勢，準用下列第五目及第六目要求：

(一)不應少於六位，若搭配交易密碼使用則不應少於四位且交易密碼應符合本款固定密碼之相關規定。

(二)建議得採英數字混合使用，且宜包含大小寫英文字母或符號。

(三)不應訂為相同之英數字、連續英文字或連號數字，系統預設密碼不在此限。

(四)不應與帳號、使用者代號、交易密碼相同。

(五)連續錯誤達五次時不得再繼續執行交易，須重新申請密碼。

(六)變更後之固定密碼不得與原固定密碼相同。

(七)首次登入時，應強制變更系統產製的預設密碼；若未於 30 日內變更者，則不得再以該預設密碼執行簽入。

(八)超過一年未變更，電子支付機構應做妥善處理。

前項第一款硬體金融憑證簽章安全設計得替代第二款至第五款之任一款安全設計，第二款至第五款安全設計得替代第六款或第七款安全設計。

第五條　電子支付機構於不同網路型態應確保電子支付交易符合下列安全規定：

一、專屬網路：應符合訊息完整性、訊息來源辨識性及訊息不可重複性之訊息防護措施。如採用前條第一款第四目憑證簽章者，應同時符合訊息不可否認性之訊息防護措施。

二、網際網路或行動網路：應符合訊息隱密性、訊息完整性、訊息來源辨識性及訊息不可重複性之訊息防護措施。如採用前條第一款第四目憑證簽章者，應同時符合訊息不

可否認性之訊息防護措施。

第六條　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。

第七條　電子支付機構對於使用者及特約機構，所採用之身分確認程序之安全設計如下：

一、確認行動電話號碼：應採用第四條第三款一次性密碼、SIM 認證或電信認證確認使用者或個人特約機構可操作並接收訊息通知。

二、確認金融支付工具：

(一)存款帳戶，其安全設計應確認申請人與該帳戶持有人為同一統一編號且係透過臨櫃或視訊櫃員機方式開立或為第一類或第二類數位存款帳戶；驗證存款帳戶時，

應透過開戶金融機構、金融資訊服務事業或票據交換所辦理且無須進行交易驗證碼(有卡)驗證或一次性密碼(無卡)驗證。

(二)信用卡，其安全設計應確認申請人與信用卡持卡人為同一統一編號且係透過信用卡授權交易方式，以確認該卡片之有效性(如預授權)；驗證信用卡有效性時，應透過信用卡發卡機構、聯合信用卡處理中心或金融資訊服務事業之「信用卡輔助持卡人身分驗證平臺」辦理。

(三)確認個人使用者之金融支付工具，除依前二目辦理外，應採用下列任一方式辦理：

1、開戶金融機構或信用卡發卡機構於約定連結存款帳戶付款或綁定信用卡驗證時，依前款規定確認該個人使用者於開戶金融機構或信用卡發卡機構留存之行動電話號碼；如有異常之情事，得採用第四條第一款、第二款、第五款或第六款之安全設計加強確認。

2、透過開戶金融機構、信用卡發卡機構、金融資訊服務事業、票據交換所或聯合信用卡處理中心確認申請人留存之行動電話號碼與開戶金融機構或信用卡發卡機構留存之行動電話號碼之一致性；如有異常之情事，得採用第四條第一款、第二款、第五款或第六款之安全設計加強確認。

三、以臨櫃審查、符合電子簽章法之憑證簽章或透過視訊櫃員機，確認使用者身分：

(一)臨櫃審查，其安全設計應了解使用者動機、查證電話與住址、辨識具照片之身分證明文件、留存影像、留存印鑑或簽名、約定收付款限額及注意周邊環境或觀察有無異常舉止或遭脅迫。

(二)憑證簽章，其安全設計應採用第四條第一款第四目之安全設計。

(三)視訊櫃員機(以下簡稱 VTM)，其安全設計應符合下列安全規定：

1、VTM 應具備確認使用者本人申辦業務之舉證能力及方法（如照片、影像或聲音），並留存驗證紀錄及交易軌跡，遇有爭議時則可調閱相關紀錄。

2、VTM 應具備身分證相關規範辨識要項進行辨識之模組並能協助辨識身分證明文件以利判斷真偽，其中應能檢視國民身分證18種防偽特徵，惟排除手觸(壓凸觸摸圖形)及翻轉(折光變色油墨)兩項防偽設計。

3、VTM 應能檢視環境，並提供即時檢視現場影像及收音，輔助後台人員觀察有無異常舉止或遭脅迫。

4、應限制VTM直接連結電子支付機構內部網路並建置必要防護措施（如防火牆、防毒偵測、入侵偵測等），並關閉不必要服務。

5、VTM如產製儲值卡，應符合下列要求：

(1)卡片發卡、個人化或金鑰管理，其金鑰應儲存於經第三方認證(如FIPS 140-2 Level 3以上)之硬體安全模組；如放置於無人看管處應增加保全24小時監控。

(2)應具備卡片沒收裝置。

前項第一款 SIM 認證，其安全設計應確認申請人及該門號持有人為同一統一編號且係透過用戶身分模組（Subscriber Identity Module，SIM）連線至所屬電信業者，確認該SIM之有效性、交易訊息確實由該 SIM 所發送且留存於電信業者資料庫之門號與使用者輸入或服務提供者帶入之門號相符。

第一項第一款電信認證，其安全設計除符合 SIM 認證要求外，應為使用者至電信業者直營門市臨櫃申辦，交付國民身分證或外

國人護照及其他足以辨識身分之證明文件並排除電信儲值卡、親子卡、預付卡、企業卡、委託代辦等無法辨識本人親辦親簽之門號。

第八條　電子支付機構於使用者或特約機構登入電子支付平臺時應進行身分確認，使用者或特約機構應以帳號及第四條第一款至第三款之任一款、第四款之任一項技術或第五款至第七款之任一款安全設計辦理。

前項帳號之安全設計：

一、不得使用顯性資料(如統一編號、身分證號、行動電話號碼、電子郵件帳號、信用卡號、存款帳號等)作為唯一之識別，否則應另行增設使用者代號以資識別。

二、同一帳號在同一時間內僅能登入一個連線(session)控制之系統。

三、如增設使用者代號，至少應依下列方式辦理：

(一)不得為電子支付機構已知之使用者或特約機構之顯性資料。

(二)如輸入錯誤達五次，電子支付機構應做妥善處理。

(三)新建立時不得相同於帳號及密碼；變更時，亦同。

第九條　電子支付機構對於不同交易類型，應依其不同應用範圍，採用下列交易安全設計：

一、代理收付實質交易（含實體通路支付服務交易）：使用者以儲值卡款項支付、以電子支付帳戶款項支付、以約定連結存款帳戶付款支付、提出提前付款請求或提出取消暫停支付請求時，及使用者以約定連結存款帳戶付款支付儲值款項時，應依其不同交易限額，採用下列交易安全設計：

(一)儲值卡進行線上即時交易

1、辦理指定稅費或每筆交易金額等值新臺幣一千元以下

者，應採用第四條第二款晶片金融卡、第三款一次性密碼、第四款兩項以上技術之任一項技術、第六款知識詢問、第七款固定密碼之任一款安全設計；如為具加解密運算能力之晶片卡、記憶型晶片卡與其密碼、磁條卡與其密碼者得採用第四條第一款第一目訊息加密安全設計；如採用第六款知識詢問安全設計者，應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，電子支付機構應於十四日內返還帳款，持卡人應配合協助電子支付機構之後續調查作業；具加解密運算能力之晶片卡配合採用其他技術防護措施(如消費行為分析、卡片黑名單檢查或電文完整性檢查)並提供使用者與特約機構權益保障者，該筆交易金額可達等值新臺幣一千五百元，最高不超過當日累計等值新臺幣三千元為限。

2、每筆交易金額超過等值新臺幣一千元者，應採用第四條第一款第二目訊息押碼或第三目訊息簽章或第四款兩項以上技術之安全設計；如採用訊息押碼或訊息簽章者，應採用具安全認證之晶片型儲值卡或端末安全模組進行押碼或簽章。

3、電子支付機構發行附隨電子支付帳戶儲值卡，如採用代碼化(Tokenization)技術及行動裝置安全儲存媒介(SE，Secure Element)機制，應依循「信用卡業務機構辦理行動信用卡業務安全控管作業基準」第四章特殊安全設計之「安全儲存媒介」（SE）及「行動裝置」規範辦理。

(二)電子支付帳戶進行線上即時交易

1、辦理指定稅費，應採用第四條第一款金融憑證簽章、第二款晶片金融卡、第三款一次性密碼、第四款兩項

以上技術之任一項技術、第六款知識詢問、第七款固定密碼之任一款安全設計。

2、每筆交易金額未達等值新臺幣五千元，或每日交易金額未達等值新臺幣二萬元，或每月交易金額未達等值新臺幣五萬元者，應採用第四條第一款金融憑證簽章至第七款之任一款安全設計。

3、每筆交易金額達等值新臺幣五千元且未達等值新臺幣五萬元，或每日交易金額達等值新臺幣二萬元且未達等值新臺幣十萬元，或每月交易金額達等值新臺幣五萬元且未達等值新臺幣二十萬元者，應採用第四條第一款金融憑證簽章至第四款之任一款安全設計。

4、每筆交易金額達等值新臺幣五萬元以上，或每日交易金額達等值新臺幣十萬元以上，或每月交易金額達等值新臺幣二十萬元以上者，應採用第四條第一款金融憑證簽章至第四款之任一款安全設計，惟排除軟體 OTP 及簡訊 OTP。

(三)儲值卡進行非線上即時交易

1、採用接觸式或非接觸式介面且應用於辦理指定稅費或每筆交易金額等值新臺幣一千元以下者，應採用第四條第一款第一目訊息加密安全設計，由儲值卡端末設備確認儲值卡及由儲值卡確認儲值卡端末設備或電子支付機構之合法性；具加解密運算能力之晶片卡配合採用其他技術防護措施（如消費行為分析、卡片黑名單檢查或電文完整性檢查）並提供使用者與特約機構權益保障者，該筆交易金額可達等值新臺幣一千五百元，最高不超過當日累計等值新臺幣三千元為限。

2、採用接觸式或非接觸式介面且每筆交易金額超過等值新臺幣一千元者，應採用第四條第一款第一目增強要

求之訊息加密安全設計，由儲值卡端末設備確認儲值卡及由儲值卡確認儲值卡端末設備或電子支付機構之合法性。

3、以網際網路或行動網路者，應採用第四條第一款第一目增強要求之訊息加密安全設計，由儲值卡端末設備確認儲值卡及由儲值卡確認儲值卡端末設備或電子支付機構之合法性。

二、收受儲值款項：

(一)儲值卡進行線上即時儲值交易

1、採用具加解密運算能力晶片卡、記憶型晶片卡、磁條卡且透過專屬網路者，應採用第四條第一款第一目訊息加密之安全設計，由儲值卡確認儲值卡端末設備或電子支付機構之合法性。

2、採用具安全認證之晶片型儲值卡且透過專屬網路者，應採用第四條第一款增強要求之訊息加密安全設計，由儲值卡確認儲值卡端末設備或電子支付機構之合法性。

3、採用網際網路或行動網路者，應採用第四條第一款第一目增強要求之訊息加密安全設計，由儲值卡確認儲值卡端末設備或電子支付機構之合法性。

(二)儲值卡進行非線上即時儲值交易

1、採用具加解密運算能力晶片卡、記憶型晶片卡、磁條卡且透過接觸式或非接觸式介面者，應採用第四條第一款第一目訊息加密之安全設計。

2、採用具安全認證之晶片型儲值卡且透過接觸式或非接觸式介面者，應採用第四條第一款第一目增強要求之訊息加密安全設計。

3、採用網際網路或其他離線方式者，應採用第四條第一

款第一目增強要求之訊息加密安全設計。

三、辦理國內外小額匯兌

(一)每筆交易金額未達等值新臺幣五萬元，或每日交易金額未達等值新臺幣十萬元，或每月交易金額未達等值新臺幣二十萬元者，應採用第四條第一款金融憑證簽章、第二款晶片金融卡、第三款一次性密碼、第四款兩項以上技術之任一款安全設計。

(二)每筆交易金額達等值新臺幣五萬元，或每日交易金額達等值新臺幣十萬元，或每月交易金額達等值新臺幣二十萬元者，應採用第四條第一款硬體金融憑證簽章安全設計。

四、電子支付帳戶進行事先約定支付交易：

(一)電子支付機構經使用者事先約定得進行自動交易扣款，約定時電子支付機構應依第一款及第三款不同交易類型及限額採用相應之交易安全設計。

(二)電子支付機構經使用者事先約定得接受由特約機構發動限定性繳稅費之扣款指示，約定時電子支付機構應依第一款不同交易類型及交易限額採用相應之交易安全設計，惟與特約機構間之訊息交換，應符合第五條及第六條之安全設計。另使用者向特約機構或電子支付機構終止扣款約定後，無需承擔未約定交易之損失，特約機構或電子支付機構應於十四日內返還帳款，使用者應配合協助後續調查作業。

(三)電子支付機構經使用者事先約定得提供特約機構一次性虛擬帳號付款或委託他人代收之服務，約定時電子支付機構應採用第四條第一款金融憑證簽章至第四款之任一款安全設計。

五、帳務清算及結算交易：採用網際網路或行動網路者應採

用第四條第一款第二目訊息押碼或第三目訊息簽章或第四款兩項以上技術之安全設計；如採用第四條第一款第二目訊息押碼或第三目訊息簽章者，應採用具安全認證之晶片型儲值卡或端末安全模組進行押碼或簽章。

採用前項安全設計，得直接進行該類交易安全設計，使用者得無須先登入電子支付平臺；另電子支付機構依使用者事先約定執行扣款服務時，使用者得亦無須先登入電子支付平臺。

第十條　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 FXML 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：透過金融資訊服務事業或票據交換所，間接向 FXML 之憑證註冊中心提出申請。

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，限制扣款額度。

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，透過金融資訊服務事業或票據交換所，向開戶金融機構以憑證簽章提出扣款指示，經金融機構、金融資訊服務事業或票據交換所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，確認訊息隱密性、訊息完整性、訊息來源辨識性及訊息不可重複性後撥付款項。

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，得依本基準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、第三款第一目第 2 子目及第四款第二目有關驗證金融憑證之規定。

第十一條　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：

(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)除儲值卡端末設備外，應設計連線(Session)控制及網頁逾時(TimeOut)中斷機制，使用者或特約機構超過十分鐘未使用應中斷其連線或採取其他保護措施；但使用者以第四條第四款第二目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，但僅具收款功能之操作畫面不在此限。

(三)應辨識合作第三方網站或應用系統傳送之訊息，確保訊息隱密性、訊息完整性、來源辨識性及訊息不可重複性並妥善保護使用者及特約機構資料。

(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。

(六)應避免存在網頁程式安全漏洞(如 Injection、Cross-Site Scripting 等)。

(七)應偵測網頁與程式異動時，進行紀錄與通知措施。

(八)採用固定密碼進行身分確認者，應加強下列安全機制：

1、採用適當保護機制，防止以模擬瀏覽器(如 WebView、WebBrowser 等)方式竊取敏感資料(如不支援模擬瀏覽器、網頁程式動態變化、App 外開指定瀏覽器等)。

2、提供端點對端點加密機制。係指於使用者或特約機構端(如瀏覽器)輸入固定密碼後立即加密，傳送至電子支付機構可信任網段(如經兩道防火牆隔離之獨立網段)於符合 FIPS 140-2 Level 3 以上之硬體安全模組(如 HSM)內進行解密，並於硬體安全模組內或於無洩漏解密資料疑慮之安全環境進行驗證。

3、確定為使用者行為(如於登入成功及失敗均及時通知使用者、採用圖形驗證碼經人工確認、搭配風險評估增加額外認證等)。

(九)應設計於使用者及特約機構修改個人資料、約定或變更提領電子支付帳戶款項之銀行存款帳戶時，應採用第四條第一款至第五款之任一款安全設計，惟異動行動電話號碼或兩項以上技術，且採用軟體 OTP 或簡訊 OTP 安全設計者，應加強防護機制(可評估第四條第三款第二目第 2 子目防護機制)。

(十)應設計個人資料顯示之隱碼機制。

(十一)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。

(十二)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。

(十三)應提供使用者及特約機構安全宣導，強化風險認知與交易確認。

二、實體通路支付服務程式：

(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)電子支付機構辦理代理收付實質交易、儲值卡款項移轉交易或辦理國內外小額匯兌時，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、使用者及特約機構端電腦應用程式：

(一)應採用被作業系統認可之數位憑證進行程式碼簽章(CodeSign)。

(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)採用第四條第二款晶片金融卡辦理國內外小額匯兌時，須於使用者端經由人工確認(如插拔卡、特殊按鍵等)交易內容後才完成交易；或於交易過程增加額外具「兩項以上技術」之介面設計認證機制，若採用經本會審核之確認型讀卡機或載具並可人工確認交易內容者，得不執行本措施。

四、使用者及特約機構端行動裝置應用程式：

(一)應建立應用程式發布程序，由兩人以上或採用兩項(含)以上技術管控。

(二)應於發布前檢視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資安、法遵及風控等主管同意，以利綜合評估是否符合「個人資料保護法」之告知義務。

(三)應用於個人資料查詢、辦理國內外小額匯兌時，如偵測行動裝置疑似遭破解(如 root、jailbreak、USB debugging 等)，應提示使用者注意風險並限制辦理國內外小額匯兌。

(四)應於顯著位置(如官網、應用程式下載頁面等)提示使用者及特約機構於行動裝置上安裝防護軟體。

(五)應於官網上提供應用程式之名稱、版本與下載位置。

(六)應建立偽冒應用程式偵測、下架或告警機制。

(七)電子支付機構每年應辦理下列檢測：

1、由合格實驗室依據經濟部工業局「行動應用APP基本資安檢測基準」辦理並通過檢測，且由資安專責主管確認完成改善。

2、針對應用程式及其應用伺服器之完整功能辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞。如因使用工具檢測可能導致之誤判或有解讀差異，電子支付機構得自行評估相關漏洞是否列為可承擔之風險，如屬可承擔風險並留存該風險評估紀錄者，不在此限。

3、辦理國內外小額匯兌者，應由評估單位針對應用程式及其應用伺服器依據本基準及OWASP公布之Mobile APP Security Checklist L2項目辦理並通過檢測，且由資安專責主管確認完成改善。

4、應就本目合格實驗室及評估單位所提交之報告建立檢

視機制，並送資安專責主管監控及執行資訊安全管理作業。

(八)應用程式及其應用伺服器新功能首次上線、系統架構異動或既有功能異動時，應針對新增或異動之程式辦理下列檢測：

1、辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞，如因使用工具檢測可能導致之誤判或有解讀差異，電子支付機構得自行評估相關漏洞是否列為可承擔之風險，如屬可承擔風險並留存該風險評估紀錄者，不在此限。

2、辦理國內外小額匯兌者，應依據 OWASP 公布之 Mobile Top 10 項目辦理並通過檢測，且由資安專責主管確認完成改善，如因故需緊急上線者仍應於一個月內完成。

(九)採用行動裝置儲存金鑰之安全設計，應符合下列要求：

1、應採用下列任一技術保護金鑰：

(1)採用晶片安全設計者，金鑰應儲存於安全元件內，並能防堵市面上常見之攻擊破解方法。

(2)採用軟體保護技術(如白箱加密法並搭配程式碼混淆技術)並經評估單位確認安全防護。

2、辦理國內外小額匯兌者，應確認金鑰儲存於使用者指定之行動裝置。

3、應於交易時增設存取控管或人工確認，限制由可信任行動應用程式存取金鑰，以防止遭受惡意程式發動阻斷服務攻擊或執行偽冒交易。

(十)採用空中傳輸(OTA)方式下載敏感資料前，應符合下列要求：

1、應確認使用者及特約機構身分(如密碼)，並採用嚴密的技術防護措施，且能有效防範相關資料被竊取。

2、應確認行動裝置及應用程式之正確性，並進行端點(行動裝置應用程式)對端點(電子支付機構)全程加密防護。

(十一)採用安全元件作為儲存裝置時，應確認使用者及特約機構指定之安全元件編號(如 SE ID)、並於 SE 內增設存取控管，限制由可信任應用程式存取。

(十二)辦理國內外小額匯兌並採用近距離無線通訊(NFC)技術進行付款交易資料傳輸者，應經由使用者人工確認其意思表示（如密碼、圖形驗證碼）。

(十三)採用 WebView、WebBrowser 存取具個人資料或認證資訊(如固定密碼)之網頁時，應無留存記錄或依據使用者或特約機構授權範圍辦理。

五、條碼掃描技術：

(一)條碼掃描支付過程中，所存取之資訊應遵循該業務所需最小化原則。

(二)採用交易資訊類條碼者，應用程式應以彈出式視窗或其他方式提供接收方檢視條碼之資料內容，再由接收方處理後續事宜。

(三)被掃模式採用交易指示類條碼者，因係屬使用者產生授權資訊同意扣款性質，應設定條碼合理使用時效，且在時效內以使用一次為限，惟辦理大眾運輸者除外。

(四)條碼受理終端所提交之條碼訊息請求應確保傳輸過程中的資訊完整性及隱密性，並確保在傳輸過程中不被篡改及洩露。

(五)條碼受理終端相關應用程式，應能針對所解析之條碼進行格式檢查，確保資料格式合理性，預防程式碼注入。

(六)條碼受理終端相關應用程式，應能針對所解析之交易指示類條碼進行來源辨識性及完整性檢查，對於未驗

證通過之條碼應予明確提示並拒絕執行交易。

(七)條碼受理終端相關應用程式，對所解析之條碼產生網站連結，應採包括但不限於白名單或伺服器認證等機制進行網站合法性檢查，以預防連結惡意網站或執行惡意程式風險。

(八)主掃模式及被掃模式等各類應用情境，所生成之交易指示類條碼收付不得共用，以確保專碼專用。

六、Application Programming Interface（API）訊息交換：

(一)應使用 HTTP 強制安全傳輸（Http Strict Transport Security，HSTS）協議，以防止 SSL 剝離（Strip）攻擊。

(二)應正面表列並限制僅接受所需之 HTTP 請求方法（如 GET、POST）。

(三)應採用 HTTP 請求表頭（header） content-type 欄位（如 application/xml、application/json 等）並確保回應內容與表頭所宣告內容類型（content-type）一致。

(四)應進行欄位格式檢查以防止常見之網頁應用程式威脅（如 Cross-Site Script、SQL Injection、Remote Code Execution 等）。

(五)認證資訊（如 credentials、password、tokens、API keys 等）應採用標準之 HTTP 授權表頭（Authorization header）或本體（Body）傳送，不得以 URL 之參數形式傳送。

(六)應設定安全性表頭（Security Headers），限定代理存取端僅針對指定之內容類型進行處理（X-Content-Type-Options： nosniff），並防止辦理身分確認之網頁為其他網站嵌入（X-Frame-Options：deny）。

七、Software Development Kit（SDK）軟體開發套件：應依據實際應用範圍，符合本條相關規範，如將SDK嵌入於第三方行動裝置應用程式時，該SDK仍應符合本條第四款，惟未辦理個人資料查詢或國內外小額匯兌者，得排除第四款第三目至第八目規定。

第十二條　環境及儲值卡端末設備面之安全需求及安全設計

一、環境及儲值卡端末設備面之安全需求

(一)建立安全防護策略

1、保持儲值卡端末設備與環境之實體完整性。

2、確保儲值卡端末設備交易之安全性。

3、建置有效或即時之管控名單管理機制。

4、非接觸式儲值卡應降低交易被意外觸發之機率。

5、應用於儲值卡進行非線上即時儲值交易，儲值卡端末設備應具有安全模組之設計，惟若安全模組係置於電子支付機構後端，於每次交易時由儲值卡端末設備採連線方式從電子支付機構取得與儲值卡相互認證之金鑰者，則不在此限。

6、應用於儲值卡進行非線上即時儲值交易或儲值卡進行非線上即時交易，若採用具加解密運算能力晶片卡、記憶型晶片卡或磁條卡，且應用於提供單筆交易金額超過等值新臺幣一千元交易之特約機構，應採取降低偽卡交易之必要措施(如消費行為分析、卡片黑名單檢查、電文完整性檢查)。

(二)提高系統可靠性之措施。

(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。

二、環境及儲值卡端末設備面之安全設計

(一)保持儲值卡端末設備與環境之實體完整性，應採用下

列各項安全設計：

1、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。

2、應確定與儲值卡端末設備合作廠商簽訂資料保密契約，並應將參與儲值卡端末設備安裝、維護作業之人員名單交付造冊列管，如有異動，應隨時主動通知電子支付機構更新之。

3、儲值卡端末設備安裝、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，並應配合隨時檢視儲值卡端末設備硬體是否遭到不當外力入侵或遭裝置側錄設備。

4、電子支付機構應不定時派員抽檢安裝於特約機構或電子支付機構之儲值卡端末設備，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)確保儲值卡端末設備交易之安全性，應符合下列規範

1、儲值卡內含錄碼及資料，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儲值卡端末設備。

2、應確保儲值卡端末設備之合法性，另儲值卡端末設備應有唯一之儲值卡端末設備代號。

3、應用於單筆交易金額超過等值新臺幣一千元之交易，儲值卡端末設備之安全模組應個別化（即每一儲值卡端末設備之認證金鑰皆不相同）。

(三)為有效防範非法儲值卡進行交易，電子支付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)電子支付機構應有效防止特約機構不當扣款，其儲值卡端末設備應包含下列設計，以降低非接觸式儲值卡在持卡人無交易之意願下，交易被意外觸發之機率：

1、感應距離限縮至十公分（含）以下。

2、交易過程應有聲音、燈號或圖像等之提示。

(五)非線上即時儲值交易之儲值卡端末設備應具有安全模組之設計，進行儲值交易另應包含下列設計：

1、逐筆授權儲值交易。

2、限制其單筆儲值金額。

3、限制其儲值總額（如：日限額），額度用罄應連線至電子支付機構重新授權可儲值額度。

4、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)採用具加解密運算能力晶片卡、記憶型晶片卡或磁條卡，且應用於提供單筆交易金額超過等值新臺幣一千元交易之特約機構，如管控名單之驗證未送回電子支付機構進行即時驗證者，電子支付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)儲值卡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、具備可模擬儲值卡讀卡機模式（reader mode ）之行動裝置等），可不適用第二款第一目、第二款第二目第 2 子目、第 3 子目及第五目之規定。

(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)應制定儲值卡端末設備管理規章，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、特約機構與電子支付機構簽約與管理辦法等。

第十三條　儲值卡之安全需求及安全設計

一、儲值卡類型

(一)儲值卡為下列類型之一者，得適用於辦理指定稅費或單筆交易金額等值新臺幣一千元以下交易：

1、具加解密運算能力之晶片卡。

2、記憶型晶片卡與其密碼。

3、磁條卡與其密碼。

(二)儲值卡為安全認證之晶片卡者，得適用於辦理單筆金額超過等值新臺幣一千元交易。前述所稱「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：

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

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

3、我國國家標準 CNS 15408 EAL4+(含增項 AVA_VLA.4及 ADV_IMP.2)。

4、EMVCo Security Evaluation Process。

5、其他經主管機關認可之驗證標準。

二、儲值卡之安全需求

(一)建立安全防護策略

1、確認儲值卡之合法性。

2、採用密碼者，應有一定之安全設計。

3、儲存於儲值卡之個人資料必須保護。

(二)制定作業管理規範：制定儲值卡交貨控管流程。

三、儲值卡之安全設計

(一)儲值卡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)若採用密碼者，應具有下列之安全設計：

1、密碼不應少於四位。

2、密碼連續錯誤達五次時應限制使用，須重新申請密碼。

3、變更後之密碼不得與變更前一次密碼相同。

4、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)儲存於儲值卡之個資必須保護：若使用儲值卡儲存個人資料，應設計存取控制或持卡人確認之機制，以限制其讀取。

(四)制定儲值卡交貨控管流程：發行機構應針對儲值卡之生命週期進行妥善之管理，應制定儲值卡製發卡與交貨控管流程、管制外包製卡作業及落實實體儲值卡之安全控管。

第十四條　電子支付機構之資訊安全政策、內部組織及資產管理應符合下列要求：

一、資訊安全政策應經董事會、常務董事會決議或經其授權之經理部門核定。但外國銀行在臺分行應由其負責人簽署。

二、前款資訊安全政策應對所有員工及相關外部各方公布與傳達。

三、應訂定資訊作業相關管理及操作規範。

四、第一款資訊安全政策及前款管理及操作規範應每年檢討修訂，並於發生重大變更(如新頒布法令法規)時審查，以持續確保其合宜性、適切性及有效性。

五、應依據電子支付平臺之作業流程，識別人員、表單、設備、軟體、系統等資產，建立資產清冊、作業流程、網路架構圖、組織架構圖及負責人，並定期清點以維持其正確性。

六、應定義人員角色與責任並區隔相互衝突的角色。

七、應依據作業風險與專業能力選擇適當人員擔任其角色並定期提供必要教育訓練。

第十五條　電子支付平臺之系統維運人員管理應符合下列要求：

一、應建立人員之註冊、異動及撤銷註冊程序，用以配置適當之存取權限。

二、應至少每年定期審查帳號與權限之合理性，人員離職或調職時應盡速移除權限，以符合職務分工與牽制原則。

三、硬體設備、應用軟體、系統軟體之最高權限帳號或具程式異動、參數變更權限之帳號應列冊保管；最高權限帳號使用時須先取得權責主管同意，並保留稽核軌跡。

四、應確認人員之身分與存取權限，必要時得限定其使用之機器與網路位置（IP）。

五、人員超過十分鐘未操作電腦時，應限制使用者個人資料顯示於螢幕。

六、於登入作業系統進行系統異動或資料庫存取時，應留存人為操作紀錄，並於使用後儘速變更密碼；但因故無法變更密碼者，應建立監控機制，避免未授權變更，並於使用後覆核其操作紀錄。

七、帳號應採一人一號管理，避免多人共用同一個帳號為原則，如有共用需求，申請與使用須有其他補強管控方式，

並留存操作紀錄且應能區分人員身分。

八、採用固定密碼者，應符合第四條第七款規定，並應定期變更密碼：提供人員使用之帳號至少三個月一次；提供系統連線之帳號，至少每三個月一次或其他補強管控方式（如限制人工登入）。

九、加解密程式或具變更權限之公用程式（如資料庫存取程式）應列冊管理並限制使用，該程式應設定存取權限，防止未授權存取，並保留稽核軌跡。

第十六條　電子支付作業環境之個人資料保護應符合下列要求：

一、為維護所保有個人資料之安全，應採取下列資料安全管理措施：

(一)訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，應採取防範資料洩漏之適當措施。

(二)針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。

(三)作業過程有備份個人資料之需要時，對備份資料予以適當保護。

二、保有個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物者，應採取下列設備安全管理措施：

(一)實施適宜之存取管制。

(二)訂定妥善保管媒介物之方式。

(三)依媒介物之特性及其環境，建置適當之保護設備或技術。

三、為維護所保有個人資料之安全，應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員約定保密義務 。

四、應針對電子支付作業環境，包含資料庫、資料檔案、報

表、文件、傳檔伺服器及個人電腦等進行清查盤點是否含有個人資料並編製個人資料清冊，並進行風險評估與控管。

五、應建置留存個人資料使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況，包括檔案、螢幕畫面、列表。

六、應建立資料外洩防護機制，管制個人資料檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁或網路檔案、或列印等方式傳輸，並應留存相關紀錄、軌跡與數位證據。

七、如刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：

(一)刪除、停止處理或利用之方法、時間。

(二)將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

八、為持續改善個人資料安全維護，其所屬個人資料管理單位或人員，應定期提出相關自我評估報告，並訂定下列機制：

(一)檢視及修訂相關個人資料保護事項。

(二)針對評估報告中有違反法令之虞者，規劃、執行改善及預防措施。

九、如自第三方機構(如電信業者)取得使用者或特約機構個人資料(如姓名、住址、電話、電子郵箱、繳款紀錄、電信評分等)者，電子支付機構應要求第三方機構須事先取得使用者或特約機構同意。

十、前款自我評估報告，應經董（理）事會、常務董（理）

事會決議或經其授權之經理部門核定。但外國銀行在臺分行或未設董（理）事會者，應由其負責人簽署。

第十七條　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或特約機構端操作環境。

(二)機敏資料於網際網路上傳輸。

(三)使用者或特約機構身分識別資料（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、使用者或特約機構身分識別資料中之固定密碼，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、應減少金鑰儲存的地點，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。

第十八條　電子支付平臺之實體安全應符合下列要求：

一、主機房與異地機房應避免同時在地震斷層帶、海岸線、山坡地、海平面下、機場飛航下、土石流好發區域、百年洪水氾濫區域、核災警戒範圍區域、工安高風險區域，

並應有相關防護措施，以避免受到地震、海嘯、洪水、火災或其他天然或人為災難之損害。

二、營運設備應集中於機房內，機房應建立門禁管制，以確保僅允許經授權人員進出；非授權人員進出應填寫進出登記，並由內部人員陪同與監督；進出登記紀錄應定期審查，如有異常應適當處置。

三、應於主機房及異地機房內建立全天候監視設備並確保監視範圍無死角。

四、應有足夠營運使用之電力、供水、用油等供應措施，當發生供應措施中斷時，應至少維持七十二小時運作時間，並應介接二家以上或異地二線以上網際網路電信營運商互為備援。

五、油槽儲存及消防安全應符合相關法規規定。

六、應設置環境監控機制，以管理電信、空調、電力、消防、門禁、監視及機房溫濕度等，並自動告警與通知。

七、機房管理應具備與機房相當之操作環境，或獨立可管制人員操作系統與設備之監控室。

前項第七款監控室應符合下列要求：

一、應具門禁與監視設備，且必須留存連線及使用軌跡，並定期稽核管理。

二、系統維運人員應經授權進入監控室使用監控室內專屬電腦設備；或應使用指定設備由內部網路以一次性密碼登入並經服務管控設備（如防火牆）使用監控室內專屬電腦設備。

三、連線過程須以內部網路、專線或虛擬私有網路進行。

四、監控室之網路設備與電腦設備如為電子支付作業環境之範圍，應符合本基準相關規定。

第十九條　電子支付作業環境之營運管理應符合下列要求：

一、應避免於營運環境安裝程式原始碼。

二、應建立定期備份機制及備份清冊，備份媒體或檔案應妥善防護，確保資訊之可用性及防止未授權存取。

三、應建立回存測試機制，以驗證備份之完整性及儲存環境的適當性。

四、相關留存紀錄應確保數位證據之收集、保護與適當管理程序，至少留存二年。

五、應訂定系統安全強化標準，建立並落實電子支付作業環境之系統安全設定。

第二十條　電子支付作業環境之脆弱性管理應符合下列要求：

一、應偵測網頁與程式異動，紀錄並通知相關人員處理。

二、應偵測惡意網站連結並定期更新惡意網站清單。

三、應建立入侵偵測或入侵防禦機制並定期更新惡意程式行為特徵。

四、應建立病毒偵測機制並定期更新病毒碼。

五、應建立上網管制措施，限制連結非業務相關網站，以避免下載惡意程式。

六、應隨時掌握資安事件，針對高風險或重要項目立即進行清查與應變。

七、應針對系統維運人員定期執行電子郵件社交工程演練與教育訓練，至少每年一次。

八、每季應進行弱點掃描，並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，填寫評估結果與處理情形，採取適當措施並確保作業系統及軟體安裝經測試且無弱點顧慮之安全修補程式。

九、應避免採用已停止弱點修補或更新之系統軟體與應用軟體，如有必要應採用必要防護措施。

十、電子支付平臺上線前及每半年應針對異動程式進行程式

碼掃描或黑箱測試，並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，執行矯正、紀錄處理情形並追蹤改善。

十一、電子支付平臺每年應執行滲透測試，以加強資訊安全。

第二十一條　電子支付作業環境之網路管理應符合下列要求：

一、網路應區分網際網路、非武裝區（Demilitarized Zone；以下簡稱 DMZ）、營運環境及其他（如內部辦公區）等區域，並使用防火牆進行彼此間之存取控管。機敏資料僅能存放於安全的網路區域，不得存放於網際網路及 DMZ 等區域。對外網際網路服務僅能透過 DMZ 進行，再由 DMZ 連線至其他網路區域。

二、電子支付作業環境與其他網路間之連線必須透過防火牆或路由器進行控管。

三、系統僅得開啟必要之服務及程式，使用者及特約機構僅能存取已被授權使用之網路及網路服務。內部網址及網路架構等資訊，未經授權不得對外揭露。

四、應檢視防火牆及具存取控制（Access control list，ACL）網路設備之設定，至少每年一次；針對高風險設定及六個月內無流量之防火牆規則應評估其必要性與風險；針對已下線系統應立即停用防火牆規則。

五、使用遠端連線進行系統管理作業時，應使用足夠強度之加密通訊協定，並不得將通行碼紀錄於工具軟體內。

六、應管控內部無線網路之使用人員申請，連線至電子支付作業環境時應加強身分確認並使用必要防護措施進行隔離、限制。

七、經由網際網路連接至內部網路進行遠距之系統管理工作，應遵循下列措施：

(一)應審查其申請目的、期間、時段、網段、使用設備、

目的設備或服務，至少每年一次。

(二)應建立授權機制，依據其申請項目提供必要授權，至少每年檢視一次。

(三)變更作業應加強身分認證，每次登入可採用照會或二項（含）以上安全設計並取得主管授權。

(四)應定義允許可連結之遠端設備，並確保已安裝必要資訊安全防護。

(五)應建立監控機制，留存操作紀錄，並由主管定期覆核。

第二十二條　電子支付作業環境之系統生命週期管理應符合下列要求：

一、應訂定資訊安全開發設計規範並落實執行。

二、對於委外開發的應用軟體，應執行監督並確保其有效遵循本基準規定。

三、應確保系統軟體和應用軟體安裝最新安全修補程式。

四、對於測試用之機敏資料，應先進行資料遮蔽處理或管制保護。

五、於開發階段起至營運階段，應遵循變更控制程序處理並留存相關紀錄；營運環境變更（如執行、覆核）應由二人以上進行，以相互牽制。

六、系統軟體變更應先進行技術審查並測試；套裝軟體不應自行異動，並應先進行風險評估。程式不應由開發人員自行換版或產製比對報表，應建立程式原始碼管理機制，以符合職務分工與牽制原則。

第二十三條　電子支付作業環境之委外管理應符合下列要求：

一、委外處理前應先對受託廠商進行適當之安全評估，並依據最小權限及資訊最小揭露原則進行安全管控設計。

二、委託契約或相關文件中，應明確約定下列內容：

(一)受託廠商應遵守本基準及其他適當資訊安全國際標準要求，確保委託人資料之安全。

(二)對受託廠商應依本基準內容進行適當監督。

(三)當委外業務安全遭到破壞時，受託廠商應主動、即時通知委託人。

(四)交付之系統或程式應確保無惡意程式及後門程式，其放置於網際網路之程式應通過程式碼掃描或黑箱測試。

三、應對委外廠商進行資訊安全稽核或由委外廠商提出資訊安全稽核報告，至少每年一次。

第二十四條　電子支付作業環境之資訊安全事故管理應符合下列要求：

一、應將各作業系統、網路設備及資安設備之日誌及稽核軌跡集中管理，進行異常紀錄分析，設定合適告警指標並定期檢討修訂。

二、應建立資訊安全事故通報、處理、應變及事後追蹤改善作業機制，並應留存相關作業紀錄。

三、如有資訊安全事故發生時，其系統交易紀錄、系統日誌、安全事件日誌應妥善保管，並應注意處理過程中軌跡紀錄與證據留存之有效性。

第二十五條　電子支付作業環境之營運持續管理應符合下列要求：

一、應進行營運衝擊分析，定義最大可接受系統中斷時間，設定系統復原時間與資料復原時點，採取必要備援機制並應考量如有系統復原時間限制狀況下，建立安全距離外之異地備援機制，以維持交易可用性。

二、應建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其合理範圍內。

三、應每年驗證及演練其營運持續性控制措施，以確保其有效性，並應保留相關演練紀錄及召開檢討會議。

第二十六條　電子支付機構應盤點與資訊安全相關法規規定，並將相關資訊安全要求與內部控制制度結合，定期進行法令遵循自

評，以確保資訊安全之法令遵循性。

本基準所訂之資訊系統及安全控管項目，電子支付機構應透過內部控制制度進行定期檢核，並應於依本條例第十一條申請許可時及其後每年四月底前，由會計師進行檢視，提出資訊系統及安全控管作業評估報告，亦得併入內部控制制度查核報告辦理。

前項評估報告內容應至少包含評估人員資格、評估範圍、評估時所發現之缺失項目、缺失嚴重程度、缺失類別、風險說明、具體改善建議及社交演練結果，且應送稽核單位進行缺失改善事項之追蹤覆查。該報告應併同缺失改善等相關文件至少保存二年。

為確保交易資料之隱密性及安全性，並維持資料傳輸、交換或處理之正確性，主管機關於必要時，得要求電子支付機構提高資訊系統標準及加強安全控管作業。

第二十七條　本基準修正條文第七條第二款第三目，自中華民國一百十二年四月一日施行。

本基準經本會理事會議通過，函報主管機關備查後施行，修正時亦同。

附表一：不同交易類型依其不同應用範圍，所應採用交易安全設計一覽表

				加密押碼簽章	晶片金融卡	一次性密碼	兩項以上技術	視訊會議	知識詢問	固定密碼
代理收付實質交易款項（含實體通路支付服務交易）	儲值卡進行線上即時交易	繳納指定稅費 或 每筆交易 <= 1K		訊息加密 *具加解密運算能力之晶片卡(註二) *記憶型晶片卡與其密碼 *磁條卡與其密碼	0	0	任一		0 (註一)	0
		1K < 每筆交易		押碼 / 簽章 *具安全認證之晶片型儲值卡 *端末安全模組進行押碼簽章			任二			
	電子支付帳戶進行線上即時交易	繳納指定稅費		金融憑證簽章	0	0	任一		0	0
		每筆交易 < 5K 每日交易 < 20K 每月交易 < 50K		金融憑證簽章	0	0	任二	0	0	0
		5K <= 每筆交易 < 50K 20K <= 每日交易 < 100K 50K <= 每月交易 < 200K		金融憑證簽章	0	0	任二			
		50K <= 每筆交易 100K <= 每日交易 200K <= 每月交易		金融憑證簽章	0	0 排除軟體OTP及簡訊OTP	任二			
	儲值卡進行非線上即時交易	接觸式 或 非接觸式介面	繳納指定稅費 或 每筆交易 <= 1K	訊息加密 *具加解密運算能力之晶片卡(註二) *記憶型晶片卡與其密碼 *磁條卡與其密碼						

			1K < 每筆交易	增強要求之訊息加密						
		網際網路或行動網路		增強要求之訊息加密						
收受儲值款項	線上即時儲值交易	專屬網路	● 具加解密運算能力晶片卡 ● 記憶型晶片卡 ● 磁條卡	訊息加密						
			● 具安全認證之晶片型儲值卡	增強要求之訊息加密						
		網際網路或行動網路		增強要求之訊息加密						
	非線上即時儲值交易	接觸式或非接觸式介面	● 具加解密運算能力晶片卡 ● 記憶型晶片卡 ● 磁條卡	訊息加密						
			● 具安全認證之晶片型儲值卡	增強要求之訊息加密						
		網際網路或行動網路		增強要求之訊息加密						
辦理國內外小額匯兌		身分限制 *第二類電子支付帳戶	每筆交易 < 50K 每日交易 < 100K 每月交易 < 200K	金融憑證簽章	0	0	任二			
		*第一類電子支付帳戶	50K <= 每筆交易 100K <= 每日交易 200K <= 每月交易	硬體金融憑證簽章						
帳務清算及結算交易		網際網路或行動網路		押碼 / 簽章 *具安全認證之晶			任二			

		片型儲值卡 *端末安全模組進行押碼簽章						

註一：採用第六款知識詢問者，應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，電子支付機構應於十四日內返還帳款，持卡人應配合協助電子支付機構之後續調查作業。

註二：配合採用其他技術防護措施（如消費行為分析、卡片黑名單檢查或電文完整性檢查）並提供使用者與特約機構權益保障者，該筆金額可達等值新臺幣一千五百元，最高不超過當日累計等值新臺幣三千元為限。