

電子支付機構資訊系統標準及安全控管作業基準

部分條文修正條文對照表

修正條文	現行條文	說明
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	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	一、配合第四條第一項第四款增修實體設備分類之規範，爰配合增訂第二十六款有關「智慧型穿戴裝置」之用詞定義。 二、配合第四條第一項第六款開放金融 Fast-ID (全稱「金融機構行動身分識別標準化機制」(Financial Fast Identity Online))之交易安全設計之相關規範，爰增訂第二十七款有關「金融 Fast-ID」之用詞定義。

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	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+	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	(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。	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	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、支付核心系統：指支持本條例第四條第一項業務項目持續運作必要之系統或設備。 二十四、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。 二十五、開放應用程式介面 (Open Application Programming Interface，Open API)：為「電腦作業系統(Operating system)」或「程式函式庫」開放提供給應用程式呼叫使用的程式碼。 <u>二十六、智慧型穿戴裝置</u>：指具穿戴性、<u>無線連接網路功能，允許使用者自行安裝或執行應用程式，並提供資訊處理、通訊或其他智慧功能之個人使用裝置，主要為智慧手錶、智慧手環或智慧眼鏡。</u> <u>二十七、金融Fast-ID</u>：由<u>金融行動身分</u>	設備。 二十三、支付核心系統：指支持本條例第四條第一項業務項目持續運作必要之系統或設備。 二十四、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。 二十五、開放應用程式介面 (Open Application Programming Interface，Open API)：為「電腦作業系統(Operating system)」或「程式函式庫」開放提供給應用程式呼叫使用的程式碼。	
---	---	--

<u>識別聯盟推動之「金融行動身分識別標準化機制」(Financial Fast Identity Online)。</u>		
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	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	一、為兼顧風險控管及使用使用者便利性，新增設備約定憑證簽章之安全設計規範，亦即使用者與電子支付機構透過所約定持有實體設備上，完成裝置門號一致性認證後，可透過設備約定憑證簽章作為設備認證之交易安全設計，爰增訂第一項第一款第四目第四子目規定。 二、為提升使用兩項以上技術安全設計強度，避免使用者遭詐騙集團偽冒、盜用情事，爰修正第一項第四款規定，以使用者與電子支付機構間約定實體設備為必要採取技術，移列為第一目，搭配另二項技術選擇其中之一，並明定實體設備類型、控管及交易相關限制等規範，以強化約定實體設備之管控措施。 三、現行第七條第二項有關 SIM 認證及第三項有關電信認證規定，係屬交易安全設計機制，爰移列本條增訂第一項第五款行動電話號碼認證之安全設計，並配合實務運作上驗證機構對行動電話號碼

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	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	之驗證內容及強度予以分類。 四、參酌金融監督管理委員會之「金融服務業辦理數位身分驗證指引」暨其所附「以金融 Fast-ID 作為信物，並提供金融服務為例，說明數位身分驗證之參與者及作業程序」，增訂第一項第六款金融 Fast-ID 之安全設計。 五、現行第一項第五款之後各款，款次變更。
---	--	---

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，	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。 4、<u>如為設備約定憑證簽章，應符合下列要求：</u> <u>(1)應用範圍限</u>	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	
---	--	--

<u>於確認本條第一項第四款第一目約定實體設備。</u> (2) <u>私鑰應儲存於安全元件內。</u> (3) <u>核發設備約定憑證簽章時，應確認設備為使用者與電子支付機構所約定持有之實體設備，且該約定持有之實體設備應通過第五款第二目或第三目行動電話號碼認證之交易安全設計。</u> (4) <u>應建立異常登入偵測機制，並於設備約定憑證簽章遭疑似竊取或冒用等異常情形發生時，重新核發設備約定憑證簽章。</u> 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	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，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	
--	---	--

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，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	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<u>下列三項之任兩項以上技術</u>： (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)<u>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（</u>	
---	---	--

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<u>採用本款第一目技術，並選擇第二目或第三目任一項技術：</u> <u>（一）約定實體設備：</u> <u>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（如電腦、行動裝置、智慧型穿戴裝置等）。如與使用者約定第二台以上具付款功能之約定實體設備時，應符合下列要求：</u> <u>1、於已約定之實體設備上提出申請，採用第</u>	<u>如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等）。</u> （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<u>確認真人（Liveness Detection）、本人（Biorecognition）</u>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	
---	---	--

<u>一款憑證簽章、第二款晶片金融卡、本款第二目或第三目之任一款安全設計。</u> 2、<u>電子支付機構應控管使用者約定之實體設備數量，同類型之實體設備於同一時間應以約定一台為限。</u> 3、<u>約定之實體設備為智慧型穿戴裝置時，應限制僅得從事實體通路支付交易。</u> (二) 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）。 (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	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	
--	---	--

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	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	
--	--	--

目第2子目 防護機制)。 <u>五、使用行動電話號碼認證，其安全設計依所採用之技術，應分別符合下列要求：</u> <u>(一)門號身分一致性</u> 認證：應以使用者留存於電子支付機構之行動電話號碼，連線至所屬電信業者，確認該門號申辦時所留存之身分證號或統一證號與使用者於電子支付機構留存之證號一致。 <u>(二)裝置門號一致性</u> 認證：應確認使用者留存於電子支付機構之行動電話號碼與裝置上用戶身分模組 (Subscriber Identity Module, SIM) 所對應之行動電話號碼一致，且係透過SIM連線至所屬電信業者，確認該SIM對應行動電話號碼、SIM之有效性、交易訊息確實由該SIM所發送。 <u>(三)SIM 認證：其安全設計除符合裝置門號一致性認證要求外，應確認使用者</u>	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。	
---	---	--

<u>及該行動電話號碼持有人為同一身分證號或統一證號。</u> <u>六、使用金融Fast-ID，其安全設計應符合下列要求：</u> <u>(一) 金融Fast-ID裝置驗證：透過驗證金融機構於同一設備且同一連線階段下完成身分核驗後，確認驗證金融機構所留存之身分證號或統一證號與使用者於電子支付機構留存之證號一致。</u> <u>(二) 金融Fast-ID門號驗證：完成前目驗證時，電子支付機構與驗證金融機構間交換使用者留存之行動電話號碼確認一致性。</u> <u>七、使用視訊會議，其安全設計應符合下列要求：</u> <u>(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。</u> <u>(二) 應依相關規定留存影像或照片，以利後續查證。</u> <u>(三) 若依規定須驗證</u>		
---	--	--

留存證件者應核對確認。 <u>八</u>、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。 <u>九</u>、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七款之任一款安全設計,第二款至第七款安全設計得替代第八款或第九款安全設計。		
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<u>第一項第三款</u>一次性密碼、<u>第五款行動電話號碼認證任一技術</u>或<u>第六款第二目金融Fast-ID門號驗證</u>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	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、<u>SIM認證或電信認證</u>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	一、配合第四條增訂第一項第五款規定,刪除第二項及第三項,及修正第一款、第二款第三目文字。 二、第三款第一目增訂臨櫃審查之應用情境說明文字。 三、增訂第四款規定,明確規範個人使用者從事跨機構間國內外小額匯兌時,加強身分確認程序之相關機制,並為強化確認第二金融支付工具之驗證強度,爰規定使用者所提供之金融工具應包含本人存款帳戶。

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份驗證平臺」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	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份驗證平臺」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；	
--	---	--

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<u>第四條第一項第一款、第二款、第五款第二目或第三目、第六款、第七款或第八款</u>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<u>第四條第一項第一款、第二款、第五款之第二目或第三目、第六款、第七款或第八款</u>之安全設計加強確認。 三、以臨櫃審查、符合電	如有異常之情事，得採用<u>第四條第一款、第二款、第五款或第六款</u>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<u>第四條第一款、第二款、第五款或第六款</u>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	
---	--	--

子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(如總公司、實體直營服務據點)，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<u>第一項第一款</u>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	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	
---	---	--

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	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。 <u>前項第一款SIM認證，其安全設計應確認申請</u>	
--	---	--

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。 四、接受個人使用者從事跨機構間國內外小額匯兌所增加之身分確認程序，應符合下列要求： (一)採確認使用者與行動電話號碼持有人為同一統一編號者，應採用第四條第一項第五款第三目SIM 認證或第六款第二目金融Fast-ID門號驗證。 (二)採確認使用者本人之第二項金融支付工具者，應確認使用者所提供之金融支付工具包括本人存款帳戶。	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。 <u>第一項第一款電信認證</u>，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<u>第一項第一款至第三款之任一款、第四款或第五款之任一項技術或第六款至第九款之任一款</u>安全設計辦理。 前項帳號之安全設	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、配合第四條增訂第一項第五款及第六款規定，第一項酌作文字修正。 二、為利業者遵循及保留實務作業彈性，增訂第二項第一款有關帳號輸入方式之規範。 三、現行第二項各款，款次變更；另增加使用顯性資料作為帳號之安全

計： 一、<u>帳號除得由使用者手動輸入設定外，亦得於驗證約定裝置後，由系統自動帶出，惟應符合訊息隱密性。</u> 二、<u>如使用顯性資料（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）及第四條第一項第九款作為登入方式，應確認使用者登入設備為依第四條第一項第四款第一目所定約定實體設備或另行增設使用者代號以資識別。</u> 三、<u>同一帳號在同一時間內僅能登入一個連線(session)控制之系統。</u> 四、<u>如增設使用者代號，至少應依下列方式辦理：</u> （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。	一、<u>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。</u> 二、<u>同一帳號在同一時間內僅能登入一個連線(session)控制之系統。</u> 三、<u>如增設使用者代號，至少應依下列方式辦理：</u> （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。	控管機制，爰修正第二款規定。
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	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	一、配合第四條增訂第一項第五款行動電話號碼驗證及第六款金融Fast-ID之安全設計，修正第一款第二目有關電子支付帳戶進行線上即時交易時，應用該等交易安全設計之

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<u>第一項第二款</u>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、<u>第八款</u>知識詢問、<u>第九款</u>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<u>第一項第一款</u>第一目訊息加密安全設計；如採用<u>第八款</u>知識詢問安全設計者，	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	相關規定。 二、酌作文字修正。
--	---	-------------------------------

應確保非用 戶本人授 使用之權 於掛失後 需承擔遭 冒損失， 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 四條第一項 第一款第二 目訊息押碼 或第三款訊 息簽章或第 四款兩項以	本人授權使 用之交易於 掛失後無需 承擔冒用之 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 章目訊息簽 章或第四款 兩項以上技 術之安全設 計；	
--	--	--

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<u>第四條第一項第一款金融憑證簽章</u>、第二款晶片金融卡、第三款一次性密碼、第	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	
--	---	--

四款兩項以上技術之任一項技術、<u>第五款第二目裝置門號一致性認證</u>或<u>第三目SIM認證</u>、<u>第六款金融Fast-ID</u>、<u>第八款知識詢問</u>、<u>第九款固定密碼</u>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<u>第一項第一款金融憑證簽章至第九款</u>之任一款安全設計，惟排除門號身分一致性認證。 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	之任一項技術、<u>第六款知識詢問</u>、<u>第七款固定密碼</u>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。	
--	---	--

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<u>第一項第一款</u>金融憑證簽章至第六款之任一款安全設計，惟排除門號身分一致性認證。 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<u>第一項第一款</u>金融憑證簽章至第六款之任一款安全設計，惟排除軟體OTP、簡訊OTP及門號身分一致性認證。 (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	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<u>第一項第一款</u>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	
--	--	--

元以下者，應採用第四條第一項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，應採用第四條第一項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。	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	
---	---	--

息加密安全設計，由儲值卡末端設備確認儲值卡及由儲值卡確認儲值卡末端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<u>第一項</u>第一款第一目增強要求之訊息加密安全設計，由儲值卡末端設備確認儲值卡及由儲值卡確認儲值卡末端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末端設備或電子支付機構之合法性。	末設備確認儲值卡及由儲值卡確認儲值卡末端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末端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末端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	
--	--	--

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<u>第一項第一款</u>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<u>第一項第一款第一目</u>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<u>第一項第一款第一目</u>增強要求之訊息加密安全設計。 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。	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	
---	---	--

過接觸式或非接觸式介面者，應採用第四條<u>第一項第一款</u>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<u>第一項第一款</u>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<u>第一項第一款</u>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<u>第一項第一款</u>硬體金融憑證簽章安全設計。	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扣款指示(包含限定性繳稅費及不特定金額代理收付實質交易之自動交易扣款)，約定時電子支付機構應依第一款不同交易類	
---	---	--

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扣款指示(包含限定性繳稅費及不特定金額代理收付實質交易之自動交易扣款)，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。電子支付機構與特約機構合作時，應符合下列規定： 1、應確保交易資訊(包含但不	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。電子支付機構與特約機構合作時，應符合下列規定： 1、應確保交易資訊(包含但不限於存款帳號、信用卡卡號、交易內容、交易授權及清算等資訊)之隱密性、安全性，及資料傳輸、交換或處理之正確性。 2、確認交易訊息自特約機構與電子支付機構約定之網路位置(IP)或完整網域名稱(FQDN, Fully Qualified Domain Name)發送，並驗證為特	
--	--	--

限於存款帳號、信用卡卡號、交易內容、交易授權及清算等資訊)之隱密性、安全性,及資料傳輸、交換或處理之正確性。 2、確認交易訊息自特約機構與電子支付機構約定之網路位置(IP)或完整網域名稱(FQDN, Fully Qualified Domain Name)發送,並驗證為特約機構與電子支付機構事先約定之認證資訊,以確保交易訊息之來源可靠。 3、應於使用者約定自動交易扣款時,與特約機構針對個別使用者約定去識別化之序號作為發動扣款指示之專屬授權編號,且授權編號不得共用。 4、應使用加密演算法針對交易訊息進行	約機構與電子支付機構事先約定之認證資訊,以確保交易訊息之來源可靠。 3、應於使用者約定自動交易扣款時,與特約機構針對個別使用者約定去識別化之序號作為發動扣款指示之專屬授權編號,且授權編號不得共用。 4、應使用加密演算法針對交易訊息進行押碼、加密運算或數位簽章,以防止交易訊息遭第三者知悉或竄改。 (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	
---	---	--

押碼、加密運算或數位簽章，以防止交易訊息遭第三者知悉或竄改。 (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<u>第四條第一項第一款金融憑證簽章至第六款之任一</u>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<u>第四條第一項第一款第二目</u>訊息押碼或<u>第三目</u>訊息簽章或<u>第四款</u>兩項以上技術之安全設計；如採用<u>第四條第一項第一款第二目</u>訊息押碼或<u>第三目</u>訊息簽章者，應採用具安全認證之晶片型儲值卡或<u>端末安全模組</u>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。	目訊息簽章或<u>第四款</u>兩項以上技術之安全設計；如採用<u>第四條第一款第二目</u>訊息押碼或<u>第三目</u>訊息簽章者，應採用具安全認證之晶片型儲值卡或<u>端末安全模組</u>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。	
第十一條 電子支付平臺之設計原則，應符合下列要求：	第十一條 電子支付平臺之設計原則，應符合下列要求：	一、配合<u>第四條第一項第四款</u>規定，<u>第一款第二目</u>酌作文字修正。

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<u>第一項第四款第二目</u>所定之<u>約定實體設備</u>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	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<u>第二目</u>所定之<u>使用者所持有之實體設備</u>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	二、為防範使用者遭詐騙集團偽冒、盜用情事，爰增訂第一款第九目有關異動行動電話號碼及異動裝置時之安全設計相關規範。 三、為防止詐騙集團透過分享使用者螢幕或截圖方式取得付款碼，增訂第四款第七目第4子目之資安檢測規範及第五款第三目掃碼技術限制，並考量電子支付之付款碼於時效內原即以使用一次為限，故第五款第三目設定付款碼合理使用時效為五分鐘以內，俾兼顧防制詐騙與使用者體驗之便利性。 四、考量實務運作，爰增訂第四款第十五目，有關Deep Link跳轉機制之安全控管措施，以配合現行技術發展程度，管理機構間之傳輸機制及訊息來源辨識、確認訊息傳輸經合法授權，並保障資料傳輸之安全性。 五、為保障使用者個人資料安全，爰增訂第五款第九目有關條碼內容如涉及個人資料或其他機敏資料時，應採加密機制等管理機制，以防止資料遭未授權存取或洩露。
--	--	---

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	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<u>第四條第一項第一款至第七款</u>之任一款安全設計，惟異動行動電話號碼或兩項以上技術，應符合下列要求： <u>1、異動行動電話號碼，應採下列任一方式辦理：</u> (1)<u>採用第四條第一項第一款、第二款、第四款第一目、第五款或第六款之任一款安全設計。</u> (2)<u>確認異動後之行動電話號碼與使用者</u>	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	
---	--	--

於金融機構開立存款帳戶時所留存之行動電話號碼一致，且以透過臨櫃或視訊櫃員機方式開立之存款帳戶、第一類或第二類數位存款帳戶為限。 2、異動兩項以上技術，應採用第四條第一項第一款至第七款之任一安全設計，且採用軟體 OTP 或簡訊 OTP 安全設計者，應加強防護機制（可評估第四條第一項第三款第二目第 2 子目防護機制）。異動約定實體設備為行動電話裝置者，應採用下列任一方式辦理： (1) 採用第四條第一項第一款第四目第四子目設備約定憑證簽章者，	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	
---	--	--

<u>應配合第四條第一項第四款第二目或第三目之任一項技術。</u> (2) <u>採用第四條第一項第四款兩項以上技術者，應以原約定實體設備向使用者確認異動行動電話裝置。</u> (3) <u>採用第四條第一項第五款第二目裝置門號一致性認證或第三目SIM認證。</u> (4) <u>採用第四條第一項第六款金融 Fast-ID。</u> (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	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、	
--	---	--

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	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、由合格實驗室依據行動應用資安聯盟「行動應用APP基本資安檢測基準」辦理並通過檢測。 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描或黑箱測試，並修正中/高風險漏洞。 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	
---	---	--

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)採用第四條第一項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、	OWASP 公布之 Mobile Application Security Checklist L2 項目辦理檢測。 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。如本目第2子目及第3子目因檢測結果與實際應用之解讀存有差異或因故無法修補者，電子支付機構得由資安專責主管進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。 (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、辦理程式碼掃描或黑箱測	
--	---	--

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、由合格實驗室依據行動應用資安聯盟「行動應用APP基本資安檢測基準」辦理並通過檢測。 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描或黑箱測試，並修正中/高風險漏洞。 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	試，並修正中/高風險漏洞，如屬前目第4子目可承擔風險者，不在此限。 2、辦理國內外小額匯兌者，依據OWASP公布之Mobile Top 10項目辦理之檢測，應修正中/高風險漏洞始得上線(或異動)，如因故需緊急上線者，應於一定期限內完成修正，於完成前應有相應之處置作為及控管機制。 (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	
---	---	--

OWASP 公布之 Mobile Application Security Checklist L2 項目辦理檢測。 4、<u>行動應用程式之畫面擷取與螢幕分享，應符合檢測基準有關行動應用程式於非使用者主動進行的畫面擷取與螢幕分享時應主動警示使用者之技術要求，但支付付款條碼畫面應禁止擷取。</u> 5、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。如本目第2子目及第3子目因檢測結果與實際應用之解讀存有差異或因故無法修補者，電子支付機構得由資安專責主管進行評估相關漏洞是	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	
---	--	--

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。 (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、辦理程式碼掃描或黑箱測試，並修正中/高風險漏洞，如屬前目第 4 子目可承擔風險者，不在此限。 2、辦理國內外小額匯兌者，依據 OWASP 公布之 Mobile Top 10 項目辦理之檢測，應修正中/高風險漏洞始得上線(或異動)，如因故需緊急上線者，應於一定期限內完成修正，於完成前應有相應之處置作為及控管機制。 (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	(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。 (十四) 行動應用程式有使用第三方函式庫或元件之需要時，應評估安全風險及妥善管控程序，並應留存	
--	---	--

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护。 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	評估記錄。 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<u>合理使用</u>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	
---	--	--

(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、	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)	
--	---	--

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。 （十四）行動應用程式有使用第三方函式庫或元件之需要時，應評估安全風險及妥善管控程序，並應留存評估記錄。 （十五）採用 <u>Deep Link 跳轉機制時，應確認連結與應用程式間之對應關係，傳遞參數之合法性與完整性，並防止未經授權之存取或冒用。跨應用程式資料傳輸時，如涉及個人資料或其他機敏資料，應符合訊息隱密性及訊息完整性之安全設計。</u> 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	n 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、sameorigin）。 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	
---	--	--

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，<u>應採取適當安全措施(如限制畫面擷取與螢幕分享功能、標示警語等)</u>，防止條碼遭擷取、重製或由第三人冒用；<u>並應設定條碼使用時效於五分鐘以內</u>，且在時效內以使用一次為限，惟辦理大眾交通運輸者除外。 (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	第三方行動裝置應用程式時，電子支付機構須確認(例如採數位簽章方式等)其嵌入第三方行動裝置應用程式之SDK與符合本條第四款規定之行動裝置應用程式所嵌入之SDK相同，以確保該SDK已符合本條第四款規定，惟未辦理個人資料查詢或國內外小額匯兌者，得免除適用第四款第三目至第八目規定。 八、開放應用程式介面(Open API)：如有使用第三方開放應用程式介面之需要時，應進行安全風險評估及妥善管控程序，並應留存評估記錄。	
---	---	--

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。 <u>(九) 條碼內容如涉及個人資料或其他機敏資料者,應採加密機制或其他符合第六條訊息隱密性之安全設計處理,以防止資料遭未授權存取或洩露。</u> 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/jso n 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、 sameorigin)。		
--	--	--

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，電子支付機構須確認(例如採數位簽章方式等)其嵌入第三方行動裝置應用程式之SDK與符合本條第四款規定之行動裝置應用程式所嵌入之SDK相同，以確保該SDK已符合本條第四款規定，惟未辦理個人資料查詢或國內外小額匯兌者，得免除適用第四款第三目至第八目規定。 八、開放應用程式介面(Open API)：如有使用第三方開放應用程式介面之需要時，應進行安全風險評估及妥善管控程序，並應留存評估記錄。		
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，並依最小權限(least privilege)及僅知原則(need-to-know)配置適當之權限。 二、應至少每年定期審查帳號與權限之合理性及異常存取紀錄，人員離職或調職時應盡速移除權限，以	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，並依最小權限(least privilege)及僅知原則(need-to-know)配置適當之權限。 二、應至少每年定期審查帳號與權限之合理性及異常存取紀錄，人員離職或調職時應盡速移除權限，以	配合第四條修正，酌修文字。

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符合下列要求： (一)應和日常維運帳號區隔，且應列冊保管。 (二)應使用特權帳號管理系統，並採取適當之限制存取權限並評估設定之合理性，以降低帳號密碼被洩露的風險；無法由特權帳號管理系統納管之帳號，密碼應採兩人以上分持管理或其他管控措施，以符合作業牽制原則。 (三)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，且定期覆核使用結果。 (四)用於提供網際網路服務之伺服器及AD(網域服務)主機者，應採雙因子認證。 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	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符合下列要求： (一)應和日常維運帳號區隔，且應列冊保管。 (二)應使用特權帳號管理系統，並採取適當之限制存取權限並評估設定之合理性，以降低帳號密碼被洩露的風險；無法由特權帳號管理系統納管之帳號，密碼應採兩人以上分持管理或其他管控措施，以符合作業牽制原則。 (三)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，且定期覆核使用結果。 (四)用於提供網際網路服務之伺服器及AD(網域服務)主機者，應採雙因子認證。 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<u>第一項第九款</u>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。	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，定義最大可容忍中斷時間，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	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，定義最大可容忍中斷時間，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	參考「金融機構資通安全防護基準」第十七條規定，增訂第四款有關電子支付機構應就防範服務中斷之壓力測試結果製作報告及注意異常情形監控等加強控管規定。

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。 四、應就防範服務中斷之<u>壓力測試結果製作報告。如遇尖峰作業、大量活動或例行業務處理量較大等時段，應特別注意各類異常情形之監控並加強檢核系統資源，俾事先提出因應措施。</u>	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。	
第二十七條 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	第二十七條 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	一、考量部分兼營電子支付機構之銀行或中華郵政股份有限公司未提供註冊及開立電子支付帳戶或發行儲值卡，僅利用存款帳戶與境外機構合作或協助其於我國境內從事電子支付機構業務相關行為，而未涉及利用電子支付帳戶或儲值卡實際經營業務，爰增訂第三項規定。 二、現行第三項及第四項，移列為第四項及第五項；修正後第四項，酌作文字修正。

查核報告辦理。 <u>兼營電子支付機構如未提供註冊及開立電子支付帳戶或發行儲值卡，僅利用存款帳戶與境外機構合作或協助其於我國境內從事電子支付機構業務相關行為者，不適用前項規定。</u> 第二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。	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。	
<u>第二十八條 電子支付機構不符合第八條第二項、第十一條第四款第七目第四子目、第十五目、第五款第三目與第九目，有關帳號安全設計、行動應用程式畫面擷取與螢幕分享、採用 Deep Link 跳轉機制及條碼內容如涉及個人資料或其他機敏資料之規定者，應於中華民國一百十五年十二月三十一日前，調整至符合規定。</u> <u>電子支付機構不符合第四條第一項第一款與第四款至第六款、第七</u>		一、<u>本條新增。</u> 二、<u>考量電子支付機構依修正條文第四條、第七條、第八條及第十一條相關新增或變動內容，調整各該安全控管作業等，均需要時間配合進行商業條件議定、簽約、調整或建置系統、評估人力配置及相關作業規章，爰依據所需合理時間，分別給予緩衝期至一百十五年十二月三十一日或一百十六年六月三十日前調整完成，俾利會員辦理。</u>

<u>條第一款與第二款及第十一條第一款第九目，有關設備約定憑證簽章、使用兩項以上技術、使用行動電話號碼認證、使用金融Fast-ID、確認行動電話號碼、確認金融支付工具、異動行動電話號碼與兩項以上技術之規定者，除經主管機關核准外，應於中華民國一百十六年六月三十日前，調整至符合規定。</u>		
第二十九條 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。	第二十八條 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。	條次變更。