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條文修正總說明

按「電子支付機構資訊系統標準及安全控管作業基準辦法」（以下簡稱本辦法）係於一百零四年四月二十七日訂定發布，並自一百零四年五月三日施行。茲考量約定連結存款帳戶付款之便利性及行動支付趨勢下優化使用者體驗，爰修正本辦法有關約定連結存款帳戶付款機制、固定密碼安全設計、交易安全設計、連線中斷機制及支付指示再確認等相關規定，修正重點如下：

一、 增加約定連結存款帳戶付款機制作業機制類型：為使約定連結存款帳戶付款之作業機制具多元性，除原有直接向開戶金融機構提出扣款指示之「直接連結機制」外，增加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，間接向開戶金融機構提出扣款指示之「間接連結機制」。（修正條文第三條）

二、 簡化固定密碼安全設計：為便利使用者登入電子支付平臺，簡化密碼採取英數字混合使用之要求，並放寬變更後之密碼不得與變更前一次密碼相同。（修正條文第五條）

三、 增加交易安全設計之態樣：考量行動支付發展趨勢下，電子支付機構優化使用者體驗之需求，兼顧交易安全性及支付便利性，調整交易安全設計之規定，增加圖形鎖或手勢之安全設計方式，且容許使用者以與電子支付機構所約定持有之設備進行交易，並以C類交易安全設計作為登入電子支付平臺之身分確認方式，得直接進行A類、B類及C類交易。（修正條文第七條）

四、 放寬連線中斷機制及支付指示再確認要求：考量行動支付發展趨勢下，電子支付機構優化使用者體驗之需求，兼顧交易安全性及支付便利性，對於使用者以與電子支付機構所約定持有之設備進行交易，得延長連線中斷之時間；另考量電子支付機構於實體通路提供支付服務之情境，與使用現金、信用卡、電子票證等其他支付工具相同，交易雙方可面對面確認交易條件及支付指示內容，放寬得不適用支付指示再確認之規定。（修正條文第十條）

五、 調整約定連結存款帳戶付款機制之設計原則要求：配合增加「間接

連結機制」之作業類型，調整申請方式、約定連結程序、交易程序等相關規定，並增列風險控管、終止約定連結申請及兼營電子支付機構簡化規定。（新增條文第十條之一）

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條文修正條文對照表

修正條文	現行條文	說明
第三條　本辦法用詞定義如下： 一、電子支付機構業務：指本條例第三條第一項各款業務。 二、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。 三、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。 四、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	第三條　本辦法用詞定義如下： 一、電子支付機構業務：指本條例第三條第一項各款業務。 二、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。 三、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。 四、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	電子支付機構辦理連結存款帳戶付款服務時，除得直接與開戶金融機構連結(即直接連結機制)外，亦得透過金融資訊服務事業或票據交換所，間接與開戶金融機構連結(即間接連結機制)，為配合直接連結機制及間接連結機制之相關規定，第十三款原「金融機構」文字修正為「開戶金融機構」，並明定直接連結機制及間接連結機制之定義。

過網際網路服務業者進行訊息傳輸。	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。	（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。	
五、訊息防護措施區分如下：	五、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。	（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。	（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。	（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。	（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	（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。 六、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	送或接收訊息行為。 六、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)。	下簡稱 SHA)。	
七、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。	七、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。	
八、一次性密碼（One Time Password；以下簡稱 OTP)：指運用動態密碼產生器、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。	八、一次性密碼（One Time Password；以下簡稱 OTP)：指運用動態密碼產生器、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。	
九、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設備。	九、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設備。	
十、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、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。	
十一、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。	十一、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。	
十二、實體通路支付服務（Online To	十二、實體通路支付服務（Online To	

Offline，020）：指電子支付機構就電子支付機構業務，利用行動裝置或其他可攜式設備於實體通路提供服務。	Offline，020）：指電子支付機構就電子支付機構業務，利用行動裝置或其他可攜式設備於實體通路提供服務。	
十三、約定連結存款帳戶付款：指電子支付機構辦理代理收付實質交易款項業務，依使用者與開戶金融機構間之約定，向開戶金融機構提出扣款指示，連結該使用者存款帳戶進行轉帳，由電子支付機構收取代理收付款項，並於該使用者電子支付帳戶記錄代理收付款項金額及移轉情形之服務，作業機制如下： (一)直接連結機制：指電子支付機構直接向開戶金融機構提出扣款指示，連結使用者存款帳戶進行轉帳之機制。 (二)間接連結機制：指電子支付機構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，間接向開戶金融機構提出扣款指示，連結使用者存	十三、約定連結存款帳戶付款：指電子支付機構辦理代理收付實質交易款項業務，依使用者與金融機構間之約定，向金融機構提出指示，連結該使用者存款帳戶進行轉帳，由電子支付機構收取代理收付款項，並於該使用者電子支付帳戶記錄代理收付款項金額及移轉情形之服務。	

款帳戶進行轉帳之機制。		
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，得以帳號及固定密碼登入。 前項帳號及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、密碼不應訂為相同的英數字、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，電子支付機構應	第五條　電子支付帳戶使用者登入電子支付平臺時應進行身分確認，得以帳號及固定密碼登入。 前項帳號及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、密碼不應訂為相同的英數字、連續英文字或連號數字，預設密碼不在此限。 五、密碼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二次密碼相同。 八、密碼超過一年未變更，電子支付機構應做妥善處理。	一、第一項酌作文字修正。 二、考量使用者利用可攜式設備(例如行動電話或平板電腦等)以固定密碼登入電子支付平臺時，切換英數字元不便，爰修正第二項第五款，簡化固定密碼安全設計，改為建議採取英數字混合使用之方式作為固定密碼。 三、為避免使用者須記憶多組密碼之問題，增進使用者登入之便利性，且第二項其餘各款有關固定密碼之安全設計應可保護使用者電子支付帳戶之安全性，爰修正第二項第七款，放寬變更後之密碼不得與變更前一次密碼相同。

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。	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。 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	第七條　電子支付機構執行前條所列交易應進行身分確認，各類交易安全設計並應符合下列要求： 一、A 類交易安全設計：指採用固定密碼之安全設計，其安全設計應符合第五條第二項之規定。 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	一、本條第一項序文係針對第六條之交易安全設計，規定各類型交易應符合之具體方式，為與第六條採一致性文字，並避免與第五條身分確認程序之安全設計混淆，爰酌作文字修正。 二、鑒於實務上交易安全設計方式之多樣化，爰修正第一項第一款規定，除固定密碼外，增訂A類交易得採用圖形鎖或手勢之安全設計。 三、配合第一項第一款規定之修正，同時修正第一項第三款第三目之１之規定，除固定密碼外，增訂用圖形鎖或手勢之安全設計。該等安全設計應限於使用者與電子支付機構所約定之資訊，且無第三人知悉，而非使用者在裝備上自行設定而未與電子支付機構約定之固定密碼、圖形鎖或手勢。 四、修正第一項第三款第三目之２之文字，將「實體」二字移至句首，以明確使用者所持有的設備應以「實體設備」為

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、使用者所持有的實體設備(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、使用者所擁有的生物特徵(如指紋、臉部、虹	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(如登入密碼)。 2、使用者所持有的設備(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實體設備。 3、 使用者所擁有的生物特徵(如指紋、臉部、虹膜、聲音、掌	限。 五、為提升使用者利用電子支付平臺之便利性，並兼顧其交易安全性，如使用者所使用之設備(例如行動電話或平板電腦等可攜式設備)係使用者與電子支付機構約定持有之設備，並配合以第一項第三款第三目之1(即使用者採用其與電子支付機構所約定之資訊)或之3(使用者所擁有之生物特徵)所規定之任一項安全設計作為登入電子支付平臺之身分確認機制者，使用者可直接進行 A 類、B 類及 C 類交易，爰增訂第二項。 六、原第二項遞移為第三項，同時修正第八款規定，憑證私鑰儲存容許採用較高等級之安全設計，兼顧實務作業情形及電子支付機構資訊風險控管。

膜、聲音、掌紋、靜脈、簽名等)：電子支付機構應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，必要時應增加多項不同種類生物特徵。 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。 使用者以前項第三款第三目之 2 所定使用者所持有的實體設備進行交易，且電子支付機構採用前項第三款第三目之 1 或之 3 所定安全設計作為使用者登入電子支付平臺之身分確認方式，得直接進行 A 類、B 類及 C 類交易。 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	紋、靜脈、簽名等)：電子支付機構應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，必要時應增加多項不同種類生物特徵。 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。 前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	

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 140-1 Level 2(含)以上或其他相同安全強度之認證等晶片硬	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 140-1 Level 2 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。	

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所定使用者所持有的實體設備進行交易，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	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或採取其他保護措施。 (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。	一、為確保使用者之電子支付帳戶安全及資訊安全，第一款第二目原規定電子支付平臺之網際網路設計，應包括網頁逾時中斷機制，時間以十分鐘為限，以降低因使用者閒置時間過長所造成之未經授權使用及資訊外洩等風險。惟使用者與電子支付機構約定持有之設備如智慧型手機或平板電腦等行動裝置，多為隨身設備，可適度降低因使用者閒置時間過長所造成之未經授權使用及資訊外洩等風險，故增訂第一款第二目但書規定，明定於該等情形下，使用者介面逾時中斷機制之時限得由十分鐘延長為三十分鐘。 二、現行第五款有關約定連結存款帳戶付款設計要求之規定移列並新增為第十條之一，故原第六款則遞移為第五款。

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：	(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。	三、考量使用者於實體通路進行交易時，係當場為支付指示，已知悉支付指示之內容，故無再確認之必要，爰於第五款第一目增訂但書規定，明文規定實體通路支付服務不適用再確認之規定。

(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)應針對所需最小權限進行存取控制。 (二)應於官網上提供行	(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)應針對所需最小權限進行存取控制。 (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)於安裝或首次啟動應用程式時，得提示使用者於行動裝置上安裝防毒軟體。 (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。 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。	動裝置疑似遭破解，應提示使用者注意風險。 (四)於安裝或首次啟動應用程式時，得提示使用者於行動裝置上安裝防毒軟體。 (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。 五、約定連結存款帳戶付款設計要求： (一)電子支付機構應向金融機構申請金融憑證，並向金融機構約定為執行本款作業之專屬憑證。應用時須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。 (二)約定連結程序：使用者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，使用者得以臨櫃、網路銀行或透	

(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。	過電子支付機構依前目所定方式等機制，向金融機構提出約定連結申請，並提供該使用者之金融機構存款帳號及其電子支付機構之電子支付帳戶帳號，經金融機構確認使用者身分後完成設定。不同身分確認機制，依據其適用之風險類別，應限制不同交易額度。 (三)交易程序：電子支付機構透過本款第一目所定方式向金融機構提出代使用者辦理扣款指示，經金融機構確認無誤後，撥付款項至電子支付帳戶。 (四)私鑰保護：該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 140-1 Level 2 或其他相同安全強度之硬體安全模組內並限制匯出功能。 (五)存取控制：應建立管控機制，限制非授權人員或程式存	

	取私鑰及本款作業之相關程式。 (六)資金移轉：金融機構將資金移轉至使用者之電子支付帳戶時，考量帳戶管理機構不同，視為跨行交易。 (七)即時通知機制：電子支付機構應要求金融機構建立即時通知機制，由金融機構於進行資金移轉後，立即向使用者通知。 六、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。 (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。	
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		一、本條新增。 二、本條由現行第十條第五款條文移列，並新增及修正相關規定，以明定約定連結存款帳戶付款

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。		設計應符合之原則。 三、配合本辦法第三條第十三款有關直接連結機制及間接連結機制之定義，爰增訂第一款，明定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。 四、第二款由現行第十條第五款第一目條文移列並修正，規定電子支付機構應依其連結之方式為直接連結機制或間接連結機制，分別向開戶金融機構或專用存款帳戶銀行申請金融憑證，作為執行本條作業之專屬憑證。 五、第三款係規定約定連結存款帳戶之程序。 (一)第一目由現行第十條第五款第二目前段條文移列並修正，規定開戶金融機構得受理使用者親自依臨櫃、電子銀行(例如以晶片金融卡或憑證等方式進行身分確認)方式申請約定連結存款帳戶服務，或透過電子支付機構依第二款規定之方式向開戶金融機構提出申請。 (二)第三款第二目由現行第十條第五款第二目中段條文移列並修正，規定使用者提出連結申請時，應提供使用者本身

(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		之相關資訊(如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)予開戶金融機構，經開戶金融機構確認使用者身分後，完成約定連結存款帳戶之設定。 (三)增訂第三款第三目規定，明定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任一項交易面介面安全設計之方式進行使用者身分確認，並應依所採取之不同身分確認方式以及該等方式之風險類別，限制使用者之轉帳交易額度。 (四)增訂第三款第四目規定，為符合電子支付機構提供約定連結存款帳戶付款服務，俾利使用者進行小額支付及款項移轉之本旨，且為確保使用者進行電子支付交易之安全性，爰增訂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進行交易時，每月累計移轉金額最高不得超過新臺幣三十萬元。 六、第四款由現行第十條第五款第三目條文移列並修正，規定直接連結機制及間接連結機制下之

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 140-1 Level 2(含)以上或其他相同安全強度之硬體安全模組內並限制匯出功能。 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，		帳戶扣款交易程序。 七、第五款由現行第十條第五款第四目條文移列，並增訂憑證私鑰儲存容許採用較高等級之安全設計，兼顧實務作業情形及電子支付機構資訊風險控管。 八、第六款由現行第十條第五款第五目條文移列。 九、並酌作文字修正。 十、第七款由現行第十條第五款第七目條文移列，規定電子支付機構應要求開戶金融機構建立通知機制，於完成轉帳交易後向使用者通知。且為兼顧開戶金融機構進行通知時之實務作法，刪除本款「即時」及「立即」之規定。 十一、為避免電子支付機構發生系統故障異常、人為疏失或遭受惡意攻擊、或其他內部控制之重大缺失，導致向專用存款帳戶銀行或開戶金融機構發送大量異常扣款指示，爰增訂第八款之風險控管機制，規定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。 十二、增訂第九款，明定使用者終止連結申請之設計要求，並於第一

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		目規定使用者得以原先申請約定連結之方式或其他與電子支付機構或開戶金融機構約定之方式申請終止連結。另如使用者未透過電子支付機構而直接向開戶金融機構申請撤銷連結時，為使開戶金融機構與電子支付機構均能得知使用者撤銷連結存款帳戶之資訊，於第九款第二目規定開戶金融機構對電子支付機構之通知義務。 十三、鑒於兼營電子支付業務之電子支付機構(例如銀行或中華郵政股份有限公司)及開戶金融機構可能為同一法律主體，且未準用本條例有關專用存款帳戶之規定，本條第二款至第四款所規定之金融憑證申請程序、約定連結程序及交易程序，可予適度簡化，爰增訂第十款之簡化規定。

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，自發布日施行。	第二十四條　本辦法自中華民國一百零四年五月三日施行。	增訂第二項規定，明定本次修正條文自發布日施行。