金融機構辦理電子銀行業務安全控管作業基準

本會 99 年 7 月 29 日第 9 屆第 28 次理監事聯席會議討論通過
金管會 99 年 8 月 31 日金管銀國字第 09900311870 號函洽悉
本會 102 年 3 月 28 日第 10 屆第 26 次理監事聯席會議討論通過
金管會 102 年 6 月 3 日金管銀國字第 10200120550 號函洽悉
本會 103 年 11 月 27 日第 11 屆第 13 次理監事聯席會議討論通過
金管會 104 年 1 月 13 日金管銀國字第 10300348710 號函洽悉
本會 105 年 1 月 28 日第 11 屆第 25 次理監事聯席會議討論通過
金管會 105 年 3 月 18 日金管銀國字第 10500036310 號函洽悉
本會 105 年 6 月 30 日第 11 屆第 29 次理監事聯席會議討論通過
金管會 105 年 8 月 16 日金管銀國字第 105 00193690 號函洽悉
本會 105 年 12 月 22 日第 12 屆第 3 次理監事聯席會議討論通過
本會 106 年 2 月 23 日第 12 屆第 5 次理監事聯席會議討論通過
金管會 106 年 5 月 11 日金管銀國字第 10600092510 號函洽悉

第一條　中華民國銀行商業同業公會全國聯合會(以下簡稱本會)為確保金融機構辦理電子銀行業務具有一致性基本準則之安全控管作業，特訂定本基準。

第二條　本作業基準用詞定義如下：

一、電子銀行(Electronic Banking)業務：係指在金融機構與客戶(自然人及法人)間，透過各種電子設備及通訊設備，客戶無須親赴金融機構櫃台，即可直接取得金融機構所提供之各項金融服務。

二、存款帳戶:係指金融機構受理客戶臨櫃申請所開立之存款帳戶及以網路方式所開立之數位存款帳戶。

三、概括約定繳稅費：係指客戶透過電子銀行、授權事業單位或授權扣款金融機構發動交易指示,直接由其客戶事先約定之轉出帳戶扣款至政府機關或事業單位之指定帳戶，繳納其各類稅費。

四、檔案傳輸協定(File Transfer Protocol；以下簡稱 FTP)：係指網路上進行檔案傳輸之標準協議。

五、行動裝置：係指包含但不限於智慧型手機、平板電腦等具通訊及連網功能之設備。

六、行動應用程式(mobile application；以下簡稱行動 APP)：係指安裝於行動裝置上之應用程式。

七、銷售端末設備(Point Of Sale；以下簡稱 POS)：係指一設備可讀取商品資訊、連結付款機制、記錄商品銷售行為並將資料傳送至後台進行帳務處理。

八、應用程式與應用程式間資料傳輸(Application to Application；以下簡稱 AP2AP)：係指金融機構與客戶端事先約定應用系統相互傳輸通訊與規格,以達到自動化資訊交換，並執行各項查詢或交易行為。

九、雙音多頻訊號(Dual-Tone Multi-Frequency；簡稱 DTMF)：係指將電話撥號按鍵之每一按鍵設定成一組高頻與低頻兩個聲音，透過按鍵傳送訊息。

十、常用密碼學演算法如下：

（一）對稱性加解密系統：指採用資料加密標準(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)等運算進行資料加密。

（二）非對稱性加解密系統：指採用 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)等運算進行資料加密。

（三）訊息鑑別系統：指採用訊息鑑別碼(Message Authentication Code；以下簡稱 MAC；如 DAA、HMAC)、雜湊函式(Hash Function；如 SHA256)等運算，將不定長度資料產生固定長度之資料進行比對。

十一、 憑證機構(Certification Authority；以下簡稱 CA)：係指居公正客觀地位，查驗憑證申請人身分資料正確性及其與待驗證公開金鑰間之關連性，並據以簽發公開金鑰憑證之單位。

十二、 限定性繳款：係指客戶透過電子銀行、授權事業單位或授權扣款金融機構發動交易指示，直接由其客戶之轉出帳戶扣款至金融機構或事業單位之指定帳戶，繳納其費用或款項。

十三、 插拔卡：為一種人工確認方式。可於交易確認時，用以確認由人工進行交易，無法以惡意程式模擬。此設計應要防止避免系統組態或服務之改變而誤判。

十四、 特殊按鍵：為一種人工確認方式。可於交易確認時，用以確認由人工進行交易，無法以惡意程式模擬。此設計應要防止可由程式模擬特殊按鍵。

十五、 阻斷服務(Denial of Service；以下簡稱 DoS)：係指惡意程式發動阻斷攻擊，導致服務中斷；當操控兩台以上電腦針對特定目標進行阻斷服務攻擊者，稱為分散式阻斷服務(Distributed DoS；以下簡稱 DDoS)。

十六、 空中傳輸(Over The Air；以下簡稱 OTA)：透過無線傳輸方式，進行軟體、參數、相關資料之下載或更新。

十七、 敏感資料：係指如重要參數、晶片金融卡基碼、憑證私鑰、個人資料及製卡個人化資料等。

十八、 白箱加密法(White-box Cryptography；WBC)：係指將應用程式中加密運算之金鑰資訊得以充分被隱藏，降低演算法遭攻擊之機率。

十九、 程式碼混淆技術：係指將程式碼轉換為相同功能，且難於閱讀與理解之技術。此技術可運用於程式原始碼或編譯後之位元組碼(bytecode)，藉此以提升程式被逆向工程反組譯程式碼後之理解難度。

二十、 安全元件(Secure Element；以下簡稱 SE)：提供各種服務應用所需之安全運算及確保相關資料之隱密性，可用來存載金融卡、信用卡、儲值帳戶或金融機構帳戶等支付工具應用程式與相關資料；此媒介可為不同之形式，如 USIM、外接裝置、行動裝置內建晶片及 MicroSD 等。

二十一、近距離無線通訊 (Near Field Communication；以下簡稱 NFC)：是一種短距離之高頻無線通訊技術，允許電子裝置間進行非接觸式端點對端點資料傳輸。

二十二、網路 ATM(Electronic ATM；以下簡稱 eATM)：於網際網路上透過卡片讀卡機，以軟體程式存取 PC/SC 讀卡機，提供除現金提存外之實體 ATM 功能。

第三條　電子銀行業務之訊息傳輸途徑

客戶端利用電子設備及通訊設備與金融機構進行訊息傳輸時所使用之網路型態，區分如下：

一、專屬網路：指透過撥接(Dial-Up)、專線(Lease-Line)或虛擬私有網路(Virtual Private Network)等方式進行訊息傳輸。

二、網際網路(Internet)：指世界各地不同之網路，以 TCP/IP 通訊協定互相連線，提供連線者互通信息，互傳資料與共享各類資源。

三、加值網路(Value Added Network)：指提供網路附加價值之服務，如自動錯誤偵測及修復、通訊協定轉換及訊息儲存及後送等；惟實際運用時應依個別加值網路服務業者與金融機構間傳輸途徑之不同，分別納入前述專屬網路或網際網路傳輸途徑予以規範。

四、行動網路：指透過無線網路服務(如 4G、WiFi)進行訊息傳輸。惟實際運用時應依個別服務業者與金融機構間傳輸途徑之不同，分別納入前述專屬網路或網際網路傳輸途徑予以規範。

五、公眾交換電話網路(Public Switched Telephone Network；以下簡稱 PSTN)：指透過電信服務業者(Telecom)提供之傳輸設備與線纜，將聲波訊息經由各區域間佈建之交換機房(telecom room)或基地台(base station)，傳送至金融機構之電信交換機進行訊息傳輸。

第四條　電子銀行業務之交易類別及風險

客戶端利用電子設備及通訊設備以連線方式發送訊息至金融機構進行交易指示之交易類別，並依據其執行結果對客戶權益之影響區分風險之高低，區分如下：

一、電子轉帳及交易指示類

係指該交易指示直接涉及資金轉移或直接影響客戶權益者。

(一)服務項目

1、電子交易、轉帳授權、帳務通知　服務項目舉例如下：

存提款、轉帳、匯兌、匯款、消費、投資、基金下單、債票券下單、款項繳納、授信、付款指示等交易。

2、申請指示　服務項目舉例如下：

外匯業務：開發信用狀申請及修改信用狀申請。 存款業務：新戶得申辦(1)數位存款帳戶、(2)同意金融機構查詢聯徵中心信用資料。 已開立存款帳戶者得申辦(1)結清銷戶、(2)約定轉入帳號、(3)受理客戶傳真指示扣款無須再取得客戶扣款指示正本、(4)金融卡。 授信業務：已開立存款帳戶或既有貸款戶或既有信用卡戶得申辦(1)無涉保證人之個人貸款，惟房貸及車貸限於原抵押權擔保範圍內之增貸、(2)同意金融機構查詢聯徵中心信用資料。 既有貸款戶得申辦授信條件變更。 新戶但為他行既有非數位存款帳戶、貸款或信用卡客戶得申辦同意金融機構查詢聯徵中心信用資料。

信用卡業務：新戶得申辦(1)信用卡、(2)同意金融機構查詢聯徵中心信用資料。 已開立存款帳戶者或既有信用卡戶或既有貸款戶得申辦(1)信用卡、(2)同意金融機構查詢聯徵中心信用資料。 既有信用卡戶得申辦(1)長期使用循環信用持卡人轉換機制、(2)同意信用卡分期產品約款。 財富管理業務：已開立存款帳戶者得申辦(1)信託開戶、(2)認識客戶作業(KYC)、(3)客戶風險承受度測驗、(4)同意信託業務之推介或終止推介。 共同行銷業務：同意共同行銷。

(二)高風險及低風險性之交易

依據其交易指示執行結果對客戶權益影響之不同，可再行區分為高風險性之交易及低風險性之交易。

交易風險類別	說明
高風險	係指該訊息執行結果，對客戶權益有重大影響之各類電子轉帳及交易指示。
低風險	係指該訊息執行結果對客戶權益無重大影響之各類電子轉帳及交易指示，內容包括下列各項： １、辦理上述申請指示類之服務。 ２、辦理 ATM 存提款之服務。 ３、依法令規定應為照會、認識客戶作業。 ４、辦理約定轉入帳戶之轉帳。 ５、辦理客戶直接向金融機構或間接透過金融資訊服務事業、票據交換所等平台，進行概括約定繳稅費及限定性繳款之扣款約定及扣款服務。 ６、 設定約定轉入帳戶，惟設定非同一統一編號帳戶者須先臨櫃申請後才能透過線上新增；其交易限額同１０之（２)要求，若配合採用各種嚴密之技術防護措施，提供客戶確認交易內容並能 防止或偵測交易內容被竄改，其限額可由個別金融機構 視其風險承擔之能力斟酌予以適當提高。 ７、 同一統一編號帳戶間轉帳。 ８、 貸款撥款至同一統一編號帳戶或學校之就學貸款指定帳戶。 ９、 客戶非直接獲取金融機構之服務且需其人工確認客戶身分與指示內容之申請指示類。 １０、非約定轉入帳戶 （１)ATM、POS 等之低風險性交易，其限額應符合

	現行 ATM 作業及 POS 作業相關規定。 （２）網際網路之低風險性交易，以每一帳戶每筆不超過等值新臺幣五萬元、每天累積不超過等值新臺幣十萬元、每月累積不超過等值新臺幣二十萬元為限。 （３）透過網站、行動 APP、電子郵件、傳真、FTP 或 AP2AP 等方式傳送且未經金融機構人工確認客戶身分與指示內容者，其交易限額同（２）要求。 （４）配合採用各種嚴密之技術防護措施(如簡訊簡碼回傳)，提供客戶確認交易內容並能防止身分確認資料與交易內容被竄改者，其非約定轉入帳戶之轉帳限額，可由個別金融機構視其風險承擔之能力斟酌予以適當提高，最高不超過當日累計等值新臺幣二佰萬元為限;若經客戶事先申請且由金融機構人工與客戶確認其指定人員之身分與指示內容者(如電話照會)，其交易限額不在此限。 １１、個人資料異動。

二、非電子轉帳及交易指示類

係指與資金轉移無關或不直接影響客戶權益之服務項目，其服務項目舉例如下：

非電子轉帳及交易指示類	服務項目
查詢	１、 帳務類查詢： 存放款餘額查詢、交易明細查詢、額度查詢、歸戶查詢、託收票據查詢、匯入匯款查詢、信用狀查詢等交易。 ２、 非帳務類查詢： 匯率查詢、利率查詢、共同基金查詢、金融法規查詢、股市行情查詢、投資理財資訊查詢、業務簡介查詢等交易。 ３、 個人資料查詢。
通知	入扣帳通知、存款不足通知、存放款到期通知、放款繳息通知、託收票據狀況通知、消費通知等交易。

第五條　　交易面之安全需求

一、交易面之安全需求依安全防護措施之不同分述如下：

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

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

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

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

(五)無法否認傳送訊息(Non-repudiation of sender)：係指傳送方無法否認其傳送訊息行為。

(六)無法否認接收訊息(Non-repudiation of receiver)：係指接收方無法否認其接收訊息行為。

二、各訊息傳輸途徑所應達到之安全防護措施如下：

訊息傳輸途徑	專屬網路			網際網路及公眾交換電話網路		
交易類別 / 防護措施	電子轉帳及交易指示類		非電子轉帳及交易指示類	電子轉帳及交易指示類		非電子轉帳及交易指示類
	高風險	低風險		高風險	低風險	
訊息隱密性	非必要	非必要	非必要	必要	網際網路：必要、公眾交換電話網路：備註二	網際網路：必要、公眾交換電話網路：備註一
訊息完整性	必要	必要	非必要	必要	網際網路：必要、公眾交換電話網路：備註三	非必要
訊息來源辨識	必要	非必要	非必要	必要	非必要	非必要
訊息不可重複性	必要	必要	非必要	必要	必要	非必要
無法否認傳送訊息	必要	非必要	非必要	必要	非必要	非必要
無法否認接受訊息	必要	非必要	非必要	必要	非必要	非必要

【表格說明】

必要(Mandatory)：係指金融機構必須具備該項防護措施。

非必要(Conditional)：係指金融機構得視情況自行決定是否需要具備該項防護措施。

備註一：透過網際網路傳送非電子轉帳及交易指示類之足以識別該個人之資料訊息時，應具備訊息隱密性之防護措施；透過公眾交換電話網路(如語音、傳真)時，因此網路之特性無須符合訊息隱密性之安全需求。

備註二：透過公眾交換電話網路(如語音、傳真)時，
因此網路之特性無須符合訊息隱密性之安全需求，惟若以雙音多頻訊號傳送固定密碼者，應以干擾訊號或其他機制防止該頻率遭側錄。

備註三：透過公眾交換電話網路(如語音、傳真)時，因此網路之特性不易透過各項演算法驗證訊息完整性，應採用其他方式告知使用者並進行交易內容確認(如雙向簡訊)。

第六條　交易面之訊息傳輸安全需求

防護措施	安全設計之基本原則/基本配備
訊息隱密性	1、訊息處理： 可採對稱性加解密系統或非對稱性加解密系統。 (1)對稱性加解密系統其應至少採用金鑰有效長度為112位元以上之三重資料加密演算法(Triple DES)或金鑰有效長度為128位元以上之進階資料加密演算法(AES)或其他安全強度相同之演算法。 (2)非對稱性加解密系統其應至少採用金鑰長度為2048位元以上之RSA演算法或金鑰長度為256位元以上之橢圓曲線演算法(Elliptic curve cryptography，ECC)或其他安全強度相同之演算法。 (3)須全文加密。 2、金鑰交換： 採對稱性加解密系統時，其金鑰交換可分訊息加密金鑰與金鑰保護金鑰之交換。 (1)訊息加密金鑰交換：訊息加密金鑰乃用來對訊息做加密，不應以明碼或人工方式直接交換此金鑰，應使用對稱性加解密系統(如DES)或非對稱性加解密性統(如RSA)或依協商訊息加密金鑰(如採Diffie-Hellman Key Agreement)交換之。安全強度同前述「訊息隱密性」有關訊息處理(1)及(2)之規定。 (2)金鑰保護金鑰交換：金鑰保護金鑰乃用來對訊息加密金鑰做加密(如採DES、RSA)或依此協商訊息加密金鑰(如採

	Diffie-Hellman Key Agreement)。 （2.1）對稱性金鑰保護金鑰之交換應採離線交換(如以碼單或寫入具安全防護之媒體)，以降低該金鑰洩漏之風險；當採碼單交換時,應將金鑰拆分成兩個以上,利用秘密分持(如分 A、B 碼)進行交換；當採媒體交換時，應將媒體及保護機制(如密碼)分持進行交換。 （2.2）非對稱性金鑰保護金鑰之交換，其公開金鑰可透過憑證或其他通道交換，惟透過非信賴之通道交換應輔以其他可信賴之驗證機制，以確保所取得公開金鑰之正確性。 3、金鑰生命週期： 金鑰應於使用一段期間後更換之，以確保其安全性。
訊息完整性	1、訊息處理： 可採訊息鑑別系統、對稱性加解密系統或非對稱性加解密系統。 （1）訊息鑑別系統應採用 160 位元以上之 SHA 演算法、採用 64 位元以上之 DAA 運算或其他安全強度相同之演算法。 （2）對稱性加解密系統同前述「訊息隱密性」有關訊息處理之對稱性加解密系統規範。 （3）非對稱性加解密系統同前述「訊息隱密性」有關訊息處理之非對稱性加解密系統規範。 2、金鑰交換： 同前述「訊息隱密性」有關金鑰交換之規範。 3、金鑰生命週期： 同前述「訊息隱密性」有關金鑰生命週期之規範。
訊息來源辨識	1、訊息處理： 同前述「訊息完整性」有關訊息處理之規範。 2、金鑰交換： 同前述「訊息隱密性」有關金鑰交換之規範。 3、金鑰生命週期： 同前述「訊息隱密性」有關金鑰生命週期之規範。
訊息不可重複性	如使用序號、一次性亂數、時間戳記等機制。
無法否認 傳送訊息	1、訊息處理： 須針對交易訊息使用數位簽章(Digital Signature)或採用其他訊息簽章認證等機制，同前述「訊息隱密性」有關訊息處理之非對稱性加解密系統規範。 2、公開金鑰交換： 訊息簽章使用對應之公開金鑰須透過憑證交換，且此憑證須由憑證機構所核發。 3、金鑰生命週期：

	同前述「訊息隱密性」有關金鑰生命週期之規範。
無法否認接受訊息	同前述「無法否認傳送訊息」規範。

第七條　交易面之介面安全設計

係指客戶發送訊息時，其介面及訊息之通訊傳輸應達到之安全防護措施之設計方法，亦即金融機構於系統開發設計時，應加以考量或應具備之基本原則及項目。應用於高風險交易之安全設計可應用於低風險交易；應用於低風險交易之安全設計可應用於身分確認(如簽入作業)。

各項介面安全設計，區分如下：

一、使用憑證簽章得應用於高風險交易，其安全設計應簽署適當內容並確認該憑證之合法性、正確性、有效性、保證等級及用途限制。

二、使用晶片金融卡僅限應用於低風險交易，其安全設計應符合晶片金融卡交易驗證碼之安全設計。

三、使用一次性密碼（One Time Password，OTP）僅限應用於低風險交易，其安全設計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。

四、使用「兩項以上技術」僅限應用於低風險交易，其安全設計應具有下列三項之任兩項以上技術：

（一）客戶與金融機構所約定之資訊，且無第三人知悉（如密碼、圖形鎖、手勢等)。

（二）客戶所持有之設備，金融機構應確認該設備為客戶與金融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）客戶提供給金融機構其所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)，金融機構應直接或間接驗證該生物特徵。間接驗證係指由客戶端設備(如行動裝置)驗證或委由第三方驗證，金融機構僅讀取驗證結果，必要時應增加驗證來源辨識。

五、使用視訊會議僅限應用於低風險交易，其安全設計應查驗本人並核對證件照片。

六、使用知識詢問僅限應用於低風險交易且應用範圍應符合第九條第六款之要求；其安全設計應利用客戶之其他資訊(如保單資訊、信用卡申請資料或繳款方式等)，以利有效識別客戶身分。

七、使用固定密碼僅限應用於低風險交易且應用範圍應符合第九條第六款之要求；

（一）透過網際網路傳輸途徑並採用戶代號及固定密碼進行唯一驗證之簽入介面，其安全設計應具備之安全設計原則如下：

１、用戶代號之安全設計：

（１） 不得使用客戶之顯性資料(如統一編號、身分證號、手機號碼、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。

（２）不應少於六位。

（３）不應訂為相同之英數字、連續英文字或連號數字。

（４）同一用戶代號在同一時間內僅能登入一個連線(session)控制之系統。

（５）如增設使用者代號，至少應依下列方式辦理：

甲、不得為金融機構已知之客戶顯性資料。

乙、如輸入錯誤達五次，金融機構應做妥善處理。

丙、新建立時不得相同於用戶代號及密碼；變更時，亦同。

２、固定密碼之安全設計：

（１）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目相關規定。

（２）建議採英數字混合使用，且宜包含大小寫英文字母或符號。

（３）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。

（４）不應與用戶代號、使用者代號、交易密碼相同。

（５）密碼連續錯誤達五次，不得再繼續執行交易。

（６）變更密碼不得與前一次相同。

（７）首次登入時，應強制變更預設密碼；若未於 30 日內變更預設密碼者，則不得再以該預設密碼執行簽入。

（８）密碼超過一年未變更，金融機構應做妥善處理。

（９）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，可進行加密保護或加入不可得知的資料運算；採用加密演算法者，其金鑰應儲存於經第三方認證(如 FIPS 140-2 Level 3 以上)之硬體安全模組內並限制匯出功能。

(二) 透過公眾交換電話網路傳輸途徑並採用戶代號及固定密碼進行唯一驗證之簽入介面，其安全設計應符合第一目網際網路有關用戶代號之（２）、（３）、（４）及固定密碼之安全設計，惟密碼長度不應少於四位。

八、 採用存款帳戶進行身分確認者，僅限應用於辦理開立數位存款帳戶或申請信用卡，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方式開立，以確認該帳戶之有效性(如透過財金公司之跨行金融帳戶資訊核驗平台進行驗證)；辦理開立數位存款帳戶者並應依「銀行受理客戶以網路方式開立數位存款帳戶作業範本」之規定辦理。辦理申請信用卡者另應增加第七條第一款至第五款之任一款安全設計。

九、採用信用卡進行身分確認者，僅限應用於辦理開立數位存款帳戶或申請信用卡，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，確認該卡片之有效性(如預授權）；辦理開立數位存款帳戶者並應依「銀行受理客戶以網路方式開立數位存款帳戶作業範本」之規定辦理。

十、委由第三方進行身分確認者僅限應用於低風險交易，其驗證方式應符合上述安全規定並與第三方以契約約定雙方權利義務關係及賠償責任。

第八條　　交易類別之安全設計

一、「非電子轉帳及交易指示類」中「帳務類查詢」及「個人資料查詢」之限制

（一）應採用第七條第一款至第三款之任一款、第七條第四款之任一項技術、第七條第五款至第七款或第七條第十款之任一款安全設計進行身分確認(如簽入作業)。

（二）若涉及第三方居間代理者除以契約約定者外，金融機構與第三方之間其安全機制應具備「訊息來源辨識」之基本防護措施。

二、「電子轉帳及交易指示類」之安全設計

（一）應採用第七條第一款至第十款之任一款安全設計進行身分確認。

（二）客戶辦理「限定性繳款」以本人帳戶繳納本人帳單者，其交易指示雖未經客戶事先約定轉出帳戶，但因其轉入帳戶已限定為個別金融機構與個別事業單位事先以契約約定規範之，故金融機構得不使用第七條介面之安全設計；惟金融機構得斟酌透過帳務異動通知，達成客戶事後覆核，以提高其安全控管層次。

（三）辦理授信業務應採用第七條第一款至第七款之任一款安全設計，但辦理下列業務，其安全設計須遵循規範如下：

１、辦理本行新戶但為他行既有非數位存款、貸款或信用卡客戶，同意金融機構查詢聯徵中心信用資料(申請階段)，應採用下列任一方式之安全設計：

（１）採用第七條第一款憑證簽章之安全設計。

（２）採用第七條第五款視訊會議，上傳身分證影像檔，並搭配第七條第二款非數位存款帳戶晶片金融卡之安全設計。

２、辦理本行既有數位存款帳戶之貸款契約成立，應採用第七條第一款之硬體憑證簽章及第七條第五款視訊會議之方式辦理簽約對保，惟如係本行既有第一類適用高風險交易之數位存款帳戶或第二類數位存款帳戶者，得採用第七條第一款至第七款之任一款安全設計方式辦理簽約對保。

３、辦理本行既有信用卡客戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計：

（１）採用第七條第一款憑證簽章及第七條第五款視訊會議。

（２）採用第七條第三款一次性密碼，並將款項撥入本人非數位存款帳戶。

（３）依「長期使用循環信用持卡人轉換機制」申辦信用貸款方案者，採用第七條第一款至第七款之任一款安全設計。

(四)辦理新戶申請信用卡，僅限採用第七條第一款、第八款或第九款之任一款安全設計。

第九條　交易面之安全設計

一、採用第七條第一款憑證簽章之安全設計

（一）應採用經本會認可之憑證機構及其所簽發之憑證，並遵循憑證機構之憑證作業基準檢核其憑證措施，以加強安控機制，維護網路交易安全。

（二）使用憑證應用於「電子轉帳及交易指示類」時，應確認憑證之合法性、正確性、有效性、保證等級及用途限制。

(三)接受他行憑證訊息時，應使用經本會認可之憑證機構簽發之憑證並遵循「金融XML憑證共用性技術規範」且於高風險交易時必須使用硬體裝置儲存金鑰。接受他行憑證載具時，應使用經本會審核通過之中介軟體所支援之憑證載具。

(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)應用於簽入作業時，應簽署足以識別該個人之資料(如：統一編號)；於帳務交易時，應簽署完整付款指示。

(六)應用於高風險交易或依據「銀行受理客戶以網路方式開立數位存款帳戶作業範本」開立第一類帳戶並採用高風險之介面安全設計進行身分驗證者，憑證私鑰應儲存於經第三方認證之硬體裝置。該裝置之晶片應符合我國國家標準CNS 15408 EAL 4+(含增項AVA_VLA.4及ADV_IMP.2)或共通準則(Common Criteria) ISO/IEC 15408 v2.3 EAL 4+(含增項AVA_VLA.4及ADV_IMP.2)或ITSEC level E4或FIPS 140-2 Level 3以上或其他相同安全強度之認證，以防止該私鑰被匯出或複製。若晶片與產生交易指示為同一設備，則應於客戶端經由人工確認(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。

(七)擔任憑證註冊中心受理客戶憑證註冊或資料異動時，其臨櫃作業應增加額外具「兩項以上技術」之安全設計或經由另一位人員審核。

二、採用第七條第二款晶片金融卡之安全設計

(一)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與有效性。

(三)於帳務性交易時，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、採用第七條第三款一次性密碼之安全設計

(一)採用軟體OTP(含簡訊傳送OTP)不得運用於設定約定轉入帳戶。

(二)所產生之一次性密碼，如應用於低風險非約定轉帳交易時，且該密碼與交易內容無關者，應限定該密碼於產生時起120秒內有效。應用於ATM無卡提款產生之一次性「提款序號」，其有效時限可由個別金融機構考量風險承擔之能力與客戶便利性斟酌訂定與調整，惟應不逾該序號產生時起30分鐘。

(三)考量電腦或行動裝置，可能同時遭植入惡意程式竊取登入密碼及OTP，應用於非約定轉入帳戶轉帳交易時，應加強防護機制(如設備指定、推播確認、郵件回覆、採用非交易設備確認交易內容等)

四、採用第七條第四款生物特徵之安全設計

金融機構應依據其風險承擔能力調整生物特徵之錯誤接受度，以能有效識別客戶身分，必要時應增加其他身分確認機制(如密碼)；採用間接驗證者，應事先評估客戶身分驗證機制之有效性。

五、採用第七條第五款視訊會議之安全設計

(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。

(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、採用第七條第六款知識詢問或第七條第七款固定密碼之安全設計

(一) 僅限應用於非首次之認識客戶作業、非首次之客戶風險承受度測驗、信託業推介及終止推介同意書、信用卡業務（新戶申辦信用卡除外)、貸款申請、約定轉入帳戶轉帳、概括約定繳稅費之扣款、限定性繳款之扣款、同一統一編號帳戶間轉帳、共同行銷、不涉及帳務通知或交易之個人資料異動。

(二) 應用於信用卡申辦或貸款申請之契約簽訂時，應增加另一照會機制(如簡訊OTP、兩項以上技術等)。

七、採用行動裝置儲存金鑰之安全設計

(一) 應採用下列任一技術保護金鑰：

1、採用晶片安全設計者，金鑰應儲存於符合我國國家標準 CNS 15408 EAL5、共通準則(Common Criteria)ISO/IEC 15408 v2.3 EAL 5 或 FIPS 140-2 Level 3 以上或其他安全強度相同之安全元件(SE)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)。

３、經第三方機構確認其安全防護。

(二) 透過金鑰運算(如 OTP、TAC 等)應用於非約定轉入帳戶之轉帳交易，應確認金鑰儲存於客戶指定之行動裝置。

(三) 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，以防止遭受惡意程式發動阻斷服務攻擊或偽冒交易。

八、應用於信用卡申辦或貸款申請時，客戶意思表示同意金融機構查詢聯徵中心信用資料，系統應留存記錄(如日期、來源 IP 或電話號碼、同意內容或版本、身分驗證結果等)。

九、個人資料顯示應採取隱碼機制。但如系統已對客戶進行身分確認者(如簽入作業)，得不隱碼其確認交易之必要資訊，或已採取本基準第七條第一款至第四款之任一安全設計者，變更個人資料欄位得不予隱碼處理。

十、應用於法人客戶之高風險交易且未依據無法否認傳送訊息與無法否認接收訊息之訊息傳輸安全設計使用數位簽章者，應遵循下列必要措施：

(一) 應針對金融機構本身及客戶進行風險評估，訂定交易額度與管控機制，並提報董(理)事會或經其授權之經理部門核定，但外國銀行在臺分行，得由總行授權之人員為之。

(二) 應提供客戶交易再確認機制，並確保在安全實體環境下交付給客戶(如雙通道啟用)，客戶端應於每筆交易須經由至少兩人以上進行交易內容再確認，包含一位交易建檔人員及一位以上授權人員。

(三) 交易再確認機制應採用第七條第二款至第四款任一介面之安全設計，並使用硬

體設備保護敏感資料。

硬體設備為防止敏感資料外洩得採用資料輸出管控機制、遮蔽作用之塗層保護機制、破壞偵測與歸零清除保護機制、開機自我測試機制、防止電磁干擾保護機制或其他足以保護設備內敏感資料之安全設計。

若硬體設備具對外連結介面者(如 USB、藍芽、ISO 7816)需限定單一操作程序並符合我國國家標準 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之認證。

(四)應提供完整交易之身分確認、交易再確認、交易異動、訊息通知等軌跡紀錄。

(五)應提供額度授權機制，經由客戶妥善評估後授權其指定交易人員，藉以協助管理之帳戶與交易額度。

(六)應建置防偽冒與洗錢防制偵測系統之風險分析模組與指標，於異常交易行為發生時立即告警並妥善處理；該風險分析模組與指標應定期檢討修訂。

(七)傳輸敏感資料時，應提供端點對端點加密機制(如 end-to-end encryption, E2EE)，於客戶端輸入資料時立即加密，傳送至金融機構端符合 FIPS 140-2 Level 3 以上之硬體安全模組(如 HSM)內進行解密，以避免中間人(Man In The Browser、Man In The Middle)竊取；傳輸固定密碼者須於硬體安全模組內進行驗證。

(八)應建立通知機制，於進行交易再確認或敏感資料異動時立即通知客戶。

(九)應偵測釣魚網站，提醒客戶防範網路釣魚。

(十)應提供客戶安全教育宣導，強化風險認知與交易確認要求。

第十條　交易面之應用系統之安全設計：

一、提供網際網路應用系統，應遵循下列必要措施：

(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(Session)控制及網頁逾時(TimeOut)中斷機制，客戶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)應辨識客戶輸入與系統接收之非約轉交易指示一致性，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。

(五) 應設計於客戶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登入個人網路銀行者，應加強安全機制，如於登入成功及失敗均及時通知客戶、採用人工確認(如圖形驗證碼)進行登入或登入身分確認資料採逐步驗證等機制。

二、提供使用者端程式，應遵循下列必要措施：

（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）於低風險非約定轉入帳戶轉帳或高風險交易時，須於客戶端經由人工確認(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，得不執本措施。

三、提供行動裝置應用系統，應遵循「金融機構提供行動裝置應用程式作業規範」。

第十一條　管理面之安全需求及安全設計

一、管理面之安全需求

應依其內部相關規範辦理，並加強系統上線前之相關測試檢核措施。本安全需求係著重於防範金融機構電腦資源，遭外部以電子銀行相關管道入侵威脅及破壞；期能有效地維護電腦資源之整體性及其隱密性，並保護電腦系統作業安全及維持其高度可使用性。

防護措施	目的
建立安全防護策略	為保障系統安全，唯有經授權之客戶得以存取系統資源，並降低非法入侵之可能性。
提高系統可靠性之措施	提昇電腦系統之可靠性及高度可使用性，亦即減少電腦系統無法使用之機會。
制定作業管理規範	作業管理規範包含金融機構及客戶端兩部分，目的在確定金融機構內部之責任制度、核可程序及確定客戶與金融機構間之責任歸屬。

二、管理面之安全設計

系統管理面之安全設計係指針對系統開發設計時，於系統管理面應加以考量或應具備之基本原則及基本項目。

防護措施	安全設計
建立安全防護策略	應以下列方式處理及管控： 1、系統應依據網路服務需要區分網際網路、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。

	2、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；針對已下線系統應停用防火牆規則。 3、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。 4、應建立病毒偵測機制並定期更新病毒碼。 5、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。 網際網路應用系統應以下列方式處理及管控： 1、應偵測網頁與程式異動，紀錄並通知相關人員處理。 2、應偵測惡意網站連結並定期更新惡意網站清單。 得以下列方式處理及管控： 1、建置安全防護軟硬體。(如：安控軟體、偵測軟體等) 2、設計存取權控制(Access Control)如使用密碼、身分證字號、磁卡、IC卡等。 3、簽入(Login)時間控制。 4、單次簽入(Single-Sign-on)。 5、撥接控制(Dial-up Control)。 6、專線(Lease-Line)使用。 7、記錄客戶查詢電話。 8、控制密碼錯誤次數。 9、電腦系統密碼檔加密。 10、留存交易紀錄(Transaction Log)及稽核追蹤紀錄(Audit Trail) ；針對網際網路應用系統應將其作業系統、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。 11、分級。 12、業務面控制如約定帳戶、限定金額等。 13、系統提供各項服務功能時，應確保個人資料保護措施。

提高系統可靠性之措施	應以下列方式處理及管控： 1、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。 2、定期更換提供給操作者之應用軟體及作業系統密碼。 3、系統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。 4、系統應將重要參數檔加密防護。(如：電腦系統密碼檔)。 網際網路應用系統應以下列方式處理及管控： 1、應避免於營運環境安裝程式原始碼。 2、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。 3、應建立系統安全強化標準，並落實系統安全設定。 4、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。 5、系統僅得開啟必要之服務及程式，客戶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。 6、系統首次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。 7、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。 8、應建立 DDoS 攻擊監控與事故應變機制，並每年進行程序演練。 得以下列方式處理及管控：

	1、建立備援及故障預防措施： （1）預備主機、伺服器、通訊設備、線路、週邊設備等備援裝置。 （2）放置網路伺服器於上鎖密室中。
制定作業管理規範	1、制定安全控管規章含設備規格、安控機制說明、安控程序說明等。 2、編寫客戶端之操作手冊及制訂完整契約，應於 eATM 交易畫面揭示使用 eATM 金融交易之風險。

第十二條　環境及端末設備面之安全需求及安全設計

一、環境面之安全需求

促使金融機構著重於環境及端末設備面之安全控管，強化其所提供之自動化設備之安全防護，以防範遭受外力破壞。

防護措施	基本需求
建立安全防護策略	1、為保持自動化服務區之環境實體完整性，定期檢視是否有增減相關裝置。 2、其安全防護依「銀行公會會員安全維護執行規範」第四條辦理。 3、自動化服務區環境之安全除應依「自動櫃員機之安全維護準則」辦理外，並應保持自動化服務區之環境實體完整性，定期檢視是否有增減相關裝置。 其檢視步驟至少應包括下述： （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)，並應定期陳核並追蹤考核。 （4）金融機構之個別自動櫃員機/自動化服務區應指定該金融機構鄰近之分支機構負責監管。
提高系統可靠性之措施	1、自動化設備之監視系統應依「銀行公會會員安全維護執行規範」第一條辦理。 2、自動化設備之警示通報系統應依「銀行公會會員安全維護執行規範」第六條辦理。
制定作業管理規範	於金融機構內部環境管理部分應落實管理準則之規範。

二、端末設備面之安全設計

防護措施	安全設計
建立安全防護策略	自動櫃員機之安全設計： 1、自動櫃員機金庫裝置應符合美規 UL291 LEVEL 1 標準或歐規 CEN L 或日本自動販賣協會 Level 3 或其他相同安全強度之金庫標準。自動櫃員機之附屬設備（如硬幣存款機）其外殼材質與厚度應符合 1.35mm 厚度之無塗層鋼板或 1.42mm 之鍍鋅鋼板或 1.91mm 厚度之銅或鋁板等標準，以提供基本安全防護。 2、自動櫃員機鍵盤(KEY BOARD/PIN PAD)應符合亂碼化鋼製安全鍵盤(EPP)規格。 3、自動櫃員機讀卡機(CARD READER)應符合下述之標準： （1）ISO 標準 1/2/3 軌磁卡讀寫功能 （2）ISO 7816 4、自動櫃員機應具備 H/W DES 亂碼化裝置 (Triple DES)。 5、自動櫃員機應具備斷電卡片自動退出裝置。 6、自動櫃員機應具備卡片沒收裝置。 7、自動櫃員機應具備標準通訊介面。 8、運用自動櫃員機(CD/ATM)處理卡片交易時，應符合下述規範： （1）卡片內含錄碼及資料，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自動櫃員機。 （2）應確定自動櫃員機協力廠商應與金融機構簽訂資料保密協定。並應將參與自動櫃員機安裝、維護作業之人員名單交付金融機構造冊列管，如有異動，應隨時主動通知金融機構更新之。 （3）自動櫃員機協力廠商人員至自動櫃員機裝設現場作業時，均應出示經由金融機構認可之識別證件。除安裝、維護作業外，並應配合金融機構隨時檢視自動櫃員機硬體是否遭到不當外力入侵或遭裝置側錄設備。 （4）不定時派員抽檢行內外之自動櫃員

	機，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。 （５）應與裝設地點之商家訂立檢核契約。 （６）應確保自動櫃員機之合法性。自動櫃員機應有唯一之 ID(端末設備代號)，且針對晶片卡交易應依每筆交易動態產製不可預知之端末設備查核碼，並檢核資料之正確性與有效性。 ９、自動櫃員機及其附屬設備應具備辨識新臺幣鈔券或硬幣真偽之功能。 實體卡片銷售端末設備之安全設計： 運用銷售端末設備(POS)處理交易時，應符合下述規範： １、卡片內含錄碼及資料，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銷售端末設備。 ２、應確保銷售端末設備之合法性。銷售端末設備應有唯一之 ID(端末設備代號)，且針對晶片卡交易應依每筆交易動態產製不可預知之端末設備查核碼，並檢核資料之正確性與有效性。 ３、應確定銷售端末設備協力廠商應與金融機構簽訂資料保密協定。並應將參與銷售端末設備安裝、維護作業之人員名單交付金融機構造冊列管，如有異動，應隨時主動通知金融機構更新之。 ４、銷售端末設備協力廠商人員至特約商店現場作業時，均應出示經由金融機構認可之識別證件。除安裝、維護作業外，並應配合金融機構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。 ５、不定時派員抽檢安裝於特約商店之銷售端末設備，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。 ６、應與商家訂立檢核契約。
提高系統可靠性之措施	得以下列方式處理及管控：

	1、規劃備援線路。 2、規劃備援電路或 UPS。

第十三條　支付工具面之安全需求及安全設計

一、支付工具面之安全需求

防護措施	基本需求
建立安全防護策略	晶片金融卡之晶片應至少符合「晶片金融卡規格安控等級」如我國國家標準 CNS 15408 EAL 5、共通準則(Common Criteria) ISO/IEC 15408 v2.3 EAL 5 或 ITSEC level E4 等，並能防堵市面上常見之攻擊破解方法。
提高系統可靠性之措施	1、晶片金融卡之發卡及相關軟硬體安全應至少符合「晶片金融卡規格安控等級」。 2、使用各種晶片端末設備，均應經本會晶片端末驗證小組測試通過，確保系統運作之互通性及可靠性。 3、應確保卡片端點對端點之交易安全。
制定作業管理規範	應揭示客戶使用卡片之注意事項，至少應包含下述： 1、建議密碼設定，不得與其個人顯性資訊(如生日、身分證、車號、電話號碼、帳號及相關資料號碼)相同。 2、密碼資訊不應書寫於實體卡片上，並須定期變更密碼。 3、與客戶之契約規定應載明持卡人應負責事項，如保管權、使用權、遺失主動通報權及不當操作致毀損責任等。 4、應於卡片上揭示掛失、二十四小時客服專線及拾獲擲回地址等資訊，並於發卡時主動告知客戶。

二、支付工具面之安全設計

防護措施	安全設計
建立安全防護策略	實體卡片之安全設計： 交易驗證碼(TAC) 1、運用晶片之運算技術，每次交易均由晶片內部自動產生一組唯一之交易碼作為驗證每筆交易之不可否認性，用以確保交易安全。

	2、發行多功能卡片（兩種以上功能），其連線(on-line)金融交易至少應符合上述安全措施，俾達到由發卡金融機構端至客戶端安全。
提高系統可靠性之措施	得以下列方式處理及管控： 1、應做卡片容量規劃。 2、晶片金融卡之發卡及相關軟硬體安全應至少符合「晶片金融卡規格安控等級」。
制定作業管理規範	1、編寫客戶實體卡片之操作指示手冊，並制訂完整合約述明客戶及金融機構之權利義務關係。 2、制定「金融機構晶片金融卡交貨流程」與「安全模組控管作業原則」，除管制外包製卡作業外亦落實實體卡片之安全控管。

第十四條　其他

一、電子銀行業務倘與第三方進行資料傳輸或服務委外時，除應符合訊息來源辨識外，應簽訂相關契約，明訂其須符合本基準之相關規定及雙方責任。

二、本基準應報經主管機關核備實施，修正時亦同。