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

壹、前言

中華民國銀行商業同業公會全國聯合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。

貳、電子銀行業務之定義

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。

參、電子銀行業務之訊息傳輸途徑

係指客戶端利用電子設備及通訊設備與金融機構進行交易時所使用的網路型態。

一、金融機構專屬網路

金融機構專屬網路係直接以連線方式(撥接(Dial-Up)、專線(Lease-Line)或虛擬私有網路(Virtual Private Network，VPN)等方式)傳輸訊息。

二、網際網路(Internet)

客戶端利用電子設備及通訊設備，透過網際網路服務與金融機構間進行交易。網際網路(Internet)係一個提供全球資訊之網路環境，提供使用者連結至個別網址，以便進一步使用 Internet 之各種資訊及資源。

三、加值網路(Value Added Network，VAN)

加值網路係指運用基礎通訊網路所建置之設施，提供正常傳輸外附加價值之服務，諸如自動錯誤偵測及修復(automatic error detection and correction)、通訊協定轉換(protocol conversion)及訊息儲存及後送(message storing and forwarding)等，以增加網路使用之附加價值。惟實際運用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，分別納入前述金融機構專屬網路或網際網路傳輸途徑予以規範。

四、行動網路

客戶端利用電子設備及通訊設備，透過電信服務業者(Telecom)與金融機構間進行交易。電信服務業者在各區域間佈建縝密之基地台(base station)，以負責訊息之傳送及接收。惟實際運用行動網路進行交易指示時，應依個別電信服務業者與金融機構間傳輸途徑之不同，分別納入前述金融機構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,PSTN)

客戶端利用通訊設備，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。

肆、電子銀行業務之交易類別及風險

係指由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。

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：

台外幣存提款、台外幣轉帳、匯兌、台外幣匯款、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：已開立存款帳戶者得線上申辦結清銷戶、約定轉入帳號及受理客戶傳真指示扣款無須再取得客戶扣款指示正本。 授信業務：已開立存款帳戶或既有貸款客戶或既有信用卡客戶者得線上申辦無涉保證人之個人信貸、房貸及車貸於原抵押權擔保範圍內之增貸、個人信貸之既有信用卡客戶依『長期使用循環信用持卡人轉換機制』申請信用貸款方案及線上取得客戶同意銀行查詢聯徵中心信用資料。 信用卡業務：已開立存款帳戶或既有信用卡客戶者得線上申辦信用卡、長期使用循環信用持卡人轉換機制、客戶線上同意信用卡分期產品約款及線上取得客戶同意銀行查詢聯徵中心信用資料。 財富管理業務：已開立存款帳戶得線上申辦信託開戶、認識客戶作業(KYC)、客戶風險承受度測驗及線上取得客戶同意信託業務之推介或終止推介。 共同行銷業務：線上同意共同行銷。

（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、 依法令規定應為照會、認識客戶作業。 3、 事先約定轉入帳戶轉帳。

	4、 設定約定轉入帳戶，惟非同戶名帳戶須先臨櫃申請後才能透過線上新增；其交易限額同９．２要求，若配合採用各種嚴密的技術防護措施時，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。 5、 概括約定及限定性繳費繳稅之稅費轉帳。 6、 同戶名帳戶間轉帳。 7、 貸款撥款至同戶名帳戶或學校之就學貸款指定帳戶。 8、 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。 9、非約定轉入帳戶 ９．１、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。 ９．２、網際網路之低風險性交易，以每戶每筆不超過五萬元、每天累積不超過十萬元、每月累積不超過二十萬元為限。 ９．３、透過網站、電子郵件、傳真、FTP 或 AP2AP 等方式傳送且未經人工確認客戶身分與指示內容者，其交易限額同９．２要求。 ９．４、配合採用各種嚴密的技術防護措施時，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。

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： 個人資料、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。
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。

伍、本基準之構面

本基準構面包括交易面、管理面、環境面及支付工具面等四大構面之安全需求及安全設計，其基本標準如下：

一、交易面之安全需求及安全設計

(一)交易面之安全需求

交易面之安全需求依安全防護措施之不同分述如下：

1、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。

2、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。

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

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

5、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。

6、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	金融機構專屬網路			網際網路		
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
	高風險性之交易	低風險性之交易		高風險性之交易	低風險性之交易	
訊息隱密性	非必要	非必要	非必要	必要	必要	備註一
訊息完整性	必要	必要	非必要	必要	必要	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

【備註】

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，應具備訊息隱密性防護措施。

(三)交易面之安全設計

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低風險交易；應用於低風險交易之安全設計可應用簽入作業。

１、介面之安全設計：

（１）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。於簽入作業時，應簽署足以識別該個人之資料(如：身分證字號)；於帳務交易時，應簽署完整付款指示；於憑證展期時，應簽署展期訊息。

（２）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。

（３）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，金融機構應能防止該密碼被側錄或再應用。惟採用軟體 OTP(含簡訊傳送 OTP)不得運用於設定約定轉入帳戶；針對非約定帳戶轉帳，考量行動裝置可能遭植入惡意程式竊取登入密碼及 OTP，應加強防護機制(如設備指定、推播確認、郵件回覆等)。

（４）使用「兩項(含)以上技術」僅限應用於低風險交易，其安全設計應具有下列兩項(含)以上技術：

- ◆ 客戶與銀行所約定的資訊，且無第三人知悉（如設備密碼、登入密碼等）。
- ◆ 客戶所持有的設備，金融機構應確認該設備為客戶與銀行所約定持有的實體設備（如密碼產生器、密碼卡、晶片卡、電腦、手機、憑證載具等）。
- ◆ 客戶所擁有的生物特徵(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，必要時應增加多項不同種類生物特徵。

（５）使用視訊會議僅限應用於低風險交易，為防止人頭戶偽冒申請，其安全設計應取得清晰雙證件照片、與原留存證件核對、查驗本人及確認真實視訊環境，以防止透過科技預先錄製影片，並依相關規定留存紀錄。

（６）使用知識詢問僅限應用於簽入及低風險交易，其應用範圍應符合伍、一、(三)、４、（６)之要求；其安全設計應利用客戶之其他資訊(如保單資訊、信用卡資訊等)，以利有效識別客戶身分。

（７）使用固定密碼僅限應用於簽入及低風險交易，其應用範圍應符合伍、一、(三)、４、（６)之要求；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後，惟若金融機構另佐以其他簽入驗證或交易驗證者，得將下述密碼之安全設計列為最低要求。

（７・１）用戶代號之安全設計：

（７・１・１）金融機構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。

（７・１・２）不應少於六位。

（７・１・３）不應訂為相同的英數字、連續英文字或連號數字。

（７・１・４）客戶於申請後若未於一個月（日曆日）內變更密碼，則不得再以該用戶代號執行簽入。

（７・１・５）客戶同一時間內只能登入一次密碼。

（７・１・６）如增設使用者代號，至少應依下列方式辦理：

（７・１・６・１）不得為客戶之顯性資料。

（７・１・６・２）如輸入錯誤達五次，金融機構應做妥善處理。

（７・１・６・３）新建立時不得相同於用戶代號及密碼；變更時，亦同。

（７・２）密碼之安全設計：

（７・２・１）不應少於六位。若搭配交易密碼使用則不應少於四位。

（７・２・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。

（７・２・３）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。

（７・２・４）密碼與代號不應相同。

（７・２・５）密碼連續錯誤達五次，不得再繼續執行交易。

（７・２・６）變更密碼不得與前一次相同。

（７・２・７）首次登入時，應強制變更預設密碼。

（７・２・８）密碼超過一年未變更，金融機構應做妥善處理。

２、網際網路應用系統之安全設計：

金融機構提供網際網路應用系統，應遵循下列必要措施：

（１）載具密碼不應於網際網路上傳送。

（２）系統應設計連線(Session)控制及網頁逾時(TimeOut)中斷機制。

（３）系統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。

（４）系統應辨識客戶輸入與系統接收之非約轉交易指示一致性。

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

（６）系統應偵測網頁與程式異動時，進行紀錄與通知措施。

（７）元件應驗證網站正確性。

（８）元件應採用被作業系統認可之數位憑證進行程式碼簽章(CodeSign)。

（９）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

抽拔卡、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(含)以上技術」之介面設計認證機制。

（１０）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，得不執行本安全設計之第(4),(9)等必要措施項目。

（１１）一有駭客入侵時，金融機構即應依狀況關閉服務、伺服器或網站，以確保交易安全。

3、訊息傳輸之安全設計：

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・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(含以上)之三重資料加密演算法(Triple DES)或金鑰有效長度為 128 位元(含以上)之進階資料加密演算法(AES)或其他安全強度相同之演算法。 （１・２)非對稱性加解密系統其應至少採用金鑰長度為 1024 位元(含以上)之 RSA 演算法或金鑰長度為 256 位元(含以上)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。 （１・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。 （２・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。安全強度應符合上述(１・１)及(１・２)之規定。 （２・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・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)，當採明碼交換時，應利用秘密分持(如分 A、B 碼)，以降低該金鑰洩漏之風險。 (２・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(Certificate)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： 可採對稱性加解密系統或非對稱性加解密系統。 (１・１)對稱性加解密系統如 DES(使用押碼(Message Authentication Code，MAC))等機制，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。 (１・２)非對稱性加解密系統如 RSA(使用數位簽章(Digital Signature))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)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： 可採對稱性加解密系統或非對稱性加解密系統。對稱性加解密系統如 DES(使用押碼(Message Authentication Code，MAC))等機制，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。 (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、時戳等機制。
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(Certification Authority，CA)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。

備註：憑證機構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。

4、交易訊息之安全限制：

(１)「非電子轉帳及交易指示類」中「帳務類查詢」之限制

透過網際網路執行「非電子轉帳及交易指示類」中「帳務類查詢」之交易指示訊息，其運用之安全機制應具備「訊息隱密性」之基本防護措施，若涉及第三方居間代理者除以契約約定者外，銀行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。

(２)「電子轉帳及交易指示類」之限制

(２・１) 金融機構應與事業單位以契約規範「限定性繳費稅」業務。「限定性繳費稅」倘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前述介面之安全設計；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。

(２・２) 透過網際網路執行「電子轉帳及交易指示類」之低風險交易指示訊息，除限定性繳費稅交易外，其運用安全機制若不具備「無法否認傳遞訊

息」、「無法否認接收訊息」等基本防護措施者，則其運用之對稱性加解密系統之金鑰長度不得小於128位元(如強制高加密型SSL、EV SSL)，且必須增設安全設計(如固定密碼、OTP)，並配合採用各種嚴密的技術防護措施且能有效防範密碼資料被竊取或交易資料被竄改，以健全安全防護機制。

（２・３）透過公眾交換電話網路(PSTN)無法提供加密功能者(如電話銀行交易)，因係以明碼資料於線上傳輸，故以約定轉出功能，且轉入帳號逐戶約定，公用事業費及各類稅費繳納以概括約定方式為限，惟倘屬限定性繳費稅之低風險性交易，得採非約定轉出功能；金融機構得增設安全設計(如固定密碼、OTP等)，以健全安全防護機制。採用固定密碼安全設計者得以干擾訊號或其他機制防止密碼遭側錄。

（3）採用憑證簽章安全設計之安全規定

（３・１）金融機構應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。

（３・２）使用憑證應用於「電子轉帳及交易指示類」時，金融機構應確認憑證之合法性、正確性、有效性、保證等級及用途限制。

（３・３）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的憑證載具。

（３・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。

（３・５）應用於高風險交易時，憑證私鑰應儲存於符合Common Criteria EAL 4+(至少包含增項AVA_VLA.4 或AVA_VAN.5)或ITSEC level E4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。若晶片硬體與產生交易指示為同一設備，則應於客戶端經由人工確認(如抽拔卡、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(含)以上技術」之介面設計認證機制。

（３・６）金融機構擔任憑證註冊中心，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(含)以上技術」之安全設計或經由另一位人員審核。

（4）採用晶片金融卡安全設計之安全規定

（４・１）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)。

（４・２）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。

（４・３）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(TAC，Transaction Authentication Code)。

（４・４）元件於存取卡片時應設計防止第三者存取。

（４・５）應提示收回卡片妥善保管。

（５）採用行動裝置之安全規定

（５・１）採用晶片金融卡安全設計者，基碼應儲存於安全元件(SE)內，其晶片應符合「晶片金融卡規格安控等級」。

（５・２）行動裝置安全元件(SE)因其長期於連接網際網路之環境，應於交易時增設存取控管，以防止遭受惡意程式發動阻絕服務攻擊(DoS)或偽冒交易。

（６）採用固定密碼或知識詢問之安全規定

（６・１）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、貸款申請、事先約定轉入帳戶轉帳、概括約定及限定性繳費繳稅之稅費轉帳、同戶名轉帳及繳費之低風險交易。

（６・２）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)。

(7) 應用於信用卡申辦或貸款申請時，客戶意思表示同意查詢聯徵資料，系統應留存記錄(如日期、來源 IP、同意書內容或版本、身分驗證結果等)。

(8) 個人資料之保護

透過網際網路呈現個人資料，金融機構應採用「兩項(含)以上技術」等技術保護，有效防範資料被竊取，以落實個人資料保護。

５、雙因素認證：

以上所述採用「兩項(含)以上技術」係指伍、一、(三)、1、(4) 所述技術。

二、管理面之安全需求及安全設計

(一)管理面之安全需求

金融機構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金融機構於系統開發設計時，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隔出獨立的邏輯網域(如 Internet, DMZ, Intranet)，每個網域皆有既定的防護措施並有通訊閘道管制過濾網域間資料的存取。 2、系統應採用入侵偵測與防護措施，提高資安防護。 3、系統應將重要參數檔加密防護。(如：電腦系統密碼檔) 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、記錄使用者查詢電話。 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)。 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、建置病毒偵測軟體(Virus Detection Software)，定期對網路節點及伺服器進行掃毒並應定期更新病毒碼。 2、系統應進行弱點掃瞄與修補。 3、系統應配合作業系統修正檔公佈，盡速修補系統漏洞。

	4、定期更換提供給操作者之應用軟體及作業系統密碼。 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，金融機構應於 eATM 交易畫面揭示使用 eATM 金融交易之風險。

三、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	於銀行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 或日本自動販賣機協會 Level 3 或其他相同安全強度之金庫標準。 2、自動櫃員機鍵盤(KEY BORD/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）金融機構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）金融機構應與裝設地點之商家訂立檢核契約。 （６）金融機構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。 實體卡片銷售端末設備之安全設計： 運用銷售端末設備(Point Of Sale ：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、金融機構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、金融機構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、金融機構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。

四、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 Common Criteria 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、金融機構應確保卡片 END TO END 之交易安全。
制定作業管理規範	金融機構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、金融機構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、金融機構發行多功能卡片（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，俾達到由發卡銀行端至客戶端安全。
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。

陸、其他

一、本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。

柒、名詞解釋

一、AES(Advanced Encryption Standard)：係指進階資料加密演算法。比 DES 加密演算法更進階的加密標準，在目前對稱式金鑰加密的應用中廣泛被採用的一種演算法。

二、AP2AP(Application to Application)：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。

三、CA(Certification Authority)：係指憑證機構。為一可信賴第三方，符合本國電子簽章法，具有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。

四、DoS(Denial of Service)：係指惡意程式發動阻絕攻擊，導致服務中斷。

五、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，提供除現金吐鈔外之實體 ATM 功能。

六、ECC(Elliptic Curve Cryptography)：係指橢圓曲線演算法。於 1985 年由 Koblitz 與 Miller 各別提出的公開金鑰密碼學技術。在相同的安全強度下，ECC 的密碼學金鑰長度可遠較其他公開金鑰密碼系統(如 RSA)小且處理速度較快。

七、EV SSL(Extended Validation SSL)：為遏止網路釣魚的詐騙行為，建立使用者對網際網路的信心，CA/Browser Forum 於 2007 年 6 月頒布了第一版 EV SSL Guidelines，加強(1)辨識憑證申請者之程序, (2)簽發與管理憑證的規定, (3)EV SSL 特有憑證內容的規定, (4)瀏覽器辨識 EV SSL 憑證的處理事項。採用 EV SSL 憑證者，符合加密強度之要求並於瀏覽器以醒目方式告知使用者，通常以綠色底色代表正常、紅色底色代表異常、白色底色表示正常

但網站安裝的是一般 SSL 伺服器憑證。

八、FTP(File Transfer Protocol)：係指網路上進行檔案傳輸的標準協議。為避免傳輸過程中密碼與檔案內容明文傳遞，可透過 FTP over SSL 等方式進行傳輸加密。

九、Triple DES(Triple Data Encryption Standard)：係指三重資料加密演算法。相當於是對每個資料塊應用三次 DES 加密的演算法，以透過增加 DES 的密鑰長度的方式來避免原 DES 的密鑰長度被暴力破解。可分為 Two Keys 及 Three Keys 兩種，其金鑰長度分別為 112 及 168 位元。

十、概括約定：客戶與金融機構事先約定本人某一轉出帳戶可透過電子銀行發動交易指示，繳納金融機構所提供之公用事業費及各類稅費服務。

十一、限定性繳費稅：金融機構(帳務代理行)與事業單位(委託機構)以契約約定規範轉入帳戶、單筆轉入額度與繳費爭議之處理方式，而客戶可透過事業單位或其委託機構網站或扣款金融機構之電子銀行服務發動交易指示給參與服務之扣款金融機構，由其客戶帳戶扣款繳納費用。

十二、抽拔卡：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。

十三、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。

十四、強制高加密型 SSL：為一種伺服器強制加密數位憑證。用戶連結安裝了強制高加密型伺服器數位憑證的網站或伺服器時，於每次進行加密過程時其所產生 "階段金鑰"(Session Key)，無論用戶端加密強度為何，強制使用指定金鑰長度進行加密。