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
本會 106 年 11 月 30 日第 12 屆第 3 次理監事聯席會議討論通過
金管會 107 年 3 月 14 日金管銀國字第 10702029320 號函洽悉
本會 107 年 10 月 25 日第 12 屆第 21 次理監事聯席會議討論通過
金管會 108 年 2 月 18 日金管銀國字第 10702255770 號函洽悉
本會 107 年 10 月 25 日第 12 屆第 21 次理監事聯席會議討論通過
金管會 108 年 2 月 18 日金管銀國字第 10702255770 號函洽悉
本會 108 年 6 月 27 日第 12 屆第 6 次理事會議討論通過
金管會 108 年 10 月 23 日金管銀國字第 1080216776 號函洽悉
本會 109 年 6 月 18 日第 13 屆第 7 次理監事聯席會議討論通過
金管會 109 年 7 月 7 日金管銀國字第 10901401891 號函洽悉
本會 109 年 8 月 14 日第 13 屆第 8 次理監事聯席會議討論通過
金管會 109 年 12 月 24 日金管銀國字第 1090143726 號函洽悉
本會 110 年 3 月 4 日第 13 屆第 12 次理監事聯席會議討論通過
金管會 110 年 4 月 15 日金管銀國字第 11001337391 號函洽悉
本會 111 年 1 月 20 日第 13 屆第 18 次理監事聯席會議討論通過
金管會 111 年 5 月 16 日金管銀國字第 1110205052 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（含以多功能視訊櫃檯開立之新臺幣活期及定期存款帳戶）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、授權事業單位或金融機構發動交易指示，由客戶事先約定本人之轉出帳戶繳納政府機關或事業單位之各類稅費。

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、限定性繳稅費：係指客戶透過電子銀行、授權事業單位或金融機構發動交易指示，由客戶之轉出帳戶繳納政府機關、金融機構或事業單位之各類稅費及投資款項。

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、敏感資料：係指如登入帳號、固定密碼、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。

十七、安全元件(Secure Element)：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。

十八、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。

十九、可信賴執行環境(Trusted Execution Environment)：係指獨立於行動裝置作業系統的一個受信任的執行環境，允許受信任的應用程式通過安全軟體授權在此環境執行，達到與其他部分的隔離。

二十、結構型商品：係指

(一)「銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法」第二條所稱之結構型商品。

(二)「信託業營運範圍受益權轉讓限制風險揭露及行銷訂約管理辦法」第二十二條之一所稱之境內結構型商品及「境外結構型商品管理規則」第二條所稱之境外結構型商品。

二十一、消費扣款：係指客戶向實體或虛擬之特約商店進行物品、勞務或其他交易時，使用發卡機構核發之金融卡或透過電子銀行/行動銀行，委託發卡機構直接由客戶之指定帳戶即時扣款，轉入收單機構或特約商店指定帳戶之功能；前述金融卡包含但不限於磁條金融卡、晶片(感應式)金融卡、行動金融卡。

二十二、程序演練(Table Top Exercise, TTX)：係指一種紙上驗證作業程序的方

法，用於假想情境發生並推估局勢發展，依據事先規劃的作業程序模擬執行，以驗證情境應變之完整性。

二十三、 多功能視訊櫃檯(Video Teller Machine；以下簡稱 VTM)：係指一具有視訊、掃描及證件之辨識模組、具有可觀察客戶親簽及周邊之環境監控模組、24 小時保全及直接連結金融機構內部網路之設備。

二十四、 客戶端電腦應用程式：指金融機構提供並安裝於客戶端電腦(如 Windows, UNIX, MacOS)之應用程式(如 EXE,OCX,SCR,COM,DLL 等)。

二十五、C3 憑證：指符合我國電子簽章法且經本會認可之憑證，其註冊中心應為金融機構，且身分識別方式有二：採當面辦理者，必須由本人親自辦理或持有授權文件之代理人親自辦理，採非當面辦理者，得以視訊或由往來金融機構確認客戶身分等方式辦理。

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：

1、 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。

2、 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。

3、 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。

4、 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。

5、 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，其服務項目舉例如下：存提款、轉帳、匯兌、匯款、消費、投資（如基金、債票券、結構型商品）、款項繳納、授信、付款指示等交易。

２、申請指示，其服務項目舉例如下：

（１）外匯業務：開發信用狀申請、修改信用狀申請。

（２）存款業務

甲、 客戶得申辦數位存款帳戶、同意金融機構查詢聯徵中心信用

資料。

乙、 已開立存款帳戶者得申辦結清銷戶、約定轉入帳號、受理客戶傳真指示扣款無須再取得客戶扣款指示正本、晶片金融卡、非約定轉帳。

丙、 客戶得以多功能視訊櫃檯開立之新臺幣活期及定期存款帳戶。

（3）授信業務

甲、 本行既有個人客戶及新戶得申辦無涉及抵押權或質權設定之個人貸款、限於原抵押權擔保範圍內增貸之房貸及車貸、同意金融機構查詢聯徵中心個人信用資料。

乙、 本行既有法人客戶、法人新戶及法人戶之負責人得申辦無涉及抵押權或質權設定之貸款、同意金融機構查詢聯徵中心信用資料。

丙、 既有貸款戶得申辦授信條件變更。

丁、 保證人得申辦同意金融機構查詢聯徵中心信用資料、成立保證契約。

戊、 法人戶依信保基金規定應查詢之關係人(如配偶)得申辦同意金融機構查詢聯徵中心信用資料。

（4）信用卡業務

甲、 新戶得申辦信用卡、同意金融機構查詢聯徵中心信用資料。

乙、 已開立存款帳戶者或既有信用卡戶或既有貸款戶得申辦信用卡、同意金融機構查詢聯徵中心信用資料。

丙、 既有信用卡戶得申辦長期使用循環信用持卡人轉換機制、同意信用卡分期產品約款。

（5）財富管理業務：認識客戶作業(KYC)、客戶風險承受度測驗、同意第二條第二十款第一目結構型商品業務之推介或終止推介。

（6）信託業務：已開立存款帳戶者得申辦信託開戶或終止信託契約、認識客戶作業(KYC)、客戶風險承受度測驗、同意信託業務之推介或終止推介、同意成為專業投資人之簽署、專業投資人表示已充分審閱而無須適用審閱期之聲明。

（7）共同行銷業務：同意共同行銷。

(二)交易指示

1、高風險交易：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，包含非約定轉帳交易超過最高限額之交易指示。

2、低風險交易：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） 辦理前目第二子目之申請指示。

（2） 辦理 ATM 之存提款服務。

（3） 照會、認識客戶、協助電子支付機構確認客戶身分等作業。

（4） 辦理約定轉入帳戶之設定及轉帳。

（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、票據交換所平台，進行概括約定繳稅費及限定性繳稅費之扣款約定及扣款服務。

（6） 任一金融機構同一統一編號帳戶間轉帳、定存或投資。

（７） 貸款撥款至任一金融機構同一統一編號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、交易指示及資料預處理。

（９） 辦理非約定轉入帳戶之轉帳。

（１０）個人資料異動（如用於身分確認之密碼、用於非約轉交易之聯絡資訊、用於雙方約定之通知方式等）。

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者。

(一)查詢

１、帳務類：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、帳單查詢、借款繳息清單、繳費單、扣繳憑單、扣費憑單、補充保費等。

２、非帳務類：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。

３、個人資料類：聯絡資訊等。

(二)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。

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)訊息來源辨識性(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)訊息不可否認性(Non-repudiation)：係指傳送方或接收方無法否認其傳送或接收訊息行為。

二、各訊息傳輸途徑所應達到之安全防護措施如下（彙總如附表）：

(一)專屬網路

１、訊息隱密性：非必要。

２、訊息完整性：辦理電子轉帳及交易指示類高風險及低風險交易者為必要。

３、訊息來源辨識性：辦理電子轉帳及交易指示類高風險交易者為必要。

４、訊息不可重複性：辦理電子轉帳及交易指示類高風險及低風險交易者為必要。

５、訊息不可否認性：辦理電子轉帳及交易指示類高風險交易者為必要。

(二) 網際網路及公眾交換電話網路

１、訊息隱密性

(１)辦理電子轉帳及交易指示類高風險交易為必要。

(２)辦理電子轉帳及交易指示類低風險交易，若利用網際網路作為訊息傳輸途徑者為必要，若利用公眾交換電話網路作為訊息傳輸途徑者

為非必要，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。

(３)辦理非電子轉帳及交易指示類，若利用網際網路作為訊息傳輸途徑並傳送足以識別該個人之資料訊息者為必要。

２、訊息完整性

(１)辦理電子轉帳及交易指示類高風險交易為必要。

(２)辦理電子轉帳及交易指示類低風險交易，若利用網際網路作為訊息傳輸途徑者為必要、若利用公眾交換電話網路作為訊息傳輸途徑者，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、語音播報再確認)。

(３)辦理非電子轉帳及交易指示類為非必要。

３、訊息來源辨識性：辦理電子轉帳及交易指示類高風險交易者為必要。

４、訊息不可重複性：辦理電子轉帳及交易指示類高風險及低風險交易者為必要。

５、訊息不可否認性：辦理電子轉帳及交易指示類高風險交易者為必要。

前述必要係指金融機構必須具備該項防護措施；非必要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。

第六條　交易面之訊息傳輸安全需求

一、訊息隱密性

(一)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：應至少採用 3DES 112bits 以上、AES 128bits 以上或其他安全強度相同之演算法；惟應用於 TLS 時，不得使用 3DES 演算法並建議使用數據認證加密模式(Authenticated Encryption with Associated Data, AEAD)。

２、非對稱性加解密系統：應至少採用 RSA 2048bits 以上、ECC 256bits 以上或其他安全強度相同之演算法。

３、須全文加密

(二)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)或非對稱性加解密系統(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) ；惟應用於 TLS 時，建議使用 Elliptic Curve Diffie-Hellman Exchange 方式進行金鑰交換。

(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)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。

(三)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。

二、訊息完整性

(一)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 SHA 160bits 以上、DAA 64bits 以上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。

(二)金鑰交換：同前述「訊息隱密性」有關金鑰交換之規範。

(三)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。

三、訊息來源辨識性：

(一)訊息處理：同前述「訊息完整性」有關訊息處理之規範。

(二)金鑰交換：同前述「訊息隱密性」有關金鑰交換之規範。

(三)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。

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：

(一)訊息處理：應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。

(二)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。

(三)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。

第七條　交易面之介面安全設計

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，相關安全設計區分如下，並應符合第九條規定：

一、使用憑證簽章，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、保證內容及用途限制。

二、使用晶片金融卡，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），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」，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、

SIM卡認證等)。

(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，其安全設計應由金融機構人工與客戶確認其身分與指示內容。

六、使用知識詢問，其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、信用卡繳款方式等)，以利有效識別客戶身分。

七、使用固定密碼，其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，系統預設密碼不在此限。

(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)變更密碼不得與原密碼相同。

(７)首次登入時，應強制變更系統預設密碼；若未於30日內變更者，則不得再以該密碼執行簽入。

(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明文匯出功能。

３、採用圖形鎖或手勢之安全設計者，準用前一子目之(５)及(６)規定。

(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，其安全設計應符合前目第一子目用戶代號之(５)之乙與丙及第二子目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，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；驗證他行存款帳戶有效性時，應採用符合財金公司之「跨行金融帳戶資訊核驗」機制辦理，以有卡方式核驗者應驗證晶片金融卡交易驗證碼，以無卡方式核驗者應發送簡訊或推播驗證一次性密碼。

九、採用信用卡，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)；驗證他行信用卡有效性時，應透過聯合信用卡處理中心及財金公司之「信用卡輔助持卡人身分驗證平臺」辦理。

十、採用電信認證，其安全設計應確認申請人與該門號租用人為同一統一編號且係透過用戶身分模組（Subscriber Identity Module，SIM）連線至該電信業者，確認該SIM之有效性並應要求電信業者或電信認證服務提供者遵循下列事項：

(一)應為客戶至電信業者直營門市臨櫃申辦，交付國民身分證及具辨識力之第二身分證明文件並完成親簽後申辦之門號，且應排除儲值卡、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。

(二)如自電信業者取得門號相關個人資料(如姓名、住址、電話、電子郵箱、繳款紀錄、電信評分等)者，金融機構應要求電信業者或電信認證服務提供者須取得門號租用人個資提供第三人之同意，金融機構亦需向客戶取得個資蒐集、處理及利用之同意。

第八條　交易類別之安全設計

一、「非電子轉帳及交易指示類」：辦理帳務類、個人資料類之查詢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、或第七條第五款至第七款之任一款安全設計進行身分確認。

二、「電子轉帳及交易指示類」之交易指示：辦理高風險交易每筆或每批應採用第七條第一款硬體金融FXML憑證簽章安全設計，辦理低風險交易應採用第七條第一款至第七款之任一款安全設計進行身分確認，其中非約定轉帳交易每筆應採用第七條第一款至第四款之任一款安全設計進行身分確認，但辦理下列業務，應遵循下列要求：

(一)辦理「限定性繳稅費」應遵循下列要求：

１、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。

２、進行消費扣款之入帳帳戶，事業單位應指定一用於款項收取作業之活期性存款帳戶，客戶無需輸入該存款帳戶以避免遭竄改，另以行動APP進行每筆達等值新臺幣五千元以上之消費扣款時，應以簡訊、APP推播、電子郵件或其他方式通知，若無法及時通知，應於如對帳單上提示請客戶提供及時聯繫管道，以利後續帳務通知，確保客戶權益，另金融機構得採用第七條第一款、第三款、第四款之任一款安全設計進行客戶身分確認後提供取消通知機制。

３、客戶辦理事業單位或金融機構發動交易指示之扣款約定時，扣款金融機構應採用第七條第一款至第四款之任一款安全設計進行客戶身分確認。

４、金融機構接受事業單位或其他金融機構發動扣款約定或交易指示時，應符合第五條交易面之安全需求。

5、客戶向事業單位或金融機構終止扣款約定後，無需承擔遭冒用之損失，金融機構或事業單位應於十四日內返還帳款，客戶應配合協助後續調查作業。

(二)辦理ＡＴＭ無卡提款業務，於申請時應採用第七條第一款硬體憑證簽章、第二款晶片金融卡、第三款密碼搭配指定之硬體設備產生一次性密碼或第四款『兩項以上技術』等安全設計進行身分確認，於交易時應採用第七條第三款密碼搭配指定之硬體設備產生一次性密碼或第四款『兩項以上技術』進行身分確認」，其提款金額應符合第四條第一款第二目低風險交易之限額規定，且與晶片金融卡之提款限額併計。

(三)個人辦理實體ＡＴＭ轉帳業務，每筆達等值新臺幣一萬元(含)以上時，應以簡訊、APP 推播、電子郵件或其他方式通知，若無法及時通知，應於如對帳單上提示請客戶提供及時聯繫管道，以利後續帳務通知，確保客戶權益，另金融機構得採用第七條第一款、第三款、第四款之任一款安全設計進行客戶身分確認後提供取消通知機制。

(四)辦理「結構型商品交易」應遵循下列要求：

1、交易及扣款帳戶以同一統一編號為限。

2、限非首次辦理之同類型結構型商品交易。

3、金融機構應提供交易內容供客戶確認，並考量電子交易風險承受度，單筆交易超過等值新臺幣一仟萬、每日累計交易金額超過等值新臺幣三仟萬以上之交易應採用第七條第一款高風險交易之安全設計進行客戶身分確認，以防止交易糾紛。

4、金融機構應留存客戶辦理交易指示及確認風險揭露相關紀錄（如:日期、同意內容或版本及身分驗證結果等）。

(五)辦理「非約定轉入帳戶」應遵循下列要求：

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，其交易限額同前一子目要求。

4、若採用之技術防護措施（如憑證簽章、晶片金融卡、非簡訊傳送之一次性密碼、視訊會議、第三人覆核、簡訊簡碼回傳、直接人臉辨識軌跡等），提供客戶確認該筆交易內容並能防止身分確認資料與交易內容被竄改者，該筆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，最高該轉出帳號不超過當日累計等值新臺幣三佰萬元為限，並留存該技術評估紀錄。

5、若經客戶事先以臨櫃或視訊會議申請指定照會人員且由金融機構人工確認其指定人員之身分與指示內容者(如電話照會)，其交易限額由雙方依據風險承受度約定之。

三、「電子轉帳及交易指示類」之申請指示

(一)辦理存款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，應遵循下列要求：

1、臨櫃開立存款帳戶之存戶得線上首次申請晶片金融卡並親赴銀行櫃檯確認身分後辦理領卡。

2、辦理已持有晶片金融卡舊戶申請補換發晶片金融卡者，客戶應先登入網路銀行、行動銀行或網路 ATM 並採用第七條第三款一次性密碼或第四款「兩項以上技術」之安全設計進行身分確認、再郵寄至原留存通訊住址、客戶須透過該銀行 ATM 以舊卡啟用新卡並以系統驗證新舊卡內帳戶號碼係為一致。(如有一晶片金融卡設定多個帳戶號碼之情形，應以該卡片之主要帳戶號碼做驗證。)

3、辦理申請網路銀行或晶片金融卡之非約定轉帳功能應採用第七條第一款至第五款任一款進行設定，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計。

4、辦理申請約定非同一統一編號之約定轉入帳戶，須透過線上逐筆採用第七條第一款至第五款任一款進行設定，並排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計設定，並應遵循下列要求：

(1)首次設定非同一統一編號帳戶者須先經臨櫃或採用第七條第五款視訊會議確認身分後方可為之。

(2)電話語音或網路銀行之新約定帳戶應於申辦日後次一日始生效，惟同一統一編號帳戶經評估並無遭詐騙損失之虞者除外。

(3)約定轉入帳戶之設定，其交易限額同第八條第二款第五目之2要求，若配合採用各種嚴密之技術防護措施，提供客戶確認設定內容並能防止或偵測設定內容被竄改，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。

5、辦理開立數位存款帳戶業務應依「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；惟依據第七條第十款電信認證辦理開立第三類數位存款帳戶時需搭配第七條第五款視訊會議安全設計查驗本人並核對證件照片，另應確認門號使用電信業者服務已超過半年且近 6 個月內繳款正常並沒有停話紀錄。

6、透過 VTM 辦理開立新臺幣活期及定期存款帳戶業務應採用第七條第五款視訊會議安全設計並遵循下列要求：

(1)依臨櫃存款開戶相關規定辦理。

(2)限具本國國籍成年自然人親自辦理。

(3)開立之存款帳號，應有相關區別機制。

(4)相關開戶及印鑑卡等業務書件親自簽名。

(5)開戶視訊過程進行錄音及錄影，並至少留存六個月，其他交易文件保存期限則依各業務相關規範辦理。

(6)開戶初期設計有別於一般臨櫃開立帳戶之管控方式(如交易功能、金額)。

(7)客戶輸入基本資料時，即時檢核客戶是否為高風險客戶，俾引導至臨櫃辦理。

(8)VTM 提供蒐集、處理及利用各人資料告知事項內容，供客戶審閱及確認等功能，並具備檢核機制。

(9)帳戶交易持續加強各項疑似洗錢或資恐交易表徵之監控。

7、辦理晶片金融卡密碼解鎖作業，應採用第七條第一款至第三款任一款安全設計，惟排除以數位存款帳戶之安全設計解鎖臨櫃帳戶之晶片金融

卡、以第三類數位存款帳戶之安全設計解鎖第一類及第二類數位存款帳戶之晶片金融卡、以第二類數位存款帳戶或第一類低風險數位存款帳戶之安全設計解鎖第一類高風險數位存款帳戶之晶片金融卡並排除軟體OTP與簡訊OTP，且應於發卡行之端末設備(如ATM、POS、VTM等)進行，並針對解鎖用之敏感資料採用符合第五條訊息隱密性要求，進行端點對端點加密防護。

(二)辦理個人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，應遵循下列要求：

１、辦理本行個人新戶(含借款人及保證人)同意金融機構查詢聯徵中心信用資料(申請階段)，應採用第七條第一款憑證簽章之安全設計，但如為他行既有非數位存款客戶，得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之安全設計，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進行身分確認。

(３)採用第七條第八款存款帳戶之安全設計並上傳身分證影像檔，其中採用無卡方式核驗以簡訊或推播方式發送一次性密碼者，應依據客戶本人留存於非數位存款帳戶銀行的手機號碼進行發送。

(４)採用第七條第十款電信認證之安全設計，上傳身分證影像檔，並搭配第七條第五款視訊會議或第八款存款帳戶之財金公司之「跨行金融帳戶資訊核驗」進行身分確認，並視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近6個月內繳款正常並沒有停話紀錄等)。

２、辦理本行個人既有數位存款帳戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計：

(１)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，應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。

(２)本行既有第一類適用低風險交易之數位存款帳戶，辦理簽約對保應採用下列任一方式之安全設計：

甲、採用第七條第一款之硬體憑證簽章辦理簽約對保。

乙、採用第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」，並搭配第七條第六款知識詢問或上傳身分證影像檔之安全設計機制辦理簽約對保者，得將款項撥入本人非數位存款帳戶。

丙、採用第七條第四款包含生物特徵之「兩項以上技術」搭配第九條第一款第一目第三子目軟體C3憑證簽章或第七條第六款知識詢問辦理簽約對保，得將款項撥入本人存款帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。

(３)本行既有第三類數位存款帳戶，辦理簽約對保應採用下列任一方式之安全設計：

甲、採用第七條第一款之硬體憑證簽章安全設計。

乙、採用第七條第五款視訊會議辦理簽約對保者，限將款項撥入本人非數位存款帳戶。

丙、採用第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」，並搭配第七條第六款知識詢問或上傳身分證影像檔之安全設計機制辦理簽約對保者，得將款項撥入本人非數位存款帳戶。

丁、採用第七條第四款包含生物特徵之「兩項以上技術」搭配第九條第一款第一目第三子目軟體C3憑證簽章或第七條第六款知識詢問辦理簽約對保，得將款項撥入本人存款帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)

(４)本行既有第三類數位存款帳戶，經確認資金使用於特定目的用途且借款人同意貸款款項直接撥入第三方公司之實體帳戶者，如採第七條第四款包含生物特徵之「兩項以上技術」及第七條第一款硬體憑證簽章辦理簽約對保者，得將款項撥入他行第三方公司之實體帳戶。

３、辦理本行個人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，得將款項撥入本人非數位存款帳戶、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。

(３)採用第七條第三款一次性密碼及第七條第五款視訊會議，得將款項撥入本人第一類適用低風險交易之數位存款帳戶及第三類數位存款帳戶。

(４)採用第七條第四款包含生物特徵之「兩項以上技術」，得將款項撥入本人非數位存款帳戶、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。

(５)採用第七條第四款包含生物特徵之「兩項以上技術」搭配第九條第一款第一目第三子目軟體C3憑證簽章或第七條第六款知識詢問辦理簽約對保，得將款項撥入本人存款帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。

(６)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。

４、辦理本行個人新戶之貸款契約或保證人保證契約成立，簽約對保方式應採用下列任一方式之安全設計：

(１)採用第七條第一款硬體憑證簽章之安全設計，得將款項撥入本人存款帳戶。

(２)採用第七條第八款存款帳戶之安全設計並上傳身分證影像檔，其中採用無卡方式核驗以簡訊或推播方式發送一次性密碼者，應依據客戶本人留存於非數位存款帳戶銀行的手機號碼進行發送，得將款項撥入本人存款帳戶。

(３)採用第七條第十款電信認證之安全設計者，上傳身分證影像檔，且限將款項撥入本人非數位存款帳戶，並視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近6個月內

繳款正常並沒有停話紀錄、人工照會)。

5、辦理「個人貸款」及「房貸及車貸原抵押權擔保範圍內」之增貸，對原保證人增貸保證契約成立，簽約對保方式應採用第七條第一款至第五款之任一款安全設計。

6、辦理個人購屋貸款依「個人購屋貸款定型化契約應記載事項」第十三條及個人購車貸款依「個人購車貸款定型化契約應記載事項」第十二條（擔保物權連結條款）借款人或第三人提供擔保物設定抵押權予金融機構時，該抵押權擔保範圍僅限本貸款契約之債務，借款人因未來需求，需經擔保物提供人另以書面同意時，應採用第七條第一款硬體憑證簽章之安全設計。

(三)辦理法人授信業務應遵循下列要求：

1、辦理本行既有法人客戶及法人新戶同意金融機構查詢聯徵中心信用資料，應採用下列安全設計機制：

(1)採用第七條第一款硬體憑證簽章之安全設計。

(2)法人戶之負責人或保證人或依信保基金規定應查詢之關係人(如配偶)同意金融機構查詢聯徵中心信用資料之安全設計，應比照個人授信案件有關本行新戶同意金融機構查詢聯徵中心信用資料之安全設計。

2、辦理本行既有法人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)採用第七條第一款硬體憑證簽章之安全設計。

(2)透過本行法人戶申請平台驗證檢核既有客戶事先以授權書方式授權原留存印鑑之安全設計。上述檢核流程應透過公司負責人進行線上身分驗證後傳送印鑑，公司負責人身分驗證須依第八條第三款第二目第一子目個人貸款身分確認機制，相關檢核及驗證軌跡、紀錄等應比照第九條第七款規定辦理。

3、辦理3位以下本國籍自然人股東之法人新戶(不包括有法人股東之公司)之貸款契約成立，簽約對保方式應採用第七條第一款硬體憑證簽章之安全設計。

4、辦理法人戶之負責人或保證人契約成立之簽約對保方式，應採用下列任一方式之安全設計：

(1)採用第七條第一款硬體憑證簽章之安全設計。

(2)採用第七條第五款視訊會議，並搭配第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」。

5、法人戶徵授信相關文件之上傳，應採用法人戶及其負責人貸款契約成立之安全設計機制。

(四)信用卡業務除辦理新戶申辦信用卡業務應採用第七條第一款、第八款、第九款或第十款之任一款安全設計，其中採用第十款電信認證者，應視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近6個月內繳款正常並沒有停話紀錄、人工照會)；辦理其他信用卡業務應採用第七條第一款至第七款之任一款安全設計。

(五)辦理財富管理業務應採用第七條第一款至第七款之任一款安全設計，但本基準另有限制者，從其規定。

(六)辦理信託業務應採用第七條第一款至第七款之任一款安全設計，但本基準另

有限制者，從其規定。

四、首次辦理電子轉帳及交易指示類低風險交易之服務者應與資安、法遵及風控等單位(以下簡稱二道防線)建立各部門間之連繫機制、確認相關作業符合本基準及相關定型化契約等相關法令規定，留存驗證軌跡及建立各部門建議事項追蹤控管機制後，若合規即可開辦，並於開辦後六個月內重新檢視並作成報告交由二道防線確認。內部稽核單位應依據交易量與金額等評估新種業務之風險，排定內部稽核計畫辦理查核，並對評估風險偏高者適時辦理專案查核，以落實內部控制三道防線之運作；惟經主管機關核准採行風險導向內部稽核制度之金融機構，其內部稽核單位應將新種業務納入年度風險評估範圍，並就風險評估結果為高風險者列入次年度查核項目。

五、金融機構委由第三方辦理第七條第二款至第七款介面安全設計者僅限應用於「非電子轉帳及交易指示類」或「電子轉帳及交易指示類」之低風險交易，其驗證方式應符合上述安全規定並得與第三方以契約約定雙方權利義務關係及賠償責任。

第九條　交易面之安全設計具體要求

一、採用第七條第一款憑證簽章，應遵循下列安全設計：

(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。已通過審查之憑證及適用範圍如下：

１、採用經本會核可之金融 FXML 憑證得辦理非電子轉帳及交易指示類、電子轉帳及交易指示類之高風險和低風險交易。

２、採用內政部簽發之自然人憑證或經濟部簽發之工商憑證僅能應用於非電子轉帳及交易指示類、電子轉帳及交易指示類之申請指示服務。

３、採用經密碼保護之臺灣網路認證公司簽發第三級商務 EC+憑證、第三級商務 XML 憑證或中華電信公司簽發第三級 Public CA 憑證。上述 C3 憑證僅能應用於非電子轉帳及交易指示類、電子轉帳及交易指示類之申請指示服務。如若以臨櫃或第七條第一款至第五款之任一款安全設計進行憑證申請之身分確認者，方能辦理不涉及非約定轉入帳戶轉帳之低風險交易，惟金融機構應確保金鑰儲存安全。

(二)使用憑證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)；應用於書面同意時，應簽署依相關法令規定之指定書件；應用於帳務交易時，應簽署完整付款指示。

(六)應用於高風險交易或開立第一類適用高風險交易之數位存款帳戶進行身分驗證者，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，應遵循下列安全設計：

(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，應遵循下列安全設計：

(一)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。

(二)採用簡訊傳送 OTP 時，應遵循下列安全設計：

1、應用於電子轉帳交易指示類時，應與發送行銷廣告之門號有所區隔。

2、應用於電子轉帳交易指示類並以簡訊傳送 OTP 重新設定固定密碼或重新綁定兩項以上技術時應加強防護機制(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 卡認證、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或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)，該機制應排除固定密碼或電子郵件認證。

3、應用於非約定轉入帳戶轉帳交易時，應遵循下列安全設計：

(1)手機號碼之異動應採用第七條第一款至第五款任一款進行設定，惟排除透過軟體 OTP 或簡訊傳送 OTP 之安全設計。

(2)考量客戶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 卡認證、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或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)。

4、應用於開立第二類數位存款帳戶時，手機號碼之設定應於臨櫃辦理，另異動應採用臨櫃或第七條第一款至第五款任一款進行設定，惟排除透過軟體 OTP 或簡訊傳送 OTP 之安全設計。

四、採用第七條第四款「兩項以上技術」，應遵循下列安全設計：

(一)採用直接驗證生物特徵技術者，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。又金融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)，以期有效識別客戶身分；若無法有效確認真人或本人時應增加其他安全設計。

(二)採用間接驗證生物特徵技術者，應事先評估客戶身分驗證機制之有效性，善盡告知客戶使用上之風險，並提供間接驗證機制關閉管道，且應加強控制措施(可參考前款第二目第2子目範例)。

五、採用第七條第五款視訊會議之安全設計應確認真人(Liveness Detection)、本人(Biorecognition)辦理，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。

(一)應依相關規定留存影像或照片，以利後續查證。

(二)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時，僅限應用於辦理非電子轉帳及交易指示類及下列電子轉帳及交易指示類之業務：

(一)存款業務

１、約定轉入帳戶轉帳。

２、概括約定繳稅費之扣退款。

３、限定性繳稅費之扣退款與設定(如基金定期定額、信用卡繳款)。

４、同一統一編號帳戶間轉帳、定存或投資。

(二)授信業務(新戶除外)。

(三)信用卡業務（新戶除外）。

(四)財富管理業務

１、非首次之認識客戶作業。

２、非首次之客戶風險承受度測驗。

３、同意第二條第二十款第一目結構型商品業務之推介或終止推介。

(五)信託業務

１、非首次之認識客戶作業。

２、非首次之客戶風險承受度測驗。

３、信託業推介及終止推介同意書。

４、同意簽署為專業投資人。

５、專業投資人聲明表示已充分審閱而無須適用審閱期之規定。

(六)共同行銷業務。

(七)不涉及帳務通知或交易指示之個人資料異動。

(八)協助電子支付機構確認客戶身分。

七、應用於信用卡申辦或貸款申請時，系統應留存足以證明客戶意思表示同意金融機構查詢聯徵中心信用資料之紀錄(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)，且相關紀錄內容可完整呈現供日後查驗。

八、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)， 得不隱碼其帳號及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款安全設計者，變更個人資料欄位得不予隱碼處理。

九、應用於法人客戶之高風險交易且未能使用符合我國電子簽章法之數位簽章者，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非我國憑證機構通過 WebTrust 或 ETSI 認可具密碼保護且可應用於法人金融交易簽章之憑證、第七條第二款或第三款安全設計，並使用安全元件(Secure Element)、可信賴執行環境(Trusted Execution Environment)、安全載具(如動態密碼產生器)或增強防護機制之行動裝置應用程式軟硬體，以保護敏感資料，並遵循下列安全設計：

１、安全元件應符合我國國家標準 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。

２、可信賴執行環境應符合 GlobalPlatform 標準或其他相同安全強度之認證。

３、安全載具應具備資料輸出管控機制、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。

４、行動裝置之應用程式應符合「金融機構提供行動裝置應用程式作業規範」第十五條安全防護措施或其他足以保護設備內敏感資料之安全設計。

(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)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。

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。

(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)應辨識合作第三方網站或應用系統傳送之訊息，確保訊息隱密、訊息完整、來源辨識及不可重複並要求妥善保護客戶資料。

(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)採用固定密碼進行網路銀行身分確認者，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、針對固定密碼應提供端點對端點加密機制。係指於客戶端(如瀏覽器)輸入資料後立即加密，傳送至金融機構可信任網段(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；如用戶代號為個人統一編號者，其使用者代號仍應加強防護(如雜湊、加密、混淆)。

3、確定為客戶行為(如於登入成功及失敗均及時通知客戶、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)。

(八)應提供客戶安全教育宣導，強化風險認知與交易確認。

二、提供客戶端電腦應用程式，應遵循下列必要措施：

(一)可執行程式(如 EXE,COM 等)應採用被作業系統認可之數位憑證進行程式碼簽章(CodeSign) 且安裝過程不應出現憑證相關安全警告。

(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，得不執行本措施。

三、透過 QR Code 進行資料傳輸，應遵循下列必要措施：

(一)QR Code 表示的資料應為辦理該業務所需最小化為原則。

(二)應用於電子轉帳及交易指示類時，應設計合理使用時效，且在時效內以使用一次為限

(三)所產生之 QR Code，如具客戶個人資料應符合訊息隱密性、如應用於電子轉帳及交易指示類時，應符合訊息完整性、訊息來源辨識性與訊息不可重複性。

(四)應針對解析 QR Code 後進行格式檢查，如為網站連接應進行網站合法性檢查。

四、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。

(一)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。

(二)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。

(三)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。

(一)建立安全防護策略

1、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(如 Any IP, Any port 等)及六個月內無流量之防火牆規則應評估其必要性與風險；針對已下線系統或無作業需求應停用防火牆規則。

(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。

(6)應偵測釣魚網站，如有發現應採取必要措施（如通知、警告或限制存取等）。

(7)應納管最高權限帳號(含作業系統及應用系統)，避免系統維護人員持用最高權限帳號辦理日常維護作業。

2、網際網路應用系統除前子目外應增加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。

3、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可將其作業系統、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。

(二)提高系統可靠性之措施

1、應以下列方式處理及管控：

(1)金融機構對 ATM、電腦、伺服器之系統軟體、工具軟體或應用程式應避免採用已停止弱點修補或更新之軟體，如有必要應採用必要防

護措施，並於安裝作業時，應檢視無惡意程式(如病毒、木馬、後門、蠕蟲、間諜、詐騙、側錄等)，並透過偵測機制定期掃描。

(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）。

２、網際網路應用系統除前子目外應增加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)系統或新功能首次上線前及針對異動程式至少每半年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。

３、得以下列方式處理及管控：

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。

(三)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。

１、制定網路資安事件應變管理機制(如網路安全監控作業、內部通報處理程序)。

２、制定變更管理程序(如程式更新程序、程式更新覆核程序、檢視檔案完整性程序)。

３、制定系統日誌管理程序(如收錄重要事件、定期檢視、提示警告、追蹤處理)

４、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。

５、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。

(一)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。

(二)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。

(三)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

(一)建立安全防護策略

１、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：

甲、ISO 標準 1/2/3 軌磁卡讀寫功能

乙、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：

甲、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。

乙、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。

丙、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。

丁、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。

戊、應與裝設地點之商家訂立檢核契約。

己、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。

２、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。

３、VTM 之安全設計

(１)VTM 之金融卡金庫（如提供現金提存功能者）、鍵盤、讀卡機及處理卡片交易時，應比照第十二條第二項第一款第一目第一小目至第三小目及第八小目自動櫃員機之安全設計。

(２)VTM 應具備確認客戶本人申辦業務之舉證能力及方法（如照片、影像或聲音），並留存驗證紀錄與交易軌跡，遇有爭議時則可調閱相關紀錄。

(３)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。

(４)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。

(５)VTM 應直接連結金融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。

(６)VTM 如產製或存取晶片金融卡或簽帳金融卡，應符合下列要求：

甲、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。

乙、應具備卡片沒收裝置。

(二)提高系統可靠性之措施

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

(一)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。

(二)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。

(三)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

(一)建立安全防護策略

實體卡片之安全設計，至少應包含下述：

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。

(二)提高系統可靠性之措施

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」。

(三)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(含金控及其子公司)進行資料傳輸或服務委外時，除應符合訊息來源辨識外，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。

附表一：各訊息傳輸途徑所應達到之安全防護措施

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
訊息來源辨識性	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
訊息不可否認性	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、語音播報再確認)。