附件一

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10500193690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
本會 111 年 12 月 22 日第 14 屆第 3 次理監事聯席會議討論通過
金管會 112 年 6 月 14 日金管銀國字第 1120202881 號函洽悉
本會 113 年 12 月 19 日第 14 屆第 6 次理事會議核議通過
金管會 114 年 3 月 18 日金管銀國字第 1130152842 號函洽悉
本會 114 年 6 月 26 日第 14 屆第 7 次理事會議核議通過
金管會 115 年 1 月 7 日金管銀國字第 1140223782 號函修正後洽悉

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、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。

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。

中華民國銀行商業同業公會全國聯合會
金融業務電子化委員會
1150107 版本

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)：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、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，包含但不限於：Web phone、App phone。

(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)：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。

十二、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。

十三、公開金鑰基礎建設(Public Key Infrastructure)成員如下：

(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。

(二)註冊中心(Registration Authority)：係指擔任驗證憑證申請人及憑證請求等資訊正確性之工作。

(三)憑證用戶(Subscriber)：係指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰(Private Key)者。憑證用戶可以是自然人或組織。

(四)信賴憑證者(Relying Party)：係指相信憑證主體名稱與該主體公開金鑰及私密金鑰連結關係之個人或組織。

十四、一次性密碼技術：係指以下三種方式擇一辦理

(一)基於時間因子演算的一次性密碼：係指一種以金鑰與當前時間計算而產生的一次性密碼。

(二)基於計數器數值演算的一次性密碼：係指一種以金鑰與當前計數器數值計算而產生的一次性密碼。

(三)基於來源訊息演算的一次性密碼：係指一種以金鑰與接收資料計算而產生的一次性密碼。

十五、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。

十六、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」(以下簡稱衍商辦法)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：係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、臨櫃辦理：係指透過面對面，由本人親自辦理或持有授權文件之代理人親自辦理。

二十六、C3 憑證：指符合我國電子簽章法且經本會認可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(含商務 XML Plus)或中華電信公司簽發第三級 Public CA 憑證，其註冊中心應為金融機構。

二十七、信賴等級(Level of Assurance, LoA)：係指對利用數位身分驗證機制驗證申請人或客戶所宣稱身分結果之可信程度，依據安全設計與交易風險區分為最高(LoA 5)、高(LoA 4)、中(LoA 3)、低(LoA 2)、最低(LoA 1)等五個信賴等級。

二十八、個人統一編號：係指內政部核發之國民身分證統一編號及外來人口統一證號。

二十九、統一編號：係指個人統一編號、營利事業機構與非營利機構的法人身分代號。

三十、 數位身分驗證(Digital Identity Authentication)：係指於數位金融環境利用適當之技術與機制，確認申請人或客戶為其所宣稱身分之過程。包含身分登錄(identity enrollment)、信物管理(credential management)及身分驗證(identity authentication)三階段。

三十一、電信認證：銀行取得客戶同意後，由客戶透過載有 4G／5G 門號 SIM 卡（或配合電信業者更新之最新技術）之行動裝置，經過第三方認證機構連線至客戶所屬之電信業者，以客戶之行動電話號碼，身分證號碼等資料，與電信業者之行動門號租用人申請資料比對，確認客戶與該門號租用人為同一個人統一編號。

三十二、經銀行核驗的電信認證：除滿足前款電信認證之相關規定外，該門號須經銀行採低信賴等級以上安全設計進行身分驗證。

第三條　訊息分類

一、公開資訊：包含但不限於官網之匯利率。

二、個人資訊：個人資料保護法之個人資料，包含但不限於銀行帳號，惟排除個人統一編號及特種個資(包含病歷、醫療、基因、性生活、健康檢查、犯罪前科)。

三、身分識別資訊：個人統一編號、網銀登入之用戶代號及使用者代號。

四、身分核驗資訊：固定密碼、生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)。

五、機敏資訊：製卡個人化資料、非對稱式加密之私密金鑰、對稱式加密之加密金鑰、個人資料保護法之特種個資。

第四條　訊息保護

一、訊息加密機制：可採用下列任一機制進行全訊息加密。

(一)對稱性加解密：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)。

(二)非對稱性加解密：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。

二、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)於經第三方認證(至少符合 FIPS 140-2 Level 3 或同等規格以上)之硬體安全模組內進行解密，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。

三、金鑰交換機制：採對稱性加解密時，其金鑰交換可分訊息加密金鑰與金鑰保護金鑰之交換，應遵循下列要求：

(一)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。安全強度應依據第一款訊息加密機制辦理。

(二)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。

四、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。

第五條　訊息處理

一、訊息傳輸：

(一)於網際網路(Internet)上傳輸個人資訊、身分識別資訊、身分核驗資訊或機敏資訊應採用第四條第一款訊息加密機制。採用用戶代號及固定密碼進行網路銀行身分確認(如簽入作業)且該用戶代號如為個人統一編號者，其使用者代號仍應加強防護(如雜湊、加密、混淆)，又該固定密碼應採用第四條第二款端點對端點加密機制。

(二)於公眾交換電話網路(Public Switched Telephone Network)上以雙音多頻訊號傳輸身分核驗資訊之固定密碼者，應以干擾訊號或其他機制防止遭側錄。

(三)於內部網路(Intranet)上傳輸客戶之身分核驗資訊或機敏資訊應採用如雜湊、加密、混淆、編碼等機制加強防護。

二、訊息儲存：

(一)身分核驗資訊之固定密碼應先進行不可逆運算(如雜湊)，另為防止透過預先產製雜湊值推測密碼,可採用加密、混淆等機制加強防護。

(二)身分核驗資訊之生物特徵、機敏資訊應採用訊息加密機制。

(三)前二目採用加密演算法者，其金鑰應儲存於經第三方認證(至少符合 FIPS 140-2 Level 3 或同等規格以上)之硬體安全模組內並限制明文匯出功能。

三、訊息顯示：

(一)個人資料顯示應採取隱碼機制。但如系統已採用最低信賴等級以上安全設計對客戶進行身分確認者，得不隱碼其帳號及確認交易之必

要資訊；另已採用中信賴等級以上、簡訊 OTP 或軟體 OTP 任一安全設計進行身分確認者，變更個人資料欄位得不予隱碼處理。

(二)須取得客戶同意，始得顯示其同意之個人資料(如自然人戶名)給交易對方，以利交易確認。

第六條　數位身分驗證機制

數位身分驗證機制包含身分登錄、信物管理及身分驗證三階段。客戶於首次啟用數位金融服務時，金融機構透過身分登錄及信物管理作業，以核驗並確認客戶所提供之身分資料與客戶本身之關聯性，並綁定、核發及啟用信物。嗣後客戶於每次使用數位金融服務時，金融機構透過身分驗證作業，依據客戶所提示信物及身分驗證程序確認客戶身分，各階段相關要求參照附錄一辦理。

金融機構使用之安全設計應參照附錄四常見安全設計(如憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊、信用卡資訊、電信認證、金融 Fast ID、行動自然人憑證等)及附錄五身分驗證要求辦理；如非屬附錄四列舉之安全設計，得參考附錄二格式及附錄三範例撰寫報告及評估信賴等級，惟須經二道防線確認並留存軌跡。

第七條　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、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、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個人貸款、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。

丁、既有信用卡戶，辦理其他信用卡業務。

(５)財富管理業務：

甲、認識客戶作業(KYC)。

乙、客戶風險承受度測驗。

丙、衍商辦法結構型商品業務之同意推介或終止推介、同意成為專業客戶、專業客戶聲明已充分審閱而無須適用審閱期。

(６)信託業務：

甲、已開立存款帳戶者得申辦各類信託開戶(含簽約)及變更、增補或終止信託契約

乙、認識客戶作業(KYC)

丙、客戶風險承受度測驗

丁、同意信託業務之推介或終止推介

戊、同意成為專業投資人之簽署

己、專業投資人表示已充分審閱而無須適用審閱期之聲明。

庚、依信託契約約定之信託財產運用範圍，為申請運用指示：

i. 同一統一編號帳戶間轉帳、定存或投資(含交易取消)。

ii. 辦理約定轉入帳戶之付款。

iii. 辦理非約定轉入帳戶之付款指示。

iv. 受益人行使表決權。

辛、依信託契約約定由委託人或信託監察人行使同意權。

(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辦理低風險交易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、國外提款之磁條密碼、網路銀行使用者代號等）。

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。

第八條　交易類別信賴等級及業務要求(第三類數位存款帳戶應依附錄六規定辦理)

一、「非電子轉帳及交易指示類」：

(一) 辦理帳務類之查詢應採用最低信賴等級以上之安全設計進行身分確認，惟排除電信認證安全設計。

（二）辦理個人資料類之查詢應採用最低信賴等級以上之安全設計進行身分確認，惟排除電信認證安全設計。

二、「電子轉帳及交易指示類」之交易指示：

（一）高風險交易

辦理高風險交易，應遵循下列任一要求：

1、採用最高信賴等級之安全設計進行身分確認。

2、應用於法人客戶且未能使用符合我國電子簽章法之數位簽章者，應採用高信賴等級以上之安全設計進行身分確認，惟排除VTM視訊會議、自然人憑證及工商憑證等安全設計，並應遵循下列必要措施：

(1)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。

(2)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。

(3)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。

(4)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。

(5)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。

(6)應建立通知機制,於進行交易再確認或機敏資訊異動時立即通知客戶。

（二） ATM服務

1、辦理ATM存提款業務，應採用晶片金融卡進行身分確認。

2、辦理ATM無卡存款業務，應採用最低信賴等級以上安全設計進行身分確認。

3、辦理ATM無卡提款業務，應遵循下列要求：

（１）於申請及交易時應採用中信賴等級以上之安全設計進行身分確認，惟排除自然人憑證、工商憑證、軟體憑證及視訊會議等安全設計。

甲、若採用晶片金融卡安全設計者，該卡應為該帳戶所申請。

乙、若採用一次性密碼安全設計者，應以密碼搭配指定之硬體設備產生一次性密碼。

（２）提款金額應符合第八條第二款第六目第一子目低風險交

易之限額規定，且與晶片金融卡之提款限額併計。

4、實體 ATM 轉帳與通知

（1）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。

（2）金融機構得採用中信賴等級以上、簡訊 OTP 或軟體 OTP 等任一安全設計進行身分確認，惟排除晶片金融卡、視訊會議及金融 Fast ID 等安全設計，提供個人取消實體 ATM 轉帳通知機制。

(三)繳稅費及消費扣款

1、限定性繳稅費

（1）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中信賴等級以上、簡訊 OTP 或軟體 OTP 等任一安全設計進行身分確認，惟排除工商憑證及視訊會議等安全設計。

（2）辦理客戶發動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，進行限定性繳稅費扣款及退款(如基金定期定額、信用卡繳款)服務，應採用最低信賴等級以上之安全設計進行身分確認，惟排除信用卡資訊安全設計及電信認證安全設計。

（3）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六條數位身分驗證機制；惟金融機構應以簡訊、App 推播、電子郵件或其他方式通知，以利客戶事後覆核。

（4）金融機構接受客戶、事業單位、其他金融機構或金融資訊服務事業、票據交換所平台等發動交易指示(如扣款約定、扣款、退款、終止扣款約定)時，應依據第五條訊息處理方式辦理。

（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。

2、概括約定繳稅費

（1）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之扣款約定時，扣款金融機構應採用中信賴等級以上、簡訊 OTP 或軟體 OTP 等任一安全設計進行身分確認，惟排除工商憑

證及視訊會議等安全設計。

（２）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六條數位身分驗證機制；惟金融機構應以簡訊、App 推播、電子郵件或其他方式通知，以利客戶事後覆核。

（３）金融機構接受客戶、事業單位、其他金融機構或金融資訊服務事業、票據交換所平台等發動交易指示(如扣款約定、扣款、退款、終止扣款約定)時，應依據第五條訊息處理方式辦理。

（４）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。

３、消費扣款

（１）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。

（２）金融機構得採用中信賴等級以上、簡訊 OTP 或軟體 OTP 任一安全設計進行身分確認，惟排除晶片金融卡、視訊會議及金融 Fast ID 等安全設計，提供客戶取消消費扣款通知機制。

(四)同一統一編號轉帳交易

任一金融機構同一統一編號帳戶間轉帳、定存或投資應採用低信賴等級以上、知識詢問或固定密碼等任一安全設計進行身分確認，惟排除自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊等安全設計。

(五)約定轉入帳戶轉帳交易(又稱約轉交易)

約轉交易應採用低信賴等級以上、知識詢問或固定密碼等任一安全設計進行身分確認，惟排除自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊等安全設計。

(六)非約定轉入帳戶轉帳交易(又稱非約轉交易)

非約轉交易每筆應採用中信賴等級以上、簡訊 OTP 或軟體 OTP 等任一安全設計進行身分確認，惟排除自然人憑證、工商憑證、軟體憑證及視訊會議等安全設計，並應遵循下列要求：

1、透過網際網路之低風險交易，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。

2、透過網站、行動 App、電子郵件、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。

3、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、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)，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。

4、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。

5、若採用簡訊傳送一次性密碼並應用於非約定轉入帳戶轉帳交易者，應遵循下列要求：

（1）手機號碼之異動應採用臨櫃、中信賴等級以上、簡訊 OTP 或軟體 OTP 等任一安全設計進行身分確認，惟採用簡訊 OTP 者應驗證舊有之門號號碼及新換之門號號碼。

（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 等身分核驗資訊或機敏資訊，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)。

(七)結構型商品交易

1、非首次辦理之同類型結構型商品交易應採用低信賴等級以上、知識詢問或固定密碼等任一安全設計進行身分確認，惟排除自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊等安全設計。

2、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元，每日累計交易金額超過等值新臺幣參仟萬元以上應採用最高信賴等級之安全設計進行身分確認，以加強風險控管。

3、辦理結構型商品交易應遵循下列業務要求：

（１）交易及扣款帳戶以任一金融機構同一統一編號為限。

（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）。

(八)信託業務

辦理依信託契約約定之信託財產運用範圍，為申請運用指示：

１、辦理任一金融機構同一統一編號帳戶間轉帳、定存或投資(含交易取消)應參照前(四)目同一統一編號轉帳交易之安全設計辦理。

２、辦理約定轉入帳戶之付款應參照前(五)目約定轉入帳戶轉帳交易之安全設計辦理。

３、辦理非約定轉入帳戶之付款應參照前(六)目非約定轉入帳戶轉帳交易之安全設計辦理。

(九)授信業務

客戶指示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之低風險交易，既有客戶應採用最低信賴等級以上之安全設計進行身分確認，新戶應採用低信賴等級以上之安全設計進行身分確認。

三、「電子轉帳及交易指示類」之申請指示：

(一)外匯業務

開發信用狀申請、修改信用狀申請應採用低信賴等級以上之安全設計進行身分確認，惟排除自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊等安全設計。

(二)存款業務

１、晶片金融卡

（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應採用下列任一方式之安全設計：

甲、 客戶應先登入網路銀行、行動銀行或網路 ATM 並採用一次性密碼或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。

乙、 適用高風險交易之第一類數位存款帳戶，應採用高信賴等級以上之安全機制。

丙、 適用低風險交易之第一類數位存款帳戶、第二類數位存款帳戶，應採用中信賴等級以上、軟體 OTP 或透過簡訊傳送 OTP 等任一安全設計。

丁、 法人客戶應採用高信賴等級以上之安全機制。

（３）辦理已持有晶片金融卡舊戶啟用補換發晶片金融卡應採

用下列任一方式之安全設計(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。)：

甲、 須透過該銀行 ATM 以舊卡並以系統驗證新舊卡內帳戶號碼係為一致。

乙、 以視訊會議核驗身分方式辦理；如採用非多功能視訊櫃檯(VTM)之視訊會議機制者，應搭配憑證簽章、一次性密碼或兩項以上技術等安全設計進行身分確認，惟排除一次性密碼之軟體 OTP 及透過簡訊傳送 OTP 等安全設計。

丙、 採用中信賴等級以上之安全機制。

（４）辦理晶片金融卡密碼解鎖應採用中信賴等級以上之安全設計進行身分確認，惟排除自然人憑證、工商憑證、軟體憑證、兩項以上技術、金融 Fast ID 及視訊會議等安全設計，並應遵循下列要求：

甲、 應於發卡行之端末設備(如 ATM、POS、VTM 等)進行。

乙、 應依據第五條訊息處理方式針對機敏資訊進行端點對端點加密防護。

丙、 不得以數位存款帳戶之安全設計解鎖臨櫃帳戶之晶片金融卡。

丁、 不得以適用第七條低風險交易之第一類數位存款帳戶或第二類數位存款帳戶之安全設計解鎖第一類(不含限適用第七條低風險交易)數位存款帳戶之晶片金融卡。

２、約定轉入帳號

（１）辦理申請約定同一統一編號之約定轉入帳戶應採用低信賴等級以上、知識詢問或固定密碼任一種安全設計進行身分確認，惟排除經銀行核驗的電信認證及存款帳戶資訊安全設計。

（２）首次設定非同一統一編號帳戶者須先經臨櫃或採用視訊會議確認身分後方可為之。

（３）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中信賴等級以上之安全設計進行身分確認，惟排除自然人憑證、工商憑證及軟體憑證等安全設計。

（４）透過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。

（５）約定轉入帳戶之設定，其交易限額同第八條第二款第六

目第一子目要求，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。

3、非約定轉入帳號

已開立存款帳戶者申辦電子銀行（如網路銀行、行動銀行、網路 ATM）或晶片金融卡之非約定轉帳功能應採用中信賴等級以上之安全設計進行身分確認，惟排除自然人憑證、工商憑證及軟體憑證等安全設計。

4、其他業務

（1）已開立存款帳戶者申辦結清銷戶應採用低信賴等級以上之安全設計、知識詢問或固定密碼等任一安全設計進行身分確認，惟排除經銀行核驗的電信認證及存款帳戶資訊等安全設計。

（2）同意金融機構查詢聯徵中心信用資料應採用低信賴等級以上之安全設計、知識詢問或固定密碼等任一安全設計進行身分確認，惟排除經銀行核驗的電信認證及存款帳戶資訊等安全設計。

(三)授信業務

1、同意查詢聯徵信用資料(個人含借款人、保證人等)

（1）本行個人既有客戶，應採用最低信賴等級以上之安全設計進行身分確認。

（2）本行個人新戶但為他行既有非數位存款客戶，應採用低信賴等級以上之安全設計進行身分確認。

（3）本行個人新戶，應採用中信賴等級以上之安全設計進行身分確認。

2、簽約對保業務(個人含借款人、保證人等)

除另有規定外，限撥入本人任一金融機構同一統一編號帳戶：

（1） 本行個人既有客戶(數位存款帳戶及信用卡戶除外)，應採用最低信賴等級以上之安全設計進行身分確認。

（2） 本行個人新戶，應採用低信賴等級以上之安全設計進行身分確認。

（3） 本行個人既有數位存款帳戶(數存一高及數存二)，應採用最低信賴等級以上之安全設計進行身分確認。

（4） 本行個人既有數位存款帳戶(數存一低)，應採用低信賴等級以上之安控設計，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:新增撥款簡訊通知、晶片金融卡、一次性密碼、視訊會議或其他安全設計)。

（5） 本行個人既有信用卡客戶，應採用下列任一方式之安全設計：

甲、 採用憑證簽章及視訊會議之安全設計。

乙、 採用一次性密碼，限撥入本人非數位帳戶、第一類(不含限適用第七條低風險交易)數位存款帳戶或第二類數位存款帳戶。

丙、 採用一次性密碼及視訊會議之安全設計。

丁、 採用包含生物特徵之「兩項以上技術」，限撥入本人非數位帳戶、第一類(不含限適用第七條低風險交易)數位存款帳戶或第二類數位存款帳戶。

戊、 採用包含生物特徵之「兩項以上技術」搭配 C3 軟體憑證或知識詢問之安全設計，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） 本行個人既有信用卡客戶，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，應採用最低信賴等級以上安全設計進行身分確認。

3、「擔保物權連結條款」規定之同意書簽署

個人購屋貸款依「個人購屋貸款定型化契約應記載事項」第十三條或個人購車貸款依「個人購車貸款定型化契約應記載事項」第十二條，沿用原抵押權需擔保物提供人同意簽署，其安全設計應依下列辦理：

（1） 擔保物提供人為借款人或保證人或本行既有客戶，依識別之身分別(即既有戶、數位存款戶等)，比照「貸款契約」成立簽約對保之安全設計辦理。

（2） 擔保物提供人為借款人或保證人以外之第三人且為本行新戶，應採用高信賴等級以上(限 FXML 硬體憑證、硬體自然人憑證、工商憑證 IC 卡且為正卡)之安全設計辦理。

4、同意查詢聯徵信用資料(法人)

（1） 本行既有法人戶及法人新戶，應採用高信賴等級以上之安全設計進行身分確認。

（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)，應依其屬本行既有客戶或新戶，分別採用個人授信業務同意金融機構查詢聯徵中心信用資料之各項安全設計進行身分確認。

5、簽約對保業務(法人)

（1） 本行既有法人客戶，應採用高信賴等級以上之安全設計進行身分確認。

（２） 3位以下本國籍自然人股東之法人新戶，應採用高信賴等級以上之安全設計進行身分確認。

（３） 法人戶負責人或保證人，應採用中信賴等級以上之安全設計進行身分確認。

６、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。

７、辦理授信業務應遵循下列業務要求：

（１） 應用於貸款申請時，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。

（２） 透過本行法人申請平台驗證檢核既有客戶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之身分確認機制，相關檢核及驗證軌跡、紀錄等應比照前一子目辦理。

(四)信用卡業務

１、新戶申辦信用卡業務、同意金融機構查詢聯徵中心信用資料，應採用最低信賴等級以上之安全設計進行身分確認，惟排除一次性密碼、兩項以上技術、知識詢問及固定密碼等安全設計，若採用電信認證者，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)。

２、已開立存款帳戶者或既有信用卡戶或既有貸款戶申辦信用卡、同意金融機構查詢聯徵中心信用資料，應採用最低信賴等級以上之安全設計進行身分確認，惟排除存款帳戶資訊、信用卡及電信認證等安全設計。

３、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，應採用最低信賴等級以上之安全設計進行身分確認，惟排除存款帳戶資訊、信用卡資訊及電信認證等安全設計。

４、既有信用卡戶辦理其他信用卡業務，應採用最低信賴等級以上之安全設計進行身分確認，惟排除存款帳戶資訊、信用卡資訊及電信認證等安全設計。

５、應用於信用卡申辦時，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。

(五)財富管理業務

1、認識客戶作業(KYC)應採用低信賴等級以上之安全設計進行身分確認。

2、非首次之認識客戶作業(KYC)應採用最低信賴等級以上之安全設計進行身分確認。

3、客戶風險承受度測驗應採用低信賴等級以上之安全設計進行身分確認。

4、非首次之客戶風險承受度測驗應採用最低信賴等級以上之安全設計進行身分確認。

5、衍商辦法結構型商品業務之同意推介或終止推介應採用最低信賴等級以上之安全設計進行身分確認。

6、同意成為專業客戶應採用最低信賴等級以上之安全設計進行身分確認。

7、專業客戶聲明已充分審閱而無須適用審閱期應採用最低信賴等級以上之安全設計進行身分確認。

(六)信託業務

1、已開立任一金融機構存款帳戶者得申辦各類信託開戶(含簽約)及變更、增補或終止信託契約應採用低信賴等級以上之安全設計進行身分確認。

2、首次認識客戶作業(KYC)應採用低信賴等級以上之安全設計進行身分確認。

3、非首次之認識客戶作業(KYC)應採用最低信賴等級以上之安全設計進行身分確認。

4、首次客戶風險承受度測驗應採用低信賴等級以上之安全設計進行身分確認。

5、非首次之客戶風險承受度測驗應採用最低信賴等級以上之安全設計進行身分確認。

6、同意信託業務之推介或終止推介應採用最低信賴等級以上之安全設計進行身分確認。

7、同意簽署為專業投資人應採用最低信賴等級以上之安全設計進行身分確認。

8、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應採用最低信賴等級以上之安全設計進行身分確認。

9、依信託契約約定由委託人或信託監察人行使同意權應採用最低信賴等級以上之安全設計進行身分確認。

10、依信託契約約定之信託財產運用範圍申請「受益人行使表決權」指示應採用最低信賴等級以上之安全設計進行身分確認。

(七)共同行銷業務

共同行銷業務應採用低信賴等級以上、知識詢問或固定密碼等任一安全設計進行身分確認，惟排除經銀行核驗的電信認證及存款帳戶資訊等安全設計。

(八)其他業務

1、非首次認識客戶作業應採用最低信賴等級以上之安全設計進行身分確認，首次認識客戶作業應採用低信賴等級以上之安全設計進行身分確認。

2、不涉及帳務通知或交易指示之個人資料異動、協助電子支付機構確認客戶身分應採用低信賴等級以上之安全設計，或知識詢問或固定密碼安全設計進行身分確認，惟排除自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊等安全設計。

3、照會、涉及帳務通知或交易指示之個人資料異動、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、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、國外提款之磁條密碼、網路銀行使用者代號等應採用中信賴等級以上、簡訊 OTP 或軟體 OTP 等任一安全設計進行身分確認，惟排除自然人憑證、工商憑證及軟體憑證等安全設計。

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數位身分驗證機制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。

六、 各項業務適配之身分核驗安全設計，須遵循下列要求：

(一) 首次申辦高風險交易之業務須經主管機關核准後實施。

(二) 各項業務欲採用之身分核驗安全設計，若低於業務其信賴等級要求，應取得二道防線確認，並留存驗證軌跡。

(三) 採用非屬附錄四所述之身分核驗安全設計，應取得二道防線確認，並留存驗證軌跡。

第九條　應用系統安全設計：

一、 提供網際網路應用系統，應遵循下列要求：

(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，防止未經銀行同意以模擬瀏覽器(如 WebView、WebBrowser 等)方式竊取身分核驗資訊或機敏資訊(如不支援模擬瀏覽器、網頁程式動態變化或 App 外開指定瀏覽器等)。

2、 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，應遵循下列要求：

(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，應遵循下列要求：

(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，應依其業務屬性設計合理使用時效，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」。

第十條　端末設備安全設計

一、 自動櫃員機

（一）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。

（二）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。

（三）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

（四）自動櫃員機應具備 H/W DES 亂碼化裝置(Triple DES)。

（五）自動櫃員機應具備斷電卡片自動退出裝置。

（六）自動櫃員機應具備卡片沒收裝置。

（七）自動櫃員機應具備標準通訊介面。

（八）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。

(九) 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。

二、實體卡片銷售端末設備

(一) 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。

(二) 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。

(三) 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。

(四) 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。

(五) 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。

(六) 應與商家訂立檢核契約。

第十一條　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、 本基準經本會理事會通過並函報金融監督管理委員會核備後實施，修正時亦同。

金融機構辦理電子銀行業務安全控管作業基準

附錄

目錄

附錄一、數位身分驗證機制三階段要求說明

一、數位身分驗證機制之身分登錄階段及信物管理階段

應依下列定義進行信賴等級(LoA)評估，評估結果取身分登錄及信物管理兩階段最低之結果得出整體綜合性之信賴等級，並留存「數位身分驗證機制之信賴等級評估報告」(表例參考請詳附錄二)。另常見安全設計評分範例，請詳附錄三。

(一)身分登錄階段

1. 最低保證等級(Level 1)

申請人自我宣稱或證實所提具之身分資訊具唯一性可辨識唯一身分，且申請人有簽署服務條款以表示理解與同意。

2. 低保證等級(Level 2)

(1) 滿足 Level 1 之要求。

(2) 足以表示其身分客觀存在：申請人提示可靠來源之資料，本身信賴等級應達 LoA2 或經政府機關核准之身分證明文件，且該資料已由申請人向信任機構進行註冊，並可透過公開且客觀方式檢驗資料正確性與有效性。

3. 中保證等級(Level 3)

(1) 滿足 Level 2 之要求。

(2) 由申請人提示一個經可靠來源之資料，本身信賴等級應達 LoA3 或經政府機關核准之身分證明文件，並經信任機構驗證。

4. 高保證等級(Level 4)

(1) 滿足 Level 3 之要求。

(2) 申請人提示兩個不同可靠來源之資料，其一應經信任機構驗證（本身信賴等級皆應達 LoA3 或經政府機關核准之身分證明文件)，其二做為其一資料身分之補強（本身信賴等級至少為 LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑，或原開戶時之留存簽名)。

(3) 若為法人臨櫃辦理帳戶，應以書面同意由其指定人員申請，經核驗後辦理。書面同意例如，蓋有公司名稱之簽名章及負責人印鑑或簽名。

(4) 若為內政部核發之硬體自然人憑證或經濟部核發之工商憑證 IC 卡(正卡)，基於信賴其權威性與合法性，可不再提示第二可靠來源資料做為補強。

5. 最高保證等級(Level 5)

(1) 滿足 Level 4 之要求。

(2) 須經人工查驗（如臨櫃辦理、VTM)。

(二)信物管理階段

1. 最低保證等級(Level 1)
   (1) 信物有制定作業安全政策及作業程序(如啟用、綁定、保存、更換及撤銷等)。
   (2) 信物須由申請人或經信物服務提供單位授權之人員啟用。
2. 低保證等級(Level 2)
   (1) 滿足 Level 1 之要求。
   (2) 信物必須加密保護，如對稱式或非對稱式之加密保護。
   (3) 信物必須親自交付或檢查交付方式與該申請人合理關聯。
3. 中保證等級(Level 3)
   (1) 滿足 Level 2 之要求。
   (2) 信物啟用時須驗證個體和信物關聯性。
   (3) 信物具防竄改或防資料外洩之保護措施(如數位簽章或存於硬體載具但設定為鎖定狀態)。
   (4) 若信物因效期需進行更換或展期者,依身分登錄進行身分核驗。
4. 高保證等級(Level 4)
   (1) 滿足 Level 3 之要求
   (2) 保存信物之硬體設備且具備竄改檢測機制，如符合 FIPS 140-2 Level 2 或其他相同安全強度之認證。
   (3) 若使用 TEE、安全載具、行動裝置做為信物，應符合 Global Platform 標準或其他相同安全強度之認證，或具備資料管控、破壞偵測、自我測試等防護機制;行動裝置應用程式須依「行動裝置應用程式作業規範」具備防入侵、執行期間保護及機敏資料防護機制，以確保安全性與防竄改能力。
   (4) 若信物作業程序包含更換或展期，依身分登錄進行身分核驗。
   (5) 若信物作業程序包含啟用，只允許在指定時間內完成。
   (6) 若信物作業程序包含信物簽收及保存，須經申請人或其授權代理人同意。
5. 最高保證等級(Level 5)
   (1) 滿足 Level 4 之要求。
   (2) 必須採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制，如符合 FIPS 140-2 Level 3 或其他相同安全強度之認證。
   (3) 應具「電子簽章法」之不可否認性，亦即能確認簽署人身分，確保簽署意願，並透過私鑰簽署、時間戳與完整性驗證，防止否認或篡改，以推定為本人親自簽名或蓋章。
   (4) 信物更換或展期依身分登錄進行身分核驗。

二、數位身分驗證機制之身分驗證階段

應考量各項安全設計身分驗證過程中可能所遇之作業活動風險，並採取適當措施進行控管，除評估可能所遇之作業活動風險外，亦可參考常見安全設計身分驗證階段要求(詳參附錄五)，另金融機構應自行評估並留意可能之作業活動風險，如：

1. 線上破解：透過不斷猜測信物值的方式，並重複嘗試登入系統，以獲取真正的信物值
2. 線下破解：利用身分驗證過程以外的分析技術，獲取與信物產製相關的機密資訊。
3. 信物複製：客戶持有的信物或產製信物的方式遭非法複製。
4. 釣魚攻擊：攻擊者誘使個體與偽冒的驗證者互動，進而竊取足以偽冒該個體之機敏資料。
5. 竊聽攻擊：攻擊者監聽客戶身分驗證作業之過程，以獲取關鍵訊息，並在後續的主動攻擊中冒充該客戶。
6. 重送攻擊：攻擊者攔截並重送客戶與金融機構之間正常往來的驗證資訊，藉此冒充客戶進行身分驗證。
7. 連線劫持：當客戶與金融機構完成身分驗證並開始交換訊息後，攻擊者介入兩者之間的通信管道，進而冒充客戶或金融機構，攔截並控制會話資料交換。
8. 中間人攻擊：攻擊者介入客戶與金融機構之間，攔截並篡改身分驗證資訊，並同時冒充客戶與金融機構，與雙方分別互動，以便利用一方傳送的驗證訊息成功欺騙另一方。
9. 信物竊取：攻擊者竊取用於產製或儲存信物的裝置。
10. 欺騙偽裝攻擊：攻擊者冒充另一客戶，以執行其原本無法完成的行為。

附錄二、數位身分驗證機制之信賴等級評估報告

階段	重點檢核項目	評分理由 （所有Level等級，均需滿足前一等級的所有要求）	保證等級
身分登錄	• Level 1 □申請人自我宣稱或證實所提具之身分資訊具唯一性可辨識唯一身分。 □申請人有簽署服務條款以表示理解與同意。	• Level 1評分理由	
	• Level 2 □申請人提示之身分資訊，由可靠來源提供。 □申請人提示之可靠來源資料滿足LoA2（低信賴等級）或經政府機關核准之身分證明文件，且該資料已由申請人向信任機構進行註冊，並可透過公開且客觀方式檢驗資料正確性與有效性。	• Level 2評分理由	

	• Level 3 □申請人提示之可靠來源資料滿足LoA3（中信賴等級）或經政府機關核准之身分證明文件。 □申請人提示之可靠來源資料經信任機構驗證。	• Level 3評分理由	
	• Level 4 □申請人提示兩個不同可靠來源之資料，其一應經信任機構驗證（本身信賴等級皆應達LoA3或經政府機關核准之身分證明文件），其二做為其一資料身分之補強（本身信賴等級至少為LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑，或原開戶時之留存簽名）。 □**若**為法人臨櫃辦理帳戶，應以書面同意由其指定人員申請，經核驗後辦理。書面同意例如，蓋有公司名稱之簽名章及負責人印鑑或簽名。 □**若**為內政部核發之硬體自然人憑證或經濟部核發之工商憑證IC卡(正卡)，基於信賴其權威性與合法性，可不再提示第二可靠來源資料做為補強。	• Level 4評分理由	

	・Level 5 □經人工查驗（如臨櫃辦理、VTM）	・ Level 5評分理由	
階段	重點檢核項目	評分理由 （所有Level等級，均需滿足前一等級的所有要求）	保證等級
信物管理	信物：＿＿		
	・ Level 1 □信物有制定作業安全政策及作業程序（如啟用、綁定、保存、更換及撤銷等）。 □信物須由申請人或經信物服務提供單位授權之人員啟用。	・ Level 1評分理由	
	・ Level 2 □信物經加密保護。 □信物親自交付或檢查交付方式與該申請人合理關聯。	・ Level 2評分理由	

	• Level 3 □信物啟用時須驗證個體和信物關聯性。 □信物具防竄改或防資料外洩之保護措施。 □**若**信物因效期需進行更換或展期者，依身分登錄進行身分核驗。	• Level 3評分理由	
	• Level 4 □保存信物之硬體設備具防竄改保護措施且具備竄改檢測機制，如符合FIPS 140-2 Level 2或其他相同安全強度之認證。 □**若**使用TEE、安全載具、行動裝置做為信物，應符合Global Platform標準或其他相同安全強度之認證，或具備資料管控、破壞偵測、自我測試等防護機制;行動裝置應用程式須依「行動裝置應用程式作業規範」具備防入侵、執行期間保護及機敏資料防護機制，以確保安全性與防竄改能力。 □**若**信物作業程序包含更換或展期，依身分登錄進行身分核驗。 □**若**信物作業程序包含啟用，只允許在指定時間內完成。 □**若**信物作業程序包含信物簽收及保存，須經用戶或其授權代理人同意。	• Level 4評分理由	

	・Level 5 □必須採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制，如符合FIPS 140-2 Level 3或其他相同安全強度之認證。 □應具「電子簽章法」之不可否認性，亦即能確認簽署人身分，確保簽署意願，並透過私鑰簽署、時間戳與完整性驗證，防止否認或篡改，以推定為本人親自簽名或蓋章。 □信物更換或展期依身分登錄進行身分核驗。	・ Level 5評分理由	
信賴等級			

附錄三、身分核驗安全設計及信賴等級評估範例

一、以 FXML 硬體憑證為例

階段	評分原因	評分	評等結果
身分登錄	應於臨櫃辦理或書面同意由法人戶指定人員核驗身分後辦理。 ● 金融機構向申請人詳細說明業務應用系統憑證使用，及申請單與合約書上之權利與義務規範，相關業務運作的作業流程與提供使用說明與操作文件，經申請人同意並確認。(Level 1) ● 申請人出示身分證，並可透過公開且客觀方式檢驗真偽後，確認其客觀存在。(Level 2) ● 申請人提示身分證，並經信任機構驗證其身分證之有效性，提供申請人密碼函，完成申請人註冊申請作業。(Level 3) ● 法人戶經書面同意由法人戶指定人員核驗身分後辦理。(Level 4) ● 臨櫃辦理經人工查驗。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	應採用經本會核可由臺灣網路認證公司或中華電信公司簽發之金融用戶憑證(以下簡稱金融 XML 憑證)。 ● 信物政策與作業流程：遵循經銀行公會核准之憑證管理中心憑證實務作業基準。信物須由申請人啟用。(Level 1) ● 信物臨櫃辦理並親自交付。(Level 2) ● 信物啟用：申請人至少經過身分識別碼及密碼的檢核驗證確認關聯性，登入至註冊中心，將產生的憑證申請訊息經由申請人私鑰簽章後傳送至註冊中心。(Level 3) ● 信物啟用只允許在指定時間內完成。(Level 4)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態）、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄	Level 5

	● 信物簽收及保存須經申請人同意：憑證使用之範圍依憑證實務作業基準、憑證申請人與 FUCA 之合約中規定，憑證用戶使用憑證時，憑證用戶必須妥善保管及儲存與憑證相關之私密金鑰，避免遺失、曝露、被竄改或為第三者任意使用或竊用。(Level 4) ● 信物展期、更換：憑證更新由憑證用戶遵照 FUCA 與註冊中心的業務需求與作業規範辦理，憑證系統如有配合業務系統安全性管控的需求時，則不提供憑證更新之功能，憑證用戶必須重新產生新金鑰對，才可向 FUCA 申請憑證簽發。(Level 4) ● 金融 XML 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。(Level 5) ● 具「電子簽章法」之不可否認性。(Level 5)	改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 ■Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA5		

二、以硬體自然人憑證為例

階段	評分原因	評分	評等結果
身分登錄	內政部簽發之硬體自然人憑證： ● 申請人親赴申辦戶所櫃檯，詳閱用戶約定條款並同意條款內容後填寫申請資料表（如：姓名、身分證字號、電子郵件等）。（Level 1） ● 申請人提示本人身分證，並可透過公開且客觀方式檢驗真偽，確認其客觀存在，且經戶役政資料庫查驗其有效性。(Level 2)、(Level 3) ● 內政部為法定最高發證主管機關(內政部為法定國民身分證核發機關)，採用其本身所核發之身分證，做為內政部核發自然人憑證申請時之身分證明查驗，基於信賴其權威性與合法性，可不再提示第二可靠來源資料做為補強。(Level 4) ● 臨櫃辦理經人工查驗。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	內政部簽發之硬體自然人憑證： ● 信物政策與作業流程：遵循內政部憑證管理中心憑證實務作業基準。(Level 1) ● 信物交付：臨櫃親自交付。(Level 2) ● 信物簽收及保存須經申請人同意：臨櫃申辦之申請人於簽名確認申請時，將於戶所一併完成憑證接受作業，申請人不需另行開卡即可使用。(Level 4) ● 申請人如未能於憑證簽發後 90 天內，完成憑證接受作業，	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態）、信物更換或展期依身分登錄進行身分核驗。	Level 4

	則視為拒絕接受憑證，該憑證將自動被停用。(Level 4) ● 信物展期：將憑證 IC 卡插入讀卡機，並輸入身分證字號/居留證號、生日及 PIN 碼。 (Level 4) ● 應採用晶片憑證載具(FIPS 140-2 Level 2 by CPS)。(Level 4，不符合 Level 5)	■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA4		

註：原先採用硬體自然人憑證及工商憑證為最高信賴等級，現依據 ISO 29115 原則評估後調整為高信賴等級。

三、以工商憑證 IC 卡(正卡)為例

階段	評分原因	評分	評等結果
身分登錄	經濟部簽發之工商憑證 IC 卡(正卡)： ● 填寫憑證申請書，並簽署服務條款以表示理解與同意。(Level 1) ● 事業主體所指派之臨櫃申請人必須填寫個人資料，註冊中心對臨櫃申辦人核對身分，無誤後於申請書上簽名。臨櫃申請人攜帶身分證向戶役政資料庫查驗，營利事業登記證向國稅局查驗。(Level 2)、(Level 3) ● 憑證申請書蓋用事業主體登記及負責人之印鑑章(與事業主體登記時使用之印鑑章同款)，指派臨櫃申辦人至臨櫃申請。(Level 4) ● 臨櫃辦理經人工查驗。 (Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件,或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	經濟部簽發之工商憑證 IC 卡(正卡)： ● 信物政策與作業流程：遵循經濟部工商憑證實務作業基準。(Level 1) ● 信物交付：臨櫃或函郵交付。 (Level 2) ● 信物啟用：申請人進行 IC 卡開卡時，輸入申請憑證時所設定之用戶代碼，並表示接受憑證，將獲得發卡中心以亂數設定的 IC 卡初始 PIN 碼。(信物由申請人啟用，符合 Level 1；啟用須驗證個體和信物關聯性，符合 Level 3) ● 申請人如未能於憑證簽發後 30 天內完成憑證接受作業，則視為拒絕接受憑證，該憑證將自動被廢止。(Level 4)	■Level 1:信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施(如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收	Level 4

	● 信物展期：憑證正卡不允許展期。(Level 4) ● 應採用晶片憑證載具(FIPS 140-2 Level 2 by CPS)。(Level 4，不符合Level 5)	及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA4		

註：原先採用硬體自然人憑證及工商憑證為最高信賴等級，現依據 ISO 29115 原則評估後調整為高信賴等級。

四、以法人高風險憑證為例－安全載具(如動態密碼產生器)

階段	評分原因	評分	評等結果
身分登錄	限法人戶並應於臨櫃辦理或書面同意由法人戶指定人員核驗身分後辦理。 ● 填寫相關申請書與服務約定條款。(Level 1) ● 身分證為可靠來源提供，為客觀存在。(Level 2) ● 申請人攜帶身分證並經戶役政資料庫查驗。(Level 3) ● 法人戶書面同意由法人戶指定人員核驗身分後辦理。(Level 4) ● 臨櫃辦理經人工查驗。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件,或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	安全載具(如動態密碼產生器) ● 信物遵循金融機構相關政策與作業流程。(Level 1) ● 信物交付：親自交付。(Level 2) ● 信物啟用:由申請人依據密碼單上密碼於期限內進行啟用，並作為驗證個體和信物關聯性。(Level 3) ● 信物簽收及保存：相關簽收與保存立約於服務約定條款，完成申請或簽署則視為經申請人同意。(Level 4) ● 信物展期、更換：使用期限到期須臨櫃重新辦理。(Level 4) ● 安全載具應具備資料輸出管控機制、遮蔽作用之塗層保護	■Level 1:信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施(如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收	Level 4

	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機敏資訊之安全設計。(Level 4)、(不符合Level 5)	及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA4		

五、以法人高風險憑證為例－具密碼保護之安全元件(SE)、可信賴執行環境(TEE)為例

階段	評分原因	評分	評等結果
身分登錄	限法人戶並應於臨櫃辦理或書面同意由法人戶指定人員核驗身分後辦理。 ● 填寫相關申請書與服務約定條款。(Level 1) ● 身分證為可靠來源提供，為客觀存在。(Level 2) ● 申請人攜帶身分證並經戶役政資料庫查驗。(Level 3) ● 法人戶書面同意由法人戶指定人員核驗身分後辦理。(Level 4) ● 臨櫃辦理經人工查驗。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	應採用於具密碼保護之安全元件(Secure Element)、可信賴執行環境(Trusted Execution Environment)，以保護機敏資訊，並遵循下列安全設計		
	● 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。(Level 5) 信物管理政策及信物交付、啟用、更換與展期等流程，應依實務作業評估所達之保證等級，此處僅先針對安全元件應符合之防竄改硬體裝置規格評估達Level 5中其中一項因素評估。 ● 不具「電子簽章法」之不可否認性。(不符合Level 5)	■Level 1:信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施(如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分	Level 4 (SE)

		核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
	● 可信賴執行環境應符合 Global Platform 標準或其他相同安全強度之認證。（具硬體安全防護性，但強度依各廠商實作之硬體架構而有差異。）(Level 4) 信物管理政策及信物交付、啟用、更換與展期等流程，應依實務作業評估所達保證等級進行評估，此處僅先針對可信賴執行環境應符合之防竄改硬體裝置規格評估達 Level 4 中其中一項因素評估。	■Level 1:信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施(如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯	Level 4（TEE）

		出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	SE：LoA4、TEE：LoA4		

六、以法人高風險憑證為例－行動裝置應用程式為例

階段	評分原因	評分	評等結果
身分登錄	限法人戶並應於臨櫃辦理或書面同意由法人戶指定人員核驗身分後辦理。 ● 填寫相關申請書與服務約定條款。（Level 1） ● 身分證為可靠來源提供，為客觀存在。（Level 2） ● 申請人攜帶身分證並經戶役政資料庫查驗。（Level 3） ● 法人戶書面同意由法人戶指定人員核驗身分後辦理。（Level 4） ● 臨櫃辦理經人工查驗。（Level 5）	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	應增強行動裝置應用程式軟硬體設備之防護機制，以保護機敏資訊，並遵循下列安全設計： ● 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機敏資訊之安全設計。 一、防入侵機制：避免使用疑似遭破解的行動裝置、確保 App 完整性、確保函式庫完整性、防止螢幕遭覆蓋、確保逆向工程無法取得重要機敏資料。 二、執行期間保護機制：防止應用程式被打包或監聽、防止執行未授權程式碼、防止使用螢幕快照或延伸螢幕、防止於模擬器上執行、如偵錯模式應提示使用者注意風險。 三、機敏資料保護機制：保護記憶體參數及儲存檔案、使用設備保護金鑰、防止設備被複製。	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態）、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機	Level 4

	經上述第十五條要求以符合具防竄改保護措施且具備竄改檢測機制。(Level 4) 信物管理政策及信物交付、啟用、更換與展期等流程，應依實務作業評估所達之保證等級，此處僅先針對行動裝置應用程式應符合之防竄改保護措施評估達 Level 4 中其中一項因素評估。	制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA4		

七、以 C3 軟體憑證為例

階段	評分原因	評分	評等結果
身分登錄	**<u>應依據銀行實際辦理作業進行評估</u>。** <u>若銀行實務規定以**晶片金融卡**申請銀行核發之 C3 軟體憑證：</u> ● 法人高風險：Level 4 ● 臨櫃辦理：Level 4 ● 數存一高：Level 4 ● 數存一低：Level 3 ● 數存二：Level 3 ● 數存三:①(連結本人之金融支付工具或電信認證):Level 1、②(跨行金融帳戶資訊核驗):Level 2、③(跨行金融帳戶資訊核驗+視訊):Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件,或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	・法人：Level 4 ・臨櫃：Level 4 ・數存一高:Level 4 ・數存一低:Level 3 ・數存二：Level 3 ・數存三： ① Level 1、 ② Level 2、 ③ Level 3
信物管理	● 信物政策與作業流程：遵循經銀行公會核准之憑證管理中心憑證實務作業基準。(Level 1) ● 信物交付：金融機構檢核申請人憑證管理中心回覆訊息的正確性、完整性與有效性，並確認申請人憑證記載之資訊正確無誤後，將用戶憑證傳送予申請人。(Level 2) ● 應採用金融 XML 憑證、C3 憑證或非對稱性加解密系統(如 PGP)。(Level 2) ● 信物啟用：確認憑證內容的申請人相關資訊與申請人註冊時的一致，且為申請人本人之正確資訊。(Level 3)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態）、信物更換或展期	Level 3

	● 私鑰經對稱或非對稱加密保護，以確保金鑰儲存安全，且由私鑰進行憑證之數位簽章保護，以達防竄改保護措施。(Level 3) ● TWCA 之軟體憑證載體均通過第三方專家檢測，金鑰妥適保管且無已知之弱點。(Level 3) ● 信物展期：不提供憑證展期。(Level 4) ● 信物更換：不接受用戶進行憑證變更，如用戶之識別資訊或其他記載於憑證之資訊須變更時應依規定廢止憑證後，重新申請憑證簽發。 (Level 4) ● 未達採用信物具防竄改保護措施且具備竄改檢測機制(不符合 Level 4)	依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA3、LoA2(數存三②)、LoA1(數存三①)		

註：原先採用金融 XML 軟體憑證、C3 軟體憑證為低信賴等級，經 ISO 29115 原則評估後，調整為中信賴等級(須具第三方專家檢測，並出具報告)、低信賴等級或最低信賴等級。

八、以 FXML 軟體憑證為例

階段	評分原因	評分	評等結果
身分登錄	● 金融機構向申請人詳細說明業務應用系統憑證使用，及申請單與合約書上之權利與義務規範，相關業務運作的作業流程與提供使用說明與操作文件，經申請人同意並確認。(Level 1) ● 金融機構驗證申請人所提示之身分與證明文件(如身分證)。(Level 2) ● 申請人提示身分證並經信任機構驗證。(Level 3) ● 由申請人提示第二個不同可靠來源資料。 (Level 4) ● 臨櫃辦理經人工查驗。 (Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	● 信物政策與作業流程:遵循經銀行公會核准之憑證管理中心憑證實務作業基準。 (Level 1) ● 信物啟用:申請人至少經過身分識別碼及密碼的檢核驗證確認關聯性，登入至註冊中心，將產生的憑證申請訊息經由申請人私密金鑰簽章後傳送至註冊中心。(Level 2)、(Level 3) ● 應採用金融XML憑證、C3憑證或非對稱性加解密系統(如PGP)。(Level 2) ● 私鑰經對稱或非對稱加密保護，以確保金鑰儲存安全，且由私鑰進行憑證之數位簽章保護，以達防竄改保護措施。(Level 3) ● TWCA 之軟體憑證載體均通過第三方專家檢測，金鑰妥適保管且無已知之弱點。(Level 3)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄	Level 3

	● 信物展期、更換：不提供憑證展期；憑證更新由憑證用戶遵照 FUCA 與註冊中心的業務需求與作業規範辦理，憑證系統如有配合業務系統安全性管控的需求時，則不提供憑證更新之功能，憑證用戶必須重新產生新金鑰對，才可向 FUCA 申請憑證簽發。（Level 3） ● 信物啟用只允許在指定時間內完成。(Level 4) ● 信物簽收及保存須經申請人同意：憑證使用之範圍依作業基準、憑證申請人與 FUCA 之合約中規定，憑證用戶使用憑證時，憑證用戶必須妥善保管及儲存與憑證相關之私密金鑰，避免遺失、曝露、被竄改或為第三者任意使用或竊用。(Level 4) ● 未達採用信物具防竄改保護措施且具備竄改檢測機制。（不符合 Level 4）	進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA3		

註：原先採用金融 XML 軟體憑證、C3 軟體憑證為低信賴等級，經 ISO 29115 原則評估後，調整為中信賴等級(須具第三方專家檢測，並出具報告）、低信賴等級或最低信賴等級。

九、以法人晶片金融卡為例

階段	評分原因	評分	評等結果
身分登錄	應於臨櫃辦理或書面同意由法人戶指定人員核驗身分後辦理。 ● 金融機構依據相關開戶契約書訂定申請作業相關聲明與申請人須臨櫃簽署以表示理解與同意。(Level 1) ● 代表人身分證及第二證件為可靠機構來源提供，為客觀存在。 (Level 2) ● 代表人提示身分證並經信任機構驗證。 (Level 3) ● 法人戶經書面同意由其指定人員申請，經核驗後辦理。(Level 4) ● 於臨櫃辦理經人工查驗。 (Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	● 信物政策與作業流程：依金融機構晶片金融卡作業流程。(Level 1) ● 信物啟用：信物經申請人啟用。(Level 1) ● 信物交付：信物經本人臨櫃領取或掛號簽收。(Level 2) ● 信物啟用過程透過預設密碼驗證關聯性。(Level 3) ● 信物更換:臨櫃申請:國民身分證及原留印鑑;ATM/eATM 申請：晶片金融卡登入；線上申請，臨櫃出示身分證查驗領取。 (Level 4) ● 信物啟用僅允許在指定時間內完成。 (Level 4) ● 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	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進	Level 4

	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。(Level 5) ● 不具「電子簽章法」之不可否認性。(不符合 Level 5)	行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA4		

十、以臨櫃及數存一高風險晶片金融卡為例

階段	評分原因	評分	評等結果
身分登錄	臨櫃申辦帳戶： ● 各銀行依據相關開戶契約書訂定申請作業相關聲明與申請人須臨櫃簽署以表示理解與同意。(Level 1) ● 雙證件為可靠來源提供，為客觀存在。(Level 2) ● 提示身分證並經信任機構驗證。(Level 3) ● 申請人提示第二個不同可靠來源資料，做為身分資料之補強。(Level 4) ● 於臨櫃辦理經人工查驗。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(Level 2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人客戶經書面同意由法人客戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
	數存一高風險帳戶： ● 各金融機構依據「個人網路銀行業務服務定型化契約範本」訂定申請作業相關聲明與申請人須臨櫃簽署或線上勾選同意以表示理解與同意。(Level 1) ● 插卡驗證自然人憑證，足以表示其身分客觀存在，所提示為可靠來源之資料，該資料已由申請人向該第三方註冊單位(可靠來源)進行註冊(Level 2)，並採自然人憑證依照該信物之驗證規範經信任機構進行驗證(Level 3)。 ● 內政部作為法定最高發證主管機關，採用其所核發之身分證明文件或信物(自然人憑證(LoA4))，做為核發之其他信物申請時之身分證明查驗，基於信賴其權威性與合法性，可不再	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 4

	提示第二可靠來源資料做為補強。(Level 4) ● 非經 VTM 進行人工查驗。(不符合 Level 5)		
信物管理	● 信物政策與作業流程：依金融機構晶片金融卡作業流程。(Level 1) ● 信物啟用：信物經申請人啟用。(Level 1) ● 信物交付：信物經本人臨櫃領取或掛號簽收。(Level 2) ● 信物啟用過程透過預設密碼驗證關聯性。(Level 3) ● 信物更換：臨櫃申請：國民身分證及原留印鑑；ATM/eATM 申請：晶片金融卡登入；線上申請，臨櫃出示身分證查驗領取。(Level 4) ● 信物啟用僅允許在指定時間內完成。 (Level 4) ● 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。(Level 5) ● 不具「電子簽章法」之不可否認性。(不符合 Level 5)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態）、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	Level 4
總結	LoA4		

十一、 以數存一低風險及數存二晶片金融卡為例

階段	評分原因	評分	評等結果
身分登錄	● 各銀行依據「個人網路銀行業務服務定型化契約範本」訂定申請作業相關聲明與申請人須臨櫃簽署或線上勾選同意以表示理解與同意。(Level 1) 數存一低： ● 插卡驗證自然人憑證，足以表示其身分客觀存在，所提示為可靠來源之資料，該資料已由申請人向該第三方註冊單位(可靠來源)進行註冊(Level 2)，並採自然人憑證依照該信物之驗證規範經信任機構進行驗證(Level 3)。 ● 內政部作為法定最高發證主管機關，採用其所核發之身分證明文件或信物(自然人憑證(LoA4))，做為核發之其他信物申請時之身分證明查驗，基於信賴其權威性與合法性，可不再提示第二可靠來源資料做為補強。(Level 4) ✓ 此處雖評估等級已達 Level 4，考量一般業務委員會評估認為數存一低實務上身分登錄之強度與數存二身分登錄強度相同，故經一般業務委員會建議以 Level 3 作為最後身分登錄評估結果。	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	數存一低：Level 3

	● 各銀行依據「個人網路銀行業務服務定型化契約範本」訂定申請作業相關聲明與申請人須臨櫃簽署或線上勾選同意以表示理解與同意。(Level 1) 數存二： ● 透過驗證自行臨櫃申辦之帳戶資訊，申請人之身分經可靠來源(自行)提供，足以表示其身分客觀存在(Level 2)，並經信任機構驗證(Level 3)。	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供,客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	數存二：Level 3

信物管理	● 信物政策與作業流程：依金融機構晶片金融卡作業流程。(Level 1) ● 信物啟用：信物經申請人啟用。(Level 1) ● 信物交付：信物經本人臨櫃領取或掛號簽收。(Level 2) ● 信物啟用過程透過預設密碼驗證關聯性。(Level 3) ● 信物更換：臨櫃申請：國民身分證及原留印鑑；ATM/eATM 申請：晶片金融卡登入；線上申請，臨櫃出示身分證查驗領取。(Level 4) ● 信物啟用僅允許在指定時間內完成。(Level 4) ● 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。(Level 5) ● 不具「電子簽章法」之不可否認性。(不符合 Level 5)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態）、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	Level 4
總結	LoA3		

十二、 以數存三晶片金融卡為例

階段	評分原因	評分	評等結果
身分登錄	● 各銀行依據「 個人網路銀行業務服務定型化契約範本」訂定申請作業相關聲明與申請人須臨櫃簽署或線上勾選同意以表示理解與同意。(Level 1) 依「銀行受理客戶以網路方式開立數位存款帳戶作業範本」受理開立第三類帳戶： ● ①應採用連結本人之金融支付工具(存款帳戶、信用卡或其他經主管機關認定金融支付工具)或電信認證機制。所提示之可靠來源之資料，如信用卡、電信認證機制（此處之電信認證非屬銀行舊客戶），本身信賴等級未達 LoA2 或經政府機關核准之身分證明文件，故此處身分登錄不滿足 Level 2。(不符合 Level 2) ● ②透過他行臨櫃申辦之帳戶資訊，並經跨行金融帳戶資訊核驗機制驗證，申請人之身分經可靠來源(銀行)提供，本身信賴等級達 LoA2 以上，足以表示其身分客觀存在(Level 2)。 ● ③跨行金融帳戶資訊核驗+視訊，參照「視訊會議－手機或平板裝置」結果：Level 3。(Level 3)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	①(連結本人之金融支付工具或電信認證):Level 1 ②(跨行金融帳戶資訊核驗):Level 2 ③(跨行金融帳戶資訊核驗+視訊):Level 3

信物管理	● 信物政策與作業流程：依金融機構晶片金融卡作業流程。(Level 1) ● 信物啟用：信物經申請人啟用。(Level 1) ● 信物交付：信物經本人臨櫃領取或掛號簽收。(Level 2) ● 信物啟用過程透過預設密碼驗證關聯性。(Level 3) ● 信物更換：臨櫃申請：國民身分證及原留印鑑；ATM/eATM申請：晶片金融卡登入；線上申請，臨櫃出示身分證查驗領取。 (Level 4) ● 信物啟用僅允許在指定時間內完成。 (Level 4) ● 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。(Level 5) ● 不具「電子簽章法」之不可否認性。(不符合 Level 5)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態）、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	Level 4
總結	①(連結本人之金融支付工具或電信認證): LoA1 ②(跨行金融帳戶資訊核驗): LoA2 ③(跨行金融帳戶資訊核驗+視訊): LoA3		

十三、 以法人高風險 OTP－安全載具(如動態密碼產生器)為例

階段	評分原因	評分	評等結果
身分登錄	限法人戶並應於臨櫃辦理或書面同意由法人戶指定人員核驗身分後辦理。 ● 填寫相關申請書與服務約定條款，以表示理解與同意。(Level 1) ● 身分證為可靠來源提供，為客觀存在。(Level 2) ● 申請人攜帶身分證並經戶役政資料庫查驗。(Level 3) ● 書面同意由其指定人員申請，經核驗後辦理。(Level 4) ● 臨櫃辦理經人工查驗。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	安全載具(如動態密碼產生器) ● 信物遵循金融機構相關政策與作業流程。(Level 1) ● 信物交付：親自交付。(Level 2) ● 信物啟用：由申請人依據密碼單上密碼於期限內進行啟用，並作為驗證個體和信物關聯性。(Level 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機敏資訊之安全設計。(符合 Level 4)、(不符合 Level 5) ● 信物簽收及保存：相關簽收與保存立約於服務約定條款，完成申請或簽署則視為經申請人同意。(Level 4)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄	Level 4

	● 信物展期、更換：使用期限到期須臨櫃重新辦理。(Level 4)	進行身分核驗。TEE、安全載具、行動裝置做為信物，符合Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA4		

十四、 以法人高風險 OTP－具密碼保護之安全元件(SE)、可信賴執行環境(TEE)為例

階段	評分原因	評分	評等結果
身分登錄	限法人戶並應於臨櫃辦理或書面同意由法人戶指定人員核驗身分後辦理。 ● 填寫相關申請書與服務約定條款，以表示理解與同意。(Level 1) ● 身分證為可靠機構來源提供，為客觀存在。(Level 2) ● 申請人攜帶身分證並經戶役政資料庫查驗。(Level 3) ● 書面同意由其指定人員申請，經核驗後辦理。(Level 4) ● 臨櫃辦理經人工查驗。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
信物管理	應採用於具密碼保護之安全元件(Secure Element)、可信賴執行環境(Trusted Execution Environment)，以保護機敏資訊，並遵循下列安全設計 ● 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。(Level 5) 信物管理政策及信物交付、啟用、更換與展期等流程，應依實務作業評估所達之保證等級，此處僅先針對安全元件應符合之防竄改硬體裝置規格評估達 Level 5 中其中一項因素評估。	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄	Level 4 (SE)

	● 不具「電子簽章法」之不可否認性。(不符合 Level 5)	進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
	● 可信賴執行環境應符合 Global Platform 標準或其他相同安全強度之認證。（具硬體安全防護性，但強度依各廠商實作之硬體架構而有差異。）(Level 4) 信物管理政策及信物交付、啟用、更換與展期等流程，應依實務作業評估所達之保證等級，此處僅先針對可信賴執行環境應符合之防竄改硬體裝置規格評估達 Level 4 中其中一項因素評估。	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法	Level 4 (TEE)

		匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA4		

十五、 以法人高風險 OTP－行動裝置應用程式為例

階段	評分原因	評分	評等結果
身分登錄	限法人戶並應於臨櫃辦理或書面同意由法人戶指定人員核驗身分後辦理。 ● 填寫相關申請書與服務約定條款，以表示理解與同意。(Level 1) ● 身分證為可靠機構來源提供，為客觀存在。(Level 2) ● 申請人攜帶身分證並經戶役政資料庫查驗。(Level 3) ● 書面同意由其指定人員申請，經核驗後辦理。(Level 4) ● 臨櫃辦理經人工查驗。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5

信物管理	應增強防護機制之行動裝置應用程式軟硬體設備，以保護機敏資訊，並遵循下列安全設計： ● 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機敏資訊之安全設計。 一、防入侵機制：避免使用疑似遭破解的行動裝置、確保 App 完整性、確保函式庫完整性、防止螢幕遭覆蓋、確保逆向工程無法取得重要機敏資料。 二、執行期間保護機制：防止應用程式被打包或監聽、防止執行未授權程式碼、防止使用螢幕快照或延伸螢幕、防止於模擬器上執行、如偵錯模式應提示使用者注意風險。 三、機敏資料保護機制：保護記憶體參數及儲存檔案、使用設備保護金鑰、防止設備被複製。 經上述第十五條要求以符合具防竄改保護措施且具備竄改檢測機制。(Level 4) 信物管理政策及信物交付、啟用、更換與展期等流程，應依實務作業評估所達之保證等級，此處僅先針對行動裝置應用程式應符合之防竄改保護措施評估達 Level 4 中其中一項因素評估。	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 ■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	Level 4
總結	LoA4		

十六、 以簡訊或軟體 OTP 為例

階段	評分原因	評分	評等結果
身分登錄	應於臨櫃辦理或依據第一類(不含限適用第六條低風險交易)數位存款帳戶、適用第六條低風險交易之第一類數位存款帳戶或第二類數位存款帳戶開戶程序核驗身分後辦理。 臨櫃申辦帳戶： ● 參照「臨櫃晶片金融卡」身分登錄之評估為 Level 5	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	臨櫃：Level 5
	數存一高風險帳戶： ● 參照「數存一高風險晶片金融卡」身分登錄之評估為 Level 4	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	數存一高：Level 4

	數存一低風險帳戶： ● 參照「數存一低風險晶片金融卡」身分登錄之評估為 Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	數存一低： Level 3
	數存二： ● 參照「數存二晶片金融卡」身分登錄之評估為 Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	數存二： Level 3

信物管理	● 信物包含 OTP、產生 OTP 之金鑰、傳輸通道、接收載體或裝置，構成一整個信物。共同確保 OTP 的傳遞、接收和使用之安全性。 ● 信物遵循金融機構相關政策與作業流程。(Level 1) ● 信物交付：確認手機號碼或裝置綁定進行一次性密碼發送或推播等，以檢查交付方式與該申請人合理關聯。(Level 2) ● 用於產生一次性密碼之金鑰應依據第五條訊息傳輸方式辦理，於網際網路(Internet)上傳輸個人資訊、身分識別資訊、身分核驗資訊或機敏資訊應採用第四條第一款訊息加密機制(Level 2)。除應符合第五條訊息傳輸外，應對 OTP 設有防護機制，例如最少位數、有效時限、錯誤次數失效等。 ● 信物啟用：申請時確認留存本行手機號碼後，發送交易驗證碼並輸入後，完成申請與啟用流程，作為驗證個體和信物關聯性。(Level 3) ● 信物不具防竄改保護措施。(不符合 Level 3)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	Level 2
總結	LoA2		

註：原先一次性密碼適用於臨櫃辦理、或依據第一類(不含限適用第六條低風險交易)數位存款帳戶、適用第六條低風險交易之第一類數位存款帳戶或第二類數位存款帳戶者，為中信賴等級。經依據 ISO 29115 原則評估後，推播 OTP 及語音 OTP 為中信賴等級；簡訊 OTP 及軟體 OTP 為低信賴等級。

十七、 以簡訊或軟體 OTP（線上辦理貸款之純貸戶）為例

階段	評分原因	評分	評等結果
身分登錄	線上辦理貸款之純貸戶： ● 填寫相關貸款總約定書，申請人簽署以表示理解與同意。(Level 1) ● 上傳身分證影本，無法透過公開且客觀方式檢驗其真偽。(不符合 Level 2)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 □Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 □Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 1
信物管理	● 信物包含 OTP、產生 OTP 之金鑰、傳輸通道、接收載體或裝置，構成一整個信物。共同確保 OTP 的傳遞、接收和使用之安全性。 ● 信物遵循金融機構相關政策與作業流程。(Level 1) ● 信物交付：確認手機號碼或裝置綁定進行發送或推播，以檢查交付方式與該申請人合理關聯。(Level 2) ● 用於產生一次性密碼之金鑰應依據第五條訊息傳輸方式辦理，於網際網路(Internet)上傳輸個人資訊、身分識別資訊、身分核驗資訊或機敏資訊應採用第四條第一款訊息加密機制(Level 2)。除應符合第五條訊息傳輸外，應對 OTP 設有防護機制，例如最少位數、有效時限、錯誤次數失效等。 ● 信物啟用：申請時確認留存本行手機號碼後，發送交易驗證碼	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄	Level 2

	並輸入後，完成申請與啟用流程，作為驗證個體和信物關聯性。(Level 3) ● 信物不具防竄改保護措施。(不符合 Level 3)	進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA1		

註：依據金管銀國字第 1120202881 號函文，有關採用安控基準第七條低信賴等級機制之安全設計，以應用於該機制身分登錄時採用的核身機制為原則，例如：以信用卡核身申請之一次性密碼原則應用於該信用卡業務、以第三類數位存款帳戶核身申請之兩項以上技術原則應用於該帳戶之金融業務。

十八、 以簡訊或軟體 OTP（數存三）為例

階段	評分原因	評分	評等結果
身分登錄	數存三： ● 參照「數存三晶片金融卡」身分登錄之評估 依「銀行受理客戶以網路方式開立數位存款帳戶作業範本」受理開立第三類帳戶： ● ①(連結本人之金融支付工具或電信認證): Level 1 ● ②(跨行金融帳戶資訊核驗): Level 2 ● ③(跨行金融帳戶資訊核驗+視訊): Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	①(連結本人之金融支付工具或電信認證):Level 1 ②(跨行金融帳戶資訊核驗):Level 2 ③(跨行金融帳戶資訊核驗+視訊):Level 3
信物管理	● 信物包含 OTP、產生 OTP 之金鑰、傳輸通道、接收載體或裝置，構成一整個信物。共同確保 OTP 的傳遞、接收和使用之安全性。 ● 信物遵循金融機構相關政策與作業流程。(Level 1) ● 信物交付：確認手機號碼或裝置綁定進行發送或推播，以檢查交付方式與該申請人合理關聯。(Level 2) ● 用於產生一次性密碼之金鑰應依據第五條訊息傳輸方式辦理，於網際網路(Internet)上傳輸個人資訊、身分識別資訊、身分核驗資訊或機敏資訊應採用第四條第一款訊息加密機	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4:保存信物之軟硬體設備具防竄改保護措施	Level 2

	制(Level 2)。除應符合第五條訊息傳輸外，應對 OTP 設有防護機制，例如最少位數、有效時限、錯誤次數失效等。 ● 信物啟用：申請時確認留存本行手機號碼後，發送交易驗證碼並輸入後，完成申請與啟用流程，作為驗證個體和信物關聯性。 (Level 3) ● 信物不具防竄改保護措施。(不符合 Level 3)	且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	①(連結本人之金融支付工具或電信認證): LoA1 ②(跨行金融帳戶資訊核驗): LoA2 ③(跨行金融帳戶資訊核驗+視訊): LoA2		

註：

1. 依據金管銀國字第 1120202881 號函文，有關採用安控基準第七條低信賴等級機制之安全設計，以應用於該機制身分登錄時採用的核身機制為原則，例如：以信用卡核身申請之一次性密碼原則應用於該信用卡業務、以第三類數位存款帳戶核身申請之兩項以上技術原則應用於該帳戶之金融業務。
2. 原先一次性密碼適用於第三類數位存款帳戶，為低信賴等級。經依據 ISO 29115 原則評估後，簡訊 OTP 及軟體 OTP 為最低信賴等級或低信賴等級。

十九、 以簡訊或軟體OTP（信用卡）為例

階段	評分原因	評分	評等結果
身分登錄	依信用卡業務機構管理辦法核發信用卡並核驗身分後辦理。 ● 參照「信用卡資訊」之身分登錄之評估：Level 1	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 □Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 □Level 3：由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4:由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 1
信物管理	● 信物包含OTP、產生OTP之金鑰、傳輸通道、接收載體或裝置，構成一整個信物。共同確保OTP的傳遞、接收和使用之安全性。 ● 信物遵循金融機構相關政策與作業流程。(Level 1) ● 信物交付：確認手機號碼或裝置綁定進行發送或推播，以檢查交付方式與該申請人合理關聯。(Level 2) ● 用於產生一次性密碼之金鑰應依據第五條訊息傳輸方式辦理，於網際網路(Internet)上傳輸個人資訊、身分識別資訊、身分核驗資訊或機敏資訊應採用第四條第一款訊息加密機制(Level 2)。除應符合第五條訊息傳輸外，應對OTP設有防護機制，例如最少位數、有效時限、錯誤次數失效等。	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等),且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進	Level 2

	● 信物啟用：申請時確認留存本行手機號碼後，發送交易驗證碼並輸入後，完成申請與啟用流程，作為驗證個體和信物關聯性。（Level 3） ● 信物不具防竄改保護措施。(不符合 Level 3)	行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA1		

註：依據金管銀國字第 1120202881 號函文，有關採用安控基準第七條低信賴等級機制之安全設計，以應用於該機制身分登錄時採用的核身機制為原則，例如：以信用卡核身申請之一次性密碼原則應用於該信用卡業務、以第三類數位存款帳戶核身申請之兩項以上技術原則應用於該帳戶之金融業務。

二十、 以語音或推播 OTP 為例

階段	評分原因	評分	評等結果
身分登錄	應於臨櫃辦理或依據第一類(不含限適用第六條低風險交易)數位存款帳戶、適用第六條低風險交易之第一類數位存款帳戶或第二類數位存款帳戶開戶程序核驗身分後辦理。 臨櫃申辦帳戶： ● 參照「臨櫃晶片金融卡」身分登錄之評估為 Level 5	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	臨櫃：Level 5
	數存一高風險帳戶： ● 參照「數存一高風險晶片金融卡」身分登錄之評估為 Level 4	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(Level 3 或經申請人機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	數存一高：Level 4

	數存一低風險帳戶： ● 參照「數存一低風險晶片金融卡」身分登錄之評估為 Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	數存一低： Level 3
	數存二： ● 參照「數存二晶片金融卡」身分登錄之評估為 Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	數存二： Level 3
信物管理	● 信物包含 OTP、產生 OTP 之金鑰、傳輸通道、接收載體或裝置，構成一整個信物。共同確保 OTP 的傳遞、接收和使用之安全性。 ● 信物遵循金融機構相關政策與作業流程。(Level 1)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該	Level 3

	● 信物交付：確認手機號碼或裝置綁定進行發送或推播，以檢查交付方式與該申請人合理關聯。(Level 2) ● 語音、推播 OTP：用於產生一次性密碼之金鑰應依據第五條訊息傳輸方式辦理，於網際網路(Internet)上傳輸個人資訊、身分識別資訊、身分核驗資訊或機敏資訊應採用第四條第一款訊息加密機制(Level 2)。除應符合第五條訊息傳輸外，應對 OTP 設有防護機制，例如最少位數、有效時限、錯誤次數失效等。 ● 防竄改保護措施：現行語音通話技術，如 VoLTE、VoNR 和 VoIP，廣泛採用 SRTP 加密協議，有效降低通話內容被竊聽或遭竄改的風險。針對推播 OTP 的場景，若採用 TLS 等加密協議，可確保傳輸過程的安全性，並將 OTP 安全地推送至指定用戶的 App 進行接收，進一步提升整體保護效果。(Level 3) ● 信物啟用：申請時確認留存本行手機號碼後，發送交易驗證碼並輸入後，完成申請與啟用流程，作為驗證個體和信物關聯性。 (Level 3)	申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA3		

二十一、　以語音或推播 OTP（數存三）為例

階段	評分原因	評分	評等結果
身分登錄	數存三： ● 參照「數存三晶片金融卡」身分登錄之評估 依「銀行受理客戶以網路方式開立數位存款帳戶作業範本」受理開立第三類帳戶： ● ①(連結本人之金融支付工具或電信認證): Level 1 ● ②(跨行金融帳戶資訊核驗): Level 2 ● ③(跨行金融帳戶資訊核驗+視訊): Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	①(連結本人之金融支付工具或電信認證):Level 1 ②(跨行金融帳戶資訊核驗):Level 2 ③(跨行金融帳戶資訊核驗+視訊):Level 3
信物管理	● 信物包含 OTP、產生 OTP 之金鑰、傳輸通道、接收載體或裝置，構成一整個信物。共同確保 OTP 的傳遞、接收和使用之安全性。 ● 信物遵循金融機構相關政策與作業流程。(Level 1) ● 信物交付：確認手機號碼或裝置綁定進行發送或推播，以檢查交付方式與該申請人合理關聯。(Level 2) ● 語音、推播 OTP：用於產生一次性密碼之金鑰應依據第五條訊息傳輸方式辦理，於網際網路(Internet)上傳輸個人資訊、身分識別資訊、身分核驗資訊或機敏資訊應採用第四條第一款訊	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等),且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。	Level 3

	息加密機制(Level 2)。除應符合第五條訊息傳輸外，應對 OTP 設有防護機制，例如最少位數、有效時限、錯誤次數失效等。 ● 防竄改保護措施：現行語音通話技術，如 VoLTE、VoNR 和 VoIP，廣泛採用 SRTP 加密協議，有效降低通話內容被竊聽或遭竄改的風險。針對推播 OTP 的場景，若採用 TLS 等加密協議，可確保傳輸過程的安全性，並將 OTP 安全地推送至指定用戶的 App 進行接收，進一步提升整體保護效果。(Level 3) ● 信物啟用：申請時確認留存本行手機號碼後，發送交易驗證碼並輸入後，完成申請與啟用流程，作為驗證個體和信物關聯性。(Level 3)	□Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	①(連結本人之金融支付工具或電信認證): LoA1 ②(跨行金融帳戶資訊核驗): LoA2 ③(跨行金融帳戶資訊核驗+視訊): LoA3		

註：

1. 依據金管銀國字第 1120202881 號函文，有關採用安控基準第七條低信賴等級機制之安全設計，以應用於該機制身分登錄時採用的核身機制為原則，例如：以信用卡核身申請之一次性密碼原則應用於該信用卡業務、以第三類數位存款帳戶核身申請之兩項以上技術原則應用於該帳戶之金融業務。
2. 原先一次性密碼適用於第三類數位存款帳戶，為低信賴等級。經依據 ISO 29115 原則評估後，依據不同戶別申請而來以區分等級。

二十二、　以語音或推播 OTP（信用卡）為例

階段	評分原因	評分	評等結果
身分登錄	**信用卡：** ● 參照「信用卡資訊」身分登錄之評估為 Level 1	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 □Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 □Level 3：由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4:由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 1
信物管理	● 信物包含 OTP、產生 OTP 之金鑰、傳輸通道、接收載體或裝置，構成一整個信物。共同確保 OTP 的傳遞、接收和使用之安全性。 ● 信物遵循金融機構相關政策與作業流程。(Level 1) ● 信物交付：確認手機號碼或裝置綁定進行發送或推播，以檢查交付方式與該申請人合理關聯。(Level 2) ● 語音、推播 OTP：用於產生一次性密碼之金鑰應依據第五條訊息傳輸方式辦理，於網際網路(Internet)上傳輸個人資訊、身分識別資訊、身分核驗資訊或機敏資訊應採用第四條第一款訊息加密機制(Level 2)。除應符合第五條訊息傳輸外，應對 OTP 設有防護機制，例如最少位數、有效時限、錯誤次數失效等。 ● 防竄改保護措施：現行語音通話技術，如 VoLTE、VoNR 和 VoIP，	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進	Level 3

	廣泛採用 SRTP 加密協議，有效降低通話內容被竊聽或遭竄改的風險。針對推播 OTP 的場景，若採用 TLS 等加密協議，可確保傳輸過程的安全性，並將 OTP 安全地推送至指定用戶的 App 進行接收，進一步提升整體保護效果。(Level 3) ● 信物啟用：申請時確認留存本行手機號碼後，發送交易驗證碼並輸入後，完成申請與啟用流程，作為驗證個體和信物關聯性。(Level 3)	行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA1		

註：依據金管銀國字第 1120202881 號函文，有關採用安控基準第七條低信賴等級機制之安全設計，以應用於該機制身分登錄時採用的核身機制為原則，例如：以信用卡核身申請之一次性密碼原則應用於該信用卡業務、以第三類數位存款帳戶核身申請之兩項以上技術原則應用於該帳戶之金融業務。

二十三、　以兩項以上技術為例－臨櫃或 VTM 辦理、法人、數存一高風險帳戶

階段	評分原因	評分	評等結果
身分登錄	參照不同戶別之身分登錄評估： ● 臨櫃或 VTM 辦理：Level 5 ● 法人：Level 5 ● 數存一高：Level 4	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	臨櫃或 VTM 辦理、法人：Level 5 數存一高：Level 4
信物管理	前述兩項以上技術之約定資訊、設備或生物特徵應遵循以下要求。 應採用於具密碼保護之安全元件(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設備，以保護機敏資訊，並遵循下列安全設計： ● 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	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。	Level 4

	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。 ● 可信賴執行環境應符合Global Platform標準或其他相同安全強度之認證。 ● 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機敏資訊之安全設計。 ● 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機敏資訊之安全設計。	■Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA4		

二十四、　以兩項以上技術為例－臨櫃或 VTM 辦理、法人、數存一高風險、數存一低、數存二、數存三③帳戶

階段	評分原因	評分	評等結果
身分登錄	參照不同戶別之身分登錄評估： ● 臨櫃或 VTM 辦理：Level 5 ● 法人：Level 5 ● 數存一高：Level 4 ● 數存一低：Level 3 ● 數存二：Level 3 ● 數存三③(跨行金融帳戶資訊核驗+視訊)：Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	臨櫃或 VTM 辦理、法人：Level 5 數存一高：Level 4 數存一低、數存二、數存三③：Level 3
信物管理	● 應用於電子轉帳交易指示類並以簡訊傳送一次性密碼重新綁定兩項以上技術者，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。	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。	Level 3

		□Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA3		

註：依據金管銀國字第 1120202881 號函文，有關採用安控基準第七條低信賴等級機制之安全設計，以應用於該機制身分登錄時採用的核身機制為原則，例如：以信用卡核身申請之一次性密碼原則應用於該信用卡業務、以第三類數位存款帳戶核身申請之兩項以上技術原則應用於該帳戶之金融業務。

二十五、　以兩項以上技術為例－數存三②帳戶

階段	評分原因	評分	評等結果
身分登錄	參照不同戶別之身分登錄評估： ● 數存三②(跨行金融帳戶資訊核驗)：Level 2	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 □Level 3：由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	數存三②：Level 2
信物管理	● 應用於電子轉帳交易指示類並以簡訊傳送一次性密碼重新綁定兩項以上技術者，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。	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物	Level 3

		簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA2		

註：依據金管銀國字第 1120202881 號函文，有關採用安控基準第七條低信賴等級機制之安全設計，以應用於該機制身分登錄時採用的核身機制為原則，例如：以信用卡核身申請之一次性密碼原則應用於該信用卡業務、以第三類數位存款帳戶核身申請之兩項以上技術原則應用於該帳戶之金融業務。

二十六、　以兩項以上技術為例－數存三①帳戶、信用卡戶

階段	評分原因	評分	評等結果
身分登錄	參照不同戶別之身分登錄評估： ● 數存三①(連結本人之金融支付工具或電信認證)：Level 1 ● 依信用卡業務機構管理辦法核發信用卡：Level 1	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 □Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 □Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 1
信物管理	● 應用於電子轉帳交易指示類並以簡訊傳送一次性密碼重新綁定兩項以上技術者，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。	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。	Level 3

		□Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA1		

註：依據金管銀國字第 1120202881 號函文，有關採用安控基準第七條低信賴等級機制之安全設計，以應用於該機制身分登錄時採用的核身機制為原則，例如：以信用卡核身申請之一次性密碼原則應用於該信用卡業務、以第三類數位存款帳戶核身申請之兩項以上技術原則應用於該帳戶之金融業務。

二十七、　以視訊會議－VTM 為例

階段	評分原因	評分	評等結果
身分登錄	● 各銀行依據相關開戶契約書訂定申請作業相關聲明並經申請人簽署以表示理解與同意。(Level 1) ● 申請人出示國民身分證，透過 VTM 身分證辨識要項之模組進行真偽辨識，以確認其客觀存在。(Level 2) ● 提示經內政部核發之身分證，並經 Z21 查驗身分證有效性。(Level 3) ● 申請人提示第二證件如健保卡做為身分證之補強。(Level 4) ● 透過 VTM 視為類臨櫃之人工查驗後辦理。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	Level 5
額外控管要求	應符合**「金融機構辦理多功能視訊櫃檯(VTM)作業自律規範」**之要求。例如， (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，應遵循下列要求： 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(至少符合 FIPS 140-2 Level 3 或同等規格以上)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。 滿足以上要求，可視為符合信物管理之高保證等級 Level 4
總結	LoA4

二十八、　以視訊會議－手機或平板裝置為例

階段	評分原因	評分	評等結果
身分登錄	● 登入系統並勾選同意金融機構相關視訊服務約定事項條款，以表示理解與同意。（Level 1） ● 申請人提示相關身分資訊，且此身分資訊為可靠來源提供。例如，透過留存於本行臨櫃手機號碼接收簡訊 OTP，申請人之身分訊息經可靠來源(銀行)提供，以表示其客觀存在；或提示透過 Mydata 平台之個人身分資訊，該身分資訊經可靠來源(銀行或政府機關等)提供；或透過 ATM 申辦視訊服務等可確認申請人身分資訊經可靠來源提供之措施(由銀行進行評估身分資訊經可靠來源提供之措施)。（Level 2） ● 連線視訊客服進行人臉及身分證查驗。若透過 ATM 申辦視訊服務，插入晶片金融卡經信任機構驗證。(Level 3)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 3
額外控管措施	應符合以下之要求： (1) 採用客戶行動裝置者，應符合「金融機構提供行動裝置應用程式作業規範」。 (2) 採用銀行提供裝置者(如平板、電腦、行動裝置)，應符合「金融機構資通安全防護基準」。 (3) 應導入機制協助確認真人及本人，以防止透過科技預先錄製影片、製作面具、模擬影像或深度偽造(deepfake)等機制偽冒身分。 滿足以上要求，可視為符合信物管理之中保證等級 Level 3		
總結	LoA3		

二十九、　以知識詢問為例

階段	評分原因	評分	評等結果
身分登錄	於臨櫃辦理或依據數位存款帳戶開戶程序核驗身分後辦理： ● 臨櫃辦理：Level 5 ● 數存一高：Level 4 ● 數存一低：Level 3 ● 數存二：Level 3 ● 數存三：①(連結本人之金融支付工具或電信認證):Level 1、②(跨行金融帳戶資訊核驗):Level 2、③(跨行金融帳戶資訊核驗+視訊):Level 3 依信用卡業務機構管理辦法核發信用卡： 依據信用卡資訊之身分登錄評估：Level 1	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	開戶： ・臨櫃：Level 5 ・數存一高：Level 4 ・數存一低：Level 3 ・數存二：Level 3 ・數存三： ① Level 1、 ② Level 2、 ③ Level 3 信用卡戶：Level 1

信物管理	● 信物政策與作業流程：遵循金融機構相關政策與作業流程。(如有，符合 Level 1) ● 信物啟用:信物經申請人自行設定後即啟用。(Level 1) ● 信物交付：申辦帳戶時自建即交付。(Level 2) ● 信物由使用者啟用後並妥善保存，惟信物本身保存於使用者未經加密保護。(不符合 Level 2)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 □Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	Level 1
總結	LoA1		

三十、 以固定密碼為例

階段	評分原因	評分	評等結果
身分登錄	應於臨櫃辦理或依據數位存款帳戶開戶程序核驗身分後辦理。 ● 臨櫃辦理：Level 5 ● 數存一高：Level 4 ● 數存一低：Level 3 ● 數存二：Level 3 ● 數存三：①(連結本人之金融支付工具或電信認證):Level 1、②(跨行金融帳戶資訊核驗):Level 2、③(跨行金融帳戶資訊核驗+視訊):Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	·臨櫃：Level 5 ·數存一高:Level 4 ·數存一低:Level 3 ·數存二：Level 3 ·數存三： ④ Level 1、 ⑤ Level 2、 ⑥ Level 3
信物管理	● 信物政策與作業流程：遵循金融機構相關政策與作業流程。(Level 1) ● 信物啟用：信物經申請人輸入初始密碼並變更或自行設定後啟用。(Level 1) ● 信物交付:申辦帳戶時交付自建或初始密碼。(Level 2) ● 信物由使用者啟用後並妥善保存，惟信物本身保存於使用者未經加密保護。(不符合 Level 2) ● 信物由申請人依據密碼單上密碼於期限內進行啟用，	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 □Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分	Level 1

	或輸入身分證字號、使用者代號、自行設定的初始密碼，作為驗證個體和信物關聯性。（Level 3）	核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA1		

三十一、　以存款帳戶資訊為例

階段	評分原因	評分	評等結果
身分登錄	應於臨櫃辦理或依據數位存款帳戶開戶程序核驗身分後辦理。 ● 臨櫃辦理：Level 5 ● 數存一高：Level 4 ● 數存一低：Level 3 ● 數存二：Level 3 ● 數存三：①(連結本人之金融支付工具或電信認證):Level 1、②(跨行金融帳戶資訊核驗):Level 2、③(跨行金融帳戶資訊核驗+視訊):Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	·臨櫃：Level 5 ·數存一高:Level 4 ·數存一低:Level 3 ·數存二：Level 3 ·數存三： ① Level 1、 ② Level 2、 ③ Level 3
信物管理	● 信物政策與作業流程：遵循金融機構相關政策與作業流程。(Level 1) ● 信物啟用：此處所評估之信物為存款帳戶資訊，故未有信物啟用程序。(Level 1) ● 信物交付：此處所評估之信物為存款帳戶資訊，故未有信物交付程序。(Level 2) ● 信物由使用者啟用後並妥善保存，存款帳戶資訊本身保存於使用者雖未經加密保護，然透過跨行金融帳戶資訊核驗機制，	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載	Level 2

	搭配簡訊發送或推播驗證之傳輸通道應採加密機制，以防止遭中途攔截，故評估其安全性程度達 Level 2 之加密保護。(Level 2)	具但設定為鎖定狀態)、信物更換或展期依身分登錄 Level 2 以上進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA1(數存三①)、LoA2		

三十二、　以信用卡資訊為例

階段	評分原因	評分	評等結果
身分登錄	郵寄申辦信用卡： ● 各金融機構依據相關申請作業，申請人填寫並簽署信用卡申請書，以表示理解與同意。(Level 1) ● 附上身分證正反面影本及相關財力證明文件，備齊後郵寄至金融機構，並電話照會或人工審核，惟無法證明其身分證真偽。(不符合 Level 2)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 □Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 □Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 1
	線上申辦信用卡： 有以下方式進行申辦，包含透過本行信用卡資訊核驗、他行信用卡資訊核驗、本行存款帳戶資訊核驗、他行臨櫃存款帳戶資訊核驗、硬體自然人憑證核驗申辦， 考量以信用卡辦理之情形眾多，無法驗證該信用卡當初申辦時之身分登錄控管與強度，故依信用卡業務機構管理辦法核發信用卡，其身分登錄將比照最低保證等級申辦之信用卡(如郵寄方式辦理)之身分登錄為 Level 1。	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 □Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 □Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經	Level 1

		書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	
信物管理	● 信物政策與作業流程：遵循金融機構相關政策與作業流程。(Level 1) ● 信物啟用：信物經申請人開卡啟用。(Level 1) ● 信物交付:臨櫃申辦親自交付,線上申辦則透過掛號簽收信用卡後得信用卡資訊。(Level 2) ● 信物由使用者啟用後並妥善保存，惟信用卡卡號本身未經加密保護,故取得信用卡資訊後可能透過「信用卡輔助持卡人身分驗證平台」完成驗證。(不符合 Level 2) ● 信物啟用過程輸入卡號、有效期限、開卡密碼，作為驗證個體和信物關聯性。 (Level 3)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 □Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	Level 1
總結	LoA1		

三十三、　以經銀行核驗之電信認證為例

階段	評分原因	評分	評等結果
身分登錄	該門號須經銀行採低信賴等級以上安全設計進行身分驗證。 ● 臨櫃辦理：Level 5 ● 數存一高：Level 4 ● 數存一低：Level 3 ● 數存二：Level 3 ● 數存三：②(跨行金融帳戶資訊核驗):Level 2、③(跨行金融帳戶資訊核驗+視訊):Level 3	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	・臨櫃：Level 5 ・數存一高：Level 4 ・數存一低：Level 3 ・數存二：Level 3 ・數存三： ② Level 2、 ③ Level 3
信物管理	應排除儲值卡、親子卡、預付卡、企業卡等無法辨識本人親辦親簽之門號。 ● 信物政策與作業流程:遵循電信業者相關政策與作業流程。(Level 1) ● 信物啟用：由申請人或電信業者啟用。(Level 1) ● 信物交付：信物經本人臨櫃領取。若為線上申辦，電信業者可透過宅配交付,並經客服連繫確認申請資料與配送地址。 (Level 2)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施(如數位簽章或	Level 2

	● SIM卡採數位簽章對SIM卡內重要資料簽署加密，並儲存於Secure Element安全模組，具有硬體隔離功能，SIM卡實際規格強度依各廠商實作之硬體架構而有差異，尚無法確保達Level 4以上硬體強度，具Level 3之防竄改保護措施。而若有手機遺失或SIM卡遭竊取情形，依《詐欺犯罪危害防制條例》限制門號使用且有相關罰則，及依電信業者「行動寬頻服務契約」應立即通知業者辦理暫停通信。(Level 3) ● 信物啟用：信物開通方式包含致電客服進行開通作業、未於期限內開通將自動開通、若採電子簽名將於指定生效日自動開通等方式，惟信物非親自交付者，未於期限內開通將自動開通，信物與本人關聯性薄弱。(不符合Level 3) ● 信物更換：比照身分登錄之身分核驗要求辦理。(Level 3)	存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合Global Platform標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA2		

註：新增「經銀行核驗的電信認證」用以與「電信認證」進行區隔。

三十四、　以電信認證為例

階段	評分原因	評分	評等結果
身分登錄	● 申請人臨櫃或線上至電信業者申辦門號，申辦程序應依電信事業受理電信服務相關規範辦理，簽署相關服務條款以表示理解與同意。(Level 1) ● 考量非直營門市之門號申辦流程存有疑慮，未能確保其身分客觀存在，故不符合 Level 2。	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 □Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 □Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 1
信物管理	應排除儲值卡、親子卡、預付卡、企業卡等無法辨識本人親辦親簽之門號。 ● 信物政策與作業流程：遵循電信業者相關政策與作業流程。(Level 1) ● 信物啟用：由申請人或電信業者啟用。(Level 1) ● 信物交付：信物經本人臨櫃領取。若為線上申辦，電信業者可透過宅配交付，並經客服連繫確認申請資料與配送地址。(Level 2)	■Level 1：信物有制定並遵行適當政策與作業流程(如：啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施(如數位簽章或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。	Level 2

	● SIM卡採數位簽章對SIM卡內重要資料簽署加密，並儲存於Secure Element安全模組，具有硬體隔離功能，SIM卡實際規格強度依各廠商實作之硬體架構而有差異，尚無法確保達Level 4以上硬體強度，具Level 3之防竄改保護措施。而若有手機遺失或SIM卡遭竊取情形，依《詐欺犯罪危害防制條例》限制門號使用且有相關罰則，及依電信業者「行動寬頻服務契約」應立即通知業者辦理暫停通信。(Level 3) ● 信物啟用：信物開通方式包含致電客服進行開通作業、未於期限內開通將自動開通、若採電子簽名將於指定生效日自動開通等方式，惟信物非親自交付者，未於期限內開通將自動開通，信物與本人關聯性薄弱。(不符合Level 3) ● 信物更換：比照身分登錄之身分核驗要求辦理。(Level 3)	□Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。TEE、安全載具、行動裝置做為信物，符合Global Platform標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA1		

三十五、　防護機制－SIM 認證(註)（MID 裝置確認）

階段	評分原因	評分	評等結果
身分登錄	● 申請人臨櫃或線上至電信業者申辦門號，申辦程序應依電信事業受理電信服務相關規範辦理，簽署相關服務條款以表示理解與同意。(Level 1) ● 申請人開戶時留存之手機門號已與銀行完成約定，銀行視為可靠來源可進行資料正確性與有效性查驗，以確認申請人註冊門號客觀存在。(Level 2)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 □Level 3:由申請人提示經可靠來源核發之身分資料(LoA3或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 2
信物管理	● 信物政策與作業流程：遵循電信業者相關政策與作業流程。(Level 1) ● 信物啟用：由申請人或電信業者啟用。(Level 1) ● 信物交付：信物經本人臨櫃領取。若為線上申辦，電信業者可透過宅配交付，並經客服連繫確認申請資料與配送地址。 (Level 2) ● SIM 卡採數位簽章對 SIM 卡內重要資料簽署加密，並儲存於 Secure Element 安全模組，具有硬體隔離功能，SIM 卡實際規格強度依各廠商實作之硬體架構而有差異，尚無法確保達 Level 4 以上硬體強度，具 Level 3 之防竄改保護措施。而若有手機遺失或 SIM 卡遭竊取情形，依《詐欺犯	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用、綁定、保存、更換及撤銷等)，且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改或防資料外洩之保護措施（如數位簽章或存於硬體載具但設定為鎖定狀態）、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄	Level 2

	罪危害防制條例》限制門號使用且有相關罰則，及依電信業者「行動寬頻服務契約」應立即通知業者辦理暫停通信。(Level 3) ● 信物啟用：信物開通方式包含致電客服進行開通作業、未於期限內開通將自動開通、若採電子簽名將於指定生效日自動開通等方式，惟信物非親自交付者，未於期限內開通將自動開通，信物與本人關聯性薄弱。(不符合 Level 3) ● 信物更換：比照身分登錄之身分核驗要求辦理。(Level 3)	進行身分核驗。TEE、安全載具、行動裝置做為信物，符合 Global Platform 標準、具備資料管控、破壞偵測等防護機制，或依行動裝置應用程式作業規範具備防入侵、執行期間保護等防護機制。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA2		

註：此處 SIM 認證為現有安控基準中所提之「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)」，故非單一之安全設計，應作為加強控制且搭配安全設計之防護機制。

三十六、　以金融Fast ID為例

階段	評分原因	評分	評等結果
身分登錄	依「**金融機構辦理快速身分識別機制安全控管作業指引**」，申請人首次申請應採臨櫃、硬體自然人憑證、晶片金融卡任一款核驗身分。 ● **硬體自然人憑證** (Level 4) ● **晶片金融卡(限臨櫃申請開戶或經線上申請第一類高風險數位存款帳戶)** -臨櫃申請開戶之晶片金融卡(Level 4) -經線上申請第一類高風險數位存款帳戶晶片金融卡(Level 4) **臨櫃** ● 閱讀並勾選同意銀行相關服務約定事項條款,以表示理解與同意。(Level 1) ● 申請人出示身分證明，並可透過公開且客觀方式檢驗真偽後，確認其客觀存在。(Level 2) ● 申請人提示身分證，並經戶役政資料庫查驗。(Level 3) ● 申請人提示第二個不同可靠來源資料(Level 2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。(Level 4) ● 臨櫃辦理經人工查驗。(Level 5)	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2:申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 ■Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 ■Level 5：經人工查驗。	臨櫃：Level 4 硬體自然人憑證：Level 4 臨櫃申請開戶之晶片金融卡：Level 5、數一高晶片金融卡：Level 4

信物管理	● 信物政策與作業流程：遵循金融機構相關政策與作業流程。(Level 1) ● 信物啟用：信物須經申請人啟用步驟(Level 1)。啟用時需輸入身分證字號及簡訊 OTP，以驗證個體與信物之關聯性。(Level 3) ● 信物交付：客戶於同一設備且同一連線階段下完成身分核驗後，於在裝置內進行生物特徵設定或綁定，並產生 FIDO 金鑰對，私鑰妥善儲存於客戶裝置內，公鑰儲存於 FIDO 伺服器。(Level 2) ● 信物更換:驗證有效之原金鑰或重新透過原註冊程序與啟用程序。(Level 3) ● 私鑰儲存於申請人之行動裝置,其硬體載具具備相關防竄改保護措施，如一般 iOS 或 Android 系統手機具備安全加密模組(如 Android Keystore 或 Apple Secure Enclave)，提供防竄改及防資料外洩保護措施。公鑰儲存於硬體安全模組內並限制匯出功能，以達信物防竄改或防資料外洩之保護措施。(Level 3)	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等),且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 ■Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。 □Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	Level 3
總結	LoA3		

三十七、　以行動自然人憑證為例

階段	評分原因	評分	評等結果
身分登錄	● 申請人線上申請填寫基本資料後，需詳閱「隱私權保護政策及使用聲明」，並勾選表示理解與同意後，方能繼續申請作業，身分證明策略發布於內政部行動自然人憑證官網及內政部憑證管理中心憑證實務作業基準。（Level 1） ● 申請人使用硬體自然人憑證於 PC 插卡或行動裝置 NFC 感應，並於行動自然人憑證網站或行動自然人憑證 App 輸入 ID 及卡片 PIN 碼，以驅動自然人憑證私鑰，並以私鑰對相關申請參數進行簽章後，送至行動自然人憑證系統進行憑證及簽章有效性驗證。（符合 Level 2、Level 3）	■Level 1：申請人自我宣稱，且申請人有簽署服務條款以表示理解與同意。 ■Level 2：申請人的身分訊息經可靠來源提供，客觀存在。 ■Level 3：由申請人提示經可靠來源核發之身分資料(LoA3 或經政府機關核准之身分證明文件)，並經信任機構驗證。 □Level 4：由申請人提示第二個不同可靠來源資料(LoA2 或經政府機關核准之身分證明文件，或原開戶時之留存印鑑或簽名)，並做為身分資料之補強。法人戶經書面同意由法人戶指定人員核驗身分後辦理。 □Level 5：經人工查驗。	Level 3
信物管理	● 信物政策與作業流程：遵循內政部憑證管理中心憑證實務作業基準及內政部行動自然人憑證官網說明。(Level 1) ● 信物啟用：完成硬體自然人憑證驗證後使用行動自然人憑證 App 掃描 PC 官網顯示之 QR Code 後啟動生物辨識進行驗證；或直接於 App 上申請綁定啟動生物辨識進行驗證。一旦生物辨識成功即完成裝置及信物綁定與啟用。(Level 3) ● 信物展期：憑證到期前 60 天，開啟 App 會自動跳出展期畫面輸入身分證字號並經生物辨識成功，驅動行動自然人	■Level 1：信物有制定並遵行適當政策與作業流程(如:啟用,綁定,保存,更換及撤銷等),且信物須由申請人或信物服務提供單位授權之人員啟用。 ■Level 2：加密保護、必須親自交付或檢查交付方式與該申請人合理關聯。 □Level 3：啟用須驗證個體和信物關聯性、具防竄改保護措施(如:數位簽章,或存於硬體載具但設定為鎖定狀態)、信物更換或展期依身分登錄進行身分核驗。	Level 2

	憑證簽署申請相關資訊上傳至行動自然人憑證系統查驗後完成展期重新簽發 1 年效期憑證。（Level 3） ● 信物更換：無信物更換服務，一律申請廢止後另依原申請程序進行新信物申請。(廢止申請透過 PC 以硬體、行動自然人憑證登入驗證，或透過 App 輸入「身分證字號 」 後進行生物辨識驗證。) ● 憑證金鑰對在申請人信賴之行動載具內產製金鑰對(Level 2)，惟未能確保是否經第三方專家檢測，以評估其信物經安全保護且金鑰不會遭外洩或破解。(不符合 Level 3)	□Level 4：保存信物之軟硬體設備具防竄改保護措施且具備竄改檢測機制、信物啟用只允許在指定時間內完成、信物簽收及保存須經申請人同意、信物更換或展期依身分登錄進行身分核驗。 □Level 5：採用防竄改之硬體裝置保存信物，以防被非法匯出或複製且具竄改檢測機制及自動銷毀刪除機制、信物更換或展期依身分登錄進行身分核驗、應具「電子簽章法」之不可否認性。	
總結	LoA2		

附錄四、身分核驗安全設計及信賴等級評估彙總表

安全設計		身分登錄/信物管理	信賴等級
一、憑證簽章	FXML 硬體憑證	身分登錄 Level 5	最高 LoA5
		信物管理 Level 5	
	硬體自然人憑證	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	工商憑證 IC 卡(正卡)	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	法人高風險憑證－安全載具(如動態密碼產生器)	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	法人高風險憑證－具密碼保護之安全元件(SE)	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	法人高風險憑證－可信賴執行環境(TEE)	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	法人高風險憑證－行動裝置應用程式	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	C3 軟體憑證	身分登錄 Level 3、Level 2(數存三②)、Level 1(數存三①)	最低 LoA1(數存三①)、 低 LoA2(數存三②)、

安全設計		身分登錄/信物管理	信賴等級
		信物管理 Level 3	中 LoA3
	FXML 軟體憑證	身分登錄 Level 5	中 LoA3
		信物管理 Level 3	
二、晶片金融卡	法人晶片金融卡	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	臨櫃晶片金融卡	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	數存一高風險	身分登錄 Level 4	高 LoA4
		信物管理 Level 4	
	數存一低風險	身分登錄 Level 3	中 LoA3
		信物管理 Level 4	
	數存二	身分登錄 Level 3	中 LoA3
		信物管理 Level 4	
	數存三①(連結本人之金融支付工具或電信認證)	身分登錄 Level 1	最低 LoA1
		信物管理 Level 4	
	數存三②(跨行金融帳戶資訊核驗)	身分登錄 Level 2	低 LoA2
		信物管理 Level 4	

安全設計		身分登錄/信物管理	信賴等級
	數存三③(跨行金融帳戶資訊核驗+視訊)	身分登錄 Level 3	中 LoA3
		信物管理 Level 4	
三、一次性密碼	法人高風險 OTP－安全載具(如動態密碼產生器)	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	法人高風險 OTP－具密碼保護之安全元件(SE)	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	法人高風險 OTP－可信賴執行環境(TEE)	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	法人高風險 OTP－行動裝置應用程式	身分登錄 Level 5	高 LoA4
		信物管理 Level 4	
	簡訊或軟體 OTP	身分登錄 Level 5(臨櫃)、Level 4(數存一高)、Level 3(數存一低、數存二)	低 LoA2
		信物管理 Level 2	
	簡訊或軟體 OTP（線上辦理貸款之純貸戶）	身分登錄 Level 1	最低 LoA1
		信物管理 Level 2	
		身分登錄 Level 1	最低

安全設計		身分登錄/信物管理	信賴等級
	簡訊或軟體 OTP（數存三①）	信物管理 Level 2	LoA1
	簡訊或軟體 OTP（數存三②）	身分登錄 Level 2	低 LoA2
		信物管理 Level 2	
	簡訊或軟體 OTP（數存三③）	身分登錄 Level 3	低 LoA2
		信物管理 Level 2	
	簡訊或軟體 OTP（信用卡）	身分登錄 Level 1	最低 LoA1
		信物管理 Level 2	
	語音或推播 OTP	身分登錄 Level 5(臨櫃)、Level 4(數存一高)、Level 3(數存一低、數存二)	中 LoA3
		信物管理 Level 3	
	語音或推播 OTP（數存三①）	身分登錄 Level 1	最低 LoA1
		信物管理 Level 3	
	語音或推播 OTP（數存三②）	身分登錄 Level 2	低 LoA2
		信物管理 Level 3	
	語音或推播 OTP（數存三③）	身分登錄 Level 3	中 LoA3
		信物管理 Level 3	

安全設計		身分登錄/信物管理	信賴等級
	語音或推播 OTP（信用卡）	身分登錄 Level 1	最低 LoA1
		信物管理 Level 3	
四、兩項以上技術	臨櫃或 VTM 辦理、法人、數存一高風險帳戶	身分登錄 Level 5(臨櫃或 VTM 辦理、法人)、Level 4(數存一高)	高 LoA4
		信物管理 Level 4	
	臨櫃或 VTM 辦理、法人、數存一高風險、數存一低、數存二、數存三③帳戶	身分登錄 Level 5(臨櫃或 VTM 辦理、法人)、Level 4(數存一高）、Level 3(數存一低、數存二、數存三③)	中 LoA3
		信物管理 Level 3	
	數存三②帳戶	身分登錄 Level 2	低 LoA2
		信物管理 Level 3	
	數存三①帳戶、信用卡戶	身分登錄 Level 1	最低 LoA1
		信物管理 Level 3	
五、視訊會議	VTM	身分登錄 Level 5	高 LoA4
		信物管理 Level 4 額外控管要求	
	手機或平板裝置	身分登錄 Level 3	中 LoA3
		信物管理 Level 3 額外控管要求	
六、知識詢問	知識詢問	身分登錄	最低

安全設計		身分登錄/信物管理	信賴等級
		Level 5(臨櫃)、Level 4(數存一高)、Level 3(數存一低、數存二、數存三③)、Level 2(數存三②)、Level 1(數存三①、信用卡)	LoA1
		信物管理 Level 1	
七、固定密碼	固定密碼	身分登錄 Level 5(臨櫃)、Level 4(數存一高)、Level 3(數存一低、數存二、數存三③)、Level 2(數存三②)、Level 1(數存三①)	最低 LoA1
		信物管理 Level 1	
八、存款帳戶資訊	存款帳戶資訊	身分登錄 Level 5(臨櫃)、Level 4(數存一高)、Level 3(數存一低、數存二、數存三③)、Level 2(數存三②)、Level 1(數存三①)	最低 LoA1(數存三①)、 低 LoA2
		信物管理 Level 2	
九、信用卡資訊	信用卡資訊	身分登錄 Level 1	最低 LoA1
		信物管理 Level 1	
十、電信認證	經銀行核驗之電信認證	身分登錄 Level 5(臨櫃)、Level 4(數存一高)、Level 3(數存一低、數存二、數存三③)、Level 2(數存三②)	低 LoA2

安全設計		身分登錄/信物管理	信賴等級
		信物管理 Level 2	
	電信認證	身分登錄 Level 1	最低 LoA1
		信物管理 Level 2	
十一、金融 Fast ID	金融 Fast ID	身分登錄 Level 5(臨櫃)、Level 4(硬體自然人憑證、臨櫃申請開戶之晶片金融卡、數一高晶片金融卡)	中 LoA3
		信物管理 Level 3	
十二、行動自然人憑證	行動自然人憑證	身分登錄 Level 3	低 LoA2
		信物管理 Level 2	

附錄五、身分驗證階段常見安全設計要求

一、憑證簽章

身分驗證階段	（一）應確認憑證之合法性、正確性、有效性、保證等級及用途限制。 （二）應簽署適當內容；於簽入作業時，應簽署足以識別該個人之資料(如：個人統一編號)、於書面同意時，應簽署依相關法令規定之指定書件；應用於交易指示時，應簽署完整付款指示。

二、晶片金融卡

身分驗證階段	（一）應由原發卡行依據交易類型核驗對應之交易驗證碼（如：簽入得採餘額查詢交易） （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、一次性密碼

身分驗證階段	（一）應運用一次性密碼技術產生並限制一次性使用。 （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。

四、兩項以上技術

身分驗證階段	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、晶片護照、金鑰等)。 （三）客戶提供給金融機構其所擁有之生物特徵，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。 1、採用直接驗證生物特徵技術者，應確認真人及本人辦理並符合「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要求。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加強其他安全設計，並應透過第三方依據 ISO/IEC30107 攻擊樣態逐一進行檢測，以確保感測器所擷取的生物特徵是客戶的真實生物特徵，而非經過變造或偽冒。 2、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;若該機制出現偽冒風險時，應加強其他安全設計(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)。

五、視訊會議

身分驗證階段	(一) 應留存政府核發用於身分識別之證件(如國民身分證、居留證或護照等)影像檔並進行驗證；若客戶係本國籍未成年人，應增加核驗其法定代理人之上述證明文件。 (二) 應導入機制協助確認真人及本人，以防止透過科技預先錄製影片、製作面具、模擬影像或深度偽造(deepfake)等機制偽冒身分。 (三) 應由金融機構確認客戶指示內容與其意思表示。

六、知識詢問

身分驗證階段	應核驗客戶所知悉之靜態資訊(如國小就讀學校)或動態資訊(如前次繳款紀錄)。

七、固定密碼

身分驗證階段	(一) 應核驗與客戶所約定之密碼。 (二) 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： 甲、不得使用客戶之顯性資料(如個人統一編號、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。 乙、不應少於六位。 丙、不應訂為相同之英數字、連續英文字或連號數字。 丁、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。 戊、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。 (丁)變更時得核驗原使用者代號後辦理且不得與原使用者代號相同。 (2)固定密碼之安全設計： 甲、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。 乙、建議採英數字混合使用，且宜包含大小寫英文字母或符號。 丙、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。 丁、不應與用戶代號、使用者代號、交易密碼相同。 戊、密碼連續錯誤達五次，不得再繼續執行交易。 己、變更時得核驗原密碼後辦理且不得與原密碼相同。 庚、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。 辛、密碼超過一年未變更，金融機構應做妥善處理。 (3)採用圖形鎖或手勢之安全設計： 甲、連續錯誤達五次，不得再繼續執行交易。 乙、變更不得與原設定相同。 (三)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，其固定密碼之安全設計，應遵循前子目身分驗證相關要求，惟密碼長度不應少於四位。

八、存款帳戶資訊

身分驗證階段	(一)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。 (二)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、信用卡

身分驗證階段	(一) 確認申請人與信用卡持卡人為同一個人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)。 (二) 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、電信認證

身分驗證階段	確認申請人與該門號租用人為同一個人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。

十一、經銀行核驗之電信認證

身分驗證階段	確認申請人與該門號租用人為同一個人統一編號、該門號經銀行註冊，且透過用戶身分模組(Subscriber Identity Module, SIM）連線至該電信業者，確認該SIM之有效性。

附錄六、交易類別信賴等級及業務要求

（限適用第三類數位存款帳戶）

一、「非電子轉帳及交易指示類」：

辦理帳務類及個人資料類之查詢比照第八條第一款規定辦理。

二、「電子轉帳及交易指示類」之交易指示：

(一)ATM 服務

１、辦理 ATM 存提款業務，應採用晶片金融卡進行身分確認。

２、辦理 ATM 無卡存款業務，應採用最低信賴等級以上進行身分確認。

３、辦理 ATM 無卡提款業務，應遵循下列要求：

（１）於申請及交易時得採用下列任一種安全設計：

甲、採用晶片金融卡安全設計者，該卡應為該帳戶所申請。

乙、採用一次性密碼安全設計者，應以密碼搭配指定之硬體設備產生一次性密碼。

丙、兩項以上技術之安全設計。

（２）提款金額應符合第八條第二款第六目第一子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。

４、實體 ATM 轉帳與通知

（１）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。

（２）金融機構得採用憑證簽章、一次性密碼、兩項以上技術等任一安全設計進行身分確認，提供個人取消實體 ATM 轉帳通知機制。

(二)繳稅費及消費扣款業務

１、限定性繳稅費

（１）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金融 FXML 憑證、

晶片金融卡、一次性密碼、兩項以上技術等任一安全設計進行身分確認。

（２）辦理客戶發動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，進行限定性繳稅費扣款及退款(如基金定期定額、信用卡繳款)服務，應採用最低信賴等級以上之安全設計進行身分確認，惟排除信用卡資訊及電信認證安全設計。

（３）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六條數位身分驗證機制；惟金融機構應以簡訊、App 推播、電子郵件或其他方式通知，以利客戶事後覆核。

（４）金融機構接受客戶、事業單位、其他金融機構或金融資訊服務事業、票據交換所平台等發動交易指示(如扣款約定、扣款、退款、終止扣款約定)時，應依據第五條訊息處理方式辦理。

（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。

２、概括約定繳稅費

（１）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之扣款約定時，扣款金融機構應採用金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術等任一安全設計進行身分確認。

（２）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六條數位身分驗證機制；惟金融機構應以簡訊、App 推播、電子郵件或其他方式通知，以利客戶事後覆核。

（３）金融機構接受客戶、事業單位、其他金融機構或金融資訊服務事業、票據交換所平台等發動交易指示(如扣款約定、扣款、退款、終止扣款約定)時，應依據第五條訊息處理方式辦理。

（４）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。

３、消費扣款

（１）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。

（２）金融機構得採用憑證簽章、一次性密碼、兩項以上技術(不含金融 Fast ID)任一安全設計進行身分確認，提供客戶取消消費扣款通知機制。

(三)同一統一編號轉帳交易

任一金融機構同一統一編號帳戶間轉帳、定存或投資應採用晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼等任一安全設計進行身分確認。

(四)約定轉入帳戶轉帳交易(又稱約轉交易)

約轉交易應採用晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼等任一安全設計進行身分確認。

(五)非約定轉入帳戶轉帳交易(又稱非約轉交易)

非約轉交易每筆應採用金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術等任一安全設計進行身分確認，並應遵循下列要求：

１、透過網際網路之低風險交易，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」規定辦理。

２、透過網站、行動 App、電子郵件、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。

３、若採用簡訊傳送一次性密碼並應用於非約定轉入帳戶轉帳交易者，應遵循下列要求：

（１） 手機號碼之異動應採用臨櫃、憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議等

任一安全設計進行身分確認,惟採用簡訊OTP者應驗證舊有之門號號碼及新換之門號號碼。

（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 等身分核驗資訊或機敏資訊，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)。

(六)結構型商品交易

１、非首次辦理之同類型結構型商品交易應採用金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼等任一安全設計進行身分確認。

２、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元，每日累計交易金額超過等值新臺幣參仟萬元以上應採用 FXML 硬體憑證之安全設計進行身分確認，以加強風險控管。

３、辦理結構型商品交易應遵循下列業務要求：

（１）交易及扣款帳戶以任一金融機構同一統一編號為限。

（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）。

(七)信託業務

辦理依信託契約約定之信託財產運用範圍，為申請運用指示：

１、辦理任一金融機構同一統一編號帳戶間轉帳、定存或投資(含交易取消)應參照前(三)目同一統一編號轉帳交易之安全設計辦理。

２、辦理約定轉入帳戶之付款應參照前(四)目約定轉入帳戶轉帳交易之安全設計辦理。

３、辦理非約定轉入帳戶之付款應參照前(五)目非約定轉入帳戶轉帳交易之安全設計辦理。

(八)授信業務

客戶指示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之低風險交易，參照第八條第二款第(九)目規定辦理，進行身分確認。

三、「電子轉帳及交易指示類」之申請指示：

(一)外匯業務

開發信用狀申請、修改信用狀申請應採用金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術、視訊會議等任一安全設計進行身分確認。

(二)存款業務

１、晶片金融卡

（１）辦理已持有晶片金融卡舊戶申請補換發晶片金融卡應採用下列任一方式之安全設計：

甲、採用第八條第三款第二目第一子目第二點甲之要求辦理。

乙、採用與舊卡相同信賴等級以上之安全機制。

（２）辦理已持有晶片金融卡舊戶啟用補換發晶片金融卡應採用下列任一方式之安全設計(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。)：

甲、採用第八條第三款第二目第一子目第三點甲或乙之要求辦理。

乙、採用與舊卡相同信賴等級以上之安全機制。

（３）辦理晶片金融卡密碼解鎖應採用金融 FXML 憑證、晶片金融卡、一次性密碼任一種安全設計進行身分確認，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計，並應遵循下列要求：

甲、應於發卡行之端末設備(如 ATM、POS、VTM 等)進行。

乙、應依據第五條訊息處理方式針對機敏資訊進行端點對端點加密防護。

丙、不得以第三類數位存款帳戶之安全設計解鎖第一類或第二類數位存款帳戶之晶片金融卡。

２、約定轉入帳號

（１）辦理申請約定同一統一編號之約定轉入帳號應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼及行

動自然人憑證等任一種安全設計進行身分確認。

（２）首次設定非同一統一編號帳號者須先經臨櫃或採用視訊會議確認身分後方可為之。

（３）辦理申請約定非同一統一編號之約定轉入帳號，須透過線上逐筆採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術及視訊會議等任一種安全設計進行身分確認，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計。

（４）透過電話語音或網路銀行之新約定帳號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。

（５）約定轉入帳號之設定，其交易限額同附錄六第二款第五目第一子目要求。

３、非約定轉入帳號

已開立存款帳戶者申辦電子銀行（如網路銀行、行動銀行、網路 ATM）或晶片金融卡之非約定轉帳功能應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術及視訊會議等任一種安全設計進行身分確認，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計。

４、其他業務

（１）已開立存款帳戶者申辦結清銷戶應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、固定密碼、知識詢問及行動自然人憑證等任一種安全設計進行身分確認。

（２）同意金融機構查詢聯徵中心信用資料應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、固定密碼、知識詢問及行動自然人憑證等任一種安全設計進行身分確認。

(三)授信業務

１、同意查詢聯徵業務(個人_含借款人、保證人等)

本行個人既有客戶，應採用最低信賴等級以上之安全設計進行身分確認。

２、簽約對保業務(個人_含借款人、保證人等)，應採用下列任一方式之安全設計，除另有規定外，款項限撥入本人任一金融機構同一統一編號帳戶：

（１）本行個人既有客戶，應採用下列任一方式之安全設計：

甲、採用硬體自然人憑證安全設計。

乙、採用視訊會議安全設計辦理簽約對保者，限撥入本人非數位帳戶。

丙、採用存款帳戶之「跨行金融帳戶資訊核驗」，並搭配知識詢問安全設計或上傳身分證影像檔或透過 MyData 平台取得身分證電子檔或查詢身分證領/補/換資料(限於申請階段已上傳身分證影像檔或透過 MyData 平台取得身分證電子檔者)，且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，得將款項撥入本人帳戶，並視貸款金額之大小、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:新增撥款簡訊通知、晶片金融卡、一次性密碼、視訊會議或其他安全設計)。

丁、採用包含生物特徵之「兩項以上技術」搭配 C3 軟體憑證或知識詢問安全設計辦理簽約對保，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)。

（２）本行個人既有客戶，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，如採包含生物特徵之「兩項以上技術」及硬體自然人憑證辦理簽約對保者，得將款項撥入他行第三方公司之實體帳戶。

３、「擔保物權連結條款」規定之同意書簽署

依個人購屋貸款依「個人購屋貸款定型化契約應記載事項」第十三條或個人購車貸款依「個人購車貸款定型化契約應記載事項」第十二條，沿用原抵押權需擔保物提供人同意簽署，其安全設計應依下列辦理：

（１）擔保物提供人為借款人或保證人或本行既有客戶，依識別之身分別(即既有戶、數位存款戶

等)，比照「貸款契約」成立簽約對保之安全設計辦理。

（２）擔保物提供人為借款人或保證人以外之第三人且為本行新戶，應採用 FXML 硬體憑證、硬體自然人憑證及工商憑證 IC 卡(正卡)等任一種安全設計辦理。

(四)信用卡業務

信用卡業務比照第八條第三款第(四)目規定辦理,進行身分確認。

(五)財富管理業務

１、認識客戶作業(KYC)應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證等任一種安全設計。

２、非首次之認識客戶作業(KYC)應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

3、客戶風險承受度測驗應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證等任一種安全設計。

４、非首次之客戶風險承受度測驗應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

5、衍商辦法結構型商品業務之同意推介或終止推介應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

６、同意成為專業客戶應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

7、專業客戶聲明已充分審閱而無須適用審閱期應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

(六)信託業務

1、已開立任一金融機構存款帳戶者得申辦各類信託開戶(含簽約)及變更、增補或終止信託契約應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證等任一種安全設計。

2、首次認識客戶作業(KYC)應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證等任一種安全設計。

3、非首次之認識客戶作業(KYC)應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

4、首次客戶風險承受度測驗應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證等任一種安全設計。

5、非首次之客戶風險承受度測驗應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

6、同意信託業務之推介或終止推介應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

7、同意簽署為專業投資人應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、

經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

8、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應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

9、依信託契約約定由委託人或信託監察人行使同意權應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

１０、依信託契約約定之信託財產運用範圍申請「受益人行使表決權」指示應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。

(七)共同行銷業務

共同行銷業務應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼及行動自然人憑證等任一種安全設計進行身分確認。

(八)其他業務

１、非首次之認識客戶作業(KYC)應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證等任一種安全設計。首次認識客戶作業(KYC)應採用憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證等任一種安全設計。

２、不涉及帳務通知或交易指示之個人資料異動、協助電子支付機構確認客戶身分應採用晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問及固定密碼等任一種安全設計進行身分確認。

3、照會、涉及帳務通知或交易指示之個人資料異動、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、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、國外提款之磁條密碼、網路銀行使用者代號等應採用晶片金融卡、一次性密碼、兩項以上技術及視訊會議等任一種安全設計。

4、個人資料顯示應採取隱碼機制。但如系統已採用最低信賴等級以上安全設計對客戶進行身分確認者，得不隱碼其帳號及確認交易之必要資訊；另已採憑證簽章、晶片金融卡、一次性密碼、兩項以上技術及視訊會議等任一種安全設計進行身分確認者，變更個人資料欄位得不予隱碼處理。

附錄七、業務應用情境及信賴等級對照表

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
1	非電子轉帳及交易指示類	查詢業務	帳務類之查詢	最低信賴等級以上	最低信賴等級以上	-	電信認證
2			個人資料類之查詢	最低信賴等級以上	最低信賴等級以上	-	電信認證
3	電子轉帳及交易指示類之交易指示	高風險交易	高風險交易	最高信賴等級	-	-	-
4			應用於法人客戶且未能使用符合我國電子簽章法之數位簽章者	高信賴等級以上	-	-	VTM 視訊會議、自然人憑證及工商憑證
5		ATM 服務	ATM 存提款	晶片金融卡	晶片金融卡	-	-
6			ATM 無卡存款	最低信賴等級以上	最低信賴等級以上	-	-
7			ATM 無卡提款(**申請及交易**)	中信賴等級以上	晶片金融卡、一次性密碼、兩項以上技術	·若採用晶片金融卡安全設計者，該卡應為該帳戶所申請。 ·若採用一次性密碼安全設計者，應以密碼搭配指定之硬體設備產生一次性密碼。	自然人憑證、工商憑證、軟體憑證及視訊會議

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
8			取消實體 ATM 轉帳通知	中信賴等級以上、簡訊 OTP 或軟體 OTP	憑證簽章、一次性密碼、兩項以上技術	-	晶片金融卡、視訊會議及金融 Fast ID
9		繳稅費及消費扣款(限定性繳稅費)	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	中信賴等級以上、簡訊 OTP 或軟體 OTP	金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術	-	工商憑證及視訊會議
10			辦理客戶發動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，進行限定性繳稅費扣款及退款(如基金定期定額、信用卡繳款)服務	最低信賴等級以上	最低信賴等級以上	-	信用卡資訊及電信認證
11		繳稅費及消費扣款(概括約定繳稅費)	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之扣款約定時	中信賴等級以上、簡訊 OTP 或軟體 OTP	金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術	-	工商憑證及視訊會議
12		繳稅費及消費扣款(消費扣款)	取消消費扣款通知	中信賴等級以上、簡訊 OTP 或軟體 OTP	憑證簽章、一次性密碼、兩項以上技術(不含金融 Fast ID)	-	晶片金融卡、視訊會議及金融 Fast ID

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
13		同一統一編號轉帳交易	任一金融機構同一統一編號帳戶間轉帳、定存或投資	低信賴等級以上、知識詢問或固定密碼	晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼	-	自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊
14		約定轉入帳戶轉帳交易(又稱約轉交易)	約轉交易	低信賴等級以上、知識詢問或固定密碼	晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼	-	自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊
15		非約定轉入帳戶轉帳交易(又稱非約轉交易)	非約轉交易	中信賴等級以上、簡訊 OTP 或軟體 OTP	金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術	-	自然人憑證、工商憑證、軟體憑證及視訊會議
16			若採用簡訊傳送一次性密碼並應用於非約定轉入帳戶轉帳交易者(**手機號碼之異動**)	臨櫃、中信賴等級以上、簡訊 OTP 或軟體 OTP	臨櫃、憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議	·採用簡訊 OTP 者應驗證舊有之門號號碼及新換之門號號碼	-

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
17		結構型商品交易	非首次辦理之同類型結構型商品交易	低信賴等級以上、知識詢問或固定密碼	金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼	–	自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊
18			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元，每日累計交易金額超過等值新臺幣參仟萬元以上	最高信賴等級	FXML 硬體憑證	–	–
19		信託業務	辦理依信託契約約定之信託財產運用範圍，為申請運用指示：**辦理任一金融機構同一統一編號帳戶間轉帳、定存或投資(含交易取消)**	低信賴等級以上、知識詢問或固定密碼	晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼	–	自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
20			辦理依信託契約約定之信託財產運用範圍，為申請運用指示：**辦理約定轉入帳戶之付款**	低信賴等級以上、知識詢問或固定密碼	晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼	-	自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊
21			辦理依信託契約約定之信託財產運用範圍，為申請運用指示：**辦理非約定轉入帳戶之付款**	中信賴等級以上、簡訊 OTP 或軟體 OTP	金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術	-	自然人憑證、工商憑證、軟體憑證及視訊會議
22		授信業務	客戶指示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之低風險交易(**既有客戶**)	最低信賴等級以上	最低信賴等級以上	-	-
23			客戶指示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之低風險交易(**新戶**)	低信賴等級以上	低信賴等級以上	-	-

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
24	電子轉帳及交易指示類之申請指示	外匯業務	開發信用狀申請、修改信用狀申請	低信賴等級以上	金融 FXML 憑證、晶片金融卡、一次性密碼、兩項以上技術、視訊會議	-	自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊
25		存款業務	晶片金融卡(**舊戶申請補換發**)	應先登入網路銀行、行動銀行或網路ATM 並採用一次性密碼或兩項以上技術、再郵寄至原留存通訊住址。	·應先登入網路銀行、行動銀行或網路ATM並採用一次性密碼或兩項以上技術、再郵寄至原留存通訊住址。 ·採用與舊卡相同信賴等級以上	-	-
26				**數一高存款帳戶**，應採用高信賴等級以上			
27				**數一低存款帳戶**、**數存二存款帳戶**，應採用中信賴等級以上、軟體 OTP 或透過簡訊傳送 OTP			
28				**法人客戶**應採用高信賴等級以上			

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
29			晶片金融卡(**舊戶啟用補換發**) 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。	ATM	·ATM ·以視訊會議核驗身分方式辦理 ·採用與舊卡相同信賴等級以上	採用ATM須透過該銀行ATM以舊卡並以系統驗證新舊卡內帳戶號碼係為一致	-
30				以視訊會議核驗身分方式辦理		採用非多功能視訊櫃檯(VTM)之視訊會議機制者，應搭配憑證簽章、一次性密碼或兩項以上技術等安全設計進行身分確認，惟排除一次性密碼之軟體OTP及透過簡訊傳送OTP等安全設計	-

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
31				採用中信賴等級以上之安全機制		-	-
32			晶片金融卡(**密碼解鎖**)	中信賴等級以上	金融 FXML 憑證、晶片金融卡、一次性密碼	·不得以數位存款帳戶之安全設計解鎖臨櫃帳戶之晶片金融卡 ·不得以數一低或數存二存款帳戶之安全設計解鎖數一高存款帳戶之晶片金融卡 ·不得以數存三存款帳戶之安全設計解鎖數存一或數存二存款帳戶之晶片金融卡	自然人憑證、工商憑證、軟體憑證、兩項以上技術、金融 Fast ID、視訊會議、軟體 OTP 及簡訊 OTP

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
33			約定轉入帳號(**申請約定同一統一編號之約定轉入帳戶**)	低信賴等級以上、知識詢問或固定密碼	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼及行動自然人憑證	-	經銀行核驗的電信認證及存款帳戶資訊
34			約定轉入帳號(**首次設定非同一統一編號帳戶者**)	臨櫃或採用視訊會議	臨櫃或採用視訊會議	-	-
35			約定轉入帳號(**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**)	中信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術及視訊會議	-	自然人憑證、工商憑證、軟體憑證、軟體OTP及簡訊OTP
36			非約定轉入帳號(**已開立存款帳戶者申辦電子銀行（如網路銀行、行動銀行、網路ATM）或晶片金融卡之非約定轉帳功能**)	中信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術及視訊會議	-	自然人憑證、工商憑證、軟體憑證、軟體OTP及簡訊OTP
37			已開立存款帳戶者申辦結清銷戶	低信賴等級以上、知識詢問或固定密碼	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、固定密碼、知識詢問及行動自然人憑證	-	經銀行核驗的電信認證及存款帳戶資訊
38			同意金融機構查詢聯徵中心信用資料	低信賴等級以上、知識詢問或固定密碼	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、固定密碼、知識詢問及行動自然人憑證	-	經銀行核驗的電信認證及存款帳戶資訊

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
39		授信業務	同意查詢聯徵業務(個人_含借款人、保證人等)	**本行個人既有客戶**，最低信賴等級以上	本行個人既有客戶，最低信賴等級以上	–	–
40				**本行個人新戶但為他行既有非數存客戶**，低信賴等級以上		–	–
41				**本行個人新戶**，中信賴等級以上		–	–
42			簽約對保業務(個人含借款人、保證人等) 除另有規定外，限撥入本人任一金融機構同一統一編號帳戶	**本行個人既有客戶(數位存款帳戶及信用卡戶除外)**，最低信賴等級以上	本行個人既有客戶，應採用下列任一方式之安全設計： ·採用硬體自然人憑證安全設計。 ·採用視訊會議安全設計辦理簽約對保者，限撥入本人非數位帳戶。 ·採用存款帳戶之「跨行金融帳戶資訊核驗」，並搭配知識詢問安全設計或上傳	–	–
43				**本行個人新戶**，低信賴等級以上		–	–
44				**本行個人既有數位存款帳戶(數存一高及數存二)**，最低信賴等級以上		–	–

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
45				**本行個人既有數位存款帳戶(數存一低)**，低信賴等級以上，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:新增撥款簡訊通知、晶片金融卡、一次性密碼、視訊會議或其他安全設計)。	身分證影像檔或透過MyData 平台取得身分證電子檔或查詢身分證領/補/換資料(限於申請階段已上傳身分證影像檔或透過MyData 平台取得身分證電子檔者)，且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，得將款項撥入本人帳戶，並視貸款金額之大	-	-

46				**本行個人既有信用卡客戶**，應採用下列任一方式之安全設計： ·採用憑證簽章及視訊會議 ·採用一次性密碼，限撥入本人非數位帳戶、數一高存款帳戶或第二類存款帳戶。 ·採用一次性密碼及視訊會議之安全設計。 ·採用包含生物特徵之「兩項以上技術」，限撥入本人非數位帳戶、數一高或第二類數位存款帳戶。 ·採用包含生物特徵之「兩項以上技術」搭配 C3 軟體憑證或知識詢問之安全設計，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶	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:新增撥款簡訊通知、晶片金融卡、一次性密碼、視訊會議或其他安全設計)。 ·採用包含生物特徵之「兩項以上技術」搭配 C3 軟體憑證或知識詢問安全設計辦理簽約對保，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)。	–	–

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
				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)。			
47				**本行個人既有信用卡客戶**，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，最低信賴等級以上	–	–	–
48				–	本行個人既有客戶，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，如採包含生物特徵之「兩項以上技術」及硬體自然人憑證辦理簽約對保者，得將款項撥入他行第三方公司之實體帳戶。	–	–

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
49			「擔保物權連結條款」規定之同意書簽署 依個人購屋貸款依「個人購屋貸款定型化契約應記載事項」第十三條或個人購車貸款依「個人購車貸款定型化契約應記載事項」第十二條，沿用原抵押權需擔保物提供人同意簽署	擔保物提供人為借款人或保證人或本行既有客戶，依識別之身分別(即既有戶、數位存款戶等)，比照「貸款契約」成立簽約對保之安全設計辦理。	擔保物提供人為借款人或保證人或本行既有客戶，依識別之身分別(即既有戶、數位存款戶等)，比照「貸款契約」成立簽約對保之安全設計辦理。	-	-
50				擔保物提供人為借款人或保證人以外之第三人且為本行新戶，應採用高信賴等級以上(限 FXML 硬體憑證、硬體自然人憑證、工商憑證 IC 卡且為正卡)	擔保物提供人為借款人或保證人以外之第三人且為本行新戶，應採用 FXML 硬體憑證、硬體自然人憑證及工商憑證 IC 卡(正卡)等任一種安全設計辦理	-	-
51			同意查詢聯徵信用資料(法人)	**本行既有法人戶及法人新戶**，高信賴等級以上	-	-	-

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
52				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)，應依其屬本行既有客戶或新戶，分別採用個人授信業務同意金融機構查詢聯徵中心信用資料之各項安全設計進行身分確認。		–	–
53			簽約對保業務(法人)	**本行既有法人客戶**，高信賴等級以上		–	–
54				**3 位以下本國籍自然人股東之法人新戶**，高信賴等級以上		–	–
55				**法人戶負責人或保證人**，中信賴等級以上		–	–
56			法人戶徵授信相關文件之上傳	採用法人戶及其負責人貸款契約成立之安全設計機制		–	–

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
57		信用卡業務	新戶申辦信用卡業務、同意金融機構查詢聯徵中心信用資料	最低信賴等級以上	最低信賴等級以上	若採用電信認證者，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)。	一次性密碼、兩項以上技術、知識詢問及固定密碼
58			已開立存款帳戶者或既有信用卡戶或既有貸款戶申辦信用卡、同意金融機構查詢聯徵中心信用資料	最低信賴等級以上	最低信賴等級以上	-	存款帳戶資訊、信用卡及電信認證
59			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	最低信賴等級以上	最低信賴等級以上	-	存款帳戶資訊、信用卡及電信認證
60			既有信用卡戶辦理其他信用卡業務	最低信賴等級以上	最低信賴等級以上	-	存款帳戶資訊、信用卡及電信認證

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
61		財富管理業務	認識客戶作業(KYC)	低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證	-	-
62			客戶風險承受度測驗	低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證	-	-
63			非首次之認識客戶作業(KYC)	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
64			非首次之客戶風險承受度測驗	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-
65			衍商辦法結構型商品業務之同意推介或終止推介	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-
66			同意成為專業客戶	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
67			專業客戶聲明已充分審閱而無須適用審閱期	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-
68		信託業務	已開立任一金融機構存款帳戶者得申辦各類信託開戶(含簽約)及變更、增補或終止信託契約	低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證	-	-
69			首次認識客戶作業(KYC)	低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證	-	-
70			首次客戶風險承受度測驗	低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證	-	-

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
71			非首次之認識客戶作業(KYC)	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-
72			非首次之客戶風險承受度測驗	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-
73			同意信託業務之推介或終止推介	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
74			同意簽署為專業投資人	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-
75			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	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-
76			依信託契約約定由委託人或信託監察人行使同意權	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	-	-

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
77			依信託契約約定之信託財產運用範圍申請「受益人行使表決權」指示	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	–	–
78		共同行銷業務	共同行銷業務	低信賴等級以上、知識詢問或固定密碼	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼及行動自然人憑證	–	經銀行核驗的電信認證及存款帳戶資訊
79		其他業務	非首次認識客戶作業	最低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問、固定密碼、存款帳戶資訊驗證、信用卡資訊、經銀行核驗的電信認證、電信認證及行動自然人憑證	–	–
80			首次認識客戶作業	低信賴等級以上	憑證簽章、晶片金融卡、一次性密碼、兩項以上技術、視訊會議、存款帳戶資訊驗證、經銀行核驗的電信認證及行動自然人憑證	–	–

項次	應用情境類別	業務類別	應用情境	業務信賴等級	第三類數位存款帳戶	安全設計備註	排除安全設計
81			不涉及帳務通知或交易指示之個人資料異動、協助電子支付機構確認客戶身分	低信賴等級以上，或知識詢問或固定密碼	晶片金融卡、一次性密碼、兩項以上技術、視訊會議、知識詢問及固定密碼	-	自然人憑證、工商憑證、軟體憑證、經銀行核驗的電信認證及存款帳戶資訊
82			照會、涉及帳務通知或交易指示之個人資料異動、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、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、國外提款之磁條密碼、網路銀行使用者代號等	中信賴等級以上、簡訊 OTP 或軟體 OTP	晶片金融卡、一次性密碼、兩項以上技術及視訊會議	-	自然人憑證、工商憑證及軟體憑證

本表所列資訊僅供參考，如有差異，請以本基準規定為準。