

金融機構辦理電子銀行業務安全控管作業基準修訂摘要

壹、用詞定義

一、結構型商品：係指

- (一)「銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法」第二條所稱之結構型商品。
- (二)「信託業營運範圍受益權轉讓限制風險揭露及行銷訂約管理辦法」第二十二條之一所稱之境內結構型商品及「境外結構型商品管理規則」第二條所稱之境外結構型商品。

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

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

貳、電子銀行業務之交易類別及風險

一、電子轉帳及交易指示類

(一)服務項目

1、申請指示，其服務項目舉例如下：

(1)授信業務

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

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

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

(二)交易指示

1、高風險交易：係指該訊息執行結果，對客戶權益有重大影響之各類電子轉帳及交易指示，包含非約定轉帳交易超過最高限額之交易指示。

2、低風險交易：係指該訊息執行結果對客戶權益無重大影響之各類電子轉帳及交易指示，內容包括下列各項：

- (1)辦理約定轉入帳戶之設定及轉帳。
- (2)任一金融機構同一統一編號帳戶間轉帳、定存或投資。
- (3)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。
- (4)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。
- (5)辦理非約定轉入帳戶之轉帳。

參、交易面之介面安全設計

客戶發送訊息時，其介面及訊息之通訊傳輸應達到之安全防護措施，相關安全設計區分如下，

並應符合第九條規定：

一、使用憑證簽章，其安全設計應簽署適當內容並確認該憑證之合法性、正確性、有效性、保證內容及用途限制。

二、使用「兩項以上技術」，其安全設計應具有下列三項之任兩項以上技術：

(一) 客戶所持有之設備，金融機構應確認該設備為客戶與金融機構所約定持有之實體設備(如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具、SIM 卡認證等)。

肆、交易類別之安全設計

一、「電子轉帳及交易指示類」之交易指示：辦理高風險交易每筆或每批應採用硬體金融 FXML 憑證簽章安全設計，辦理低風險交易應採用憑證簽章、晶片金融卡、一次性密碼、「兩項以上技術」、視訊會議、知識詢問、固定密碼之任一款安全設計進行身分確認，其中非約定轉帳交易每筆應採用憑證簽章、晶片金融卡、一次性密碼、「兩項以上技術」之任一款安全設計進行身分確認，但辦理下列業務，應遵循下列要求：

(一) 辦理「非約定轉入帳戶」應遵循下列要求：

- 1、透過網站、行動 APP、電子郵件、傳真、FTP 或 AP2AP 等方式傳送且未經金融機構人工確認客戶身分與指示內容者，其交易限額同前一子目要求。
- 2、若採用之技術防護措施(如憑證簽章、晶片金融卡、非簡訊傳送之一次性密碼、視訊會議、第三人覆核、簡訊簡碼回傳、直接人臉辨識軌跡等)，提供客戶確認該筆交易內容並能防止身分確認資料與交易內容被竄改者，該筆非約定轉入帳戶之轉帳限額，可由個別金融機構視其風險承擔之能力斟酌予以適當提高，最高該轉出帳號不超過當日累計等值新臺幣三百萬元為限，並留存該技術評估紀錄。
- 3、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。

二、「電子轉帳及交易指示類」之申請指示

(一) 辦理存款業務應採用憑證簽章、晶片金融卡、一次性密碼、「兩項以上技術」、視訊會議、知識詢問、固定密碼之任一款安全設計，但辦理下列業務，應遵循下列要求：

- 1、辦理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憑證簽章、晶片金融卡、一次性密碼、「兩項以上技術」、視訊會議之任一款進行設定，並排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計設定，並應遵循下列要求：

(1) 約定轉入帳戶之設定，其交易限額同非約定轉入帳戶低風險交易限額要求，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。

- 2、辦理晶片金融卡密碼解鎖作業，應採用憑證簽章、晶片金融卡、一次性密碼之任一款安全設計，惟排除以數位存款帳戶之安全設計解鎖臨櫃帳戶之晶片金融卡、以第三類數位存款帳戶之安全設計解鎖第一類及第二類數位存款帳戶之晶片金融卡、以第二類數位存款帳戶或第一類低風險數位存款帳戶之安全設計解鎖第一類高風險數位存款帳戶之晶片金融卡並排除軟體 OTP 與簡訊 OTP，且應於發卡行之端末設備(如 ATM、POS、VTM 等)進行，並針對解鎖用之敏感資料採用符合訊息隱密性要求，進行端點對端點加密防護。

(二) 辦理個人授信業務應採用憑證簽章、晶片金融卡、一次性密碼、「兩項以上技

術」、視訊會議、知識詢問、固定密碼之任一款安全設計，但辦理下列業務，應遵循下列要求：

- 1、辦理本行個人新戶(含借款人及保證人)同意金融機構查詢聯徵中心信用資料(申請階段)，應採用憑證簽章之安全設計，但如為他行既有非數位存款客戶，得採用下列任一方式之安全設計：
 - 2、辦理本行個人既有數位存款帳戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計：
 - (1)本行既有第一類適用低風險交易之數位存款帳戶，辦理簽約對保應採用下列任一方式之安全設計：
 - 甲、採用存款帳戶之財金公司「跨行金融帳戶資訊核驗」，並搭配知識詢問或上傳身分證影像檔之安全設計機制辦理簽約對保者，得將款項撥入本人非數位存款帳戶。
 - 乙、採用包含生物特徵之「兩項以上技」搭配軟體 C3 憑證簽章或知識詢問辦理簽約對保，得將款項撥入本人存款帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。
 - (2)本行既有第三類數位存款帳戶，辦理簽約對保應採用下列任一方式之安全設計：
 - 甲、採用硬體憑證簽章安全設計。
 - 乙、採用視訊會議辦理簽約對保者，限將款項撥入本人非數位存款帳戶。
 - 丙、採用存款帳戶之財金公司「跨行金融帳戶資訊核驗」，並搭配知識詢問或上傳身分證影像檔之安全設計機制辦理簽約對保者，得將款項撥入本人非數位存款帳戶。
 - 丁、採用包含生物特徵之「兩項以上技術」搭配軟體 C3 憑證簽章或知識詢問辦理簽約對保，得將款項撥入本人存款帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。
 - (3)本行既有第三類數位存款帳戶，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」及硬體憑證簽章辦理簽約對保者，得將款項撥入他行第三方公司之實體帳戶。
 - 3、辦理本行個人既有信用卡客戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計：
 - (1)採用包含生物特徵之「兩項以上技術」搭配軟體 C3 憑證簽章或知識詢問辦理簽約對保，得將款項撥入本人存款帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。
 - 4、辦理本行個人新戶之貸款契約或保證人保證契約成立，簽約對保方式應採用下列任一方式之安全設計：
- (三)辦理法人授信業務應遵循下列要求：
- 1、辦理本行既有法人客戶及法人新戶同意金融機構查詢聯徵中心信用資料，應採用下列安全設計機制：
 - (1)採用硬體憑證簽章之安全設計。
 - (2)法人戶之負責人或保證人或依信保基金規定應查詢之關係人(如配偶)同意

金融機構查詢聯徵中心信用資料之安全設計，應比照個人授信案件有關本行新戶同意金融機構查詢聯徵中心信用資料之安全設計。

2、辦理本行既有法人客戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計：

(1)採用硬體憑證簽章之安全設計。

(2)透過本行法人戶申請平台驗證檢核既有客戶事先以授權書方式授權原留存印鑑之安全設計。上述檢核流程應透過公司負責人進行線上身分驗證後傳送印鑑，公司負責人身分驗證須依個人貸款身分確認機制，相關檢核及驗證軌跡、紀錄等應比照相關規定辦理。

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

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

(1)採用硬體憑證簽章之安全設計。

(2)採用視訊會議，並搭配存款帳戶之財金公司「跨行金融帳戶資訊核驗」。

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

(四)辦理信託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、固定密碼之任一款安全設計，但本基準另有限制者，從其規定。

伍、交易面之介面安全設計具體要求

一、採用憑證簽章，應遵循下列安全設計：

(一)應採用經本會認可之憑證機構及其所簽發之憑證，並遵循憑證機構之憑證作業基準檢核其憑證措施，以加強安控機制，維護網路交易安全。已通過審查之憑證及適用範圍如下：

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

2、採用經密碼保護之臺灣網路認證公司簽發第三級商務 EC+憑證、第三級商務 XML 憑證或中華電信公司簽發第三級 Public CA 憑證。上述 C3 憑證僅能應用於非電子轉帳及交易指示類服務、電子轉帳及交易指示類之申請指示服務，如若以臨櫃或憑證簽章、晶片金融卡、一次性密碼、「兩項以上技術」、視訊會議之任一款安全設計進行身分確認者，方能辦理不涉及非約定轉入帳戶轉帳之低風險交易，惟金融機構應確保金鑰儲存安全。

(二)應用於高風險交易或開立第一類適用高風險交易之數位存款帳戶進行身分驗證者，憑證私鑰應儲存於經第三方認證之硬體裝置。

二、採用一次性密碼，應遵循下列安全設計：

(一)採用簡訊傳送 OTP 時，應遵循下列安全設計：

1、應用於電子轉帳交易指示類時，應與發送行銷廣告之門號有所區隔。

2、應用於電子轉帳交易指示類並以簡訊傳送 OTP 重新設定固定密碼或重新綁定兩項以上技術時應加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP 綁交易、語音 OTP、SIM 卡認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易內容或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)，該機制應排除固定密碼或電子郵件認證。

3、應用於非約定轉入帳戶轉帳交易時，應遵循下列安全設計：

- (1) 考量客戶交易使用之電腦或行動裝置，可能遭植入惡意程式竊取 OTP 等敏感資料，應加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP 綁交易、語音 OTP、SIM 卡認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易內容或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)。

三、採用知識詢問或固定密碼之安全設計時，僅限應用於辦理非電子轉帳及交易指示類及下列電子轉帳及交易指示類之業務：

(一) 財富管理業務

- 1、非首次之認識客戶作業。
- 2、非首次之客戶風險承受度測驗。
- 3、同意用詞定義第二十款第一目結構型商品業務之推介或終止推介。

(二) 信託業務

- 1、非首次之認識客戶作業。
- 2、非首次之客戶風險承受度測驗。
- 3、信託業推介及終止推介同意書。
- 4、同意簽署為專業投資人。
- 5、專業投資人聲明表示已充分審閱而無須適用審閱期之規定。

陸、交易面之應用系統之安全設計：

一、提供網際網路應用系統，應遵循下列必要措施：

(一) 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、針對固定密碼應提供端點對端點加密機制。係指於客戶端(如瀏覽器)輸入資料後立即加密，傳送至金融機構可信任網段(如經兩道防火牆隔離之獨立網段)於符合 FIPS 140-2 Level 3 以上之硬體安全模組(如 HSM)內進行解密，並於硬體安全模組內或於無洩漏解密資料疑慮之安全環境進行驗證；如用戶代號為個人統一編號者，其使用者代號仍應加強防護(如雜湊、加密、混淆)。

二、提供客戶端電腦應用程式，應遵循下列必要措施：

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

三、透過 QR Code 進行資料傳輸，應遵循下列必要措施：

- (一) QR Code 表示的資料應為辦理該業務所需最小化為原則。
- (二) 應用於電子轉帳及交易指示類時，應設計合理使用時效，且在時效內以使用一次為限
- (三) 所產生之 QR Code，如具客戶個人資料應符合訊息隱密性、如應用於電子轉帳及交易指示類時，應符合訊息完整性、訊息來源辨識性與訊息不可重複性。
- (四) 應針對解析 QR Code 後進行格式檢查，如為網站連接應進行網站合法性檢查。

柒、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。