本會112年3月30日第14屆第5次理監事聯席會議核議通過
金管會113年1月29日金管銀外字第1120135878號函洽悉

金融機構使用電子簽名機制安全控管作業規範

第一條　為強化銀行使用電子簽名機制提供客戶線上簽署電子文件之安全控管，並有一致性之作業準則，特訂定本作業規範(以下簡稱本規範)。

銀行使用電子簽名機制之安全控管作業，依本規範之規定；本規範未規定者，依「金融機構辦理電子銀行業務安全控管作業基準」(以下稱「安控基準」)之規定。

第二條　本規範用詞定義如下：

一、線上簽署：指客戶透過電子簽名平臺於線上簽署相關書件，排除行員實體見證客戶於裝置線上親簽之作業。

二、電子簽名機制：指採用美國國家標準研究院(NIST)、歐洲電信標準協會(ETSI)或 ISO 所制定或核可之簽章格式及演算法進行電子文件簽章。

三、電子簽名平臺：指辦理電子簽名相關作業之應用軟體、作業系統及其硬體設備，銀行得自建或委由第三方辦理。

四、電子簽名作業環境：指電子簽名平臺、用於管理或防護電子簽名平臺之系統(如防毒軟體)及其平臺與系統維運人員之應用軟體、作業系統及其硬體設備。

五、系統維運人員：指電子簽名平臺之作業人員，負責管理或操作營運環境之應用軟體、系統軟體、硬體、網路、資料庫、客戶服務、業務推廣、帳務管理或會計管理等作業。

六、接觸式介面：指使用裝置內的探針以物理方式接觸另一設備(如卡片)，進行資料交換。

七、非接觸式介面：指使用裝置內的感應設備(如 NFC 近場通訊、藍芽等)以非接觸方式靠近另一設備(如

卡片)，進行資料交換。

八、 申請指示類業務：

(一)安控基準電子轉帳及交易指示類之申請指示所列示之服務項目。

(二)衍生性金融商品業務，辦理與安控基準申請指示服務中有關財富管理業務得提供之同類服務項目者。

九、 交易指示類業務：安控基準電子轉帳及交易指示類之低風險交易，及衍生性金融商品同一統一編號交割款項入扣帳指示，並排除申請指示所列示之服務項目。

十、 評估單位：指同時符合下列條件之外部專業機構或銀行內部之個人或團隊。

(一)資訊安全管理知識(如 CISM、ISO 27001LA 等)。

(二)資訊安全技術能力(如 CISSP)。

(三)模擬駭客攻擊能力(如 CEH、CIH 等)。

(四)熟悉金融領域載具應用、系統開發或稽核經驗(如 CISA)。

第三條　銀行受理既有法人客戶申辦電子簽名時應進行身分核驗，並取得同意以電子簽名線上簽署電子文件，留存申請紀錄以供備查。相關安全設計應符合下列要求：

一、應留存意思表示之確認(如公司及負責人印鑑)並辨識相符。

二、銀行應取得法人客戶書面同意指派電子文件簽署人(以下簡稱簽署人)，簽署人亦得由法人客戶指派之兩位以上電子簽名授權人員(以下簡稱授權人員)以電子簽名向銀行指派，惟法人客戶之授權人員以電子簽名方式指派簽署人時，不得涉及任一授權人員與簽署人為同一人之情形。

三、授權人員應由法人客戶以書面同意方式向銀行指派。

銀行應針對業務及客戶進行風險評估，訂定申請資格與管控機制，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。

第四條　銀行受理既有法人客戶辦理電子簽名之註冊、簽名、註銷、異動等作業，應符合下列要求：

一、註冊作業：

(一)客戶於完成第三條身分核驗後，得於客戶端或銀行端(含第三方平臺)電子簽名平臺產生電子簽名金鑰對，完成註冊作業。

(二)客戶如未能於臨櫃或同一設備且同一連線階段(session)下完成前目註冊作業者，得將第三條身分核驗結果產製一啟用碼，供客戶接續完成註冊作業。

(三)前目啟用碼應搭配如簡訊 OTP 或軟體 OTP 等機制再次核驗客戶身分，並訂定三天內之有效期限，且在期限內以使用一次為限。

(四)配合簽名作業之身分核驗，應採用並設定晶片金融卡、一次性密碼或兩項以上技術任一款安全設計。

二、簽名作業：

(一)採用前款於註冊作業設定或綁定之晶片金融卡、一次性密碼或兩項以上技術任一款安全設計進行身分核驗，惟採用簡訊傳送 OTP 者應加強防護，該防護機制應經過銀行風險評估，並應留存評估紀錄及核決層級。

(二)採用美國國家標準研究院(NIST)、歐洲電信標準協會(ETSI)或 ISO 所制定或核可之簽章格式及演算法進行電子文件簽章，銀行並應取得所採用簽章格式及演算法符合上開規定之具公信力第三方證明。

(三)針對簽章內容進行核驗，以確認簽署人身分及依據簽署之電子文件辦理相關業務。

三、註銷作業：應採用適當身分核驗方式後辦理註銷電子簽名之帳戶。

四、異動作業：應驗證有效之電子簽名或依第三條規定

重新辦理身分核驗後異動所採用之身分辨識機制。

第五條　銀行進行簽名作業，對於不同金鑰持有及儲存機制，適用下列應用範圍：

一、簽名私鑰儲存於客戶端或銀行端(含第三方平臺)者得辦理申請指示類業務。

二、簽名私鑰於客戶端產生並儲存於客戶端者得辦理申請指示類及交易指示類業務。

第六條　電子簽名平臺管理，應遵循下列要求：

一、銀行自建電子簽名平臺者，其電子簽名平臺與電子簽名作業環境應符合「金融機構資通安全防護基準」相關要求。

二、銀行採用第三方平臺提供電子簽名服務者，應遵循下列事項：

(一)應建立評估機制，內容包含但不限於內部控制制度、財務健全性、營運持續性、資料安全及資料保護等並留存紀錄及核決層級。

(二)第三方之電子簽名平臺與電子簽名作業環境應取得有效 ISO 27001 及 AICPA SOC，另使用雲端服務者應取得有效 ISO 27017 及 CSA STAR 等國際認證或報告。

(三)於服務契約終止或轉移時，應將客戶留存於第三方之個人資料與身分確認資料刪除(如電子簽名金鑰)。

三、除前二款規定外，銀行並應符合「安控基準」相關規範。

第七條　銀行與客戶約定使用電子簽名，至少應告知下列事項以確保客戶權益：

一、銀行應取得客戶同意使用電子簽名機制及簽署電子文件。

二、銀行應告知客戶有關使用電子簽名及讀取電子文件所需之軟體及硬體等設備條件。

三、客戶同意使用電子文件簽署文件的範圍。

四、客戶有權利得索取紙本或非電子文件形式之紀錄或

備份、客戶行使權利之程序、取得紙本或非電子文件形式紀錄或備份之相關費用資訊。

五、 客戶得於一定期間前以書面或其他與銀行所約定之方式，向銀行請求停止電子簽名機制之使用。惟客戶先前以電子簽名所簽署之電子文件，效力不受影響。

提供電子簽名服務之書面契約，應包含約定雙方之權利義務關係(例如過失責任歸屬以及銀行得視需要採取其他適當措施確認電子文件之有效性)、適用範圍、爭議處理程序、爭議管轄法院、契約暫停或終止條款以及相關風險揭露等，同時應遵循個人資料保護法、金融消費者保護法及銀行法等相關法令規定，不得違反法令強制或禁止規定，且不得有侵害客戶利益或其他不當之行為。如有疑義時，應作有利客戶之解釋為原則。

銀行若發生異常事故、重大缺失或違反法令之情事，於影響客戶權益時應儘速通知客戶，並應儘速採取適當之因應措施以降低對客戶可能造成之影響。

銀行應建立消費者爭端解決機制，包括解決時程、程序及補救措施。當發生消費爭議時，提供客戶申訴管道，以妥適處理消費爭議。

第八條　銀行應盤點與資訊安全相關規定，並將相關要求與內部控制制度結合，定期進行法令遵循自評，以確保資訊安全之法令遵循性。

本規範所訂之資訊系統及安全控管項目，應透過內部控制制度進行定期檢核，並應依相關規範定期由評估單位進行檢視，提出資訊系統及安全控管作業評估報告。

前項評估報告內容應至少包含評估人員資格、評估範圍、評估時所發現之缺失項目、缺失嚴重程度、缺失類別、風險說明、具體改善建議及社交演練結果，且應送稽核單位進行缺失改善事項之追蹤覆查。該報告應併同缺失改善等相關文件至少保存二年。

銀行應確保其本身、主管機關及中央銀行，或其指定之人能取得辦理電子簽名之相關資訊（包括相關系統之查核

報告）及實地查核權力。

為確保交易資料之隱密性及安全性，並維持資料傳輸、交換或處理之正確性，銀行於必要時得提高電子簽名作業環境相關資訊系統標準及加強安全控管作業。

第九條　本規範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。