金融機構辦理行動金融卡安全控管作業規範

附件一

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106年12月29日金管銀國字第10600311110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9月4日金管銀國字第1090140258號函洽悉

第一條　中華民國銀行商業同業公會全國聯合會（以下簡稱本會）為確保金融機構辦理行動金融卡具有一致性安全控管，特訂定本作業規範。

第二條　本規範用詞定義如下：

一、行動金融卡：係指透過空中傳輸下載個人化資料至行動裝置，發行具行動交易功能之金融卡。

二、交易主金鑰：係指用來產生交易金鑰之金鑰。

三、交易金鑰：係指用於交易，以產生交易驗證資訊（如：TAC,Transaction Authentication Code、ARQC,Authorization Request Cryptogram、TAVV, Transaction Authentication Verification Value 或AAV, Accountholder Authentication Value 等）之金鑰。

四、交易金鑰更新：金鑰採軟體保護技術者，因採交易金鑰機制，須適時管理交易金鑰之有效性，並更新金鑰至持卡人行動載具。

五、製卡個人化資料：係指足以製作成金融卡所需之完整個人化資料。

第三條　行動金融卡申辦作業應符合下列控管要求：

一、發卡對象限已開立存款帳戶且已申請實體金融卡者，惟第三類數位存款帳戶需經透過跨行金融資訊網路事業之「跨行金融帳戶資訊核驗」進行身分驗證。

二、行動金融卡分類如下：

(一)第一類行動金融卡：線上申辦應依據金融機構辦理電子銀行安全控管基準（以下簡稱安控基準）第七條第一款至第四款任一款安全設計進行身分確認。若以行動電話門號OTP驗證，設定該門號應採兩項以上技術機制。

(二)第二類行動金融卡：線上申辦應依據安控基準第七條第一款至第七款之任一款安全設計進行身分確認。

三、行動金融卡應用範圍及交易限額如下：

(一)第一類行動金融卡可應用於安控基準第四條低風險之第2、4、5、7、10項，其限額要求如下，應用於非約定轉帳交易時，每筆最高限額為3萬元、每日累計最高限額為3萬元、每月累計最高限額為10萬元；應用於提款交易時，

每筆最高限額為2萬元、每日累計最高限額為2萬元、每月累計最高限額為2萬元。

(二)第二類行動金融卡僅可應用於消費交易。

(三)金融卡消費額度應由金融機構訂定，其風險控管機制應將行動金融卡併入管理。

四、應控管每一存款帳戶申請之行動金融卡數量。

五、執行金融卡個人化作業時，於處理或傳輸金融卡個人化資料後，不得留存製卡個人化資料。

六、個人化資料在空中傳輸過程，應符合安控基準第五條訊息隱密性及訊息完整性之安全需求。

七、下載個人化資料前，應確認使用之行動裝置或安全儲存媒介，為申請人申辦時指定之行動裝置或安全儲存媒介。

八、行動金融卡下載後，應以原留存發卡行之通訊管道（如簡訊或電子郵件）或雙方約定方式通知申請人。

第四條　執行亂碼化作業時，應符合下列控管要求：

一、伺服器端若儲存或處理交易主金鑰，應採用硬體安全模組(HSM，Hardware Security Module)處理加解密相關作業，且該設備應通過FIPS 140-2 Level 3 以上或其他相同安全強度之認證。

二、有關對稱性金鑰，應依金鑰之用途及不同之通信單位，建立各自之獨立金鑰，避免不同用途或不同單位共用相同之金鑰。

三、金鑰之使用、儲存、備份、傳送與銷毀，應確保其內容不以任何形式洩露。

四、保存金鑰之設備或媒體，於更新或報廢時，應具適當之存取控管程序，以確保金鑰無洩露之虞。

五、金鑰交換應符合安控基準第五條訊息隱密性及訊息完整性之安全需求。

第五條　行動裝置端之金鑰管理作業應符合下列控管要求：

一、金鑰採硬體保護技術且應用於第一類行動金融卡時，金鑰應儲存於符合我國國家標準 CNS 15408 EAL5、共通準則(Common Criteria)ISO/IEC 15408 v2.3 EAL 5、FIPS 140-2 Level 3 以上或其他相同安全強度之安全元件(SE)內，並能防堵市面上常見之攻擊破解方法。若應用於第二類行動金融卡時，金鑰應儲存於符合EMVCo Security Evaluation Process或其他相同安全強度之安全元件內，並能防堵市面上常見之攻擊破解方法。

二、金鑰採軟體保護技術時，應符合下列控管要求：

(一)第一類行動金融卡採遠端交易與近端交易應使用不同的金

鑰或採不同演算法。

(二)行動裝置所存放之交易金鑰，一次可存放多把，並限制每把金鑰可使用次數。

(三)交易金鑰更新時，系統應比對確認為客戶與金融機構所約定持有之行動裝置，如發現異常，應進行監控。

(四)交易金鑰使用時，應於使用者裝置端進行驗證（如密碼、指紋）。

(五)交易金鑰更新時，行動裝置與伺服器端應通過雙向確認且相關資料的傳輸過程應符合安控基準第五條訊息隱密性及訊息完整性之安全需求。

(六)第一類行動金融卡遠端交易所使用的交易金鑰之控管機制應較近端交易更為嚴謹（如減少每次下載的金鑰數量或縮短效期等）。

第六條　應用系統應符合下列控管要求：

一、應設定可容忍交易錯誤次數之邊界值，應對此邊界值建立相關警示監控機制。

二、當使用者驗證錯誤累積錯誤次數達設定之邊界值時，必須暫時停止該卡片之使用。

三、於交易驗證時，交易驗證碼之交易序號應大於前次留存的交易序號。

第七條　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。