信用卡業務機構辦理手機信用卡業務安全控管作業基準

中華民國101年11月6日

信用卡業務機構辦理手機信用卡業務安全控管作業基準總說明

行動通信設備與無線通訊多元化的發展，手機單純的通話用途隨著無線通信技術成熟的運用與快速的演進，同時利用晶片的防偽和高可攜性的安全特質，進而衍生許多的日常生活應用。而結合近端行動通信技術及行動交易手機上之安全儲存媒介（SE，Secure Element)〔註一〕的近端行動交易（Proximity Mobile Payment）應用，更將信用卡消費與行動支付帶入嶄新科技的里程碑。

近來信用卡業務機構（發卡機構）相繼與信用卡組織及行動通信業者攜手合作，藉由通信業者架構的通訊環境及先進的技術，結合信用卡與行動交易手機上之安全儲存媒介（SE）做為信用卡消費支付工具，針對特定的使用者在約定的特約商店中進行體驗測試計劃，如感應式行動付款、下載智慧型海報（Smart Poster）電子優惠券（E-coupon)、簡訊電子優惠券服務等，讓使用者在生活應用中明顯感受到更多的便利與娛樂。基於此成功的經驗，進而開創相關金融商機及業務，也因此建構多元化透通性之支付環境，同時也透過手機螢幕與鍵盤提供的介面，期能開創市場多功能應用的商機，考量信用卡新種業務的差異〔註二〕及風險，為保障持卡人權益，健全信用卡業務發展，同時衡酌市場之實際需要及業界實務，並參考相關信用卡組織之規範，研訂本手機信用卡業務安全控管作業基準（以下簡稱本安控基準)，俾利信用卡業務機構遵循。

本安控基準主要規範信用卡業務機構（發卡機構）自主發行或與行動通信業者共用安全儲存媒介（SE)，針對安全儲存媒介進行晶片個人化作業（Personalization）之安全控管。倘以接觸式方式進行晶片個人化作業或信用卡業務機構（發卡機構）獨立使用信用卡應用程式儲存媒介者，則依據信用卡組織作業規範辦理即可。

安全儲存媒介發行方式	信用卡晶片個人化作業方式	安全控管基準
信用卡業務機構（發卡機構）自主發行	依傳統信用卡方式,將資料交付個人化處理中心作業	信用卡組織作業規範
	透過空中傳輸(OTA,Over the Air）方式進行信用卡晶片個人化作業	信用卡組織作業規範及本安控基準
與行動通信業者共用安全儲存媒介	透過空中傳輸（OTA）方式進行信用卡晶片個人化作業	信用卡組織作業規範及本安控基準

另有關本業務的相關名詞定義於「第二章、手機信用卡業務之定義」。

茲將本基準要點說明如次：

一、信用卡與行動交易手機上之安全儲存媒介的整合應用，依據各信用卡組織公告之規格與作業規範（附錄：手機信用卡交易之信用卡組織規範），發行具近端行動交易之手機信用卡業務，信用卡業務機構（發卡機構）可因業務需求，包含但不限於整合行動通信業者（MNO, Mobile Network Operator）及 TSM（Trusted Service Manager）服務平台〔註三〕等不同業者相關的作業，透過空中傳輸（OTA）的技術及通訊的傳輸方式完成信用卡個人化的作業，經過完成信用卡個人化作業及相關開通程序後，手機信用卡就如一般感應式的實體信用卡，可在裝有感應設備之信用卡特約商店以感應交易（Contactless Transaction）進行消費簽帳；本安控基準「第三章、手機信用卡作業模式」，概述手機信用卡作業模式在作業流程中涉及個人化資料傳輸之主要途徑，作為信用卡業務機構之參考，業務機構得依內部流程規範、信用卡組織及金融主管機關在安全控管的機制下訂定細部作業流程。

二、鑒於新技術的應用有別於現行的晶片個人化作業製程，針對使用者晶片內信用卡資料的流向，增訂本安控基準以為依循；本業務中，若經由 TSM 服務平台提供安全管理服務，則該 TSM 應經信用卡組織認證。TSM 服務平台主要是提供包含但不限於信用卡業務機構、行動通信業者等便利且安全可靠的平台，透過此服務平台與各系統之間運作的整合，為確保行動通信業者（MNO）與應用服務供應商營運模式的安全性，服務平台提供金鑰管理以及維護，同時執行包含但不限於公正的安全策略(Security Policy)及管理安全儲存媒介（SE）中應用程式與其生命週期，整體作業均在發卡程序規範及卡片個人化標準文件所要求的安全標準程序下進行〔註四〕；因此，在空中傳輸（OTA）行動網路的環境中，個人化的一切安全操作流程及安全認證均以此標準程序之協定為基礎，建立安全模式，此外，本安控基準「第四章、手機信用卡之安全管控」就安全設計通則及特殊安全設計訂定安全的作業原則。

三、本作業除依據信用卡會員申請書約定條款辦理外，於「第五章、手機信用卡發卡機構與手機信用卡持卡人間權利義務」亦規範本業務之發卡機構應提供相關操作與使用說明，並制定完整合約述明與持卡人間權利義務關係。

行動交易手機的應用，從手機間通話的語音服務，進而發展多媒體開啟數據應用服務，如今結合服務供應商、金融商品、空中傳輸（OTA）、近距離無線通訊（NFC，Near Field

Communication）等無線通信的技術及 TSM 服務平台，已進入感應式行動應用服務，在高規格安全的作業規範下，讓行動交易手機擁有更多功能及應用，行動通信帶來金融交易可以在不同時間地點提供服務的便利性，這是以往傳統資訊架構所無法達成的，近些年在國外針對無線通信的應用，也積極進行各種試用計畫，在行動交易手機逐漸走入與生活整合應用階段，整合感應式晶片卡應用已是相關服務供應商努力推展的目標，就現行信用卡業務而言，已正式邁入另一服務層次，透過異業結盟合作及成熟的通信技術，在種種安全規範下有效率的將行動交易手機結合信用卡服務做廣泛的應用，同時也節省發卡成本。本安控基準，從許多構面研訂縝密的安全機制，確實保護這些信用卡的資訊，同時提供使用者一個既安全又便利的無線行動金融服務。

註一：安全儲存媒介（SE，Secure Element）：

儲存應用程式（Application）與相關資料（Data）之安全模組。可依不同方式將信用卡相關資料寫入，如將資料交付個人化處理中心進行晶片個人化作業，或透過空中傳輸（OTA）方式下載……等等。

註二：有別於傳統信用卡的差異主要是在信用卡資料的安全儲存媒介、信用卡晶片個人化作業及資料傳輸方式；一般信用卡為實體製卡，客戶個人信用卡資料於信用卡發卡機構製卡時，即以一般接觸式的方法進行晶片個人化作業，同時錄製於實體信用卡晶片內；而本業務則可採取信用卡發卡機構自主發行或與行動通信業者共用安全儲存媒介（SE）兩種可能選項。若客戶向信用卡發卡機構申請並藉由通信服務，由客戶自行在手機上啟動下載個人信用卡資料的功能，則經過 TSM 服務平台以 OTA 的技術及通訊的傳輸方式，將信用卡相關資料傳輸至客戶特定的行動交易手機上之安全儲存媒介，而完成信用卡個人化的作業，並經相關開卡程序後，即如現行非接觸式實體信用卡，可在裝有接收設備之信用卡特約商店以感應交易（Contactless Transaction）消費簽帳，後續消費交易的處理程序相同。

註三：TSM 服務平台(Trusted Service Manager): TSM 服務平台能讓下載信用卡相關資訊到手機的整個流程既效率且安全,它能搭起銀行與電信業者之間的橋樑, 並確保持卡人卡片資訊是充份安全的。

註四：現有的標準發卡程序規範中，安全通道協定(SCP，Secure Channel Protocol)便定義了初始更新(Initialize Update)及外部認證(External Authenticate)的安全認證程序。而 EMV 卡片個人化標準文件（EMV CPS，EMV Card Personalisation Specification）也定義了對稱加密的安全協定為重要基礎，同時提供交易訊息完整性鑑別(MAC，Message Authentication Code)及加密傳輸等功能作為建立安全通道與認證。

信用卡業務機構辦理手機信用卡業務安全控管作業基準

本案業經金融監督管理委員會101年11月6日金管銀票字第10100348700號函准予備查。

第一章、前言：

一、為確保信用卡業務機構辦理手機信用卡業務具有一致性安全控管，特訂定本作業基準。

二、本作業基準主要規範信用卡業務機構（發卡機構）自主發行或與行動通信業者共用安全儲存媒介（Secure Element）時，針對安全儲存媒介進行信用卡晶片個人化作業（Personalization）之安全控管作業。

三、信用卡業務機構（發卡機構）與行動通信業者共用安全儲存媒介時，行動通信業者為安全儲存媒介之所有權人，手機信用卡發卡機構具有安全儲存媒介部分空間－特定安全區域之使用權、控管權及信用卡應用程式所有權；行動通信業者應依據本安控基準及信用卡組織規範，妥善管理該安全儲存媒介，並與手機信用卡發卡機構共同服務手機信用卡持卡人。

四、信用卡業務機構（發卡機構）自主發行安全儲存媒介時，信用卡業務機構（發卡機構）為安全儲存媒介之所有權人，手機信用卡發卡機構具有該安全儲存媒介全部空間－全部安全區域之使用權、控管權及信用卡應用程式所有權；手機信用卡發卡機構可提供安全儲存媒介之特定部分空間供服務供應商使用。手機信用卡發卡機構應依據本安控基準及信用卡組織規範，妥善管理該安全儲存媒介，並服務手機信用卡持卡人。

安全儲存媒介發行方式	信用卡晶片個人化作業方式	安全控管基準
信用卡業務機構（發卡機構）自主發行	依傳統信用卡方式,將資料交付個人化處理中心作業	信用卡組織作業規範
	透過空中傳輸（OTA）方式進行信用卡晶片個人化作業	信用卡組織作業規範及本安控基準
與行動通信業者共用安全儲存媒介	透過空中傳輸（OTA）方式進行信用卡晶片個人化作業	信用卡組織作業規範及本安控基準

第二章、手機信用卡業務之定義：

手機信用卡業務係指信用卡業務機構（發卡機構）依據信用卡組織公告規格（Specification）與作業規範，發行具近端行動交易功能之手機信用卡並辦理相關業務。相關名詞定義如下：

一、安全儲存媒介（SE，Secure Element）：

儲存應用程式（Application）與相關資料（Data）之安全模組。可依不同方式將信用卡相關資料寫入，如將資料交付個人化處理中心進行晶片個人化作業，或透過空中傳輸（OTA）方式下載等等。安全儲存媒介可有不同選擇，包含但不限於置於手機上之USIM卡、Micro SD卡、手機上之晶片或外部裝置（如手機套、貼片…等等）。

二、安全區域（SD，Security Domain）

安全儲存媒介（SE）中切分具加密特性之儲存空間。單一安全儲存媒介（SE）可切分為多個安全區域並支援多個應用程式（Multi-application）。安全儲存媒介（SE）中各個安全區域之控管者會建立該安全區域之控管金鑰（Key），使用該金鑰僅可控管對應的安全區域，即安全儲存媒介（SE）中所有安全區域各自獨立，各區域下的應用程式與相關資料由該區域控管者全權管控，未經授權者無法更改。

三、近端行動交易（Proximity Mobile Payment）

持卡人使用內含安全儲存媒介之行動通信設備，於裝有感應設備之信用卡特約商店以感應交易（Contactless Transaction）消費簽帳。

四、空中傳輸（OTA，Over the Air）

使用行動通信業者無線傳輸方式，進行安全儲存媒介內軟體、參數設定、相關資料之下載或更新。

五、近端行動通信技術

支援各種信用卡行動交易設備可採用之無線通信技術。例如：近距離無線通訊（NFC，Near Field Communication）技術，以內建NFC晶片與感應線圈之NFC手機為例，當其他寫有特定應用程式（Application，如門禁、晶片紅利、支付工具…等等應用程式）之晶片與NFC晶片連結，可運用手機中感應線圈以執行感應式交易。

六、行動交易手機

通過行動通信業者主管機關或其委託機構之認證、可支援行動交易之工具。

七、行動交易手機製造商

開發製造行動交易手機者。

八、行動通信業者

具有行動通信執照的行動網路營運商（MNO，Mobile Network Operator），提供行動通信服務予手機信用卡持卡人。

九、服務供應商（Service Provider）

提供安全儲存媒介中應用程式與相關服務者。

十、手機信用卡發卡機構

信用卡業務機構經主管機關同意開辦手機信用卡業務者，為手機信用卡發行與晶片個人化作業執行者。

十一、安全儲存媒介（SE）製造商

依據信用卡組織公告規格，提供手機信用卡發卡機構、行動通信業者或行動交易手機廠商合格安全儲存媒介以存放應用程式及個人化資料者。

十二、TSM（Trusted Service Manager）服務平台

TSM服務平台能讓下載信用卡相關資訊到手機的整個流程既效率且安全，它能搭起銀行與電信業者之間的橋樑，並確保持卡人卡片資訊是充份安全的〔註〕。

十三、手機信用卡操作介面軟體

存放於手機或安全儲存媒介中，由手機信用卡發卡機構提供手機信用卡持卡人使用、查詢信用卡業務機構提供應用程式之軟體。

十四、敏感性資料

係指製作成偽冒信用卡之所需資料。

註：TSM服務平台可提供之服務包括下列事項：

（一）管理/傳輸手機信用卡持卡人認證。

（二）管理、執行NFC相關服務；例如透過OTA空中傳輸方式將應用程式與相關資料下載至安全儲存媒介中、透過OTA空中傳輸方式對安全儲存媒介執行個人化作業。

（三）管理安全儲存媒介中應用程式與其生命週期。

（四）居間為服務供應商與行動通信業者交換、傳遞訊息。

第三章、手機信用卡作業模式

一、手機信用卡發卡機構自主發行安全儲存媒介且手機信用卡個人化並未透過 OTA 方式完成者，則其資料作業方式依據信用卡組織作業規範辦理。

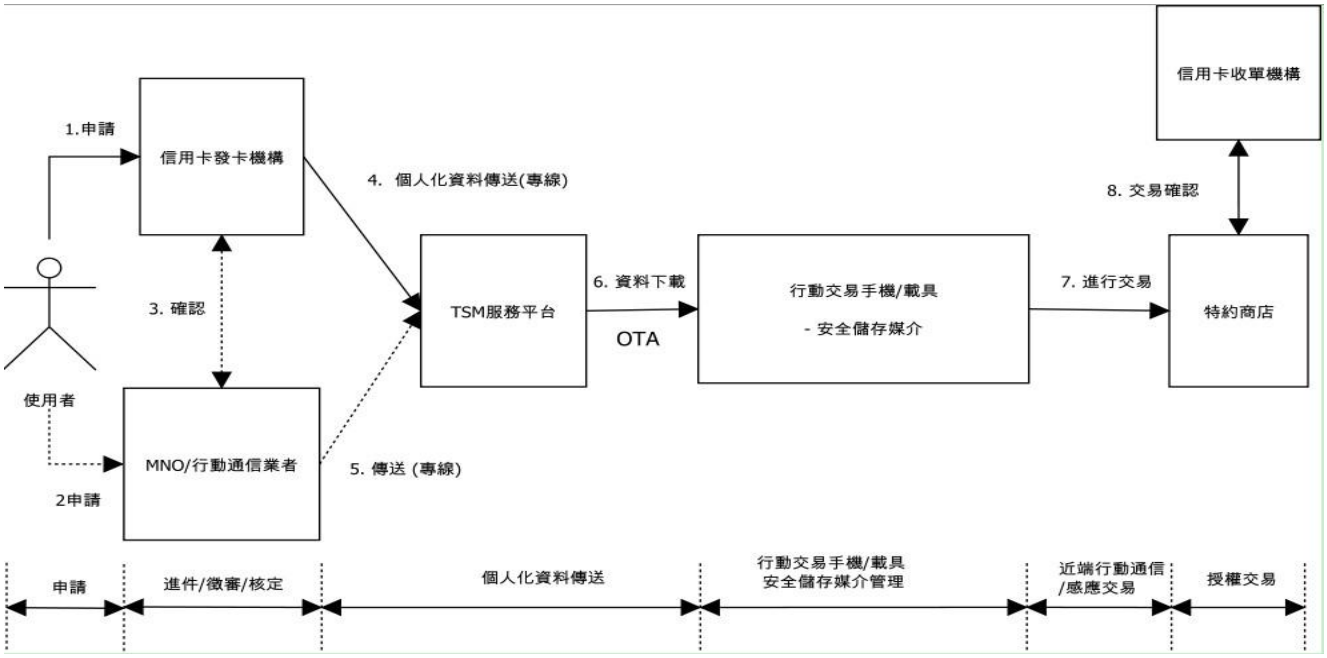
二、手機信用卡發卡機構透過空中傳輸（OTA）的技術及傳輸方式，完成手機信用卡晶片個人化作業，其作業方式如下：

（一）使用者向信用卡業務機構申請手機信用卡核准後，信用卡業務機構將信用卡個人化資料（Perso Data）、手機號碼及安全儲存媒介編號傳送至 TSM 服務平台。

（二）TSM 服務平台向行動通信業者確認手機號碼及安全儲存媒介編號之正確性。

（三）倘資料正確，TSM 服務平台透過行動通信業者網路執行空中傳輸（OTA）作業，將信用卡應用程式（payment application）與個人化資料傳送至持卡人手機，並寫入安全儲存媒介及安全區域中。

本業務資訊傳輸之途徑如下:



註：以上虛線程序為選擇性。

1. 使用者取得申辦之行動交易手機後，向行動通信業者及信用卡發卡機構提出申請（如上圖 1，2）。
2. 信用卡發卡機構及行動通信業者依內部程序進行「審核」之程序；其中雙方可針對持卡人信用卡與行動交易手機做身份上的確認（如上圖 3）。

3. 核可後之資料透過安全的資料傳輸方式及程序（如上圖 4，5）傳送至 TSM 服務平台執行信用卡及手機資料彙整。
4. TSM 服務平台在安控的基礎下透過空中下載的技術，將信用卡的資料下載至行動交易手機之 SE/SD 完成信用卡個人化作業（如上圖 6）。
5. 結合信用卡與行動交易手機如同現行非接觸式信用卡，經過開卡成功後即可於裝有接收設備之信用卡特約商店以感應交易（Contactless Transaction）消費簽帳（如上圖 7，8）。

第四章、手機信用卡之安全管控

安全設計通則：

本通則包含訊息隱密性、訊息完整性、來源辨識性、不可重覆性及金鑰管理之安全要求，其標準如下：

一、訊息隱密性：應採對稱性加解密系統或非對稱性加解密系統，針對訊息進行全文加密，以防止未經授權者取得訊息之明文。

（一）對稱性加解密系統應採用下列演算法之一：

1. 美國國家標準與技術中心（National Institute of Standards and Technology；以下簡稱 NIST）之三重資料加密演算法（Triple Data Encryption Algorithm; 以下簡稱 TDEA 演算法），金鑰有效長度為 112 位元雙金鑰之三重資料加密演算法(Two Key Triple Data Encryption Algorithm;以下簡稱 2TDEA)或 168 位元三金鑰之三重資料加密演算法(Three Key Triple Data Encryption Algorithm; 以下簡稱 3TDEA)。
2. NIST 之進階加密標準（Advanced Encryption Standard；以下簡稱 AES 演算法），金鑰長度為 128、192 或 256 位元。

（二）非對稱性加解密系統應採用下列演算法之一：

1. RSA 加密標準（Rivest、Shamir、Adleman Encryption Standard；以下簡稱 RSA 演算法），金鑰長度 1024 位元(含以上)。
2. 橢圓曲線數位簽章演算法（Elliptic Curve Digital Signature Algorithm；以

下簡稱 ECDSA 演算法)，質數模數為 256 位元(P-256)。

二、訊息完整性：應採用可防止蓄意篡改訊息之加解密技術，可採對稱性加解密系統進行押碼(Message Authentication Code, MAC)或非對稱性加解密系統產生數位簽章(Digital Signature)等機制。

（一）對稱性加解密系統應採用下列演算法之一：

1. TDEA 演算法，金鑰有效長度為 112 位元(2TDEA)或 168 位元(3TDEA)。

2. AES 演算法，金鑰長度為 128、192 或 256 位元。

（二）非對稱性加解密系統應採用下列演算法之一：

1. RSA 演算法，金鑰長度 1024 位元(含以上)。

2. ECDSA 演算法，質數模數為 256 位元(P-256)。

三、來源辨識性：應確保持卡人之正確性，密碼/驗證碼可採用下列任一種持卡人認證方式。

（一）固定密碼/驗證碼：採用此方式應有下列之安全設計：

1. 固定密碼/驗證碼的長度不應少於四位。

2. 不得為相同之數字或連號數字。

3. 固定密碼/驗證碼輸入連續錯誤達五次即不得再繼續執行後續動作或交易，必須透過信用卡發卡機構的服務中心，確認身份或狀況後重新啟動相關作業。

（二）動態密碼/驗證碼：動態密碼/驗證碼係運用動態密碼產生器、簡訊、或以其他方式運用一次性密碼/驗證碼（One Time Password；以下簡稱 OTP）原理，隨機產生限定一次使用之密碼/驗證碼者。

四、不可重覆性：應防止以先前成功之交易訊息完成另一筆交易，可採用序號、日期時間或時序或密碼學挑戰-回應(Challenge-Response)等機制。

五、金鑰管理（Key Management)：金鑰管理應有下列之安全基本原則。

（一）確保金鑰之安全性及品質(避免產生弱金鑰)，應以硬體金鑰保護模組(HSM,Hardware Security Module)產生亂碼化金鑰並存放金鑰，同時符合國際資訊安全規範。

（二）金鑰使用、儲存、備份、傳送與銷毀，應確保金鑰之內容不以任何之形式洩露。

（三）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。

（四）自主發行或共用安全儲存媒介之防火牆設計須確保內部資料安全，建立保護措施，避免未經授權之存取或竄改晶片資料。

（五）金鑰交換(Key Exchange)及個人化資料下載(Personalization)應依安全設計通則之訊息隱密性及訊息完整性。

（六）非發卡機構如須刪除共用安全儲存媒介資料時，其原因、細節及權責應明訂於與發卡機構之合約中。

（七）非發卡機構處理或傳輸信用卡個人化資料後，不得留存其敏感性資料。

特殊安全設計：

本安全設計包含安全儲存媒介、行動交易手機、空中傳輸及 TSM 服務平台等四大構面之安全要求，其標準如下：

一、安全儲存媒介（SE）

（一）硬體（Hardware）與作業系統（Operation System）應依據信用卡組織規定設計。

（二）信用卡應用程式（Credit Card Application）應採用符合信用卡組織標準之應用程式。

（三）手機信用卡發卡機構與行動通信業者共用行動通信業者安全儲存媒介（SE）時，行動通信業者必須取得合作之手機信用卡發卡機構共用同意後，據以制定作業基準並確實執行，手機信用卡發卡機構應定期要求合作之行動通信業者提供相關紀錄文件與報告。

二、行動交易手機

（一）手機信用卡操作介面軟體，由手機信用卡發卡機構依信用卡組織規格與行動通信業界標準設計並建置，提供手機信用卡持卡人使用手機進行應用程式下載、交易模式設定或讀取信用卡相關資料。

（二）手機信用卡發卡機構得提供手機信用卡持卡人以下列方式啟用信用卡：

1. 手機信用卡發卡機構自主發行安全儲存媒介,且手機信用卡發卡機構事先完成手機信用卡個人化作業（並未透過 OTA 方式完成者)。持卡人可於取得安全儲存媒介後依現行電話或網路方式完成卡片啟用。
2. 透過 OTA 空中傳輸進行信用卡個人化資料下載時同時完成卡片啟用：
   (1) 須依安全設計通則之來源辨識性進行身分驗證完成後，下載個人化資料並完成卡片啟用。
   (2) 密碼/驗證碼之傳輸須依安全設計通則之訊息隱密性原則進行加密。
   (3) 透過 OTA 空中傳輸進行信用卡個人化資料下載完成後，由持卡人依現行電話或網路方式完成卡片啟用。

（三）手機信用卡發卡機構得提供手機信用卡持卡人使用手機進行交易模式設定如下：

1. 自動模式：手機信用卡於正常運作時，持卡人可隨時進行行動交易。
2. 手動模式：行動交易手機開機的狀況下，當手機信用卡接近感應讀卡機（Contactless Reader)，於手機螢幕詢問使用者是否允許進行交易，若不允許則中止交易；持卡人亦可於準備進行交易前，主動操作手機以開啟信用卡功能。
3. 上述交易模式之切換須依安全設計通則之來源辨識性進行身分驗證。

（四）手機信用卡發卡機構得提供手機信用卡持卡人於使用手機讀取信用卡相關資料之方式如下：

1. 一般查詢：信用卡卡號應依簽單規定隱藏部分卡號，持卡人可隨時查詢。
2. 完整卡號查詢:顯示完整信用卡卡號等信用卡相關資料(不含卡片背面末三碼)，須依安全設計通則之來源辨識性原則進行身分驗證確保持卡人之正確性。

（五）手機信用卡交易超過主管機關規定免簽名金額上限時，須依安全設計通則三、來源辨識性進行身分驗證，俾達到密碼驗證不可否認性，始能完成交易，以增加其安全性。

三、空中傳輸

OTA 空中傳輸進行信用卡個人化時，應遵循事項如下：

（一） 下載個人化資料前，TSM 服務平台必須確認使用之安全儲存媒介，為持卡人指定使用之安全儲存媒介。

（二） 個人化資料在空中傳輸過程，皆須依安全設計通則之訊息隱密性原則進行加密。

（三） 前款加密之金鑰應依安全設計通則之金鑰管理原則建立安全防護。

（四） 進行下載個人化資料時，手機信用卡發卡機構應依安全設計通則之來源辨識性原則設計持卡人身分驗證機制。

四、TSM 服務平台

本服務平台需經信用卡組織認證及依其規範辦理，開發建置時，應考量金鑰管理、網路與系統、資料安全及實體環境安全等，並列入應具備基本項目如下：

（一） 金鑰管理（Key Management）：

應依安全設計通則之金鑰管理原則管理。

（二）網路與系統（Network and Systems）：

1. TSM 服務平台之網路系統設備必須符合下列安全需求：建置安全防護軟硬體，如防火牆(Firewall)、安控軟體、偵測軟體等，同時對所有網路節段(Segment)(包括但不限於連接到公眾網路、DMZ 區網路以及內部企業網路)必須要以防火牆區隔。
2. 對高機密或高敏感性資料，各機構間傳輸網路應採取實體或虛擬之封閉型網路，如專線或虛擬私有網路 VPN（Virtual Private Network）。
3. 卡片個人化格式的資料庫必須要與空中傳輸作業的伺服器以防火牆區隔。
4. 卡片發行的資料庫與硬體金鑰保護模組(HSM, Hardware Security Module)必須單獨置放在一個網路節段，並與公眾網路節段、企業內部網路節段隔開。
5. 開放環境必須建置病毒偵測軟體(Virus Detection Software)，定期對網路節點及伺服器進行掃毒。
6. 建立備援及故障預防措施，如預備主機、伺服器、通訊設備、線路、週邊設備等備援裝置，同時建立相關機器設備或機房的安控規範。
7. 建立電腦資源存取控制機制與安全防護策略，防範未經授權存取系統資源，並降低非法入侵之可能性，相關設計應加以考量下列原則：

(1). 依安全設計通則之訊息隱密性原則進行電腦系統密碼檔加密，並控制密碼錯誤次數，同時必須強制更換應用軟體及網路作業系統之預設密碼。

(2). 留存交易紀錄(Transaction Log)及稽核追蹤紀錄(Audit Trail)。

(3). 設計存取權控制(Access Control)機制，如使用密碼、晶片卡等。

(4). 系統應依其存放資料重要性與敏感性分級管理。

(5). 簽入(Login)時間控制。

（三）資料安全（Data Security)：

服務平台應建立完善之資料安全防護機制，於提供各項服務功能時，應確保個人資料保護措施，其安全要求如下：

1. 作業程序必須確保行動交易手機與個人化資料必須是一對一關係，同時晶片之單一安全區域（SD）僅能被單一組個人化資料寫入。
2. 資料交換之必要性：各項資料，尤其是高機密或高敏感性資料（包括但不限於持卡人個人資料、信用卡資料），應謹慎評估是否有交換之必要性。
3. 個人化資料的儲存必須以加密的方式保護，加密方式應進行風險評估，以決定採取何種等級的安全保護措施。
4. 個人化資料於網路上的傳輸，須依安全設計通則之訊息隱密性原則進行加密，同時採用強化的安全協定和防護措施，如 SSL、TLS 或是 IPSec 等。

（四）實體環境安全（Physical Security)：

服務平台應建置在完善且可靠的機房環境，其保護設施應具備之基本原則及項目如下：

1. 建置完善的預警機制及防護措施(門禁、入侵防護、火災防護)，並且必須能夠即時的回應及處理。
2. 應定義高安全區域(單一安全區域或是有層次的安全區域)，並設有完整的管制措施。
3. 所有提供個人化傳輸、資料管理、金鑰管理等相關的伺服器軟硬體都必須置放於高安全區域。

4. 建立全天候（365 天、24 小時）錄影設備，同時必須涵蓋機房出入口與伺服器所在位置，且錄影資料必須適當留存至少六個月。

第五章、手機信用卡發卡機構與手機信用卡持卡人間權利義務

手機信用卡發卡機構除應依信用卡會員申請書約定條款辦理外，並應提供手機信用卡相關操作與使用說明，並另制定完整合約述明與手機信用卡持卡人間權利義務關係。合約內容應包含事項如下：

一、特殊卡片型態、共用安全儲存媒介（SE）之卡片及交易特性、可能風險與相關限制（含手機信用卡發卡機構與行動通信業者終止合約後之權利義務）。

二、手機信用卡持卡人有卡片遺失、被竊或其他喪失佔有等情事，於通知手機信用卡發卡機構後，可能之自負額應與一般感應式信用卡相同。

三、與行動通信業者共用安全儲存媒介（SE）有資料交換需求，應依據電腦處理個人資料保護法及相關法令規定辦理，並於申請書等文件明確告知交換之資料是否包含個人資料。

第六章、其他

一、信用卡業務機構於開辦手機信用卡業務前，應取得主管機關與信用卡組織之核准，並進行相關系統測試檢核、內部作業控制並定期稽核。

二、本業務發卡機構與 TSM 合作進行信用卡晶片個人化作業及相關作業委外辦理時，應依主管機關頒訂之「金融機構作業委託他人處理內部作業制度及程序辦法」暨其相關規定辦理。

三、本業務發卡機構倘需與非金融機構進行合作或資料傳輸連結時，應簽訂相關契約，明訂其須符合本安控基準相關作業安全要求或應配合事項及違反時之處理作法。

四、本安控基準應報經主管機關核備後實施，修正時亦同。

附錄、手機信用卡交易之信用卡組織規範

一、EMVCo. 規範：

遵循 EMVCo Contactless Mobile Payment 中 Contactless Mobile Payment Architecture Overview 及 EMVCo Handset Requirements for Contactless Mobile Payment 有關手機非接觸式支付的建構規範及其相關細部準則，針對以晶片卡為主的各項交易事項（包含但不限於非接觸式行動支付之晶片、手機、通訊協定、支付架構、相關技術…等之必要條件)進行安全規範。

二、Visa 組織規範：

信用卡業務機構之手機信用卡委外廠商必須遵守 Visa Card Vendor Program 規範，此規範含括以下安全要求文件：

（一）Global Logical Security Validation Requirements for Card Personalization Vendors

此文件規範相關廠商於開發、建置、卡片組成、資料傳輸、作業處理等各階段必須符合的金鑰管理、網路與系統、資料安控等安全需求。

（二）Global Physical Security Validation Requirements for Card Vendors

此文件規範相關廠商於卡片生產、磁條錄碼、卡片個人化、晶片嵌入、晶片啟始化、晶片個人化、卡片儲存、卡片運送、卡片郵寄等作業前後必須符合的實體安全需求。

（三）Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors

此文件規範相關廠商提供有關 Visa 產品之資料準備、加密支援、包裝運送、倉庫儲存派送等服務所必須符合的實體安全需求。

（四）Global Security Validation Requirements for Over-the-Air Secure Element Personalization Vendors

此文件規範對行動通信設備提供有關個人化、處理支付帳戶資料等空中傳輸服務之廠商所必須符合的安全需求。

三、MasterCard 組織規範

（一）Security Guidelines for Mobile Payment Solutions 行動交易解決方案安全原則

此文件提供近端行動交易解決方案在開發、評估以及導入上的安全原則。除針對目前已實行之行動交易解決方案之外，亦對於未來更複雜之行動交易解決方案提供安全原則的參考方針。

（二）Security Requirements for Mobile Payment Personalization 行動交易個人化作業安全規範定義空中傳輸（OTA）下載及個人化服務提供者需遵守之邏輯和實體安全原則。

（三）Security Requirements for Mobile Payment Provisioning 行動交易下載及更新安全規範

針對執行行動交易資料準備、管理和提供之機構，定義其所需遵守之安全層級。此文件所定義之安全規範，僅保證萬事達卡 PayPass 應用程式與符合 CAST 驗證之安全儲存媒介（SE）間，安全的空中傳輸（OTA）下載及更新。

四、PCI DSS（Payment Card Industry Data Security Standards）資料安全作業標準

由信用卡組織（American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.）成立之 PCI 安全標準委員會（Payment Card Industry Security Standards Council）所制定，為儲存、處理或傳輸信用卡持卡人帳戶或交易資訊之信用卡業務相關機構必須遵守之安全規範。