# 電子支付機構資訊系統標準及安全控管作業基準辦法條文

第三條　本辦法用詞定義如下：

一、電子支付機構業務：指本條例第三條第一項各款業務。

二、電子支付平臺：指辦理電子支付機構業務相關之應用軟體、系統軟體及硬體設備。

三、電子支付作業環境：指電子支付平臺、網路、作業人員及與該電子支付平臺網路直接連結之應用軟體、系統軟體及硬體設備。

四、網路型態區分如下：

(一)專屬網路：指利用電子設備或通訊設備直接以連線方式（撥接（Dial-Up）、專線（Leased-Line）或虛擬私有網路（Virtual Private Network，VPN）等）進行訊息傳輸。

(二)網際網路（Internet）：指利用電子設備或通訊設備，透過網際網路服務業者進行訊息傳輸。

(三)行動網路：指利用電子設備或通訊設備，透

過電信服務業者進行訊息傳輸。

五、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。

六、常用密碼學演算法如下：

(一)對稱性加解密演算法：指資料加密標準(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)。

(二)非對稱性加解密演算法：指 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)。

(三)雜湊函數：指安全雜湊演算法（Secure Hash Algorithm；以下簡稱 SHA)。

七、系統維運人員：指電子支付平臺之作業人員，其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、使用者服務、業務推廣、帳務管理或會計管理等作業。

八、一次性密碼（One Time Password ；以下簡稱 OTP)：指運用動態密碼產生器、晶片金融卡或以其他方式運用 OTP 原理，產生限定一次使用之密碼。

九、行動裝置：指包含但不限於智慧型手機、平板電腦等具通信及連網功能之設備。

十、機敏資料：指包含但不限於密碼、個人資料、

身分認證資料、信用卡卡號、信用卡驗證碼或個人化資料等。

十一、近距離無線通訊(Near Field Communication；以下簡稱NFC)：指利用點對點功能，使行動裝置在近距離內與其他設備進行資料傳輸。

十二、實體通路支付服務(Online To Offline，O2O)：指電子支付機構就電子支付機構業務，利用行動裝置或其他可攜式設備於實體通路提供服務。

十三、約定連結存款帳戶付款：指電子支付機構辦理電子支付機構業務，依使用者與開戶金融機構間之約定，向開戶金融機構提出扣款指示，連結該使用者存款帳戶進行轉帳，由電子支付機構收取支付款項，並於該使用者電子支付帳戶記錄支付款項金額及移轉情形之服務，作業機制如下：

(一)直接連結機制：指電子支付機構直接向開戶金融機構提出扣款指示，連結使用者存款帳

戶進行轉帳之機制。

(二)間接連結機制：指電子支付機構經由專用存款帳戶銀行介接金融資訊服務事業或票據交換所，間接向開戶金融機構提出扣款指示，連結使用者存款帳戶進行轉帳之機制。

第四條　　電子支付機構於受理使用者註冊時，所採用之身分確認程序之安全設計如下：

一、確認行動電話號碼：應確認使用者可操作並接收訊息通知。

二、確認金融支付工具之持有人與電子支付帳戶使用者相符，方式如下：

(一)確認存款帳戶持有人：應向金融機構查詢或確認存款帳戶持有人身分證統一編號或商業統一編號。個人使用者無身分證統一編號者，應提供其他身分證明文件及其號碼等資料供金融機構確認。

(二)確認信用卡持有人：應向信用卡發卡機構查詢或確認持有人身分證統一編號。

三、確認證明文件影本：得採上傳或拍照方式取得

完整清晰可辨識之影像檔。

四、臨櫃確認身分：臨櫃受理使用者註冊，應了解使用者動機、查證電話與住址、辨識具照片之身分證明文件、留存影像、留存印鑑或簽名、約定收付款限額及注意周邊環境。

五、以電子簽章確認身分：應透過憑證進行簽章、驗證憑證有效性,並確認該憑證之身分與電子支付帳戶使用者相符。

第六條　電子支付機構對於不同交易類型，應依其不同交易限額，採用下列交易安全設計：

一、辦理代理收付實質交易款項(含實體通路支付服務交易)，於使用者以電子支付帳戶款項支付、以約定連結存款帳戶付款支付、提出提前付款請求或提出取消暫停支付請求時，及使用者以約定連結存款帳戶付款支付儲值款項時，應依其不同交易限額,採用下列交易安全設計：

(一)每筆交易金額未達等值新臺幣五千元，或每日交易金額未達等值新臺幣二萬元，或每月交易金額未達等值新臺幣五萬元者,應採用 A

類交易安全設計。

(二)每筆交易金額達等值新臺幣五千元且未達等值新臺幣五萬元，或每日交易金額達等值新臺幣二萬元且未達等值新臺幣十萬元，或每月交易金額達等值新臺幣五萬元且未達等值新臺幣二十萬元者，應採用 B 類交易安全設計。

(三)每筆交易金額達等值新臺幣五萬元以上，或每日交易金額達等值新臺幣十萬元以上，或每月交易金額達等值新臺幣二十萬元以上者，應採用C類交易安全設計。

二、於使用者進行電子支付帳戶間款項移轉之支付時，應依其不同交易限額，採用下列交易安全設計：

(一)每筆交易金額未達等值新臺幣五萬元，或每日交易金額未達等值新臺幣十萬元，或每月交易金額未達等值新臺幣二十萬元者，應採用C類交易安全設計。

(二) 每筆交易金額達等值新臺幣五萬元，或每日

交易金額達等值新臺幣十萬元以上，或每月交易金額達等值新臺幣二十萬元以上者，應採用D類交易安全設計。

前項D類交易安全設計得替代C類交易安全設計，C類交易安全設計得替代B類交易安全設計，B類交易安全設計得替代A類交易安全設計。