「電子票證應用安全強度準則」第四條、第五條及第七條條文勘誤表

更正後文字	原列文字
第四條 本準則用詞定義如下： 一、加值機構：係指接受發行機構委託辦理加值作業之特定機構。 二、線上即時交易：係指持卡人利用電子設備或通訊設備，透過各種網路型態，經由特約機構、加值機構或直接與發行機構即時連線進行交易者，包含特約機構與發行機構間、加值機構與發行機構間、加值機構或特約機構與其所屬之端末設備間之即時訊息傳輸。 三、前款所稱網路型態如下： (一)專屬網路：指利用電子設備或通訊設備以撥接(Dial-Up)、專線(Leased-Line)或虛擬私有網路(Virtual Private Network，VPN)等連線方式進行訊息傳輸。 (二)網際網路：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。 四、非線上即時交易：係指持卡人持電子票證，利用各種介面類型，於端末設備進行交易，而不與發行機構即時進行連線者。 五、前款所稱介面類型如下： (一)接觸式介面：利用磁性、光學或電子型式之電子票證，與端末設備以實際接觸方式進行訊	第四條 本準則用詞定義如下： 一、加值機構：係指接受發行機構委託辦理加值作業之特定機構。 二、線上即時交易：係指持卡人利用電子設備或通訊設備，透過各種網路型態，經由特約機構、加值機構或直接與發行機構即時連線進行交易者，包含特約機構與發行機構間、加值機構與發行機構間、加值機構或特約機構與其所屬之端末設備間之即時訊息傳輸。 三、前款所稱網路型態如下： (一)專屬網路：指利用電子設備或通訊設備以撥接(Dial-Up)、專線(Leased-Line)或虛擬私有網路(Virtual Private Network，VPN)等連線方式進行訊息傳輸。 (二)網際網路：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。 四、非線上即時交易：係指持卡人持電子票證，利用各種介面類型，於端末設備進行交易，而不與發行機構即時進行連線者。 五、前款所稱介面類型如下： (一)接觸式介面：利用磁性、光學或電子型式之電子票證，與端末設備以實際接觸方式進行訊

息傳輸。	息傳輸。
(二)非接觸式介面：利用無線射頻、紅外線或其他無線通訊技術實作之電子票證，與端末設備以非實際接觸方式進行訊息傳輸。	(二)接觸式介面：利用磁性、光學或電子型式之電子票證，與端末設備以實際接觸方式進行訊息傳輸。
(三)網路及其他離線方式：利用電子票證，透過網路、通訊設備及其他方式，與遠端之特約機構或加值機構進行訊息傳輸，而不與發行機構即時連線進行授權者。	(三)網路及其他離線方式：利用電子票證，透過網路、通訊設備及其他方式，與遠端之特約機構或加值機構進行訊息傳輸，而不與發行機構即時連線進行授權者。
六、交易類型：	六、交易類型：
(一)線上即時消費交易：係指消費交易發生時，其消費是否合法之驗證，必須透過連線，將相關資訊送回發行機構進行處理者。	(一)線上即時消費交易：係指消費交易發生時，其消費是否合法之驗證，必須透過連線，將相關資訊送回發行機構進行處理者。
(二)非線上即時消費交易：係指消費交易發生時，其消費是否合法之驗證，不需透過連線送回發行機構進行處理者。	(二)非線上即時消費交易：係指消費交易發生時，其消費是否合法之驗證，不需透過連線送回發行機構進行處理者。
(三)線上即時加值交易：係指加值交易發生時，其加值之授權，必須透過連線，將相關資訊送回發行機構進行處理者。	(三)線上即時加值交易：係指加值交易發生時，其加值之授權，必須透過連線，將相關資訊送回發行機構進行處理者。
(四)非線上即時加值交易：係指加值交易發生時，其加值之授權，不需透過連線將相關訊息送回發行機構進行處理者。	(四)非線上即時加值交易：係指加值交易發生時，其加值之授權，不需透過連線將相關訊息送回發行機構進行處理者。
(五)票證款項移轉交易：係指將具儲值功能之記名式電子票證款項移轉至同一持卡人電子支付帳戶，其移轉之授權，必須透過連線，將相關訊息送回發行機構進行處理者。	(五)票證款項移轉交易：係指將具儲值功能之記名式電子票證款項移轉至同一持卡人電子支付帳戶，其移轉之授權，必須透過連線，將相關訊息送回發行機構進行處理者。
(六)帳務清結算交易：包含特約機構或加值機構與其所屬端末	(六)帳務清結算交易：包含特約機構或加值機構與其所屬端末設備間之批次帳務訊息、特約

設備間之批次帳務訊息、特約機構或加值機構與發行機構間之批次帳務訊息、加值機構與發行機構間之非線上即時加值額度授權請求訊息等。 七、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)。 八、動態密碼：係運用動態密碼產生器或以其他方式運用一次性密碼(One Time Password；以下簡稱 OTP)原理，隨機產生限定一次使用之密碼者。	機構或加值機構與發行機構間之批次帳務訊息、加值機構與發行機構間之非線上即時加值額度授權請求訊息等。 七、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)。 八、動態密碼：係運用動態密碼產生器或以其他方式運用一次性密碼(One Time Password；以下簡稱 OTP)原理，隨機產生限定一次使用之密碼者。
第五條 發行機構對於電子票證各項交易類型，應依電子票證應用之範圍，考量商品或服務之性質與交易金額等因素，區分應用範圍等級，並依據本準則之規定辦理。 商品或服務之性質可區分為二類： 一、第一類：繳納政府部門規費、稅	第五條 發行機構對於電子票證各項交易類型，應依電子票證應用之範圍，考量商品或服務之性質與交易金額等因素，區分應用範圍等級，並依據本準則之規定辦理。 商品或服務之性質可區分為二類： 一、第一類：繳納政府部門規費、稅

捐、罰緩或其他費用及支付公用事業（依據民營公用事業監督條例第二條定義）服務費、電信服務、學雜費、醫藥費、公共運輸（依據發展大眾運輸條例第二條定義及纜車、計程車、公共自行車、公共汽機車）、停車等服務費用、依公益勸募條例辦理勸募活動之捐贈金、配合政府政策且具公共利益性質經主管機關核准者、支付特約機構受各級政府委託代徵收之規費、稅捐與罰緩、或受公用事業委託代收之服務費。 二、第二類：支付各項商品或服務之費用。 交易金額可區分為二種： 一、小額交易：電子票證僅支付於單筆消費金額新臺幣壹仟元以下之交易。 二、不限金額交易：電子票證非僅支付於小額交易。 前二項商品或服務之性質及交易金額可區分二個應用範圍等級： 一、第一級：為辦理支付小額交易或第一類之商品或服務交易。 二、第二級：為辦理第二類之商品或服務且支付不限金額交易。	捐、罰緩或其他費用及支付公用事業（依據民營公用事業監督條例第二條定義）服務費、電信服務、學雜費、醫藥費、公共運輸（依據發展大眾運輸條例第二條定義及纜車、計程車、公共自行車、公共汽機車）、停車等服務費用、依公益勸募條例辦理勸募活動之捐贈金、配合政府政策且具公共利益性質經主管機關核准者、支付特約機構受各級政府委託代徵收之規費、稅捐與罰緩、或受公用事業委託代收之服務費。 二、第二類：支付各項商品或服務之費。 交易金額可區分為二種： 一、小額交易：電子票證僅支付於單筆消費金額新臺幣壹仟元以下之交易。 二、不限金額交易：電子票證非僅支付於小額交易。 前二項商品或服務之性質及交易金額可區分二個應用範圍等級： 一、第一級：為辦理支付小額交易或第一類之商品或服務交易。 二、第二級：為辦理第二類之商品或服務且支付不限金額交易。
第七條 前條各項交易安全所稱訊息隱密性、訊息完整性、來源辨識性及不可重覆性之安全設計應符合下列要求： 一、訊息隱密性A：應採用下列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	第七條 前條各項交易安全所稱訊息隱密性、訊息完整性、來源辨識性及不可重覆性之安全設計應符合下列要求： 一、訊息隱密性A：應採用下列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

3DES 112bits、AES 128bits 或其他安全強度相同(含)以上之演算法及金鑰進行加密運算。	3DES 112bits、AES 128bits 或其他安全強度相同(含)以上之演算法及金鑰進行加密運算。
(二)非對稱性加解密系統應採用 RSA 1024bits、ECC 256bits 或其他安全強度相同(含)以上之演算法及金鑰進行加密運算。自一〇六年一月一日起，新發行並應用於本項之電子票證不應採用低於 RSA 1024bits 之金鑰長度進行加密運算。	(二)非對稱性加解密系統應採用 RSA 1024bits、ECC 256bits 或其他安全強度相同(含)以上之演算法及金鑰進行加密運算。自一〇六年一月一日起，新發行並應用於本項之電子票證不應採用低於 RSA 1024bits 之金鑰長度進行加密運算。
二、訊息完整性	二、訊息完整性
(一)B1 防護措施：應採用下列防止非惡意篡改訊息之檢核碼技術之一：	(一)B1 防護措施：應採用下列防止非惡意篡改訊息之檢核碼技術之一：
1、縱向冗餘校驗(Longitudinal Redundancy Check，LRC)。	1、縱向冗餘校驗(Longitudinal Redundancy Check，LRC)。
2、循環冗餘校驗(Cyclic Redundancy Check，CRC)。	2、循環冗餘校驗(Cyclic Redundancy Check，CRC)。
3、使用雜湊(Hash)演算法產生訊息摘要(Message Digest)。	3、使用雜湊(Hash)演算法產生訊息摘要(Message Digest)。
(二)B2 防護措施：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。	(二)B2 防護措施：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。
1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。	1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。
2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。	2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。
(三)B3 防護措施：除須符合本條第二款第二目 B2 所要求之強度外，加值交易訊息之金額須參與訊息完整性之運算。	(三)B3 防護措施：除須符合本條第二款第二目 B2 所要求之強度外，加值交易訊息之金額須參與訊息完整性之運算。

三、來源辨識性 (一)C1 防護措施：應確保持卡人之正確性，可採用下列任一種持卡人認證方式；採用下列第 1 至第 3 方式者，其認證方式並應採用對稱性加解密系統或非對稱性加解密系統，由發行機構確認電子票證之合法性，以防範非法之電子票證。 1、具加解密運算能力之晶片卡。 2、記憶型晶片卡與固定密碼。 3、磁條卡與磁條卡密碼。 4、用戶代號與動態密碼。 5、用戶代號與固定密碼。 (二)C2 防護措施：應採用具訊息認證功能之晶片型電子票證或端末安全模組，確保訊息來源之正確性，可採對稱性加解密系統進行押碼或非對稱性加解密系統產生數位簽章等機制。 1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。 2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。 (三)C3 防護措施：應採用知識詢問(如卡號、有效月年及檢查碼)或設備綁定並搭配下列配套措施，由發行機構確認電子票證之合法性，以防範非法之電子票證。 1、應建置防偽冒偵測系統，建立風險分析模組與指標，用以於異常交易行為發生時即時告警並妥善處理。該風險分析模組與指標應定期檢討修訂。	三、來源辨識性 (一)C1 防護措施：應確保持卡人之正確性，可採用下列任一種持卡人認證方式；採用下列第 1 至第 3 方式者，其認證方式並應採用對稱性加解密系統或非對稱性加解密系統，由發行機構確認電子票證之合法性，以防範非法之電子票證。 1、具加解密運算能力之晶片卡。 2、記憶型晶片卡與固定密碼。 3、磁條卡與磁條卡密碼。 4、用戶代號與動態密碼。 用戶代號與固定密碼。 (二)C2 防護措施：應採用具訊息認證功能之晶片型電子票證或端末安全模組，確保訊息來源之正確性，可採對稱性加解密系統進行押碼或非對稱性加解密系統產生數位簽章等機制。 1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。 2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。 (三)C3 防護措施：應採用知識詢問(如卡號、有效月年及檢查碼)或設備綁定並搭配下列配套措施，由發行機構確認電子票證之合法性，以防範非法之電子票證。 1、應建置防偽冒偵測系統，建立風險分析模組與指標，用以於異常交易行為發生時即時告警並妥善處理。該風險分析模組與指標應定期檢討修訂。

2、非用戶本人授權使用之交易於掛失後無需承擔遭冒用之損失，發行機構應於十四日內返還帳款，持卡人應配合協助發行機構之後續調查作業。	2、非用戶本人授權使用之交易於掛失後無需承擔遭冒用之損失，發行機構應於十四日內返還帳款，持卡人應配合協助發行機構之後續調查作業。
(四)D1 防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由端末設備確認電子票證之合法性，以防範非法之電子票證。	(四)D1 防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由端末設備確認電子票證之合法性，以防範非法之電子票證。
(五)D2 防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由端末設備確認電子票證之合法性，以防範非法之電子票證。	(五)D2 防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由端末設備確認電子票證之合法性，以防範非法之電子票證。
1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。	1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。
2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。	2、非對稱性加解密系統應採用本條第一款第二目之非對稱性加解密系統演算法。
(六)E1 防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由電子票證確認端末設備或發行機構之合法性，以防止未經授權之端末設備逕行交易。	(六)E1 防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由電子票證確認端末設備或發行機構之合法性，以防止未經授權之端末設備逕行交易。
(七)E2 防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由電子票證確認端末設備或發行機構之合法性，以防止未經授權之端末設備逕行交易。	(七)E2 防護措施：應採用對稱性加解密系統或非對稱性加解密系統，由電子票證確認端末設備或發行機構之合法性，以防止未經授權之端末設備逕行交易。
1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。	1、對稱性加解密系統應採用本條第一款第一目之對稱性加解密系統演算法。
2、非對稱性加解密系統應採用	2、非對稱性加解密系統應採用

本條第一款第二目之非對稱性加解密系統演算法。 四、不可重覆性 F：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。	本條第一款第二目之非對稱性加解密系統演算法。 四、不可重覆性 F：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。