電子票證應用安全強度準則

條文	說明
第一條　本準則依電子票證發行管理條例第四條第二項訂定之。	明定法源依據。
第二條　發行機構應依本準則規定之安全需求與設計，建立安全防護措施，以確保電子票證應用之安全強度，保護消費者之權益。	明定本準則之立法宗旨及訂定目的。
第三條　前條所稱之安全需求與設計說明如下： 一、發行機構於交易面應依據應用範圍等級，落實本準則對於交易訊息之隱密性、完整性、來源辨識性及不可重覆性之各項規定。 二、發行機構於管理面應防範發行機構、特約機構及加值機構之交易系統，遭受未經授權之存取、入侵威脅及破壞，有效維護交易系統之整體性及其隱密性，並保護交易系統作業安全及維持其高度可使用性。 三、發行機構於端末設備與環境面應實施安全控管，強化端末設備之安全防護，以防範非法交易或遭受外力破壞。 四、發行機構於電子票證面應依據應用範圍等級，選用適當型式之電子票證。	明定本準則所規定安全需求與設計之範圍。
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：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	明定本準則相關用詞之定義。

Network，VPN)等)進行訊息傳輸。 （二）網際網路：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：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，於加值機構或特約機構之端末設備進行交易，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，與特約機構或加值機構之端末設備以實際接觸方式進行訊息傳輸。 （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，與特約機構或加值機構之端末設備以非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。 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。 （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。 （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。	

<table>
<tr>
<td>（五）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。</td>
<td></td>
</tr>
<tr>
<td>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（如下表），並依據本準則之規定辦理。
一、商品或服務之性質
<table>
<tr><th>商品或服務之性質</th><th>說明</th></tr>
<tr><td>第一類</td><td>繳納政府部門規費及支付公用事業(依據民營公用事業監督條例第二條定義）服務費、學雜費、醫藥費、公共運輸（依據大眾運輸條例第二條定義及纜車、計程車、公共自行車）、停車等服務費用，或配合政府政策且具公共利益性質經主管機關核准者屬之。</td></tr>
<tr><td>第二類</td><td>支付各項商品或服務之費用</td></tr>
</table>
二、交易金額
<table>
<tr><th>交易金額</th><th>說明</th></tr>
<tr><td>小額交易</td><td>電子票證僅支付於單筆消費金額新台幣壹仟元以下之交易。</td></tr>
<tr><td>不限金額交易</td><td>電子票證非僅支付於小額交易。</td></tr>
</table>
三、應用範圍等級
<table>
<tr><th colspan="2">商品或服務之性質</th><th>第一類</th><th>第二類</th></tr>
<tr><td rowspan="2">交易金額</td><td>小額交易</td><td>第一級</td><td>第一級</td></tr>
<tr><td>不限金額交易</td><td>第一級</td><td>第二級</td></tr>
</table>
</td>
<td>一、明定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。
二、對於電子票證之應用範圍非僅限於繳納政府部門規費及支付公用事業服務費、學雜費、醫藥費、公共運輸、停車等服務費用且單筆消費金額超過 1,000 元之交易，其性質已類屬貨幣，為保障消費者權益及健全電子票證之經營，則應採取較嚴格之防護措施。</td>
</tr>
</table>

第六條　發行機構於交易面應確保電子票證交易符合下列安全規定：

一、線上即時消費交易

連線類型		專屬網路		網際/行動網路	
應用範圍等級 / 防護措施		第一級	第二級	第一級	第二級
訊息隱密性		非必要	非必要	A	A
訊息完整性		B1	B1	B2	B2
來源辨識性	訊息認證或持卡人認證	C1	C2	C1	C2
不可重覆性		F	F	F	F

二、非線上即時消費交易

介面類型		接觸式/非接觸式		網路及其他離線方式	
應用範圍等級 / 防護措施		第一級	第二級	第一級	第二級
訊息隱密性		非必要	非必要	A	A
訊息完整性		B1	B2	B2	B2
來源辨識性	電子票證認證	D1	D2	D2	D2
	端末認證	E1	E2	E2	E2
不可重覆性		F	F	F	F

三、線上即時加值交易

連線類型		專屬網路		網際/行動網路	
應用範圍等級 / 防護措施		第一級	第二級	第一級	第二級
訊息隱密性		非必要	非必要	A	A
訊息完整性		B1	B1	B2	B2
來源辨識性	發卡端認證*	E1	E2	E2	E2
不可重覆性		F	F	F	F

(*:僅適用於具認證與儲值功能之電子票證)

一、為確保電子票證交易之合法性以維護交易安全，於交易面應考量交易之訊息隱密性(Confidentiality)、訊息完整性(Integrity)、來源辨識性或認證(Authentication)與不可重複性(Non-Repeatable)等四項要素，並明定其安全需求。

二、線上即時消費交易因透過不同型態之網路進行，因此對於上述四項要素之安全需求著重於不同網連線類型而應具有不同之安全需求，爰於第一款明定。

三、非線上即時之消費交易，無法與發行機構之主機端即時連線確保交易之合法性與完整性，爰電子票證與端末設備應進行雙向認證。因此介面類型為考量風險之主要因素，爰於第二款將介面類型區分為接觸式、非接觸式及網路及其他離線方式。

四、加值交易方面亦可依前述消費交易之考量，將即時加值交易區分其不同網路型態之規定，並將非線上即時加值交易區分其介面類型。此外，若：(1)電子票證之類型屬於具認證與儲值功能，則在防護措施方面須進行發卡端（線上即時）或端末設備（非線上即時）之認證，以確保加值額度儲存於電子票證時之訊息來源之合法性與完整性；(2)若加值之額度係儲存於發行機構伺服器端，則無涉發卡端認證議題，爰於第三款及第四款明定。

五、帳務清算及結算交易應考量連線類型之不同而具有不同之安全需求，爰於第五款明訂。

六、第六款明定交易訊息中若包含個人資料者之保護機制。

四、非線上即時加值交易

介面類型		接觸式/非接觸式		網路及其他離線方式	
應用範圍等級 / 防護措施		第一級	第二級	第一級	第二級
訊息隱密性		非必要	非必要	A	A
訊息完整性		B1	B3	B3	B3
來源辨識性	端末認證	E1	E2	E2	E2
不可重覆性		F	F	F	F

五、帳務清算及結算交易

連線類型		專屬網路		網際/行動網路	
應用範圍等級 / 防護措施		第一級	第二級	第一級	第二級
訊息隱密性		非必要	非必要	A	A
訊息完整性		B1	B1	B2	B2
來源辨識性	訊息認證	非必要	非必要	C2	C2
不可重覆性		F	F	F	F

六、第一款至第五款之交易訊息中若包含電腦處理個人資料保護法所定義之個人資料，為確保其隱密性，應採對稱性加解密系統或非對稱性加解密系統進行個人資料之加密，以防止未經授權者取得個人資料，其安全強度應不得低於第七條對訊息隱密性之規定(A)。

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：

防護措施		安全設計之基本原則
訊息隱密性	A	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： （一） 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)。 （二） 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： （一） RSA 加密標準（Rivest、Shamir、Adleman Encryption Standard；以下簡稱 RSA 演算法），金鑰長度 1024 或 2048 位元。 （二） 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) 。
訊息完整性	B1	應採用下列防止非惡意篡改訊息之檢核碼技術之一： 一、 縱向冗餘校驗 (Longitudinal Redundancy Check，LRC) 二、 循環冗餘校驗 (Cyclic Redundancy Check，CRC) 三、 使用雜湊(Hash)演算法產生訊息摘要(Message Digest)

一、訊息隱密性、訊息完整性、來源辨識性等安全性之確保，其強度取決於所使用之加解密演算法，而演算法之強度會隨著資訊設備之處理能力與速度演進而逐漸減弱，因此必須隨著時間之演進，予以評估並視需要更新電子票證與其基礎設施以支援合乎當時水準之演算法，維持電子票證應用之安全強度，爰訂定適當之演算法標準。

二、本條對於密碼學演算法之選定，係考量業界實務，並參考美國國家標準和技術中心(NIST)所訂定個人識別確認之密碼學標準（NIST Special Publication 800-78-1,Cryptographic Algorithms and Key Sizes for Personal Identity Verification，該標準係為美國聯邦政府所制定，提供聯邦政府機構據以遵循）。

三、本條所稱之訊息隱密性係指訊息傳遞過程中針對交易資料之加密處理，若於本準則第六條所規定為必要者，一律以公開公開且經驗證為安全之加解密演算法進行加密處理。

四、本條所稱之訊息完整性係指確保資料傳遞過程中未經篡改，篡改之發生可能為非惡意如資料傳輸過程如線路品質不佳而產生資料錯誤者，常見之防範技術為冗餘校驗與雜湊等；亦可能為惡意者如駭客攻擊修改訊息內容者，此類之攻擊則必須以金鑰為基礎之密碼學運算加以防護。此外為確保非線上即時加值時資料之完整性，特別要求若為高風險交易者，應將加值金額一併加入參與密碼學運算，以防止針對加值金額之惡意篡改並確保加值之授權確以逐筆之方式進行。

五、本條所稱之來源辨識性，包含訊息認證或使用者認證、電子票證之認證、端末與發卡端之認證等：

（一）使用者認證係指發行機構於線上即時消費交易，須確認使者用之合法性以遂行交易，其型式可能為 C1 中所述，若使用者使用實體

		B2	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： （一） TDEA 演算法，金鑰有效長度為 112 位元(2TDEA)或 168 位元(3TDEA)。 （二） 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： （一）RSA 演算法，金鑰長度 1024 或 2048 位元。 （二）ECDSA 演算法，質數模數為 256 位元(P-256) 。	之電子票證、內建公開安全之加解密演算法、且於進行認證時將交易訊息參與加解密運算而產生認證訊息，則稱為訊息認證，因此訊息認證除可確保使用者身份之合法性，亦可確保交易訊息未遭篡改（訊息完整性）。此外特約機構、加值機構與發行機構間之帳務清結算交易，訊息接收方確保發送方之身份，在本準則中亦屬訊息認證之範圍。 （二）電子票證認證係指非線上即時消費交易中，端末設備確保使幅者所使用實體電子票證之合法性。 （三）端末認證係指非線上即時消費與加值交易中，實體電子票證確保端末設備合法性。 （四）發卡端認證係指線上即時加值交易中，若使用者使用具認證與儲值功能之實體電子票證，來接收發卡端傳送之加值訊息，使用者須確保發卡端之合法性。 六、為確保交易之不可重複性，常用之方式為每筆交易中加入序號、日期時間或時序或密碼學挑戰-回應至交易訊息中，以確保其唯一性與可追蹤性。
		B3	除須符合 B2 之所要求之強度外，加值交易訊息之金額須參與訊息完整性之運算	
來源辨識性	訊息認證或持卡人認證	C1	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： 一、 用戶代號與固定密碼。 二、 磁條卡與磁條卡密碼。 三、 用戶代號與動態密碼:動態密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（One Time Password；以下簡稱 OTP）原理，隨機產生限定一次使用之密碼者。 四、 以密碼學運算為基礎,提供認證功能之晶片型電子票證。	
		C2	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。 一、 對稱性加解密系統應採用下列演算法之一： （一） TDEA 演算法，金鑰有效長度為 112 位元(2TDEA)或 168 位元(3TDEA)。 （二） 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： （一） RSA 演算法，金鑰長度 1024 或 2048 位元。 （二） ECDSA 演算法，質數模數為 256 位元(P-256) 。	
		D1	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。	

	電子票證認證	D2	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。 一、 對稱性加解密系統應採用下列演算法之一： （一） TDEA 演算法，金鑰有效長度為 112 位元(2TDEA)或 168 位元(3TDEA)。 （二） 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： （一） RSA 演算法，金鑰長度 1024 或 2048 位元。 （二） ECDSA 演算法，質數模數為 256 位元(P-256) 。	
	端末/發卡端認證	E1	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。	
		E2	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。 一、 對稱性加解密系統應採用下列演算法之一： （一） NIST 之 TDEA 演算法，金鑰有效長度為 112 位元(2TDEA)或 168 位元(3TDEA)。 （二） NIST 之 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： （一） RSA 演算法，金鑰長度 1024 或 2048 位元。 （二） ECDSA 演算法，質數模數為 256 位元(P-256) 。	
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。	
第八條　發行機構於管理面應採取下列防護措施：				為避免發行機構、特約機構與加值機構之交易系統遭受未經授權之存取、入侵威脅及破壞，及系統上線前應具備相關測試檢核措施，爰明定發行機構於管理面應採取之防護措施。

<table><tr><th>防護措施</th><th>安全需求</th></tr><tr><td>建立安全防護策略</td><td>一、建立電腦資源存取控制機制與安全防護措施。 二、交易必須可被追蹤。 三、監控非法交易。 四、須防止小規模之特約機構不當扣款。 五、完善之金鑰管理。</td></tr><tr><td>提高系統安全之措施</td><td>提昇電腦系統之安全及可用性</td></tr><tr><td>制定作業管理規範</td><td>制定作業管理規範</td></tr></table>	
第九條　前條發行機構管理面安全需求之安全設計應符合下列要求： <table><tr><th>安全需求</th><th>安全設計</th></tr><tr><td>建立電腦資源存取控制機制與安全防護措施</td><td>應防範未經授權存取系統資源，並降低非法入侵之可能性。應以下列方式處理及管控： 一、建置安全防護軟硬體，如防火牆(Firewall)、安控軟體、偵測軟體等。 二、控制密碼錯誤次數。 三、電腦系統密碼檔加密。 四、留存交易紀錄(Transaction Log)及稽核追蹤紀錄(Audit Trail)。 五、設計存取權控制(Access Control)如使用密碼、晶片卡等。 六、簽入(Login)時間控制。 七、遠端存取應使用虛擬私有網路(VPN)。 八、系統資源應依其重要性與敏感性分級管理。 九、強制更換應用軟體及網路作業系統之預設密碼。 十、系統提供各項服務功能時，應確保個人資料保護措施。</td></tr><tr><td>交易必須可被追蹤</td><td>交易紀錄明細應包含下列資訊，並留存於發行機構主機備查：</td></tr></table>	為達成前條之防護措施，明定發行機構具體之安全設計要求。

	一、用戶代號或卡號。 二、交易金額。 三、端末設備代號。 四、交易序號或交易日期、時間。		
監控非法交易	發行機構應監控非法交易		
須防止小規模之特約機構不當扣款	實收資本額低於八千萬元且年營業額低於六千萬元之特約機構應以下列任一方式進行持卡人交易確認，但提供第一類商品或服務者，不在此限： 一、刷卡或插卡。 二、輸入密碼。 三、任何由系統所提供予持卡人進行確認之設計。		
完善之金鑰管理	金鑰管理應有下列之安全考量： 一、應確保金鑰品質(避免產生弱金鑰)。 二、金鑰之使用、儲存、傳送與銷毀，應確保金鑰之內容無洩露之虞。 三、金鑰應備份以確保其可用性。 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。		
提昇電腦系統之安全及可用性	應建立異地備援及故障預防措施，包含： 一、預備主機、伺服器、通訊設備、線路、週邊設備等備援裝置。 二、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。 三、定期更新系統修補程式（Patch, Hotfix）。 四、確保伺服器、網路設備之實體安全。		
制定作業管理規範	應確定發行機構、特約機構與加值機構內部之責任制度、核		

<table>
<tr><td></td><td>可程序及與持卡人之間之責任歸屬，應包含：
一、制定安全控管規章含設備規格。
二、安控機制說明、安控程序說明。
三、金鑰管理措施或辦法。
四、制定持卡人使用安全須知及完整合約。</td><td></td></tr>
<tr><td colspan="2">第十條　發行機構於端末設備與環境面應採取下列防護措施：
<table><tr><th>防護措施</th><th>安全需求</th></tr><tr><td>建立安全防護策略</td><td>一、保持端末設備與環境之實體完整性。
二、確保端末設備交易之安全性。
三、建置有效或即時之管控名單管理機制。
四、非接觸式電子票證應降低交易被意外觸發之機率。
五、非線上即時加值應具有端末安全模組之設計。
六、非線上即時交易，若採用應用範圍等級第一級之電子票證，且使用於提供第二類商品或服務之特約機構，應設置監視設備。
七、網際網路應用系統開發注意事項。</td></tr><tr><td>提高系統可用性之措施</td><td>提高系統可用性之措施</td></tr><tr><td>制定作業管理規範</td><td>制定作業管理規範：內部環境管理部分應落實管理規則之規範。</td></tr></table></td><td>為確保發行機構、特約機構與加值機構實施環境及端末設備面之安全控管，明定發行機構於端末設備與環境面應採取之防護措施。</td></tr>
<tr><td colspan="2">第十一條　前條發行機構端末設備與環境面安全需求之安全設計應符合下列要求：
<table><tr><th>安全需求</th><th>安全設計</th></tr><tr><td>保持端末設備與環境之實體完整性</td><td>應採用下列各項安全設計：
一、定期檢視是否有</td></tr></table></td><td>為達成前條之防護措施，明定發行機構端末設備與環境面安全需求之安全設計。</td></tr>
</table>

	增減相關裝置 （一）原始設施確實逐項編號。 （二）比對現場相關設施及裝置是否與原始狀態一致。 （三）建立檢視清單(Checklist)，並應定期覆核並追蹤考核。 二、應確定與端末設備合作廠商簽訂資料保密契約，並應將參與端末設備安裝、維護作業之人員名單交付造冊列管，如有異動，應隨時主動通知發行機構更新之。 三、端末設備合作廠商人員至現場作業時，均應出示經認可之識別證件。除安裝、維護作業外，並應配合隨時檢視端末設備硬體是否遭到不當外力入侵或遭裝置側錄設備。 四、發行機構應不定時派員抽檢安裝於特約機構或加值機構之端末設備，檢視該硬體是否遭到不當外力入侵，並檢視其軟體是否遭到不法竄改。		

確保端末設備交易之安全性	運用端末設備處理交易時，應符合下述規範： 一、電子票證內含錄碼及資料，除帳號、卡號、有效期限、交易序號及查證交易是否發生之相關必要資料外，其他資料一律不得儲存於端末設備。 二、應確保端末設備之合法性，另端末設備應有唯一之端末設備代號。 三、應用範圍屬第二級之交易，端末設備之安全模組應個別化(即每一端末設備之認證金鑰皆不相同)。		
建置有效或即時之管控名單管理機制	為有效防範非法電子票證進行交易，發行機構應建置管控名單管理機制，對於線上即時交易應即時更新，非線上即時交易應每日更新。		
非接觸式電子票證應降低交易被意外觸發之機率	端末設備應包含下列設計，以降低非接觸式電子票證在持卡人無交易之意願下，交易被意外觸發之機率： 一、感應距離限縮至六公分（含）以下。 二、交易過程應有聲音、燈號或圖像等之提示。		
非線上即時加值應具有端末安全模組之設計	非線上即時加值交易之端末設備應具有安全模組之設計，進行加值交易另應包含下列		

	設計： 一、逐筆授權加值交易。 二、限制其單筆加值金額。 三、限制其加值總額（如：日限額），額度用罄應連線至發行機構重新授權可加值額度。 四、安全模組應進行妥善之管理，如製發卡與交貨控管流程、管制製卡作業、落實安全模組之安全控管等。		
非線上即時交易，若採用應用範圍等級第一級之電子票證，且使用於提供第二類商品或服務之特約機構，應設置監視設備，或採取其他必要之措施以降低偽卡交易	應用範圍等級第一級之電子票證，若使用於提供第二類商品或服務之特約機構進行非線上即時交易，發行機構應要求特約機構設置錄影監視設備且於營業時間內保持全時錄影，或採取其他必要之措施以降低偽卡交易。		
網際網路應用系統開發注意事項	若電子票證持卡人透過瀏覽器以網際網路進行交易，網路應用系統之開發應有下列設計： 一、網站應採用網頁安全傳輸協定（Secure Sockets Layer；簡稱SSL）加密或其他安全強度不得低於第七條對訊息隱密性之規定(A)之方式加密傳輸資料。 二、系統應依每筆交易動態隨機變動端末設備查核碼		

	或以亂碼化保護。 三、系統應設計具遮罩功能之圖形驗證碼(Graphic One Time Password ；簡稱 GOTP) 或隨機按鈕等方式。 四、系統應設計動態頁面呈現或限制滑鼠點選，以防止模擬鍵盤控制（ SendKey Control）攻擊。 五、系統應有連線(Session)控制及網頁逾時(Timeout)中斷機制。 六、若有多網頁設計，系統應驗證前一網頁正確性。 七、客戶端元件應驗證網站正確性。 八、客戶端元件應具有防盜用機制，以驗證正確網站。 九、客戶端元件應具有作業系統認可之程式碼簽章憑證(CodeSign)。 十、客戶端元件應具存取卡片時限定為獨占模式之設計。 十一、客戶端元件應具有需經人工介入以完成交易之設計。 十二、如有駭客入侵時，發行機構應即關閉網路服務，以確保交易安全。		
提高系統可用性之措施	應以下列方式處理及管控：		

	一、規劃備援線路。 二、規劃備援電路或不斷電系統（Uninterruptible Power Supply；簡稱UPS）。	
制定作業管理規範	應制定端末設備管理規章，含設備規格、安控機制說明、安控程序說明、安全模組控管作業原則、管控名單管理機制、特約機構與加值機構簽約與管理辦法等。	

第十二條　發行機構應依據應用範圍等級選用下列適當型式之電子票證：

應用範圍等級	適用電子票證類型
第一級	電子票證應為下列類型之一，第三點至第五點僅限於線上即時交易： 一、具加解密運算能力之晶片卡。 二、記憶型晶片卡與固定密碼。 三、用戶代號與動態密碼。 四、磁條卡與固定密碼。 五、用戶代號與固定密碼。
第二級	電子票證應為下列類型之一： 一、符合第六條之安全規定，且經安全認證之晶片卡。 二、用戶代號與經安全認證之動態密碼產生器(如OTP Token) (限以線上即時方式進行交易)。

前項所稱「安全認證」係指經主管機關確認其安全等級通過行政院國家通訊傳播委員會或共同準則相互承認協定（Common Criteria Recognition Arrangement；CCRA）認可之驗證機構進行第三方驗證，符合或等同於下列任一標準者：

一、共同準則（Common Criteria）ISO/IEC15408 v2.3 EAL4+ (含增項

一、考量電子票證應用之多元性，其型式可能有實體與虛擬，而實體之電子票證亦有是否經安全評估等差異，故為確保交易之安全及保障持卡人之權益，爰於第一項對於不同應用範圍等級明定適用之電子票證。

二、第二項明定「安全認證」之標準。

<table>
<tr><td>AVA_VLA.4 及 ADV_IMP.2)。
二、共同準則（Common Criteria）ISO/IEC15408 v3.1 EAL4+ (含增項 AVA_VAN.5)。
三、我國國家標準 CNS 15408 EAL4+(含增項 AVA_VLA.4 及 ADV_IMP.2)。
四、其他經主管機關認可之驗證標準。</td><td></td></tr>
<tr><td>第十三條　發行機構對電子票證應採取下列防護措施：
<table><tr><th>防護措施</th><th>安全需求</th></tr><tr><td>建立安全防護策略</td><td>一、確認電子票證之合法性。
二、採用戶代號與固定密碼者，應有一定之安全設計。
三、儲存於電子票證之個人資料必須保護。</td></tr><tr><td>制定作業管理規範</td><td>制定電子票證交貨控管流程</td></tr></table></td><td>明定發行機構對電子票證應採取之防護措施。</td></tr>
<tr><td>第十四條　前條發行機構電子票證安全需求之安全設計應符合下列要求：
<table><tr><th>安全需求</th><th>安全設計</th></tr><tr><td>確認電子票證之合法性</td><td>應以下列任一方式確保電子票證之合法性：
一、具有獨立且唯一之識別碼。
二、電子票證具有認證之功能。</td></tr><tr><td>若採用戶代號與固定密碼者，應有一定之安全設計</td><td>採用戶代號及固定密碼者，應有下列之安全設計：
一、用戶代號之安全設計：
（一）發行機構如使用客戶之顯性資料(如統一編號、身分證號及帳號)作為識別，應另行增設持卡人代號以資識別。
（二）不得少於六位。
（三）不得訂為相同</td></tr></table></td><td>為確保發卡機構可符合前條規定，爰於本條規範其所應採取之相關安全措施。</td></tr>
</table>

	之英文字或數字、連續英文字或連號數字。 （四）客戶於申請後若未於一個月（日曆日）內變更密碼，則不得再以該用戶代號執行簽入。 （五）客戶同一時間內只能登入一次密碼。 （六）如增設持卡人代號，至少應依下列方式辦理： 1、不得為客戶之顯性資料。 2、如輸入錯誤達五次，發行機構應做妥善處理。 3、新建立時不得與用戶代號相同；變更時，亦同。 二、密碼之安全設計： （一）不得少於六位。若搭配交易密碼使用則不得少於四位。 （二）建議採英文字或數字混合使用，且宜包含大小寫英文字母或符號。 （三）不得訂為相同之英文字或數字、連續英文字或連號數字。 （四）密碼與代號不		

	得相同。 （五）密碼連續錯誤達五次，不得再繼續執行交易。 （六）變更密碼不得與前一次相同。 （七）首次登入時，應強制變更預設密碼。		
儲存於電子票證之個資必須保護	若使用電子票證儲存個人資料，應設計存取控制或持卡人確認之機制，以限制其讀取。		
制定電子票證交貨控管流程	發行機構應針對電子票證之生命週期進行妥善之管理，包含： 一、制定電子票證製發卡與交貨控管流程。 二、管制外包製卡作業。 三、落實實體電子票證之安全控管。		
第十五條　發行機構應按季向主管機關申報異常交易金額，若年度累計總金額超過實收資本額之百分之一，應即向主管機關提報改善計畫。			為確保電子票證之交易安全，爰明定發行機構應按季向主管機關申報異常交易金額，另其年度累計總金額達一定比率時，應向主管機關提報改善計畫。
第十六條　發行機構應依第五條有關商品或服務之性質及交易金額等之分類，按季向主管機關或其指定機構申報統計資料。			明定發行機構應按季向主管機關或其指定機構申報第五條有關商品或服務之性質及交易金額等統計資料。
第十七條　發行機構應委託會計師查核依本準則規定辦理之情形，並於年度終了後二個月內，將查核情形報主管機關備查。			為確保發行機構所辦理電子票證業務之安全機制符合本準則之規定，爰明定發行機構應委託會計師查核，並將查核情形向主管機關申報。
第十八條　本準則公布施行後，現有已發行電子票證並經核准辦理電子票證業務之發行機構及已辦理電子票證業務之銀行，有不符第九條「須防止小規模之特約機構不當扣款」之規定者，應自本準則發布施行後六個月內調整之。			明定電子票證發行機構有不符本準則第九條「須防止小規模之特約機構不當扣款」之規定者，應自本準則發布施行後六個月內調整之。
第十九條　本準則自發布日施行。			規定本準則之施行日。