國立交通大學

管理學院碩士在職專班
科技法律組

碩 士 論 文

電子簽章法關於憑證機構管理規範之研究

研 究 生：宋浸琪

指導教授：羅明通　博士

劉尚志　博士

中 華 民 國 九 十 六 年 八 月

電子簽章法關於憑證機構管理規範之研究

A Study on Certificate Authority Management Regulations of Electronic Singature Act

研 究 生：宋浸琪
指導教授：羅明通
指導教授：劉尚志

Student：Wen-Chi Sung
Advisor：Dr. Ming-To Lo
Advisor：Dr. Shang-Jyh Liu

國 立 交 通 大 學

管理學院碩士在職專班

科技法律組

碩 士 論 文

A Thesis
Submitted to Institute of Technology Law
College of Mangement
National Chiao Tung University
In partial Fulfillment of the Requirements
for the degree of
Master
in

Technology Law

Auguest, 2007

Hsinchu, Taiwan, Rupublic of China

中華民國九十六年八月

電子簽章法關於憑證機構管理規範之研究

學生：宋浸琪　　指導教授：羅明通博士

指導教授：劉尚志博士

國立交通大學管理學院碩士在職專班科技法律組

摘　　要

網路安全爲電子商務及電子化政府時代最重要之課題，而公開金論基礎建設透過公開金鑰密碼技術，構成網路安全與信賴之基礎。亦即藉由憑證機構的驗證，於電子文件傳送時，提供「身分識別」、「隱密性」、「資料完整性」及「不可否認性」等四種安全保證。簡言之，憑證機構爲公開金鑰基礎建設之核心，而完備妥善之法制規範方能保障消費者利益並促進產業發展。

目前我國關於憑證機構之法制規範，係規定於「電子簽章法」及其子法（施行細則、憑證實務作業基準應載明事項準則及外國憑證機構許可辦法）作爲規範基礎，就憑證機構之管理規範係採「低度管理」原則，僅要求憑證機構於成立時，書面審查其所提出之憑證實務作業基準，如此並無法確保憑證機構之可信賴性及保障電子交易之安全。

觀諸國際間立法現況，就憑證機構管理規範之發展趨勢均改採「高度管理」原則，並建有相當規模的規範法制。相較之下，我國法規並未相應就憑證機構之營運管理透過法制進行較詳細規範。隨著憑證應用之持續發展及成長，如何因應憑證機

構實務需求並符合國際發展趨勢與國際接軌，有必要對現行憑證機構管理規範作全面之檢討。

本論文從實務面及技術面的角度出發，首先，先強調憑證機構需要完備法制規範之重要性，並了解我國及世界先進各國憑證應用及憑證機構之發展現況。其次，從整理比較我國與世界先進各國對憑證機構之實務運作及規範，檢討我國憑證機構之相關規範。最後，提出具體修法建議作爲本文之結論。

A Study on Certificate Authority Management

Regulations of Electronic Singature Act

Student：Wen-Chi Sung　　Advisors：Dr. Ming-To Lo

Dr. Shang-Jyh Liu

Institute of Technology Law
National Chiao Tung University

ABSTRACT

Internet security is becoming the most important issue of the E-Commerce and E-Government era. Internet security and reliance can be protected by Public Key Infrastructure (PKI), which employs the use of public key cryptography technologies.

In other words, 'Authentication', 'Confidentiality', 'Integrity', and 'Non-Repudiation' are four kinds of security measures that can be safeguarded by PKI verifying through Certificate Authority (CA) while transferring E-Documents.
In short, CA is an essential part of PKI and the legislation should be more mature and comprehensive so that it may integrate consumers' interests as well as develop Certification Service Providers.

The 'Electronic Signature Act' and its inherent regulations, is the sole legal instrument in executing CA in our country at present. (Including: Enforcement Rules of the Electronic Signatures Act, Standards of the Certification Practice Statement, and Regulations Governing Permission of Foreign Certification Service Providers).

The Act regulates CA through less intervention, which only requires document examination (Certification Practice Statement, CPS) before licensing. Accordingly, current procedures are insufficient to guarantee customer reliance on CA and Internet security.

On the other hand, the international CA management's trend is towards "more intervention" provided with complete legal institutions. By comparison, the R.O.C. lacks detailed regulations to manage CA's operation. This should be the critical issue to comply with international standards. Due to the rapid growth and progress of certificating utilization, it is time to examine the relevant CA legal system.

From a pragmatic and technological point of view, this thesis discusses the importance of Certificate Authority Management Regulations and goes on to introduce the current advanced situation of international certificate application and CA service providers in the R.O.C. and the other countries.

Furthermore, it re-evaluates the R.O.C regulations by comparing them with the practice in other developed countries.
The conclusion of the thesis, will submit an effective proposal as a viable alternative.

誌　　謝

西元 2002 年，是我自政大法律系畢業後的第 11 年，也是我進入交大科技法律研究所的第 1 年。猶記參加交大科法所筆試的當時，剛因腹膜炎手術出院，大病初癒體能尚未恢復，考場在 4 樓，爬樓梯時傷口還隱隱作痛。放榜當日，自家中上網得知免口試直接錄取，與外子興奮的像個小孩子在屋內跳進跳出，興奮的期待新的學生生活的開展。

從事企業法務工作 10 年，渴望想進修成長的心日益壯大，埋首於傳統產業工作的我，驀然驚覺自己錯過了台灣科技發展的黃金 10 年！幸運的我能直接進入交大科法所就讀，取得直接成為「科技法律人」的捷徑，怎能不懷著感恩的心雀躍不已呢。

所上多元又彈性的課程、熱情專業開明的師資、開放具國際視野的學習環境，加上絕對是一時之選、臥虎藏龍之同儕學習，使我的在職研究生生活精采而豐富。作家海明威說：「如果你有幸年輕時住在巴黎，它會一生跟著你，有如一場可帶走的盛宴。」台積電董事長張忠謀先生，也曾重新詮釋這段話：「在哈佛的那一年，絕對是我生命中可帶走之盛宴。」對我而言，成為交大科法所的一份子，將成為我一生中具有深遠影響之盛宴。

感謝羅明通老師在我最徬徨時願意收留我當我的指導教授，羅老師嚴謹專業的治學方法及態度，將使我一生學習受用無窮。感謝劉尚志老師的包容與鼓勵，讓在職又身為母親的我能一路堅持而有所依恃。同時也感謝李復甸老師的支持與配合，讓我能順利完成口試及時畢業。更要感謝當初幫我寫推薦函的蘇永欽、謝銘洋及吳嘉生老師，他們是促成這一切美好的功臣。

感謝資策會科法中心的資料提供。感謝同學彥汶、郁超、佩文及學長仕謙在我撰寫論文時給予的支援與協助。感謝我母親及兩位妹妹佩漙與佩玲的全力幫忙照顧孩子，讓我能專心於課業無後顧之憂。也要感謝我公婆的包容與體諒。最要感謝的是外子世欽，身兼司機、奶爸、打字員、跑腿小弟、張老師還有訓導主任等多重角色，讓我能有毅力、有紀律的修完學分、完成論文。

當然我也要感謝菩薩，在讓我進交大科法所的同時，還賜給我一個聰明可愛的寶貝兒子曜枎，他是我不斷堅持學習成長前進的動力，我的交大研究生生活，有了他的全程參與，更添色彩與樂趣。

最後，謹以本文獻給所有幫忙我成就碩士學位之人，謝謝大家。

宋浭琪 謹誌於台北自家　2007 年 8 月 26 日

目　　錄

頁次

表 目 錄

圖 目 錄

一、緒　論

1.1　研究動機

電子商務及電子化政府時代，在開放且虛擬的網路環境中，進行有別於傳統之非面對面的交易與訊息交換，如何所傳輸資料被竊取、竄改或避免身分被冒用，並使交易與訊息交換之當事人於事後均無法否認交易或訊息交換之存在，此爲網路交易安全中重要的課題。故爲保護網路交易安全而伴生對於身分識別 (Authentication)[1]、隱密性 (Confidentiality)[2]、資料完整性 (Integrity)[3]及不可否認性 (Non-Repudiation)[4]之需求，均端賴電子認證體系完善之運作。

目前全球各界公認最有效之保護線上交易安全的方式[5]當爲「公開金論基礎建設」(Public Key Infrastructure, PKI)[6]。所謂「公開金論基礎建設」，係指以公開金鑰(Public Key)[7] 密碼技術爲主體，所構成之網路安全與信賴基礎建設與架構，透過金鑰及公正第三人—憑證機構(Certificate Authority, CA) 的驗證，於電子文件傳送時，提供「身分識別」(Authentication)、「隱密性」(Confidentiality)、「資料完整性」(Integrity)及「不可否認性」(Non-repudiation)等四種安全保證。

公開金論基礎建設所提供之上述四種安全保證，前三種係透過科學技術[8]來提供保證，惟有第四種「不可否認性」(Non-repudiation)，即證明雙方確實進行

---

[1] 亦即資料來源辨識，文件接收者可確認此文件之發送者的身分，避免被冒名傳送假資料。

[2] 資料之隱密性得以維持，只有獲授權者可以存取。

[3] 資訊沒有遭到未獲授權而作出的更改或毀壞的情況，亦即資訊的現有狀態與傳輸前的原本狀態相同。

[4] 提供原本的證據，使發件人不能否認曾發出信息，而收件人也不能否認曾收取信息。

[5] 經濟部商業司編印，2004 台灣 PKI 年鑑，經濟部，台北，民國 93 年 10 月出版，頁 4。

[6] 運用公開金鑰及電子憑證以確保網路交易的安全性及確認交易對方身分之機制。公開金鑰基礎建設係以網路認證之信任機制爲基礎，交易雙方相互地信任其認證機構，搭配金鑰對之產製及數位簽章等功能，即可經由其認證機構核發之電子憑證(以電子形式發出的證書，其所儲存的數據可用以驗證憑證擁有人的身分)確認彼此的身分，並提供四項重要的安全保障。

[7] 非對稱式密碼演算法中用來加密或驗章可公開之金鑰。

[8] 「身分識別」：透過確認用戶端的身分－係運用公鑰/私鑰技術(Public/Private Key)；「隱密性」：保護敏感的資訊－係運用 SSL, S/MIME, IPSec 技術；「資料完整性」即確保資料在交易過程中未經　變更－則是使用雜湊函數(SHA1,MD5)原理。

過交易，即係透過電子簽章法之立法技術，透過舉證責任轉換來賦予法律上之效力。目前我國公開金論基礎建設(PKI)應用之法制規範，係以「電子簽章法」及其子法作爲規範基礎。

我國電子簽章法於民國 90 年 11 月 14 日總統府公告，民國 91 年 4 月 1 日正式施行，全文共 17 條，其主要規範重點除明定電子簽章、電子文件的法律地位及效力外，另一規範重點則在憑證機構[9]之管理規範。此乃由於憑證機構在公開金論基礎中扮演身分認證機制之重要角色，爲確保其公信力及中立之地位，當然需有適當及完備之法制規範使憑證機構業者得以遵循發展，並供主管機關管理以及保障消費者之權益。

詳言之，在電子簽章的應用當中，由於憑證機構扮演確認電子簽章使用者身分真實性的功能，其扮演重要及不可或缺的第三人角色。憑證機構在簽發憑證時，爲讓任何第三人可確認電子簽章使用者的身分真實性，因此必須依其交易上的需要，查驗不同內容的資料，如電子簽章使用者的身分證明、或未來可能基於商務的需求而須查核電子簽章使用者的信用或資產狀況等，以確認電子文件上所簽署表彰的電子簽章使用者確實存在。

依此，可以預見的是，當交易雙方對電子文件的真實性產生質疑時，如果電子文件上僅有簽署電子簽章時，僅能知悉電子文件之簽署者。但該簽署者究竟是否真實存在，在網路上無法透過其他方式得知其真正性。此時，如使用經憑證機構查驗電子簽章使用者資料真實性的電子簽章，而且附有「憑證」證明電子簽章使用者的身分真實性。則當交易雙方對電子文件的真實性發生爭議時，憑證機構即可確認該電子文件上所簽署的電子簽章是屬於何人所有，此時電子簽章使用者自無法否認其真實性，而達到證明的功能。

---

[9] 指提供數位簽章製作及電子認證服務之機構，亦即係指居於公證客觀地位，查驗憑證申請人身分資料之正確性，及其與待驗證公開金鑰及私密金鑰間之關聯性與合法性，並據以簽發公開金鑰憑證之單位。

然有疑問者，憑證機構是否會確實查驗電子簽章使用者的身分？何以憑證機構所簽發的憑證可被信賴？就此部分，憑證機構雖在其核發憑證的作業規範(此即所謂「憑證實務作業基準」)中聲明，憑證機構會確實查驗電子簽章使用者的身分真實性，並且會採取嚴格的內部稽核措施及資訊安全維護規範，以避免內部員工未盡查驗責任或監守自盜乃至防止外部駭客竄改或竊取個人資料等語。惟就消費者的立場來考量，仍會產生疑問的是，如何確認這個憑證機構是值得信賴的？

1.2 研究目的

鑑於前述，本論文之研究目的即在對我國現行法制中，檢討關於憑證機構之規範，其重點如下：

1. 對於憑證機構之管理是否完備

目前我國電子簽章法中，對於憑證機構的管理，主要是由憑證機構依憑證實務作業基準自律管理的方式。是以，就憑證機構安全性的認定而言，消費者在選擇憑證機構時，除透過憑證實務作業基準來認識憑證機構的作業程序與安全稽核內容外，實須多費心瞭解憑證機構的實際運作程序與內容，而憑證機構亦應須採取具體作爲讓消費者充分信賴其安全及獨立性。

至於憑證機構如遭受類似天災人禍等不可抗力事由，致無法提供憑證服務時，是否仍應遵循電子簽章法的規定，似有疑問。依主管機關所公布的「憑證實務作業基準應載明事項準則」[10]的說明，主管機關已要求憑證機構必須於憑證實務作業基準中載明檔案資料的儲存及控管方式，其中要求憑證機構載明面對天災人禍等不可抗力事由的檔案資料防護措施的具體內容，以確保檔案資料的完整性及維護憑證的永續性。然而，在實務運作上有無真正落實執行，如何監控？

[10] 依據我國《憑證實務作業基準應載明事項準則》第 27 條之規定：「憑證機構應於其作業基準中載明危害及災變復原程序之規劃。」

2. 對於消費者之保護是否妥適

其次，以消費者的角度來思考，網路使用者普遍針對網路交易及網路環境的安全性存有相當大的疑慮。因此，對於此種網路憑證的新興科技服務，消費者多少存在著懷疑與不信任的不確定風險考量。爲此，除了推廣與強化使用電子簽章機制的信心，以確保網路交易安全外，相關配套機制，如網路認證保險、網路信賴交易機制乃至消費者保護措施等，都是健全網路交易環境所必須的工具。

爲確保消費者的使用權益，及因應消費者面對高科技技術時所可能欠缺的專業能力，我國電子簽章法規定：就憑證機構經營或提供認證服務的相關作業程序，致當事人受有損害，或致善意第三人因信賴該憑證而受有損害時，係透過過失推定及舉證責任倒置的方式，要求憑證機構必須證明其經營或提供認證服務的行爲無任何過失，始得免負賠償責任，以維護消費者的權益並平衡專業能力的落差。

就此部分，我國在消費者保護方面亦立有「消費者保護法」專法加以規範，就企業經營者所提供的服務，要求必須無安全上的危險，同時要求必須於明顯處標示警告標示及緊急處理危險的方法[11]。準此而言，憑證機構所提供的服務，自然必須遵守消費者保護法的規範意旨。此外，因消費者保護法亦賦予主管機關得公告憑證服務的定型化契約應記載事項與不得記載事項，其有違反者，該契約條款將被認定無效[12]。在憑證機構、主管機關與消費者三方間，就憑證服

[11] 依據我國《消費者保護法》第 7 條之規定：「從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性。商品或服務具有危害消費者生命、身體、健康、財產之可能者，應於明顯處爲警告標示及緊急處理危險之方法。企業經營者違反前二項規定，致生損害於消費者或第三人時，應負連帶賠償責任。但企業經營者能證明其無過失者，法院得減輕其賠償責任。」

[12] 依據我國《消費者保護法》第 17 條之規定：「中央主管機關得選擇特定行業，公告規定其定型化契約應記載或不得記載之事項。違反前項公告之定型化契約，其定型化契約條款無效。該定型化契約之效力，依前條規定定之。企業經營者使用定型化契約者，主管機關得隨時派員查核。」

務的提供及規範與消費者保護法，其間之適用競合問題，亦須建立一套遊戲規則。

同時，由於我國係採公領域與私領域憑證機構並行制度[13]，機關亦可擔任憑證機構。復依學者[14]見解，現行國家賠償責任有兩種，在兩種國家賠償責任之中，公務員違法責任採過失賠償主義，須有公務員個人有故意或過失，始成立國家賠償[15]；而公共設施之瑕疵責任中，則採無過失賠償主義[16]。因此，在機關因提供憑證服務而導致人民受有損害時，其賠償責任方面尚有國家賠償法之適用，故國家機關擔任憑證機構時是否亦有國家賠償責任的問題，亦值得探討。

3. 是否能順應時代潮流與國際接軌並積極促進相關產業發展

電子商務是一個全球性的市場，因此當網路使用者欲於其他國家網站上購買商品或外國企業傳遞電子文件而使用電子簽章機制時，則台灣憑證機構核發的憑證是否爲當地國家的憑證機構所承認，換言之，當地網站或企業是否應該信賴由台灣憑證機構所簽署的憑證而以此確認電子簽章使用者的身分真實性？

上述問題涉及到憑證機構或憑證的相互承認，依電子簽章法第 15 條之規定，基本上對於依外國法律組織、登記的憑證機構所簽發的憑證，須在國際互惠及安全條件相當的原則下，經主管機關許可後，取得與本國憑證相同的效力。但就此部分，仍存有一些疑問，有待主管機關進一步確認，例如電子簽章法並未就本國的憑證機構安全性爲規範，則單就外國憑證機構要求安全條件相當的描述，究竟應該如何解讀？是外國憑證機構許可辦法第 5 條所規範之內容要

---

[13] 依據我國《電子簽章法》第 2 條第 5 款之規定：「憑證機構：指簽發憑證之機關、法人。」

[14] 吳庚著，行政法之理論與實用，三民書局，台北，民國 90 年 8 月增訂 7 版，頁 665。

[15] 依據我國《國家賠償法》第 2 條第 2 項之規定：「公務員於執行職務行使公權力時，因故意或過失不法侵害人民自由或權利者，國家應負損害賠償責任。公務員怠於執行職務，致人民自由或權利遭受損害者亦同。」

[16] 依據我國《國家賠償法》第 3 條第 2 項之規定：「公有公共設施因設置或管理有欠缺，致人民生命、身體或財產受損害者，國家應負損害賠償責任。」

求，亦或另有所指？有無觸及違反 WTO 的反歧視性原則？等問題均待進一步釐清。

另一個亟待解決的問題是，如果外國憑證機構未經主管機關的許可而交易雙方已經約定承認或使用該外國憑證時，依我國電子簽章法的規定，該外國憑證因未經許可係屬無效的憑證。既然如此，那麼在交易雙方間，其交易行爲的效力，應該如何認定？而該未經許可的外國憑證，在證據法則上，是否真的無法達到證明的目的，亦值得探討研究。

觀諸電子簽章法全文，關於與憑證機構相關規範，僅規定於第 11 條至第 15 條。其中第 11 條規定關於「憑證機構應製作及公布憑證實務作業基準」、第 12 條規定「違反第 11 條之罰則」、第 13 條規定「憑證機構終止服務之程序」、第 14 條規定「憑證機構之損害賠償責任」、以及第 15 條則是規定「外國憑證機構所簽發憑證之效力」，總共 5 個條文，如再扣除第 15 條，則實際上我國現行法制對憑證機構之管理規範僅有 4 條。簡言之，我國對於憑證機構之管理規範目前僅要求憑證機構負有對外揭露義務(亦即僅書面審查其所提出之憑證實務作業基準)，原希望藉此促使憑證機構在相關重要事項方面，能確實擬定公開明確的處理政策與作業程序，以便消費者判斷憑證機構服務之可信度。然在實務上憑證機構是否均確實「奉行不悖」還是僅「行禮如儀」，主管機關無從確認及控管。

申言之，我國現行電子簽章法制就憑證機構之管理規範係採低度管理原則（電子簽章法第 11 條）[17]，但憑證機構所提供者係身分認證服務，在電子交易中就交易當事人之身分提供認定依據，而在採低度管理之原則下，並無法確保憑證機構之可信賴性及保障電子交易之安全。

[17] 我國現行憑證機構之核定，依據我國《電子簽章法》第 11 條之規定，係採書面審查制度，即憑證機構製作憑證實務作業基準送經主管機關書面審查核定後，即可對外提供簽發憑證服務。

相較於國際間就憑證機構管理規範之發展趨勢均改採「高度管理」[18]原則，目前我國法規並未相應就憑證機構之營運管理透過法制進行較詳細規範。隨著憑證應用之持續發展及成長，如何因應憑證機構實務需求並符合國際發展趨勢與國際接軌，有必要對現行憑證機構管理規範作全面之檢討。

同時，關於憑證機構之責任，除如前述就消費者保護之立場而探討與消費者保護法之間的適用競合問題外，尚涉及憑證機構所依附之新興科技---網際網路有關。憑證機構提供電子憑證認證，須仰賴專業機房供主機置放及網際網路連線，倘該憑證機構非同時爲電信業者時，如因電信業者所提供之機房服務及網際網路連線中斷而導致簽發及管理憑證作業有疏失時，而在電信業者受電信法責任限制保護[19]之情形下，憑證機構無法將責任轉嫁時，應採取何種處理方式，使責任較爲衡平而不致扼殺憑證機構業者生存空間？

至於跨國交互認證及外國憑證效力認定部分，除涉及技術面的問題，因爲各國公開金鑰基礎建設架構的不同，導致應用程式難有單一設計，而增加跨國交互認證困難度外，跨國交互認證主要的困難與障礙乃在於各國憑證機構之營運方式及法令規範之差異性，亦即各國憑證機構因憑證政策、憑證實務作業基準、使用範圍、憑證保證等級等不同，導致彼此難以整合並建立相互信任之機制。

緣筆者任職於國內憑證機構「是方全球憑證中心」之二類電信業者是方電訊股份有限公司，負責公司法律事務，在實務操作上即因現行法制規範不足而深感無所適從，尤其是當公司於去年因不堪虧損而決定終止憑證服務業務，且將原有客戶及其服務移轉予由其直接承接相關機器設備及原廠授權，所申請新

---

[18] 所謂「高度管理」係指現行書面審查外，憑證機構尚須提交通過外部稽核機構之稽核報告，透過外部稽核機制確保憑證機構之營運與其憑證實務作業基準記載達一致性；而透過實質審查亦可增加憑證機構營運之可信賴性，對於推行憑證互通及憑證機構管理制度之國際接軌有所助益。

[19] 依據我國《電信法》第 23 條之規定：「用戶使用電信事業之電信機線設備，因電信機線設備障礙、阻斷，以致發生錯誤、遲滯、中斷或不能傳遞而造成損害時，其所生損害，電信事業不負賠償責任，但應扣減所收之費用。」

成立之「威利全球憑證中心」時，並無應有之規範可供依循而延宕時程徒增相當多之經營成本，因此引起筆者對相關問題探討之動機。

本論文之研究目的，即以憑證機構業者之角度出發透過「是方全球憑證中心」移轉至「威利全球憑證中心」之實務承接經驗，對現行憑證機構管理規範作檢視及檢討，並就筆者之實務經驗結合國際趨勢之相關規定，提出建議增修方向以期促進相關產業良性發展暨加速國際化並保障交易安全。

1.3 研究範圍及方法

1.3.1 研究範圍

本論文研究客體爲「憑證機構之相關規範」，研究範圍係自實務面之角度出發，先從憑證機構於公開金鑰基礎建設之定位與功能開始，了解我國及各主要先進國家之電子認證新興科技產業發展現況及電子憑證應用情況，進而探討各國法制對憑證機構規範之現況及趨勢，檢討我國法制之不足之處，其中主要重點集中於憑證機構之管理、注意義務及責任限制等方面，最後提出建議修法方向，以其在兼顧產業發展及消費者保護之兩大目的中，取得最大之平衡點。

1.3.2 研究方法

本論文研究方法係以我國現行電子簽章法爲基礎，佐以研究者本身產業實務及參與相關修正草案說明會所習得之經驗及知識爲輔，而相關之研究方法概述如下：

1. 歷史方法

將先回顧電子認證服務發展之歷史與經驗，分析各外國立法例之利弊得失，並檢討其優缺長短，並參酌我國之國情環境，希望能提出符合我國情需要以及確實可行修法建議。

2. 比較分析

就所蒐集之國內外文獻、法規資料、實務運作資料及官方文件等，建立其

架構體系。以介紹性文獻爲始，進而就所蒐集之國內外資料，按國別分別以其推動電子認證服務之政策面、法規範面及其實務運作面進行歸納與分析。同時，將電子簽章之科技技術層面及法律層面的問題綜合分析，加上研究者本身之實務經驗，以兼顧二者之需求及特性，使其不致窒礙難行。

1.3.3 論文架構

本論文一共五個章節，茲將架構概述如下：

1. 第一章：緒論

本章闡述本論文之研究動機、研究目的、研究範圍及研究方法，藉以建立本論文之架構與目標。

2. 第二章：公開金鑰基礎建設中憑證機構定位與功能

本章闡述憑證機構在公開金鑰基礎建設中之定位及功能。首先先簡介公開金鑰基礎建設架構及相關概念，包含「電子簽章」、「數位簽章」、「公開金鑰密碼系統」及「公開金鑰基礎建設」等，以建立對公開金鑰基礎建設之認識，並切入本章所定「公開金鑰基礎建設中憑證機構定位與功能」之研究重點，以突顯憑證機構於公開金鑰基礎建設架構之重要性。

接著整理介紹我國及技術先進各國公開金鑰基礎建設之應用現況及發展趨勢，進而自憑證應用領域現況及發展趨勢探討公私領域應用現況所生之相關規範需求，並歸納衍生出公私領域憑證應用之現況及目前制度問題之所在。最後闡述在現行法制下民間憑證機構所面臨之困境，以彰顯修法之重要性。

3. 第三章：憑證機構於電子簽章及交易法制之法律問題

本章從探討憑證機構之法律定位出發，討論其公證第三人之角色與傳統法律概念中之「公證人」及「戶政機關」概念之異同。進而討論憑證機構與交易主體(憑證註冊者及憑證驗證者)間之法律關係，包含憑證機構者與憑證註冊者間之認證服務契約關係、憑證機構與憑證驗證者間之信賴關係以及憑證註冊者

與憑證驗證者間之法律關係之一般法律交易關係，以釐清憑證機構運作所生之法律關係。

接著進入實務面探討憑證機構之設立、管理與廢止之相關問題，藉由整理比較各國對憑證機構管理之法制現況以突顯現行規範之不足。同時亦藉由整理比較各國對憑證機構所課予之責任法例，進一步探討憑證機構應擔負之注意義務及法律責任，以尋求兼顧交易安全、消費者保護及促進產業發展間之平衡點。

4. 第四章：我國現行法對憑證機構之規範及檢討

本章係針對我國現行法制關於憑證機構規範，分別就「電子簽章法」及其三部子法：「電子簽章法施行細則」、「憑證實務作業基準應載明事項準則」及「外國憑證機構許可辦法」，作整理介紹並提出具體之檢討，以彰顯我國法制不備之處。

5. 第五章：電子簽章法制關於憑證機構管理規範之修法建議－代結論

本章提出我國對電子簽章法制關於憑證機構管理規範之修法建議，以作爲本論文之結論。先闡述建立憑證機構管理規範完備法制之重要性，再進而歸結本論文研究之心得，提出對電子簽章法制關於憑證機構管理規範之修法建議，期使我國能建立完備之憑證機構規範法制，以應付一日千里之電子商務需求及與國際接軌，促使電子認證事業蓬勃發展，並保障交易安全及消費者權益。

公開金鑰基礎建設中憑證機構定位與功能

公開金鑰基礎建設架構及相關概念之簡介

2..1.1　電子簽章與數位簽章[20]

1. 電子簽章

電子簽章（electronic signature），指以電子形式存在，依附在電子文件並與其邏輯相關，可用以辨識電子文件簽署者身分及表示簽署者同意電子文件內容。

2. 數位簽章

數位簽章（digital signature），指使用數學演算法（或稱雜湊函數）將電子文件轉化爲固定長度之數位資料（訊息摘要），並用簽署者之私鑰對其加密形成一簽體，使任何人可藉未轉化前之原始資料訊息、簽體及與私鑰相關連之公鑰，驗證該簽體是否使用與簽章公鑰相對應之私鑰製作，以及簽體製作後，原始資料訊息是否遭受竄改。

3. 電子簽章之技術範圍大於數位簽章[21]

數位簽章專指以「非對稱型」密碼技術製作的電子簽章，而電子簽章的製作技術除了可應用「非對稱型」的密碼技術(Asymmetric Cryptography)[22]之外，由於近年來生物科技等用於鑑別身分的技術（指紋、聲紋、眼紋、DNA）也正蓬勃發展中，爲免立法影響到科技的創新發展，主要的國際組織如：聯合國及歐盟近年來積極推動各國應採取「技術中立」的原則（於下列 4 說明），不要限定僅能使用「非對稱型」密碼技術作爲製作電子簽章的唯一技術，凡是任何可

---

[20]「電子簽章相關問題集」，http://hca.doh.gov.tw/HCA/QA/ESignQA.html#q6，第 6 題，2007/7/30 visited。

[21] 陳群顯著，「電子簽章法之研究」，東吳大學，法學院法律專業法律碩士班碩士論文，民國 89 年 7 月，頁 5。

[22] 使用兩把不同的金鑰分別用以加密和解密的方法。其特性爲不能根據用以加密的金鑰計算出解密的金鑰。

以轉成電子形式之技術，只要能符合特定的安全需求（例如：能夠確保資料的完整性、鑑別使用者的身分及防止事後否認），皆可用來製作電子簽章。

4. 「技術中立」之立法例[23]

如何規範電子簽章之效力，目前立法例上所採之立法技術，大致可歸納爲三種模式：

(1) 技術特定立法：此種立法模式，係以「非對稱性密碼技術」（Asymmetric Cryptosystem）爲基礎之數位簽章（Digital Signature），由於目前此種技術與安全性上均已相當成熟，在應用上亦最爲普遍，故直接就該技術加以規範，馬來西亞於西元 1997 年所訂立之數位簽章法即爲適例。此種立法方式，係以現實應用爲考量，故對於數位簽章之應用技術以及相關法律責任，均有明確的規範。然因其僅對特定技術立法，日後可能會因法律的引導作用，反而對其他技術造成排擠效應，扼殺其他技術發展的空間。

(2) 混合式立法：此模式又稱爲「二階式模式」（two-tier approach）。其基本上先就所有電子簽章之效力作一般、原則性的規範；但是於同一法律中，另行針對以某種特定技術（通常即是數位簽章技術）所做成之電子簽章加以規定，並對以此種技術所做成之簽章，推定其產生一定的法律效力。此規範模式目前爲多數國家與國際組織所採。除歐盟、新加坡外，聯合國國際貿易委員會於西元 2001 年所公布之「電子簽章模範法」亦採此模式。此模式之優點在於：其不僅爲未來其他技術預先設定了法律承認的空間，同時也對現行數位簽章之應用，作了可資遵循的明確規範。然批評者則認爲，混合式的立法，一方面僅以概括承認電子簽章效力的方式，預先爲其他技術的發展作一般性的規範；而另一方面，針對現已成熟之數位簽章技術，

[23] 黃大洲著，「技術中立？技術特定？」，http://gcis.nat.gov.tw/eclaw/docu_2_19.asp，2007/7/30 visited。

卻在同一部法律中作特別性的規定，其結果不僅使規範架構比重失衡，且實質上亦可能如前述「技術特定立法模式」一樣，產生對數位簽章過份保護，反排擠其他技術發展空間之效果。

(3) 嚴格的技術中立立法：此種立法模式又稱爲「最低要求模式」(minimalist approach)，以美國之立法爲代表。在此模式下，立法者通常僅對電子簽章以必要、廣義的方式作定義，並概括的承認其效力，對於數位簽章或以其他特定技術做成之簽章，則在規定中隻字未提。採此模式之優點，在於能夠鼓勵多樣電子簽章技術的使用，而由市場自由競爭來決定何種技術最能爲大眾所信賴。但相反的，由於對電子簽章定義及規範之刻意簡化，在缺乏相關知識及法律引導的情況下，消費者是否具備足夠知識，來判斷其所使用之電子簽章技術之安全性，實令人存疑。

就我國現行電子簽章法之立法方式而言，依電子簽章法第 2 條第 2 款及電子簽章法施行細則第 2 條規定，只要是以電子形式存在，具有「附加於電子文件」、「與電子文件相結合」或是「與電子文件邏輯相關聯」等三種情形之一，並可以達成辨識及確認電子文件簽署人身分、資格及電子文件真僞之功能者，即可認爲係該法所稱之「電子簽章」。由於須符合「辨識及確認電子文件簽署人身分、資格及電子文件真僞之功能」之要件上限制，因此與上述(3)嚴格的技術中立模式中廣泛承認各類電子簽章之規範方式有所不同。如符合電子簽章定義者，電子簽章法則於第九條概括的賦予其法律效力。而對於現已成熟的數位簽章技術的應用，電子簽章法中亦以相當的篇幅，就其應用作特別的規定。因此，就立法技術而言，電子簽章法雖仍以技術中立爲主要立法原則，然並不採嚴格的技術中立立法模式，而是比較偏向混合式的立法。

從網際網路(Internet)通行無國界的角度觀之，由於各國立法原則之分歧，將使各國對電子簽章效力的認定產生不一致，而爲跨國性的電子交易投下不確

定性的因素，因此可能造成無謂的爭議及損失。例如：在美國法對電子簽章的規定下，僅僅在電子文件尾端鍵入姓名，並有簽名之意思，便可符合其法律定義下之電子簽章；然該種簽章在採技術特定立法模式之國家，卻可能因未使用該特定技術，而被視爲沒有簽章。對於此種歧異，聯合國雖企圖以制訂模範法[24]的方式來解決，然依現狀觀之，各國一致地完全採用該模範法之可能性仍微乎極微。

2.1.2 公開金鑰密碼系統[25]

密碼學〔Cryptography〕是維護所有資料安全技巧之總稱。藉由密碼學的幫助，可使發送端將訊息安全的送出，接收端在沒有他人竊聽、盜取或更改該訊息的安全環境下，將收到的訊息還原成可解讀的格式；密碼學最基本的兩個步驟分別爲加密和解密。

加密〔Encryption〕：利用複雜的函式，我們稱之爲加密演算法〔encryption algorithm〕，和特別的加密鑰匙〔encryption key〕，將明文〔plaintext，即原始的訊息〕轉換成密文〔ciphertext，即被轉換過的訊息〕的過程。

解密〔decryption〕：與上述過程恰好相反。利用複雜的函式和解密鑰匙〔decryption key〕把密文轉換成明文的過程。某些系統的加密key和解密key相同，有些則不同。

加密演算法使用的金鑰加密演算法可分爲兩種，一種爲對稱式金鑰加密法（Symmetric Key Encryption）、另一爲非對稱式金鑰加密法（Asymmetric Key Encryption），或稱爲公開金鑰加密法（Public Key Encryption）。

1. 對稱型加密法

---

[24] 聯合國於 1996 年通過《聯合國電子商務模範法》(UNCITRAL Model Law on Electornic Commerce 1996)。

[25] 蕭姿妍、鍾慧萱合著，「E-payment SSL 線上交易系統」，http://www.csie.nctu.edu.tw/~project/2003/team7/crypto.htm ，2007/7/30 visited。

對稱型加密法即所謂「對稱金鑰演算法」(symmetric-key algorithm)或「秘密金鑰演算法」(secret-key algorithm),其所使用之加密及解密之金鑰,爲相同一把金鑰,意指使用相同一組密碼來加解密。使用對稱式金鑰加密的好處在於其加解密速度快,不會對系統產生太大的負擔,因此若雙方都握有同一把對稱式金鑰,則可對訊息傳送做加解密的動作。但由於加、解密是同一把金鑰,所以這把金鑰無法公開,於是又稱做「私密金鑰」〔private key或secret key〕。此爲對稱金鑰演算法也稱做私鑰或秘密金鑰演算法之故。

由於訊息的加密和解密採用相同的金鑰。所有參與者都必須完全信任且彼此瞭解,而每一位參與者都保有一把金鑰複本。傳送者和接收者在交換訊息之前,必須分享相同的金鑰。而在協調產生金鑰的過程中,任何有關金鑰產生的訊息都必須保證不會被竊聽(透過安全通道來分配) 。一旦金鑰被第三者取得或算出,則訊息不保。這類的演算法常常用來對資料區塊〔block〕或資料流〔stream〕做加密。區塊演算法是先將訊息等分成大小相同的區塊,一次對一個區塊做加密。串流演算法則是一次對一個位元做加密。由於可能的金鑰總數非常大,除非拿到解密的金鑰,否則幾乎無法破解對稱金鑰演算法。

對稱型加密法速度快,適合加密大量資料。然而,在公眾網路上通訊者之間的金鑰分配(金鑰產生、傳送和儲存)是很麻煩的。所以,秘密金鑰加密法很難直接應用於電子商務上,除非有安全的金鑰分配方式;著名的對稱型加密演算法有DES、IDEA、TripleDES等。

2. 非對稱型加密法

非對稱型加密法即所謂「非對稱金鑰演算法」(asymmetric-key algorithm)或「公開金鑰演算法」(public-key algorithm),於西元1976年,由Diffie和Hellman首度提出,其最大之特點在於發送方(加密)及接收方(解密)採用兩把不同的金鑰,一把稱爲公開金鑰,另一把稱爲私密金鑰(Private Key),意即公開金鑰爲公開對外,而私密金鑰則由擁有人自行保存,兩支金鑰配對使用。

西元 1978 年，Ron Rivest、Adi Shamir 和 Len Adleman 提出符合公開金鑰密碼系統的演算法，稱爲 Rivest-Shamir-Adleman（RSA）演算法，一直到今天，RSA 還是一個最簡單、最被廣泛使用的公開金鑰演算法，並且其同時能滿足加/解密和電子簽名兩項需求。雖然其安全性至今尚未有人能以數學定理嚴格的證明，一般皆認爲 RSA 演算法是相當安全的，也沒有公開文獻對它提出有效的破解方式，因此目前大部分的系統都還是以 RSA 作爲其公開金鑰演算法。

3. 目前公開金鑰密碼系統主要應用在下列三方面[26]：

(1) 加密/解密

(2) 金鑰的交換

(3) 電子簽名

茲將此三種應用說明如下：

(1) 加密/解密

公開金鑰密碼系統雖然解決了金鑰的散佈問題，但是由於其演算法都是大量的數學運算，所以相對於秘密金鑰密碼系統來說，速度相當的慢。以 RSA 和 DES 來做比較，其加/解密的速度可以相差到 1000 倍，所以在實際應用時，通常不會以公開金鑰演算法去加/解密真正要傳輸的資料，而改以加/解密一些較小、且必須要用公開金鑰演算法去加密的資料。

(2) 金鑰的交換 （Key Exchange）

由於速度慢是公開金鑰演算法的致命傷，所以一般還是以秘密金鑰演算法來加密資料，但使用者可以用公開金鑰演算法來做秘密金鑰的交換[27]，使得傳輸資料雙方可以安全的得到相同的金鑰。其步驟如下(假設 A 要傳送資料給 B)：

---

[26] 黃士殷、朱成康合著，「公開金鑰密碼系統」，http://www.cse.yzu.edu.tw/people/list?sort=12 ，2007/6/30 visited。

[27] 經由非安全管道傳送私密金鑰之機制。

① A 取得 B 的公開金鑰；

② A 以亂數產生一秘密金鑰，並且用 B 的公開金鑰加密，傳送給 B；

③ B 將收到的資料用其私密金鑰解開，取得 A 產生的秘密金鑰；

④ A 和 B 開始用此秘密金鑰通訊。

此系統常常被稱爲 Hybrid Cryptosystem，使用此方式來作爲加密系統，除了速度快以外，安全性也很高，因爲所使用的秘密金鑰都是在每次要傳輸時，以亂數產生，每次傳輸所使用的金鑰皆不同，所以被破解的機率很低，就算秘密金鑰被破解，也只會洩漏出那次傳輸的資料，對於之前或之後的傳輸並沒有影響，使用者只需保護好他們的私密金鑰即可。

(3) 電子簽名

電子簽名在資訊電子化的過程當中，扮演一個非常重要的角色，在網路上的應用非常的廣，所有電子公文的認證，電子錢幣的交易等等，都會使用到電子簽名。但是在傳統的文件電子化後，一些認證的問題也隨之產生，傳統的簽名方式已無法使用在現今的電子檔案上面，所以必須發展一種新的電子簽名方式，而且其最少要滿足下列需求：

① 身份認證：要能證明此份文件確實是被簽名者親自簽名；

② 不可僞造性：此份簽名必須無法被他人僞造；

③ 不可重複使用性：文件上的簽名無法被拿到其他文件上重複使用；

④ 不可改變性：文件被簽名後，就無法再改變；

⑤ 不可否認性：簽名者簽過名後，就無法否認此簽名爲其所簽；

⑥ 可驗證性：此簽名必須能讓第三者驗證，以解決紛爭。

利用公開金鑰演算法來達到電子簽名的需求的方法簡述如下：

假設 A 要對某文件簽名，而 B 要驗證此簽名是否正確；

① A 用他的私密金鑰對此文件加密，也就是做簽名；

② A 將此份簽名連同原始文件一同送給 B；

③ B 用 A 的公開金鑰對簽名解密，並與原始文件比對，若正確無誤，則驗證成功。

茲將上述例子檢驗如下：

① 身份認證：B 用 A 的公開金鑰來驗證，所以可確定是 A 自己簽名的；

② 不可僞造性：因爲只有 A 有他自己的私密金鑰，所以沒有他人能僞照 A 的簽名；

③ 不可重複使用性：由於簽名是對那份文件加密，不同的文件有不同的簽名，所以無法將此簽名重複使用在別的文件上；

④ 不可改變性：在簽名過後，任何人只要對原始文件做更動，就會和用公開金鑰解密出來的文件不同，簽名即告無效；

⑤ 不可否認性：由於只有 A 擁有其私密金鑰，一旦簽名後，就不能否認此簽名；

⑥ 可驗證性：因爲任何人都可取得 A 的公開金鑰，所以任意第三人均可驗證 A 的簽名。

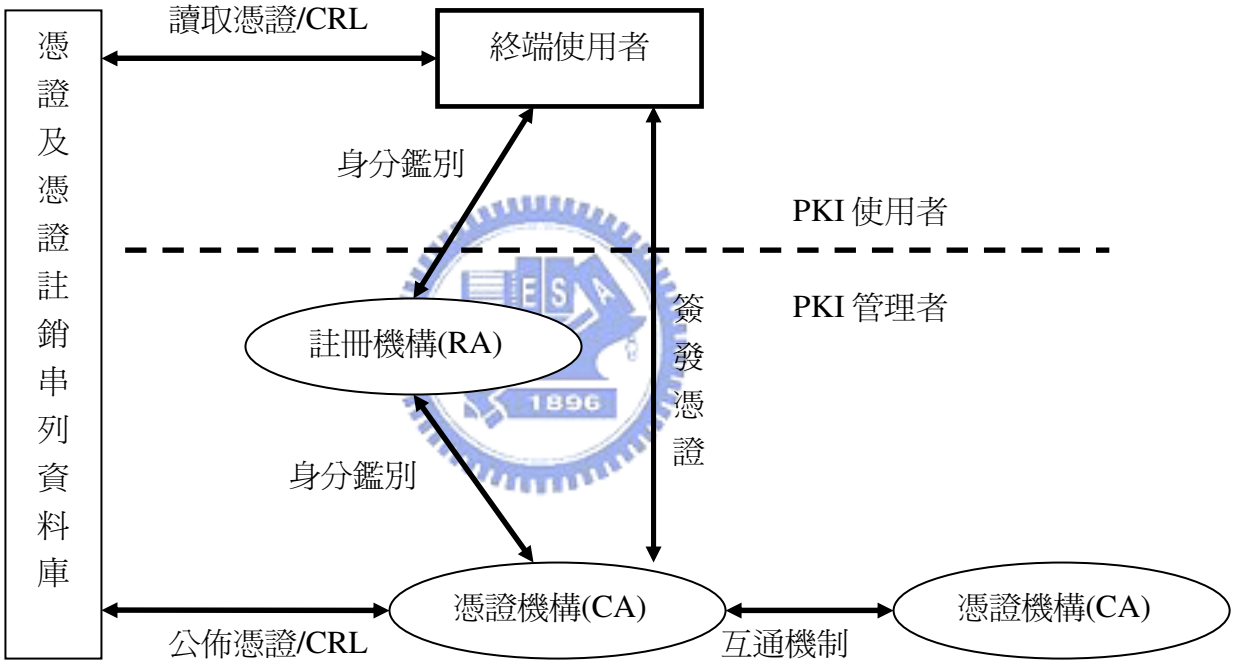
在公開金鑰演算法中，以私密金鑰加密的資訊只能由相關的公開金鑰所解密，反之亦然。而且幾乎不可能從加密金鑰推算出解密金鑰。因此，公開金鑰密碼系統可以讓素昧平生的雙方，無須事先交換金鑰即可達秘密通訊的特性，由此可知，公開金鑰的優點在於其安全完整性和鑑別性高。

2.1.3 公開金鑰基礎建設

誠如前述，網路上之資訊既需仰賴加密技術保護其安全但又必須兼顧便利性（得以數位簽章方式傳送）及流通性（得將一把金鑰公開）之前提下，採用公開金鑰密碼系統是就目前技術水準而言，是公認最佳之選擇。在公開金鑰密碼系統中，每個使用者均擁有一個金鑰對，其中公開金鑰放在網路上公開散佈，而私密金鑰則由使用者保存，爲了讓公開金鑰使用者的身分之間產生緊密之連結而不會發生誤用之情形，公開金鑰基礎建設便應運而生。

公開金鑰基礎建設主要即是利用對於訊息的加密金鑰與解密金鑰不是同一把金鑰之非對稱加密技術，並運用公開金鑰及電子憑證以確保網路交易的安全性及確認交易對方身分之機制。公開金鑰基礎建設係以網路認證之信任機制爲基礎，交易雙方相互地信任其認證機構，搭配金鑰對之產製及數位簽章等功能，即可經由其認證機構核發之電子憑證確認彼此的身分，並提供資料完整性、資料來源辨識、資料隱密性、不可否認性等四種重要的安全保障。[28]

1-1：公開金鑰基礎建設運作示意圖[29]



資料來源：Adams, Sylvester, Zolotarev, Zuccherato, 2000

在公開金鑰基礎建設模型中，有 4 個主要元件[30]：

[28] 台灣電腦網路危機處理暨協調中心，「公開金鑰基礎建設之運作：以 GPKI 爲例」，http://www.cert.org.tw/document/column/show.php?key=99 ，2007/7/30 visited。

[29] 尤弘任著，「基於公開金鑰基礎建設之電子文件系統」，台灣科技大學，資訊管理研究所碩士論文，民國 95 年 6 月，頁 13。

[30] 朱建達著，「建立於公開金鑰基礎建設的單一切入系統」，交通大學，資訊科學研究所碩士論文，民國 90 年 6 月，頁 21。

1. 憑證使用者（Certificate user）：使用者自己產生一個金鑰對後，分別交給註冊中心與憑證中心以取得一份憑證；或者在需要與另外一位使用者溝通的時候，向憑證貯藏中心要求查詢這一位使用者的憑證。
2. 註冊中心（Registration Authority, RA）：使用者將金鑰對交給註冊中心驗證之後，註冊中心會一份經過認可但尚未簽署的憑證，交由憑證中心來完成簽署。
3. 憑證中心（Certificate Authority, CA）：憑證中心在憑證上簽章，完成簽署手續，並存入憑證貯藏中心，讓憑證可以經由查詢而得到，如果憑證出現問題，或是依使用者之要求，憑證中心可依照程序來廢止一份憑證。
4. 憑證貯藏中心（Certificate Repository）即目錄伺服器（Directory Server）：儲存憑證中心所簽署出之憑證，與憑證廢止清單（Certificate revocation, CRL），後者列有所有憑證中心公告廢止之憑證，讓所有人得隨時查詢到最新的資訊。

誠如前述，由於在實務運作上，公開金鑰演算法的速度很慢，如需簽名的文件很大，則會使簽名很沒效率；同時如需將簽名儲存，將佔去相當大之容量，二者均會造成整體公開金鑰系統運作速度的遲緩；而且如要將簽名交由第三人保管，通常不希望第三人知道所簽名之文件內容，因此簽名整份文件亦不可行；基於上述之需求，故須應用「單向雜湊函數」[31]（One-Way Hash Function）來取代簽名整份文件，將電子文件之訊息摘要（Message Digest）[32]加以簽章。

所謂「單向函數」係指：若我們有一變數 x，讓我們可以很容易計算出 f(x)，但卻很難由 f(x)反推回 x，則此 f()函數就稱爲一單向函數。而所謂「雜湊函數」（hash function），係一種數學演算法；簡而言之，係指可以將一個變動長度的

[31] 同註 26。

[32] 由雜湊演算法將訊息濃縮後之摘要，類似訊息之「數位指紋」。訊息摘要可以公開，且無法從訊息摘要中還原解讀出原訊息的內容。

字串轉爲固定長度字串的函數，稱爲此字串的雜湊，且通常雜湊都會比原來的長度還短。故所謂「單向雜湊函數」就是一個單向的雜湊函數，亦即算出一個字串的雜湊是容易的，但卻很難由雜湊推回原本的字串。同時，一個好的單向雜湊函數，尚須滿足近似「無碰撞」(collision-free）的特性，即很難找到兩個不同字串產生出相同的雜湊。因此相同訊息輸入經由壓縮函數運算產生輸出結果必定相同，且決無法由輸出的結果推算出輸入的訊息。

利用單向雜湊函數的特性，我們可以在電子簽名之前，先將電子文件加以雜湊，成爲一固定長度的字串，(此長度通常都很小，亦即訊息摘要)，然後對此字串以私密金鑰加密，得出來即爲此份電子文件的簽名。當要驗證此簽名時，先用公開金鑰將此簽名解密，然後算出原電子文件的雜湊，兩相比較若相等，則因爲「無碰撞」的特性，可證明此電子簽名確實是針對這份電子文件所做的簽名。由於此雜湊長度很小，用公開金鑰演算法並不會浪費很多時間，儲存簽名的空間也可以大幅減少。並且在交由第三人保管時，別人也無法由雜湊得到原始的電子文件(單向性使然)。同時，利用單向雜湊函數的特性，亦會達到「保密」之功能；當第三人在電子文件傳輸之過程中即使將訊息攔截下來，其所得到的也只是一串無意義的亂碼(訊息摘要)，而第三人無法將此亂碼還原成電子文件，故能有「保密」之效果。[33]

由上可知，將雜湊函數與公開金鑰基礎建設架構互相搭配，即可提供身分識別 (Authentication)、隱密性 (Confidentiality)、資料完整性 (Integrity)及不可否認性 (Non-repudiation) 等四項功能需求。茲將此機制簡述如下[34]：

1. 首先，電子文件透過單向雜湊函數的運算，產生訊息摘要，而單向雜湊函數並具有保持電子文件完整性(Integrity)之功能。

---

[33] 洪清波著，「以單向雜湊函數爲基礎之認證機制」，樹德科技大學，資訊工程研究所碩士論文，民國 94 年 6 月，頁 13。

[34] 經濟部，「PKI 互通技術及應用研究報告」，http://www.pki-pma.org.tw/learn/download/1/2005-02-02-03.pdf，頁 12，2007/7/30 visited。

2. 其次，該訊息摘要以發送人之私密金鑰加密，此舉即可使收受人向憑證中心查詢發送人的公開金鑰及電子憑證是否有效；如收受人得以發送人寄存於憑證中心處之公開金鑰解密，則因發送人之私密金鑰原則上僅有發送人得以持有及使用，因此發送人無法否認該訊息摘要爲其簽發及傳送，便可證明該訊息摘要是由發送人所簽署，達到「不可否認性」之功能；而收受人向憑證中心查詢及驗證發送人資料的動作，即是「身分識別」、「可驗證性」之功能。
3. 之後，再將該訊息摘要以收受人寄存於憑證中心處的公開金鑰加密，而該訊息摘要只有收受人所保管之私密金鑰方得解密，如此第三人即使攔截到訊息也無法輕易解開該訊息摘要，而具有「隱密性」之功能。
4. 經過上述 2、3 兩道加密程序後，即形成一數位簽章，發送人於網路上所傳輸之內容正是附有數位簽章之電子文件。
5. 收受人於收到該附有數位簽章之電子文件後，首先用自己之私密金鑰解開收受人寄存於憑證中心處的公開金鑰所爲之加密；因只有收受人得以解密，而具有「隱密性」之功能。
6. 其次，收受人再以發送人寄存於憑證中心處的公開金鑰解開，發送人以其私密金鑰所爲之加密。此時收受人即可確信該電子文件爲發送人所簽發，亦因發送人不能否認該數位簽章係由其所簽署，故具有「不可否認性」之功能。
7. 經過上述第 5、6 兩道解密程序後，即可獲得完整之訊息摘要；而如將電子文件全文利用單項雜湊函數運算，亦可獲得另一之訊息摘要，如將二訊息摘要比對後完全相同，即可信賴該電子文件於傳輸時全程均未經僞造變造或更改，故具有「資料完整性」之功能。

而整個公開金鑰基礎建設要能正常運作，公開金鑰的認證扮演重要的關鍵

角色，來驗證公開金鑰的歸屬者之簽名及證明此簽名確實是用其私密金鑰所加密，此即爲「憑證管理中心」（Certificate Authority，簡稱 CA）之重要性。電子交易之雙方透過向「憑證管理中心」申請「公開金鑰憑證」（public-key certificate），此憑證包含了申請者的基本資料和申請者的公開金鑰，而憑證管理中心會對此憑證做簽名，表示憑證管理中心確定憑證爲申請人所有，而使用者每次要使用他人的公開金鑰時，也是先取得對方的憑證，驗證是否有憑證管理中心的簽名，若驗證無誤，才能信任此憑證內的公開金鑰爲對方所擁有，如此達到認證之功能。

2.2 憑證機構於公開金鑰基礎建設之定位及功能

綜合上述，公開金鑰基礎建設機制運作模式需先爲每個通訊個體產生一組私密金鑰（簡稱私鑰）與公開金鑰（簡稱公鑰）的金鑰對，私鑰由通訊個體秘密保存，並將公鑰公佈。通訊個體可透過私鑰進行數位簽章或解密，而其他通訊個體則可使用他人的公鑰進行數位簽章的查證或資料加密。因此將面臨公鑰有效性鑑識，及如何鑑別私鑰持有者身分及識別公鑰完整性的問題。實務上主要是採用憑證基礎法來查證公鑰的有效性：憑證基礎系統需要一個客觀中立之可信賴憑證機構（Certificate Authority, CA），負責產生、管理及維護通訊個體之公鑰憑證。

簡言之，整個公開金鑰密碼系統要能正確運作、公鑰要能散佈達到公開目的，公開金鑰的認證是關鍵，因此「憑證管理中心」認證角色之重要性便在此，實言之，整個公開金鑰基礎建設機制的安全就建構在憑證管理中心是否可以在完全、毫不懷疑的被信任的基礎上建構出來。憑證管理中心根據註冊管理中心(Rigistraction Authority, RA)[35]認證的結果，爲合法的使用者簽發憑證，並將憑證

[35] 指負責確認用戶之身分或其他屬性，但不簽發憑證亦不管理憑證者。註冊中心是否單獨爲其行爲負責及其應負責任之範圍。依所適用之憑證政策或協議定之，註冊中心負責對憑證主體做身分之識別及鑑別，但不做憑證之簽發。

以人工傳送的方式公佈至網路上公開的儲存庫供所有使用者查詢。若是使用者欲廢止他目前所擁有的憑證，亦或是一憑證已過期，憑證管理中心亦須將這些憑證集合起來，產生憑證廢止清冊，並公告周知或以其他方式送給使用者。如此當使用者收到一憑證時，便可以經由檢查憑證廢止清冊判斷此憑證是否已失效。

在公開金鑰基礎建設之運作流程簡述[36]即爲：由註冊中心統籌、審核使用者的憑證申請，然後將憑證申請送至憑證中心處理；憑證中心發出憑證，並將發出憑證資訊公告於目錄服務（Directory Service, DS）中。故可得知，憑證機構於公開金鑰基礎建設架構中係扮演橋樑的角色，以公正第三人（Entrusted Third Party, ETP）的身分，利用憑證管理資訊系統(包括：憑證管理系統、註冊管理系統、目錄伺服器)對憑證作業流程執行嚴密的管理，提供憑證管理服務。其服務項目包括：申請者註冊、憑證的簽發、廢止、管理、產生稽核記錄等；亦即保管公開金鑰、核發電子憑證、接受憑證之交易相對人之驗證，使之信賴該電子憑證之效力，進而確認與其交易相對人之身分，以確保網路交易之安全性及安定性。

在此整理公開金鑰基礎建設所提供之服務如下[37]：

1. 數位簽章管理服務：確保私鑰及公鑰的一致性與完整性。
2. 密鑰及公鑰管理服務：金鑰保護、回復、稽核等措施。
3. 憑證管理服務：建立可信賴的公開金鑰機制(CRL, CKL)。
4. 目錄服務：個體相關訊息的保護(E-mail, Phone, Fax)。
5. 終端實體啓始服務：提供可信賴環境之驗證。
6. 個體符記管理服務：提供 Smart Card, IC card 之發行、儲存與保護。
7. 用戶端介面服務：提供標準及互通介面。

---

[36] 「是方全球憑證服務問答集」，https://www.chiefca.com.tw/FAQ03.php，2007/07/30 visited。

[37] 同註 34，頁 46。

8. 時戳服務：防止重送(replay)攻擊並達成時序同步(logical synchronous)。

同時，憑證管理中心的另一項重要任務是必須管理或是制訂與其他 PKI 互通的策略（包含國內與跨國），並於必要時爲其他憑證管理中心簽發互信憑證，以便執行公開金鑰基礎建設 互通的業務。對整體公開金鑰基礎建設發展環境而言，這項任務在可見的未來將益發重要。

2.3 我國公開金鑰基礎建設之應用領域現況及發展趨勢[38]

已如前述，依電子簽章法制，組織團體或法人企業皆可經營憑證機構業務，但在正式發放憑證前需先向憑證機構主管機關經濟部提出憑證實務作業基準（Certification Practice Statement，CPS），待經濟部審核通過後始可經營憑證機構業務。憑證機構應對其營運失誤所導致的任何損失負法律責任；就其效力來看，電子簽章法規定在國際互惠及安全條件相當原則下，經主管機關許可，由國外憑證機構所簽發之憑證與國內憑證機構簽發之憑證具有相同效力。

我國政府從民國 86 年開始規劃公開金鑰基礎建設、翌年(民國 87 年)2 月啓用「政府憑證管理中心」，期間通過電子簽章法、建立政府憑證總管理中心[39]、

---

[38] 經濟部商業司編印，2005 台灣 PKI 年鑑，台北，民國 95 年 2 月出版，第 7 頁以下。

[39] 憑證機構基本上提供的是一種「安全」及「信賴」的服務，憑證機構最重要的資產就是因其具備的專業能力及管理能力，足以讓使用者產生信任及信賴，願意相信它的「公信力」。但是，在實際的網路交易行爲中，可能交易雙方並非同一個憑證機構的使用者，雙方如何相互信賴呢？有兩個不同的機制：

1. 設計層級式的信賴體系，例如使用者甲的憑證是由「安心憑證機構」簽發，使用者乙的憑證是由「信心憑證機構」所簽發，但是「安心憑證機構」的公鑰憑證是由上一層的「一心憑證機構」所簽發（類似背書的作用），「信心憑證機構」的公鑰憑證也是由「一心憑證機構」簽發。所以，使用者甲及使用者乙雖然不是同一個憑證機構的使用者，但是因爲他們的憑證是由一個雙方可以共同信賴的「一心憑證機構」來背書，所以使用者甲及使用者乙即可以建立信賴的關係。因此，在層級式的信賴體系中，必須有一個全國總憑證機構作爲最高的信任來源。

2. 設計網路式的信賴體系，例如使用者甲的憑證是由「安心憑證機構」簽發，使用者乙的憑證是由「信心憑證機構」所簽發，雖然「安心憑證機構」與「信心憑證機構」沒有一個共同上的上層憑證機構爲其背書，但是兩者可以相互背書，所以使用者甲與使用者乙可以建立信賴關係。兩種不同的信賴體系各有其優缺點，政府將兼採兩者的優點，並設立國家總憑證機構。國家總憑證

內政部憑證管理中心、工商憑證管理中心等。目前我國 PKI 應用領域爲政府金融業以及醫療業。在政府憑證(GCA)方面：有內政部的自然人憑證(MOICA)、經濟部的工商憑證(MOEACA)、以及研考會的政府憑證、組織及團體憑證等，在於提供如網路報稅等便民服務；在醫療方面則有衛生署的醫療憑證管理中心，醫療憑證(HCA)應用有利於電子病歷發展，爲機密性需求高的醫療資訊提供安全的防護。茲將各政府憑證機構主要應用整理如下表：

表 2-1：各政府憑證機構主要應用

憑證機關	主管機關	主要應用
政府憑證管理中心(GCA)	研考會	● 公文電子交換系統 ● 網路報稅系統 ● 勞農保網路申辦系統 ● 電子採購系統
組織及團體憑證管理中心(XCA)	研考會	● 公文交換 e 網通 ● 勞農保網路申辦 ● 證期會公文電子交換 ● 農委會公文電子交換
內政部憑證管理中心(MOICA)	內政部	● 內政部（地政系統、戶政系統） ● 財政部（綜合所得稅申報系統） ● 交通部（公路監理系統） ● 經濟部（工商資料查詢系統） ● 勞保局（勞農保資料查詢系統） ● 中華電信公司（e 櫃檯作業系統）
工商憑證管理中心(MOEACA)	經濟部	● 公司線上申辦系統 ● 政府採購投領標系統 ● 勞保局網路申報及查詢作業系統 ● 外籍旅客消費特定貨物退還營業稅系統 ● 工商 e 網通作業平台 ● 財政部網路報繳稅系統—營業稅申報繳稅 ● 中央公債及國庫券電子連線投標作業系統

機構它扮演憑證機構中的憑證機構角色（類似於中央銀行扮演銀行中的銀行）。國家總憑證機構將不對一般使用者提供憑證簽發服務，而是對憑證機構提供憑證簽發的服務，以及研訂相關之技術規範等。

醫療憑證管理中心(MOICA)	衛生署	● 健保 IC 卡醫療專區 ● 醫療院所病歷電子化 ● 電子病歷索引中心 ● 醫院公文電子交換作業 ● 院際間醫療資訊交換或流通 ● 醫療院所內各類醫事人員電子化證照 ● 醫療院所健保費用連線申報作業 ● 醫療院所法定傳染病與出生之通報作業 ● 醫事人員電子證書 ● 醫事人員繼續教育訓練學分登記

資料來源：政府各憑證管理中心網站(2005/09)

在民間領域方面：目前共有 11 家核可之憑證機構[40]：主要應用領域在電子商務與金融交易及產業供應鏈等，所簽發之憑證總數估計約爲 65 萬張。在電子商務方面的應用可涵蓋：電子交易、電子發票、電子產證、通關貿易等應用；而在產業供應鏈方面則涵蓋：物流業、汽車業、電子業、鋼鐵業、石化業及印刷業等共 4000 多家大中小型企業。茲將各民間憑證機構主要應用及憑證數現況整理如下表：

表 2-2：各憑證機構及其主要應用

憑證服務提供者	營運公司	主要應用
信用卡（SET）憑證機構	台灣網路認證	● 信用卡 SET 交易
1. 網際 NB 憑證 2. 企業 EC 憑證 3. 商務 EC 憑證 4. 金融 XML 憑證	台灣網路認證	● 電子商務 ● 網路銀行 ● 網路下單 ● 期貨交易 ● 股務代理

[40] 事實上至筆者撰寫本論文時，網際威信及財金資訊之憑證業務均在進行併入台灣網路認證事宜，而是方電訊之憑證業務亦已由新成立之台網國際所承接。

金融最高層憑證機構（TFCA）	台灣網路認證	● 金融最高層憑證機構
金融政策憑證機構（TFPCA）	台灣網路認證	● 金融政策憑證機構
台灣金融用戶憑證機構（TFUCA）	台灣網路認證	● 金融交易 ● 電子支票
網際威信 VTN	網際威信	● 電子商務 ● 金融交易
網際威信（金融 XML 憑證）	網際威信	● 金融交易
台灣商務最高憑證中心	網際威信	● 電子商務
中華電信通用憑證管理中心	中華電信	● 企業憑證 ● 設備憑證 ● 一般用途
是方全球憑證服務	是方電信	● 一般用途
財金資訊股份有限公司	財金資訊公司	● 網路繳稅 ● 網路銀行

資料來源：經濟部商業司核定(許可)憑證機構名單(2005/09)

由上述統計可知，目前我國電子憑證應用範圍仍以公部門應用所佔比例最高，而私部門在電子憑證商業行爲之應用則以金融業爲首。以下進一步重點說明我國電子憑證應用現況：

1. 自然人憑證

我國自民國 92 年 4 月起由內政部開始核發一般民眾的網路身分證—自然人憑證，截至民國 95 年 8 月 5 日爲止核發數爲 1226226 張[41]，爲全球核發數量最多的國家。自然人憑證爲民眾的網路身分證，可透過網路直接進行電子化政府的各項服務，如：繳稅、繳罰款、申辦戶政等。同時，由於憑證上含有電子

[41] 內政部憑證管理中心，http://moica.nat.gov.tw/html/index.htm，2007/08/05 visited。

簽章與電子密碼，除了申請者與憑證機構之外，任何人即使拾獲此憑證也無法讀取資料，故其安全性是可以確保的。

雖然自然人憑證應用項目逐漸增加，但使用率卻不高，民眾對於網路作業仍舊不習慣，或者因使用複雜度高而導致使用率較低。倘若自然人憑證的應用未能符合民眾需求，將會是影響普及率的一項障礙。內政部目前正思考是否將自然人憑證原有的網路洽公服務拓展與其他應用結合，如結合金融卡、公司內部管理、駕照、健保卡、圖書證等功能，使其成爲一卡多用的網路身分證。對此，除了需思考民眾的便利性外，相關法律問題[42]與市場商機問題均有待謹慎研究。

2. 工商憑證

工商憑證爲企業在網路上與政府溝通的身分證，由經濟部於民國 92 年 8 月起正式啓用簽發公司行號憑證，提供企業各項便利且安全的線上作業申請。目前工商憑證應用服務項目包括公司預查、證明、抄錄與變更登記全程網路申辦作業、線上政府標案參與、勞保局網路申報及查詢作業系統（線上勞保申辦、查詢與申請等），國稅局也積極規劃營業稅、營利事業所得稅等網路申報系統。工商憑證創造 G2B 新價值鏈，是邁向電子化政府一個重要的里程碑。工商憑證規劃爲「單一正卡，多張副卡」，主要爲因應多個應用系統及多位承辦人員使用，減少卡片共用的情況，方便公司行號內部做有效控管及權責區分。

3. 醫療憑證

科技之進步與資訊之發達，使得現今醫療環境也逐漸改變，一方面民眾對個人病歷資料隱私愈來愈重視，另一方面醫療院所處在既競爭又合作的關係下，亦開始思考如何提昇醫療照護品質及醫療資訊的整合。衛生署於民國 92 年 6 月正式開始發放「醫事憑證 IC 卡」，目前主要兩項應用爲電子病例交換及醫療院所與衛生署之電子公文交換，未來將規劃與健保 IC 卡整合。

---

[42] 相關法律問題：例如隱私權之保護等。

此憑證以公開金鑰基礎建設作爲確保醫療資訊電子化作業安全機制，發放對象爲全國各醫事機構及人員。配合明全民健保 IC 卡之使用，醫生若要讀取病人健保 IC 卡內的醫病資訊，可透過醫師卡憑證之認證後始可進行存取，並對病人的電子病歷進行電子簽章，而所有的轉診轉檢資訊亦將透過醫療院所之憑證進行電子簽章，確實保障民眾就醫時所產生的私密性或敏感性資料。

4. 金融憑證

由於金融業對資訊傳輸與金流交易方面的高度安全需求，加上整體金流程序電子化帶來成本節省效益因素，使得該產業投入採行電子憑證的意願相對較高。目前金融業電子憑證均採用電子簽章機制維護交易傳輸安全，用以驗證網路交易中，使用者的身分真實性。

國內金融領域的電子憑證應用有金融 EDI 憑證、信用卡線上交易之 SET 憑證、網路銀行轉帳之 SET 憑證及 Non-SET 憑證等，銀行公會爲統一各銀行電子金融憑證規格，並保障往來客戶資料與交易的安全性，於民國 91 年 11 月正式啓用我國金融最高層憑證機構（Financial Root Certification Authority，FRCA），制訂相關規範並統籌各銀行間不同的憑證規格，以達跨行互通之效。目前，任何通過憑證政策管理中心（PMA）核可之銀行（亦即 User CA），其所發放給客戶的憑證皆可互通，達到一張憑證跨行使用的網路銀行功能。

2.4 各國公開金鑰基礎建設之應用現況及發展趨勢[43]

1. 美國

美國於西元 1998 年所通過之「消除政府紙張作業法案」強制規定，各個聯邦單位必須於西元 2003 年 10 月 21 日前開始提供電子化政府服務。雖然該法案本身並無強制規定各個聯邦單位必須採取公開金鑰基礎建設機制來實現電子化政府之目標，然而 PKI 功能及其搭配生物測定學等技術的優勢，再與其他現行

[43] 同註 38，頁 10 以下。

電子簽章替選解決方案比較後，美國聯邦政府認定公開金鑰基礎建設可提供較高層級的身分辨識及安全服務，因此始有美國聯邦政府公開金鑰基礎建設架構概念(Federal PKI；FPKI)概念的產生。

美國電子化政府架構下政府總服務管理部門(General Services Administration)於西元 2003 年 7 月發布電子驗證政策草案，內容列出四個保證等級—最小、低、基本及高且規範電子化政府應用均需對應到電子驗證政策所列的保證等級。

整體而言，公開金鑰基礎建設在美國各州政府部門之應用，因爲教育訓練缺乏、總體經濟發展趨緩及 911 攻擊事件之發生等，未如預期般的大幅成長。美國聯邦政府對電子簽章增加使用爲帶動各州政府採用之主要動力，其中伊利諾州及華盛頓州於西元 2000 年即展開數位簽章計畫，爲創先使用的州。

2. 歐盟

(1) 丹麥

丹麥科學技術與創新部(Ministry of Science, Technology and Innovation)與丹麥電信公司 TDC 簽署爲期 4 年之服務合約，提供丹麥公民企業及公家部門基本電子簽章技術與服務；丹麥政府部門第一個提供電子簽章於其線上服務者爲海關與稅務管理部門(Customs and Tax Administration)。

(2) 芬蘭

芬蘭社會保險局勞工部及國家稅務局(the Social Insurances Institution of Finland, the ministry of labour, the National Board og Taxation)於西元 2003 年共同簽署將建立新電子化政府服務之線上身分驗證系統。原本芬蘭政府計畫使用電子 ID 卡形式作爲電子化政府服務身分驗證功能用途，但推廣進度並不如預期順利；新系統將提供不需要使用讀卡機的線上身分驗證功能，其安全條件足以提供使用者在線上進行較低敏感性的交易服務，其應用以政府與銀行往來監業

務爲優先施行範疇。

(3) 法國

法國政府於西元 2004 年成立電子行政發展局(Agency for the Development of Electronic Administration；ADAE)並提出兩項重要計畫-建立公共服務入口網站及智慧卡應用。電子行政發展局的建立被視爲法國推動電子化政府的重要措施；在智慧卡推動部分主要目的爲簡化法國公民使用政府服務流程。

(4) 英國

英國政府負責推動企業上網，且透過協調等手段規範和促進電子商務的機構(the Office of the E-envory)於西元 2003 年 7 月 31 日公佈「智慧卡政策方針(Smart Card Policy Framework)」文件草案，作爲公共門實施智慧卡應用的基本準則，主要爲協助推動電子化政府的落實。茲將其內涵簡述如下：

①以政府互通架構爲準則建立智慧卡標準，確保政府與產業的智慧卡能夠彼此相容。

②以整合與協調的方式於公部門推動智慧卡，並由「the Office of the E-envory」負責智慧卡最佳實作應用範例的分享與傳播工作。

③確保智慧卡的實施符合資料保護法或其他相關法案規範，以保障公民權益。

④政府單位需考量未來再智慧卡中加入電子簽章功能，以提供安全的電子化政府與電子商務服務。

3. 日本

日本電子簽章與憑證服務法對憑證服務業者任命有一規範，且說明憑證服務業者爲由總務省公共管理部（Ministry of Public Management, Home Affairs, Posts and Telecommunications，MPMHAPT）、經濟產業省（Economy, Trade and Industry，METI）及法務部（Ministry of Justice，MOJ）依其功能主責管理。除

此之外，西元 2000 年 4 月，15 家日本資訊領導大廠在法務部支持下，共同發表一份 B2B 電子商務憑證應用指導方針，加速公開金鑰基礎建設應用之推動。

日本目前主要公開金鑰基礎建設應用將從下列幾個方面來說明：

(1) 網路基礎建設服務：一般電腦資料中心(Internet data Center, IDC)業者皆有提供公開金鑰基礎建設服務。

(2) 金融服務：以 Identrus 銀行體系爲主，日本 4 家主要銀行均採 Identrus 憑證，但大多數銀行之線上系統並無導入公開金鑰基礎建設機制，而是放在 B2B 業務；另外電子錢包在日本亦不普遍。由於無法確保其投資報酬率，公開金鑰基礎建設於日本金融領域的應用面臨瓶頸。

(3) B2B 電子商務：過去私有之專屬網路之 B2B 網路，目前已逐漸轉換 XML[44]爲方式，公開金鑰基礎建設之使用亦隨之普及。

(4) 電子化政府服務：已有提供大量之應用，尤其以國家身分證智慧卡(National ID Smart Card)爲主要驅動之力量。此國民卡係一多用途卡片，可同時用於如網路購物、網路銀行等商業行爲，以及電子化政府各項服務。國民卡推動至今最大之推廣困難爲缺乏商業應用及付費配套措施。

(5) B2C 電子商務：如 DoCoMo 及 KDDI 皆規劃提供服務。

(6) 電子化醫療服務：主要由一家財團法人機構 OCHIS(Organization for Promoting community Healthcare Information Systems) 負責運作，以公開金鑰基礎建設及 XML 標準作爲醫院診所間之資料交換基礎。

(7) 企業內部公開金鑰基礎建設應用：依據日本「電子簽章法」(e-Signature Law)，日本憑證機構可自願性接受政府之認證並受取得認證標章。

---

[44] 西元 1968 年國際組織(International Standards Organization , ISO) 所公佈之名爲「標準通用標示語言」(Standard Generalized Markup Langange, SGML)的精簡版/子集合，同註 35，頁 110。

整體而言，日本公開金鑰基礎建設應用相當多元，除一般熟知的 4 個基本應用：身分鑑別、資料完整性、私密性及不可否認性外，尚有如日期及時間認證、屬性認證、數位內容認證、區域憑證、簽章文件長期保存等多樣化之應用。

4. 中國大陸

中國大陸對於電子交易在發展之初並無一國家制訂的法規主體，上海市政府率先成立第一家上海電子憑證機構，負責簽發數位憑證。隨後，廣東省電子交易條例於西元 2003 年 1 月正式施行，條文中規範憑證機構只可在獲得省資訊產業管理機構條件認可下，以及提交憑證業務經營管理標準與數位憑證管理系統作爲省資訊產業管理機構存檔記錄情況下，始可著手經營其憑證業務。上述之省資訊產業管理機構則每年對這些憑證機構進行稽核審查。

自西元 1999 年展開建設憑證機構熱潮，由於陷入：供過於求、市場預期過於樂觀、營運定位不清及商業模式尚未形成等因素，營利型憑證機構正面臨龐大風險之處境：諸如市場、政策、技術及資金等風險。

第一家於西元 1998 年成立至西元 2005 年 7 月已有超過 70 家憑證機構、累計共發出 500 萬張憑證，營運較佳的幾家主要係靠電子化政府相關計畫維運，例如網路報稅、社會福利系統、年度稽核及整合系統註冊費等。

自西元 2003 年 10 月開始規劃國家層級國家憑證機構架構，並將成立國家公開金鑰基礎建設協調管理委員會，作爲最上層之管理單位。後於西元 2004 年 8 月 28 日第十屆全國人民代表大會常務委員會第十一次會議通過「中華人民共和國電子簽名法」。

5. 香港

目前香港有 3 家憑證機構獲「香港電子交易條例」(Hong Kong electronic Transaction Ordinances；ETO)核准，其中有 2 家是政府單位，1 家爲民間公司。

爲擴大公開金鑰基礎建設的應用，香港特區政府(HKSAR)各單位正大力推

廣電子商務導入使用及機制，其中包括：

(1) 電子化政府之應用

如香港市民 IC 卡、通關申報、電子照顧系統、出入境申報、運輸物流、註冊及選舉以及國內稅收等。

(2) 電子商務之應用

如網路下注(eWin,HK Jockey Club)、線上證券交易(香港證交所)網路銀行服務、安全資料傳輸(證監會、金融管理局)等。

(3) 學界或民間自發性的從事相關研發及活動：

由資訊設備廠商、憑證機構業者、銀行及電信公司等組成之「香港 PKI Forum」目前有 30 個會員，正進行交互認證及憑證互通之討論。

6. 新加坡

由新加坡「資通訊發展部」(IDA)出資 51%股份及 NETS 公司出資 49%股份，於西元 1997 年合資成立之專業認證服務公司-「Netrust 公司」，係東南亞國家中第一家成立之憑證機構，並於 2001 年 6 月取得新加坡政府第一張憑證機構核可執照，是目前唯一取得執照之公司。

「Netrust」主要係提供政府機關企業及民眾一個完整之線上認證及安全架構之解決方案，涵蓋之業務範圍爲：

(1) 安全認證服務：核發主機端及客戶端憑證及網站憑證。

(2) 安全應用軟體：PC 安全軟體、E-Mail 安全軟體、遠端登入軟體、單一簽入軟體。

(3) 安全顧問服務：企業私有憑證機構之建置與代管、目錄服務、企業內部虛擬網路安裝、教育訓練、Entrust PKI 模組銷售。

(4) 安全解決方案：安全資料儲存、安全資料存取、安全檔案傳輸及安全入口網站等。

新加坡於西元 1998 年 7 月通過「電子交易法」(Electronic Transactions ACT) 西元 1999 年制定 CA 規範(Electronic Transactions(CA) Regulations)，IDA 爲主管機關，規範憑證機構設立條件如下：

(1) 財務

健全之財務狀況：資本額不少於新加坡幣 500 萬元。

專業之賠償金機制：投保金額不少於新加坡幣 100 萬元。

銀行保證或債券達新加坡幣 100 萬元。

(2) 營運

① 憑證實務作業基準(CPS)須經核准。

② 程序及處理須通過每年安全查核。

③ 所屬相關人員最近 10 年需無破產或犯罪紀錄。

④ 認證核准後核發憑證機構標章。

基本上，新加坡政府也認同公開金鑰基礎建設應用的重要關鍵在於應用案例的多寡，因此特別歸納出下列政府相關應用項目，作爲推動公開金鑰基礎建設及廣發電子憑證的手段：

(1) 公共政府服務卡：含身份識別門禁管制電子憑證等多用途。

(2) 網路採購系統(MINDEF & GeBiz)。

(3) 中央提存基金系統(Central Provident Fund, CPF)。

(4) 海關及查緝系統(Customs & Exercise Department)。

(5) 土地資訊及登錄查詢系統(INLIS)。

(6) 建築及營建資訊系統(CORENET e-Submission)。

(7) 電子住宿出租系統(STARS e-Lodgement System)。

(8) B2B Hub：含電子目錄、訂單處理、發票查詢、電子支付與應收帳款處理。

(9) 貿易財務系統：含信用狀及電匯等。

(10) 電子專利系統 e-Patent System。

(11) eNets 線上付款機制。

新加坡電子交易法由資訊通信發展機構（Info-communications Development Authority，IDA）負責管理與執行。在已制訂的電子交易法與電子交易（憑證機構）條例規範下，一項憑證機構自願性執照發放方案成立，此方案規定憑證機構執照發放的標準，以及後續經營條件之標準，包括財務狀況、營運政策與程序、記錄追蹤能力等均視爲可否成爲核可憑證機構的評量條件。

國際組織東協電子劃社群（e-ASEAN or ASEAN e-community）建議應由憑證機構自願性選擇是否成爲鑑定核可憑證機構，而非以強制性方式要求每一憑證機構均需通過評核成爲鑑定核可的憑證機構。如此的構想主要爲希望讓憑證機構在成熟的憑證市場環境下自由發展。在公開金鑰基礎建設架構下，憑證機構負責驗證公開金鑰和個人的私密金鑰，在憑證尚未成爲數位憑證格式前，憑證機構可以扮演個人實體的驗證中心，亦即進行面對面的驗證服務，實際驗證所發放的憑證可以用來證明個人的公開金鑰，以及其簽章是否屬實。新加坡的 Pte 公司爲第一家發放數位簽章金鑰的憑證機構；ID Safe Pte 公司則爲第二家憑證機構，但目前已停止營運。

7. 澳洲

澳洲對於憑證服務架構及業者並無制訂特定的法律規範，但澳洲聯邦政府的 Gatekeeper 計畫[45]則針對與政府業務相關的交易制訂公開金鑰技術的策略，任何與政府單位或由私部門提供政府單位進行相關驗證技術或加密技術等安全系統的使用，均於 Gatekeeper 計畫中做一策略性規範，用以支持澳洲各省管轄範圍的電子交易。

除了上述計畫，澳洲 ABN-DSC 政府計畫亦授予澳洲人民在進行每一筆商

[45] 澳洲政府 NOIE(the National Office fir Information Economy)所進行之專案計劃，結合公私部門，將 PKI 級數及應用落實於 e 政府及電子商務中。

業交易時，根據其澳洲商業序號（Australian Business Number，ABN）申請數位簽章憑證（Digital Signature Certificate，DSN）。這項 ABN-DSC 計畫將與每一筆交易契約內容作連結，用以驗證交易寄送人的數位簽章身份，任何一個單位或個體收到由 Gatekeeper 或 ABN-DSC 計畫提供的數位簽章技術均稱爲一個憑證機構。

澳洲在公開金鑰基礎建設的應用領域如下：

(1) 澳洲新版所得稅系統：爲全球最大之公開金鑰基礎建設應用系統，已核發 10 張營利事業所得稅申報之電子憑證，以及 50 萬張個人所得稅申報之電子憑證；其中 ANZ 銀行所簽發之 IDentrus 用途憑證已通過交互認證，可作爲報稅之用。

(2) 澳洲健康局(Health e-Signature Authority)：已發 4 千餘張電子憑證，供健康照顧專家使用，初期用於醫生對政府申報之報表或表單，新應用將擴及電子病歷及醫生對醫生之調閱病歷，目前面臨的挑戰乃在於如何整合現有之醫療軟體。

(3) 信用卡結合 IC 卡：以便使用於 ANZ 銀行之卡及美國運通銀行之 Blue 卡，內含 PKI 電子憑證，主要目的爲防止磁條卡被複製僞造、於網路上暴露卡號及密碼，將應用於無紙化交易。

澳洲政府之「Gatekeeper 計畫」已將評鑑工作委外給「專家資訊稽核公司」(IT AUDitor)執行，並與標準驗證團體合作監管各公開金鑰基礎建設及憑證機構業者。

8. 韓國

韓國於西元 1999 年正式通過並施行電子簽章法，以技術中立原則使之符合各種除了公開金鑰基礎建設以外的其他相關技術。

韓國目前之「國家根憑證中心」(National Root CA,又稱最高憑證中心)由其

「資訊安全局」(Koera Information Security Agency)負責核發憑證給下屬核可憑證機構並負責營運管理。同時透過國家根憑證中心可與國外憑證中心及國內政府之根憑證中心互通，其運作方式與我國之國家級憑證機構類似。

韓國電子簽章法明訂資訊及通信部（Minister of Information and Communication，MIC）爲憑證機構的主管機關，並交由韓國資訊安全局（Korea Information Security Agency，KISA）執行憑證機構的鑑定審核工作。韓國資訊及通信部制訂多項與電子憑證服務和鑑定核可憑證機構管理等指導方針，明訂出符合安全可信賴的憑證服務需求條件。爲有效監督核可憑證機構，韓國 KISA 定期進行憑證機構安全管理的檢查工作，並執行電子簽章和電子憑證技術發展工作，研究上述兩項及跨國互通等相關技術標準。

2.5 自憑證應用領域現況及發展趨勢探討公私領域應用現況所生之相關規範需求[46]

綜上可知，世界各國的公開金鑰基礎建設的發展皆然，有由政府所建置的公領域公開金鑰基礎建設憑證中心(PKI GCA)，亦有民間私領域所建置的公開金鑰基礎建設，我國亦同。理論上這兩個領域所發的憑證，是以一個共存共榮的方式存在著，而不以競爭作爲發展的考量，亦即政府須考量民間公開金鑰基礎建設存在之必要性，而留一些空間給民間業者發展；相對地，民間公開金鑰基礎建設業者須體認到由政府發出各種身分種類憑證，主要適用於電子化政府之相關應用。但如民間的應用系統要應用至公領域系統所發的憑證時，則政府的態度是不鼓勵也不反對，由市場自由決定。但就全球憑證機構的發展來看，亦呈現差異化現象：全球目前有許多大型的憑證機構領域，例如 VeriSign 在美國主導了網路伺服器憑證市場的視聽，也對一般大眾對公開金鑰基礎建設的認知產生很大的影響力；而歐洲則倡議公平的產業環境以鼓勵市場的充份競爭；

[46] 同註 38，頁 66 以下。

在亞洲公開金鑰基礎建設的推動則多爲公部門主導，並多屬於涉及全民或企業的國家型計畫。這種現象反應出在歐美地區憑證中心的存在多建立在信賴之上；而在亞洲地區憑證中心的存在則是有了公部門「權威」的介入(這或許是文化或民族性差異使然)，且此類憑證機構大多存在於大範圍的應用（例如電子化政府），而小範圍的特定應用較不普及；而在憑證應用進展中，似乎遺忘了將之應用在網域名稱系統（Domain Name System, DNS）這種大範圍的應用領域。

下表是民國 94 年網路報稅活動之分析，可看到應用憑證及戶號的方式，其中有原有政府憑證中心及發出的自然人憑證及由私領域憑證機構所發出之金融憑證兩大類，此正是表示個人綜合所得稅申報等典型的電子化政府應用，是允許私領域所發憑證作爲身分鑑別的憑證。

表 2-3：民國 94 年度網路報稅活動所用身分憑據類別統計表

	原有政府憑證中心	內政部自然人憑證	金融憑證	戶號	總計
件數	2,624	193,369	37,724	1,436,466	1,670,163
佔以憑證報稅之比率	1.1%	822.8%	16.1%	NA	NA

資料來源：中華電信 (2005/09)

然所需探討的是，民間所發的憑證，在電子化政府的相關領域應用時，則要如何規範呢？如有明確之規範可依循，則可讓私領域所發憑證應用於各個領域之電子化政府應用，如此不但可促進民間私領域憑證發展亦可降低政府施政之成本。簡言之，需進一步探討「如何規範政府應用系統使用民間憑證機構憑證機構所簽發憑證」，此問題分爲二個層次討論：其中一個是「規範政府應用系統使用民間憑證機構所簽發憑證的管理模式」，另一則是「應否制定政府應用系

統限定使用政府公開金鑰基礎建設的憑證中心(GPKI CA)[47]所發憑證之規範」，在此分別解析如下。

2.5.1 規範政府應用系統使用民間憑證機構所簽發憑證的管理模式

1. 依管理之強度有三個程度之管理：

(1) 高度管理，其內容爲：

① 強制許可制(特許制)，必須要通過驗證後方允許使用。

② 政府要制定嚴謹的流程辦法與技術規範。

③ 對應用系統使用民間憑證機構所簽發憑證進行實質審查，在通過審查後才允許上線。

④ 定實質的鼓勵措施，否則相關應用系統的配合意願會很低。

(2) 適度管理，其內容爲：

①自願認可制(認許制)，由政府資訊應用系統自行承諾按規範實作。

②由政府研擬「政府應用系統使用民間憑證機構所簽發憑證的檢核總表」，各應用系統以總檢核表向研考會(電子化應用系統的推行主管機關)提出申請。

③ 考會書面審查該申請，審查通過後系統始得上線。

④ 實質的鼓勵措施，讓應用系統有誘因自願參加認可。

(3) 低度管理，其內容爲：

① 報備制，各應用系統只要將應用民間憑證機構所發憑證，向主管機關報備即可。

---

[47] GPKI 是政府公開金鑰基礎建設「Government Public Key Infrastructure」之簡稱，我國之 GPKI 是一個階層式的憑證管理架構，以行政院研考會設置的政府憑證總管理中心(Government Root CA，GRCA)，做爲整個 GPKI 的信賴其點(Trust Anchor)，GRCA 將簽發 CA 憑證給 GPKI 的下層 CA。

② 政府研擬「政府應用系統使用民間憑證機構所簽發憑證的檢核總表」，並對各應用機關教育宣導。

③ 各應用系統自行使用檢核總表評估檢查。

④ 檢查後向主管機關提出報備，以便登錄管理。

2. 我國政府在民國 94 年公開金鑰基礎建設策略會議中之會議結論

(1) 同意開放政府資訊應用系統使用民間憑證機構所簽發的憑證。

(2) 以民間憑證機構安全等級或由政府應用系統自行決定所接受民間憑證機構憑證，而相關管理模式應參考電子簽章法修法方向。

而上述所指之電子簽章法修法方向，係指參照國際立法趨勢，對於對外提供認證服務的業者之許可條件，除依現行法之「書面審查」憑證實務作業基準外，尚須有公證第三者提交稽核報告之實質稽核，亦即均朝高度管理的方案發展。

2.5.2 應否制定政府應用系統限定使用政府公開金鑰基礎建設的憑證中心(GPKI CA)所發憑證之規範[48]

關於此部分，須就五大面向討論，分別探討如下：

1. 政府資訊應用系統資安等級需求

政府資訊應用系統資安等級，依照對國家及民生經濟的重要性，可以分成爲 A、B、C 及 D 四個安全等級。基於資訊安全是全面性的，故關於應考量在高安全等級的應用系統，須一致要求限定使用政府公開金鑰基礎建設的憑證中心所發出之憑證，而排除民間憑證機構所簽發憑證之使用，以使該資訊應用系統之資安防護，均可達到相同之等級。

2. 對於處理個人隱私資料的應用系統須符合高安全性需求

[48] 同註 38，頁 68 以下。

經查大部分民間憑證機構所簽發的自然人憑證中記載有身分證號全碼，當使用此類憑證用以進行例如報稅、保險及醫療之應用時，便有可能以身分證字號追蹤其所辦理之各項事務，而侵害到個人隱私。而有些民間憑證機構在審驗個人憑證的申請時，並無嚴謹的申請人身分識別與鑑別作業，而有可能遭他人假冒身分申請憑證。其次，在目前網路報稅如使用個人憑證，在簽章確認後取得之財稅資料，亦有可能遭人下載而外洩。而且民間憑證機構所簽發憑證之金鑰對的儲存媒體大多爲以軟體形式，雖具有可攜性高之優點，但缺點即是容易有私密金鑰外洩之情況發生。

由上可知，由於資訊應用系統所處理的個人隱私資料的等級需求高，故現定其應用系統僅得使用政府公開金鑰基礎建設的憑證中心所發出之憑證亦有其必要。

3. 憑證主體與憑證生命週期的同步要求程度之需求

有些政府資訊應用系統對於憑證主體(Certificate Subject)與憑證生命週期(Certificate Life Cycle)的同步要求程度較高，例如在公司執行業務方面，經濟部對於廢止公司憑證之要求，係於一家公司清算解散後才廢止該公司的憑證，經濟部工商憑證管理中心連線到工商資料庫，例如接收到一家公司已經解散之訊息時，經濟部工商憑證管理中心就會執行逕予廢止該公司憑證的作業。另外，又如自然人憑證主體改名或更改身分證字號時，原該用戶的身分便以失效，則經濟部工商憑證管理中心及內政部憑證管理中心也同步啓動相關憑證廢止作業，因此當憑證主體身分資料變更作業開始進行時，就可在很小的時間差下，完成憑證主體與憑證生命週期的同步變更，因而避免產生漏洞造成後遺症。

民間憑證機構則無如此同步之機制，目前各個民間憑證機構的憑證實務作業基準大都未規範其用戶應有主動報告其身分消失的義務。極有可能該憑證主體已消失，但是其相對的憑證卻仍然「逍遙法外」地仍爲該憑證機構有效的憑證。

因此，因某些政府資訊應用系統對憑證主體與憑證生命週期須同步之高度要求，故只可以使用政府公開金鑰基礎建設的憑證中心所簽發的憑證。

4. 公權力與公文書的需求

憑證在網路世界中，被推定爲具有現實世界的電子身分證與印鑑證明的效用，這兩個證明在現實生活中都是由政府機關簽發，政府的資訊應用系統，非屬政府與私人機構間(G2B)或是政府與人民間(G2C)，而係屬於公領域的事務，故應當以政府所發的憑證作爲電子身分及印鑑證明，尤其在一些政府與民間涉及重大權利及義務的應用上，就要特別的注意要能使用政府公開金鑰基礎建設的憑證中心所發的憑證。

民間憑證機構所簽發憑證，對外做身分認證服務已經通過審驗與核定，而其核定者就是電子簽章法的主管機關經濟部，但民間憑證機構簽發的憑證是否有符合政府機關公文書的要求，或就是被視爲準公文書，在慣例上，並沒有民間機構所的證明書可以被看成是公文書。

因此如果政府的某些應用系統，只適於公文書者，就必須限制使用政府公開金鑰基礎建設的憑證中心所發的憑證了。

5. 基於政府對民間的責任及賠償的需求

我國目前使用的憑證的應用系統使用者及一般大眾的認知上，常會將應用系統的使用與賠償責任問題，歸責到憑證機構，不會知道大部分是因應用系統的使用憑證金鑰對或作業流程不妥善所致，憑證機構主要是對身分認證的保證而已。主管機關目前也沒有餘裕可以制定通則或規定，以釐清兩者之間的責任，故一旦發生因爲使用憑證而產生糾紛時，目前沒有規範可作參考。

目前應用系統是政府的，而憑證是民間憑證機構所簽發的，如果真有糾紛時，首要解決的是，到底憑證機構與政府各要負多少責任，如前所述，目前並

沒有相關規範可作參考；次要解決的問題是政府如果要負損害賠償責任，有國家賠償法，民間憑證機構則可以依消費者保護法、公司法等既有私法規範處理，兩者之間有很大的差異，而要調和兩者，以達成一致的賠償原則，將是一個大工程。因此若要簡化資訊應用系統及憑證機構兩者對於賠償的歧異，鼓勵政府資訊應用系統使用政府公開金鑰基礎建設的憑證中心所簽發出的憑證爲最簡單解決之道，故當涉及民間個人或組織有著重大權益關係時，即限定只能使用政府公開金鑰基礎建設的憑證中心所簽發的憑證。

2.5.3 我國政府所採取之立場

針對「應否制定政府應用系統限定使用政府公開金鑰基礎建設的憑證中心所發憑證之規範」的議題，我國政府在 94 年公開金鑰基礎建設策略會議之 GPKI 的策略會議上，並未進行充分的討論，最後主席裁決，不訂定政府應用系統限定使用政府公開金鑰基礎建設的憑證中心所發憑證之規範。亦即以後政府的各資訊應用系統，不論應用系統對於民間權益的影響有多重大，都不考慮上列的五個因素，而採取全面不分等級，一律開放可以信賴及使用民間憑證機構所簽發的憑證。

2.6 小結

由上述可知我國目前公私領域之憑證機構發展趨勢大致與亞洲各國相同，係採公私領域之憑證機構並行方式，由公領域擔任領頭之角色，率先積極投入發展，然而發展至今，由於國家憑證機構與民間憑證機構法律責任之不同，雖然政府刻意採開放之態度，民間憑證機構發展還是受到限制，且已有逐漸萎縮[49]之現象，在此提出國家憑證機構法律責任之優勢及民間憑證機構業者之發展困境[50]，作爲本章

[49] 截至民國 96 年 6 月，國內憑證機構現況：網際威信將憑證業務併入台灣網路認證；而是方電訊則將憑證中心交由新成立之台網國際承接。

[50] 蔡朝安律師、朱瑞陽律師合著「公司法修正對公司電子登記業務之影響」 http://www.pki.org.tw/Resource/Article/Article_020411_4.asp，2007/7/30 visited。

之結論：

2.6.1　國家憑證機構之法律責任

1. 國家賠償責任與憑證機構經營責任之競合

不論是由主管公司登記業務之機關即經濟部還是由政府憑證管理中心（GCA）簽發之電子憑證，因均具有公法人或機關之地位，即屬國家憑證機構。同時憑證機構簽發之電子憑證係基於公司法及電子簽章法之授權而來，因此其負責登記之人員，如果違法執行職務時，即有國家賠償法之適用，信賴登記資訊之人，自可向國家請求賠償（依國家賠償法第 2 條）；此外，電子簽章法第 14 條亦明定憑證機構就其經營或提供認證服務之相關作業程序，致當事人受有損害，或致善意第三人因其信賴該憑證而受有損害者，應負賠償責任。那麼當國家憑證機構於檢附憑證實務作業基準予經濟部後，取得經營許可，對外提供服務時，亦負有相關之賠償責任。

因此，國家憑證機構就提供電子憑證服務之憑證機構及其登記作業人員，依法即擔負國家賠償責任及憑證機構經營賠償責任，而呈現責任競合之關係。不過，於憑證機構發生賠償事由時，是否兼有國家賠償責任與憑證機構經營責任，仍須視實際個案決定，尚不可一概而論。當然，就政府憑證機構及其登記查核人員是否適用國家賠償法乃至公司登記查核之作業人員是否爲依法執行公權力？亦須視是否爲「委託行政」[51]而定，但可以確定的是，國家憑證機構對其所經營或提供認證服務是必須擔負賠償責任。。

2. 登記機關之法律責任

關於憑證機構之另一應注意之問題，即爲前述註冊中心（Register Authority, RA）[52]法律責任。在經濟部擔任憑證機構簽發公司電子憑證時，如公司爲資本

---

[51] 參照《行政程序法》第 16 條第 1 項之規定：「行政機關得依法規將其權限之一部分，委託民間團體或個人辦理。」

[52] 註冊管理系統負責受理憑證申請、中止、廢止與相關資料審核，並將審核通過之資料傳送至憑

額新台幣一億元以上者，因屬中央即經濟部管轄，因此，經濟部同時肩負登記主管機關及憑證機構之地位，其如有賠償責任，經濟部應負賠償之責，當無疑義。有爭議者爲，在公司爲資本額一億元以下，其登記主管機關爲直轄市公法人時，因登記機關之疏失，作爲憑證機構之經濟部是否應負賠償責任？

就此問題，因憑證機構爲簽發電子憑證之主體，其作業程序如有疏失，不論登記機關爲何，表現之憑證機構既爲經濟部，當負賠償責任。且從公司電子憑證之信賴性基礎在於嚴格之身分認證程序，其因登記機關之疏失所致認證錯誤，憑證機構要難執爲免除賠償之事由，如以民法第 224 條之履行輔助人[53]及行政程序法第 15 條之行政委託[54]作爲法源基礎，則登記機關可以是居於履行輔助人或因上級機關之行政委託之地位，履行登記查核義務，其相關權義之歸屬，自應由憑證機構之經濟部負責。

另一個延伸的問題爲，登記機關是否應與核發憑證機關負連帶賠償責任？如從電子簽章法第 2 條第 5 款中對憑證機構之定義係指「簽發憑證之機關、法人」，則實際上負責驗證簽章資料之人雖爲直轄市公法人，其因作業疏失致發生賠償責任時，依文義解釋，登記機關尚非簽發憑證之法人，則登記機關就其作業疏失之對外法律責任，仍不須依電子簽章法第 14 條負有賠償責任，至於登記機關與憑證機構之內部責任分擔，則宜透過行政責任或契約方式分配之。

證管理中心，進行憑證簽發、廢止等作業。本憑證管理中心之註冊管理系統在實體架構上分爲前端註冊管理系統及註冊管理主系統兩部份。前端註冊管理系統負責現場受理申請人之申請、書面資料審核及身份認定等作業。前端註冊管理系統須能驗證憑證申請者本人及其書面證明資料之正確性，或具備公正的用戶資料庫得以驗證憑證申請者本人身份。註冊管理主系統負責與憑證管理系統連線之進行憑證簽發、廢止等作業。

[53] 參照《民法》第 224 條之規定：「債務人之代理人或使用人，關於債之履行有故意或過失時，債務人應與自己之故意或過失負同一責任。但當事人另有訂定者，不在此限。」

[54] 參照《行政程序法》第 15 條第 1 項之規定：「行政機關得依法規將其權限之一部分，委任所屬下級機關執行之。行政機關因業務上之需要，得依法規將其權限之一部分，委託不相隸屬之行政機關執行之。」

2.6.2 民間憑證機構所面臨之困境與因應之道

1. 政府憑證機構所具有之優勢地位

法律上「人」的概念分爲兩種，即自然人與法人。法人又分爲營利及公益之社團法人及公益財團法人，其中，扮演社會活動之要角者當爲公司法人。當經濟部及內政部決定自行設置憑證機構簽發公司電子憑證及自然人、財團法人及公益社團法人之電子憑證時，可以說全國人民均將取得政府機關所簽發之電子憑證。確實達到「人人有憑證之政策目標」。而且純就憑證機構證明身分及資格真實性而論，有任何一個民間憑證機構會比政府所設置之憑證機構具有更強大公信力與信賴性基礎嗎？

在此以經濟部所設置之憑證機構爲例，說明政府憑證機構所具有之優勢地位：

(1) 強大之公信力

由政府所設置之憑證機構，因政府機關及公務員之責任體系所塑造出之國家高權及公信之形象，將使其所簽發之公司電子憑證具有強大之公信力。

(2) 對抗效力

在公司登記事項中，除了設立登記是公司之生效要件外，有應登記之事項而不登記，或已登記之事項有變更而不爲變更之登記，如公司代表人之變更，未經登記，是不得對抗任何第三人。

(3) 專業審查

登記申請之際，申請人除了爲證明登記事項內容之真實性而有義務提出相關文件之外，並有專業之國家公務員，審查登記事項，確保其正確性。

(4) 行政罰責

登記事項變更時，除要求特定人有申請變更登記之義務，對於虛僞不實之申請者或應登記事項而不爲登記之情形，並有相關罰則處罰（如公司第 9 條）。

(5) 國家賠償責任

登記人員如爲違法執行職務時，因有國家賠償法之適用，信賴登記資訊之人，自可向國家請求賠償。

(6) 充足之無限賠償額擔保

政府所設置之憑證機構如有面對任何賠償責任時，將有國庫作爲無限額賠償擔保。

1. 因應之道—電子化政府之憑證政策應由營運憑證機構之思維轉以憑證管理之角度規劃

在一般民眾不論自然人與法人均以取得政府憑證機構所簽發之電子憑證爲優先考量規劃前提下，令人不得不思考民間憑證機構之未來市場究應著眼於何處？

當國家憑證機構所簽發之電子憑證比民間憑證機構所簽發之電子憑證更具有公信力基礎，且有較好之責任基礎架構下，基於什麼樣的原因能夠說服消費者選擇使用民間憑證業者所簽發之電子憑證？

雖然會有論者主張政府憑證機構所簽發之電子憑證僅能適用於公行政體系，不得適用於商務運作體系，且配合電子簽章法第 14 條第 2 項之規定，憑證機構就憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，不負賠償責任，以此作爲不得將公行政體系之電子憑證應用於商務使用之手段。然而如仔細審視電子憑證之功能與作用，不過是證明網路交易當事人一方之身分真實性，且當政府機關都願意甘冒負擔極大之行政責任、簽發電子憑證用以證明交易一方之身分真實性時，憑證機構負不負賠償責任，早已不是雙方交易之核心，而且究竟憑證機構之賠償責任是否得以無限擴張，是一個值得深思之疑問。

在這樣的思考下，不得不思考民間憑證機構的未來在哪裡？是成爲政府憑證機構之委外營運管理者，還是有機會讓民間憑證機構成爲電子商務之基礎產業？

就此問題，學者看法如下[55]：

(1) 政府設置憑證機構之缺點

如上所述，經濟部及內政部等各部會均將設置憑證機構發放電子憑證，而現行之規劃方式，將致政府憑證機構與民間憑證機構處於功能重疊及資源未能有效利用之缺憾，蓋因電子憑證原只是證明電子簽章使用者之身分真實性。此項功能，事實上民間憑證機構均能稱職扮演，且從政府之應用層面來說，並無各部會均應設置憑證機構之必然性，各部會設置憑證機構無異是疊床架屋，不但增加政府爲維護營運憑證機構所需之預算成本，更無法有效帶動民間憑證機構之市場活絡，也未能達到經濟規模效益，更增加不同憑證機構之管理難度。加上電子簽章法之立法原則強調由民間主導，則政府自行設置營運管理憑證機構是否徹守此一原則，似值得考慮再三。直言之，現行政府電子憑證架構實未能有效促使電子憑證擴大應用層面。

(2) 因應之道 — 電子化政府之憑證政策應由營運憑證機構之思維轉以憑證管理之角度規劃

如以創造電子簽章需求市場之觀點爲基礎，若能將設置於各個部會之憑證機構或政府憑證中心之維至於落實於實際上營運之管理方面，將營運管理之預算成本，轉以「憑證管理」之角度規劃，即可因不須設置憑證機構，達到節省政府大量預算、進而促使民間憑證機構藉由大量核發電子憑證，提升服務品質，並且真正落實由民間主導之立法原則。如此，各部會將不須設置憑證機構並無須負擔憑證簽發與管理風險，讓政府除得節省大量之預算需求外，並降低政府潛藏之賠償風險值，更讓民間憑證機構得就憑證服務之提供有相互競爭之條件，以此建立多元性之電子憑證服務供應源，並刺激電子憑證市場迅速成熟。

[55] 同註 50。

三、憑證機構於電子簽章及交易法制之法律問題

網路交易之雙方，需要網路上之身分證明，以便確認對方之身分，故要有一個公正的認證中心，提供身份證明的服務，此機構負責核發電子憑證，以建立買賣雙方對於網路交易之信任基礎。從前章公開金鑰基礎建設架構與運作模式即可得知，憑證註冊者、信賴憑證效力之交易相對人(憑證信賴者)及憑證機構正是 PKI 架構中最重要之三個主體。而憑證機構之設計之目的，實爲網路交易匿名性之補強制度，爲避免因未面對面交易而可能產生之誤會及詐欺行爲，期待藉由憑證機構作爲公正第三人來確保交易雙方之存在與正確，以維持網路交易秩序最基本之穩定與安全之需求。

由此可見，網路法制基礎在於電子簽章法制，而電子簽章法制之基礎則在於交易主體之定位及規範。因此，本章之重點，在於討論憑證機構之法律地位及所簽發憑證之效力、與交易主體間及其他相關權利義務關係與爭議之處理、憑證機構之設立、管理與廢止、以及憑證機構之責任等憑證機構於電子簽章及交易法制所生之法律問題。

3.1 憑證機構之法律定位[56]

3.1.1 公正第三人

從前面說明可知，網路交易安全須仰賴數位簽章技術，而數位簽章技術中加、解密技術需搭配公開金鑰基礎建設(PKI)，藉由憑證機構作爲橋樑，方能使網路上電子交易相對人信賴電子訊息發送人之身分，並進而確認該電子訊息內容之完整性，亦即藉由憑證機構建立網路交易安全及安定機制。

因此，憑證機構係居於公正第三人之地位，並製作簽章用的公、私鑰，並提供電子文件存證、公證及時戳的服務。私鑰就好比是私人的印鑑，公鑰則好比是印鑑證明，簽署者(憑證註冊者)利用私鑰在電子文件上簽章，產生的電子

[56] 同註 21，頁 57 以下。

文件稱爲簽體，收到簽體的一方(交易相對人、憑證信賴者)則可以向憑證機構申請簽署者之公鑰，以驗證簽體之真僞。在此狀況下，憑證機構之資訊安全性及專業能力必須達到一定的基準，才能對外提供服務。

然須特別說明清楚的是：憑證機構對於無法擔保電子訊息內容的真實性，憑證機構所負之法律責任僅限於確保電子訊息之完整性。詳言之，憑證機構之法律責任在於核發電子憑證予已提供相關身分資料憑證註冊者，在憑證註冊者以約定之方式，使用憑證機構所提供之加、解密技術發送電子文件時，讓電子文件收受者得向憑證機構驗證該電子憑證之真實性，並確保該電子文件之完整性。至於憑證註冊者所提供之身分資料及電子文件內容是否正確，則屬於憑證註冊者本身應擔負之法律責任，而非憑證機構所須負擔之責任範圍。

3.1.2 公證人

1. 公證人之法律定位

公證制度，係由法院公證人或民間公證人，就人民之法律行爲或私權事實，依其請求作成公證書。簡單來說，公證制度就是透過國家公權力，來幫助一般民眾保存證據，或保障私權預防糾紛。現代公證制度具有保全證據、預防糾紛及疏減訟源的功能；因爲藉由公證行爲，交易雙方事後不能否認公證書之真正性，亦不能否認交易內容之存在性與真實性，故可以避免一些無謂的爭執與糾紛；即使日後產生糾紛，亦可減省舉證之困難。而公證人依其職務，就其聽取的陳述與所見的狀況，及其他實際體驗之方法與結果，所作成的文書稱爲「公證文書」。經公證人做成之公證書具有實質之證據力。

2. 憑證機構於電子交易中扮演類似實體交易中的公證人角色

在網路世界電子交易的雙方未曾謀面的情況下，無法確認彼此的身分，且亦因電子文件無法公證保存。故在公開金鑰基礎建設的架構中，設計憑證機構亦扮演著類似實體交易中的公證人角色，讓電子交易的當事人無法去否認該次

交易之存在及內容之真實性。亦即藉由憑證機構此一值得信賴之第三人，分別確認交易當事人之身分，並藉由電子簽章技術之不可否認性，保持電子文件從發送到收受之完整性，展現與實體公證制度相同之功能，讓網路世界電子交易與實體世界傳統交易一樣安全可靠。

3. 公證人與憑證機構法律地位之差異

公證人，由於公證法之明確就於其資格[57]、及其關於公證[58]與認證[59]之法律效力加以規範。只要符合公證法之規定，法律即賦予經公證人所做成之公證書一定之法律效力[60]。

惟觀諸現行電子簽章法，並未有如公證法之法制規模來規範憑證機構之法律地位、設立資格及所簽發電子憑證之法律上效力；質言之，當事人之電子文件及數位簽章，如經憑證機構之認證服務者，現行電子簽章法即賦予其取得等同於書面文件及親自簽章之法律效力；憑證機構地位極爲重要，卻無一定規模的條款來規範憑證機構，此情形會隨著電子交易規模之日益增長，使得憑證機構的地位日趨重要而益顯現行規範不足之窘境。

3.1.3 戶政機關

1. 憑證機構所提供之認證服務如同戶政機關所核發之印鑑證明

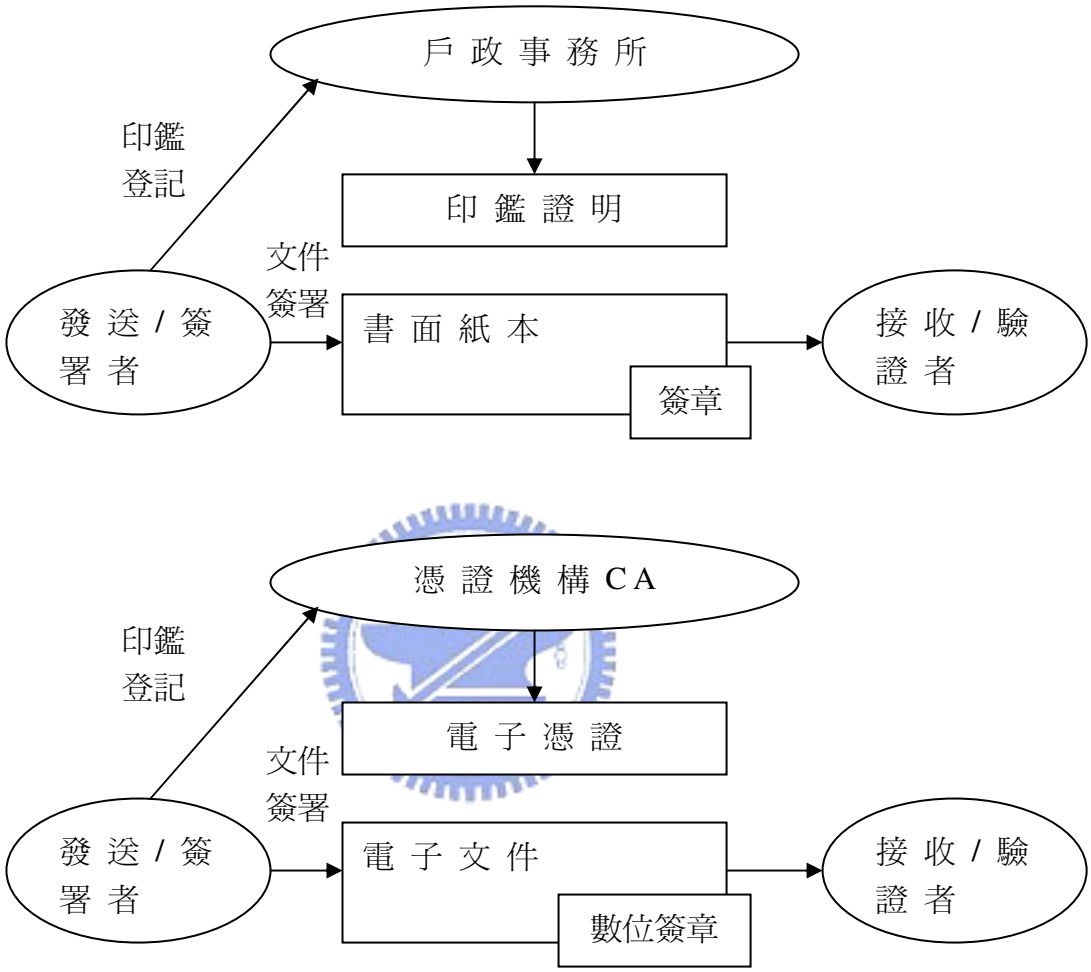
自然人於實體世界交易所需之身分及印鑑證明，依我國戶籍法之規定係由戶政機關[61]所核發，藉由公務機關公權力之行使，確認當事人之身分。而網路交易之身分確認，則是藉由憑證機構所提供之電子憑證，作爲雙方交易信賴之基礎。從此角度而言，憑證機構所提供之認證服務如同戶政機關所核發之印鑑

[57] 我國《公證法》第二章：關於公證人資格之規定。
[58] 我國《公證法》第三章：關於公證之規定。
[59] 我國《公證法》第四章：關於認證之規定。
[60] 我國《公證法》第 11 條及 13 條係有關於公證文書之生效要件及得請求逕受強制執行之規定。
[61] 我國《戶籍法》第 2 條之規定：「戶籍行政之主管機關：在中央爲內政部；在直轄市爲直轄市政府；在縣(市爲縣 (市) 政府。

證明。

茲將二者運作模式比較如下圖：

圖 3-1：戶政機關與憑證機構認證比較圖[62]



2. 戶政機關與憑證機構法律地位之差異

人民向戶政機關申請印鑑證明，其法律性質是屬於公法關係，只要人民依法申請，戶政機關即有核發之義務；而戶政機關核發印鑑證明係屬行政機關單

[62] 李科逸著，「電子簽章法重要法律議題之探討及初議」，2000 年全國科技法律研討會論文集，交通大學，新竹，頁 745。

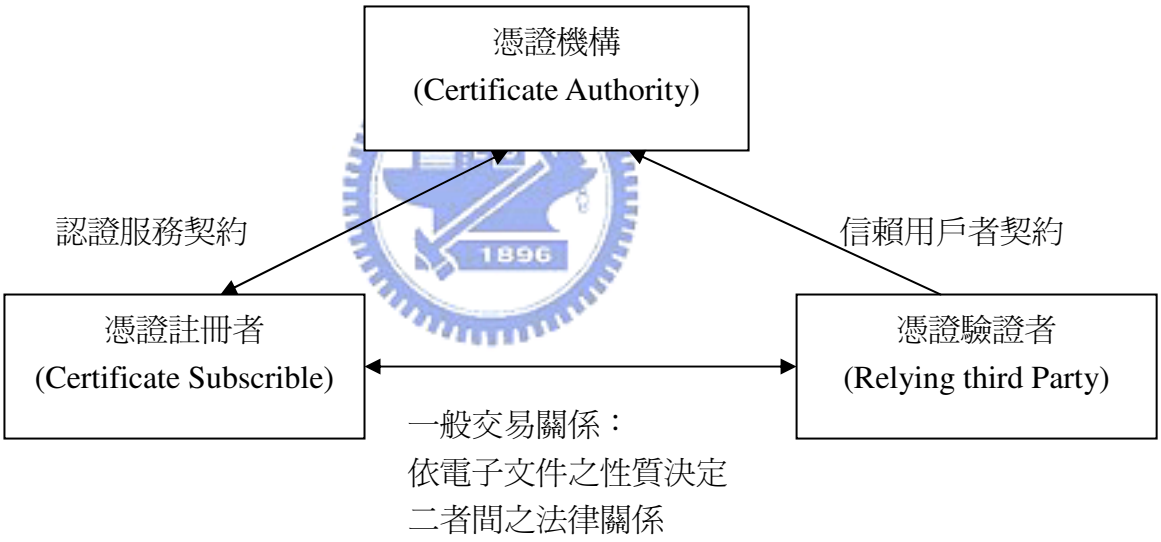
方行政行爲之作成[63]，故申請人與戶政機關之間並無合意增刪修改其內容之權力，且如有爭執應循行政救濟途徑解決。

但憑證機構簽發電子憑證之行爲則屬於私法之範疇，原則上並不屬於公法之性質而適用契約自由原則，當事人可視需求與憑證機構約定電子憑證之內容及效力。

3.2 憑證機構與交易主體(憑證註冊者及憑證驗證者)間之法律關係

憑證機構與交易主體(憑證註冊者及憑證驗證者)間之法律關係由下圖即可清楚了解：

圖 3-2：憑證機構與憑證註冊者及憑證驗證者間之法律關係



憑證機構與交易主體(憑證註冊者及憑證驗證者)間爲三方關係，分別是憑證機構與憑證註冊者間之「認證服務契約」關係、憑證機構與憑證驗證者間之「信賴用戶者契約」關係、及憑證註冊者與憑證驗證者間之「一般交易」關係，茲一一分析如下：

---

[63] 依《行政程序法》第 92 條第 1 項之規定：「本法所稱行政處分，係指行政機關就公法上具體事件所爲之決定或其他公權力措施而對外直接發生法律效果之單方行政行爲。」戶政機關核發印鑑證明應屬行政處分，故其救濟程序應可循行政救濟途徑解決。

3.2.1 憑證機構與憑證驗證者間之法律關係－認證服務契約關係

憑證機構與憑證註冊者間之法律關係，係三方關係之肇始，在信任電子簽章之基礎上，由於憑證註冊者申請憑證之行爲，才有因信任對方存在而加以驗證產生法律關係，進而才衍生憑證驗證者因信賴電子憑證，於受有損害時而向憑證機構求償之法律關係，故爲此三方關係中最基礎之法律關係。

1. 認證服務契約之主體

透過公開金鑰基礎建設爲基礎的數位簽章架構，當中認證服務憑證之設計，其目的是要彌補網路交易匿名性所做出的補強制度，期待由公正第三者來確保交易雙方之存在與正確，避免因爲欠缺面對面交易而產生不必要之誤會及詐欺行爲，以維持網路交易秩序之穩定與安全。因此，若不能確認交易主體，便不能將網路交易之法律關係清楚地規範與說明。由圖 3-2 可知，認證服務憑證主體主要有三：分別是憑證機構、憑證用戶及信賴憑證者，其中前者的身分依簽章法第二條一定爲機關或法人；而後二者之主體需爲權利主體，即簽章當事人應爲自然人或法人。

2. 認證服務契約之訂立

所謂契約之訂立，是指當事人雙方依照要約和承諾的程序達成合意的行爲和過程。認證服務契約之訂定亦不例外，在此分別討論之。

(1) 認證服務契約中的要約

在認證服務契約的訂立過程中，要約通常是由用戶因交易需求所發出的，憑證機構則是承諾方。一般認證服務契約的訂立過程，若是臨櫃申請之情形，憑證申請者到憑證機構的註冊中心提交一份內容完整並附帶個人簽名的申請書，而該申請書通常係從憑證機構的網站下載，亦可以於註冊中心、原受理申請處或其他受理申請處領取，申請書附件一般包括憑證用戶合約，若爲隨附申

請表格背面之憑證用戶合約則該憑證用戶合約爲憑證機構一方事前擬定之定型化契約條款。至於身分識別程序中個人身分之驗證，可能會要求提供身分證明文件，例如：附有照片的身分證 、護照或學生證等以確認申請人身分；對於企業或機關等法人，可能會要求提供該法人、機關的授權委託書、官方或有關部門的註冊、證明及登記文件，和申請者本人的身分證明文件及憑證機構可能需要的其他文件。

(2) 認證服務契約中的承諾

承諾是受要約人接受要約的意思表示。認證服務契約訂立過程中的承諾即係憑證機構對憑證申請的許可。在作出許可承諾的過程中，憑證機構應完成身分識別和鑑別之程序。例如：在臨櫃申請個人憑證的情形下，註冊中心要判斷申請者的身分證明文件是否有效、確認申請人身分及憑證內容資料之正確性與影本內容之同一性；若是法人或機關申請憑證的情形，註冊中心先要識別申請代理人的身分，過程與上面所述個人憑證申請人的識別和鑑別之程序判斷相同；同時，註冊中心要判斷授權委託書、法人註冊證明或登記文件及法人登記證等真實性，以及這些文件的複印文件與原件內容的同一性。如果經過識別正確無誤，上述個人或法人的身分屬實，則憑證機構通常就會許可用戶對憑證的申請，亦即作出承諾，其方式是在憑證申請表簽署同意申請，此時認證服務契約即告成立。如果上述個人或法人的身分不屬實，則憑證機構可能就無法同意憑證的申請，即爲拒絕要約，認證服務契約就不成立。

(3) 認證服務契約之屬性[64]

① 認證服務契約爲服務供應之契約

自表面觀之，憑證機構提供認證服務，係因申請人付費向憑證機構申請而

[64] 工研院電通所，「認證服務契約研究」，我國 PKI 互通管理及推動計畫、PKI 法律及政策研究報告，92 年 2 月，http://www.e-studio.com.tw/downloads/learn/20050202-06.pdf，2007/07/30 visited。

憑證機構簽發憑證，似爲財產權移轉契約；然就認證服務之內涵，實則憑證機構提供者並非憑證之簽發而是「身分之認證服務」，因憑證機構不僅負有提供憑證簽發之義務，且在特定條件下尚有暫時停用及廢止憑證之義務。故就後者暫時停用及廢止憑證之義務而言，認證服務契約並無法以財產移轉契約之概念涵蓋，應屬於契約雙方約定由當事人一方提供服務予另一方之服務契約。

② 認證服務契約屬要式契約

一般契約如以是否以一定方式履行，可區分爲要式及不要式契約：

(i) 要式契約：係指契約之成立，除當事人雙方意思表示合致外，須作成一定之書面，方可成立或生效之契約[65]，最典型者爲不動產物權契約[66]。

(ii) 不要式契約：係指當事人雙方意思表示合致，契約即成立或生效，一般大部分的契約均屬之。

認證服務契約屬要式或不要式契約，自不同角度觀察或有不同之認定。如從認證服務契約的訂立過程中，憑證的申請人往往須提交一份內容完整的附個人簽名的申請書，而該申請書的格式和項目都是由憑證機構預先擬定，該憑證機構在完成對申請者進行身分識別和鑑別程序後，並同意其申請時，認證服務契約即告成立。因此，在通常情況而言，認證服務契約若要求採用憑證申請書爲申請之形式，無論其要求以書面文件或電子文件爲之，其須採取一定形式，才能夠成立生效，而認證服務契約應被認爲係要式契約。然或若認爲認證服務契約爲申請人所提出之要約，憑證機構須就其擬定之申請程序確認當事人所提供的資料是否真實，始同意（作出承諾），而雙方意思表示才算合致，或者由憑證機構逕行簽發憑證，申請人不一定須完備申請程序，而認爲認證服務契約爲

[65] 如未具備一定方式，究屬契約不成立或無效之問題，因在實際運作上，無論契約不成立或無效，當事人均無需履行，故在此不做進一步學理討論。

[66] 我國《民法》第 760 條之規定：「不動產物權之移轉或設定，應以書面爲之。」

不要式契約者。

依我國立法原則，契約以不要式爲原則，要式爲例外[67]，如相關法律未規範者，就現行法制而言，認證服務契約應屬不要式契約。惟本論文認爲，就實務運作而言，基於證明需求以便於有爭議時釐清責任歸屬，宜採要式契約爲佳。

③ 認證服務契約屬雙務契約

契約之分類若以其作用區分 ，可分爲雙方負擔契約與一方負擔契約。雙方負擔契約係指當事人雙方互負義務之契約。例如買賣、僱傭等。其中又可分爲：

(i) 雙務契約：即當事人雙方互負居於給付與對待給付關係之契約。

(ii) 不完全雙務契約：即當事人雙方雖各負有債務，但其債務並不居於給付與對待給付之關係。

(iii) 一方負擔契約：係指僅一方當事人負擔給付義務之契約，例如贈與、保證等。

而在認證服務契約中，憑證機構的義務基本上就是提供憑證認證服務，亦即憑證用戶得請求之權利；而憑證用戶的義務基本上就是支付費用，亦即是憑證機構得請求之權利，雙方互付對待給付義務，因此認證服務契約應屬雙務契約。

④ 認證服務契約屬有償契約

若契約以有無對價給付區分，可分有償契約與無償契約。有償契約，即當事人雙方各因給付而取得對待給付之契約，例如：承攬 、互易等。而無償契約，即當事人一方只爲給付而未取得對待給付者，例如：贈與、使用借貸等。有償契約是指當事人之間互爲對價給付的契約。

在認證服務契約中，憑證用戶繳納費用獲取憑證和認證服務，而憑證機構

[67] 王澤鑑，「債法原理」，三民書局，台北，2006 年 9 月再刷，頁 127。

則收取費用然後簽發憑證並提供認證服務，因此認證服務契約應屬有償契約。

⑤ 認證服務契約屬混合契約

契約以有無名稱區分，可區分爲有名契約與無名契約。有名契約又稱爲典型契約，係指民法債篇各論中有標明名稱之契約，如買賣、租賃等等，而民事特別法中有規定者，亦屬之。無名契約又稱爲非典型契約，係指法律未特別規定而賦予一定名稱之契約，一般最常見爲因應商業交易需要，企業常創設所謂定型化契約條款者,其意乃爲由一方當事人爲與多數人訂約而事先擬定而 由相對人決定是否接受之契約條款，通常多以書面爲之，但概念上並不以此爲必要。

無名契約又分爲：

(i) 純無名契約：係指以法律全無規定之事項爲內容，即其內容不符任合有名契約要件之契約。

(ii) 混合契約：係指由數個典型（或非典型）契約之部分而構成之契約。

憑證機構所提供之電子認證服務內容並無法以單一有名契約之規範所涵蓋，而其性質上兼有承攬契約及委任契約之性質[68]，故應認爲認證服務契約屬混合契約。

⑥ 認證服務契約屬繼續性契約

若契約以債之內容是否可因一次給付而實現區分，可分爲一時與繼續性契約。

(i) 一時性契約：係指債之內容，因一次給付即可實現之契約，例如買賣、贈與等。

[68] 同註 21，頁 40。

(ii) 繼續性契約：係指債之內容，非一次給付即可完結，而是需持續一段時間方可實現之契約，例如：租賃、合夥等。

憑證機構對憑證用戶之服務有其繼續性，其必須於一定期限內持續提供認證服務（包括提供憑證廢止等服務 ）及扮演具公信力的角色，而非僅單純簽發憑證（一次給付）者，因此認證服務契約之性質屬繼續性契約無庸置疑。

⑦ 認證契約屬定型化契約

認證服務契約，一般多由憑證機構事前擬定之制式合約，故屬定型化契約條款，除應遵守電子簽章法之相關規定外，亦不得違反相關法律關於定型化契約相關規定。另外，憑證用戶通常是以消費或理財爲目的，接受憑證機構所提供之認證服務；因此，消費者與憑證機構間具有消費關係，而有消費者保護法之適用。

依消費者保護法第 2 條第 7 項規定 ：「定型化契約：指企業經營者爲與不特定多數人訂立契約之用而單方預先擬定之契約條款」等語。憑證機構因應交易需要，避免締約時要與個別憑證用戶磋商，與不特定多數憑證用戶訂立契約之契約條款，通常爲憑證機構單方事前擬定之制式契約條款，應屬一般契約條款。依消費者保護法施行細則第 10 條第 1 項之規定：「本法所稱一般條款，指企業經營者爲與不特定多數人訂立契約之用，而單方預先擬定之契約條款」。一般條款之內容，由於未經當事人間具體之磋商與合意，因而必須於具備一定要件，始可拘束當事人，憑證機構與用戶間之定型化契約條款若要發生拘束力則憑證機構必須對憑證用戶明白提示該一般條款，提供憑證用戶合理之機會了解條款內容、以及憑證用戶同意使用該條款，同時該條款必須非異常條款。若違反規定，則該條款不構成契約之內容。

無例外地，憑證機構與用戶之定型化契約條款之實質內容也必須符合相關規定；而定型化契約一般條款之效力，將依有否違反誠實信用原則及顯失公平等爲基準判斷之。換言之，憑證機構與用戶雙方責任限制之約定，不得違反誠

信原則，亦不得對消費者顯失公平，否則該條款爲無效；如消費者保護法第 12 條第 1 項之「定型化契約中之條款違反誠信原則，對消費者顯失公平者 ，無效」。至於一般條款有否違反誠信原則，並對相對人顯失公平則應衡量憑證機構，與憑證用戶雙方之利益爲判斷；如消費者保護法施行細則第 13 條之「定型化契約條款是否違反誠信原則，對消費者顯失公平，應斟酌契約之性質 、締約目的、全部條款內容、交易習慣及其他情事判斷之」。

換言之，憑證機構與憑證用戶以定型化契約約定責任限制，判斷該責任限制是否違背誠信原則及顯失公平時，必須考慮斟酌契約之種類、性質、目的、條款內容、危險控制能力、風險轉嫁能力等等。雙方就責任限制約定條款之效力，需依相關事實判定，不可一概而論。

因此，憑證機構與憑證用戶契約條款不得違反法律對於定型化契約相關規定，若法律規定訂定定型化契約若違反法令應爲無效者 則該約定爲無效，故在相關，法律規範內，憑證機構於擬定與憑證用戶定型化契約時 ，不得違反訂定定型化契約之相關規定，且不得以契約免除自己法令強制規定應負之法律責任。

3.2.2 憑證機構與憑證驗證者間之法律關係－信賴關係

憑證機構與憑證驗證者間之法律關係，主要係在於憑證驗證者因信賴憑證上錯誤陳述而導致之損害，即此風險應如何分配之問題。一方面爲健全認證市場的發展，首先必須明定憑證機構及當事者的法律責任，並取得平衡。如果課予憑證機構過多或是不合理的責任，將增加經營者風險，降低民間投資認證事業之意願；另一方面，如不課予使用者善盡保管簽章設施的責任，亦可能會導致使用者疏於保管，影響電子交易的安全。是以，兩者必須取得一個平衡，憑證機構及使用者各應在合理的範圍內，以及可以預期的風險內，負起應負的責任。而此正影響憑證信賴者得求償之範圍。

現行法制依電子簽章法第 14 條第 2 項觀之，給予憑證機構得以契約簽訂方式，將此信賴關係轉換成責任的額度，即所謂「建議信賴額度」，意指依本法所

成立之憑證機構得於認證服務契約及信賴憑證者契約中載明建議之信賴額度，亦即間接的會限制了當事人間之交易金額，此一機制的目的在於提醒憑證驗證者在超出建議信賴額度之交易是不受到該電子憑證之保障。

「建議信賴額度」有下列兩種立法方式：

1. 憑證機構就其簽發之各種憑證，得請求當事者及相關業者僅能在特定範圍、特定交易金額內信賴之。我國現行法制從前揭條文觀之，似採取此種方式。
2. 憑證機構得以與憑證當事者簽訂契約之方式，排除或限制其責任，但該契約必須符合公平原則，亦即故意及重大過失責任仍然不得預先免除[69]。

「建議信賴額度」[70]是在憑證機構應負擔有限責任的原則下，爲使得憑證機構降低經營風險，並使憑證相關當事者正確的使用憑證，因此規定憑證機構可以請求相關當事人僅能在特定的範圍及金額內信賴憑證，超出保證範圍之應用，憑證機構得不負賠償責任。此類似於目前自動提款機限制每筆及每日交易金額上限之限制。

如憑證機構已經對電子憑證設定了不同程度之建議信賴額度，其中最大之優點在於憑證機構可以明確推算初期所應負擔之責任上限，在一定之情形之下，可以藉由商業保險之方式分散風險，如此才會有業者願意投入憑證機構這一個具公益性質之行業；同時憑證使用者也可以根據其交易之需求選擇其適合之電子憑證，減少不必要之支出與浪費。蓋隨著交易型態之不同，其所需之安全性與保密性也會有所不同，例如一每筆交易金額均小於 10,000 元之生活用品零售網站，與一涉及重要商業機密之 B2B 網站，其對電子交易傳輸之安全性的要求等級自然會有所不同，因此在選擇憑證機構時，可能會考慮到之因素也不相同，例如 B2B 網站在爲了維護其商業機密 及利益之前提下，可能傾向於選擇加解密技術較可靠，雖費用較高，但建議信賴額度較高之電子憑證；相

[69] 我國《民法》第 222 條之規定：「故意或重大過失之責任，不得預先免除。」

[70] 同註 21，頁 74。

反地，對於小額交易之零售網站，自然選擇建議信賴額度較低之電子憑證較符合經濟成本。

綜上所述，當憑證機構於電子憑證上載明出建議信賴額度時，憑證機構之法律責任相對地也應限制在該建議信賴額度之範圍內。另外憑證有效期間的訂定，亦明確規定了憑證機構的責任範圍，亦即憑證驗證者只能主張在憑證有效期間，信賴該電子憑證的驗證效力，一旦電子憑證超出有效期間，憑證驗證者就必須自行負起檢查憑證有效期間的注意義務。

3.2.3 憑證註冊者與憑證驗證者間之法律關係－一般法律交易關係

憑證註冊者與憑證驗證者間之法律關係，其實是一般法律上交易關係，只是當事人從實體世界移至虛擬網路世界來進行，但是在虛擬的網路世界中，當事人之間的法律關係，可能會有一些部份並不能完全適用傳統上實體世界之相關法律規定，而必須要有一些調整或詮釋，方能符合電子交易之所需。

以網路上最爲普遍交易的網路購物爲例[71]，在傳統上實體世界交易模式最爲接近者即是郵購買賣，郵購買賣本身契約的成立及生效乃是依照民法對於買賣的規定，然買賣並非書面要式契約，但由於消費者保護法第 18 條暨施行細則第 16 條規定[72]，須取得消費者聲明已受告知之「證明文件 」，在傳統郵購買賣的情形，如非使用書面文件方式，在舉證上已相當困難。何況在網路交易，消費者與企業經營者實際接觸之可能性較傳統郵購買賣更低，是否仍要對其要求「書面要式行爲」？就消費者保護法立法目的來看，告知義務的規範之所以要求「書面要式行爲 」，原因有二：一是係爲特別保護消費者，要求企業經營者以審慎的方式告知消費者；二是係爲舉證上之容易，避免爭議。因此，若能符

[71] 吳孟真著，「線上拍賣交易模式法律關係之研究」，國立成功大學，法律學系碩士論文，民國 93 年 7 月，頁 147。

[72] 我國《消費者保護法》第 18 條之規定：「企業經營者爲郵購買賣或訪問買賣時，應將其買賣之條件、出賣人之姓名、名稱、負責人、事務所或住居所告知買受之消費者。消費者保護法施行細則第 16 條：企業經營者應於訂立郵購或訪問買賣契約時，告知消費者本法第十八條所定事項及第十九條第一項之解除權，並取得消費者聲明已受告知之證明文件。」

合這兩項要件，基本上應可認同其不同於書面之告知方式，再者，電子商務注重運用網路、快速完成交易的特性，只要能運用科技發展達到傳統書面要求，似無排斥之理。

就告知義務而言，網路交易上一般以網頁方式呈現，必須注意其呈現方式，例如：字體及內容須易於閱讀、告知事項在網頁位置須醒目等等。至於爲方便舉證部分，即如何符合所謂「書面要式行爲」之證明力，電子交易由於缺乏面對面的接觸，且具有所謂匿名性之特性，故在此部份並不能一體全部適用傳統實體世界之相關規定，且法律要求當事人簽名或是作成書面，其目的不外乎希望交易之雙方可以確實確認對方之身分，並且有一深思熟慮之機會，此在網路上的電子交易中也是同等之重要。換言之，法律行爲不因爲從實體世界搬到了虛擬世界其受到的規範與保護便有所不同，因此需進一步探討電子簽章及電子文件之法律效力及相關配套措施。

1. 電子簽章之法律效力

所謂之簽名，乃是自己以手寫方式簽名之意思，其目的在於表示本人之姓名及一定之意思表示。依民法第 3 條之規定 :「依法律之規定，有使用文字之必要者，得不由本人自寫，但必須親自簽名。如有用印章代簽名者，其蓋章與簽名生同等之效力。如以指印、十字或其他符號代簽名者，在文件上，經二人簽名證明，亦與簽名生同等之效力」，因此不論是以本人手寫簽名或是以印章代替簽名，甚或以指印、十字或其他符號代簽名者，只要符合該條之相關要件，都可以發揮簽名相同之效力。

傳統簽名或蓋章的功能爲表示同意及作爲證據。常理而言，當事人在文件上簽章後，將可作爲鑑別簽署者身份的證據，同時依據文件內容確定法律上權利義務之歸屬。而電子簽章法賦予電子簽章法律效力，並不是因爲它性質上完全等同傳統簽名、蓋章，而是創設電子簽章能與傳統簽名、蓋章發揮相同之功

能，故賦予電子簽章和實體簽名、蓋章相同之法律效力，只要相對人同意[73]，便可以電子簽章取代實體之簽名蓋章。

2. 電子文件之法律效力

前已述及，立法者在考量網路或電子簽章等現代資訊通信技術在國內還未達全面性的普及，爲了避免不諳此類技術的民眾處於不利之地位，特別規定「經相對人同意者，得以電子文件爲表示方法」，也就是說，當事人欲以電子文件的方式對相對人爲某種意思表示時，就「使用電子文件的方式」這一點必須取得相對人的同意，以確保相對人之權益，因此政府機關及個人也不得強制要求相對人必須使用電子文件作爲表示方法[74]。另外，法律中規定必須以書面方式進行的不在少數，此部分實可以電子文件取代，因此明定電子文件在得以符合法律上對於書面要式要求之各項要件時，賦予電子文件與書面同等之法律效力，但前提仍是要取得相對人同意，至於須符合之要件，簡而言之，即完整性（內容可完整呈現）、保存性（可於日後取出）及可讀性（可查驗）三大要件。

最後則需考量現階段性質特殊或目前尚不宜適用之項目，授權各主管機關對於經檢視斟酌後認爲，針對各行政機關爲非相對人的情形，即便經相對人同意亦不得適用電子文件之項目，以法令或公告之方式排除前兩項規定之適用，但須注意「公平、合理，並不得爲無正當理由之差別待遇」；若各行政機關爲相對人時，直接援用法律規範要件「相對人同意」拒絕即可。

3. 電子文件與原本之提出

爲確保文件內容未遭受竄改，法律中有許多必須提出文書原本或正本之規定，因此電子簽章法第 5 條規定，依法令規定應提出文書原本或正本時，可作

---

[73] 我國《電子簽章法》第 4 條第 1 款之規定：「經相對人同意者，得以電子文件爲表示方法。」

[74] 我國《電子簽章法》第 4 條第 2 款之規定：「依法令規定應以書面爲之者，如其內容可完整呈現，並可於日後取出供查驗者，經相對人同意，得以電子文件爲之。」

爲文書原本或正本提出之電子文件，必須符合內容可完整呈現，並可供日後取出查驗之要件，方符合規定。

4. 電子文件與法定保存

爲保留書面證據，法令針對重要書面文件多設有保存期限之規定，但此種保存方式易毀損滅失且須耗費大量倉儲空間。隨著現代科技發展，儲存技術日新月異，如以數位化之方式儲存，即可簡化資料儲存及檔案保管之作業流程，並達到節省成本及人力及環保之效益，因此電子簽章法第 6 條規定，依法令規定應提出文書原本或正本者，如以電子文件可完整呈現書面文件之內容，並且可日後取出供查驗者，且以其發文地、收文地、日期與驗證、鑑別電子文件內容真僞之資料訊息，得併同其主要內容保存者爲限，便可取代書面文件而以電子文件爲保存。同時在第 2 項也規定了得依法令獲行政機關之公告，排除其適用或就其應用技術與程序另爲規定。但就應用技術與程序所爲之規定，應公平、合理，並不得爲無正當理由之差別待遇。

5. 電子文件收發文時間及地點之認定

(1) 收發文時間

原則上依當事人契約自主原則，電子文件收發文時間之認定，無論收文或發文，都先賦予當事人得自行約定之權利[75]。但法令或行政機關若有特殊考量亦得以公告方式另爲規定。

所謂發文時間，依電子簽章法第 7 條之規定，係指「電子文件以其進入發文者無法控制資訊系統之時間爲發文時間。」所謂「無法控制」之資訊系統，指的是發文者無法直接對所要寄送之電子文件或其他附加訊息再爲變更之資訊系統，如同將傳統信件投入郵筒就無法再做任何變更，至於收文時間的認定，

[75] 我國《電子簽章法》第 7 條第 1 款之規定：「電子文件以其進入發文者無法控制資訊系統之時間爲發文時間。但當事人另有約定或行政機關另有公告者，從其約定或公告。」

取決於收文者是否指定收受電子文件之資訊系統，如已指定，則以電子文件進入該資訊系統之時間爲收文時間，如送至非收文者指定之資訊系統者，則以收文者取出電子文件之時間爲收文時間，如未指定，則以電子文件進入收文者資訊系統之時間爲收文時間，即任一收文者資訊系統即可。

(2) 收發文地點

在一般交易的情形，要約、承諾、通知等，何時發出、何時到達、何地發出，對於法律行爲是否成立、生效、遲到及產生訴訟關係時，產生相當程度的影響，最後在法律上之意義爲管轄權的認定及應適用法律之問題。而電子交易並無例外，依電子簽章法第 8 條之規定，首先，無論發文者或收文者，均以其執行業務之地，推定爲電子文件之發、收文地；其次，若有一個以上執行業務之地，以與主要交易或通信行爲最密切相關之業務地爲發、收文地；如主要交易或通信行爲不明者，以執行業務之主要地爲發、收文地；最後，若發文者與收文者未有執行業務地者，以其住所爲發、收文地。

茲依電子簽章法前述規定，所決定之收發文時間及收發文地點整理如下表：

表 3-1：電子文件之收發文時間及收發文地點

	發文時間	收文時間	收文地、發文地
法律規定	依法律規定	依法律規定	
當事人約定	依當事人約定	依當事人約定	
未爲任何約定	進入發文者無法控制資訊系統之時間	電子文件進入收文者資訊系統的時間	發文者執行業務之地；收文者執行業務之地（詳見第 8 條）

已指定收受電子文件之資訊系統		送至指定之系統：以電子文件進入該系統的時間	
		非該指定之系統：收文者取出電子文件之時間	

6. 小結

綜上所述，即依電子簽章法第 4 條第 2 項之規定：「依法令規定應以書面為之者，如其內容可完整呈現，並可於日後取出供查驗者，經相對人同意，得以電子文件為之。」另依同法第 9 條第 1 項：「依法令規定應簽名或蓋章者，經相對人同意，得以電子簽章為之。」而依同法第 2 第 1 及第 2 分別定義「電子文件指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。」、「電子簽章指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。」；另依行政院消費者保護委員會所公告之「排除電子簽章法適用事項」[76]，其亦未將消費者保護法郵購買賣告知義務之「書面要求」列入，顯見亦認可電子簽章法之適用，足見以電子文件搭配電子簽章，亦可具有「書面要式行為」之證明力。

然現行上述條文關於相對人同意之規定，係指須有相對人同意始得使用電子方式為意思表示，其以相對人同意作為使用電子方式之要件，除了限制為法律行為之意思表示方式外，非經同意即不得使用電子方式，與實務應用情形有所差異，考量相對人同意條款在平衡電子商務發展與避免數位落差衝擊之重要

[76] 我國《電子簽章法》第 6 條第 3 項之規定：「第 1 項規定得依法令或行政機關之公告，排除其適用或就其應用技術與程序另為規定。但就應用技術與程序所為之規定，應公平、合理，並不得為無正當理由之差別待遇。」

性，應就其規範方式加以省思檢討。

3.3 憑證機構之設立、管理與廢止

3.3.1 憑證機構之設立

1. 憑證機構之設立方式

數位簽章制度最重要的一環就是憑證機構之設立與管理，因爲數位簽章要能達到身分識別 (Authentication)、隱密性 (Confidentiality)、資料完整性 (Integrity)及不可否認性 (Non-Repudiation)之需求，須仰賴公開金鑰基礎建設架構，而公開金鑰基礎建設架構要能順利運作，便需有完善的憑證機構之設立與管理制度。

一般而言，憑證機構之設立方式有以下三種方式，分別是特許制、認許制及報備制，此三種制度最大的不同在於主管機關審核憑證機構的權限並不相同。其中以特許制最爲嚴格，主管機關可以制訂一定之要件供相關業者參考，在業者提出申請後，主管機關仍有決定是否予以核可成立之權；而認許制則是主管機關在制訂一定之要件後，如果業者提出符合該要件之申請，主管機關就必須依法認許該業者之申請，不能夠再享有核可成立裁量權；至於報備制，則是屬於主管機關權限強度最低之一種方式，當業者向主管機關報備之後便有效成立，報備只是知會主管機關而已。

(1) 特許制

特許制是屬於最爲嚴格的一種方式，故多用於對社會交易秩序影響重大的事業上，例如：銀行法就有規定，銀行之成立採取特許制[77]，因此主管機關財政部便可以採取較爲嚴格的審查方式，在一定的社會環境之下，特許一定數目

[77] 我國《銀行法》第 2 條之規定：「本法稱銀行，謂依本法組織登記，經營銀行業務之機構。第 4 條：各銀行得經營之業務項目，由中央主管機關按其類別，就本法所定之範圍內分別核定，並於營業執照上載明之。」

之銀行成立。

(2) 認許制

認許制則是屬於較爲折衷的方式，主管機關可以依據當前之社會經濟環境需要及社會政策制訂一成立要件供由業者參考，只要有心經營憑證機構之業者能滿足該成立要件，主管機關便認許其成立。

(3) 報備制

報備制係指業者自願成立憑證機構並向主管機關完成報備手續，此時該憑證機構在法律上已便有效成立。此一成立方式屬於最爲寬鬆的制度，主管機關根本沒有任何審核的權限。

2. 憑證機構設立之資格

憑證機構設立之資格，自各國立法例觀之，最嚴格者是規定須爲股份有限公司、其次則是私法人、再其次是法人即可經營，而最寬鬆的是不作限制。茲將此四種方式略爲說明如下：

(1) 股份有限公司

即規定經營憑證機構、提供認證服務者，必須先依公司法的規定成立股份有限公司，其理由在於：「由於憑證機構的安全管理必須達到一定的水準始能確保數位簽章及憑證的安全性，且簽發的憑證、憑證註銷清冊等必須以永續經營的精神，長期維護管理，以備日後確定法律責任之用，爰規定凡是要取申請營業執照的憑證機構，必須事前通過交通部的技術審驗，才能向主管機關申請營業執照」[78]。

[78] 行政院研考會電子簽章法草案第一版第十七條第一項之立法理由。

(2) 私法人

即規定設立憑證機構之業者必須是私法人，此種規範方式係將電子簽章法適用的範圍限定在私法領域，因此僅有私法人方得經營憑證機構，政府機關之公法人則不在得經營憑證機構之範圍內。

本規範方式較前面之一種規範方式爲寬鬆，蓋因並不限定股份有限公司才可以經營憑證機構、提供認證服務，只要是依法所成立之私法人，均得經營憑證業務。其主張理由在於：「憑證機構的管理制度採用志願性的證照制度，目的即在鼓勵憑證機構申請執照，一方面便於管理，一方面對於消費者之保護更有助益，因此對於得經營憑證業務之對象，亦不宜設立過高門檻，強制規定得經營憑證機構之組織型態，導致有意願經營憑證機構之團體不得其門而入，故對於經營私領域之憑證業務之對象不限於公司方得爲之。甚且，憑證機構之公正性主要繫於其技術之安全可靠，與經營型態是否必爲公司並無相當關連性」[79]。

(3) 法人

規定設立憑證機構之業者爲私法人或公法人均可，因此政府機關及可視實際需求，成立憑證機構[80]。

(4) 不作任何限制

亦即憑證機構之業者無須具備法人之資格，亦即個人或是合夥型態[81]均不受限制。但站在消費者保護之立場，本論文認爲除非有相當之配套措施，如相

---

[79] 鄭寶清委員於民國八十八年十二月二十三日所提出之電子簽章法草案第十一條之立法說明。

[80]行政院研考會電子簽章法草案第八版中第十三條便採取此一立法方式，理由是 ：「憑證機構係一具有公信力之機構，只要使用者對其產生信賴，皆可經營及提供電子認證之相關服務。是以，歐美主要國家多依市場機制，開放公私機構及營及提供電子認證服務 」。此方式認爲電子簽章法的適用範圍兼及公私法領域，因此私法人與政府機關當然可以依據實際之需要，分別成立適當之憑證機構。

[81] 由於無法稽核人頭合夥人之問題，因此本論文認爲個人或是合夥型態，其經營風險並無不同。

當族隔之保險或責任準備金之提列等，不建議採如此寬鬆之規範方式。

(5) 小結

在現今網路高倍速時代，現代政府運作及施政亦有設立憑證機構之需求，因此本論文認爲公私領域之憑證機構之設立有其必要性及需求性，亦較符合國際立法之趨勢潮流，簡言之，機關及法人均得成立憑證機構。

3. 憑證機構設立申請之程序

除公領域之憑證機構需具備政府機關之資格外，茲就私領域憑證機構，簡述憑證機構設立申請之程序如下：

(1) 依法律規定成立法人

依電子簽章法第 2 條第 5 款之規定，憑證機構係指簽發憑證之機關、法人，因此憑證機構須先依法成立法人，才能申請成爲憑證機構。主管機關會依據下列條件來審查：獨立性、承擔風險之財務資源及能力、管理人員之經驗及專業能力、永續經營能力、軟體及硬體之可靠性、稽核制度及能力、緊急應變及回復能力、人員甄選及管理、認證機構私鑰保護能力、內部安全控制能力、終止營業之安排、保證及憑證實務作業基準書、責任之限制、保險、與其他認證機構之互通性、憑證撤銷之程序。

(2) 外國憑證機構之認許

依外國法律組織登記之憑證機構，得在國際互惠及安全條件相當的原則下，經主管機關許可，在我國境內提供認證服務。其所簽發的憑證，與本國機構所簽發的憑證具有同等效力。由於網路具有跨域時空的特性，在電子商務已朝全球化及網路化發展的趨勢下，必須建立跨國認證機制，才能讓跨國的電子商務得以實施。目前聯合國、經濟合作發展組織、歐盟等國際組織正致力於推

動跨國認證機制，主要國家的數位簽章法亦遵循上述國際組織的指導原則，規定在一定的條件下（例如同等的安全水準）承認外國憑證機構所簽發的憑證。跨國認證機制的建立，除了考量技術互通的規範之外（例如 X509 憑證標準[82]），在法律層面也要透過雙邊或是多邊的國際協議，並在國內相關法律作配套的規定，才能建立跨國認證機制。

3.2.2 憑證機構之管理

關於主管機關對憑證機構之管理，依國際立法例觀之，其管理主體有係以憑證機構爲標的者、有以電子簽章本身爲標的者、亦有採完全技術中立者，如下表所示：

表 3-2：各國認證機制管理之主要標的

	亞洲各國	歐盟各國	美國
管理主體	憑證機構	合格之電子簽章	技術中立 E-SIGN[83]中未提及憑證機構 惟其各州依其需要訂之

而管理強度則依憑證機構於設立之際(前)有無規範：須通知主管機關、法制與認證機制所規範之主體、採行自願認可制、及法規強制規定須檢測安全簽章產製裝置而有所區別。

至於落實於實際上營運之管理方面，參照各國規定，茲就 1.憑證機構得經營之業務範圍、2.憑證實務作業聲明書、3.憑證機構應揭露之相關資訊、4.

[82] X509 指令是一個多用途憑證公用程式，爲目前之標準格式。

[83] 美國「全球暨國家商務電子簽章法」(The Electronic Signature of Global & National Commerce Act, 簡稱爲美國聯邦電子簽章法 E-SIGN)。

主管機關對於憑證機構之監督、5.主管機關對於憑證機構之處罰，以及 6.憑證機構對個人資料所應有的隱私權保護措施等六個部分，茲說明如下：

1. 憑證機構得經營之業務範圍

一般而言，憑證機構得經營之業務範圍如下：

(1) 簽章公私鑰製作服務

(2) 憑證簽發服務

(3) 電子文件存證及公證服務

(4) 時戳服務

(5) 經主管機關核准辦理之業務

2. 憑證實務作業聲明書

憑證實務作業聲明書(Certificate Practice Statement, CPS)，是由憑證機構對外公告，用來陳述憑證機構如何簽發憑證及處理其他認證業務之作業準則（一份政策聲明文件）。例如：說明憑證機構的技術、安控措施、憑證的使用範圍、憑證的效期、憑證註銷及中止程序、憑證註銷清冊、憑證註銷清冊如何公布等資訊，俾供使用者判別憑證機構的專業技術能力及管理能力，並據以作爲判別法律責任歸屬的依據。故爲便利民眾瞭解電子認證之運作機制及律定相互之權利義務關係，憑證機構應以書面、電子或其他方式對外公布，其內容乃是載明憑證經營或提供電子認證服務之相關作業準則。

一般而言，憑證實務作業聲明書所應包括之內容有：

(1) 憑證機構製作電子簽章之技術、方法、設施、管理、稽核及人員等資訊。

(2) 憑證機構簽發電子憑證之註冊申請程序及鑑別申請者身分之方法。

(3) 電子憑證之註銷、中止及廢止程序，時間認定及責任歸屬。

(4) 憑證註銷、中止及廢止清冊之發布方法、更新周期及查詢方法。

(5) 憑證機構簽發之電子憑證適用範圍、使用限制、交易金額限制及責任保證等。

(6) 憑證機構之損害賠償責任及免責事項。

(7) 驗證憑證機構本身電子憑證真僞之方法及查詢其電子憑證註銷、中止及廢止資訊之方法。

(8) 其他相關事項。

3. 憑證機構應揭露之相關資訊

憑證機構所應揭露之相關資訊，例如：憑證機構所簽發之憑證、憑證中止、憑證註銷、憑證機構之營業中止及註銷許可等相關資訊，必須在網路或其他媒體公開，提供各界隨時查詢利用。其最主要的目的在於讓使用者得以知悉該憑證機構之業務情形，以供選擇憑證機構之參考。

憑證機構應查驗憑證申請者之身分，確定申請者與憑證之配對關係，並將憑證及相關資訊建置於公眾網路，對外公布下列事項供各界隨時查詢利用

(1) 憑證機構本身之憑證及公鑰。

(2) 憑證實務作業聲明書。

(3) 憑證機構本身憑證之註銷或中止。

(4) 其他足以影響簽發憑證之可靠性，或影響其執行業務及提供服務之任何事實。

如發生上述第(4)點之事件時，憑證機構應依照憑證實務作業聲明書規定之程序，以合理方式盡其所能通知任何可能受到憑證影響之當事人。

此一規定的理由有二，分別是：

(1) 明定憑證機構必須在簽發憑證前，確實查驗申請者的身分，確定申請者之公鑰及私鑰是否成配對的關係，再登錄於憑證之上，並對外公布，使申請者不能於事後否認。

(2) 基於保護消費者的權益，並便利社會大眾辨識憑證機構，憑證機構亦應主動將本身相關的資訊對外公布，俾利使用者及相關單位可以查詢利用，以維持交易秩序。

4. 主管機關對於憑證機構之監督

誠如前述，主管機關對於憑證機構之監督，依主管機關介入其經營之程度，在各國立法例中，有採取低度管理原則者，即書面審查制度僅要求憑證機構有對外揭露之義務，基本上是讓民間主導發展各項電子交易需要的電子認證服務及相關標準，讓市場機能自由運作，由業者自行協調並相互競爭。至於憑證機構與其使用者間的權利義務關係，則是依據契約自由原則，讓雙方依據契約來決定。相對地，如採高度管理原則者，係針對欲對外提供簽發憑證應用服務之憑證機構，爲確保憑證機構之營運與其憑證實務作業基準一致，特別要求於申請主管機關核定時，尚須憑證機構提供相關文件來強化書面審查之效力，甚至要求每隔一段時間繳交由第三公證單位所製作之外部稽核報告(實質審查)。

表 3-3：各國法制對於憑證機構管理規範[84]

	憑證機構於設立之際(前)須通知主管機關	法制與認證機制所規範之主體	採行自願認可制否	法規是否強制規定須檢測安全簽章產製裝置
我國	無規定	經核定或許可之(對外提供服務之憑證機構)	是 (書面審查)	無
日本	無規定	經認可之憑證機構(提供特定認證業務之	是 (書面審查與實質審查)	指定合格單位進行相關稽核

[84] 資料來源：資策會科技法律中心「電子簽章法修正草案相關法制」座談會會議資料，西元 2005 年 6 月。

		憑證機構)		
韓國	無規定	經認可之憑證機構	是 (書面審查與實質審查)	須進行相關稽核
中國	強制許可制	所有憑證機構	否，強制許可制 (書面審查與實質審查)	信息產業部進行年度檢查
上海	政府授權經營制度	所有憑證機構	否，強制許可制 (書面審查與實質審查)	市資訊辦需對其財務、業務及營運等狀況進行監督管理
廣東省	強制許可制	所有憑證機構	否，強制許可制 (書面審查與實質審查)	年度審查(憑證機構之資格一年一審)
香港	無規定	經認可之憑證機構	是 (書面審查與實質審查)	稽核報告
新加坡	無規定	經認可之憑證機構	是 (書面審查與實質審查)	稽核報告
歐盟指令	各國法令不得規範憑證機構於設立前須通	簽發合格憑證之憑證機構	是	

	知主管機關			
奧地利	所有憑證機構	所有憑證機構	是	是
比利時	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	是	是
丹麥	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	否	是
芬蘭	簽發合格憑證之憑證機構	法律規範所有憑證機構(然實務上爲簽發合格憑證之憑證機構)	否	可自由選擇
法國	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	是	是
德國	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	是	是
希臘	所有憑證機構	所有憑證機構	是	是
愛爾蘭	無此規定	簽發合格憑證之憑證機構	是	尚未進行
義大利	簽發合格憑證之憑證機構	所有憑證機構	是	是
盧森堡	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	是	無此規定
荷蘭	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	是，其由業者自律之志願認可制	可自由選擇

葡萄牙	簽發合格憑證之憑證機構	所有憑證機構	是	是
西班牙	所有憑證機構	所有憑證機構	是	否
瑞典	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	是	是
英國	無此規定	簽發合格憑證之憑證機構	是，其由業者自律之志願認可制	否
捷克	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	是	是
愛沙尼亞	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	否	否
匈牙利	所有憑證機構	對公眾簽發合格憑證之憑證機構	否	是
波蘭	簽發合格憑證之憑證機構	所有憑證機構	否	是
冰島	簽發合格憑證之憑證機構	所有(包括非對外)簽發合格憑證之憑證機構	否	是
挪威	簽發合格憑證之憑證機構	簽發合格憑證之憑證機構	否	否
瑞士	無此規定	簽發合格憑證之憑證機構，	是	否

		然其被監督管理之對象採志願制		

由上表可知，絕大部分國家立法例均對於簽發合格憑證或經核可之憑證機構均採行書面審查加實質審查之高度管理制度。

茲就亞洲部分國家進一步敘述如下[85]：

(1) 澳洲

任何在 Gatekeeper 專案或澳洲商務數字數位簽章憑證（Australian Business Number-Digital Signature Certificate, ABN-DSC）架構底下，獲得核准宣告的個人或團體都可以稱之爲「憑證管理中心」（Certification Authority, CA），且依據每一個組織架構之不同，而有各自的管理辦法。

(2) 香港

不同於其他亞洲國要求憑證管理中心需要有一個強制註冊系統（mandatory registration system），香港則採取自願登記系統（voluntary recognition system）。憑證機構業者可以自行提出申請認可的要求，但必須符合憑證業者的規範標準才能取得正式認可，換言之，在香港地區，未申請認可的憑證機構業者可以跟認可核證機關（Recognized Certification Authority, RCA）共同在市場上較勁，但最大的不同是，未認可的憑證機構業者各項作業活動，以及與客戶之間的關係，是由一般法來規範與管理，而非香港電子交易條例（Electronic Transaction Ordinance, ETO)。

由於香港電子交易條例僅承認由認可核證機關所簽發憑證的數位簽章技術，而由認可核證機關的重要性格外顯著。事實上，香港電子交易條例的重要

[85] CommerceNet Taiwan，跨國電子商務交易法律議題報告（下），2003 年 8 月，http://www.nii.org.tw/CNT/info/Report/200308_3.htm，2007/07/30 visited。

事項均與認可核證機關有緊密的關連，如認可核證機關之認可、認可核證機關對使用者的責任歸屬，以及所簽發的數位憑證管理等。

憑證機構業者可向資訊科技署署長申請成爲香港電子交易條例所指的認可核證機關，而中也規範了署長核准時所應檢附的各項詳情與文件，包括必須提供憑證機構業者的財務狀況報告、責任管理辦法、系統安全管理措施、憑證簽發標準、自我評估報告，來評斷憑證機構業者是否有足夠勝任認可核證機關之能力。

香港電子交易條例也賦予署長撤銷或暫時吊銷認可核證機關的權力，署長除依據上述相關文件來評斷之外，還可考慮核證機關是否有按照「核證作業準則」（certification practice statement, CPS）運作、是否遵守業務守則（Code of Practice），以及是否使用穩當系統等。

此外，香港電子交易條例也對於認可核證機關的運作規範了一般條文，如：認可核證機關必須使用穩當系統進行發出或撤回認可證書的服務，且需在儲存庫內公布或發出通知，並維護系統之運作。另外，認可核證機關也必須提交關於遵守香港電子交易條例，以及西元 2000 年 7 月由資訊科技署所發佈的業務守則的評估報告。

香港電子交易條例亦規定，認可核證機關必須發出及備存最新的核證作業準則，並必須將對該準則所列的該機關的作業所作的任何變更通知署長。而核證作業準則（Certification Practice Statement, CPS）是指核證機關所發出的以指明其在發出證書時使用的作業實務及標準的準則。

香港電子交易條例中最特別的規定爲指定香港郵政署擔任認可核證機關，這也是希望由政府帶頭做起，建立香港第一個認可核證機關。目前在香港有四個已獲得通過的認可核證機關，包括香港郵政核證機關（Postmaster General）、電子核證服務有限公司（Digi-Sign Certification Services Ltd）、網際威信公司（HiTrust.com），與銀聯通寶有限公司（銀通/ Jetco）。而在香港認可核證機

關營運，還是一種相當新穎的商業營運種類。

(3) 日本

日本電子簽章與認證業務法（Electronic Signatures and Certification Service Law, ESCSL）要求憑證服務供應商必須獲得日本總務省、經濟產業省，以及法務省的許可才可以營運作業。

日本電子簽章與認證業務法規定了憑證服務供應商在提供憑證服務前所應具備的各項條件，以及憑證服務的各項作業要點，此外，日本電子簽章與認證業務法也提供了當日本公安委員會（National Public Safety Commission）發現經許可的憑證服務可能引發嚴重的問題時，可以要求相關單位予以必要的措施防範，以避免傷害的發生。

(4) 馬來西亞

馬來西亞數位簽章法案（Digital Signature Act, DSA）必須授權或委任某一個管理單位，來監督或控管憑證管理中心的各項活動，此外，馬來西亞數位簽章法案也規定，主管機關必須制訂憑證管理中心的取得要件。

(5) 中國大陸

中華人民共和國電子簽名法第 18 條規定，從事電子認證服務，應當向國務院資訊產業主管部門提出申請，並提交符合中華人民共和國電子簽名法第 17 條[86]規定條件的相關材料。同時申請人應當持電子認證許可證書依法向工商行政管理部門辦理企業登記手續。

---

86 中華人民共和國《電子簽名法》第 17 條之規定：「提供電子認證服務，應當具備下列條件：
（一）具有與提供電子認證服務相適應的專業技術人員和管理人員；
（二）具有與提供電子認證服務相適應的資金和經營場所；
（三）具有符合國家安全標準的技術和設備；
（四）具有國家密碼管理機構同意使用密碼的證明文件；
（五）法律、行政法規規定的其他條件。 」

關於作業基準部分，中華人民共和國電子簽名法第 19 條規定，電子認證服務提供者應當制定、公佈符合國家有關規定的電子認證業務規則，並向國務院資訊產業主管部門備案。且電子認證業務規則應當包括責任範圍、作業操作規範、資訊安全保障措施等事項。

中華人民共和國電子簽名法第 21 條並規範電子簽名認證證書應當載明之內容有：

①電子認證服務提供者名稱；

② 證書持有人名稱；

③ 證書序列號；

④ 證書有效期；

⑤ 證書持有人的電子簽名驗證資料；

⑥ 電子認證服務提供者的電子簽名；

⑦ 國務院資訊產業主管部門規定的其他內容。

關於終止服務部分，中華人民共和國電子簽名法第 23 條規定，電子認證服務提供者擬暫停或者終止電子認證服務的，應當在暫停或者終止服務 90 日前，就業務承接及其他有關事項通知有關各方。並應當在暫停或者終止服務 60 日前向國務院資訊產業主管部門報告，並與其他電子認證服務提供者就業務承接進行協商，作出妥善安排。如電子認證服務提供者未能就業務承接事項與其他電子認證服務提供者達成協定的，應當申請國務院資訊產業主管部門安排其他電子認證服務提供者承接其業務。至於電子認證服務提供者被依法吊銷電子認證許可證書的，其業務承接事項的處理按照國務院資訊產業主管部門的規定執行。

(6) 新加坡

新加坡資訊通信發展管理局（Infocomm Development Authority, IDA）爲主管電子商務準則與政策的領導性部門。由於憑證機構必須受到部分標準與管理來確立其公信力，因此新加坡電子交易法（Singapore Electronic Transactions Act

1998, SETA）制訂係由新加坡資訊通信發展管理局擔任憑證機構的管理與許可單位。

新加坡資訊通信發展管理局於 1999 年發表了一份「憑證機構安全指導方針」（Security Guidelines for Certification Authorities）[87]，建立起憑證機構管理、系統與運作的安全準則，以達到保護憑證服務、資料與系統的完整性、機密性，與有效性之目的。而新加坡資訊通信發展管理局也頒佈了資訊科技安全指導方針（Information Technology Security Guidelines），來協助組織發展或執行資訊安全系統。

(7) 南韓

韓國電子簽章法（Electronic Signature Act 2001, ESA）規範憑證機構的權限，包括：憑證實務作業基準（Certification Practice Statement, CPS）、憑證發放、暫時停用與廢止等服務。韓國資訊與通訊部（Minister of Information and Communication, MIC）爲目前韓國憑證機構執照資格認定的主管單位，允許已核可的憑證機構（accredited certification authority, ACA）負責發放加密金鑰（encryption key）、憑證證明給加密金鑰的用戶，並且保管金鑰。在憑證服務開始運作之前，韓國資訊與通訊部要求已核可的憑證機構必須提出包含下列內容的憑證實務作業基準：

① 憑證服務的種類。

② 憑證服務的運作要點與流程。

③ 使用憑證服務的期限、條件與費用。

④ 其他憑證服務進行可能遇到的重要問題。

在韓國電子簽章法下，已核可的憑證機構必須依照憑證實務作業基準的規範，並且不可毫無理由拒絕提供認證服務，爲了達成安全及可信賴的憑證服務，

[87]http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/c980f8b6341c4a0bc82568390001fc59?OpenDocument，2007/07/30 visited。

韓國資訊與通訊部會決定並宣布已核可的憑證機構必須遵守的電子簽章憑證服務指導方針要項。

同時已核可的憑證機構若取得其他已核可的憑證機構的憑證服務，或與另一家已核可的憑證機構進行企業合併，或合併業務後設立新公司，均需對韓國資訊與通訊部報告，並且對先前已消滅的已核可的憑證機構存續狀態進行說明。

韓國電子簽章法規定，已核可的憑證機構若要暫時停止部分的憑證服務，必須在停止業務 30 天前通知客戶，並且提交報告給韓國資訊與通訊部，停止業務的期間不得超過 6 個月；若已核可的憑證機構要終止憑證服務，至少需在 60 天前通知客戶，並且提交報告給韓國資訊與通訊部；而已核可的憑證機構若因不可抗力因素需要將客戶的認證憑證與記錄讓渡給其他的已核可的憑證機構，同樣也要提交報告給韓國資訊與通訊部。韓國資訊與通訊部在收到這些報告之後將命令韓國資訊安全局（Korea Information Security Agency, KISA）接管客戶的憑證。

5. 主管機關對於憑證機構之處罰

依行政罰之種類[88]，主管機關對於憑證機構之處罰，大致有下列幾種方式：

(1) 命限期改正

(2) 處以一定範圍內金額之罰鍰

(3) 停止一部或全部業務

(4) 派員監管或接管

[88] 我國《行政罰法》第 1 條之規定：「違反行政法上義務而受罰鍰、沒入或其他種類行政罰之處罰時，適用本法。但其他法律有特別規定者，從其規定。第 2 條：本法所稱其他種類行政罰，指下列裁罰性之不利處分：一、限制或禁止行爲之處分：限制或停止營業、吊扣證照、命令停工或停止使用、禁止行駛、禁止出入港口、機場或特定場所、禁止製造、販賣、輸出入、禁止申請或其他限制或禁止爲一定行爲之處分。二、剝奪或消滅資格、權利之處分：命令歇業、命令解散、撤銷或廢止許可或登記、吊銷證照、強制拆除或其他剝奪或消滅一定資格或權利之處分。三、影響名譽之處分：公布姓名或名稱、公布照片或其他相類似之處分。四、警告性處分：警告、告誡、記點、記次、講習、輔導教育或其他相類似之處分。」

(5) 指定其他憑證機構承接

認證機制之健全發展，是電子化政府及電子商務能否普及發展之關鍵，爲健全認證市場秩序，保障消費者權益，政府宜善盡其監督管理的責任，故賦予主管機關行政處分之權利，以利採取必要的措施，導正市場秩序。同時憑證機構經撤銷許可或勒令停業者，主管機關得將其業務交由另一憑證機構承接，以保障使用者之權益。

6. 憑證機構對個人資料所應有的隱私權保護措施

公開金鑰基礎建設係因應網際網路匿名交易爲保護交易安全而生，但亦由於爲確認交易相對人之身分，交易當事人之個人資料被廣泛收集或有可能於交易認證過程中遭駭客破壞，而使個人隱私受到侵害，因此若無一完善之隱私權政策，恐怕會對資料所有人相當之不利，尤其在目前各式各樣、日新月異、層出不窮的詐騙手法翻新之狀況百出之際，憑證機構對於個人資料所應有之隱私權保護措施即險的更爲重要，因此相關規定不可忽略。

同時憑證機構若屬於壟斷式經營，則所有個人資料接落入同一業者手中，此將對憑證使用者相當之不利，因此目前各國的管理政策皆認爲應將憑證機構之經營分散化，也就是說藉由分散憑證機構之業務量，使得個人資料被分散持有，才不致於會出現壟斷性憑證機構對使用者個人資料濫用之危險性。

3.3.3 憑證機構之終止服務

憑證機構於其終止認證服務，應最小化對用戶和信賴憑證者之影響，因而其應依照其憑證實務作業基準所載明之程序，結束營運、於相當期間前通知受影響之個體，並將憑證機構相關存檔紀錄轉交保管人。通知內容並應包括憑證機構及註冊中心歸檔紀錄之保管人身分。

3.4 憑證機構之責任

3.4.1 憑證機構之注意義務

憑證機構之注意義務之程度是否適用於消費者保護法第七條之無過失責任，此須從兩個面向來考慮：一方面是爲建立消費者使用及電子憑證之信心，在公開金鑰基礎建設之架構下去從事電子交易，應課予憑證機構較高之注意程度；但在另一方面，在認證服務發展之初期，如一開始即課予憑證機構業者高程度之注意義務，在尚未看到獲利且又需負擔過重責任風險之情況下，將無進入此領域之意願。如此一來，對公開金鑰基礎建設架構之發展將有不良影響，蓋一個健全的公開金鑰基礎建設架構，需要的是有一定數目的憑證機構，讓消費者有選擇性外並可以相互交叉認證，如此可避免因爲市場壟斷而可能產生對消費者個人資料產生不利之影響。

首先將歸責原則之注意程度簡述如下：

1. 過失責任（Negligent liability）

所謂過失責任，係指凡具有理性之社會人，如因其「故意或過失」不法侵害他人之權益時，應就所生之損害，負損害賠償責任；反之，如其已盡必要之注意，而認爲無故意或過失時，對於他人之損害，及毋庸負賠償責任。[89]因此，過失責任者，謂基於故意或過失，加損害於他人時始負賠償責任之立法主義，此與加害人雖無故意或過失，仍應對其行爲所生的損害負賠償責任之無過失責任主義相對稱。

近代私法係以個人爲本位，一切權利既歸屬於個人，一切責任自亦應由個人負之。易言之，所有法律上之效果，須基於個人之意思而發生，同時對於責任之有無，其歸屬原因亦應求諸個人之主觀條件，於是乃以故意過失之有無以定責任之歸屬，如此始能保障個人之自由活動，以從事自由競爭。蓋在社會常態下，吾人苟能盡相當之注意，即足以防止損害之發生，則對於不盡其注意義

[89] 邱聰智著，新訂民法債篇通則（上），台北，2000 年 9 月新訂一版，頁 149。

務者，使負賠償責任乙節，實合乎正義之要求。否則不論有無過失，一律使負賠償責任，將造成責任感強烈者，凡事畏縮不前，其活動範圍，徒受限制，而埋沒其才亦爲社會之損失；反之，責任觀念較弱者，必將認爲縱令注意，猶不免責，何必畏首畏尾，乃更無所忌憚，益加放縱，結果甚不利於社會安全自明，故過失責任實有其作用在也。申言之，契約自由原則係積極地促進個人之自由活動，而過失責任主義則消極地保障個人之自由活動，兩者相得益彰，對於近世文明之貢獻，實不遑多論。[90]

然過失責任仍爲民法三大原則[91]之一，原則上若法律無特別之規定，憑證機構只要負過失責任即可，也就是憑證使用者必須舉證證明憑證機構確有過失，才能夠請求憑證機構就其所受之損失負起責任。以下將針對：1.憑證簽發錯誤；2.未依法或依憑證實務作業基準之規定註銷、中止或簽發憑證；3.憑證機構之履行輔助人之過失或管理疏失等三個情形說明憑證機構之過失責任原則。[92]

(1) 憑證簽發錯誤

憑證簽發錯誤，是指憑證機構對於電子憑證上之資料有錯誤之記載，以致於憑證使用者因信賴該資料而遭受損失之情形而言。原則上除非憑證機構及其代理機構可以證明已經採行與該項憑證目的相當之所有合理可行之避免憑證錯誤之措施，否則憑證機構是負損害賠償責任。

(2) 未依法或依憑證實務作業基準之規定註銷、中止或簽發憑證

憑證機構未依法或依憑證實務作業基準之規定註銷、中止或簽發憑證，將會對社會交易秩序產生相當大之影響，因爲一般人將會因信賴該憑證機構所簽

---

[90] 參照王澤鑑著，侵權行爲法第一冊，台北，三民書局，2001 年 7 月，頁 13。

[91] 由於近代市民社會是以平等契約爲基礎，而與封建社會的階級身份關係爲基礎者大爲不同，因此私法上乃以「自由平等」爲理念，基於此一理念演變成：契約自由原則、過失責任原則、所有權絕對原則此民法三大原則。

[92] 行政院研考會電子簽章法草案第一版第三十六條。

發之電子憑證而遭受到損失，且消費者對於憑證機構及電子交易失去信心，此對於一個良好的電子交易環境之建立，是一個負面之因素。所以對於憑證機構此類行爲，即應課予其賠償之義務，以避免此一情形之發生。

(3) 憑證機構之履行輔助人之過失或管理疏失

依據民法第二百二十四條之規定：「債務人之代理人或使用人，關於債之履行有故意或過失時，債務人應與自己之故意或過失負同一責任。」此一條文也可以適用於憑證機構，當憑證機構之代理人或使用人關於管理有故意或過失行爲時，憑證機構應與自己之故意過失負同一責任，因此憑證機構對於此類行爲是應該負起損害賠償責任的，惟就電信機線設備障礙、阻斷，以致發生錯誤、遲滯、中斷或不能傳遞導致電子認證服務之中斷，本論文主張則應排除在外而予以免責，將於下「責任限制」部分論述。

(4) 無過失責任理論之興起

近代因大規模企業發達之結果，危險事業日益激增，損害事件比比皆是，致過失責任主義已不足以適應現今社會之要求，於是各國立法潮流，已有由過失責任主義，轉變爲無過失主義之趨勢，我國之消費者保護法即爲一適例。蓋商品製造上若有危險瑕疵，對於消費者發生損害，被害人若仍須依民法第 184 條規定要求製造人賠償，得舉證證明製造人製造過程上有過失，這在消費者對於商品製造過程往往無法窺其堂奧之下，無異係屬「天方夜譚」，此時如猶貫徹過失責任主義，顯屬有背公平正義，從而自有制定「祇要證明係食用或使用具危險瑕疵的產品，以致生命、身體、健康、財產等法益受侵害者，即得據以求償之無過失責任法律或判例」的必要。再者，現代化企業不斷地迅速發展，固爲人類生活帶來舒適與便利，但其所附隨的危害亦不容忽視，然此類損害之發生，卻大都不能解爲該企業有過失。何也？蓋雖以最高科學水準之技術從事生產製造或服務，仍不免發生損害之情形，所在多有，故因而所生損害之損害，

即難解爲該企業之過失，既不能解爲過失，則依過失責任主義即無法令該企業賠償（歸責困難）。此外，縱使損失之發生的確有時係出於該企業之過失，然過失乙節須由被害人舉證，而有關之物證經常於事故發生時已被破壞殆盡，至於人證方面，又往往語焉不詳或雖詳而異，對於事故真相之確定，有時幾不可能，於是損害賠償責任每因舉證困難即無從加諸該企業身上。由此可見，若堅持過失責任主義，則應由企業負擔之損害賠償，受害者獲得賠償的機會甚微，雖或謂「舉證困難」一事，可依舉證責任之轉換而加以救濟，但「歸責困難」究無法解決，因而無過失責任之理論，自隨之興起。

2. 無過失責任（又稱嚴格責任，Strict Liability）[93]

無過失責任係從消費者保護之角度發展而來，其產生背景係由於自十九世紀以降，危險事業激增，意外事故頻傳，縱令企業經營者已爲相當之注意，亦無法防止危險之發生，倘嚴守過失責任原則，則受害人無法求償。故爲了適應現實環境之需要，無過失責任因應而生，此乃因企業經營者增加社會之危險負擔，且有能力將所負之危險轉嫁至其他社會團體分擔，故損害賠償之責任理應由其負擔之。

如對憑證機構採無過失責任之歸責原則，意即究竟憑證機構是否適宜課與無過失責任呢？支持認爲應課與憑證機構無過失責任的理由是[94]：

(1) 因爲憑證服務之提供具有一定程度之公益性，影響社會交易秩序之穩定甚鉅，所以必須明定憑證機構應確保其提供之業務無安全上之顧慮，對所致之損害應負損害賠償責任，才能保障憑證使用者之權益。

(2) 資訊安全環境的建立是電子商務得以發展的基石，也是憑證機構最重要的責任，故關於資訊安全之保障，憑證機構應負無過失責任，方能給予憑證申請人使用憑證充分的信心。

---

[93] 鄭玉波、陳榮隆修訂，民法債編總論，修訂二版二刷，台北，三民書局，2004 年，頁 155。

[94] 民國 88 年 12 月鄭寶清委員電子簽章法草案第 14 條便是對憑證機構課與無過失責任。

(3) 參考消費者保護法第七條規定，憑證機構似乎也是服務提供的一種企業，因此也應有該條無過失責任原則的適用，爲避免將來解釋與適用上之爭議，因此便明定憑證機構應負起無過失責任。

過失責任主義有促進行爲人提高注意防止損害發生之功能，乃其主要的特色，若改採無過失責任主義，則在損害賠償方面，行爲人是否已盡注意義務，並非重要之事，有無因此而使得行爲人產生毋庸注意的心態，以致過失事故層出不窮喪失預防損害發生之功能，不無疑慮。不過現今科學技術係日新月異，一般而論，祇要企業經營者投資於設備之改善，加強安全措施的維護，通常即可避免損害發生，然在過失責任主義制度下，若企業經營者非砸下高額投資，實無法防止損害者，則一旦此類損害發生，對加害者而言，即屬無過失之行爲，自得免除賠償責任；而同樣情形，若採無過失責任主義，則是不能據以免責的，此就保護受害人之權益以觀，較爲迅速完善自明。故在無過失責任制度下，企業爲免除賠償責任，勢必更願意投注相當金額，改善安全設備，防止發生損害。從而，處在科技高度發達之今日，採取無過失責任主義，因在防止損害發生的技術層面上通常不成問題，則當自能鞭策企業經營者改善設備，如此一來，較之過失責任主義，反而更有防止損害發生之功能。[95]

然而退一步言之，透過所謂的「過失的經濟分析」——漢德程式（Learned Hand Formula ），當 B＞PL 時（B 爲防制損害發生之成本，P 爲因之可減少的損害發生率，L 爲實際造成的損害金額），係表示企業經營者損害防制的成本大於不預防損害時所將需要支出的賠償數額，於是企業經營者即寧願負擔損害賠償責任，亦不願採取預防措施[96]，在此情形之下，冀求企業經營者盡力防止損害發生，無異於緣木求魚。

---

[95] 曾隆興，詳解損害賠償法，台北，三民書局，2004 年 4 月，頁 9。

[96] 簡資修，「危險之生成與界線：舉證責任與過度防制」，台大法學論叢 48 期，2001 年 5 月，頁 55。

因此，本論文認爲對於企業經營者所提供之產品或服務造成生命身體健康等生命法益造成之損害者，採無過失責任自應合乎吾人法感情；但對造成財產法益受損害者，如一概採用無過失責任，則似屬「保護過當」。倘若係爲避免被害人因舉證困難而求償無門之情形，則可採「推定過失責任」[97]，藉由舉證責任之轉換來處理此不公之情況。

3. 推定過失責任（又稱中間責任, Presumed Liability）

推定過失責任係指當損害發生時，受害人無須證明行爲人有故意過失，而是直接認定行爲人有故意過失而成立損害賠償責任，惟如行爲人自己能證明無任何故意過失，即得以免責謂之。蓋法諺有云：「舉證之所在，敗訴之所在」，採推定過失責任即可彌補過失責任須由受害人舉證之弊。

4. 小結

本論文以爲，就國內現況而言，著眼於國內公開金鑰基礎建設技術尚未發展成熟，尤其是互通機制之技術尚有待進一步研發，爲使憑證機構不致因預期須承擔極大的風險而阻礙我國電子認證產業之健全發展，復爲避免使用者預期毋須爲保管電子簽章不周而負責，進而疏忽其應盡的管理責任，主張在權責平衡原則下，對憑證機構之歸責程度規範宜採推定過失責任爲妥。

3.4.2 憑證機構之責任限制

如同於海商法的相關規定，當我們課予運送人推定過失之注意義務[98]時，爲避免義務人可能因單一偶發事件須承受無上限之賠償責任，而導致爲卸責而直接宣告倒閉，反而使受害人無法獲得實質賠償，且已成立之電子認證契約及

---

[97] 同註 93，頁 160。

[98] 我國《海商法》第 62 條第 2 項及第 3 項之規定：「船舶於發航後因突失航行能力所致之毀損或滅失，運送人不負賠償責任。運送人或船舶所有人爲免除前項責任之主張，應負舉證之責。」

信賴關係亦一夜歸零，進而不但妨礙產業發展，且反而付出更多社會成本。

配套的規定則有法定免責事由[99]、船舶所有人責任限制[100]及單位責任限制[101]等。因此憑證機構是否也應有類似之規定，便值得加以討論：

1. 憑證機構之免責事項

憑證機構之免責事項是指就列舉之情形下，憑證機構不負損害賠償之責任，其可能情形如下[102]：

(1) 對於任何信賴其憑證當事者之錯誤及僞造之數位簽章所致之損害企業經失，已依各該規定採行所有合理可行之預防措施。

(2) 對於相關當事者將憑證應用在與簽發目的相違背之事項，或超出憑證所載之限制事項。

2. 憑證機構可否主張責任限制

誠如前述，原則上基於爲兼顧消費者權益及商業風險之考量，憑證機構應可主張責任限制的，但是其前提是仍要符合民法第 222 條之規定：「故意或重大過失之責任，不得預先免除」，因此憑證機構可以在善盡其應負之注意義務後，

---

[99] 我國《海商法》第 69 條之規定：「因下列事由所發生之毀損或滅失，運送人或船舶所有人不負賠償責任。」

[100] **我國《海商法》第 21 條第 1 項之規定：「船舶所有人對下列事項所負之責任，以本次航行之船舶價值、運費及其他附屬費為限。」**

[101] 我國《海商法》第 70 條第 2 項之規定：「除貨物之性質及價值於裝載前，已經託運人聲明並註明於載貨證券者外，運送人或船舶所有人對於貨物之毀損滅失，其賠償責任，以每件特別提款權六六六・六七單位或每公斤特別提款權二單位計算所得之金額，兩者較高者爲限。」

[102] 新加坡《電子交易法》第 45 條之規定：「授權認證機構的責任限制 除非授權認證機構放棄適用本條規定，否則

a 如果授權認證機構遵守本法規定，依賴一項虛假陳述或僞造的數字簽名而造成損失，該機構對損失不承擔責任；

b 如果標準依據限額是由於下列原因造成擴大的費用，該機構不承擔證書內載明的額外費用：

i 由於依賴證書中關於授權認證機構應當遵守的陳述錯誤而造成損失；

ii 未能遵守第 29 條和 30 條證書發佈的規定。」

以下列兩種方式限制其應負之責任：

(1) 憑證機構就其簽發之各種憑證，得請求當事者及相關當者僅能在特定範圍、特定交易金額內信賴之。

(2) 憑證機構得以與憑證當事者簽訂契約之方式，排除或限制其責任，但該契約必須符合公平原則，亦即故意及重大過失並不得預先免除之。

3. 憑證機構信賴額度(a ecommended reliance limit)[103]

誠如前述，憑證機構信賴額度規範的理由爲：「爲健全今後認證市場的發展，首先必須明定憑證機構及當事者的法律責任，並取得平衡。如果課予憑證機構過多或是不合理的責任，將增加經營者風險，降低民間投資認證事業之意願；另一方面，如不課予使用者善盡保管簽章設施的責任，亦可能會導致使用者疏於保管，影響電子交易的安全。是以，兩者必須取得一個平衡，憑證機構及使用者各應在合理的範圍內，以及可以預期的風險內，負起應負的責任」。

4. 以下茲就各國憑證機構責任相關規定整理如下表[104]：

表 3-4：各國法制對於憑證機構責任規範

國家	賠償責任主體/對象	賠償責任範圍	責任上限	舉證責任
我國	所有憑證機構/賠償對象爲用戶與信賴憑證者	就認證服務錯誤所生之損害	憑證機構就憑證之使用範圍已爲明確限制者，就超過該使用範圍使用所生之損害不負賠償責任	舉證責任倒置
日本	經核可之憑證機構(accredited CSP)		無規定(No provision limiting the liability of CSPs, whether accredited or otherwise)	舉證責任倒置

[103]行政院研考會電子簽章法草案第一版第三十七條立法說明。

[104]資料來源：資策會科技法律中心「電子簽章法修正草案相關法制」座談會會議資料，西元 2005 年 6 月。

韓國	1. 經核定之憑證機構(license CA) 2. 任何信賴憑證者	信賴經認可之憑證所生之損害	因不可抗力之事由所生之損害，經核定憑證機構得減免其責任	舉證責任倒置
香港	經核定之憑證機構(CA)		可在發出憑證時，指明限額，在不同的憑證指明限額、類別、等級(§41) 凡以遵守本法規及業務守則者，不須對因信賴該憑證所受損害負法律責任(§42)	舉證責任倒置
新加坡	經核定之憑證機構(licensed CA)		1. 對於已遵行相關法規而生之信賴損害不負賠償責任 2. 對於超越其憑證明示限額或所建議之信賴程度而生之損害不負賠償責任	
美國聯邦電子簽章法	完全技術中立，不就憑證機構爲任何規範			
美國猶他州數位簽章法(例	1. 經核定之憑證機構(licensed CA) 2. 僅對受直接實質損		1. 憑證機構僅對其憑證所建議之使用範圍負責(46-3-309(1)) 2. 經合併之憑證機構對下列事項不負賠償責任： a. 凡已遵行相關法規，對	

示)	害之信賴憑證者負責		於憑證用戶不實之數位憑證或該憑證受偽造而生之損害不負賠償責任(46-3-309(2)(a)) b. 經核定之憑證機構對超越其建議使用範圍所受不實代表之損害不負賠償責任(46-3-308(2)(b)) c. 受核定之憑證機構僅對直接、實質損害負責，不負懲罰性賠償責任，不對損失利益、精神上之損害負賠償責任(46-3-308(2)(c))	
歐盟 比利時	1.對外簽發或對其合格憑證爲保證的憑證機構 2.任何因合理信賴而受損害的第三者(自然人或法人)	1. 合格憑證資訊之正確性 2. 確保簽章或憑證中之身分證明相符合 3. 確保簽章或憑證資訊之使用與憑證機構所簽發資訊相同	1.針對憑證使用範圍之限制 2.對憑證所適用之交易金額做限制	舉證責任倒置

丹麥 (明示採用歐盟規定)	1.對外簽發或對其合格憑證爲保證的憑證機構 2.任何合理信賴憑證之第三者(包含簽署人)	1.責任條款與歐盟規定相同 2.另增兩款： a.未廢止憑證 b.未提供已廢止憑證資訊或該資訊有誤，未指明有效期限或聲明該憑證之使用限制	1.使用範圍限制與歐盟同 2.該憑證機構不得透過事前合議免除或限縮其法定責任	
芬蘭 (直接採行歐盟規定)	1. 對外簽發或對其合格憑證爲保證的憑證機構 2. 所有信賴憑證之第三者(不論是否合理信賴)	除了歐盟規定外，另增：未廢止憑證之責任(此責任並且適用於向其他憑證機構爲憑證之保證服務的憑證機構)	於憑證中明示使用上限	

愛爾蘭(明示採用歐盟規定)	1. 對外簽發或對其合格憑證爲保證的憑證機構 2. 任何合理信賴憑之人或大眾第三者	1. 與歐盟規定同(但對於部份用語採不同詞彙) 2. 對於過失未註冊登記已廢止憑證的規定與歐盟同	與歐盟同	
瑞典(明示採用歐盟規定)	1. 對外簽發合格憑證之憑證機構 2. 任何信賴憑證者	大致上與歐盟同 此外，須確保簽發及廢止憑證之資料時間之精確	1. 不可免除責任 2. 與歐盟相同之責任上限規定	
英國(明示採用歐盟規定)	對外簽發合格憑證之憑證機構	包含歐盟的所有規定	無明確責任上限之規定 適用普通侵權行爲責任—損害必須滿足法律上之因果關係(必須可預見其損害結果)	

冰島(明示採歐規)	1. 對外簽發合格憑證之憑證機構 2. 正常使用憑證而受損害者	與歐盟同	與歐盟規定相同	舉證責任倒置
德國(採用比歐盟規定更廣義的用語)	簽發合格憑證或合格時戳之憑證機構	違反德國電子簽章法電子簽章服務或其他安全技術未符合憑證機構所使用之標準者		

由上表可知，絕大部分國家立法例均對憑證機構應負之責任內容有明確規範並設定賠償責任上限，並採舉證責任倒置之規範方式，以求平衡法益。茲就亞洲部分國家進一步敘述如下[105]：

(1) 澳洲

澳洲目前的法律並未特別明文規定出憑證服務供應商所應擔負的責任，因此大多參照一般法規或習慣法之原則。而 Gatekeeper 計劃也未提及任何有關憑證服務供應商的責任。

(2) 香港

[105] 同註 85。

香港電子交易條例中對於認可核證機關做出了法律責任限額之規定，除非認可核證機關免除本款對其適用，否則該機關如已就其發出的認可證書遵守本條例的規定及遵守業務守則，即無須就因倚據該證書證明的虛假或僞造的登記人數碼簽署所導致的任何損失負有法律責任。

如認可核證機關已就某認可證書遵守本條例的規定及遵守業務守則，除非該機關免除本款對其適用，否則該機關無須就倚據符合以下說明資訊所導致的損失：

①按照核證作業準則及業務守則屬該機關須確認的；及

②在該證書或儲存庫內是屬失實陳述的，負有超逾在該證書內指明爲倚據限額（reliance limit）的款額的法律責任。

所謂「倚據限額」（reliance limit）指就認可證書的倚據而指明的金錢限額。認可核證機關在發出認可證書時，可在證書內指明倚據限額。而認可核證機關可在不同的認可證書內指明不同的倚據限額，也可在不同的證書類型、類別或種類指明不同的倚據限額。

如有關的事實是因有關認可核證機關的疏忽而屬失實陳述的，或該機關蓄意或罔顧實情地作失實陳述，則上述之責任限額不適用。

若沒有設立法律責任限額，則認可核證機關並需花費許多額外的時間與資源來確認憑證的真僞與有效性，以免除不必要的法律責任，因而可能造成交易速度減緩並且增加交易成本的結果，無法達到電子商務提高服務效率與減少交易成本的目標。

因此，若核證機關必須承擔無限的法律責任，那麼他們可以考慮以增加憑證收費來減少風險之發生，這同樣也對消費者或廠商造成成本增加的負擔，也會阻絕有意進入核證機關業務廠商的意願，因此香港電子交易條例中做出了法律責任限額之規定。

香港電子交易條例中並規定，核證機關可向署長申請成爲就本條例而言的認可核證機關。

(3) 日本

日本電子簽章與認證業務法對於提供不實或不法服務的憑證服務供應商採取加強刑事責任之措施。但日本電子簽章與認證業務法爲對服務供應商之民事責任並無任何的說明。

(4) 馬來西亞

馬來西亞數位簽章法案認爲憑證廠商與儲存庫僅對信賴其憑證所產生的損害與損失負責。因此，馬來西亞數位簽章法案進一步於第 60 條中提出對於憑證機構所不需負責的範圍。其困難點在於如何判別馬來西亞數位簽章法案所建議規範之「合理之信賴」(Reasonable Reliance)，另外亦值得注意的事，馬來西亞數位簽章法案並未提供此憑證機構中因遺漏，而對於「合理之信賴」所造成的影響。除非憑證機構撤銷在第 61 條中馬來西亞數位簽章法案所提供不需負責的損害部份。換言之，即爲由馬來西亞數位簽章法案所認定的自然賠償其損失之部分。

此外，馬來西亞數位簽章法案第 73 條對於憑證廠商若提供不實、不正確或誤導使用者的資訊，將其視爲犯法之行爲，第 74 條第 2 款則列出了刑罰的替代責任。

(5) 中國大陸

中華人民共和國電子簽名法於第 27 條先規定電子簽名人之責任：「如電子簽名人知悉電子簽名製作資料已經失密或者可能已經失密未及時告知有關各方、並終止使用電子簽名製作資料，未向電子認證服務提供者提供真實、完整和準確的資訊，或者有其他過錯，給電子簽名依賴方、電子認證服務提供者造成損失的，承擔賠償責任。」後於第 28 條規定憑證機構亦即所謂電子認證服務提供者之責任：「電子簽名人或者電子簽名依賴方因依據電子認證服務提供者提供的電子簽名認證服務從事民事活動遭受損失，電子認證服務提供者不能證明

自己無過錯的，承擔賠償責任。」等語可知，其採取與我國相同之推定過失責任，並將舉證責任倒置予憑證機構。

(6) 新加坡

新加坡電子交易法第 45 條規定，除非憑證廠商免除本款對其適用，否則若憑證機構業者就其發出的憑證遵守新加坡電子交易法之規定，即無須就該憑證上不實或僞造之數位簽章所導致的任何損失負有法律責任。新加坡電子交易法也允許憑證機構業者在認可證書內指明法律責任限額。

(7) 南韓

爲了保護使用者，韓國電子簽章法規定已核可的憑證機構必須負擔使用者執行或使用憑證服務所造成的損失。然而若損害是由於不可抗力因素所造成，則憑證廠商的責任則會相對減少；若已核可的憑證機構可以證明該項損失與其無關，即可免除損害責任之負擔。

3.4.3 憑證機構可否因電信業主張電信法第二十三條之規定而主張免責

電信法第23條規定：「用戶使用電信事業之電信機線設備，因電信機線設備障礙、阻斷，以致發生錯誤、遲滯、中斷或不能傳遞而造成損害時，其所生之損害，電信事業不負賠償責任，但應扣減所收之費用。」憑證機構提供電子認證服務，須高度仰賴電信事業之電信機線設備，無論係以自建機房或委外主機代管方式均同。依一般民法之觀念，電信業對憑證機構業者所提供之電信服務，就憑證用戶及信賴者而言是憑證機構之履行輔助人，依民法第 224 條規定：「債務人之代理人或使用人，關於債之履行有故意或過失時，債務人應與自己之故意或過失負同一責任。但當事人另有訂定者，不在此限。」則除非憑證機構業者於合約中特別約定，否則在無法得到上游電信業者之賠償下，憑證機構業者尚須爲電信機線設備障礙、阻斷，以致發生錯誤、遲滯、中斷或

不能傳遞導致電子認證服務之中斷，所造成的損害負賠償責任，而無法將此部份之風險轉嫁，實屬失衡。

是故，建議此部份應比照海商法第 69 條之立法意旨作出規範，以使權責平衡，讓憑證機構業者得以發展生存，否則消費者仍是最終結果付出代價者。

3.5 憑證機構與交易主體(憑證註冊者及憑證驗證者)間爭議之處理

在公開金鑰基礎建設架構下，各當事人(憑證機構、憑證註冊者及憑證驗證者)間如有下述態樣之爭議時應如何處理？試分別討論如下：

1. 合法簽發之電子憑證推定

意即須依電子簽章法成立之憑證機構方受合法簽發電子憑證之推定，方受電子簽章法之保護。

2. 電子憑證上資訊真正之推定

一般而言，電子憑證上一般會記載之資訊如下：

(1) 當事者之姓名。該姓名如有被誤認之虞者，應附加名號或代號。

(2) 與簽章者私鑰相配對之公鑰。

(3) 簽章使用之加密演算法概要。

(4) 憑證之序號。

(5) 憑證之效期。

(6) 簽發者之名稱。

(7) 憑證之相關限制條件。

(8) 憑證機構之簽章。

原則上，在電子憑證有效期間內及使用範圍內，上述電子憑證上記載之內容會被推定爲真正。

3. 數位簽章真正之推定

就立法技術而言，有雙軌制及單軌制之立法例：

(1) 雙軌制：依當事人雙方約定之技術或是用經主管機關核定之安全技術及程序所製作之數位簽章，會被推定爲真正。

(2) 單軌制：僅依當事人以約定之安全技術程序所製作之數位簽章即可推定爲真正。

4. 數位簽章產生時間之推定

此即時戳(Time Stamp)服務之內容，就好比實體世界的「郵戳爲憑」，時戳所扮演的角色即爲數位化的郵戳，是資訊時代不可或缺的安全機制，時戳可以爲任何電子文件或電子交易提供準確的時間證明，並且驗證文件或交易的內容自蓋上時戳後是否曾被人修改過，電子時戳將一份訊息/文件與某特定時間關聯起來以證明該文件在某一時點就已存在，即使憑證已過期或取消仍具備不可否認性的功能。

而所謂之時戳，係指一種標記，能夠標示當事人間之通信或交易行爲發生之正確日期與時間，以及標示發送或接收此時間戳記之人或裝置。藉由時戳服務，我們也可以推定數位簽章產生之時間。

5. 電子文件收發文時間及地點之推定

關於此部分前已述及，故不在此贅述。原則上，電子文件收發文時間推定之基準，發文時間是以電子文件完成傳送時爲準；收文時間則是以收受者得取出該項文件時爲準。而電子文件收發文地是尊重當事人的約定，在當事人未爲約定或是約定不明時，其決定的標準爲：

(1) 發文地：以發送者主要執行業務之所在地爲發文地。

(2) 收文地：以收受者主要執行業務之所在地爲收文地。

(3) 在發送者無主要執行業務場所者，以其住所爲發文地。

四、檢討我國現行法對憑證機構之規範法制

誠如前述，我國「電子簽章法」於民國 90 年 11 月 14 日由總統明令公布，行政院並於民國 91 年 1 月 16 日以院臺經字 0910080314 號函發布自 91 年 4 月 1 日施行，於民國 91 年 4 月 1 日正式施行至今。其立法目的依第 1 條：「爲推動電子交易之普及運用，確保電子交易之安全，促進電子化政府及電子商務之發展，特制定電子簽章法。」規定，即知係作爲國內推動電子商務發展及電子化政府之法源依據，並賦予符合一定要件之電子文件、電子簽章與實體的書面文件或簽章能具有同等之法律效力。

有鑒於數位憑證技術目前雖已臻成熟，然其相關應用及商業模式，目前卻仍尚在發展階段，爲鼓勵電子認證產業的多元發展，避免政府因對於起步中的電子認證產業限制過多而侷限其應用，因此電子簽章法對於憑證機構之管理規範，採尊重市場機制自由發展的模式，降低對於認證業務經營之限制，以促進國內憑證相關產業的蓬勃發展。然而，憑證機構既扮演公正第三人的角色簽發憑證，若政府完全放任其經營而不適度介入規範，恐難保障使用憑證之消費者或信賴憑證之第三人的權益。爲兼顧扶植產業發展及保障消費者權益兩目的，電子簽章法乃採規範憑證實務作業基準應載明事項之管理方式，賦予主管機關適當程度介入監督認證相關服務的權力，來維護保障消費大眾之權益。

依據電子簽章法第 3 條、第 16 條、第 11 條第 2 項第 5 款及第 15 條第 2 項之授權，主管機關經濟部制定三部相關子法：「電子簽章法施行細則」、「憑證實務作業基準(Certificates Practice Statsment,簡稱 CPS)應載明事項準則」及「外國憑證機構許可辦法」。

茲就電子簽章法及 3 部子法關於憑證機構管理之規範一一臚列說明如下：

4.1 電子簽章法

4.1.1 現行條文

表 4-1：電子簽章法第 11 條至第 15 條條文內容

第 11 條	憑證機構應製作憑證實務作業基準，載明憑證機構經營或提供認證服務之相關作業程序，送經主管機關核定後，並將其公布在憑證機構設立之公開網站供公眾查詢，始得對外提供簽發憑證服務。其憑證實務作業基準變更時，亦同。 憑證實務作業基準應載明事項如下： 一、足以影響憑證機構所簽發憑證之可靠性或其業務執行之重要資訊。 二、憑證機構逕行廢止憑證之事由。 三、驗證憑證內容相關資料之留存。 四、保護當事人個人資料之方法及程序。 五、其他經主管機關訂定之重要事項。 本法施行前，憑證機構已進行簽發憑證服務者，應於本法施行後六個月內，將憑證實務作業基準送交主管機關核定。但主管機關未完成核定前，其仍得繼續對外提供簽發憑證服務。 主管機關應公告經核定之憑證機構名單。
第 12 條	憑證機構違反前條規定者，主管機關視其情節，得處新臺幣一百萬元以上五百萬元以下罰鍰，並令其限期改正，逾期未改正者，得按次連續處罰。其情節重大者，並得停止其一部或全部業務。
第 13 條	憑證機構於終止服務前，應完成下列措施： 一、於終止服務之日三十日前通報主管機關。 二、對終止當時仍具效力之憑證，安排其他憑證機構承接其業務。 三、於終止服務之日三十日前，將終止服務及由其他憑證機構承接其業務之事實通知當事人。

	四、將檔案記錄移交承接其業務之憑證機構。 若無憑證機構依第一項第二款規定承接該憑證機構之業務，主管機關得安排其他憑證機構承接。主管機關於必要時，得公告廢止當時仍具效力之憑證。 前項規定，於憑證機構依本法或其他法律受勒令停業處分者，亦適用之。
第 14 條	憑證機構對因其經營或提供認證服務之相關作業程序，致當事人受有損害，或致善意第三人因信賴該憑證而受有損害者，應負賠償責任。但能證明其行爲無過失者，不在此限。 憑證機構就憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，不負賠償責任。
第 15 條	依外國法律組織、登記之憑證機構，在國際互惠及安全條件相當原則下，經主管機關許可，其簽發之憑證與本國憑證機構所簽發憑證具有相同之效力。 前項許可辦法，由主管機關定之。 主管機關應公告經第一項許可之憑證機構名單。

4.1.2 現行條文檢討

1. 電子簽章法第 11 條：

(1) 應製作「憑證實務作業基準」之憑證機構，應僅限於對外提供簽發憑證服務之憑證機構；未對外提供簽發憑證服務之憑證機構，因屬僅供企業內部使用，故不必製作，應在此處增列區分清楚。

(2) 應於現行書面審查規範外，增訂實質審查機制，亦即：憑證機構應另行繳交外部稽核機構之稽核報告等相關文件，一併送經主管機關核定後，始得對外提供憑證簽發服務，以確保憑證機構之營運狀況與憑證憑證實務作業基準之記載一致，理由如下：

①現行憑證機構之核定，係採書面審查制度，即憑證機構製作憑證實務作業基準送經主管機關書面審查核定後，即可對外提供憑證簽發服務。前已論及，爲增加憑證機構提供服務品質之可信賴性，及爲與國際接軌而採行同等級之憑證機構管理制度，同時爲推行憑證互通機制，均有增訂實質審查機制之必要性。

②蓋憑證機構之功能，即在於證明電子簽章所有人之身分或資格之真實性，並且以證明書之「憑證」方式提供憑證服務，且憑證機構於實際電子交易機制中，是讓交易雙方得以藉由該「憑證」之存在，而確認彼此身分，進而建立電子交易之信賴關係。具體而言，憑證機構之嚴格認證程序，在實務操作上即可從三個面向觀察，即憑證機構作業實務之揭露、憑證機構完整性控制及憑證機構安全性控制。因此，憑證機構之信賴核心既爲嚴格認證程序之要求，惟憑證機構是否確實執行嚴格認證程序，事實上一般人是無法知悉。雖然爲促進大眾信賴，憑證機構之作業程序依照嚴格認證程序之要求而須公布「憑證實務作業基準」以作爲大眾參考之指標。然「憑證實務作業基準」僅係憑證機構之單方聲明事項及處理憑證之程序說明，是否確有落實執行憑證核發應進行之作業程序之規定，一般社會大眾是難以知悉與了解。

③因此，爲避免憑證機構有「說是一套，作是一套」之情形發生，以讓憑證機構能「說到做到」，應由憑證機構以外之第三人以公正之地位確實查核憑證機構是否落實執行「嚴格認證程序之要求」以及確實依照「憑證實務作業基準」之規定簽發憑證，是讓憑證機構取得「信賴性」之關鍵。透過公正第三人查核憑證機構之作業程序規定及管理狀況後，將可檢視憑證機構之可信賴度，而作爲「信賴服務提供者」地位之憑證機構始有確實憑據得以「宣稱」憑證機構有「值得信賴之基礎」。爲達到憑證機構確實執行嚴格認證程序之要求，讓憑證機構簽發憑證之作業具有可信賴性，我們藉由公正第三者進行實地查核程序，查核憑證機構之管理方式與簽發憑證之

方法不但符合「嚴格認證程序」之　要求，並且符合一定之安全程序標準，即所謂爲「外部稽核制度」。

④簡言之，建議採行增訂實質審查機制之原因即在於：作爲提供認證服務第三公正單位的憑證機構，其核心價值即在是否具有「可信賴性之基礎」，經由公開揭露憑證機構「憑證實務作業基準」之方法，雖具有憑證機構營運透明化之功能，但仍僅止於是憑證機構之單方「宣稱」之「主觀可信賴性」。

⑤在憑證機構採取許可制之制度下，且基於憑證機構之信賴本質思考復加憑證機構之市場價值考量，其外部稽核制度即應採取強制稽核制度較爲所宜。

⑥因此，爲讓憑證機構具有客觀之「信賴性基礎」並且確保憑證機構確實落實「嚴格認證程序」之信賴要求[106]，於電子簽章法日後修法之際，將憑證機構之強制稽核制度納入修法之範圍，以讓憑證機構提供之「信賴性服務」更具有說服力。

(3) 關於主管機關訂定有關憑證機關之核定，提供憑證服務之營運管理監督辦法及憑證實務作業基準等規範均未見法條中有明確授權，建議應予增訂。

(4) 本條第 3 項係立法當時之過度條款，今既電子簽章法已施行逾三年，此項規範已無存在實益，故建議於修法時一併予以刪除。

2. 電子簽章法第 12 條：

(1) 爲避免輕罪重罰之情形產生，故在立法技術上，應賦予憑證機構補正之機會及主管機關裁量權，視違反情節輕重決定是否處罰。此論點係基於行政罰法理上之「便宜原則」，即「合義務性的裁量」，處罰機關對於一個輕

[106] 普華資安股份有限公司，「我國憑證機構稽核制研究報告」，民國91年12月20日，頁39，http://www.pki.org.tw/Resource/Report/021230_%A7%DA%B0%EA%BE%CC%C3%D2%BE%F7%BAc%BD]%AE%D6%A8%EE%AC%E3%A8s%B3%F8%A7i.pdf，2007/07/30 visited。

微違反義務之行爲，就具體事實狀況認爲以不處罰爲適當時，得決定不爲處罰，即吾人所稱之「決定裁量」亦即「裁處之審酌、加減及擴張」[107]。

(2) 憑證機構違反電子簽章法第 11 條規定，情節輕重有所不同，罰鍰直接以一百萬元作爲最低處罰標準係屬過重，故建議刪除罰鍰下限，由主管機關依職權自行裁量。

3. 電子簽章法第 13 條：

(1) 本條第一項就文義而言，係規範所有憑證機構，並未區分是否經主管機關許可或核定之憑證機構，一律均須待完成法定程序後方能終止服務，如此並不符合經濟效益，故應明定規範主體限於經主管機關許可或核定之憑證機構。

(2) 同條同項第 1 款就憑證機構終止業務之通知期間，爲使主管機關及相關當事人有充足之時間就相關事宜予以因應，並求行政作業之明確化，故建議憑證機構終止服務應至少提早於六十日前通報主管機關。

(3) 同項第 1 款就憑證機構終止業務後主管機關安排其他憑證機構承接業務之規定，依現行技術與實務情況實施實有困難，且依憑證實務作業基準應載明事項準則第 28 條之規定，憑證機構已於其憑證實務作業基準載明其對於終止服務之相關計畫，對用戶權益已作相當之保障，因此建議刪除。

4. 電子簽章法第 14 條：

從對價關係及風險平衡原則考量，憑證用戶當事人與善意第三人因信賴憑證而受有損害者，二者因法益受侵害之程度不同，故法律應給予不同程度之保護，意即憑證機構應負之損害賠償責任輕重應有所不同，且二者均應有責任限

[107] 蔡振榮、鄭善印著，行政罰法逐條釋義，一版二刷，新學林出版股份有限公司，台北，2006 年 9 月，頁 52 至 53。

制。故建議憑證機構對憑證用戶當事人維持現行法推定過失責任，而對善意第三人應回歸過失責任。

5. 電子簽章法第 15 條第 2 項：

就實務運作所需及立法技術而言，外國憑證許可辦法應包含許可要件、程序及廢止許可等，故應增列授權範圍予以納入，以求明確。

4.2 電子簽章法施行細則

4.2.1 電子簽章法施行細則規範重點

主管機關依據電子簽章法第 16 條的授權，制定「電子簽章法施行細則」，就電子簽章法施行一些相關的細節性及技術性事項予以補充。

爲了明確規範那些憑證機構務必製作並將其憑證實務作業基準送請主管機關核定，施行細則第 7 條明定「對外簽發憑證服務憑證機構」之認定方式，說明哪些憑證機構屬於電子簽章法第 11 條第 1 項所謂的「對外提供簽發憑證服務」，只有當該憑證機構所簽發的憑證，是讓憑證使用者與憑證機構以外之第三人簽署電子文件時作爲證明之用，才有將其憑證實務作業基準送審之義務。

而施行細則中何以針對「對外」提供簽發憑證服務的憑證機構採比較嚴格的規範，實因「對外」提供服務的憑證機構所扮演的是公正第三人之角色，相當於網路上「戶政事務所」，負責簽發憑證及驗證服務。這和一般企業提供給企業內部員工或基於雙方信賴關係所提供之憑證服務有所不同，因而對外提供服務憑證機構的可信賴與否，攸關消費者權益甚鉅，所以電子簽章法對於「對外」提供服務憑證機構有較嚴格的規範。

另一方面，若不是「對外」提供簽發憑證服務之憑證機構，例如：僅簽發數位憑證供內部員工使用的企業，並沒有將憑證實務作業送請主管機關核定之義務。但依電子簽章法規定，經主管機關核定憑證實務作業基準之憑證機構所簽發之數位憑證，才會有等同於實體簽名蓋章之法律效力，所以這些「非對外」

簽發憑證之憑證機構若想使其所簽發之數位憑證具有法律上之效力，亦必須製作憑證實務作業基準並將其送請主管機關核定。

4.2.2 電子簽章法施行細則條文內容及說明

表 4-2：電子簽章法施行細則條文內容及說明

條文內容	條文說明
第 5 條：本法第 2 條第 5 款所稱簽發憑證之機關、法人，係指憑證上所載之簽發名義人。	明定憑證機構之認定方式。
第 7 條：電子簽章法第 11 條第 1 項所稱對外提供簽發憑證服務，係指憑證機構簽發之憑證，可供憑證用戶作爲其與憑證機構以外之第三人簽署電子文件時證明之用者。	1.明定電子簽章法第 11 條第 1 項所稱對外提供簽發憑證服務之定義，以明確界定應製作憑證實務作業基準送主管機關核定之憑證機構之範圍。 2.憑證機構對外提供簽發憑證服務者，係基於公正第三人之地位提供簽發憑證服務，其可信賴性攸關民眾利益甚鉅，電子簽章法第 11 條第 1 項課予其製作憑證實務作業基準送主管機關核定之義務，電子簽章法第 12 條並訂有罰則。 3.爲明確界定依電子簽章法須送請主管機關核定憑證實務作業基準之憑證機構範圍，爰參酌產業發展與實務現況，明定對外簽發憑證服務憑證機構之認定方式，以杜爭議。

第 8 條：憑證機構依電子簽章法第 11 條第 1 項及第 3 項規定，就其所製作憑證實務作業基準向主管機關申請核定者，應檢具下列文件： 一、申請書； 二、憑證實務作業基準； 三、憑證實務作業基準應載明事項檢核對照表； 四、其他經主管機關指定之文件。	明定憑證機構依電子簽章法規定申請核定之程序。
第 9 條：憑證機構製作之憑證實務作業基準變更時，依電子簽章法第 11 條第 1 項規定，向主管機關申請核定者，應檢具下列文件： 一、申請書； 二、變更後之憑證實務作業基準及其應載明事項檢核對照表； 三、變更內容對照表； 四、其他經主管機關指定之文件。	明定憑證機構擬變更經核定之憑證實務作業基準時，依電子簽章法第 11 條第 1 項規定申請核定應提出變更申請之程序。
第 10 條：憑證機構依電子簽章法及本細則規定所為之申請，其應備具之文件，應用中文書寫；其科學名詞之譯名，以國立編譯館規定者為原則，並應附註外文原名。 前項文件原係外文者，並應檢附原外文資料或影本。	鑑於憑證實務作業基準內容多涉及專業技術性名詞，其中並多係外文之翻譯名詞，為便利核定程序之進行，特明定申請文件應使用之語文，及檢附外文原名及原外文資料或影本之義務。

第 11 條：電子簽章法第 13 條第 1 項第 4 款所稱檔案紀錄，應包括下列資料： 一、憑證用戶註冊資料。 二、已簽發之所有憑證。 三、用戶憑證廢止清冊。 四、憑證狀態資料。 五、各版本之憑證實務作業基準。 六、憑證政策。 七、稽核或評核紀錄。 八、歸檔資料。 九、其他經主管機關指定之文件。 前項第 1 款所定之憑證用戶註冊資料，於憑證用戶有反對之表示者，不適用之。	爲明確憑證機構終止服務應進行之程序，明定電子簽章法第13條第1項第4款所稱檔案紀錄應包括之資料。

4.3 憑證實務作業基準應載明事項準則

所謂「憑證實務作業基準」，依電子簽章法第 2 條第 7 款之規定，係指「由憑證機構對外公告，用來陳述憑證機構據以簽發憑證及處理其他認證業務之作業準則」。依據最早對於憑證實務作業基準加以定義之「美國律師協會」(American Bar Association) 所提供之說明，憑證實務作業基準的形式，可能是憑證機構對於其值得信賴的系統(Trustworthy System) 以及操作與發證相關實務上之細節的聲明或相關規則，也可能是憑證機構與用戶間契約的一部份。就內容上而言，憑證實務作業基準是憑證機關對其作業的細節的陳述，現行實務上，憑證實務作業基準多是相當複雜的一種對於憑證機關所提供的具體服務，包括憑證生命週期(Life Circle)、安全控管等之管理措施所爲的詳細的描述。各

憑證機構所製作之憑證作業基準，因其簽發憑證及處理其他認證業務之作業程序及其營運方式不同而有所不同，而各憑證實務作業基準的詳盡程度亦不盡相同。

爲確保一般憑證使用者得以透過憑證機構所揭露之經營及服務相關資訊，判別憑證機構之可信賴性及憑證機構所發憑證之適用性，電子簽章法第 11 條規定，凡是對外提供簽發憑證服務之憑證機構，即該憑證機構所簽發的憑證，爲憑證使用者與憑證機構以外之第三人簽署電子文件時作爲證明之用者，均必須製作載明其經營或提供認證服務之相關作業程序之憑證實務作業基準送請主管機關核定。各憑證機構所製作之憑證實務作業基準，因其簽發憑證及處理其他認證業務之作業程序及其營運方式而有所不同，而各憑證實務作業基準的詳盡程度亦不盡相同，但送請主管機關核定之憑證實務作業基準則至少必須依主管機關所規定之標準載明清楚。其規範目的，除作爲主管機關管理之依據[108]外，同時在於協助憑證機構就其所提供之認證服務所應注意之相關事項妥善規劃，減少相關爭議產生，以提供更完善良好認證服務。

申言之，憑證機構送請主管機關核定並對外公開之「憑證實務作業基準」，爲憑證機構所對外揭露，據以簽發憑證、提供其他認證業務等具體服務之作業準則，包括憑證生命週期、安全控管等管理措施、進行簽發憑證程序等相關服務之完整規劃。實際上，憑證用戶往往透過各憑證機構之憑證實務作業基準，了解其所提供認證服務之條件，選擇符合需求之憑證產品。從法律的觀點來看，憑證機構於公開網站上公告憑證實務作業基準，即爲向不特定多數人承諾依其所載內容提供服務，依此，憑證用戶可依憑證實務作業基準之內容向憑證機構主張權利。換言之，憑證實務作業基準相當於憑證機構就其所提供服務提出之保證，憑證機構自須確實按照其對外公開之憑證實務作業基準所記載事項提供具體服務，就憑證實務作業基準之內容負誠實履行之善良管理人注意義務。倘

[108] 爲兼顧扶植產業發展及保障消費者權益兩目的，電子簽章法乃採規範憑證實務作業基準應載明事項之管理方式，賦予主管機關適當程度介入監督相關憑證服務契約的權力，來維護保障消費大眾之權益。

若憑證機構違反其義務而產生損害，依電子簽章法第十四條，憑證機構須負損害賠償責任。

4.3.1 法規沿革

1. 憑證實務作業基準應載明事項

承上所述，我國目前對於憑證機構之管理，僅規範憑證機構應有對外揭露之義務，依據電子簽章法第 11 條第 2 項之規定：「憑證機構應製作憑證事務作業基準，載明憑證機構經營或提供認證服務之相關作業程序，送經主管機關核定後，並將其公布在憑證機構設立之公開網站供公眾查詢，始得對外提供簽發憑證服務。」並未規定憑證機構應對外公開作業原則之事項。為促進產業發展初期完善營運規劃，確保憑證機構就相關重要事項已擬定公開明確之處理政策與作業程序，以利消費者判斷憑證機構就相關重要事項已擬定公開明確之處理政策與作業程序，以利消費者判斷憑證機構服務之可信賴性、減少消費糾紛及促進交易秩序之安定，主管機關爰依電子簽章法第 11 條第 2 項之規定第 5 款之授權訂定「憑證實務作業基準應載明事項」。行政院並於民國 91 年 1 月 25 日以經商字第 09002274000 號公布，目的即在於協助憑證機構就其認證服務提出妥善完整之規劃，並維護消費者知之權益。

(1) 憑證實務作業基準應載明事項規範重點

我國憑證實務作業基準應載明事項原則上依循目前國際上廣泛接受之憑證實務作業基準內容規範（RFC 2527 : Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework ）[109]訂定，全文

[109] RFC2527：「網際網路工程任務小組」(Internet Engineering Task Force; IETF)於 1999 年所公布之第 2527 號 RFC 文件：「網際網路 X.509 公開金鑰基礎建設憑證政策與憑證實務作業基準綱要」(Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework)。

共計七章 48 點，其規範重點包括：

①憑證機構應於其憑證實務作業基準之首頁，摘要並載明足以影響憑證使用者或信賴憑證者對於憑證信賴度的重要事項，以確保憑證使用者及信賴憑證者能夠特別注意該等攸關其權益之重要事項，包括：

（i）主管機關核定文號；

（ii）憑證保證等級及適用範圍；

（iii）有關法律責任之重要事項。

②憑證機構應在其憑證實務作業基準中，應載明：

（i）憑證使用者及信賴憑證者應盡義務之教示條款，以確保憑證使用者明瞭其應盡之責任與憑證正確使用之方式；

（ii）爲確保其依據所定憑證實務作業基準營運所進行之稽核、評核等措施以及憑證機構就其可能擔負之法律責任所做之財務準備；

③憑證之申請、停用、廢止等程序，以便憑證使用者了解憑證機構對於憑證生命週期之管理，以判斷其管理之可信賴性並了解使用者享有之相關權利；

④爲其所提供之憑證服務所進行之各項技術性及非技術性安全控管及所其依循之國際標準，以便憑證使用者判斷其可信賴性；

⑤就其服務相關個人資料所提供之保護方法，以及客戶權益相關事項之通知程序。

⑵ 憑證實務作業基準應載明事項準則

隨著憑證應用日益多元之發展，爲因應國內各式各樣新興之交易模式，以及近來國際 PKI 互通及相互承認等議題發展，與國際間對於憑證機構實務作業之重要事項之更新認識，故主管機關針對憑證機構之審查要求，依循國際相關標準作調整。因此，經濟部於民國 93 年 7 月 7 日以經商字第 09302102450 號函公布「憑證實務作業基準應載明事項準則」，並同時以經商字第 09302114690

號函廢止「憑證實務作業基準應載明事項」，俾使我國法制歸範能充分配合實務發展需求並落實規範目的。

(3) 訂定「憑證實務作業基準應載明事項準則」及廢止「憑證實務作業基準應載明事項」所依循之原則如下[110]：

① 最小變動原則

爲維護已通過核定業者之權益，並避免因法規之訂定與廢止造成業者業務衝擊，「憑證實務作業基準應載明事項準則」係在必要之範圍內以現行管理機制最小變動原則而訂定。

② 必要性原則

憑證實務作業基準應載明事項本身主要之目的，在於維護消費者知的權利，如過度龐雜將使消費者因閱讀困難而望之卻步，徒增核定程序之繁複。因此，「憑證實務作業基準應載明事項準則」僅將維護消費者權益之必要事項列爲應載明之事項。

③ 明確性原則

由於「憑證實務作業基準應載明事項準則」之訂定目的係爲核定憑證機構之主要依據，故規範內容及文字應力求明確，以達成規範明確性之要求爲原則。

④ 國際性原則

憑證實務作業基準之相關規範，如自外於國際發展趨勢而閉門造車，恐將造成業者在國際化經營之困難。因此，「憑證實務作業基準應載明事項準則」係本著國際性之原則、遵循國際發展趨勢而訂定，以利於未來跨國承認工作之進行。

(4)「憑證實務作業基準應載明事項準則」訂定重點[111]

「憑證實務作業基準應載明事項準則」內容分爲六章共 35 條，

---

[110] 經濟部商業司，2004 台灣 PKI 年鑑，第一版，經濟部，台北，民國 93 年 10 月，頁 52。

[111] 同註 110，頁 54。

由上可知，「憑證實務作業基準應載明事項準則」篇幅較「憑證實務作業基準應載明事項」更爲精簡，其內容除明定法源依據與名詞定義外，其他規範憑證機構應於其憑證實務作業基準中載明之重點如下：

①影響消費者對於憑證機構與其作業基準記載信賴之重要事項以及用戶與信賴憑證者應注意事項；

②憑證機構之財務責任與處理認證服務或憑證之使用所生糾紛之處理程序與所適用之法律以及請求退費之程序；

③稽核或評核事項與其應保護用戶個人資料之種類與維持資訊保密之方法；

④識別與鑑別申請與接受憑證之程序以及憑證暫時停用與憑證廢止之事項；

⑤憑證機構所採行之非技術性安全控管措施，包括其所採行之實體運作程序以及人員安全之控管措施、紀錄歸檔事項、憑證機構金鑰變更實之處理程序危害與災變復原程序之規劃以及終止憑證服務之處理程序；

⑥憑證機構所採行之技術性安全控管措施，包括其金鑰對產製及安裝私密金鑰保護憑證有效期間、公開金鑰是否歸檔與公開金鑰及私密金鑰個別之使用期限、啓動資訊保護以及其所採行之系統軟體及網路安全控管措施；

⑦憑證與憑證廢止清冊格式剖繪(Profile)[112]之事項。

4.3.2 憑證實務作業基準應載明事項與憑證實務作業基準應載明事項準則二者之比較

1. 相較於原有多達 48 點之「憑證實務作業基準應載明事項」，「憑證實務作業基準應載明事項準則」之主要變動如下：

(1) 新增名詞定義，例如：「憑證實務作業基準應載明事項準則」於第 2 條說明「啓動資訊」之用語定義，以利審查實務作業依據。

[112] 描述資料定義或格式之文件。

(2) 「憑證實務作業基準應載明事項準則」中並未就註冊中心之定義與註冊中心及憑證機構間關係爲規定，以避免似有允許憑證機構於憑證實務作業基準中排除依「電子簽章法」第 14 條應負之賠償義務之嫌，以杜絕子法之規範逾越母法之疑義。

(3) 「憑證實務作業基準應載明事項準則」中，新增憑證實務作業基準首頁應記載之重要事項，其第 3 條規範憑證機構必須於其作業基準首頁，記載所提供之認證服務是否經第三人稽核或取得任何標章，以確保消費者知的權益，並規範憑證機構若有補充其作業基準內容之其他重要文件(例如：合約或技術規範等)，應於憑證實務作業基準中加以記載，使消費者能判別憑證實務作業基準記載內容可能因此有所補充或調整。

(4) 基於必要性原則，將僅消費者權益之必要事項始列爲應載明事項：由於在實際狀況憑證機構就認證服務所應收取之費用，大都已於其公開網站明列供大眾瀏覽查詢，而且在法理上依契約自由原則及民法第 153 條第 2 項[113]之意旨，當事人應對契約必要之點意思表示一致契約方成立。因此雙方對於認證服務契約中約定費用應達成合意契約始能成立，故於「憑證實務作業基準應載明事項準則」中刪除憑證機構應於其作業基準中載明查詢費用之方法，以符合私法自治之精神與低度管理之原則。

(5) 「憑證實務作業基準應載明事項準則」中將紀錄歸檔之事項、金鑰變更程序、危害與災變復原程序以及終止，任一憑證簽發服務時之處理程序等條文配合 RFC3647[114]文件之章節調整，由原應載明事項「營運規範」章節中調整至第四章「非技術控管」加以規範。

---

[113] 我國《民法》第 153 條第 2 項之規定：「當事人對於必要之點，意思一致，而對於非必要之點，未經表示意思者，推定其契約爲成立，關於該非必要之點，當事人意思不一致時，法院應依其事件之性質定之。」

[114] RFC3647：「網際網路工程任務小組」(Internet Engineering Task Force; IETF)於 2203 年 11 月所公布之第 3647 號 RFC 文件：「網際網路 X.509 公開金鑰基礎建設憑證政策與憑證實務作業基準綱要」(Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement

(6) 「憑證實務作業基準應載明事項準則」刪除原「憑證實務作業基準應載明事項」的第七章「憑證實務作業基準之維護」，並將憑證實務作業基準變更時通知之方法修正調整至「憑證實務作業基準應載明事項準則」的總則第10 條加以規範。

2. 「憑證實務作業基準應載明事項」內容分爲七章共 48 條，而「憑證實務作業基準應載明事項準則」內容分爲六章共 36 條，茲將二者整理比較如下表:

表 4-3：憑證實務作業基準應載明事項與憑證實務作業基準應載明事項準則二者之比較表：

憑證實務作業基準應載明事項準則	憑證實務作業基準應載明事項	說明
第一章 總則	第一章 總則	
第1條：本準則依電子簽章法第11條第2項規定訂定之。	第1條：本應載明事項依電子簽章法第11條第2項之規定訂定之。	本條未修正。
第 2 條：本準則用詞之定義如下： (1)保證：指得據以信賴該個體已符合特定安全要件之基礎。 (2)保證等級：指在具相對性保證層級中之某一級數。 (3)憑證政策：指爲指明某一	第 2 條：本應載明事項用辭之定義如下： (1)保證：指得據以信賴該個體已符合特定安全要件之基礎。 (2)保證等級：指在具相對性保證層級中之某一級數。 (3)憑證政策：指爲指明某一憑證所適用之對象或情況所列	一、刪除原(7)註冊中心及(9)憑證廢止清冊中的「並可供信賴憑證者使用」。 二、增加(9) 啓動資訊。

Framework)訂定，其爲國際間評鑑憑證機構參酌之重要文件，亦爲目前國際公認之憑證實務作業基準內容之基本規範。

憑證所適用之對象或情況所列舉之一套規則，該對象或情況可爲特定之社群或具共同安全需求之應用。 (4)物件識別碼：指一種以字母或數字組成之唯一識別碼，該識別碼必須依國際標準組織所訂定之註冊標準加以註冊，並可被用以識別唯一與之對應之憑證政策；憑證政策修訂時，其物件識別碼不必然隨之變更。 (5) 用戶：指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰者。 (6)信賴憑證者：指信賴所收受之憑證者。 (7) 儲存庫：指用以儲存及供檢索憑證與其他相關憑證資訊之系統。 (8) 憑證廢止清冊：指由憑證機構以數位方式簽署之已廢止憑證表列。 (9) 啓動資訊：操作密碼模	舉之一套規則，該對象或情況可爲特定之社群或具共同安全需求之應用。 (4)物件識別碼：指一種以字母或數字組成之唯一識別碼，該識別碼必須依國際標準組織所訂定之註冊標準加以註冊，並可被用以識別唯一與之對應之憑證政策；憑證政策修訂時，其物件識別碼不必然隨之變更。 (5)用戶：指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰者。 (6)信賴憑證者：指信賴所收受之憑證及得以憑證中所載公開金鑰加以驗證之數位簽章者，或信賴憑證中所命名主體之身分(或其他屬性)及憑證所載公開金鑰之對應關係者。 (7)註冊中心：指負責確認憑證申請人之身分或其他屬性，但不簽發憑證亦不管理憑證者。註冊中心是否單獨爲其行	

組時所要求且必須被保護之金鑰以外資料值。	爲負責及其應負責任之範圍，依所適用之憑證政策或協議定之。 (8)儲存庫：指用以儲存與供檢索憑證或其他憑證相關資訊之值得信賴系統。 (9)憑證廢止清冊：指由憑證機構以數位方式簽章，並可供信賴憑證者使用之已廢止憑證表列。	
第 3 條：憑證機構應製作憑證實務作業基準(以下簡稱作業基準)重要事項置於其作業基準之首頁，載明下列事項： (1)主管機關核定文號。 (2)所簽發之憑證種類。 (3)所簽發各種憑證之保證等級。 (4)所簽發各種憑證之適用範圍及使用限制。 (5)法律責任限制及申請廢止憑證處理期間內之責任分擔。 (6)其作業基準所描述的認證	第 3 條：憑證機構應於其憑證實務作業基準（以下簡稱作業基準）之首頁摘要載明足以影響用戶或信賴憑證者對於憑證之信賴之重要事項，並應包括下列項目： (1)主管機關核定文號。 (2)所簽發之各種類憑證，其保證等級及適用範圍等重要特徵。 (3)有關法律責任之重要事項。	主要增列第(6)款：其作業基準所描述的認證服務是否經第三人稽核或取得任何標章。

服務是否經第三人稽核或取得任何標章。		
第4條：憑證機構應於其作業基準中載明其所支援憑證政策之名稱，並提供該憑證政策之物件識別碼及應載明補充其作業基準內容之其他重要文件。	第4條：憑證機構如支援特定之憑證政策，應指明該等政策，並提供該憑證政策之物件識別碼。	將原規範要求列於作業基準內容。
第5條：憑證機構應於其作業基準中載明參與認證服務運作及維持之重要成員及其分工；如係以委外方式參與提供服務者，並應載明受任者之名稱或資格。	第 5 條：憑證機構應於其作業基準中識別參與認證服務運作及維持之主要成員及其角色，並應包括下列項目： (1)擔任憑證機構者。 (2)是否設有註冊中心；如設有註冊中心，註冊中心與憑證機構間之關係。 (3)用戶及信賴憑證者之資格。 (4)以委外方式提供之主要認證服務。	刪除原(1)至(3)款。

	第 6 條：憑證機構對於憑證之適用範圍應於其作業基準中載明下列項目： (1)所發各種憑證適合之應用。 (2)表列所發憑證使用上之限制。 (3)表列所發憑證禁止使用之情況。	本條刪除。
第6條：憑證機構應於其作業基準中載明可供用戶或信賴憑證者報告遺失私密金鑰等事件及諮詢作業基準疑義之聯絡電話、郵遞地址及電子郵件信箱。	第7條：憑證機構應於其作業基準中載明至少一個聯絡電話、郵遞地址及電子郵件信箱，以供用戶或信賴憑證者報告遺失金鑰等事件。	修正文字描述。
	第8條：憑證機構應於其作業基準中載明該機構及註冊中心就其所提供服務所承擔之職責和義務。	本條刪除。
第7條：憑證機構應於其作業基準中載明下列用戶應注意事項： (1)確保在申請憑證時所提供之資訊正確無誤。 (2)用戶需自行產製金鑰時，安全的產製並保管其私密金	第 9 條：憑證機構應於其作業基準中載明下列憑證用戶應盡之義務： (1)確保在申請憑證時所提供之資訊正確無誤。 (2)安全的產製並保管其私密金鑰。	一、修正第(2)款增列「用戶需自行產製金鑰時」。 二、刪除第 2 項。

鑰。 (3)遵守對於金鑰及憑證之使用限制。 (4) 就私密金鑰資料外洩或遺失等事件作出通知。	(3)遵守對於金鑰及憑證使用之限制。 (4)就私密金鑰資料外洩或遺失作出通知。 憑證機構應於其作業基準中載明該機構所支援之憑證政策內所列之用戶義務重要規定。	
第八條：憑證機構應於其作業基準中載明下列信賴憑證者之注意事項： (1)驗證數位簽章之責任。 (2) 僅於憑證使用目的範圍內信賴該憑證。 (3) 查驗憑證狀態。 (4) 了解有關憑證機構法律責任之條款。	第十條：憑證機構應於其作業基準中載明下列信賴憑證者之注意事項： (1)驗證數位簽章之責任。 (2)僅於憑證使用目的範圍內信賴該憑證。 (3)查驗憑證狀態（是否廢止或暫時停用）。 (4)了解並同意有關憑證機構法律責任之條款。	刪除第(3)款「是否廢止或暫時停用」。
第9條：憑證機構就資訊之公布及儲存庫之維護及營運應載明下列事項： (1) 憑證、憑證狀態、憑證實務作業基準及憑證政策等資訊之公布方法。 (2) 前揭資訊公布之頻率或時間。	第 11 條：憑證機構應於其作業基準中載明該機構就提供儲存庫服務所承擔之義務，並應包括下列事項： (1)正確並及時公布憑證目前狀態相關資訊之義務。 (2)保障儲存庫之安全，並進行存取控制。	簡化規範。

(3) 儲存庫之接取控管。	(3)儲存庫資訊之可接取狀態及可用性。	
第10條：憑證機構應於其作業基準中載明作業基準變更時通知之方法。	第 12 條：憑證機構應針對所提供之各種憑證於其作業基準中分別載明任何與分擔法律責任有關之條款，並應包括下列事項： (1)在用戶或其他有權提出廢止或暫時停用憑證要求者提出要求後，至該機構實際廢止或暫時停止憑證時止之期間內，有關憑證被用以進行交易或其他活動時之處理方法。 (2)設有註冊中心者，憑證機構與註冊中心間之責任分擔。 憑證機構應於其作業基準中載明該機構所支援之憑證政策內所列有關法律責任之重要規定。	簡化規範，刪除各款規定。
第11條：憑證機構應於其作業基準中載明下列財務責任事項： (1) 憑證機構就其可能或實際發生之賠償責任所提供之財務保證。	第 13 條：憑證機構應於其作業基準中載明與該機構及其他任何在作業基準內識別之成員之財務責任有關事項，並應包括下列事項： (1)憑證機構就其可能或實際	簡化規範爲財務責任刪除並責任保險。

(2) 憑證機構就其經營是否加入任何保險。 (3) 憑證機構是否經由第三人進行財會稽核。	發生之賠償責任所提供之財務保證。 (2)憑證機構就其經營及責任是否加入任何保險。 (3)憑證機構是否經由第三人進行財會稽核。	
第 12 條：憑證機構應於其作業基準中載明就所提供之認證服務或憑證之使用所生糾紛之處理程序及所適用之法律。 第 13 條：憑證機構應於其作業基準中載明用戶是否得請求退費；用戶得請求退費者，並應載明請求退費之程序。	第14條：憑證機構應於其作業基準中載明就所提供之認證服務或憑證之使用所生紛爭之處理程序、適用法律及用戶是否得請求退費；用戶得請求退費者，並應載明請求退費之程序。	將條文內容一分爲二。
	第15條：憑證機構應於其作業基準中載明一查詢方法，以供查詢其所發出之每一種憑證之申請、簽發、更新、廢止、查詢憑證狀態及其他認證相關服務可能收取之所有費用。	本條刪除。
	第16條：憑證機構應於其作業基準中載明公布作業基準、憑證政策、所發憑証、憑證狀態	本條刪除。

	等資訊之方法、頻率及儲存庫使用相關程序。	
第14條：憑證機構應於其作業基準中載明下列稽核或評核事項： (1)稽核或評核之頻率。 (2)進行稽核或評核人員之資格。 (3)稽核或評核人員中立性之確保。 (4)稽核或評核之範圍。 (5)對於稽核或評核結果之因應方式。 (6)稽核或評核報告公開之範圍及方法。	第十七條：憑證機構應於其作業基準中載明所實施之稽核或其他評核方法，並應包括下列項目： (1)稽核或其他評核之頻率。 (2)進行稽核或評核人員之身分及資格。 (3)稽核或評核人員中立性之確保（與憑證機構之關係）。 (4)稽核或評核之範圍。 (5)對於稽核或評核結果之因應方式。 (6)相關稽核或評核報告公開之範圍及方法。	本條未修正。
第15條：憑證機構應於其作業基準中載明其所保護用戶個人資料之種類及維持資訊保密之方法： (1)應爲機密資訊之種類。 (2)個人資料保護之相關事項。	第 18 條：憑證機構應於其作業基準中載明其保護用戶個人資料及維持資訊保密之方法，包括： (1)認證服務過程中可能取得之個人資料類型及取得方法。 (2)將保持機密之資料種類。 (3)非屬機密資料之種類。 (4)資訊之商業應用：憑證機	簡化規範，將條文內容一分爲二。

	構、註冊中心或其他參與認證服務之成員而可能取得用戶、信賴憑證者之相關資訊者，對於該等資訊之內部或外部應用，包括安全性、程序及契約上之限制。 (5)個人資料與機密資訊可能公開之範圍、程序及通知方法。	
第二章 識別及鑑別程序	第二章 識別及鑑別程序	
	第19條：憑證機構應於其作業基準中載明憑證、憑證政策、作業基準、憑證狀態相關資訊、名稱及金鑰等之智慧財產權。	本條刪除。
第16條：憑證機構應於其作業基準中載明所採用之命名規則。	第 20 條：憑證機構應於其作業基準中載明憑證機構或註冊中心於註冊及發證時，識別	簡化規範，將條文內容一分爲二。

第17條：憑證機構應於其作業基準中載明申請人證明擁有與所登記之公開金鑰相對應私密金鑰之方式。	及鑑別憑證申請人之程序，並應載明下列事項： (1)命名種類。 (2)命名是否具有意義。 (3)解釋不同命名形式的規則。 (4)命名是否具有獨特性。 (5)命名爭議如何解決。 (6)證明擁有與所登記之公開金鑰相對應私密金鑰之方式。 (7)身分鑑別之要件及程序。	
第 18 條：憑證機構應於其作業基準中載明申請人身分鑑別之要件及程序。	第21條：憑證機構應於其作業基準中載明例行性金鑰更換時所採取之識別及鑑別程序。	簡化規範。
第19條：憑證機構應於其作業基準中載明憑證機構於廢止憑證及暫時停用憑證申請時，安全識別及鑑別用戶之程序。	第22條：憑證機構應於其作業基準中載明憑證被廢止而更換金鑰時所採用之識別及鑑別程序。	簡化規範，合併條文內容。
	第 23 條：憑證機構應於其作業基準中載明處理廢止憑證請求時之識別及鑑別程序。	
	第24條：憑證機構如提供憑證暫時停用服務，則應於其作業基準中載明處理憑證暫時停用請求時之識別及鑑別程序。	
第三章 營運規範	第三章 營運規範	

第20條：憑證機構應於其作業基準中載明申請各種憑證之程序。	第 25 條：憑證機構應於其作業基準中載明申請各種憑證之程序。	本條未修正。
第21條：憑證機構應於其作業基準中載明簽發憑證、憑證展期及憑證內容修改時，用戶接受憑證之程序。	第26條：憑證機構應於其作業基準中載明簽發憑證及通知憑證已簽發之程序。 第27條：憑證機構應於其作業基準中載明用戶接受憑證之程序及公布憑證之程序。	簡化規範，合併條文內容。
第22條：憑證機構提供憑證暫時停用服務者，應於其作業基準中載明下列事項： (1)得請求暫時停用憑證之事由。 (2)憑證機構得逕行暫時停用憑證之事由。 (3)有權請求暫時停用憑證之人。 (4)請求暫時停用憑證之程序。 (5)暫時停用之期間。 (6)憑證機構處理暫時停用請求之期間。 (7) 恢復使用憑證之程序。	第 28 條：憑證機構應於其作業基準中載明有關憑證暫時停用及廢止憑證之重要事項。 憑證機構提供暫時停用服務者，應於其作業基準中載明下列事項： (1)得請求暫時停用憑證之事由及憑證機構得逕行暫時停用憑證之事由。 (2)有權請求暫時停用憑證之人。 (3)請求暫時停用憑證之程序。 (4)暫時停用之期間。 (5)憑證機構處理暫時停用請求之期間。	刪除第 1 項並將第 2、3 項分爲 2 個條款。

第23條：憑證機構就憑證之廢止應於其作業基準中載明下列事項： (1)得請求廢止憑證之事由。 (2)憑證機構得逕行廢止憑證之事由。 (3)有權請求廢止憑證之人。 (4)請求廢止憑證之程序。 (5)憑證機構處理廢止憑證請求之期間。 (6)憑證機構發出憑證廢止清冊之頻率。 (7)是否提供線上憑證狀態查詢。	憑證機構就憑證之廢止，應於其作業基準中載明下列事項： (1)得請求廢止憑證之事由及憑證機構得逕行廢止憑證之事由。 (2)有權請求廢止憑證之人。 (3)請求廢止憑證之程序。 (4)憑證機構處理廢止憑證請求之期間。 (5)憑證機構發出憑證廢止清冊之頻率。 (6)信賴憑證者查詢憑證廢止清冊時須具備之要件。 (7)是否提供線上憑證狀態查詢。 憑證機構應於其作業基準中載明因私密金鑰遭破解而致憑證暫時停用或廢止時，前二項所列說明事項之不同。	
	第 29 條：憑證機構應於其作業基準中載明爲維持環境安全之目的所運用之紀錄及檢查系統，並應包括下列事項： (1)被記錄事件種類。 (2)紀錄檔處理頻率。	本條刪除。

	(3)稽核紀錄檔保留期間。 (4)稽核紀錄檔的保護。 (5)稽核紀錄檔備份程序。	
	第 30 條：憑證機構應於其作業基準中載明紀錄歸檔之政策，並應包括下列事項： (1)所記錄事件之類型，應包括所有驗證憑證內容所必須之檔案資料。 (2)歸檔保留期間。 (3)歸檔之保護。 (4)歸檔備份程序。 (5)紀錄對於時戳之要求。 (6)歸檔彙整系統是否是內部的。 (7)取得及驗證歸檔資訊之程序。	本條刪除。
	第31條：憑證機構應於其作業基準中載明提供新的公開金鑰予用戶之程序。	本條刪除。
	第 32 條：證機構應於其作業基準中載明金鑰遭破解或災變時之通知及復原程序，並分別說明下列程序： (1)電腦資源、軟體或資料遭破	本條刪除。

	壞或疑似遭到破壞時所採取之復原程序。 (2)公開金鑰被廢止時所使用之復原程序。 (3)金鑰遭破解時所採取之復原程序。 (4)發生自然災害或其他災變時，在安全環境重建完成之前（不論是在原地或在其他地點），憑證機構用以救援其設備之程序。	
	第33條：憑證機構應於其作業基準中載明憑證機構或註冊中心欲終止服務時，進行通知及檔案紀錄之保管與移交之程序。	本條刪除。
第四章 非技術性安全控管	第四章 非技術性安全控管	
第24條：憑證機構應於其作業基準中載明其所採行之實體、運作程序及人員安全之控管措施。	第 34 條：憑證機構應於其作業基準中載明其爲能安全執行金鑰產製、鑑別身分、簽發憑證、廢止憑證及歸檔等功能	將條款一分爲三分別規範。

第25條：憑證機構應於其作業基準中載明下列紀錄歸檔事項： (1) 所記錄事件之類型，應包括所有驗證憑證內容所必須之檔案資料。 (2)歸檔保留期間。 (3)歸檔之保護。 (4)歸檔備份程序。 (5)紀錄對於時戳之要求。 (6)紀錄檔處理頻率。	所採用之實體控管，並應包括下列項目： (1)實體所在及結構。 (2)實體存取。 (3)電力及空調。 (4)水災。 (5)火災防範及保護。	
第26條：憑證機構應於其作業基準中載明下列憑證機構金鑰變更時之處理程序： (1)因應驗證憑證需求，以原公開金鑰驗證新公開金鑰之處理程序。 (2)提供新的公開金鑰之方法。		
第27條：憑證機構應於其作業基準中載明危害及災變復原程序之規劃。		

第 28 條：憑證機構應於其作業基準中載明下列終止任(1)憑證簽發服務時之處理程序： (2)現行有效憑證之因應處理。 (3)紀錄檔案移交或保管年限。	第35條：憑證機構應於其作業基準中載明就其運作之程序控管而言須獲得信賴之職位，並載明識別及鑑別擔任該等職位人員之方法。	
	第36條：憑證機構應於其作業基準中載明就人員聘用、監督及培訓所進行之控管措施。	
第五章 技術性安全控管	第五章 技術性安全控管	
第 29 條：憑證機構就金鑰對之產製及安裝，應於其作業基準中載明下列事項： (1)用戶金鑰對由誰產製。 (2)金鑰對非由用戶自行產製時，私密金鑰如何安全傳送予用戶。 (3)憑證機構公開金鑰如何安全傳送予用戶或信賴憑證者。 (4)金鑰長度。。 (5)金鑰生成參數及參數品質檢驗。 (6)金鑰之使用目的。	第三十七條：憑證機構就金鑰對之產製及安裝，應於其作業基準中載明下列事項： (1)金鑰對由誰產製。 (2)金鑰對非由用戶自行產製時，私密金鑰如何安全傳送予用戶。 (3)公開金鑰如何安全傳送予實際簽發憑證者。 (4)憑證機構公開金鑰如何安全傳送予用戶或信賴憑證者。 (5)金鑰長度。 (6)公開公鑰生成參數。 (7)金鑰參數品質檢驗。 (8)金鑰經軟體或硬體產製。 (9)金鑰之使用目的。	刪除第(3)款及第(8)款。

第30條：憑證機構就私密金鑰保護，應於其作業基準中載明下列事項： (1)密碼模組是否符合特定標準。 (2)是否採行金鑰分持之多人控管。 (3)私密金鑰是否託管、備份、歸檔或輸入至密碼模組；如進行託管、備份、歸檔或輸入至密碼模組者，其方法及程序。 (4)私密金鑰之啓動、停用及銷毀方式。	第 38 條:憑證機構就私密金鑰保護，應於其作業基準中載明下列事項： (1)是否符合特定密碼模組標準。 (2)是否採行金鑰分持之多人控管。 (3)私密金鑰是否託管、備份、歸檔或輸入至密碼模組；如進行託管、備份、歸檔或輸入至密碼模組者，其方法及程序。 (4)私密金鑰之啓動、停用及銷毀方式。	本條未修正。
第31條：憑證機構應於其作業基準中載明憑證有效期限、公開金鑰是否歸檔及公開金鑰與私密金鑰各別之使用期限。	第 39 條:憑證機構就金鑰對之管理，應於其作業基準中載明下列事項： (1)公開金鑰是否歸檔；如歸檔，則負責歸檔之機關與其形式， 及對於歸檔系統之安全控管。 (2)公開金鑰及私密金鑰各別之使用期限。	簡化規範。
第32條：憑證機構應於其作業基準中載明對於啓動資訊	第40條：憑證機構應於其作業基準中載明對於啓動資訊之保	簡化規範。

之保護措施。	護，包括從產生、歸檔到銷毀之間整個生命週期之保護。	
	第41條：憑證機構應於其作業基準中載明爲防止及偵測未經授權之使用、竄改或洩露資料所採取之電腦軟硬體安控措施。	本條刪除。
第33條：憑證機構應於其作業基準中載明所採行之系統軟體及網路安全控管措施。	第42條：憑證機構應於其作業基準中載明其所採行之系統研發控管及安全管理控管措施。	簡化合併條款。
	第43條：憑證機構應於其作業基準中載明其所採行之網路安全控管措施。	
	第44條：憑證機構應於其作業基準中載明其所採行之密碼模組安全控管措施。	
第六章 格式剖繪	第六章 格式剖繪	
第34條：憑證機構就憑證之格式剖繪應於其作業基準中載明下列事項： (1)版本序號。 (2)憑證擴充欄位。 (3)演算法物件識別碼。 (4)命名形式。 (5)命名限制。	第 45 條:憑證機構就憑證之格式剖繪應於其作業基準中載明下列事項： (1)版本序號。 (2)憑證擴充欄位。 (3)演算法物件識別碼。 (4)命名形式。 (5)命名限制。	本條未修正。

(6)憑證政策物件識別碼。 (7)政策限制擴充欄位之使用。 (8)對關鍵憑證政策擴充欄位之語意處理。	(6)憑證政策物件識別碼。 (7)政策限制擴充欄位之使用。 (8)對關鍵憑證政策擴充欄位之語意處理。	
第 35 條：憑證機構就憑證廢止清冊之格式剖繪應於其作業基準中載明下列事項： (1)版本序號。 (2)憑證廢止清冊及憑證廢止清冊擴充欄位。	第 46 條：憑證機構就憑證廢止清冊之格式剖繪應於其作業基準中載明下列事項： (1)版本序號。 (2)憑證廢止清冊及憑證廢止清冊擴充欄位。	本條未修正。
	第七章 憑證實務作業基準之維護	本章刪除。
	第 47 條：憑證機構應於其作業基準中載明作業基準之變更程序及作業基準變更時是否變更其物件識別碼或其公布之網址。	
	第 48 條：憑證機構應於其作業基準中載明作業基準變更時通知或公告之對象及其程序。	
第36條：本準則自發布日施行。		

4.4 外國憑證機構許可辦法

4.4.1 外國憑證機構許可辦法總說明

爲建立安全及可信賴之網路環境，促進電子商務普及應用及推動電子化政府，透過電子簽章法明定電子文件及電子簽章之法律效力，並據以規範憑證機構之設立，以確保資訊在網路傳輸及儲存過程中之安全性，使電子交易在保護使用者權益的前提下普及應用，並使電子認證體系能妥善運行。

由於電子商務多爲全球跨國界行爲，隨著電子簽章技術之陸續推動發展，除對國內憑證機構管理機制應有規範外，對於外國憑證機構所簽發之憑證效力亦須有所規定。爲妥適因應電子商務此一跨國界經營運作之特性，並及早建立未來電子商務國際化發展之法制環境，電子簽章法特於第十五條訂定規範國際承認之條文，以利國際化電子商務之推動，並規定外國憑證機構須經主管機關許可後，其簽發之憑證始與本國憑證機構所簽發之憑證具有相同效力。

本「外國憑證機構許可辦法」（以下簡稱：本辦法）之訂定，即係基於電子簽章法第十五條第二項規定，授權主管機關配合國際實務發展，斟酌管理之需求，以訂定許可及規範外國憑證機構。

4.4.2 外國憑證機構許可辦法規範重點

爲因應電子商務跨國界經營運作之特性及需求，外國憑證機構所簽發之憑證效力如符合一定條件下應被承認，以讓外國憑證機構經主管機關許可後，其簽發之憑證與本國憑證機構所簽發之憑證具有相同效力，以符合國際趨勢。主管機關基於電子簽章法第十五條第二項之授權，訂定「外國憑證機構許可辦法」，其主要重點如下：

1. 外國憑證機構許可與本國憑證機構核定之標準相同

爲了避免違反 WTO「反歧視性原則」而使日後可能遭到他國報復，主管機關基於平等互惠及安全條件相當之原則，對外國憑證機構之許可與對本國憑證機構之核定採取同樣之標準。而外國憑證機構須經主管機關許可後，其簽發之憑證始與本國經核定憑證機構所簽發之憑證具有相同效力。

2. 主管機關得逕行許可之

爲配合國際實務發展，外國憑證機構許可辦法第 7 條明定：「主管機關得與他國、區域組織或國際組織簽訂雙邊或多邊協定或協約，對於經該他國、區域組織或國際組織許可或認可之外國憑證機構，免除其申請程序，逕行予以許可」。換言之，主管機關得於互惠原則下免除外國憑證機構的申請程序，逕行許可之。針對電子商務跨國界經營運作之特性，國際立法例對於跨國憑證之承認，多採經認可之憑證機構所簽發符合一定安全標準之憑證，便承認其法律效力，此與我國以對該外國機構之憑證實務作業基準經許可與否爲標準有所不同。我國主管機關爲配合國際趨勢發展，得於互惠原則下，免除某些已經被其他國家、區域組織或國際組織許可或認可的外國憑證機構申請程序，以及早建立未來電子商務國際化發展之法制環境。

4.4.3 外國憑證機構許可辦法內容及其說明

表 4-3：外國憑證機構許可辦法內容及其說明

條文內容	條文說明
第 1 條：本辦法依電子簽章法（以下簡稱本法）第十五條第二項規定訂定之。	明定本辦法之授權依據。
第 2 條：依外國法律組織、登記之憑證機構（以下簡稱外國憑證機構）依本法第 15 條第一項規定申請許可時，應檢具下列文件： 一、申請書。 二、變更後之憑證實務作業基準及	明定外國憑證機構依本法第 15 條第一項規定申請許可之程序。

其應載明事項檢核對照表。 三、憑證實務作業基準應載明事項檢核對照表。 四、其他經主管機關指定之文件。 前項憑證實務作業基準，應載明主管機關發布之憑證實務作業基準應載明事項。 第 1 項申請書、憑證實務作業基準應載明事項檢核對照表及其他相關文件之格式，由主管機關定之。	
第 3 條：經許可之外國憑證機構其憑證實務作業基準有變更時，應於變更後 30 日內申請許可。 外國憑證機構申請更新許可時，應檢具下列文件： 一、申請書。 二、憑證實務作業基準。 三、變更內容對照表。 四、其他經主管機關指定之文件。 前項申請書、憑證實務作業基準應載明事項檢核對照表及其他相關文件之格式，由主管機關定之。	明定經許可之外國憑證機構擬變更其憑證實務作業基準時，應提出變更申請之時點及程序。
第 4 條：依本辦法提出之文件爲外國文字者，應譯爲中文；主管機關得視需要令其文件經駐外使領館、	爲便利許可程序之進行，特明定於提出文件爲外國文件時，應使用之語文及應進行之程序。

代表處、辦事處或外交部授權之機構驗證或認證。	
第 5 條：外國憑證機構有下列情事之一者，主管機關得不予許可： 一、其憑證實務作業基準未依主管機關發布之憑證實務作業基準應載明事項辦理者。 二、申請事項有虛偽情事者。 三、對公益有重大危害者。 四、違反其他中華民國法令、公共秩序或善良風俗情節重大者。 五、其組織、登記地區對我國憑證機構所簽發之憑證有顯失互惠情事者。	明定主管機關許可之消極要件。
第 6 條：外國憑證機構有下列情事之一者，主管機關得廢止其許可： 一、其憑證實務作業基準變更，未經主管機關許可者。 二、違反其他中華民國法令、公共秩序或善良風俗情節重大者。 三、對公益有重大危害者。 四、其組織、登記地區對我國憑證機構所簽發之憑證有顯失互惠情事者。	明定主管機關於許可後，得廢止其許可之情形。
第 7 條：主管機關得與他國、區域	國際發展現況，特明定逕行許可之規

組織或國際組織簽訂雙邊或多邊協定或協約，對於經該他國、區域組織或國際組織許可或認可之外國憑證機構，免除其申請程序，逕行予以許可。	定。

4.4.4　小結

由上可知，在國際互惠原則及安全條件相當原則之前提下，只要外國憑證機構經主管機關許可，其簽發之憑證便與本國憑證機構所簽發憑證具有相同之法律效力。換言之，業者或民眾欲使用和本國憑證機構所簽發憑證相同效力的外國憑證時，首先應注意該外國憑證機構是否經過主管機關之許可。

至於外國憑證機構之許可標準，主管機關經濟部基於平等互惠之原則，對外國憑證機構之許可與對本國憑證機構之核定採取同樣之標準。亦即，申請主管機關許可之外國憑證機構應製作憑證實務作業基準，其憑證實務作業基準亦至少要載明經濟部發布之「憑證實務作業基準應載明事項」所要求事項後，送交經濟部進行許可程序。然而，有鑑於現實憑證實務發展，對於憑證機構國際承認工作之進行多係透過簽訂雙邊或多邊協約或協定之方式進行，較少由個別憑證機構自行申請許可的情形。爲因應日後國際承認實務之需求及國際發展現況，外國憑證機構許可辦法第 7 條特別定有主管機關得逕行許可之規定：「主管機關得與他國、區域組織或國際組織簽訂雙邊或多邊協定或協約，對於經該他國、區域組織或國際組織許可或認可之外國憑證機構，免除其申請程序，逕行予以許可。」據此，主管機關爲因應國際趨勢發展，得衡酌國際合作及國內發展需求，以簽訂雙邊或多邊協約或協定之方式取代個案申請之模式，以期加速國際交互承認工作之進行，以建立跨國交互承認機制、無紙化國際貿易交易環境與電子商務國際化發展之完善法制環境。

五、電子簽章法制關於憑證機構管理規範之修法建議－代結論

5.1 建立憑證機構管理規範完備法制之重要性

在現今的電子化政府及電子商業行爲中，由於憑證機構在公開金論基礎中扮演身分認證機制之角色，提供憑證簽發、對於憑證使用者身分的查驗，以及建立一套安全可靠的目錄服務系統、憑證註銷清冊等電子認證服務制度等，亦即電子簽章應用服務需高度仰賴憑證機構扮演著中立公信第三者之角色。爲此，主要科技先進國家均致力於建立完備憑證機構管理規範之法制，使其技術及管理皆能夠達到一定的安全水準，以保障交易安全及使用者的權益。

電子簽章法自民國 91 年實施至今已有 5 個年頭，比較各國立法趨勢及國內實務運作狀況，均已屆至應予檢討之時，方能應付一日千里之電子商務發展及日益頻繁之電子交易，並有效解決實務運作上所生之疑義。

茲將本論文提出檢討的重點臚列如下：

1. 現行憑證機構法制並不完備

目前現行法關於憑證機構之管理規範僅有 5 條，規範完整性顯屬不足，而且對於主管機關訂定有關憑證機關之核定，提供憑證服務之營運管理監督辦法及憑證實務作業基準等規範均未見法條中有明確授權。同時對憑證機構之核定，係僅採書面審查制度，故對憑證機構提供服務品質之可信賴性，及與國際接軌，以及推行憑證互通機制，均不足以因應。

2. 對消費者保護應有配套措施

現行法制係採過失推定及舉證責任倒置的方式，來維護消費者的權益並平衡專業能力的落差，而未採消費者保護法規定之無過失責任，在爲兼顧相關產業發展上，的確有其考量之處。但卻又規定憑證機構就憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，不負賠償責任，明示當事人間得以

特約排除。實務上運作之結果便是憑證機構以定型化契約來限縮其賠償責任，如此對消費者保護，確實有不周全之問題。

3. 對促進相關產業發展及與國際接軌應積極落實

政府應積極促進電子認證服務相關產業發展，以避免形成獨占、寡占甚至僅剩政府經營之情況。同時，爲因應電子商務、企業無紙化往來以及網路無國界之需求，建立符合國際標準之法制環境，亦屬刻不容緩之事。

5.2 對我國憑證機構管理規範之修法建議

針對上述情形，本論文提出下列幾點我國現行憑證機構規範法制應檢討修正之方向：

1. 就憑證機構關之規範法制而言：

(1) 建立憑證機構強制外部稽核之管理制度：

現行電子簽章法的立法方式係採取所謂的低度管理之「市場導向原則」。在此原則下，電子簽章法並未賦予主管機關經濟部任何強制稽核的權力。僅透過經營之初，審查憑證機構的「憑證實務作業基準」，因此只要通過第一次的文件審查，除非發生重大事件，否則從此憑證機構就此高枕無憂，且因爲並沒有任何機關或組織會針對「憑證實務作業基準」去瞭解憑證機構是否真的去落實其在「憑證實務作業基準」上所宣稱的那些事項。

然憑證機構（及/或註冊中心）是目前建構電子商務及資訊化社會之關鍵基礎建設。其所以扮演關鍵基礎建設之地位在於憑證機構係爲電子交易雙方之信賴缺口提供可信賴性之信賴服務提供者，亦即憑證機構爲具有以「信賴價值」爲核心之信賴服務提供者。而創造憑證機構之信賴價值之關鍵元素在於憑證機構 對於電子簽章所有人採行嚴格認證程式確認其身分與電子簽章之唯一關聯性。而是否確實執行嚴格認證程式並確保其作業之安全以建立信賴之基礎，爲憑證機構管理制度中之重要議題。

爲讓憑證機構具有客觀之可信賴基礎，而不僅止於憑證機構所自行宣稱具有可信賴性之主觀可信賴基礎，因此憑證機構仍須藉由公正第三人進行外部稽核，故有憑證機構外部稽核制度規劃之必要性。是以於憑證機構之管理制度上，特別是對於憑證機構取得營運許可後之動態管理上，從憑證機構之信賴本質核心在於嚴格認證程式之要求，並以憑證機構於電子交易結構中所扮演之角色觀察以及我國對於憑證機構所採取之營運核定許可之環境體制下，爲確保憑證機構具有客觀可信賴性之基礎，憑證機構之外部稽核制度建議採行「強制稽核」之管理架構。

(2) 建議憑證機構規範應制定專法

依新加坡電子交易法第四十二條[115]之授權，主管機關「通訊及資訊技術部」

---

[115] 新加坡《電子交易法》第 42 條之規定：「認證機構的有關規定

（1）部長爲規範或許可認證機構，可以頒佈條例，或者爲確定何種數位簽名符合電子簽名安全標準而頒佈條例。

（2）在不排除第（1）款普遍適用的情況下，部長可以制定有關以下內容的規定：

a 關於申請認證機構及其授權代表機構許可、或更新其許可、以及其他的有關事項；

b 認證機構的活動，包括諮詢業務的方式、方法、地點、諮詢的具體做法，以及禁止其他公眾成員未經授權不得從事該種業務；

c 認證機構的經營標準；

d 發佈關於許可授權以及雇員的資格、經驗和培訓的適當標準；

e 發佈認證機構從事商業經營活動的從業條件；

f 在設計個人發佈或使用數位證書或密鑰時所必需的書面的、印刷的或其他可視材料及廣告，應公佈其內容和發佈方式；

g 規定數位證書或密鑰的格式和內容；

h 規定複製認證機構帳戶或關於帳戶的具體內容；

I 涉及依法任命的審計官員的任命和薪酬的規定，以及規定審計官員的薪酬承擔應由專門附錄加以規定；

j 涉及認證機構的任何電子系統的設立或有關規定，其認證機構或是獨立創設，或是與其他機構合併而成，以及有關管理官員認爲合適的關於訂立和修改有關設立條件、標準和限制的規定。

k 許可證持有人處理客戶關係的方式、與客戶利益衝突的調整以及在數位證書方面對客戶應盡的責任；

l 立法宗旨的規定；以及

(Ministry for Communications and Information Technology)進一步訂定了「西元 1999 年電子交易（憑證機構）規則」，於西元 1999 年 2 月 10 日實施，將憑證機構設立及管理之標準均加以規範 ，作爲「電子交易法」之補充。該規則共分 8 章，計 37 條，對於憑證機構執照之授與、執照授與之標準（包括資金、人員、營運、稽核）、執照之撤銷與中止 、經授與執照之憑證機構的營業準則、資料儲存庫、政府機關及法令特許事業公司之適用以及監督管理等議題加以明確規範。尤其關於憑證機構執照申請之鼓勵、憑證機構取得執照之門檻、憑證機構之稽核、監督認證單位之權力、資料晚整性及隱密性之保護、憑證機構中止服務之處理、安全數位簽章等均有相當完整之規定。

香港在憑證機構管理專法方面，也依據電子交易條例第三十三條[116]授權而制訂了「認可核證機關業務守則」(Code of Practice for Recognized Certification Authorities)。該守則就憑證機構的一般責任、憑證實務作業基準、穩當系統（即構成穩當系統的指導原則、良好作業實務、保全及風險管理等）、憑證用戶身份核對、信賴額度之限制及保險、儲存庫、資訊揭露義務、終止服務、標準及技術的採用、憑證互通以及消費者保護等亦均有清楚的規範。

由於憑證機構相關規定除了法律面向之外，有關憑證實務作業基準之技術、標準、程序亦佔了絕大部分，再加上憑證機構之責任、保險制度、稽核制度、資訊揭露義務、撤銷或終止憑證後的處理等內容相當龐雜，實有制訂專法之必要。建議我國在修正電子簽章法的過程中，以條文授權主管機關另行制訂憑證機構的專法，以爲完善之管理並健全整體電子商務法制。

---

m 規定在本法或有關條例中要求的獲取服務或有關事項的費用。

（3）依照本法制定的任何條例、法規應規定：凡觸犯有關法律的違法行爲人，應處以 5 萬元以下罰金或 12 個月以下的監禁，或則二者並用。」

116 香港《電子交易條例》第 33 條第 1 款之規定：「政府資訊科技總監可在憲報刊登業務守則— (由 2004 年第 131 號法律公告修訂)

(a) 指明執行認可核證機關的功能的標準及程序；

(b) 爲施行以下條文指明本條例及業務守則的條文。」

關於憑證機構管理之專法，建議參照 RFC3647 文件中之相關規定，並給予「憑證實務作業基準應載明事項」更明確之法源及內容規範依據，規範重點在於：

① 明定憑證機構申請核定之程序。

② 明定憑證實務作業基準變更時之程序。

③ 明定憑證實務作業基準應載明之事項細則。

④ 明定憑證機構查核之程序。

⑤ 明定憑證機構核定廢止之程序。

2. 建議建立相關配套措施以保護消費者權益

(1) 考量建立憑證機構之保險制度以轉嫁責任風險

若沒有設立憑證機構的法律責任限額，則經認可的憑證機構必須花費許多額外的時間與資源來確認憑證的真偽及有效性，以免除不必要的法律責任，而可能造成交易速度減緩並也增加交易成本，因此無法達到電子商務提高服務效率與減少交易成本的目的。有鑑於此，建議設計相應保險制度來吸收憑證機構可能被求償的風險，對憑證機構的經營及消費者之保護軍事正面助益。

(2) 主管機關應制定憑證服務之定型化契約範本

主管機關應依我國消費者保護法第 17 條之規定，公告憑證服務的定型化契約應記載事項與不得記載事項，以避免憑證機構利用其企業優勢地位，單方決定相關認證服務定型化契約（用戶合約及信賴者服務合約等）條款，藉以規避責任。

3. 建議建立相關制度以促進產業發展並與國際接軌

(1) 建議增訂輔導相關辦法授權主管機關協助電子商務相關產業之發展

爲促使我國電子商務得以蓬勃發展，建議民眾從事電子交易之信心，建議仿照韓國電子電子商務基本法第 23 條[117]及第 25 條[118]之規定，於電子簽章法中明文授權，增訂相關輔導辦法，授權主管機關得協助相關產業並推動電子簽章與憑證普及應用與建構安全之電子交易環境，以及促使我國電子商務發展與國際接軌。

(2) 建立憑證機構強制許可之管理制度

在大多數承認公開金鑰基礎建設的國家立法例中，憑證機構的管理制度乃爲立法時之重要考量之一。在歐洲國家中，義大利對於憑證機構採取強制登記制；德國形式上雖承認未取得認證的憑證機構所簽發的憑證，但實質上卻希望所有憑證機構都能經過國家總憑證機構(National Root CA)發給證照；惟歐盟指令則禁止強制登記制，並希望各會員國能在「客觀、透明、合理及不歧視」的前提下採行志願授權/許可制。在亞洲各國方面，馬來西亞數位簽章法第四條第三項要求憑證機構必須向憑證機構監督單位提出證照申請，違反者將處以刑罰；但於同法第十三條又仿猶他州數位簽章法，不排除未取得證照之憑證機構所簽發之憑證效力。因此要謂其爲強制登記制則恐有疑義。而新加坡的電子交

---

117 韓國《電子商務基本法》第 23 條之規定：「電子商業的標準化

(1) 爲了促進電子商業的發展並保證有關資訊技術的可交換性，政府應根據有關法律採取下列措施：

1. 建立、修改、撤銷和分配與電子訊息有關的標準；

2. 研究和開發與電子商業有關的國內和國外標準；及

3. 爲電子商業的標準化所必需的其他事項。

(2) 應根據總統令成立韓國 EDI 委員會以研究和討論第(1)款第 1 項中規定的電子訊息的標準化問題。

(3) 政府在必要的情況下，可以由有關的研究機構和非政府組織代表它有效地實施第(1)款中各項所規定的措施。在此種情況下，它可以根據總統令的規定對這些機構或組織因此而支出的費用予以補償。」

118韓國《電子商務基本法》第 25 條之規定：「電子商業的國際合作

政府可以支持諸如有關技術和人力資源的國際交流、國際標準化及研究和開發方面的國際合作活動，以促進與電子商業有關的國際合作。」

易法雖未對憑證機構採取強制登記之管理方式，但相關規範不少，且只允許領有執照的憑證機構得於憑證中載明責任限制 。至於日本則採取志願認可制。

由上可知，對於憑證機構的管理方式的選擇，似乎只有極少國家是採取絕對強制方式，大部分都是介於強制與志願許可制之間的折衷管理模式，賦予經認可或取得證照的憑證機構某些權利或好處，如其簽發之憑證具有效力優越性、可設責任限額等。我國目前電子簽章法雖未針對憑證機構使否須經許可或認可加以規定，而由市場自由競爭機制去淘汰、選擇，但卻只有經主管機關核定憑證實務作業基準之憑證機構，方得對外提供簽發憑證服務。由於此部分乃爲影響國際間憑證互通或憑證機構跨國簽發之憑證是否相互承認之重要考量，因此建議予以修正。

(3) 建議增訂憑證機構交互認證（Cross Certification）之制度

憑證機構交互認證的好處[119]在於可以增加憑證使用者對於憑證機構的信賴程度，理由是憑證使用者除了單方面相信憑證機構所做的聲明及服務外，更可以藉由向另一個憑證機構來驗證其所聲明的真實性，這在推動電子商務的初期，是具有相當正面的效用，除了電子商務業者在選擇憑證機構時可以藉由向他憑證機構驗證獲取更多的資訊，而不致遭受不必要的損失外，間接的更可以增進消費者對電子商務業者的信賴，使消費者獲得多一層的認證保障。

然目前即因現行法對憑證機構認證的整個制度並無規範此一部分，造成憑證機構相互間規格相容性之問題，如此不但在承接上有其困難度，亦造成憑證機構間無法交互承認，如此受影響最大者即爲電子商務業者，理由是電子商務業者將於做出第一次憑證機構選擇後即必須冒著無法做第二次選擇之風險，而消費者也失去交互認證制度下的第二層保障，甚至對有心經營憑證機構的合法業者，也無法利用交互認證制度來適度增加消費者對其之信賴。如此對建立安

[119] 同註 22，頁 196。

全的電子商務環境將會形成一定障礙，因此建立交互認證制度對促進電子商務發展有其重要性。

(4) 建議政府以委託行政之方式，使民間憑證機構成爲電子商務之基礎產業

自本論文第一章之論述則可得知，亞洲各國憑證機構均採行公私電子憑證認證並行之制度，且各國政府均投入大量資源建置公領域之憑證系統，目的均希望以公領域帶動私領域之發展。然誠如於本論文第二章所討論的，民間憑證機構因公領域佔盡事實面及法律面之優勢，而使私領域之民間機構面臨發展之困境，爲電子認證服務產業之永續經營發展，避免成爲政府寡佔事業，並節省大量政府營運成本，本論文建議政府應將憑證政策應營運憑證機構之思維轉以憑證管理之角度規劃，亦即退出憑證機構市場，而將電子化政府之憑證業務工作以委託行政之方式，交由民間憑證機構經營，使民間機構得以蓬勃發展，進而使電子商務體制能健全發展。

5.3 未來與展望—後續應進一步建立之相關法制規範

我國爲出口導向之國家，國際貿易需仰賴海運產業之進步發展，方能使資訊快速流通，進而帶動物流之快速運轉，因此利用資訊科技發展電子載貨證券之應用是現在及未來發展之主流。故極需相關技術開發、產業的配合、以及制定適合的法制予以規範。

申言之，海運業相關業者[120]除本身應強化電子交易的基礎建設之外，亦須透過政府提供法制環境，來降低各種交易風險，強化產業界之競爭力。而且因電子交易無國界、全球化特性，故建議政府處理相關問題，必須以全球化角度思考，蓋載貨證券爲國際貿易之重要單據，藉由信用狀之使用，搭配商業發票、保險單等各種貿易單據使用，在國際貿易中扮演舉足輕重之角色。

[120] 依我國《航業法》第 2 條第 1 款之規定：「航業：指經營船舶運送、船務代理、海運承攬運送、貨櫃集散站、船舶出租等事業。」

是故，就此部分針對與憑證機構相關者的部分，提出下列兩點建議：

1. 政府應規劃協助海運業者設立專責憑證機構[121]

有別於一般交易，國際貿易尤其是海運業，需要更專業及專責之認證服務機構提供電子認證服務，藉此得以健全作業並整合運輸、倉儲等之「物流系統」、銀行、稅務、保險業、的「金流系統」及供應廠商、有關行業間的「資訊流系統」，俾使資訊更加透明互通與共享，以提高商機並促進海運業之發展。

2. 建立完善之憑證機構發證及驗證程序管理機制

國際貿易採行電子商務是必然之趨勢，故應特別針對國際貿易之電子憑證之簽發及驗證程序管理，建立完善之程序管理之機制，同時針對可預期的國際商業糾紛日益增加之問題，亦應詳訂紛爭處理機制及處理依據。

[121] 鍾秋華，「電子載貨證券憑證機構作業實務之研究」，國立台灣海洋大學，航運管理研究所碩士論文，2002 年 6 月。

參 考 文 獻

壹、中文參考資料

一、中文書籍及期刊

1. 王澤鑑，債法原理，三民書局，西元 2006 年 9 月再刷。
2. 王澤鑑著，侵權行爲法第一冊，三民書局，2001 年 7 月。
3. 吳庚，行政法之理論與實用，三民書局，民國九十年八月增訂七版。
4. 江偉平，「政府對電子簽章與認證機構法規所採取之對策與因應措施」，民國 88 年 12 月 9 日，產業發展協進會舉辦之 1999 企業電子化領袖論壇演講稿。
5. 邱聰智著，新訂民法債篇通則（上），輔仁大學，西元 2000 年 9 月新訂一版。
6. 杜怡靜，「電子商務發展之基石-電子簽章制度—日本電子簽章法（電子署名法）及相關制度之介紹」，萬國法律雜誌第一一九期，財團法人萬國法律基金會，2001 年 10 月。
7. 林志峰，「美國猶他州 1995 年數位簽章法」，EDI 簡訊，第十四期，1999 年 6 月。
8. 林煒鎔，「電子簽章與電子金融服務之應用－憑證機構法律責任之探討」，科技法律透析，民國 92 年 8 月 15 日。
9. 林煒鎔，「電子簽章法子法相關規範概觀/憑證機構的管理規範」，電子商務法律通，財團法人資訊工業策進會科技法律中心，2003 年 11 月。
10. 洪淑芬，「公開金鑰認證中心(CA)主管機關權責範圍探討」，資訊法務透析，民國 86 年 3 月。
11. 張真誠、林祝興、江季翰編著，電子商務安全，松崗電腦圖書資料股份有限公司，2002 年 2 月。
12. 財團法人資訊工業策進會科技法律中心，數位法律時代，書泉出版社，2005 年 11 月 30 日。
13. 馮震宇，網路法基本問題研究（一），2 版，學林文化事業有限公司，2000 年 9

月。

14. 馮震宇，「電子商務之法律保護與因應策略」，風險管理雜誌第十期，2002 年 3 月。
15. 曾隆興著，詳解損害賠償法，三民書局，2004 年 4 月。
16. 曾德宜，「美國電子簽章法述評」，立法院院聞第二十九卷第二期，民國 90 年 2 月。
17. 經濟部商業司，電子商務用語第二版，民國九十年十 2 月再版。
18. 經濟部商業司編印，2004 台灣 PKI 年鑑，民國 93 年 10 月出版。
19. 經濟部商業司編印，2005 台灣 PKI 年鑑，民國 95 年 2 月出版。
20. 楊佳政 ，「認證中心法律責任研究」，資訊法務透析，27~41 頁，民國 87 年 6 月。
21. 劉尚志主編，2000 年全國科技法律研討會論文集，國立交通大學科技法律研究所，2000 年 11 月。
22. 劉尚志、陳佳麟，網際網路與電子商務法律策略，元照出版有限公司，2001 年 3 月初版第一刷。
23. 蔡振榮、鄭善印著，行政罰法逐條釋義一版二刷，新學林出版股份有限公司，2006 年 9 月。
24. 鄭玉波、陳榮隆修訂，民法債編總論，修訂二版二刷三民書局，2004 年。
25. 簡資修著，「危險之生成與界線：舉證責任與過度防制」，台大法學論叢 48 期，2001 年 5 月。
26. 戴豪君、常天榮，「聯合國國際貿易法委員會電子商業模範法淺析」，資訊法務透析，1998 年 1 月。

二、中文學術論文

1. 尤弘任，「基於公開金鑰基礎建設之電子文件系統」，國立台灣科技大學資訊管理研究所，民國 95 年 6 月。

2. 朱建達，「建立於公開金鑰基礎建設的單一切入系統」，國立交通大學資訊管理研究所，民國 89 年 6 月。
3. 朱瑞陽，「電子商務認證制度之研究」，輔仁大學法律學研究所，民國 88 年 6 月。
4. 吳孟真，「線上拍賣交易模式法律關係之研究」，國立成功大學法律學研究所，民國 92 年 7 月。
5. 林麗真，「電子商務契約民事法律問題之研究」，國立台北大學法律學研究所博士論文，民國 93 年 6 月。
6. 林惠徵，「公開憑證基礎建設之研究-屬性憑證運用在權限管理」，中國文化大學資訊管理研究所，民國 91 年 6 月。
7. 林國祥，「政府機關網路憑證管理之研究－以警察機關爲例」，中央警察大學，資訊管理研究所，民國 91 年 6 月。
8. 陳群顯，「電子簽章法之研究」，東吳大學法律學系研究所碩士論文，2000 年 7 月。
9. 郭玲伶，「電子載貨證券在海運上應用之風險管理」，國立台灣海洋大學航運管理研究所碩士論文，2003 年 6 月。
10. 張永志，「中華民國海軍憑證中心之組織架構與建置」，國立交通大學資訊管理研究所，民國 91 年 6 月。
11. 蔡宛宜，「數位簽章立法原則之研究--以美國立法經驗爲借鏡」，國立台灣大學法律研究所碩士論文，民國 87 年 6 月。
12. 鍾秋華，「電子載貨證券憑證機構作業實務之研究」，國立台灣海洋大學航運管理研究所碩士論文，2002 年 6 月。

1. 三、中文網站資料 (2007/07/30 visited)
2. 中華人民共和國電子簽名法，
http://www.people.com.cn/BIG5/shehui/1060/2753437.html

3. 立法院國會圖書館，「各國案例介紹-電子簽章法」，
http://npl.ly.gov.tw/do/www/billIntroductionContent?id=2
4. 台灣網路認，http://www.taica.com.tw
5. 朱瑞陽，電子簽章憑證機構扮演角色與功能，2001 年 12 月 25 日，
http://www.uxb2b.com/news/news-20011225.htm
6. 我國 PKI 互通管理及推動計畫，http://gcis.nat.gov.tw/PKI/main/index.php
7. 交互認證之定義，http://www.nii.org.tw/CNT/info/Report/20011201_3.htm
8. 建置電子商務法制環境 http://gcis.nat.gov.tw/eclaw/default.asp
9. 洪淑芬，數位簽名技術/公開金鑰認證機構涉及和衍生法律問題之探討
http://www.cqinc.com.tw/grandsoft/gim/010/deil01.htm
10. 是方電訊，http://www.chiefca.com.tw
11. 香港電子交易條例，http://www.ogcio.gov.hk/chi/eto/ceto.htm
12. 普華資安股份有限公司，我國憑證機構稽核制研究報告，91 年 12 月 20 日，
http://www.pki.org.tw/Resource/Report/
13. 亞洲公開金鑰基礎建設論壇 http://www.pki.org.tw/
14. 黃鋰，電子簽章憑證機構實務運作制度之研究，2006 年 4 月 15 日
//www.moea.gov.tw/~ecobook/ms/9009/101.htm
15. 跨國電子商務交易法律議題報告（下），2003 年 8 月，
http://www.nii.org.tw/CNT/info/Report/200308_3.htm。
16. 新加坡推動電子商務相關政策研究報告，
http://www.nii.org.tw/CNT/info/Report/20011203_8.htm
17. 經濟部商業司，「電子簽章法」，
http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm
18. 電子商業答客問，「電子商業法規常見問題與解答」，經濟部電子商業應用計畫網站，.http://www.ec. org.tw/service/publish/出版品/電子商業答客問 FAQ.doc
19. 蔡朝安、朱瑞陽公司法修正對公司電子登記業務之影響

http://www.pki.org.tw/Resource/Article/Article_020411_4.asp

20. 網際威信，http://www.hitrust.com.tw/hitrustexe/frontend/default_tw.asp

貳、外文參考資料(2007/07/30 visited)

一、外文書面資料

1. Baum Michael S. and Perritt Henry H., Electronic Contracting, Publishing, and EDI Law, 1991.
2. Certification Authority Guidelines, Japan from Electronic commerce Promotion Council of Japan (ECOM).
3. Judicial Studies Board (2000), Digital Signature Guidelines，Ju-dicial Studies Board.
4. Kaplan,G.L.＆L.A.Bernstein,”Electronic Signatures in Global and National Commerce Act”，The Secured Lender,Sep/Oct.,2000.；Nettie,R.,” Electronic Signatures Legislation Raises New Question.”，Credit Union Magazine,OCT.,2000.

二、外文網站資料

1. "A proposal for a Directive on a common framework for electronic certification services", http://www.ispo.cec.be.
2. Baker & McKenzie (2000), "USA:Electronic Signatures in Global and National Commerce Act", E-Law Alert, http://www.bmck.com/ecommerce/E-SIGN_Act.htm.
3. Digital Signature Act, Malaysia, http://www.mcmc.gov.my/the_law/
4. Electronic Transactions Act, Singapore. http://www.ccs.gov.sg/
5. Electronic Transactions Act, Australia, http://www.austlii.edu.au/au/legis/cth/consol_act/eta1999256/

6. Electronic Transactions Act, Korea，
http://www.bakerinfo.com/apec/koreaapec_main.htm
7. "The requirement of a 'Signed' Contract", Contract Law in Cyberspace--Lesson 5, http://www.ssrn.com/update/lsn/cyberspace.
8. "Towards a European Framework for Digital Signatures and Encryption ", http://www.ispo.cec.be/eif/policy.
9. UNCITRAL, Uniform Rules on Electronic Signatures, December 2001. http://uncitral.org/english/electcom/m1-ec.htm
10. 日本日本認證服務 JCSI ，http://www.jcsinc.co.jp/
11. 美國 VeriSign Inc., http://www.verisign.com
12. 新加坡 Netrust Pte Ltd., http://www.netrust.net
13. 新加坡憑證中心管理局（Controller of Certificate Authority）, http://www.cca.gov.sg/eta/

附錄一：憑證用戶合約比較表

憑證機構	網際威信股份有限公司 (HiTRUST)	台灣網路認證股份有限公司 (TWCA)	是方電訊股份有限公司（CHIEF）	VeriSign	Netrust	Japan Certification Services, Inc. (JCSI)
國家	台灣	台灣	台灣	美國	新加坡	日本
合約名稱	憑證用戶合約	臺灣網路認證公司客戶認證作業約定條款	是方全球憑證服務 Class1 個人數位憑證用戶約定條款	VeriSign Public Certification Services Client ID Subscriber Agreement	Netrust Digital Certificate Application Form Subscriber Agreement	加入者同意書（タイプ 1 個人加入者用）
合約條款內容						
業者之義務	第二條 通知義務 其具體內容爲「在接受用戶憑證申請處理時不論用戶所申請憑證有否獲准，HITRUST 有義務通知其處理結果。」	第二條 服務範圍 共有以下義務：註冊服務、憑證簽發服務、憑證展期服務、憑證廢止服務、憑證索取/查詢服務、申請及掛失服務、註銷服務等	第八條 雙方義務 「是方電訊將遵循是方全球憑證服務憑證實務作業基準及相對應之憑證政策，維運其憑證及儲存庫服務，簽發、更新、暫時停用及廢止憑證，並公布憑證狀態資訊。」	第二條 通知義務 其具體內容爲「在接受用戶憑證申請處理時不論用戶所申請憑證有否獲准，HITRUST 有義務通知其處理結果。」 簽發憑證之義務若申請憑證獲准，公司即須依用戶憑證合約簽發憑證給客戶。	憑証實務作業基準-2.1.1.1 憑證機構義務 Netrust 公司將義務訂定於其憑證實務作業基準之一般條款其內容爲 Netrust 公司有確保公開金鑰密碼演算法不被洩露的義務；公司須維護私密金鑰資訊內容之安全的義務。	第六條 告知義務 JCSI 基於法令規定有就特定事項對憑證用戶之，其具體規範爲公司需主動告知以下事項：與用戶相關正確資訊之提供、電子簽章有等同簽名的效力，以及一定要使用公司所規定之電子簽章演算法等。

	簽發憑證之義務 若申請憑證獲准，公司即須依用戶憑證合約簽發憑證給客戶。	第九條 保密義務 「除法令或雙方另有約定外，任何一方對於使用服務系統所獲得之他方資料，原則上負保密之責，但因提供本系統憑證廢止及查詢服務所需，本公司有權公布客戶之相關資料。」	建立客戶身分識別及鑑別程序之義務 依是方全球憑證服務憑證實務作業基準章節三建立之。			

業者之保證責任與否認條款	第六條 保證責任 「HiTRUST 保證於製作憑證時，將會盡合理之注意，以確保用戶憑證上所載資訊之正確性；以及保證用戶之憑證、廢止憑證服務與儲存庫之使用，符合該公司之憑證實務作業基準(CPS)所規範所有具重要性的要件。」 第七條 保證責任否認 除第六項的保證責任外，HiTRUST 不負其他明示或默示的保證責任；因使用 HiTRUST 服務所下載或獲得的文件或資料，係經由憑證用戶自己獨立判斷並承擔相關風險；	未規定 保證責任 TWCA 並未如同 VeriSign 以及 HiTRUST 兩家公司，在其憑證用戶合約訂定所謂公司之保證責任條款。	第九條 保證責任 是方電訊之保證責任，限於以其憑證用戶合約、已公告之相對應憑證政策、憑證實務作業基準及相關規範有明示承諾者爲者，此外是方並未有其他明示或暗示之保證或義務；另外客戶因使用、傳遞、授權或執行其憑證、數位簽章或任何其他與本合約相關之交易或服務有違反合約之侵權行爲或違法行爲，而引起信賴憑證者或其他第三者損失時，是方電訊不負擔任何賠償責任；或 class1 等級之憑證所有者，其行爲或其結果，逾是方電	第六條 保證責任 「VeriSign 保證於製作憑證時，將會盡合理之注意，以確保用戶憑證上所載資訊之正確性；以及保證用戶之憑證、廢止憑證服務與儲存庫之使用，符合該公司之憑証實務作業基準(CPS)所規範所有具重要性的要件。」 第七條 保證責任否認 除第六項的保證責任外，VeriSign 不負其他明示或默示的保證責任；因使用 VeriSign 服務所下載或獲得的文件或資料，係經由憑證用戶自己獨立判斷並承擔相關風險；VeriSign 對	憑証實務作業基準-2.2.1.1 保證責任 NETRUST 之保證責任規範，訂定於其憑證實務作業基準，其內容爲 NETRUST 之保證責任除依憑證實務作業基準約款外，不負其他明示或默示的保證責任。除憑證實務作業基準 1.3.6.1 所載應用範圍外，NETRUST 不負任何其他憑證應用方式，所導致之任何種類損失。	憑証實務作業基準-2.2.1 保證責任 JCSI 之保證責任，並未於其憑證用戶合約規定該公司有何種保證責任，但在其憑証實務作業基準內有例如公開及私密金鑰作成時要確定親自交給憑證用戶；受理、確認並處理憑證用戶之失效申請等的一些程序性之保證事項。

	HiTRUST 對用戶從第三者所購得的產品或服務，不負任何保證責任。」		訊保證或義務範圍者是方亦不負擔任何賠償責任。	用戶從第三者所購得的產品或服務，不負任何保證責任。」		

業者之賠償責任	第九條 賠償責任 HiTRUST 之賠償責任，其僅就直接損害負責，對於所失利益、特別的、附隨的及必然的損害賠償責任均不負責。	第十二條 賠償責任 TWCA 因故意過失致客戶或第三者發生損害須負賠償責任，但例外若得以補行程序方式填補者，得以補行程序方式爲之。 第十一條 責任區分條款 雙方因發生事故致損害他方或第三者，其責任區分及賠償處理，可分事故發生（a)可明確歸責於一方者，由該方單獨負責;（b）由雙方連帶負擔者，原則上由雙方平均負擔;（c）不可歸責於任一方者，且受害之第三人亦無過失，雙方均免責，但向應負責之人請求賠償來彌補受害之第三人；（d）因不可抗力所致者，雙方對任何人均免責。」	第十一條 賠償責任 若有因可歸責於是方電訊之疏失而造成憑證用戶之失時，是方電訊應負擔賠償責任。	第九條 賠償責任 VeriSign 之賠償責任，其僅就直接損害負，對於所失利益、特別的、附隨的及必然的損害賠償責任均不負責。	憑証實務作業基準-2.2.1.2 賠償責任 NETRUST 對其自身賠償責任之規範，訂定於憑證實務作業基準內：除僅就因用戶使用憑證所致之直接損害負責外，對於間接性、特別性或可預見後果之使用所生之損害，均不負任何損害賠償責任。	第十六條 賠償責任 若有違反依合約及所訂定的憑證實務作業基準上所載其所應負之責致用戶受有損害時，用戶得請求損害賠償，其具體的賠償方法，於爭議產生時，JCSI 會向用戶明示。但不可歸責 JCSI 之事由所生之損害、所失之利益，不負賠償責任。

業者之賠償責任限制	第九條 賠償責任限制 Hitrust 賠償限額，乃依憑證的等級而各自有其賠償責任數額之上限爲新台幣 3,500 元；第二級新台幣 175,000 元；第三級新台幣 3,500,000。且前述上限數額均維持不變，與憑證的數位簽章、交易或請求的次數無關，HiTRUST 無義務就任一憑證所生之事故逾額給付。	第十二條 賠償責任限制 「如 TWCA 所造損害不得以補行程序方式加以填補者，賠償金額以當期服務費用之一百倍爲上限。」	第十一條 賠償責任限制 因可歸咎於是方，造成客戶損失時，是方對該用戶及該憑證信賴者之賠償金額，不論憑證所牽涉之交易電子簽章之次數、賠償之原因或所設服務之內容，皆以新台幣 3,000 元爲上限。	第九條 賠償責任限制 就特定憑證對任何人因使用或信賴該憑證所負的總計責任，無論數位簽章、交易或請求的次數，上限數額均維持不變，具體內容如下：第一級美金 $100.00；第二級美金 $5,000.00；第三級美金 $100,000.00，且並無義務就任一憑證所產生之事故爲逾額給付。	第九條 賠償責任限制 NETRUST 將其賠償責任限制在新加坡幣 10000.00。	第十六條 賠償責任限制 JSCI 對於一張憑證之賠償額上限，和人數交易、簽章、訴訟等次數無關，均爲日幣 1,000,000 元，其與提供 JSCI 憑證服務相關之業者，JSCI 與這些關係人對於同張用戶憑證之合計賠償額，其上限亦不會超越前述之金額。

業者之免責事由與不可抗力條款	第十條 免責事由之不可抗力條款 若任一方因不可抗力事件（地震、洪水、火災、颱風、自然災害、戰爭等）致不能履行合約義務的全部或一部，不構成違約；無法履行合約義務的一方仍應盡力履行，且該方應於該事由發生後五日內以書面告知他方。若超過卅日以上者，則未受影響的他方有權立即終止本合約。；責任限制的第一點，HiTRUST 僅就符合 NetSure 保障計畫」所核定之金額負責。	第九條 免責事由 TWCA 對客戶未妥善保存私密金鑰而遭竊或遭僞造所導致之損害，不負賠償責任。」	第十五條 免責事由之不可抗力條款 凡因不可抗力之事由，致該方當事人不能依合約規定履行義務時，該方當事人毋庸對他方負責，唯仍應提出書面說明。	第十條 免責事由之不可抗力條款 若任一方因不可抗力事件（地震、洪水、火災、颱風、自然災害、戰爭等）致不能履行合約義務的全部或一部，不構成違約；無法履行合約義務的一方仍應盡力履行，且該方應於該事由發生後五日內以書面告知他方。若超過卅日以上者，則未受影響的他方有權立即終止本合約。；責任限制的第一點，VeriSign 僅就符合 NetSure 保障計畫」所核定之金額負責。	憑證實務作業基準-2.1.1.4 免責事由之不可抗力條款 Netrust 將不對任何起因於天災或其他的不可抗力因素，以致不能或延遲履行合約義務者致生之金錢損失、損害或罰金負賠償之責。以上的事件將包括罷工,或其他的勞工爭議，暴動，市民騷動及行爲或天災,戰爭，火災，爆炸事故，地震，洪水或其他災難。	第十二條 免責事由之不可抗力條款 「type1 服務之暫時中斷」，只要發生以下情形，JCSI 不僅無須事前向用戶通知，亦不需負任何責任，其內容具體規定如下：公司遭逢須保有提供 type1 服務所需之設備之緊急情況時；遇火災、停電、天災或者戰爭、暴動、及勞資爭議等場合時；電信業者中斷電信服務之時；因技術上或運作上的理由公司所爲之服務中斷。

準據法與爭議解決模式	第十三條 準據法 「與合約有關的爭議，以中華民國法律爲準據法，但並不適用涉外民事法律適用法。」 第十四條 爭議解決 「因合約內容而發生爭議時，在訴諸任何爭議解決機制前應先通知 HiTRUST 及與爭議有關的人士，以尋求爭議的解決。若於爭議通知後，未於三十天內解決，憑證用戶得採取包括以訴訟方式爲之的爭議解決機制，並應以台北地方法院爲第一審管轄法院。」	第十四條 準據法 「本約定條款以中華民國法律爲其準據法。」 第十五條 爭議解決 「因本合約條款所發生之任何糾紛或爭議而涉訟者，應以台灣台北地方法院爲第一審管轄法院。」	未規定 準據法 是方之憑證用戶合約內，並未規定其準據法，但以該公司所在地爲我國，依法理自應以中華民國法律爲其準據法。 第十六條 爭議解決 「關於合意管轄之規定，電子簽章法公司與憑證用戶因憑證用戶合約所發生之任何爭議或糾紛，雙方均同意以台北地方法院爲第一審理管轄法院。」	第十三條 準據法 「與本合約相關的爭議，以美國加州州法爲準據法，但不包括衝突法。」 第十四條 爭議解決 客戶得以該合約爲基礎，自行決定任何爭端解決機制，但先決條件爲須立即通知 VeriSign。而若通知後六十天之內仍無法解決爭端，得尋求其他方法，例如（a）以北加州地區的美國地方法院、或位於加州Santa Clara 高等或郡立的巡迴法庭爲專屬管轄法院；或	憑証實務作業 基準-2.4.3 準據法與爭議解決 Netrust 對於 NETRUST 將其爭議解決方式規範於憑證實務作業基準內容中。 若該公司與憑證用戶雙方發生爭端而無法自行協商解決，這時須依新加坡國際仲裁中心之規則，於新加坡提起交付仲裁解決之，其作成之仲裁決定爲最終且具有拘束雙方的效力。	未規定 準據法 JCSI 之憑證用戶合約內，並未規定其準據法，但以該公司所在地爲日本，依法理自應以日本法律爲其準據法。 第十八條 爭議解決 「所有與 A_Sign Public Service 之合約有關的爭議，均以東京地方法院爲第一審專屬合意管轄法院。」

				（b）依國際商會 ICC 的調解和仲裁規則，由一個或一個以上的仲裁人解決。		

憑證用戶個人資料保護	第十八條 憑證用戶個人資料保護 依該合約因而取得客戶之相關資訊，HiTRUST 會依實務作業基準規定予以保護，內容爲 HiTRUST 不會在憑證服務過程中收集任何個人之資訊，除非資訊所有者明確且自願提供；並且亦會採取安全措施，以保護資訊所有者之資訊不會遺失、被盜用或被更改；而在網站傳輸個人資訊時會加密所有者提供之所有資訊；以合理注意來避免洩露個人資訊；保證不會將個人資訊轉賣或提供給其他買	憑證實務作業基準 - 3.8.1 第二項 憑證用戶個人資料保護 TWCA 於管理及使用用戶相關資訊時，除用戶憑證內容可公開外，其憑證用戶之身分與認證基本資料，非由憑證用戶同意或主管機核可，不得任意對外公開；以及非由憑證用戶同意不得任意銷售或租借，此外使用於憑證管理系統的任何私密金鑰皆給予妥善且隱密之保護。 第九條 保密義務 「除法令或雙方另有約定者外，用戶對使用 TWCA 系統所獲之屬資料應負保密	憑証實務作業基準 -2 .8 機密資訊 憑證用戶個人資料保護 是方規定在其憑證實務作業基準，其具體內容爲是方電訊於處理憑證簽發或申請時所取得與憑證用戶有關之個人及公司資訊，應遵循之合約規範，確保其機密性，原則上未經憑證用戶同意不應任意對外揭露，但若法令要求則不在此限；因憑證作業或管理而求而需使用與存取憑證用戶資訊，應由受授權之可信賴者提出申請並經權責主管核准；保證憑証用戶個人機密資訊絕不對外銷售、租借或使	第十八條 憑證用戶個人資料保護 VeriSign 得於憑證上放置客戶所提供的特定資訊，亦得公布客戶的憑證及其狀態資訊於儲存庫，並可取得該資訊。	憑證實務作業基準 – 2.8.1.1～2 憑證用戶個人資料保護 屬於憑證用戶重要且具敏感性之資訊除非法律有特別規定，否則在未經其同意前不得洩露給他人，並且該資訊不能被使用在非處理憑證作業與管理以外之其他目的；欲揭露憑證用戶個人資訊需得其授權；若審核結果及其相關資訊涉及敏感，則非由 Netrust 授權不得洩露他人；Netrust 除非法律規定有明示之必要,否則 Netrust 不能洩露與管理簽署者憑證相關之資訊。	第十五條 憑證用戶個人資料保護 有關「個人資料之處理」之規定，JCSI 只出於提供憑證服務之目的，才可以使用個人資料；且原則上不提供個人資料給用戶以外之第三人。

	主或作其他商業之應用。另外該資訊亦提供給美國 VeriSign 公司。	之責，且不因用約定條款終止或因其他原因失效而免除。」	用於其他業務用途；以及該公司不得使用其私密金鑰。			

用戶之義務	第三條 憑證廢止或效期屆滿義務 當憑證效期屆滿或接獲憑證廢止之通知時，用戶即不得再用該憑證於任何用途。「用戶申請時服務時，應負自行通知其交易夥伴有關憑證廢止之義務。」	第十條 通知義務 「用戶申請時服務時，應負自行通知其交易夥伴有關憑證廢止之義務。」	第八條 提供正確資訊義務 客戶於憑證申請時，應提供完整及正確資訊，並保證其皆屬事實；瞭解合約義務客戶須瞭解是方憑證實務作業基準及其憑證政策所規範之憑證核准、限制及禁止使用之範圍； 維護金鑰安全義務 用戶應安全地產製及保護其私密金鑰，並採取必要防範措施，以防止私密金鑰遭破解、遺失、揭露、修改或未經授權之使用與存取；當任何可能導致用戶之私密金	第三條 憑證廢止或效期屆滿義務 當憑證效期屆滿或接獲憑證廢止之通知時，用戶即不得再用該憑證於任何用途。	憑證實務作業基準- 2.1.4 憑證用戶義務 憑證用戶瞭解並同意其提供的資料非機密性，且允許利用其資訊於商業行爲，其利方式包括對他人散布該資料。並同意遵守並履行憑證實務作業基準及其憑證政策所載之各條款及義務，包括（a）嚴格遵從對憑證的申請和私密金鑰之妥善保管及使用程序；（b）提供真實、正確的資料在憑證申請表中；（c）確定私密金鑰具有適當的保護；（d）瞭解與憑證有關的憑證實務作	第六條 告知義務 憑證用戶有以下的告知義務用戶在申請憑證服務時，應將其正確之個人資訊告知JCSI；用戶在其私密金鑰有遭破解、遺失、外洩之虞，而有變更或廢止憑證之必要時，應立即告知JCSI 及提出失效之申請；再者爲合約亦對用戶課以須妥善保管公開金鑰與私密金鑰之義務。

			鑰或保護私密金鑰之啓動資訊遭破解之事件發生或用戶憑證內資訊不正確或變更時代，用戶應遵循第七條之規循第七條之規範請求廢止該憑證； 保證義務 用戶應保證使用己爲用戶接受且有效之憑證製作其數位簽章。」		業基準及其憑證政策之約款，並遵守相關的憑證使用限制約款; （e）任何可能導致憑證遭破解，包括遺失，誤放或暴露憑證用戶私密金鑰事件發生時，憑證用戶必須立即通知實際之管理者。	

用戶之保證責任	第六條 保證責任 客戶在向 HITRUST 申請憑證時，保證其所提供之資訊正確無誤；且亦需保證該憑證資訊不會侵害第三者的智慧財產權，亦未使用於非法的用途；自憑證產製起客戶須善加管理私密金鑰，且該憑證僅能用於符合合約授權及合法的目的範圍內；用戶須明示同意本合約約定，以作爲取得憑證的先決條件等事項。	未規定 保證責任 TWCA 之用戶憑證合約規範，並未和 HiTRUST 及 VeriSign 一樣，有所謂客戶所應負擔之保證責任部分。	憑證實務作業基準- 2.2.5 保證責任 「分別爲憑證用戶應保證下列事項：使用憑證內之公開金鑰對應之私密金鑰所製之電子簽章即爲憑證用戶之數位簽章；使用已被用戶接受且有效憑證製其數位簽章；安全保護其私密金鑰及防止未授權之存取；憑證申請時提供資料皆真實；依照憑證實務作業基準及相關政策合法使用憑證等。」	第六條 保證責任 客戶在向 VeriSign 申請憑證時，保證其所提供之資訊正確無誤；且亦需保證該憑證資訊不會侵害第三者的智慧財產權，亦未使用於非法的用途；自憑證產製起客戶須善加管理私密金鑰，且該憑證僅能用於符合合約授權及合法的目的範圍內；用戶須明示同意本合約約定，以作爲取得憑證的先決條件等事項。	未規定 保證責任 Netrust 對其憑證用戶保證責任之規範，在其用戶憑證合約內，並未如同 HiTRUST 及 VeriSign 之用戶憑證合約，有所謂客戶所應負擔之保證責任部分。	未規定 保證責任 JCSI 對其憑證用戶保證責任之規範之規範，並未和 HiTRUST 及 VeriSign 一樣，於用戶憑證合約有所謂客戶所應負擔之保證責任部分。

用戶之賠償責任	第八條 賠償責任 凡憑證用戶因違反依本合約應負的義務或責任；或提供的憑證資訊有虛假或不實陳述；或侵害他人智慧財產權；或未揭露憑證資訊上重要的事實，而此不實陳述或疏漏係起源於客戶的過失或意圖欺騙另一方等因素；或未依本合約維護私密金鑰，或使用值得信賴的系統，或採取有效措施防止私密金鑰的安全妨害、遺失、洩漏、竄改或未經授權的使用等情形發生，致第三人對追償時，負擔並賠償	憑證實務作業基準 - 3.2.3 賠償責任 TWCA 在其憑證實務作業基準(CPS)規定有以下之情事發生的話，應由用戶負擔其損害賠償責任，分別是：有用戶向註冊中心申請註冊時，因故意、過失或不當意圖提供不實資料致憑證機構或第三者受損害；用戶應妥善保管私密金鑰及密碼，若有故意或過失造成註冊中心、憑證機構或第三者受損害者；用戶提出廢止或暫停用戶憑證後，用戶有未廢止憑證之使用及立刻通知相關信賴憑證者停	第九條 賠償責任 爲用戶因使用、傳遞、授權或執行其憑證、數位簽章或任何其他與本合約相關之交易或服務或有違反本合約之侵權行爲或違法行爲，而引起信賴憑證者或其他第三人直接或間接損失應由用戶負損害賠償責任；而依用戶的爲或結果逾是方保證或義務範圍者，原則是方不負責，但例外依法令由是方負損害賠償責任時，用戶應全額賠償其因此所支付之金額。	第八條 賠償責任 凡憑證用戶因違反依本合約應負的義務或責任；或提供的憑證資訊有虛假或不實陳述；或侵害他人智慧財產權；或未揭露憑證資訊上重要的事實，而此不實陳述或疏漏係起源於客戶的過失或意圖欺騙另一方等因素；或未依本合約維護私密金鑰，或使用值得信賴的系統，或採取有效措施防止私密金鑰的安全妨害、遺失、洩漏、竄改或未經授權的使用等情形發生，致第三人對追償時，負擔並賠償	憑證實務作業基準 賠償責任 若有以下的情形，憑證用戶應負損害賠償責任： 2.3.1.1 因憑證用戶個人之疏失，導致憑業者、註冊中心、信賴憑證交易者有損失、訴訟費用及其他各項支出情形時； 2.3.1.2 憑證用戶於申請或製作憑證及對第三人使用簽章時，若有提供不實資料之情事致憑證機構或第三者受損害者；憑證用戶未妥善保管私密金鑰，並將其使用在不值得信賴之系統上所致之損害； 2.3.1.3 用戶未採取	第七條 賠償責任 用戶有遵從記載於憑證實務作業基準及憑證政策內所載用戶義務、憑證政策、憑證實務作業基準，及本合約之用戶義務；另外憑證用戶於使用憑證從事交易時必項判斷其行爲有無符合合約第七條規範。

	HITRUST 因此所受損害及相關費用的責任，其中包括律師費用。而且，任何有關的和解應事先得到 HITRUST 的書面同意，否則對 HITRUST 不生效力。而本項規定不受本合約終止或解除的影響。	止該憑證之使用的情形；用戶使用憑證有違反憑證實務作業基準或其他相關規範、或將憑證使用在其他業務範圍或違反相關法令規範或主管機關明定禁止之業務範。		VeriSign 因此所受損害及相關費用的責任，其中包括律師費用。而且，任何有關的和解應事先得到 VeriSign 的書面同意，否則對 VeriSign 不生效力。而本項規定不受本合約終止或解除的影響。	必要的措施去防止私密金鑰資料之洩露、內容被竄改或未經授權使用等情事，所遭致之損失。」	

用戶之免責事由	第十條 免責事由之不可抗力條款 免責事由方面規定在第十項，即爲若任一方因不可抗力事件（地震、洪水、火災、颱風、自然災害、戰爭等）致不能履行合約義務的全部或一部，不構成違約；無法履行合約義務的一方仍應盡力履行，且該方應於該事由發生後五日內以書面告知他方。若超過卅日以上者，則未受影響的他方有權立即終止本合約。	第十一條 免責事由之責任區分 「雙方因發生事故致損害他方或第三者，其責任區分及賠償處理，可分爲事故發生（a）可明確歸責於一方者，由該方單獨負責；（b）由雙方連帶負擔者，原則上由雙方平均負擔；（c）不可歸責於任一方者，且受害之第三人亦無過失，雙方均免責，但向應負責之人請求賠償來彌補受害之第三人；（d）因不可抗力所致者，雙方對任何人均免責。」	未規定 免責事由	第十條 免責事由之不可抗力條款 免責事由方面規定在第十項，即爲若任一方因不可抗力事件（地震、洪水、火災、颱風、自然災害、戰爭等）致不能履行合約義務的全部或一部，不構成違約；無法履行合約義務的一方仍應盡力履行，且該方應於該事由發生後五日內以書面告知他方。若超過卅日以上者，則未受影響的他方有權立即終止本合約。	未規定 免責事由	未規定 免責事由

資料來源：工研院電通所，「認證服務契約研究」，我國 PKI 互通管理及推動計畫、PKI 法律及政策研究報告，民國 92 年 2 月。

附錄二：信賴憑證者合約比較表

憑證機構	網際威信股份有限公司 (HiTRUST)	台灣網路認證股份有限公司 (TWCA)	是方電訊股份有限公司（CHIEF）	VeriSign	Netrust	Japan Certification Services, Inc. (JCSI)
國家	台灣	台灣	台灣	美國	新加坡	日本
合約名稱	信賴憑證者	無	是方全球憑證服務 信賴憑證者協議書	VeriSign Relying Party Agreement	無	依存者同意書（タイプ1）（Accredited Sign パブリックタイプ1サービス依存者利用規約）
合約條款內容						
規範重點	HiTRUST	TWCA	CHIEF	VeriSign	Netrust	JCSI

業者之義務	未規定	未規定	第四條 是方電訊之義務：是方保證（a）安全憑證儲存庫及 CRL 之可用性；（b）遵循憑證實務作業基準（CPS）及相對應之憑證政策（CP）規範，於簽發憑證時確保憑證包含所有憑證格式所要求之資訊，憑證資料之正確性；（c）依據各等級憑證做身分識別與鑑別。	未規定	未規定	未規定

業者之保證責任與保證責任之限制	第九條 保證責任 HITRUST 保證（a）除「未經確認的憑證用戶資訊」外，憑證中所有或以參照併入的資訊皆爲正確；（b）當憑證公布於儲存庫中時，該憑證已簽發給憑證上所列名的憑證用戶，且憑證用戶已藉由網站下載或經由含有憑證的電子郵件送達而接受該憑證；（c）憑證用戶均遵守憑證實務作業基準。 第十項 保證責任之否認 HITRUS 不負其他明示或默示的保證責任。信賴憑證者須獨立判斷任何因使用 HITRUS 服務所下載	未規定 保證責任	未規定 保證責任	第九條 保證責任 VeriSign 保證（a）除「未經確認的憑證用戶資訊」外，憑證中所有或以參照併入的資訊皆爲正確；（b）當憑證公布於儲存庫中時，該憑證已簽發給憑證上所列名的憑證用戶，且憑證用戶已藉由網站下載或經由含有憑證的電子郵件送達而接受該憑證；（c）憑證用戶均遵守憑證實務作業基準。 第十項 保證責任之否認 VeriSign 不負其他明示或默示的保證責任。信賴憑證者須獨立判斷任何因使用 VeriSign 服務所下載	未規定 保證責任	第七條 保證責任 JCSI 在其 public type1 服務之信賴憑證者合約（依存者利用規約）第七項提到，JCSI 僅對於記載在信賴憑證者合約，以及憑證政策（CP）之「本公司責任」範圍，負保證責任及義務。

	或獲得的文件及資料，並承擔相關風險。對於從第三者所購得的得的產品或服務，HITRUST 不負任何保證責任。			或獲得的文件及資料，並承擔相關風險。對於從第三者所購得的產品或服務，VeriSign 不負任何保證責任。		

業者之賠償責任	第十二條 賠償責任 HiTRUST，僅就直接損害負責，對於所失利益、特別的、附隨的及必然的損害賠償責任均不負責任。	未規定 賠償責任	第九條 賠償責任 是方之保證及義務，以合約、憑證實務作業基準、憑證政策及相關規範有明示承諾者爲限。因憑證用戶而引起信賴憑證者或其它第三者直接或間接之損失時，或逾是方義務範圍者，則不負擔任何責任。且信賴憑證者須自行獨立判斷所下載或獲得的文件或資料，並承擔相關風險。對於從第三者所購得的產品或服務，是方亦不負責。」	第十二條 賠償責任 VeriSign，僅就直接損害負責，對於所失利益、特別的、附隨的及必然的損害賠償責任均不負責任。	未規定 賠償責任	第十一條 賠償責任 依信賴憑證者合約及憑證實務作業基準與憑證政策所訂定 JCSI 之責任，信賴憑證者受有損害時，得請求損害賠償；但不可歸責 JCSI 之事由所生之損害、所失之利益，則不負任何賠償責任。同時第十二項規定，信賴憑證者爲依照電子簽章法所訂定之檢核規定，而使用該憑證時，JCSI 不負任何責任。同樣地，信賴憑證者怠於確認電子郵件帳號之有效性，JCSI 亦不負任何責任。」

業者之賠償金額限制	第十二條 賠償責任限制 HiTRUST 其賠償責任限制憑證等級第一級，爲新台幣 3,500 元；第二級新台幣 175,000 元；第三級新台幣,500,000 元。	未規定 賠償責任限制	第十二條 賠償責任限制 VeriSign 就特定憑證對任何人因使用或信賴該憑證所負的總計責任，訂有賠償責任上限，其憑證等級第一級，爲 100 美金；第二級新台幣 5,000 美金；第三級新台幣 100000 美金。另外無論就特定憑證的數位簽章、交易或請求的次數爲何，上限數額均維持不變，VeriSign 無義務就任一憑證所生之事故逾額給付。	第六條 賠償責任限制 「因可歸責於是方之疏失而造成信賴憑證者損失應負損害賠償責任，而賠償金額以下列金額爲上限：Sub-CA 等級爲憑證年費之兩倍；Class1 憑證爲新台幣 3000 元；Class2 憑證爲新台幣 175000 元；Class3 憑證爲新台幣 3500000 元。」	未規定 賠償責任限制	第十一條 賠償責任限制 內容爲：「無關交易、簽章、訴訟等次數或人數，一張憑證所引起的賠償額訂有上限，其上限額爲日幣 1,000,000。JCSI 與委託提供憑證服務的相關者，該憑證之合計賠償額，亦不會超越前述之上限。」

免責事由與不可抗力條款	第十七條 免責事由之不可抗力條款 VeriSign 信賴憑證者合約亦有免責事由，即不可抗力之規定，於合約，若任一方因不可抗力事件（地震、洪水、火災、颱風、戰爭等），致不能履行合約義務的全部或一部，不構成違約；無法履行合約義務的一方仍應盡力履行，且該方應於該事由發生後五日內以書面告知他方。若超過卅日以上者，則未受影響的他方有權立即終止本合約。	未規定 免責事由	第十七條 免責事由之不可抗力條款 VeriSign 信賴憑證者合約亦有免責事由，即不可抗力之規定，於合約，若任一方因不可抗力事件（地震、洪水、火災、颱風、戰爭等），致不能履行合約義務的全部或一部，不構成違約；無法履行合約義務的一方仍應盡力履行，且該方應於該事由發生後五日內以書面告知他方。若超過卅日以上者，則未受影響的他方有權立即終止本合約。	第十四條 免責事由之不可抗力條款 內容爲因天災、戰爭等不可歸責於一方當事人之不可抗力事由，致該方當事人無法履行合約之義務時，該方當事人毋庸對他方負責，唯仍應提出書面述明。	未規定 免責事由	未規定 免責事由

準據法與爭議解決模式	第十四條 爭議解決 以中華民國法律爲準據法，但不適用「涉外民事法律適用法」。至於因合約而引起的爭議，而根據合約第十五項爭議解決之規定，信賴憑證者在訴諸任何爭議解決機制之前，須通知 HiTRUST 及其他與爭議相關的任何人。若爭議未於通知後三十天內解決，得採取包括訴訟的爭議解決機制。合約之涉訟，應以 台灣台北地方法院爲第一審管轄法院。	第十四條 爭議解決 TWCA 並無信賴憑證者合約，但依法理應比照依其客戶認證作業約定條款的規定，在第十四條應以中華民國法律爲準據法，而管轄法院方面，依第十五條因本公約之任可糾紛而涉訟者，雙方同意以台灣台北地方法院爲第一審管轄法院。	第十六條 爭議解決 應以下列式處理：1.爭議之一方須提供詳細必要內容及要求賠償之書面通知給被要求賠償之另一方，其通知後雙方並應主動會面協調；2.爭議若無法三十天內解決，應將其交由雙方同意之調停者處理，並無拘束雙方的權限；3.若爭議無法在調停後五天內解決，則雙方同意進入仲裁或訴訟程序；4.進入仲裁程序後，雙方於調停後置作業五個工作天內決定仲裁者，並以台北市爲雙方諮詢仲裁者之意見，並同意接受其裁決；5.	第十四條 爭議解決 依其信賴憑證者合約規定，是以美國加州之法律爲準據法，並排除其衝突法則之適用規定，且亦不適用聯合國之國際貨物買賣合約規範，至於在合約第十五項爭端解決方式，可自行決定任何解決爭端機制，但須通知 VeriSign，於通知後六十天仍未解決，則可（a）至北加州地區的美國地方法院、或位於加州 Santa Clara 高等或郡立的巡迴法庭進行訴訟；（b）最終應在國際商會 ICC 的調解和仲裁規則下，由一個或一個以	未規定 爭議解決 並未有信賴憑證者合約之制定，而對與信賴憑證者有關之爭議解決方式，亦應依其憑証實務作業基準之規定，即爲若該公司與憑證用戶雙方發生爭端而無法自行協商解決，這時須依新加坡國際仲裁中心之規則，於新加坡提起交付仲裁解決之，其作成之仲裁決定爲最終且具有拘束雙方的效力。	未規定 爭議解決 JCSI 在其 public type1 服務之信賴憑證者合約（依存者利用規約）內並未規定爭議解決方式，故應比照其用戶憑證合約（加入者利用規約）第十八條規定，與 public type1 服務有關之利用規約所生的紛爭，均應以東京地方法院爲第一審專屬合意管轄法院。

			雙方同意以台灣台北地方法院爲第一審管轄法院，而在合約第十八條有合意管轄之規定，亦再確認一次以台灣台北地方法院爲第一審管轄法院。	上的仲裁人做必需的修改以解決爭端。		

信賴憑證者之義務	第五條 信賴憑證者之義務 信賴憑證者負擔下列義務： （a）獨立評估憑證爲任何特定目的而使用的妥適性，並使用於適當的目的； （b）使用適當的軟體、硬體來執行數位簽章驗證等運作； （c）查核欲信賴的憑證狀態，且對其憑證鏈中的所有憑證亦應查核； （d）前述所有的核驗若均爲成功，則可信賴此憑證； （e）若亦爲憑證用戶，同意受相關的憑證用戶合約所拘束。」	憑證實務作業基準-3.1.5 「信賴憑證者應依憑證內容所規定的業務範圍，及本作基準的規範使用於相關的業務系統，無任何違反相關法律的規定與侵害第三者的權利；信賴憑證者使用憑證時，應依憑證標準之憑證鏈逐一驗證該憑證的有效性及正確性，當有廢止清冊的安全機制時尚需檢核憑證是否爲廢止或暫時停用憑證；驗證交易訊息的有效性時，除驗證用戶憑證的有效性與合法性外，須依該公司憑證實務作業基準與業務系統相關規範	第三條 信賴憑證者之義務 「信賴憑證者應於信賴憑證前： （a）查詢最新版本之CRL或OCSP資料，以確認憑證有效或無效； （b）鑑別憑證用途，並僅於該憑證合法使用範圍內信賴該憑證； （c）遵循憑證實務作業基準（CPS）及相對應之憑證政策（CP）規定之任何其他相關義務； （d）應先驗證CRL 或OCSP資料簽發者數位簽章之有效性； （e）若信賴一無效之憑證，或使用於限制或禁止用途之憑	第五條 信賴憑證者之義務 信賴憑證者負擔下列義務： （a）獨立評估憑證爲任何特定目的而使用的妥適性，並使用於適當的目的； （b）使用適當的軟體、硬體來執行數位簽章驗證等運作； （c）查核欲信賴的憑證狀態，且對其憑證鏈中的所有憑證亦應查核； （d）前述所有的核驗若均爲成功，則可信賴此憑證； （e）若亦爲憑證用戶，同意受相關的憑證用戶合約所拘束。」	憑證實務作業基準-2.1.5 有關其信賴憑證者之義務，規定在其憑證實務作業基準：信賴憑證者有熟悉「憑證實務作業基準與憑證政策有關用戶憑證條款規定」之義務，且只能在合約所賦予憑證之使用範圍內使用之；信賴憑證者在利用憑證時有檢核憑證效力及正確性之義務。	第六條 信賴憑證者之義務 JCSI 在其public type1服務之信賴憑證者合約（依存者利用規約）第六項亦提到，信賴憑證者需同意憑證實務作業基準（CPS）及相對應之憑策（CP）中的信賴憑證者義務之規定，其義務內容包括： 1.信賴憑證者對用戶憑證之使用限制的理解，信賴憑證者只能在憑證用戶所記載使用目的之範圍內使用。 2.信賴憑證者於電子簽章的檢查或憑證利用時，一定要進行其有效性的確認不可。

		的規定，驗證交易限額賠償限額、使用業務範圍及法律的權責關係。」	證，該信賴憑證者應負擔其風險。」			

信賴憑證者之保證責任與賠償責任	未規定 保證責任 第十一條 賠償責任 信賴憑證者之損害賠責任 （a）未履行信賴憑證者的義務；或 （b）對憑證的信賴在該情況下係不合理 （c）未查核憑證狀態以判斷憑證是否已逾期或被廢止；發生致第三人對 VeriSign 追償時，須負擔並賠償 VeriSign 因此所受損害及相關費用的責任（包括律師費用）。且此規定不受本合約終止或解除的影響。	未規定 保證責任 憑證實務作業基準-3.3.1 第三者免責權 有關信賴憑證者之責任方面，規定在其憑證實務作業基準：因信賴憑證者或用戶的故意或過而非爲憑證機構或註冊中心之疏失造成第三者財務、信譽及其他各方面之損害時，憑證機構或註冊中心享有賠償責任豁免權，若因信賴憑證者之疏失且可歸責於信賴憑證者，而造成憑證機構或註冊中心或第三者財務、信譽及其他各方面之損害時，信賴憑證者須負損害	未規定 保證責任 第五條 賠償責任 有兩項責任分別爲：信賴憑證者應同意並確認在選擇信賴憑證資訊前，已有足夠資訊以供其作成決定，且依本合約及憑證實務作業基準規定使用儲存庫、CRL 及 OSCP 服務。應對是否信賴該憑證資訊的決定單獨負責，且同意並接受若未履行該合約所規定的信賴憑證者義務，則需自行承擔法律後果。信賴憑證者應負責檢查其欲信賴之憑證之有效性，信賴憑證者若未確實執行信賴憑證者	未規定 保證責任 第十一條 賠償責任 HiTRUST 之信賴憑證者合約亦在第十一規定有信賴憑證者之損害賠責任，其具體內容規範直接參照。	未規定 保證責任 憑證實務作業基準-Netrust 將信賴憑證者責任規定在其憑證實務作業基準，當中規定信賴憑證者應遵循 2.1.5 所載義務，因違反該義務致生符合 2.2 或 2.3 所載之，因利用憑證所致憑證機構之損失、訴訟費用或其他支出，信賴憑證者需負損害賠償責任。	未規定 保證責任 第八條 賠償責任 信賴憑證者須參考其憑證實務作業基準規定，信賴憑證者須負擔自行決定是否相信憑證用戶之憑證而與之交易後所生的一切責任與後果；第九條亦規定信賴憑證者不可利用憑證去作違反公序良俗或犯罪之行爲，以及禁止信賴憑證作有違信賴憑證者合約規定之使用憑證或進行驗證之行爲，且若因以上行爲而使 JCSI 遭受到損害時，信賴憑證者應負損害賠償責任。

		賠償責任。	之義務，應自負擔其財物損失及法律後果。			

0信賴憑證者免責事由	第十七條 免責事由 若信賴憑證者有遭受地震、颱風等不可抗力事件，在憑證業者部分內，已有詳細說明，所以在此不再討論。	未規定 免責事由	第十四條 免責事由 是方之信賴憑證者合約第十四條有不可抗力的規定，其內容在本節 1.憑證業者內之是方電訊部分已作說明，不再重覆之。	第十七條 免責事由 VeriSign 之相關說明規定即可，而第十七項不可抗力之規定，HiTRUST 與其技術提供者 VeriSign 相同。	未規定 免責事由	未規定 免責事由

資料來源：工研院電通所，「認證服務契約研究」，我國 PKI 互通管理及推動計畫、PKI 法律及政策研究報告，民國 92 年 2 月。

附錄三：附錄一及二憑證機構之簡介

一、臺灣

1. 網際威信股份有限公司(HiTRUST)

網際威信（以下簡稱 「HiTRUST 」）成立於 1998 年 3 月，爲電子認證服務 VeriSign 公司在台灣之合作夥伴。網路安全認證服務 （eCommerce Security）爲 HiTRUST 服務項目之一 ，包括 金融 XML PKI 管理服務 、 VeriSign PKI 管理服務、VeriSign 伺服器數位憑證、金融 XML 註冊認證安控系統、i-Security、應用系統安控模組 X-SMS、VeriSign 個人數位憑證、Hardware Security Module 硬體安控模組等 。目前經核定的憑證實務作業基準計有：（1）網際威信 VTN 憑證 實務作業基準；（2）網際威信（金融 XML 憑證）憑證實務作業基準；（3）台灣商務最高憑證中心憑證實務作業基準。[122]

2. 臺灣網路認證股份有限公司(TWCA)

臺灣網路認證（以下簡稱「TWCA」）由臺灣證券交易所、財金資訊公司、關貿網路公司、臺灣證券集中保管公司，及其他資訊業者所組成。目前經核定的憑證實務作業基準，計有：（1）信用卡 SET）憑證機構憑證實務作業基準；（2 ）金融最高層憑證機構（TFCA ）憑證實務作業基準；（3）金融政策憑證機構（TFPCA ）憑證實務作業基準；（4）網際 NB 憑證、企業 EC 憑證、商務 EC 憑證、金融 XML 憑證憑證實務作業基準；（5 ）台灣金融用戶憑證機構（TFUCA）憑證實務作業基準。[123]

3. 是方電訊股份有限公司(CHIEF TELECOM)

是方電訊成立於 1991 年 1 月，初期是系統整合廠商，1996 年轉型爲電信寬頻廠商 ，2000 年轉變爲二類電信業者。另外，爲提供憑證服務，成立是方

[122] webside：http://www.hitrust.com.tw/hitrustexe/frontend/default_tw.asp

[123] webside： http://www.taica.com.tw

全球憑證中心（Chief Certificate Authority）。是方憑證機構提供讓客戶依自己的需求申請各憑證。其憑證分爲：（1）Class1 憑證：讓個人適用於文件或電子郵件之加密及簽章；（2）Class2 憑證：讓自然人或法人適用於電子商務交易之加密及簽章；（3）Class3 憑證：此憑證爲最高之保證等級，適用於網路銀行、網路下單、安全網站服務等 。目前經核定之憑證實務作業基準只有 「是方全球憑證服務憑證實務作業基準」。[124]

二、美國

VeriSign Inc.

VeriSign 每日服務數千個企業與數百萬的客戶的聯繫，並傳遞關鍵性的基礎建設服務 讓網路與通訊網更加地信賴與安全。該公司藉由三大類之服務，即安全服務（Security Services）、通訊服務（Telecommunication Services）、諮詢服務（Directory Services ），創造可信賴的環境。

在該公司的產品與服務「Security & Payment Services」之項目中，分爲（1）商業安全（Commerce Security ）；（2）網路與應用安全（Network & Application Security）；（3 ）內容安全（Content Security）。[125]

三、新加坡

1.Netrust Pte Ltd.

Netrust 成立於 1997 年 5 月，是東南亞的第一個憑證中心（Certification Authority），參加 Netrust 的企業在 Keppel Telecommunications & Transportation（Keppel T&T），和 Network for Electronic Transfers（Singapore ）Pte Ltd（NETS）之間。

Netrust 提供個人、企業、政府組織完整的線上鑑別與安全基礎建設，以確保藉

[124] webside：http://www.chiefca.com.tw

[125] webside：http://www.verisign.com，2007/8/7 visited。

由網路和其他無線媒體等電子傳輸之安全。

在 Netrust 的憑證服務中，有（1）Public CA Service、（2）Private Label CA Service、（3 ）PKI Hosting Service。在 Public CA Service 中，又分爲 Netrust Net-ID Certificates、SSL Web Server Certificates、 WAP Server Certificates。[126]

四、日本

日本認證服務 JCSI

日本認證服務股份有限公司（Japan Certification Services,Inc.，以下簡稱「JCSI」)，爲日本現今憑證機構中，最早接受主管機關認定的「特定認證業務」之業者。

JCSI 的憑證服務種類可分爲：（1）SecureSign；（2 ）AccreditedSign；（3）PaymentSign。而 AccreditedSign 又分爲「AccreditedSign public service」及「AccreditedSign private service 」；「AccreditedSign public service 」是 JCSI 符合日本電子簽章法的特定認證業務之項目。在此項目中，分爲：（1）「type 1 service」：此類的電子憑證並無設定其使用範圍，且自 2002 年 4 月 1 日起，將憑證用戶之住址記載於記載項目中。（2 ）「type 2 service」：此類憑證是憑證用戶與政府間的申請、提出之使用目的，但非與政府的電子申請全部適用之。[127]

[126] webside：http://www.netrust.net，2007/8/7 visited。

[127] webside：http://www.jcsinc.co.jp/，2007/8/7 visited。

2.5 cm

96

1 cm

碩士論文

2.5 cm

電子簽章法關於憑證機構管理規範之研究

3 cm

交通大學 管理學院碩士在職專班 科技法律組

1 cm

96

碩士論文

電子簽章法關於憑證機構管理規範之研究

交通大學 管理學院碩士在職專班 科技法律組

2 cm

宋浸琪

3 cm