立法會CB(1)343/99-00(03)號文件

(立法會秘書處譯本，只供參考用)

(香港律師會用箋)

郵遞及傳真文件

香港中區
昃臣道8號
立法會大樓
立法會
陳美卿小姐

陳小姐：

《電子交易條例草案》委員會

閣下1999年11月4日的來函收悉。隨文附上香港律師會就條例草案提交的意見書，請閣下將意見書代轉法案委員會委員參閱。

謹此告知閣下，律師會將委派以下代表出席會議：

馬覺思先生
文國權先生

執業者事務部總監

(簽署)

(黃淑玲女士)
電郵地址：dpa@hklawsoc.org.hk

連附件

副本致：馬覺思先生 —— 不連附件
文國權先生 —— 不連附件

1999年11月10日

香港律師會(律師會)就《電子交易條例草案》提交的意見書

1. 引文

《電子交易條例草案》("條例草案")

"加拿大的法例模式" —— 加拿大劃一法例委員會審議的《劃一電子商貿法令》(1999年8月擬稿)。

"歐盟的法例模式" ——《歐洲議會及歐洲理事會就電子簽署的共通架構發出的指令建議》 (1999年3月25日)。

"新加坡的法例模式" —— 1998年《電子交易法令》。

"《聯合國電子貿易標準法例》" —— 聯合國全體大會於1996年11月通過的《聯合國國際貿易法例委員會電子貿易標準法例》。

"美國聯邦的法例模式" —— 《劃一電子交易法令》擬稿。該擬稿已提交劃一州立法例專員全國委員會(National Conference of Commissioners on Uniform State Laws)在科羅拉多州丹佛市召開的第108屆週年大會席上作最後通過(1999年7月23至30日)。

"立法會參考資料摘要" —— 香港特別行政區就條例草案發出的立法會參考資料摘要(ITBB/IT 107/4/1 (99) VIII)。

2. 數碼簽署

條例草案其中一項要旨是"*使電子交易中所使用的電子紀錄及數碼簽署，將如同文件交易的紀錄和簽署般獲得法律承認*"，主要原因是為了"*推動電子商貿在香港的發展*"(立法會參考資料摘要，第2段)。

條例草案第6條規定：

> "*如任何法律規則規定須由任何人作簽署，或規定文件未被任何人簽署則會有某些後果，則該人的數碼簽署即屬符合該規則，但只在有認可證書證明該數碼簽署及該數碼簽署是在該證書的有效期內產生的情況下，該數碼簽署方屬符合該規則。*"

這意味着認可核證機關發出的證書必須包含數碼簽署，該簽署才會獲得法律承認。

簽署可發揮多項作用：證明某人的身份、證明某人有意認證某份文件、將某人與某份文件的內容相聯、明確指出某人與某份文件有關。因此，有關法例應涵蓋所有形式的電子簽署，而不應只局限於承認數碼簽署。

條例草案似乎是採用功能對等的方針，期望令以電子形式進行的商業活動與傳統的文件交易方式在功能上達致對等，但條例草案第6條的條文卻未免過於限制性。事實上，政府擬採用科技中立的總體方針來草擬條例草案，但第6條的用意卻是鼓勵核證機關向資訊科技署署長申請認可(立法會參考資料摘要第10段)，兩者互相矛盾。

《聯合國電子貿易標準法例》就數碼簽署作出如下規定：

> *"(1) 如法例規定有關人士作出簽署，若在數據訊息(意思約相等於條例草案所指的電子紀錄)中使用以下方法，即屬已履行有關規定：*
>
> *(a) 利用某種方法以證明該人的身份及指出該人認同數據訊息的內容*
>
> *(b) 從原先產生或傳達有關數據訊息所希望達到的目的而言，並考慮及所有因素包括任何相關協議，所使用的方法是可靠和恰當的。"*

既然條例草案第7和第8條都依循了這個包含範圍廣泛的方針來草擬，何以又同時在條例草案中將使用數碼簽署另外區別出來？此舉實在令人費解。上文提及的《聯合國電子貿易標準法例》條文的焦點集中於簽署所發揮的兩項作用：

(a) 證明建立文件的人的身份；及

(b) 表明該人認同文件的內容。

上文(b)條確立以靈活的方針處理電子簽署的保安問題，既不禁止使用認可證書，又能較為恰如其份地讓市場自行因應建立電子紀錄的目的訂定適當的保安措施，而市場亦可在這個過程中參考法院案例。該條文不但容許締約各方藉私人協議確立所要求的保安水平，亦使法院在審理案件時能夠按此而考慮某宗交易的前因後果。

資訊科技及廣播局對律師會提出的意見作出回應時指出，該局不採用更為科技中立的方針，原因是：

> *"直至目前為止，數碼簽署以外的電子簽署技術尚未成熟，在市場上亦缺乏共通的標準。"*

然而，這個解釋與科技中立方針的精神自相矛盾，亦與當局不鼓勵科技朝着某個方向發展的宗旨不相稱。我們在北美、歐盟及新加坡的準貿易夥伴或競爭對手都沒有採用如此限制性的方針，亦沒有跡象顯示它們計劃日後採取這種方針。

條例草案把電子簽署的保安機制局限於由持牌／認可核證機關負責運作並設於香港的公開密碼匙基礎建設的保安機制。

如要令公開密碼匙基礎建設得以運作，核證機關(不論是否已獲得認可資格)必須首先要求擬發出電子訊息的發訊者出示身份證明以便核實該人的身份；一般而言，該人在所難免必須以書面方式親自出示其身份證明文件。然而，這個第一階段的核實工作並不能完全排除出現欺詐的情況。舉例來說，銀行亦曾經遇到欺詐個案，某些客戶會以虛構身份在銀行開立戶口，雖然銀行已經面見該客戶，但由於該人使用偽造的身份證明文件，以致銀行受騙。如發訊者並非居於香港，上述過程便會變得更為錯綜複雜。假如獲香港政府認可的核證機關所經營的是全球核證服務，該核證機關要進行這個第一階段核實工作便會有困難。若核證機關要依賴海外代理人，便會損害整個系統的完整性，因為某些國家可能根本沒有持牌／認可核證機關。

密碼技術業曾經進行討論，認為按照香港政府倡議的電子交易模式草擬的數碼簽署條例，無異於為商界訂立一個根本無法在市場立足的運作模式(C. Bradford BIDDLE的著作"Legislating Market Winners"，電郵地址：biddlecb@cooley.com)。

鑒於這個行業的性質特殊、創新科技日後會朝甚麼方向發展又是未知之數，業界標準又尚未有定論，故此當局如能在草擬條例草案時參照《聯合國電子貿易標準法例》或新加坡的法例模式，將會是較為可取的做法。若當局沿用條例草案內較為限制性的措辭，反而可能會使香港在這方面的發展與國際發展趨勢及標準"脫節"。資訊科技及廣播局指出，條例草案制定成為條例後，當局會視乎情況所需對該法例作進一步修訂，但此舉實在並非處理上述問題的有效方法。

要在國際貿易界爭取出類拔萃的表現，香港與海外貿易夥伴進行電子商貿時便必須採取積極主動的政策。若選擇國際上大部分競爭對手早已摒棄的"穩打穩紮"路向，到頭來或會一事無成，兼且無法達到"激發未來經濟增長的動力"的預期成效。

參閱附錄1：就美國、歐盟、加拿大及新加坡所採用的政策進行的分析。

3. 核證機關的法律責任

第36條

促進電子商貿工作的其中一個主要障礙在於保安問題。雖然利用核證機關作為可信賴的第三者是確保電子商業交易可以在網上安全進行的重要一環，但核證機關本身卻必須在可行範圍內採取最嚴密的保安措施，方可保持其系統的完整性。條例草案使用"穩當

系統”一詞，期望利用這個科技中立的詞彙來確保個別核證機關各自利用適當的機制來確保其核證服務穩當可靠，而有關的詳細規定則可由資訊科技署署長發出的業務守則加以補充。

不過，其中一項極為重要的環節是如何保持核證機關的私人密碼匙完整無缺。在很大程度上，這個問題不能與核證機關日常使用穩當系統提供服務的問題混為一談。當然，如果核證機關的日常運作能夠分毫不差、永無錯漏，自然最為理想，*但這個始終是不切實際的目標*。核證機關一旦遺失其私人密碼匙，便可能導致巨大的損失。舉例說，如有人得悉核證機關的私人密碼匙，該人便可以發出無限張表面上可以生效的偽造證書。

此外，如果核證機關本身的私人密碼匙外泄，而對應的公開密碼匙又被撤銷，則所有由該核證機關發出的證書都會無效。所有採用該核證機關服務的客戶都會被迫申領新的證書。雖然實際情況如何仍須視乎核證機關與有關客戶簽訂的合約的實際條款而定，但核證機關很可能會在合約內盡量豁除本身所須承擔的法律責任。此外，假如客戶因而所蒙受的損失與向核證機關追索補償的費用相比屬微不足道，在這個情況下，客戶很可能不會對有關核證機關採取任何法律行動。

然而，假如條例草案的宗旨是要鼓勵消費者和商界參與電子商貿活動，則這類損失的風險便不應由消費者承擔，尤其必須考慮到，消費者對認可核證機關的期望往往遠高於未獲認可的核證機關。當然，如要認可核證機關完全承擔因遺失私人密碼匙而導致損失的法律責任，涉及的數額可能會過於龐大。條例草案只是規定核證機關須以穩當方式保存該等資料，但當局實應在條例中而非在業務守則中訂明核證機關須妥為保存資料的水平。條例草案第36條似乎完全沒有觸及這個問題。

4. 對公共政策感關注的事項

另一值得關注的事項在於認可核證機關一旦無力償債或破產，有關的財務責任將會如何分配。當局應否將認可核證機關須為其預期的法律責任購買適當的保險，列為核證機關獲得認可的其中一項規定？若然，該項規定應否在條例草案中明文規定，而非交由資訊科技署署長酌情決定？

此外，條例草案給予根據該條例執行職務的公職人員豁免權，可免遭檢控。當局在此事上賦予資訊科技署署長酌情權，可就每宗申請自行決定有關的方法及費用(如有的話)，是否明智之舉？有關程序的適用情況應該絕對劃一，不應由資訊科技署長以其廣泛的酌情權按情況作出決定。

香港律師會
1999年11月9日

附錄1：

背景資料摘要：美國、歐盟、新加坡及香港所採用的電子簽署、數碼簽署及核證機關

1. "數碼簽署"

擬在電子訊息／紀錄上簽署的準簽署人首先向核證機關申請配對密碼匙，該配對密碼匙包括私人密碼匙及其在數學上相關的公開密碼匙。私人密碼匙由準簽署人持有，以建立與電子訊息／紀錄相連的數碼簽署，而公開密碼匙則交予核證機關，公開給公眾查閱。電子訊息／紀錄的收訊者會利用公開密碼匙核實有關電子訊息／紀錄的數碼簽署及其數據的完整性。

核證機關核對準簽署人的身份，並採取其他所需的步驟以確保準簽署人的身份與其所聲稱的身份確實相符。核證機關繼而發出證書，證明準簽署人與其交予核證機關的公開密碼匙相符。

數碼簽署只不過是芸芸電子簽署形式當中的其中一種而已。電子簽署的形式不勝枚舉，並各具不同的保安特徵。電子簽署可以說是一個一般用語，本身並無包含任何保安方面的涵義。本意見書在提述"電子簽署"時，將會套用這個概念。

2. **美國聯邦的法例模式**

由劃一州立法例專員全國委員會(National Conference of Commissioners on Uniform State Laws)擬備並於最近公布的《劃一電子交易法令》擬稿(連序言及書記註錄)，採用了盡量少加規管的方針。換而言之，擬議的法例條文只是提供指示性的方針，以確保在現行法例下，電子簽署和手書簽署的待遇完全一樣，並且不會為"安全"的電子簽署提供任何法律保障。該委員會認為，在可行範圍內盡量令電子簽署與手書簽署兩者完全對等至為重要。該法令第106條有關法律承認的條文訂明：

第106條 電子紀錄、電子簽署及電子合約的法律承認事宜

(a) 不得純粹因為某紀錄或簽署屬電子形式而否定其法律效力或可強制執行性。

(b) 不得純粹因為某合約是利用電子紀錄訂立而否定其法律效力或可強制執行性。

(c) 凡任何法例規定紀錄須是書面形式，或規定紀錄並非書面形式會有某些後果，則電子紀錄即屬符合該法例的規定。

(d)　凡任何法例規定由任何人作簽署，或規定文件未被任何人簽署會有某些後果，則電子紀錄如包含電子簽署，即屬符合有關法例的規定。

"電子簽署"泛指"與電子紀錄相連的或在邏輯上相聯的電子聲響、符號或程序，而該等電子聲響、符號或程序是某人為簽署電子紀錄的目的而簽立或採用的" (第9頁)

截止1999年5月24日為止，只有密蘇里州、猶他州和華盛頓州制定了限制性的法律承認法例，規定電子簽署必須為數碼簽署，並須經持牌／認可的核證機關發出有效的證書核實，才可獲法律承認為與手書簽署具有同等效力。美國其他各州仍未採用這種限制性的立法方針。

3. 歐盟的法例模式

歐洲委員會在其最近(1999年3月25日)發表的《歐洲議會及歐洲理事會就電子簽署的共通架構發出的指令建議》中，通過以下意見：

第7段："……為促使歐盟各國透過開放的網絡提供核證服務，一般而言，核證服務供應商應可隨意提供服務而無須事先獲得授權。事先獲得授權並非單單是規定有關的核證服務供應商須在獲准提供其核證服務前取得國家機關的批准，同時亦指具有相同效力的其他措施。"

第10段："……電子簽署的法律承認問題應建基於客觀準則，而不應與服務供應商獲得授權與否有任何關連。"

基於上述各項原則，歐洲委員會建議採納下列方針(第8頁)：

第5條
法律效力

1.　成員國須確保，任何先進電子簽署只要獲得合資格的證書證明並由安全的簽署裝置所產生，該先進電子簽署即 ——

(a)　就電子形式的數據而言，符合有關簽署的法例規定，猶如手書簽署符合與書面數據有關的法例規定一樣；及

(b)　在法律程序中可予接納作為證據。

2.　成員國須確保，不得純粹因為有關的簽署屬電子形式、或該電子簽署並未獲得合資格的證書證明、或該電子簽署並未獲得由認可核證服務供應商發出的合資格證書證明、或該電子簽署並非由安全簽署裝置所產生，便否定其法律效力及其在法律程序中作為證據的可接納性。

"電子簽署"泛指"與其他電子紀錄相連的或在邏輯上相聯並以此作為認證方法的電子形式數據。"

比利時盧曼市一間大學(Katholieke Universiteit Leuven)法律系轄下的法律與資訊科技聯合中心，較早時為歐洲委員會轄下負責內部市場及財經服務的單位擬備了一份題為《數碼簽署的法律問題》(The Legal Aspects of Digital Signatures)(1998年10月)的研究報告。據該份報告的結論顯示，"*德國透過立法方式訂定保安標準，不一定會廣為市場接納。只要市場不接納，這個標準便形同於無。*"

4. 新加坡的法例模式

新加坡所採用的模式是以《聯合國國際貿易法例委員會的電子貿易標準法例》(《聯合國電子貿易標準法例》)為藍本，承認電子簽署與手書簽署具有同等效力，同時並無就電子簽署的保安資格訂定標準。1998年《電子交易法令》第8條述明：

電子簽署

8(1). 凡任何法律規則規定由任何人作簽署，或規定文件未被任何人簽署會有某些後果，則電子簽署即屬符合有關法律規則的規定。

(2) 電子簽署可以任何方式予以核實，包括表明該電子簽署業已經過一個程序，而在這個程序當中，其中一方必須簽立一個符號或執行一個保安程序以核證該電子紀錄屬於該方，有關交易方可繼續進行。

在第2條，"電子簽署"泛指"與其他電子紀錄相連的或在邏輯上相聯的數碼形式的任何字母、字樣、數目字或其他符號，而該等字母、字樣、數目字或其他符號是為認證或承認該紀錄的目的而簽立或採用的。"

新加坡的《電子交易法令》只是將經由有效證書證明而產生的數碼簽署確認為安全的電子簽署，換而言之，就是推定該簽署真確無訛並完整無缺，直至相反證明成立。電子簽署本身與手書簽署無異。這樣，有關各方便可以便捷的方式自由進行電子交易，他們亦可自行決定是否採用不符合特定資格的電子簽署，而不論該簽署是否經過核實，又或是否經由持牌或無牌(或經認可或未經認可)的核證機關發出。

5. 加拿大的法例模式

加拿大劃一法例委員會在審議《劃一電子商貿法令》(1999年6月擬稿)時有如下看法：

> *"如出現某簽署是否歸屬某人的問題，這類問題屬於須予核證的事實問題。令人質疑的通常都並非某簽署是否歸屬某人的問題，而是有關簽署到底是否存在的"事實"。"*

建議在加拿大採用的模式與新加坡模式相若，兩者都將電子簽署承認為與手書簽署具有同等效力，而又沒有訂明構成電子簽署所需的任何保安資格。