《2001 年稅務(修訂)(第 2 號)條例草案》委員會

政府當局就委員會於 2002 年 12 月 13 日會議席上所提關注事項的回應及跟進行動

引言

法案委員會在 2002 年 12 月 13 日會議席上要求政府當局：

(a) 就透過「公共服務電子化計劃」系統提供的電子遞交報稅表服務，作出以下的改良：

(i) 按納稅人要求發出認收電郵，確認收妥以電子方式遞交的報稅表；

(ii) 研究接受現時被其他操作系統(例如：Linux)支援的其他中文軟件的可行性；

(iii) 在系統投入服務一年後，透過「公共服務電子化計劃」提供「貯存/繼續」功能；以及

(iv) 讓納稅人檢索上一年提交的電子報稅表，以便納稅人在修改電子報稅表上某些項目後即可遞交，而無須把全部資料再次輸入。

(b) 在條例草案作以下修改：

(i) 修改條例草案第 2（b）條，以區分分別用於簽署報稅表和認證身分的數碼簽署與通行密碼；以及

(ii) 提出委員會審議階段修正案的修訂草稿，以釋議員疑慮。

(c) 研究是否可以提供已付郵費的回郵信封以便納稅人寄回紙張報稅表，並在有需要的情況下跟稅款一併收回郵費。

2. 政府當局對以上事項的回應與跟進行動詳列如下。

按納稅人要求以電郵認收報稅表

3. 稅務局會按照建議，提升在「公共服務電子化計劃」系統提供的遞交報稅表服務，增設功能讓納稅人選擇由稅務局另發電子郵件，認收以電子方式遞交的報稅表。稅務局預計在 2004 年 4 月推出這項新功能。

與其他中文軟件的兼容性

4. 在我們示範如何透過「公共服務電子化計劃」系統使用網上報稅服務時，其中一位議員詢問該系統是否可以支援其他中文輸入法，包括手寫板等。我們的答案是肯定的。我們當時亦指出所有被「視窗」操作系統支援的輸入法(包括手寫板在內)，都會獲「公共服務電子化計劃」系統接受。至於網上報稅服務是否支援其他操作系統(例如 Linux)的問題，我們的答覆是暫時並不支援。然而，稅務局會不斷檢討和改良在「公共服務電子化計劃」平台操作的報稅系統的功能和兼容性，包括對其他操作系統(例如 Linux)的支援。

提供「貯存/繼續」功能

5. 稅務局會在「公共服務電子化計劃」的遞交報稅表系統提供「貯存/繼續」功能，讓納稅人在未能一次過填妥電子報稅表所須項目時，可以暫時貯存已輸入的資料，以便日後可在電腦檢索有關資料作修改或繼續填報之用，然後以電子方式遞交給稅務局。由於提升系統需時，稅務局預計會在 2004 年 4 月才推出這項新功能。

提供「檢索」功能以翻查去年的電子報稅表資料

6. 稅務局會提升「公共服務電子化計劃」的遞交報稅表系統，提供「檢索」功能，讓納稅人檢索在上一年度經「公共服務電子化計劃」平台遞交的報稅表，作爲填報現年度電子報稅表的預填擬本。這項功能將讓大部分納稅人只須更新或修改電子報稅表上的幾個項目即可提交報稅表，大大簡化手續。這樣，納稅人會更樂意以電子方式報稅。同樣，由於提升系統需時，稅務局預計會在 2004 年 4 月推出這個新功能。

修改條例草案第 2（b）條，以區分分別用於簽署報稅表和認證身分的數碼簽署與通行密碼

7. 條例草案第 2(b)條爲《稅務條例》加入第 2(5)條，訂明納稅人在根據該條例須提交報稅表的規定下，「簽署」一詞可提述爲包括採用數碼簽署或通行密碼[1]作爲認證或承認該報稅表。上述建議要求政府當局考慮把用以簽署報稅表的數碼簽署與用作認證而非簽署報稅表的通行密碼加以區分。

8. 工商及科技局就《電子交易條例》的檢討於 2002 年 11 月 7 日提交給立法會資訊科技及廣播事務委員會的文件中，重申政府一貫的觀點，當穩妥程度足以應付服務所牽涉的風險，個人辨認號碼(PIN)在指定情況下可被接納作爲一種電子簽署形式以符合法例上有關簽署的規定，這可讓使用者有更多選擇和更大的方便。我們認爲提交報稅表正是這類情況。

9. 我們須指出，個人辨認號碼(PIN)可被接納爲電子簽署的形式。在聯合國國際貿易法例委員會(UNCITRAL)電子商務組發出的電子簽署「示範法頒布指南」(見附錄)中，個人辨認號碼(PIN)，甚至乎點「確認」按鈕的行動等，都被視爲「電子簽署」的例子。

10. 我們亦研究過一些准許使用通行密碼以電子方式提交報稅表的國家的法例。

11. 在澳洲，按 Taxation Administration Act 1953， 第 388-60 條規定，任何人向稅務局局長遞交報稅表，都必須在核准的表格上聲明所申報的資料均屬真確無誤。該法例第 388-75 條亦規定，如報稅表是以電子方式遞交，報稅者便須將他的電子簽署載入聲明書中。如報稅者是以電話報稅，他亦須將其電話簽署載入聲明書中。上述電子簽署和電話簽署皆釋義爲經由局長批准的專用識別號碼，實際上亦即是通行密碼。就此而言，澳洲的法例把通行密碼特定爲一種簽署方式。

12. 在加拿大，當局並無明確指出通行密碼是否當作一種簽署。不過，加拿大的 Personal Information Protection and Electronic Documents Act 第 35 條規定，如議會法案(Act of Parliament)有條文訂立表格，負責執行該條文的有關當局可就相應的電子表格制定規例，而電子表

[1] 條例草案第 2(b)條原本也包括提述採用"任何其他形式的簽署"，但政府當局已同意刪除有關字眼，並在 2002 年 12 月 13 日提交委員會審議階段修正案擬稿。

格的內容須大致上與該條文所訂立的表格相若。電子表格的用途，亦同條文所訂表格的用途一樣。換言之，如紙張形式的表格須要簽署(如報稅表的情況)，相應的電子表格亦須要簽署。要符合這項要求，實際上是採用通行密碼作簽署。

13. 在英國，Income Tax (Electronic Communications) Regulations 2000 第 3 條規定，任何人都可以就某些指定的事項，以及在符合若干條件的情況下使用電子通信。當中的一項條件，就是他必須使用核准的認證方法，透過電子通信方式傳送資料。通行密碼便是用來認證遞交報稅表的核准方法。

14. 至於在美國，Internal Revenue Code 第 6061 條規定，有關部長須就接受數碼簽署或其他電子方式簽署而制定有關程序。在該等程序尚未落實的階段，部長可(A)豁免簽署的規定；或(B)就特定種類或類別的報稅表、聲明書、陳述書，或其他根據內部稅法和規定所須或准予遞交的文件，提供其他可供選擇的簽署或署名方法。由 2000 年起，納稅人可使用自行設定的個人辨認號碼，爲其電子報稅表簽署。換言之，該自行設定的個人辨認號碼，是美國當局接受的一種簽署。

15. 新加坡的 Electronic Transactions Act 第 8(1)條訂明，如法例規定需要簽署，又或如文件沒有簽署即會招致某些後果，電子簽署已能符合法例的規定。「電子簽署」的定義與我們的《電子交易條例》內的相同，即指與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爲認證或承認該紀錄的目的而簽立或採用的。這個定義明顯地將通行密碼包括在內。

16. 總括而言，經我們研究的大部分稅區，都接受納稅人在以電子方式報稅時使用通行密碼簽署報稅表，同時，聯合國國際貿易法例委員會(UNCITRAL)亦把個人辨認號碼／通行密碼視爲電子簽署。這個情況尤其切合香港的需要，因香港的報稅表由稅務委員會訂定，其一直都規定要有納稅人的簽署。在這情況下，我們需要確保電子報稅表上附有(通行密碼形式的)簽署，然後與報稅表一併遞交。這樣我們才可在現行《稅務條例》的法律基礎下，把電子報稅表納入規管範圍。該條例第 51(5)條亦訂明，簽署報稅表的人士，須當作知悉該報稅表內的所有事宜。換言之，「簽署」電子報稅表是我們執法的基本依據，只作認證並未能充分切合實際需要。

提供已付郵費的回郵信封並在有需要的情況下跟稅款一併收回郵費的可行性

17. 一位議員認爲稅務局要求納稅人購買並貼上郵票寄回紙張報稅表的安排，爲納稅人帶來不便。我們完全明白議員建議的理由，但認爲實施該建議在技術上有極大困難。

18. 首先，基於財政預算的限制，政府部門目前一律不會爲郵件「預付公務郵資」，這是所有部門都要遵守的政策，稅務局也不例外。因此，稅務局不能提供已付郵資及載有回郵地址的信封以便納稅人將紙張報稅表寄回。再者，由於「郵費」不是《稅務條例》內訂明徵收的稅款，我們不可以把郵費列於有關納稅人的評稅通知書上，並跟稅款一併收回。

財經事務及庫務局
二零零二年十二月

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001

UNITED NATIONS
New York, 2002

three functions (or roles) with respect to electronic signatures, namely, the signatory function, the certification function and the relying function. Two of those functions are common to all PKI models (i.e. creating and relying on an electronic signature). The third function is involved in many PKI models (i.e. certifying an electronic signature). Those three functions should be dealt with irrespective of whether they are in fact served by three or more separate entities (e.g. where various aspects of the certification function are shared between different entities), or whether two of those functions are served by the same person (e.g. where the certification service provider is also a relying party). Focusing on the functions performed in a PKI environment and not on any specific model also makes it easier to develop a fully media-neutral rule to the extent that similar functions are served in non-PKI electronic signature technology.

1. Electronic signatures relying on techniques other than public-key cryptography

33. Alongside "digital signatures" based on public-key cryptography, there exist various other devices, also covered in the broader notion of "electronic signature" mechanisms, which may currently be used, or considered for future use, with a view to fulfilling one or more of the above-mentioned functions of handwritten signatures. For example, certain techniques would rely on authentication through a biometric device based on handwritten signatures. In such a device, the signatory would sign manually, using a special pen, either on a computer screen or on a digital pad. The handwritten signature would then be analysed by the computer and stored as a set of numerical values, which could be appended to a data message and displayed by the relying party for authentication purposes. Such an authentication system would presuppose that samples of the handwritten signature have been previously analysed and stored by the biometric device. Other techniques would involve the use of personal identification numbers (PINs), digitized versions of handwritten signatures, and other methods, such as clicking an "OK-box".

34. UNCITRAL has intended to develop uniform legislation that can facilitate the use of both digital signatures and other forms of electronic signatures. To that effect, UNCITRAL has attempted to deal with the legal issues of electronic signatures at a level that is intermediate between the high generality of the UNCITRAL Model Law on Electronic Commerce and the specificity that might be required when dealing with a given signature technique. In any event, consistent with media neutrality in the UNCITRAL Model Law on Electronic Commerce, the new Model Law is not to be interpreted as discouraging the use of any method of electronic signature, whether already existing or to be implemented in the future.

81. For the assessment of the trustworthiness of the systems, procedures and human resources utilized by the certification service provider, the Model Law provides an open-ended list of indicative factors.

F. A technology-neutral framework

82. Given the pace of technological innovation, the Model Law provides criteria for the legal recognition of electronic signatures irrespective of the technology used (e.g. digital signatures relying on asymmetric cryptography; biometric devices (enabling the identification of individuals by their physical characteristics, whether by hand or face geometry, fingerprint reading, voice recognition or retina scan, etc.); symmetric cryptography, the use of PINs; the use of "tokens" as a way of authenticating data messages through a smart card or other device held by the signatory; digitized versions of handwritten signatures; signature dynamics; and other methods, such as clicking an "OK-box"). The various techniques listed could be used in combination to reduce systemic risk (see A/CN.9/484, para. 52).

G. Non-discrimination of foreign electronic signatures

83. The Model Law establishes as a basic principle that the place of origin, in and of itself, should in no way be a factor determining whether and to what extent foreign certificates or electronic signatures should be recognized as capable of being legally effective in an enacting State (see A/CN.9/484, para. 53). Determination of whether, or the extent to which, a certificate or an electronic signature is capable of being legally effective should not depend on the place where the certificate or the electronic signature was issued (see A/CN.9/483, para. 27) but on its technical reliability. That basic principle is elaborated upon in article 12 (see below, paras. 152-160).

V. Assistance from the UNCITRAL secretariat

A. Assistance in drafting legislation

84. In the context of its training and assistance activities, the UNCITRAL secretariat assists States with technical consultations for the preparation of legislation based on the UNCITRAL Model Law on Electronic Signatures. The same assistance is brought to Governments considering legislation based on other UNCITRAL model laws (i.e. the UNCITRAL Model Law on International Commercial Arbitration, the UNCITRAL Model Law on International Credit Transfers, the UNCITRAL Model Law on Procurement of Goods, Construction and Services, the UNCITRAL Model Law on Electronic Commerce, and the UNCITRAL Model Law on Cross-Border