立法會
Legislative Council

立法會CB(1)2273/01-02號文件

檔號：CB2/BC/12/01

《2001年稅務(修訂)(第2號)條例草案》
背景資料簡介

目的

本文件概述財經事務委員會委員就《2001年稅務(修訂)(第2號)條例草案》所研究的各項主要事宜。

條例草案的目的

2. 現時，透過公共服務電子化計劃(下稱"電子化計劃")使用數碼簽署以電子方式提交報稅表 —— 個別人士及物業稅報稅表，以及使用電子表格提交利得稅報稅表在《電子交易條例》(第553章)中已有規定。稅務局建議提供其他報稅方法，即納稅人可透過電話報稅及透過電子化計劃使用通行密碼提交報稅表。然而，《電子交易條例》或《稅務條例》(第112章)均沒有訂明這些其他方法。

3. 條例草案旨在提供法律依據：

(a) 訂明納稅人透過電子化計劃提交報稅表時，可使用通行密碼認證身份及藉以符合簽署規定；及

(b) 使納稅人可透過電話報稅。

事務委員會的商議工作

4. 內務委員會在2001年11月23日研究條例草案時，部分議員表示關注到以擬議新方式報稅時報稅表所載資料的保安問題。議員決定，有關條例草案在政策方面的問題，包括保安問題應首先交由財經事務委員會研究，然後才決定應否成立法案委員會，研究條例草案。

5. 財經事務委員會委員在2002年1月7日的會議席上所研究的各項主要事宜現綜述於下文各段。

保安方面的問題

6. 政府當局表示，在決定某一電腦系統所須或所應具備的安全水平時，必須充分考慮當中所涉及的風險。資訊科技署曾研究有關讓納稅人可透過電子化計劃使用通行密碼提交報稅表的建議，所得出的結論是，該系統符合"強化加密"的規定，而且足以防禦第三者接達對稱密碼匙，所以在傳送稅務資料方面會達到相當高的安全水平。因此，該系統的安全程度與使用數碼證書無異。

7. 政府當局亦指出，在互聯網使用通行密碼認證身份，尤其在大部分網上銀行服務方面，已經十分普遍，而且美國、加拿大和新加坡等多個其他稅務機構亦已實行網上提交報稅表，並採用通行密碼來認證納稅人身份。

8. 至於透過電話報稅方面，政府當局表示，公共電話網絡已公認為"可信賴網絡"，是銀行和公共事業公司普遍使用的電子交易媒介。在電話網絡系統盜取資料難度極高，而且基於經電話線傳送資料的特質，電話報稅所涉及的安全風險應該很低。其他稅務機構包括美國、加拿大、澳洲和新加坡等，亦已採用電話報稅的做法。

9. 事務委員會部分委員贊成當局為納稅人提供該等擬議新報稅渠道，因為此舉符合政府利用資訊科技改善政府服務的政策。他們認為，雖然在電子交易中使用通行密碼認證身份，並未能達到與使用數碼證書相同的保密程度，但由於現時已有技術可確保資料保安妥善，加上政府當局所制訂的各項措施，因此使用通行密碼在互聯網上提交報稅表是可以接受的方式。他們亦認為，鑒於海外稅務機構在使用通行密碼認證身份方面的成功經驗，以及只要政府當局審慎監督有關系統的運作，該等擬議新報稅渠道應不會引起保安問題。

擬議新報稅方式的成本效益及效率

10. 部分委員對成本效益表示關注。考慮到個別納稅人每年可能只會使用電話報稅系統一次，以及此系統在納稅人之間的使用率可能偏低，他們關注設立及維持該系統是否具成本效益。

11. 政府當局估計，本港將會有80萬名納稅人符合採用電話報稅的資格準則。雖然初期的使用率可能不會太高，但政府當局預計使用率會隨時間而逐漸增加(較長遠而言，使用率可達5%)。實施電話報稅計劃的成本總額約為480萬元，由於以人手處理報稅表及輸入資料的工作得以減省，因此每年所節省的員工開支可達90萬元。

電話報稅系統的效率

12. 事務委員會察悉，平均而言，透過電話提交薪俸稅報稅表需時約5分鐘，而提交物業稅報稅表則需時約4分鐘。電話報稅系統會將整個報稅程序的資料以數碼格式記錄及貯存。納稅人可向稅務局提出書面要求，索取貯存在其稅務檔案的資料的打印紀錄。

與《電子交易條例》的銜接問題

13. 事務委員會關注到條例草案會如何與《電子交易條例》銜接，以及政府當局會否把通行密碼的使用範圍擴展至政府其他電子服務。關於香港會計師公會(下稱"會計師公會")所提出的有關意見，事務委員會察悉李家祥議員所轉達的意見如下 ——

(a) 會計師公會原則上支持盡早推行擬議新服務，為方便提交報稅表提供額外的途徑；

(b) 為使規管電子交易的法律架構保持完整，會計師公會認為在《電子交易條例》中訂明條例草案旨在實施的改變，會是可取的做法；

(c) 儘管如此，會計師公會接受，當局可按照《電子交易條例》第14條的規定，為使用通行密碼在互聯網上提交報稅表及以電話報稅作特定安排；及

(d) 政府當局應把檢討《電子交易條例》列為優先工作，研究《電子交易條例》應否及如何配合電子交易在其他條例已訂明，但在《電子交易條例》未有訂明的特定安排。在檢討《電子交易條例》的過程中，亦應解決《稅務條例》中有關電子交易方面的任何不足之處。

14. 政府當局表示，《電子交易條例》為電子交易建立所需的法律架構。《電子交易條例》第14條訂明，如某條例接納以電子方式提交資料，並載有一項明訂條文，就該目的指明具體規定、程序或其他指定安排，則《電子交易條例》不得解釋為影響該明訂條文。政府的政策原意並不是要把有關電子交易的法律條文全部載於《電子交易條例》內，因為這做法既不可行，亦不切實際。條例草案旨在為互聯網上使用通行密碼認證身份，以提交報稅表及以電話報稅，提供完整和全面的法律架構。

15. 在財經事務委員會會議席上，政府當局表示曾於2002年3月就檢討《電子交易條例》發表公眾諮詢文件，諮詢期於2002年4月30日結束。當局在2002年3月11日向資訊科技及廣播事務委員會簡介該份諮詢文件。政府當局特別指出，透過完善的管理，當局可考慮在特定的情況下，接納以個人辨認號碼作為符合法律上簽署規定的一種電子簽署形式。當局在說明這些特定情況時，曾以條例草案中有關使用通行密碼提交報稅表的建議作為例子。政府當局建議對《電子交易條例》作出修訂，並加入一個新的附表，以便資訊科技及廣播局局長*(請參閱註1)*可藉附屬法例，在新附表內指明有關的法律條文，說明使用個人辨認號碼可獲接納為符合該等條文下簽署的規定。

---

1 資訊科技及廣播局局長過往在《電子交易條例》下可行使的法定職能，已由2002年7月1日起轉移給工商及科技局局長。

條例草案賦予稅務局局長的權力

16. 關於條例草案賦予稅務局局長的額外權力，事務委員會關注到是否有制衡措施。政府當局表示，條例草案賦予稅務局局長的權力只涉及程序上和運作上的細節，有關細節或會隨時間而有所改變。這些事宜並無涉及任何重大的政策影響。海外司法管轄區的有關稅務當局獲賦予相若的權力，就提交電子報稅表的資格準則、形式和方式及簽署規定訂立規例或作出規定。

專業團體發出的函件及有關草擬方面的問題

17. 事務委員會察悉，會計師公會及專業資訊保安協會曾就條例草案致函稅務局局長，而稅務局局長已於2002年1月11日作覆。該等函件的副本載於**附錄IV**。

18. 就該等函件提出的意見，一名委員要求政府當局檢討有關由稅務局局長批准用戶的通行密碼的實際安排，以及檢討草案第8條的擬議第51AA(6)(b)條中，使用"附於"("affix")一詞是否恰當。該委員亦質疑是否有必要在此擬議條文中加入"任何其他形式的簽署"，因為就提交報稅表的事宜而賦予稅務局局長指明認證身份形式的權力而言，這句或會令局長的有關權力範圍不明確。

19. 政府當局表示，根據律政司的意見，條例草案採用"附於"(affixed)及"局長批准"(approved by the Commissioner)的用詞實屬合適。會計師公會建議的用語不足以達到使用"通行密碼"在報稅表上"簽署"的作用。"附於"一詞的普通含意包括"附加一些東西"及"附於一些東西"，因此"通行密碼"可以"附於"報稅表上。不過，政府當局同意動議一項委員會審議階段修正案，刪除條例草案第8條中"任何其他形式的簽署"一句。

有關文件

20. 謹此附上以下有關文件 ——

2002年1月3日發出的立法會CB(1)716/01-02(03)號文件	—— 政府當局就"使用通行密碼以電子方式遞交報稅表的安全問題"擬備的文件，供財經事務委員會2002年1月7日會議之用(**附錄I**)
立法會CB(1)1120/01-02號文件	—— 財經事務委員會2002年1月7日會議的紀要

立法會CB(1)767/01-02號文件	——	財經事務委員會就"使用通行密碼以電子方式及透過電話報稅"提交的報告，供內務委員會2002年1月11日會議之用(**附錄II**)
分別於2002年1月11日及17日發出的立法會CB(1)797/01-02及CB(1)831/01-02號文件	——	庫務局局長於2002年1月11日致財經事務委員會主席的函件(**附錄III**)
分別於2002年1月8日及14日發出的立法會CB(1)749/01-02(02)和(03)及CB(1)805/01-02號文件	——	稅務局局長與會計師公會及專業資訊保安協會的往來函件(**附錄IV**)
2002年3月5日發出的立法會CB(1)1239/01-02號文件	——	政府當局向資訊科技及廣播事務委員會提交有關"檢討《電子交易條例》"的諮詢文件(有關的節錄部分載於**附錄V**)

立法會秘書處
2002年7月12日

二零零二年一月七日
參考文件

立法會財經事務委員會

使用通行密碼以電子方式遞交報稅表的安全問題

目的

本文件為議員簡述稅務局將在系統技術和行政管理方面所採取的措施，以確保納稅人使用通行密碼以電子方式遞交報稅表是在安全及穩妥的情況下進行。

背景

2. 2001年11月21日庫務局局長向立法會提交《2001年稅務(修訂) (第2號)條例草案》，為以下服務提供法律依據：

- 納稅人透過「公共服務電子化計劃」提交報稅表，可使用通行密碼認證身分並藉以簽署作實；以及
- 透過電話遞交報稅表。

3. 為回應立法會內務委員會委員的要求，本文件討論有關使用通行密碼透過電子方式遞交報稅表和以電話報稅的安全問題，並闡述稅務局將採取的系統技術和行政管理措施如何確保納稅人以上述方式提交的報稅資料安全穩妥。

系統技術措施

以通行密碼在「公共服務電子化計劃」平台傳送報稅表資料

4. 使用通行密碼在網上遞交報稅表的安全程度與使用數碼證書無異，不同之處是報稅表以通行密碼簽署，由於系統亦會使用強化加密技術網上傳送資料，因此保密水平不遜於以數碼證書遞交。由於採用加密技術，系統瀏覽器會隨機編製一組數字(一般稱為「對稱密碼匙」)，另提供稅務局的公開密碼匙，把資料由發送點加密傳送到稅務局的接收點，因此報稅表資料會受到站對站式加密保障。另一方面，納稅人的通

行密碼亦會以另一組隨機編製的數字，以及稅務局的公開密碼匙加密，確保達到更佳的保安監控效果。

5. 資訊科技署早前就使用通行密碼與數碼證書這兩個方法，在「公共服務電子化計劃」遞交報稅表方面的安全程度作出研究，結果認為兩個方法均能達到相同的安全水平，符合「強化加密」的規定，亦足以防禦第三者接達對稱密碼匙。由此可見，使用通行密碼這種簽署方法不會令資料的安全程度下降。

6. 事實上，在互聯網使用通行密碼確認身分，尤其在大部分網上銀行服務方面，已經十分普遍。稅務局在「公共服務電子化計劃」用以確認身分的通行密碼所採用的設計安全標準，會與私人電子商貿及網上銀行服務的安全標準相近。

7. 美國、加拿大和新加坡等其他稅務機構都提供網上遞交報稅表服務，而且也採用通行密碼來確認納稅人身分。

經電話網絡傳送報稅表資料

8. 公共電話網絡已公認為〝可信賴網絡〞，是銀行和公共事業公司普遍使用的電子交易媒介。由於截聽電話必須要實際接觸電話線，而且還要安裝特別的解碼設備，因此要在電話網絡盜取資料難度極高。基於經電話網絡傳送資料的特質，電話報稅所涉及的安全風險應該很低。

9. 為探討電話報稅服務的可行性，稅務局派出代表前往澳洲、新加坡和加拿大等地的稅務機構了解情況，汲取當地的經驗。電話報稅在部分國家已實行多年，廣為納稅人所接受。最近，稅務局與美國稅務當局的電子稅務管理部就有關稅務的電子服務進行交流。按美國稅務局的資料，2000年美國約有500萬份報稅表是經電話網絡遞交的。根據其他各國的經驗，我們相信經電話網絡傳送報稅表資料，在安全方面相信不會有問題。

行政管理措施

監管授權和身分確認

10. 稅務局會實施登記制度，確保只有經認證身分的獲授權人士才可以使用服務。市民如有意使用通行密碼以電子方式遞交報稅表，必須預先在稅務局登記。稅務局會給該納稅人編派稅務編號和啟動密碼，以兩封函件分

別發出。在系統登記時，納稅人必須同時輸入稅務編號和啟動密碼，然後輸入一個自選的通行密碼，才能完成整個登記程序。納稅人日後使用電子服務時，須同時輸入稅務編號和通行密碼確認身分。

11. 系統內設有監察功能，防止未獲授權者使用這項服務。如有人試圖接達一個稅務編號的檔案五次仍未能成功，有關的通行密碼就會被自動註銷。納稅人要重新申請啟動密碼，才可以使用有關服務。

12. 所有通行密碼都會以加密形式儲存。系統會使用強化加密技術和128 位元加密匙將六位數字的通行密碼加密，該加密匙會由一位副稅務局局長指定，而且只有該副局長知悉。

系統保安的控制

13. 系統將會實施一套完善的使用監管措施，以確保員工必須獲得授權才可接達系統。此外，系統亦會詳細記錄所有接達資料以供保安管理和審計追蹤。

保管通行密碼

14. 稅務局會派發通行密碼使用規則及條款，清楚列明登記用戶須留意的事宜。通行密碼必須絕對保密，並不時更新，密碼如被遺失或洩露，用戶須立即通知稅務局。

覆核使用記錄

15. 該系統會記錄所有接達和更新事項，稅務局會每天把記錄覆檢，確保所有使用事項均已獲正式授權。

結論

16. 稅務局會實施嚴密的行政和系統控制措施，確保經電子媒介和電話傳送資料安全穩妥，詳情已在上文闡述。本局在設計電話報稅系統和在「公共服務電子化計劃」下接受使用通行密碼遞交報稅表時，廣泛參考了商界和其他稅務轄區的標準。通行密碼一直獲得商界和海外各地採用，這點足以證明電話報稅和使用通行密碼是安全的電子交易方法。在電話網絡或使用通行密碼處理稅務事宜，在安全方面應該不成問題。

意見徵詢

17. 稅務局為確保使用通行密碼以電子方式遞交報稅表安全穩妥，採取了嚴密的系統技術和行政管理措施，詳情已在上文闡述，請議員備悉。《2001年稅務(修訂)(第2號)條例草案》旨在為使用通行密碼以電子方式遞交報稅表及為電話報稅提供法律基礎，以方便納稅人，謹請各位議員支持。

稅務局
2001年12月

立法會
Legislative Council

立法會CB(1)767/01-02號文件

檔　號：CB1/PL/FA

2002年1月11日內務委員會會議文件

財經事務委員會就使用通行密碼以電子方式及透過電話報稅提交的報告

目的

本文件旨在匯報事務委員會於2002年1月7日的會議上就使用通行密碼以電子方式及透過電話報稅而進行的商議工作。

背景

2. 在2001年11月23日的內務委員會會議席上，當議員研究在2001年11月21日提交立法會的《2001年稅務(修訂)(第2號)條例草案》(下稱"條例草案")時，議員察悉，條例草案旨在為使用通行密碼以電子方式及透過電話報稅提供法律架構。部分議員關注到以此等新方式報稅時報稅表所載資料的保安問題。議員同意，由於條例草案在提交立法會前，未經有關的事務委員會討論其政策方面的問題，因此或可先把此事交由財經事務委員會研究，然後才決定應否成立法案委員會，研究該條例草案。

事務委員會的商議工作

保安方面的問題

3. 政府當局表示，由於採用強化加密技術，使資料受到站對站式加密保障，因此使用通行密碼在網上遞交報稅表的安全程度，與使用數碼證書無異。使用通行密碼這種簽署方法，並不會令資料的安全程度下降。政府當局亦指出，在互聯網使用通行密碼確認身份，尤其在大部分網上銀行服務方面，已經十分普遍，而且美國、加拿大和新加坡等其他稅務機構亦已實行網上遞交報稅表，並採用通行密碼來確認納稅人身份。

4. 至於透過電話報稅方面，政府當局表示，公共電話網絡已公認為"可信賴網絡"，是銀行和公共事業公司普遍使用的電子交易媒介。在電話網絡系統盜取資料難度極高，而且基於經電話線傳送資料的特質，電話報稅所涉及的安全風險應該很低。其他稅務機構包括美國、加拿大、澳洲和新加坡等，亦已採用電話報稅的做法。

5. 委員亦察悉，稅務局已制訂行政管理措施，以確保資料保安妥善。

6. 部分委員贊成當局為納稅人提供該等擬議新報稅渠道，因為此舉符合政府利用資訊科技改善政府服務的政策。他們的意見如下——

(a) 雖然在電子交易中使用通行密碼確認身份，並未能達到與使用數碼證書相同的保密程度，但由於現時已有技術可確保資料保安妥善，加上政府當局所制訂的各項措施，因此使用通行密碼在網上遞交報稅表是可以接受的方式；

(b) 鑒於海外稅務機構在使用通行密碼認確身份方面的成功經驗，以及只要政府當局審慎監督有關系統的運作，該等擬議新報稅渠道應不會引起保安問題。

7. 稅務局局長表示，政府當局無意把通行密碼等同數碼簽署的法律地位。然而，政府當局有信心，在制訂各項有關的技術措施及行政管理措施後，使用通行密碼確認身份，可達到與使用數碼簽署相若的保安標準。

成本效益

8. 部分委員對成本效益表示關注。考慮到個別納稅人每年可能只會使用電話報稅系統一次，以及此系統在納稅人之間的使用率可能偏低，他們關注設立及維持該系統是否具成本效益。

9. 稅務局局長表示，政府當局在現階段不能就電話報稅系統的使用率提供準確的估計數字。雖然在初期的施行階段，使用率或會如政府其他電子服務般偏低，但在加強稅務局的服務方面，推行擬議的新服務是邁步向前的重要一步。稅務局正推行一個5年計劃，透過使用資訊科技加強其服務。提交報稅表的擬議新途徑，是稅務局將會全面推出的一套新電子服務的一部分。使用通行密碼認證身份的做法，亦適用於稅務局的其他電子服務，包括在互聯網上的互動稅務查詢服務。

10. 關於擬議新服務的人手影響，稅務局局長表示，在5年計劃完成後，預計稅務局可以節省人力。當局並無計劃在稅務局開設額外的首長級職位以推行擬議的新服務。

電話報稅系統的效率

11. 關於利用電話報稅一般所需的時間，事務委員會察悉，平均而言，透過電話提交薪俸稅報稅表需時約5分鐘，而提交物業稅報稅表則需時約4分鐘。稅務局會向有意使用新服務並已在稅務局登記的納稅人發出一份指南，方便他們使用該服務。委員已要求政府當局提供資料，闡釋已利用電話報稅的納稅人可否覆檢及核實他們所提交的資料的準確性。

與關乎電子交易的其他法例的銜接問題

12. 事務委員會亦曾研究《2001年稅務(修訂)(第2號)條例草案》與其他法例的銜接問題，該等法例包括《電子交易條例》(第553章)及近日提交立法會的《2001年進出口(電子交易)條例草案》。

13. 政府當局表示，《電子交易條例》為電子交易建立所需的法律架構。《電子交易條例》第14條准許為指明目的或服務在個別條例另訂條文。雖然使用通行密碼認證身份的做法可能不會全面適用於所有類型的電子交易，但只要當局訂有確保資料安全及穩妥的適當措施，該做法可恰當地適用於以電子方式提交報稅表。《2001年稅務(修訂)(第2號)條例草案》旨在提供完整和全面的法律架構，以便市民可在互聯網上使用通行密碼認證身份，以提交報稅表及以電話報稅。

14. 事務委員會亦察悉，當局現正檢討《電子交易條例》，並將會在一至兩個月內發表一份有關的諮詢文件。

15. 關於條例草案與《2001年進出口(電子交易)條例草案》是否一致的問題，政府當局答允就此方面提供資料。

專業團體的意見

16. 事務委員會察悉，稅務局局長曾接獲香港會計師公會("會計師公會")及專業資訊保安協會的兩封來函，當中載述他們對使用通行密碼提交報稅表一事所提出的關注及意見。

17. 李家祥議員曾向事務委員會講述會計師公會對擬議新服務所持的立場。簡要而言——

(a) 會計師公會原則上支持盡早推行擬議新服務，為方便提交報稅表提供額外的途徑；

(b) 為使規管電子交易的法律架構保持完整，會計師公會認為在《電子交易條例》中訂明條例草案旨在實施的改變，會是可取的做法；

(c) 儘管如此，會計師公會接受，當局可按照《電子交易條例》第14條的規定，為使用通行密碼在互聯網上提交報稅表及以電話報稅作特定安排；及

(d) 政府當局應把檢討《電子交易條例》列為優先工作，研究《電子交易條例》應否及如何配合電子交易在其他條例已訂明，但在《電子交易條例》未有訂明的特定安排。在檢討《電子交易條例》的過程中，亦應解決《稅務條例》中有關電子交易方面的任何不足之處。

18. 一名委員在察悉兩個團體的意見後指出，當局有需要檢討有關由稅務局局長批准用戶的通行密碼的實際安排，以及檢討草案第8條的擬議第51AA(6)(b)條中，使用"附於"("affix")一詞是否恰當。該條訂明：局長可藉憲報公告指明如何將數碼簽署或通行密碼或任何其他形式的簽署附於根據該條提交的報稅表內。該委員亦質疑是否有必要在此擬議條文中加入"任何其他形式的簽署"，因為就提交報稅表的事宜而賦予稅務局局長指明認證身份形式的權力而言，這句或會令局長的有關權力範圍不明確。政府當局已答允因應委員的建議及專業團體的意見，進一步檢討條例草案的草擬方式。

其他問題

19. 關於條例草案賦予稅務局局長的額外權力，事務委員會亦曾邀請政府當局向委員簡述是否有制衡措施。稅務局局長表示，海外司法管轄區的有關稅務當局亦在以電子形式提交報稅表及電話報稅方面獲賦予相若的權力。賦予稅務局局長的權力屬行政性質，並與推行擬議新服務有關。《稅務條例》下的現有法律架構對稅務局局長的權力已有足夠制衡。關於推行擬議新服務的時間，雖然部分委員認為按現行安排，在2002年4月推出新服務是適當的做法，亦有委員認為應周詳考慮有關問題，以確保擬議的法律架構恰當，以及確保技術基建安全穩妥。

徵詢意見

20. 謹請議員在考慮應否成立法案委員會研究此條例草案時，注意事務委員會的商議結果。

議會事務部1
立法會秘書處
2002年1月10日

附錄III

傳真號碼： 2530 5921
電話號碼： 2810 2370
本局檔號： FIN 43/5/144
來函檔號： 2530 5921

香港
中區昃臣道8號
立法會大樓
立法會財經事務委員會主席
劉漢銓議員

劉議員：

《2001年稅務（修訂）（第2號）條例草案》

感謝委員會給予我們機會，在2002年1月7日的會議席上，為各位議員說明《2001年稅務（修訂）（第2號）條例草案》的立法目的，並解釋我們就該修訂草案所載的建議（即使用通行密碼在「公共服務電子化計劃」遞交報稅表及透過電話報稅）所作確保有關系統安全的措施。感謝各位議員普遍贊同政府的建議，支持當局推出讓市民以通行密碼在網上提交報稅表，及電話報稅服務。據我們了解，會議席上的議員大致上都滿意有關系統的安全水平，亦有部分議員希望新服務能如期（即在本年第二季）推出。

2. 為方便各位議員審議該修訂草案，我們就各位議員在會議上的提問及關注的問題詳加解答及增補資料。

使用通行密碼提交報稅表的安全問題

3. 我們為財經事務委員會擬備的文件，已詳細載列了稅務局將採取的措施，以確保為處理使用通行密碼以電子方式及透過電話遞交報稅表而設的系統是安全及穩妥的。

4. 議員已在會議上知悉，系統所需要或所期盼的安全水平，是取決於相關的風險的考慮。，資訊科技署早前曾就在「公共服務電子化計劃」使用通行密碼遞交報稅表這建議作出詳細研究並確定這個方法的安全性。該署的研究結果顯示，建議的方法在傳送報稅表資料方面，因符合「強化加密」的規定足以防禦第三者接達對稱密碼匙，能達到極高的安全水平。該署的結論是使用通行密碼方法能達到如同使用數碼證書的安全效果。

5. 通行密碼已在互聯網廣泛地使用，尤其在大部分網上銀行服務方面。使用通行密碼在互聯網上報稅已在很多國家庭主家（包括美國、加拿大和新加坡）推行多年。稅務局建議以電子方式遞交報稅表的新方法是符合電子商務一般發展的路向。

電話報稅的程序

6. 有部分議員想了解電話報稅在香港的使用率及所涉及的程序。有關的步驟已在**附件**撮述。在開始使用電話報稅前，納稅人可以利用一份由稅務局提供的“電話報稅記錄表”，填上所須資料。這記錄表可作核對清單用途以方便報稅的過程。在納稅人完成申報後，系統會自動覆述有關的報稅表資料，以供他確認。納稅人可藉此將已輸入的資料與“電話報稅記錄表”核對是否正確，如有需要納稅人可將有關資料修改。完成整個電話報稅程序平均需時4至5分鐘。系統會將整個報稅程序的資料以數碼格式記錄及貯存。納稅人可以書面向稅務局申請印備貯存在他檔案內的資料的副本。

7. 我們估計約有800,000位納稅人符合「電話報稅」的準則。由於這是一項新服務，部分納稅人可能需要過一段時間才習慣使用這項服務。因此在服務推出初期使用率不會很高，但我們相信使用率日後會逐漸增加（長遠來說，使用率估計可達5%）。在其他稅務轄區，電話報稅的使用率是3%至9%（美國是4.1%，加拿大是2.9%，新加坡是8.5%）。稅務局會在法例通過後廣泛宣傳，推廣這項新服務。

8. 實施「電話報稅」計劃的成本額估計約480萬元（其中420萬元為非經常開支，60萬元為非經常員工開支）。我們估計因減省處理及輸入報稅表資料的工序，每年可節省的員工開支將達90萬元。

與《電子交易條例》的銜接

9. 有部份議員提問有關《2001年稅務（修訂）（第2號）條例草案》如何與《電子交易條例》銜接，並詢問當局是否會把通行密碼的使用範圍，擴展至政府其他電子服務。

10. 《電子交易條例》是為促進電子交易及推動電子商務的發展而制定，使電子紀錄和數碼簽署跟書面紀錄和簽署享有同樣的法律地位。該條例訂立一套適用於不同法例的一般架構，而同時亦容許其他條例包含條文，以獨立方式處理有關的特定情況。為此，《電子交易條例》包含一項條文（第14條），訂明如某條例接納電子方式並包含有關該目的的指明規定、程序或其他指定的明訂條文，則《電子交易條例》不得解釋為影響該明訂條文。換言之，《電子交易條例》並不妨礙有關方面為特定情況而在有關條例內加入條文，以促進電子交易和電子商務。政府的政策目標並不是要將所有有關電子交易的條文詳列在《電子交易條例》內，因為這做法既不實際亦不可行。

11. 有議員指出，我們應確保不同條例的用語一致，並引述《2001年進出口（電子交易）條例草案》為例子。《2001年進出口（電子交易）條例草案》為以電子方式遞交貨物艙單提供法律基礎，並刪除保安裝置（即用以認證的裝置）必須由貿易通提供的規定以利便將來靈活發展。《2001年稅務（條訂）（第2號）條例草案》的重點是提供另一種認證方式，符合以電子方式遞交報稅表的簽署規定及為使用通行密碼以電子方式遞交報稅表提供法律依據。該兩項條例草案都包含特定條文，以配合在特定情況下以電子方式處理文件的做法。該兩項條例草案均與《電子交易條例》的政策及立例精神相符合。

12. 資訊科技及廣播局推廣電子商務及實施《電子交易條例》的決策局，對這條例草案就使用通行密碼遞交報稅表及電話報稅的建議表示支持，以促進本港電子政府的發展。至於是否會在其他電子程序普遍使用通行密碼，資訊科技及廣播局會研究這個基本政策問題，並會隨同即將展開的《電子交易條例》檢討，諮詢公眾的意見。

稅務局局長在指明格式方面的權力

13. 議員詢問該修訂草案賦予稅務局局長的權力。條例草案第8條賦權局長指明在何種情況下報稅表可透過電子紀錄或電話報稅系統提交，指定有關電子紀錄或所須的附件的技術及其他細則，及批准使用通行密碼等。此等準則、報稅表的形式及方式，是屬程序及運作上的細節，亦會隨時間轉變。由於該等事宜並不涉及重大的政策，我們建議賦權局長處理。

14. 在其他稅務轄局，例如美國、新加坡、英國、澳洲及加拿大等地的稅務局局長亦具有相若的權力，制訂規例或指明條件，規定提交的報稅表的資料準則、形式及方式，以及電子報稅表的簽署方式。

草擬法例的具體問題

15. 部分議員提及香港會計師公會就草擬法例提出的具體建議（見該公會1月4日給稅務局局長信件的附錄），促請我們考慮公會提出的數點草擬法例方面的建議。

16. 我們仔細研究過該公會的建議，根據律政司的意見，草案採用的“附於（affixed）”及“局長批准（Approved by the Commissioner）”用詞實屬合適。該公會建議的用語不足以達到使用通行密碼在報稅表上“簽署”的用意。“附於（affixed）”一詞的普遍含意包括“附加一些東西”及“附於一些東西”，因此“通行密碼”可以“附於（affixed）”報稅表上。稅務局局長已在2002年1月11日給該公會回信詳細解釋。

17. 該公會又建議刪除修訂草案第8條“任何其他形式的簽署”一詞。我們加入這一條的用意，是為配合日後的科技發展，當有關方面在電子簽署及通行密碼以外，成功確立安全水平相同的任何其他形式的簽署時，也可以法例使用而無需再修訂法例。我們也明白公會及議員就該詞可能帶來不明確的地方表示憂慮。因此，在考慮各方面的意見後，我們願意動議委員會審議階段修正案，刪除這些字眼。

18. 我們相信以上的解釋能解答議員對該修訂草案的疑問。謹請各議員支持該修訂草案。

庫務局局長
（庫務局首席助理局長吳麗敏　　代行）

副本送：稅務局局長　(Attn:Mrs Alice Lau Mak Yee-ming)
資訊科技及廣播局局長 (Attn:Miss Adeline wong)
律政司　(Attn:Mr MY Cheung)
法律草擬專員　(Attn:Ms Lonnie Ng)

附件

「電話報稅」的程序

(i) 首先，納稅人須輸入他的「稅務編號」。系統會利用這項資料核對納稅人是否有仍未遞交的報稅表紀錄，以確定他能否使用此服務。

(ii) 接著，納稅人須輸入他在有關課稅年度的入息及申請免稅額資料。在這過程中，系統會檢查納稅人的報稅表是否適合透過電話提交。如資料顯示他並不符合指定的準則（例如納稅人有經營業務的收入），系統會通知納稅人不可以使用「電話報稅」。

(iii) 在納稅人輸入所有資料後，系統會覆述報稅表的資料，以供他確認。如有需要，納稅人可以更改有關的資料。

(iv) 如資料無誤，納稅人須要輸入他的「通行密碼」藉以簽署確認報稅表資料。

(v) 系統在核對納稅人的「通行密碼」後，會發出一個“認收編號”確認已收取報稅表資料。稅務局會建議納稅人將此“認收編號”記錄在“電話報稅記錄表”上，以作為提交報稅表的佐證。這號碼亦可方便納稅人在有需要時要求索取報稅表資料的副本，如同提交文本報稅表的情況一樣。

Our Ref. : HQ 309/405/22C

Mr. LEUNG Siu-cheong,
Chairperson,
Professional Information Security Association,
Room 904, 111 Queen's Road West,
Wah Fu Commercial Building,
Hong Kong.

11 January 2002

Dear Mr Leung,

Inland Revenue (Amendment) (No. 2) Bill 2001

Thanks for your letter of 7 January 2002 and the comments of the Association in connection with the Inland Revenue (Amendment) (No. 2) Bill 2001. I shall attempt to respond to the various points raised in the following paragraphs, in the same order as they appear in your letter.

1. **The use of a less secure system as an alternative to the current tax return submission system.**

   Data Security

   Filing tax returns through the Electronic Service Delivery (ESD) scheme platform by using a password will achieve a very high level of data security. Tax return data will be transmitted through the ESD platform using strong encryption technology [128-bit Secure Socket Layer (SSL)] and the return information will be end-to-end encrypted (i.e. from the client to the department) by using the "session" key (a group of number randomly generated by the browser) and IRD's public key. The password will be encrypted by another set of session key and IRD's public key for security control.

   Data Integrity

   The proposed solution for using a password as the signature for a return filing under the ESD Scheme will provide a very high level of data integrity. This is achieved by generating a hash value with taxpayer's web browser using the taxpayer's password, IRD's public key and the tax return data; the hash value will then be signed by the ESD front-end server private key. The hash value will be re-calculated for verification by IRD once it receives the data. As one can see, the use of asymmetric cryptographic technology is also applied here. The whole process is similar to that involving the use of digital certificate whereby the signing is done by using the taxpayer's digital certificate's private key. In both cases, the issue of data integrity can be addressed.

Non-repudiation

The proposed new section 2(5) will extend the definition of “sign” to include the adoption of a person's password. If a return was properly signed by using a taxpayer's password, by virtue of section 51(5), he will be deemed to be cognizant of the content thereof, and hence the non-repudiation issue can be addressed.

The design of our system will ensure that the electronic records will be handled in such a way that the principle of non-repudiation can be involved and demonstrated. Non-reputability is dependent upon how the integrity of an electronic record can be demonstrated. In addition, we will introduce security control measures to protect electronic records from unauthorized access. In legal proceedings, the Court will examine the evidence put before it by the IRD, and then, applying the appropriate standard of proof, the Court will decide whether or not it accepts that the non-repudiation averred should be accepted or rejected. With our proposed solution and tight security control measures, we believe that the electronic records held by the IRD will be afforded the optimum chance of being accepted by the Court as true and accurate. [NB: an electronic record produced by a computer shall be admitted in any criminal proceedings as prima facie evidence under section 22A, Evidence Ordinance (Cap. 8)]

2. Citizens bear higher risk when using the proposed "simple password" system

Use of Password

The password of a taxpayer is not limited to tax filing only; it can be used for interactive tax enquiry through Internet or the telephone network to enquire information such as tax return or demand note status or balance of Tax Reserve Certificate account. We do not consider the use of password would bear higher risk comparing to the use of a digital certificate in the circumstances. There is also a chance that a person might forget or lose the password of his digital certificate.

Whether a password itself is sufficiently secure or not in individual cases depends very much on the risk involved in the application concerned and whether the security offered by password is commensurate with the risk concerned. We do not consider that password is of the same status as digital signature in aI1 cases but in some specific cases, a password can be accepted as sufficiently secure for the purpose. The use of password has been widely adopted in the commercial sector, like internet banking and phone banking where the risks associated are higher as they involve actual monetary transactions. Yet, the password is trusted for all such matters and by all parties concerned. We note that password has also been used in other countries for return filing, like Australia, USA and Singapore for quite a number of years. To our knowledge, there has not been any report of abuse or other irregularity on the use of password for the purpose.

The taxpayer is also required to comply with our instructions as specified in the "Terms and Conditions of using Password" and keep his password confidential and to ensure that no other person knows his password. The system is designed with access control feature to guard the password from unauthorized access. As the taxpayer has taken the obligation (by agreeing to the terms and conditions)

to keep his password to himself, he cannot deny a transaction that was conducted by using his password.

3. Password affixed to a return is a security exposure

Affixing a Password to a Return

For filing through telephone, password information will be stored in IRD's database in encrypted format. The generation of the encrypted password from its 6-digit format involves the use of strong encryption algorithm (RC4) with a 128-bit encryption key. The encryption key will be specified by the Deputy Commissioner of Inland Revenue and no person other than him knows such key.

For filing through the ESD Scheme, the password will be encrypted by a session key generated by taxpayer's web browser and then by IRD's public key. The password information will also be stored in encrypted format.

It is therefore not easy to break the encrypted password. In addition, security control measure will be put in place to protect the encrypted password from unauthorized access. Decryption of the "affixed" password (encrypted) will not be made unless ordered by the Court in legal proceedings.

In addition, we wish to point out that there is a practical need to retain the password information for evidential purposes. Whenever a prosecution case goes to court for, say, submission of incorrect return, we have to prove beyond reasonable doubt that it was the taxpayer who used his own password to file the incorrect information. Thus, the password information will be crucially needed to enable the Commissioner to fulfill her duties under the IRO. This situation is fundamentally different from that in the banking industry the practice of which is governed by mutual agreement and basically only civil rights inter se are involved.

On a more general point, we wish to reiterate that a taxpayer has to “sign” a tax return rather than simply authenticate it. A tax return (which is specified by the Board of Inland Revenue) invariably requires the taxpayer's signature. In this regard, section 51(5) of the IRO provides that any person signing any return, statement, or form shall be deemed to be cognizant of all matters therein. Thus, the signing of a return is the very basis for our enforcement actions. Mere authentication is not sufficient for the purpose.

4. The Inland Revenue Commissioner is given too much power

Approving Password by the IRD

The expression that the Commissioner, may "approve" a password relies on the **Carltona** principle or the **alter ego** principle. The rationale behind this is that the Commissioner should be and remain responsible to the legislature for the exercise of a power but may exercise the power through an authorized agent except where the provision expressly or by implication requires him or her to act **personally**.

This approach provides practical flexibility while the responsibility stays where it belongs.

The whole matter concerns the approval mechanism for the password. Whilst the system would require the user to make a self-selected password, there must be a control by IRD on the requirement in respect of the number of digits, the numbers and characters chosen. As said above, we consider that the automatic validation checks built-into the system can be taken as approval or acceptance. This concept is no different from a bank accepting a customer's withdrawal request after he/she has keyed in the correct password.

Indeed, the provisions under clause 8 of the Inland Revenue (Amendment) (No.2) Bill 2001 intentionally confine the Commissioner's specification power to a handful of aspects; for instance specifications in respect of eligibility criteria, the form and manner of furnishing a tax return. They are routine and operational in nature. Under the IRO, specifications of tax returns have already been subject to a separate body's scrutiny, i.e. the Board of Inland Revenue. It therefore would unlikely be any room for abuse of power by the Commissioner. In this regard, the Commissioner also undertakes to exercise this power with care.

In the Australian legislation, 'electronic signature' and 'telephonic signatures' are also to be 'approved' by the Commissioner.

The intention for system used for electronic filing of tax return is indeed for users to submit returns using the ESD system at the moment. The expression "using a system specified by the Board of Inland Revenue" is meant to cover the ESD system and any other systems that may be introduced in future as technology advances. This is meant to render flexibility in the light of IT development.

5. Comments on the Telefiling System

Telefiling

Hong Kong is not the first tax jurisdiction to offer the telefiling service for tax returns. Telefiling has been implemented in USA since 1992, in Canada since 1998, and in Singapore since 1995.

Telefiling is intended for very simple returns. It will provide taxpayers with another convenient means of lodging tax returns. It will complement Internet filing through the ESD Scheme so as to provide a total customer solution, catering for the needs of both Internet and non-Internet users. The telefiling system allows taxpayers to file tax returns by using touch-tone telephone. Taxpayers have to fulfill certain criteria before they can use this service. The main purpose of the criteria is to confine the service to simple return cases so that the duration of the filing process can be kept at a reasonable limit.

IRD will send out 'Instruction Notes for Telefiling' along with tax returns. Taxpayers are advised to read these Instruction Notes to ascertain whether they meet the telefiling criteria before using the service. IRD will provide a 'Telefiling Record Sheet' in these Instruction Notes so as to assist taxpayer to get the required

information ready before filing his return through telephone. Taxpayer will be advised to fill in the data for his income and relevant claims in this Tax Record Sheet before he starts to file the return through telefiling. The purpose of this Telefiling Record Sheet is to smoothen the filing process. It will also facilitate verification of data by the taxpayer when the system repeats the return information at the end of the filing process. It can also serve as the taxpayer's own record of the data which he has furnished in telefiling. The telefiling system will record and store the data captured during the whole return filing process in digitized format. If the taxpayer lodges a written request, IRD will print a copy of return data and send it to the taxpayer by post.

6. The immature rollout of the alternative forms of submission

Objective of the Proposal

The system that we are going to introduce is one that meets industry standards, that is adequately secure and operationally sound even at peak periods. The use of passwords as a means of identification in both internet filing and Telefiling is commensurate with the risk associated with the filing of tax returns. Given the vast experience of Hong Kong people in the use and safekeeping of passwords over the past decades (dating back to the 1970s when the ATM machines were first introduced), we should have confidence in the secure use of passwords.

Our proposal to use password will provide an alternative means (particularly for those who do not have digital certificates) to filing their tax returns online via the ESD scheme. IRD will continue to accept the use of digital certificates for the ESD application of filing of tax return as well as physical submission. It is entirely up to the taxpayer to choose which option should be adopted.

The introduction of password for telefiling is to address the concern and the need of taxpayers who do not have access to or who prefer not to use Internet facilities. It aims at narrowing the digital divide of the community.

7. The scope of application of "password" only system must be limited

PKI

System security is always one of our major concerns. That is why we propose to implement the use of password for electronic tax filing on the ESD platform which builds upon the PKI technology and offers a secured operating environment. By accepting filing of tax return using a digital certificate or a password, we aim to encourage the use of our electronic services and this will help promote E-government and e-commerce development in Hong Kong.

Scope of the Password

Your suggestion in defining the scope of application of "simple password" to government services according to the **Risk Level** seems to follow the UK model. We note that the UK Inland Revenue allows individuals to file their Self Assessment (SA) Tax Returns electronically over the Internet by using a digital

certificate or a user ID and password. Taxpayers intending to use this service have to register with the Government Gateway, a centralized registration point for E-government services in the UK, for the Internet service for Self Assessment. A taxpayer may register either by using a password or using a digital certificate. Internet filing of SA tax return is considered as credential Level 1 transaction for which a user ID and password can be used. We **also note** that for some transactions that involve a higher level of sensitivity, such as filing of Electronic VAT Returns (HM Customs and Excise), the use of a digital certificate is required.

Therefore our proposed system of using either a digital signature or a password as a means of authentication in Internet filing of tax return by eligible individuals and property owners is similar to the practice adopted in UK, As for certain transactions, such as the electronic filing of Profits Tax returns under the e-Form Program, registration of new businesses, etc., digital certificates are still required.

ETO

The ETO was enacted to facilitate electronic transactions and drive e-business development by providing electronic records and digital signatures the same legal status as that of their paper-based counterparts. It is designed to provide a generic framework that can be applied to various legislation. However, there is scope for specific situations to be dealt with in the relevant ordinances in a self-contained manner. It is for this purpose that the ETO contains a provision (section 14) that if an ordinance accepts the electronic process and contains an express provision with specific requirements, procedures or other specifications for the purpose, then the ETO is not to be construed as affecting that express provision. In other words, the ETO does not prevent other ordinances from providing for specific situations to facilitate electronic transactions and e-business.

Under the ETO, a digital signature supported by a recognized certificate and generated within the validity of that certificate enjoys the same legal status as a hand-written signature. The objective of IRD's proposal to use password as an alternative to the use of digital certificate for authentication and fulfilment of the signature requirement in filing tax returns is to provide the public with another choice so as to encourage them to use IRD's electronic services. The level of security offered by using password for filing tax returns (whereby there is already established relationship between IRD and the taxpayer) through the ESD platform is commensurate with the risk involved. It can help promote E-government and the conduct of e-business in a secure manner. Taxpayers can determine themselves whether the password option should be used, or whether the digital signature or physical option should be adopted. It is entirely their choice and the IRD's proposal provides an additional alternative to facilitate taxpayers. ITBB, which is the policy bureau for the promotion of e-business in Hong Kong and for the operation of the ETO, supports this proposal.

ITBB is now conducting a review of the ETO with a view to ensuring that Hong Kong has the most up-to-date legislative framework for the conduct of e-business. To give the community a wider choice and to facilitate e-business and E-government development, one of the issues to be considered in the review will be whether personal identification number (PIN) or password should be

accepted as a form of electronic signature for satisfying the signature requirement under law in selected cases where the level of security offered by PIN or password is commensurate with the risk of the application involved. While the IRO amendment will serve as a reference, it will not set a precedent which will restrict the conduct of the review. ITBB is now formulating a set of preliminary proposals to update and improve the ETO and will consult the public shortly on the review.

In short, the Bill does not seek to extend the possible methodologies for effecting e-transactions in a general way. Under the Bill, the use of passwords in addition to digital certificates is intended to be applied in relation to the filing of tax returns only. Therefore, the Bill does not change the policy enshrined in the ETO. It actually facilitates electronic communications by providing for electronic tax return filing.

Yours sincerely

(Mrs LAU MAK Yee-ming, Alice)
Commissioner of Inland Revenue

c.c. Chairman & Members of
LegCo Panel on Financial Affairs

Internal

S for Tsy	(Attn: Miss Erica Ng)
SITB	(Attn: Miss Adeline Wong)
D of J	(Attn: Mr MY Cheung)
Law Draftsman	(Attn: Ms Lonnie Ng)

Our Ref. : HQ 309/405/22C
Your Ref. : C/TXP(2), M9105

11 January 2002

Ms Winnie C W Cheung
Senior Director
Hong Kong Society of Accountants
4/F, Tower Two, Lippo Centre
89 Queensway
Hong Kong

Dear Ms Cheung,

Inland Revenue (Amendment) (No.2) Bill 2001

Thank you for your letter of 4 January 2002. I write to respond to the issues raised in your letter. The remaining areas of concern can be broadly categorised into two: security and legislation. I will address these two areas one by one in the following paragraphs.

Security

I am pleased to note that after our meeting on 21 December 2001, you and your members are now less concerned than before about the purely technical issues surrounding the proposed use of passwords for submitting tax returns electronically. Nonetheless, you provided us with some further comments on the system integrity aspects.

As noted by some LegCo Members at the Financial Affairs Panel meeting held on 7 January 2002, the level of system integrity required or desired in an IT system has to be determined having due regard to the risk involved. With respect to the proposed system for the filing of a return under the Electronic Service Delivery (ESD) Scheme by using a password, you may wish to note that the Information Technology Services Department (ITSD) has carefully studied and endorsed the security of this proposal. ITSD's conclusion was that such system will attain a high level of security in the transmission of tax data by meeting the "strong encryption" requirements and protecting the session key against third party access, and that the security level of the system is the same as in the case of digital certificate.

As a matter of fact, the use of a password is widely adopted in the internet especially for most internet banking services. The design of the ESD system to use passwords for authentication and signature would adopt similar security standard as in the commercial sector for e-commerce and internet banking services. As you are well aware, internet filing with the use of a password has also been implemented in

other tax jurisdictions such as the United States, Canada and Singapore for quite some time already.

In exploring the feasibility of launching the telefiling service, IRD has sent representatives to other tax administrations, such as Australia, Singapore and Canada to study their experience in this regard. Telefiling has been adopted by most of these countries for quite a number of years now and the service was well-received by taxpayers in these countries. Recently, the department had an exchange with the representatives of the Electronic Tax Administration Division of the U.S. Internal Revenue Service on the delivery of tax-related services using electronic means. In the light of other countries' experience, we believe that transmitting tax return data through telephone network is unlikely to pose a security concern.

All in all, we consider that the level of system integrity required or desired has to be determined having due regard to the risk involved. For the purpose of filing tax returns, the security offered by a password is, in our view, fully commensurate with the risk associated with that operation.

As a related issue, in the system design, we have provided facility for taxpayers to select his own password and that we will soon launch an Interactive Tax Enquiry Service which will be accessible through the use of the same password. Hence, taxpayers can make use of his password more than once in a year. The alleged problem of the password being vulnerable to abuse which is grounded on the premise that a taxpayer is likely to write down his password, may be overstated. Having said that, I agree that taxpayers should be well-alerted of their potential obligations and liabilities on the use of passwords. To help achieve this, we will stipulate in clear layman terms the legal consequences of using passwords in the Terms and Conditions for Use of Password, and urge taxpayers to keep their passwords in strict confidence. Taxpayers have an obligation to ensure that the security of their passwords is not compromised.

Legislation

Turning to legislation, I noted that you have some concerns about the interface of the amendment Bill with the Electronic Transactions Ordinance (ETO), the lack of provisions in the amendment Bill prescribing the use of passwords, and some of the terminology used in the Bill.

Interface with ETO and statutory support for the use of password

The ETO was enacted to facilitate electronic transactions and drive e-business development by providing electronic records and digital signatures the same legal status as that of their paper-based counterparts. It is designed to provide a generic framework that can be applied to various legislation. However, there is scope for specific situations to be dealt with in the relevant ordinances in a self-contained manner. It is for this purpose that the ETO contains a provision (section 14) that if an ordinance accepts the electronic process and contains an express provision with specific requirements, procedures or other specifications for the purpose, then the ETO is not to be construed as affecting that express provision. In

other words, the ETO does not prevent other ordinances from providing for specific situations to facilitate electronic transactions and e-business.

Indeed, it is not our policy intent to put all legislative provisions concerning electronic transactions in the ETO, which may not be possible nor practical. For this reason, there are efforts by individual bureaux to make self-contained legislation to cater for specific circumstances and operation where necessary. For instance, the Import and Export (Electronic Transactions) Bill 2001 is intended to provide legal backing for the electronic submission of cargo manifests, and remove the requirement that the security device (i.e. the authentication apparatus) must be issued by Tradelink so as to allow for flexibility. The foci of our Inland Revenue (Amendment) (No. 2) Bill 2001 are to provide an alternative to the mode of authentication in satisfying the signature requirement in filing tax returns and provide the necessary legislative backing for the use of passwords in filing tax returns electronically. Both Bills contain specific provisions to cater for electronic processing in specific situations and, as provided for in section 14 of the ETO, the ETO is not to be construed as affecting those specific provisions. They are thus consistent with the policy intent and spirit of the ETO. The Dutiable Commodities (Amendment) Ordinance 2001 is another case in point. The Information Technology and Broadcasting Bureau (ITBB), which is the policy bureau for the promotion of e-business in Hong Kong and for the operation of the ETO, supports the amendment proposals in order to drive the development of E-government in Hong Kong.

We consider that the legislative provisions enabling the use of passwords should best be placed in the Inland Revenue Ordinance rather than the ETO. This is because the Administration reckons that the level of security offered by using a password to file tax return through the ESD platform is commensurate with the risk of filing tax returns and thus contemplates to introduce the use of password in the context of filing tax returns, and not in other electronic government service applications, for the time being.

As to whether or not the use of passwords should be widely adopted in other electronic processes, the ITBB will look into this general policy. The Bureau will consult the public on the issue shortly in the context of the coming ETO review.

Terminology used in the Bill

On terminology, you have made three specific suggestions. These suggestions are to (a) replace “any other signing device” by “any other means of authentication” and “affixed” by “used to authenticate” in new section 51AA(6)(b); (b) substitute “approved by the Commissioner” with “conforming to requirements prescribed by the Commissioner” in the definition of “password”; and (c) remove “any other signing device”.

Regarding (a), we do not consider it advisable to adopt your proposed wording. We have carefully examined the functions performed by traditional hand-written signatures in the existing legislation. We found that hand-written signatures have the following functions:

(i) to identify a person;

(ii) to provide certainty as to the personal involvement of that person in the act of signing;

(iii) to authenticate the content of a document; and

(iv) to associate that person with the content of a document.

Insofar as filing tax returns under the Inland Revenue Ordinance is concerned, hand-written signatures are required to fulfill all the above functions. For enforcement purpose, all tax returns, irrespective of the form in which they are furnished, must bear a signature and that in the Inland Revenue (Amendment) (No.2) Bill, we are accepting passwords as a signature, and passwords should perform similar functions as hand-written signatures. Since your proposed amendment only deals with one of the four aspects (i.e. authentication), we do not consider it appropriate and adequate to cater for tax return filing.

We understand that the very purpose of replacing our proposed terminology of "affixed" is to restrict the use of password for authentication purpose only. However, our policy intention of this amendment Bill is to accept passwords as a form of signature for return filing purposes. A tax return, which is specified by the Board of Inland Revenue, invariably requires the taxpayer's signature. In such circumstances, we need to make sure that the signature (in the form of a password) is added to the return and furnished together with the tax return. In this regard, section 51(5) of the Inland Revenue Ordinance provides, among others, that any person signing any return shall be deemed to be cognizant of all matters therein. Therefore, the signing of a return is the very basis for our enforcement action. Mere authentication is not sufficient for the purpose. To achieve our policy intention and fulfill the functions mentioned above, we consider it appropriate to retain the word "affix".

On (b), you suggested that the Commissioner should focus on approving and specifying the policies and standards to which passwords should conform instead of approving the passwords. I wish to point out that the setting up of a "password" does not only involve the selection of a 6-digit number by a taxpayer that "conforms to requirements prescribed by the Commissioner". In fact, the following processes are involved:

(i) verification of taxpayer's identification number;

(ii) selection of a 6-digit number by the taxpayer that conforms to prescribed requirements;

(iii) transmission of the selected number to the IRD's computer system;

(iv) validation checks of the selected number by IRD's computer system; and

(v) recording of the selected number in IRD's computer system.

It is thus clear that the selected number, apart from conforming to prescribed requirements, must be successfully transmitted, verified, validated and recorded in the Inland Revenue Department's computer system before it constitutes a "password". The suggested wording will only cover one of these processes ((ii) refers) and is therefore inadequate.

In fact, similar definitions of the word "password" in other jurisdictions also require the identification means to be approved by the Commissioner, e.g. the "electronic signature" and "telephone signature" in the Australian Income Tax Assessment Act 1997. It appears that such definitions have served well over all these years.

With respect to (c), the Society commented that the undefined term of "any other signing device" adds uncertainty to the security of the system. I wish to explain the rationale for including these words in the present amendment Bill. The purpose of so doing is to obviate the need to bother the Legislative Council with further technical amendment to the Inland Revenue Ordinance because of future development in technology that allows us to adopt yet another means of signing which also attains the same level of security as electronic signatures and passwords. Nevertheless, in view of the concerns expressed, the Administration has reviewed its position and is prepared to move a Committee Stage Amendment to delete these words from the Bill.

I hope the preceding paragraphs have set out clearly the Government's position on the issues raised in your letter. Last but not the least, thank you very much for your and your colleagues' valuable comments.

Yours sincerely,

(Mrs LAU MAK Yee-ming, Alice)
Commissioner of Inland Revenue

c.c. Chairman & Members of
LegCo Panel on Financial Services

Internal

S for Tsy	(Attn: Miss Erica Ng)
SITB	(Attn: Miss Adeline Wong)
D of J	(Attn: Mr MY Cheung)
Law Draftsman	(Attn: Ms Lonnie Ng)

LETTERHEAD OF HONG KONG SOCIETY OF ACCOUNTANTS

CB(1) 749/01-02(02)

BY FAX AND BY POST
(2877 1082)

Our Ref.: C/TXP(2), M9105 4 January 2002

Mrs. Alice Lau Mak Yee-ming,
Commissioner of Inland Revenue,
Inland Revenue Department,
36/F, Revenue Tower,
5 Gloucester Road,
Wanchai, Hong Kong.

Dear Mrs. Lau,

Inland Revenue (Amendment) (No.2) Bill 2001

Thank you for meeting with us on 21 December 2001 to discuss the Inland Revenue (Amendment)(No.2) Bill 2001 ("the Bill"). We found the meeting useful in clarifying the background behind and the objective of the proposed legislation. We have now received your detailed response to the Society's letter of 19 November 2001, for which we also thank you.

As a result of the discussion we are less concerned than before about the purely technical issues surrounding the proposed use of passwords for submitting returns electronically although, as indicated at the meeting, we do have some suggestions in this respect such as the need to run periodic security audits on the system protocol and not just the system itself.

We appreciate that the Inland Revenue Department (IRD) is keen to take further steps to promote the submission of "paperless returns" and would like to do so in 2002/03. However we continue to have some concerns about (a) the interface of the Bill with the Electronic Transactions Ordinance (ETO), (b) the lack of provisions in the Bill prescribing the technical and legal infrastructure to support the proposed new form of e-filing, in contrast to the situation of e-transactions under the ETO, and also (c) some of the terminology used in the Bill, which we believe is likely to create a misleading impression.

Interface with the ETO

We have expressed the view that the Bill actually extends the possible methodologies for effecting e-transactions in a general way. The use of passwords instead of digital certificates is a change of a generic nature, albeit that in this case it is intended to be applied in relation to tax returns. As such we believe that it would be better for the integrity of the legal framework governing e-transactions to have provided for the relevant changes in the ETO, in addition to making any related changes to the Inland Revenue Ordinance (IRO).

We note your position that section 14 of the ETO provides that specific provisions in respect of e-transactions contained in another Ordinance are not affected by the ETO, and that this would apply to either existing or future legislation. However, our understanding of the

policy at the time of the introduction of the ETO is different, as reflected in statements made when the legislation was first put forward. The Ordinance was intended "to provide a statutory framework for conducting by electronic communication commercial and other transactions" (extract of the Explanatory Memorandum to the Bill). In order to avoid constraining unnecessarily the development of electronic commerce, it was stated in the Legislative Council Brief to the Bill that "the Bill should (a) adopt a technology-neutral approach to cope with rapid technological changes; and (b) adopt a minimalist regulatory approach" (extract from LegCo Brief, issued by the Information Technology and Broadcasting Bureau).

Overseas there are two main streams of e-commerce legislation, namely those providing for electronic signatures, the scope of which covers passwords, voice recognition, etc. and those providing for digital signatures, which imply an underlying public key infrastructure (PKI). When the ETO was introduced, it seems clear that the Government had chosen to adopt the more information technology (IT)-driven approach of the two. Quoting again from the LegCo Brief, the Government proposed "to take action to address public concerns about the security and certainty of electronic transactions, e.g. the legal status of electronic records and digital signatures, authentication of the parties to electronic transactions, the confidentiality and integrity of electronic messages transmitted over open communication networks and non-repudiation of electronic transactions. To provide a secure and trusted environment for the conduct of electronic transactions, Government has spearheaded the establishment of a public key infrastructure (PKI) in Hong Kong". Under the circumstances it appears that a change of policy has occurred since the passage of the ETO and, if this is the case, we believe that it should be reflected in the principal piece of legislation governing e-transactions, i.e. the ETO.

In our view, the legislative intention of section 14 was unlikely to have been to provide for alternative forms of e-communications to be implicitly grafted onto the general framework following the introduction of the ETO, in ordinances governing particular types of transactions. Yet this appears to be the substance of the present proposal and if this process were to continue, then the fundamental basis and purpose of the ETO could in time be undermined. Under the circumstances, we cannot agree that the Bill as drafted "works to re-inforce the policy" as you have suggested.

Statutory support for the IT infrastructure behind the Bill

As indicated above, while our initial fears about the supporting IT infrastructure for e-filing of tax returns using passwords were to a large extent addressed on the practical level by your explanation of the system, our reservations about the lack of legislative backing for the system remain. This is a further disadvantage of trying to make the IRO "self-contained" in relation to e-transactions. While the use of digital signatures is supported in the ETO by the framework of "recognized certification authorities", use of "trustworthy systems", etc. no equivalent framework is prescribed for the use of passwords in the IRO or elsewhere, and this being the case, much more will be required to be taken "on trust" by potential users, which is not consistent with the previous policy of acting to address public concerns about security and certainty, reflected in the LegCo Brief to the ETO and referred to above. In addition, the extension of section 2 of the IRO to cover the undefined term "any other signing device" merely adds further to the uncertainty.

Comments on specific areas

Different level of security provided by password and digital signature

Integrity

We have some comments on the technical aspects of the system integrity. A digital signature of a document is the hash value of the document encrypted at the user end using the user's private key. The process is initiated by the user, which is why a digital signature provides a high degree of assurance over the user's identity and, at the same time, a similarly high degree of assurance over the integrity of the document (short of a compromise of the user's private keys). In the proposed protocol, the hash value is encrypted by the ESD front-end server's private key.

This act of signing the hash value can only be initiated (most likely automatically) at the ESD front-end once the document (the return) reaches the ESD server. Of course, the document would have been transmitted to the ESD server through a secure channel, most likely an SSL connection. However, the degree of assurance over data integrity provided by the proposed protocol is subtly different to that provided by the use of digital signatures as explained to you at our meeting.

Non-repudiation

To ensure non-repudiation, a system must be able to provide sufficient evidence on two aspects: it needs to demonstrate the integrity of a document purportedly submitted by a person, as well as to provide for a means of binding the person to the act of submitting the document. The reason that digital signature is often the preferred means for ensuring non-repudiation is that in one single process, which is initiated by the end user, both aspects are addressed. The proposed protocol by the IRD, sophisticated though it may be, really focuses on the integrity aspect. The binding of the taxpayer that submitted the return is based on a simple presumption: that the taxpayer who is able to provide a valid user id and password in accessing the electronic submission service must be the person who owns that user-id and password. So in the absence of evidence to the contrary, the Commissioner will presume - and the taxpayer accepts and agrees to the Commissioner making such presumption - that the person submitting the return using the valid user id and password is indeed the corresponding taxpayer. Clause 2 of the Bill defines the act of signing a return as including a reference inter-alia to "the adopting of a password.....for the purpose of authenticating or approving the return". We find this terminology to be somewhat opaque (see below), but leaving this aside for the time being, you indicated that the principle is to incorporate an electronic return into the existing legal framework for paper returns. Thus, it is pointed out that under s51(5) of the IRO, the relevant taxpayer will be deemed to have furnished the electronic return and to be cognizant of the contents thereof unless the contrary is proved.

A taxpayer who registers to use a password will be obliged to keep it confidential and the onus will be on him to prove that it has been compromised in the event of a dispute. We pointed out at the meeting that with a 9/10 character password, which will be used infrequently, it will be quite likely that the taxpayer will write it down. This makes the system more vulnerable to abuse and could put relatively unsophisticated taxpayers in a legally disadvantageous position. The question arises whether, in principle, this is an equitable distribution of liabilities. On a more practical level, it again points to the need to stipulate in the law minimum standards of integrity

and security in relation to the system. It also suggests that at the very minimum the IRD will be duty-bound to emphasise prominently in any promotion of the new arrangements, the potential obligations and liabilities of the taxpayer.

You also indicated at the meeting and in your subsequent response that from the evidential point of view, it will be left to the Court to determine whether the integrity and security of the system has been sufficiently well established for the relevant records to be accepted as true and accurate. As there may be no precedent decisions in Hong Kong, or relevant judgments overseas in relation to the particular system proposed, this may give rise to uncertainty, at least initially.

Problems with terminology

"Adopting"/"affixing" a password

The reference in clause (2) (proposed section 2(5)) to "the adopting of.....a password..... for the purpose of authenticating or approving the return", is not self-explanatory and does not seem to be entirely consistent with the reference in clause 8 (proposed section 51AA(6)) to "how a.....password.....is to be affixed" (i.e. is it to be "affixed or "adopted", or both, and how are they related?). Furthermore is it to be understood therefore that after the Bill is passed, the signing of a paper return is to be regarded, from the point of view of terminology, as "the adopting of a signing device for the purpose of authenticating or approving the return", If so, this seems to be somewhat clumsy. We note also that section 2 of the ETO in the definition of "electronic signature" uses the phrase "attached to or logically associated with an electronic record". We question the merit of introducing another new term, namely "affixing", in the IRO.

From a security control perspective, one should not "affix" a password (as in "attach", "append", or "add") to a document, regardless of whether or not the password is encrypted. In the banking industry, user-ids and passwords have been used for many years in electronic funds transfer systems. In major systems such as SWIFT, there have never been any attempts to affix passwords to the electronic transfer instructions. Prior to SWIFT, Tested Telex systems were used to transmit funds transfer instructions. In such systems, only the test key (i.e. a manually calculated hash value to provide for message integrity) was affixed to the instructions, but not the passwords.

The issue here is that one sometimes tries to hold onto a commonly-understood principle in the physical world, i.e. in this case, the concept that the act of signing a document means that something additional needs to be added (or affixed) to the document. Hence the requirement for the password (albeit in encrypted form) to be affixed to the return.

This practice should not be allowed from a simple security control standpoint, regardless of how well the password is encrypted or otherwise protected.

There is however no reason why the Commissioner cannot affix other information to the return to identify the taxpayer, such as a hash value (encrypted or otherwise) of the return or other information (such as a Message Authentication Code).

Whilst it may in practice be the case that a password under the IRO would be used on a one-off basis (or no more frequently than once a year) for the single purpose of submitting a return, and thus the implications of a reference to "affixing" a password might, within the confines of such a system, be less problematic, there is nevertheless a danger that this would set a precedent, resulting in the same concept being adopted in other legislation and being applied to a transactional system.

The Commissioner may "approve" a password

In Australia, the definition of electronic signatures and telephone signatures can be found in the Australian Income Tax Assessment Act 1997 (No. 38 1997).

Chapter 6 The dictionary

Part 6-5 Dictionary definitions

Division 995 Definitions

995-1 Definitions

(1) [Definitions]

*<<**electronic signature**>> of an entity means a unique identification of the entity in electronic form that is approved by the Commissioner.*

*<<**telephone signature**>>* of an entity is a unique identification of the entity that can be given by telephone and that is approved by the Commissioner.

The use of the term "electronic signature" seems to be the reason giving rise to the need for approval. Electronic signature refers to a multitude of means whereby a person's identity can be authenticated, ranging from user-ids and passwords to biometrics. "Digital signature", on the other hand, refers to a specific form of electronic signature "generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function..." (definition as per the ETO). The Commissioner of the Australian Tax Authority thus needs to be in a position to specify and approve the specific electronic signatures that can be used to support the filing of a tax return - as some of the technology is not mature or practical to implement.

The basic point is that one cannot simply substitute "electronic signature" with "password" without considering the broader implications. Whilst conceptually, the concept may be similar to a bank accepting a password and subsequently acting on an instruction, we do not believe it to be the case that banks are generally required to "approve" their clients passwords as such.

The need for the Commissioner to approve things, under the Carltona principle, is not in dispute. However, the issue here is whether the Commissioner should be obliged to approve "passwords", and the general feeling is that this should not be the case. The Commissioner should instead focus on approving and specifying the policies and standards to which passwords

should conform and the definitions in the Bill should reflect this approach (see the Appendix for suggested revisions to the wording of the Bill).

There is also another important aspect here: the Australian legislation provides for two definitions, one for electronic signature, and a separate one for telephone signatures. A probable reason is that the telephone key pad only accepts numeral (i.e. 0-9) inputs, whereas a normal password may contain other characters. Thus passwords used for telephone-based systems (i.e. IVRS - interactive voice response systems) are much weaker compared to a typical password. That is probably why the Australian legislation refers to "... a unique identification... that can be given by telephone...". The Bill does not make such differentiation.

Telefiling

While telefiling may provide an alternative means of submitting a simple return, we would question the suggestion that, in any real way, it can be regarded as narrowing the gap between internet users and non-internet users. It is basically equivalent to submitting for example a gas meter reading by telephone, which has been possible for some time. We doubt whether it will do anything to promote IT and computer awareness and understanding amongst those whose current level of knowledge is low.

General comments on security

We should like to emphasise two important points here. Firstly, we are looking at an unusual system that is used (or available for use) once a year. Each user will use it once, as it is unlikely a user will submit a return twice. Such system would be difficult to administer and manage, from both an operational standpoint and a security standpoint. Operation issues concern mainly the system's ability to handle a huge volume of traffic within a relatively short period, and to provide for availability during the peak periods. Security issues arise as few, if any, users would be able to remember by heart a password that is used only once a year. The tendency therefore is for users to write their passwords down. This is a practical reality and imposing terms and conditions cannot alter that. Also, it is general practice for passwords to be changed periodically. However, since IRD only accepts returns over a specific timeframe, it would be pointless to change the password regularly throughout the year as there will be no risk at other times. So we are looking at a system that is fundamentally different from other e-commerce systems, and its security regime must therefore be adapted to suit the specific features of that system. It is the design of this security regime that need to be reviewed, as well as the detailed technical security design of the system.

Secondly, the IRD is proposing to use user-ids and passwords for both telefiling and internet filing. As indicated above, the quality of the passwords for these two systems are going to be significantly different, purely because the range of possible values for the passwords will be significantly reduced if they are limited to numeric characters. For this reason, it would be important for the Commissioner to differentiate the security systems (and the corresponding policies and standards) used for these two systems.

Once again, we welcome the opportunity to express our views on the Bill, which we hope you will find to be helpful.

Yours sincerely,

WINNIE C.W. CHEUNG
SENIOR DIRECTOR
PROFESSIONAL & TECHNICAL DEVELOPMENT
HONG KONG SOCIETY OF ACCOUNTANTS

WCC/PMT/ay
Encl.

c.c. The Honourable Eric Li Ka-cheung, JP (2827 5086)
The Honourable Sin Chung-kai (2509 9688)
Mr. Tim Lui (Chairman of HKSA Taxation Committee) (2915 6719)
SITB (Attn: Mr. Alan Siu) (2519 9780)
Chairman, Legco Financial Affairs Panel (Attn: Mr. Anthony Wong) (2869 6794)

Appendix

Proposed Amendments to the Inland Revenue (Amendment) (No. 2) Bill 2001

The following suggested amendments are designed to clarify the meaning of some of the technical language currently used within the proposed ordinance.

Clause 2

2(a) Interpretation
"password" means any combination of letters, characters, numbers or other symbols selected by a person and ~~approved~~ conforming to requirements prescribed by the Commissioner for use in systems designated by the Commissioner for the purpose of authenticating the person's identification in communicating with the Commissioner;

Clause 8

(6)The Commissioner may by notice published in the Gazette specify requirements as to—
(a)the manner of generating or sending an electronic record or any attachment required to be furnished with an electronic record;
(b)how a digital signature or password or any other ~~signing device~~ means of authentication is to be ~~affixed~~ used to authenticate a return furnished under this section; and
(c)the software and communication in relation to any attachment required to be furnished with an electronic record.

(7)The Commissioner may ~~approve a~~ prescribe the requirements to which a password should conform and designate any system in respect of any communication with the Commissioner for the purposes of this Ordinance.

Letterhead of Professional Information Security Association

CB(1) 749/01-02(03)

Mrs. Alice Lau
Commissioner of Inland Revenue
Revenue Tower
5 Gloucester Road
Wanchai
Hong Kong

7 January 2002

Dear Mrs. Lau,

Comment on Amendment to the Inland Revenue Ordinance (Cap. 112) 2001

Professional Information Security Association (PISA) is a non-profitable organization for local information security professionals. Our objective is to promote security awareness to the IT industry and general public in Hong Kong, utilizing our expertise and knowledge to help bringing prosperity to the society in the Information Age. As such we find it a necessity to express our concerns on the captioned bill to amend the Inland Revenue Ordinance.

We appreciate the effort of the HKSAR Government to extend alternatives in filing tax returns. We would like to state that while moving in such direction we have to maintain the security of the system and balance the convenience with the risk introduced.

Although there is no actual financial transaction involved in the filing a tax return, the information involved in the tax return filing process is regarded as highly personal and confidential. Besides, as we all are aware, submission of untrue, incorrect and incomplete return may incur heavy penalties. The security and accuracy of the tax return filing system should be of paramount importance.

PISA would like to point out that,

1. The SAR Government should not use a less secure system as an alternative to the current tax return submission system.

(a) The traditional hardcopy form with **Manuscript Signature** provides a true authentication of a person and it is presentable to court for legal purpose.

(b) The **Digital Signature** provides equivalent level of security. The person's private key is owned totally by oneself (something one has) and the owner needs to enter a valid pass-phrase (something one knows) to open the private key to use. A person signs a document with his/her private key to generate a digital signature that binds the person's identity with the document content. The **signature provides the data integrity of the document content** as well. A person's digital certificate is endorsed by a trusted Certificate Authority (CA) who signs the person's certificate with the CA's own private key. The CA also provides the facilities for

revocation of certificate and storage of certificate to satisfy the legal requirements. The CA fulfills a very serious set of security requirements.

(c) "**Simple Password**" authentication scheme (using a password alone) is far less secure as using a digital signature. "Simple password" is only "something one knows", a single factor system. "Simple Password" suffers from all kinds of password cracking and social engineering attacks. Furthermore, there is no comparable facility like the CA to revoke certificates and to store expired certificates. Password constitutes only the knowledge of a piece of secret code and cannot provide the legal requirement for "non-repudiation".

You can attach a simple password to an electronic document but according to the cryptography theory this is **not** considered as signing a document. **No Data Integrity** is provided in attaching the password to the document either. They are put together but not bounded together.

(d) **To conclude, Simple Password authentication scheme should not be accepted as an alternative to the digital signature in the tax return filing system.**

2. Citizens bear higher risk when using the proposed "simple password" system

(a) Since the password for the tax return filing is used only once a year, people can hardly remember it. Due to practical human memory limitation, a user of the "simple password" system tend to either

(i) use a weak password if the system allows, or

(ii) record the password in some medium instead of memorizing it.

In either case, the password is open to threats of security exposure. The exposure of the password allows a third party to use it for authentication and signing for the purpose of filing a tax return.

(b) When a citizen cannot recall the password, they are put in disadvantage position in legal disputes. The law has held him/her liable to submit untrue tax return. However, (s)he cannot prove if the tax return was (not) submitted by him/her.

(c) The use of "simple password" generates turmoil. If a person has lost his/her credit card (s)he can report to the police to avoid holding further legal liability. However, should a person report to the police immediately when finding they have lost (forgotten) the password so as to avoid the same liability? Well, do people actually know they have forgotten something? If a legal case just actually occur, will there be an influx of people reporting the forgetting password for their safety sake?

(d) Citizens are held to more legal liability with the "simple password" system because of the inherited lack of theoretical support of such technology. **For the advantage of general public, we arrive at the same conclusion as 1(d).**

3. Password affixed to a return is a security exposure

(a) It is very dangerous to affix password with another piece of valuable information or asset, like the tax return. For example, credit card companies never send a new card with the password to the client in the same envelope, nor do they send the password with a monthly statement.

(b) Delivering password in either encrypted or unencrypted forms is insecure. Password traveling outside the login (authentication) system should only be used for account activation purpose and it must be changed immediately after the first login.

(c) Furthermore, a password **CANNOT** sign a document. There is no value affixing it to a document or tax return.

4. The Inland Revenue Commissioner is given too much power

(a) The Commissioner is given the power to approve a user's password. The meaning of "approve" is **NOT** clear. If the Commissioner has to know the password in order to approve it, the security of the system would collapse. If the Commissioner just approve the "password policy" to be implemented on the systems then the wording of the bill should better be amended to reflect the actual meaning.

(b) The Commissioner is given the power to specify the return to be furnished in the form of an electronic record sent using a system, with the template and the particulars arranged in a form as specified by the Board of Inland Revenue. However, there is no requirement in the amendment of ordinance on the compliance of security of such systems, especially related to the policy of password selection, strategy of password storage, revocation and recovery, the responsibility and accountability of failure in holding such system is also not adequate.

5. Comments on the Telefiling System

The telefiling system might provide an alternative of filing to those who have visual problems. However, since it does not provide any visual form, the expected error rate is very high. To reduce the risk of a citizen filing an erroneous return and thus prone to legal liability, the IRD should issue a visual form of report to the user for verification and should allow a grace period for amendment.

6. We are concerned with the immature rollout of the alternative forms of submission

The security of the "simple password" system depends greatly on the security policy of the system and the security of the practice of the users. Policies, guidelines and education should be in place before the rollout of the system. Implementing such system in 2002 is very risky and inconsiderate.

7. The scope of application of "password" only system must be limited

(a) The amendment sets a bad example to both the civil and commercial sectors of the society. The legal status of "simple password" scheme will hinder the healthy development of the PKI, inducing greater difficulty to persuade the business to adopt a secure business infrastructure.

(b) We are worried about the future of use of "simple password" for other personal information submission or retrieval, e.g. medical records. This opens a big door for future chaos. The bad example might be copied by business as well in introducing other insecure business systems.

(c) We suggest defining the scope of application of "simple password" to government services according to the **Risk Level** to the user if the password is compromised. Only low risk service like library loan enquiry should adopt a password system. Viewing and submission of personal information should be regarded as high-risk activities and should adopt a more secure infrastructure.

(d) The Electronic Transaction Ordinance has provided a sound legal ground for digital signature. The Ordinance also facilitates the development of the Public Key Infrastructure in Hong Kong as applying to e-business and e-government. Introducing a competing and insecure authentication and signing scheme has far reaching effect and a sense of insecurity. We call for a higher-level study before any implementation. Without any in-depth study of the capability and the impact of using the "Simple Password" as equivalent to the digital signature, it is unwise to make amendment to any ordinance. If problem should occur, Hong Kong Digital Age would step out of line. The effort in building a secure infrastructure with PKI would be upset.

We appreciate you table the above opinions to the Bills Committee meetings and is waiting for your reply and clarification. Please contact me at telephone 8104-6800 or email: sc.leung@pisa.org.hk.

Your kindly attention is highly appreciated

Yours faithfully,

Mr. LEUNG Siu Cheong
Chairperson
Professional Information Security Association

建議

在法律上承認其他形式的電子簽署

6. 根據該條例，電子紀錄及有認可證書證明的數碼簽署[2]在法律上獲得承認，這可以消除公眾對進行電子交易的疑慮。我們鼓勵政府決策局及部門檢討是否可以撤除它們工作範圍內有關法例對簽署的規定，以方便進行電子交易。至於那些有須要保留簽署規定的情況，我們認為現在是適當時候去考慮應否在法律上承認除數碼簽署以外其他形式的電子簽署[3]，以推動電子商務的發展。

7. 世界各地的政府及工商業均已發展和採用不同的電子

---

[2] 根據該條例，「數碼簽署」指簽署人的電子簽署，而該簽署是用非對稱密碼系統及雜湊函數將該電子紀錄作數據變換而產生的，使持有原本未經數據變換的電子紀錄及簽署人的公開密碼匙的人能據之確定該數據變換是否用與簽署人的公開密碼匙對應的私人密碼匙產生的，及在產生數據變換之後，該原本的電子紀錄是否未經變更。

[3] 根據該條例，「電子簽署」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為認證或承認該紀錄的目的而簽立或採用的。數碼簽署是電子簽署的其中一種。

認證技術和方式。為使市民有更多選擇及促進電子商務和電子政府的發展，我們應研究應否在法律上承認其他電子認證方式。

8. 使用個人辨認號碼（PIN）是我們應研究在該條例下承認的一種認證方式。這方式現常用於銀行服務，而海外有些電子政府服務亦有採用，例如在澳洲、新加坡、英國和美國，這種方式可用於遞交稅表；而在美國某些州分，這方式可用於換領駕駛執照。這認證方式對使用者而言無疑十分方便，因他們無須依靠其他工具或設備便可透過電子方式確認其身分。使用個人辨認號碼作為認證方式，已經過市場上多種應用服務的測試。我們因此認為在適當的情況下，假如使用個人辨認號碼的穩妥程度足以應付某些指定服務[4]所牽涉的風險，則我們可以考慮以個人辨認號碼作為符合法律上簽署規定的一種電子簽署形式。例如當有關服務所涉及的雙方相互間已建立關係，並能以穩妥方式發出、使用及核實個人辨認號碼；及採用穩妥並有為資料傳送提供加密設施的「公共服務電子化」計劃系統，則可以使用個人辨認號碼這種認證方式。採用個人辨認號碼應可為使用數碼證書及親筆簽署以外的其他選擇，而個別使用人士應可自由選擇最適合自己的認證方式。**因此，我們認為應修訂該條例及增訂附表，以便資訊科技及廣播局局長（下文簡稱「局長」）透過附屬法例的程序在附表內指明有關的法律條文，說明使用個人辨認號碼可獲接納為符合該等條文下簽署的規定**。至於有關的條文會根據正常立法程序加入附表內。

9. 此外，我們亦曾考慮其他認證方式，例如利用生物特徵以資識別身分。不過，雖然這些方式在技術上可行及經已在某些機構內部應用系統中採用，但至今未有任何架構成立以支援其在社會上廣泛應用，而且預計在短期內，亦難以找到一間獨立和可

[4] 《2001年稅務（第2號）（修訂）條例草案》已提交立法會審議。除其他事項外，該條例草案訂明納稅人在根據《稅務條例（第112章）向稅務局遞交報稅表時，可使用通行密碼作為認證方式，以符合有關簽署的規定》。

靠的第三者機構能夠蒐集全港參與電子交易人士的生物特徵資料，作確認電子交易參與人士身分之用。而這種安排現時亦未獲市民廣泛接受。再者，目前甚少機構（包括政府部門在內）具備相關技術可供在進行電子交易的過程中處理外界不同人士的生物特徵資料作認證用途。**因此，我們認為應在稍後階段當其他認證方式（包括生物特徵）更趨成熟及在市場上出現相關的架構安排時，再研究其他認證方式。**