(立法會秘書處撮譯本，只供參考用)

(國際資訊系統審計協會(香港分會)提交的意見書)

就《2001年稅務(修訂)(第2號)條例草案》提出的意見

國際資訊系統審計協會(香港分會)原則上支持稅務局提出新措施，以鼓勵市民多加使用電子服務。本會經參閱有關此事的立法會CB(1)2273/01-02號文件後，現擬提出多項意見(載於附錄1)。當條例草案最初於2001年11月刊登憲報時，本會關注的事項主要關乎使用擬議電子報稅機制的保安監控問題，特別是把報稅時使用的通行密碼視為與簽署享有同等法律地位的建議；以及採用某些技術用語及概念的問題。因此，本會就條例草案有關上述事宜的用語，以及當中的涵義，提出具體意見及作出澄清(載於附錄2)。

附錄1：就《2001年稅務(修訂)(第2號)條例草案》提出的意見

1：保安的要求

本會完全支持當局需因應電腦系統所承受的特定風險，以決定有關系統所須具備的安全水平。因此，當局必須清楚瞭解與擬議電子報稅系統相關的風險。由於報稅的資料顯然須透過公共網絡傳送，當局必須防禦其他人在資料傳送時接達用於加密資料的對稱密碼匙。本會認為，擬議系統將會使用的128位元加密匙可符合"強化加密"的規定。

然而，當局不應把傳送資料的保安問題與需要認證納稅人身份的問題混為一談。有關問題在於，由於擬議系統處理敏感的資料，而該等資料對提交者亦具法律方面的影響，單憑通行密碼進行認證是否足夠？使用通行密碼作為認證的方法與使用電子證書並不相同。

立法會CB2/BC/12/01號文件第6段最後一句所述的"...曾研究有關讓納稅人可透過....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。"似乎意味着當局就傳送的安全是否足夠的問題所下的結論，已不恰當地擴展至選取認證方法的事宜上。

事實上，透過使用另一組隨機產生的數字及稅務局的公匙，把納稅人的通行密碼加密，並無提高**傳送方面的安全程度**。有關做法只能加強保障通行密碼，使密碼不會在其他人接達訊息時顯示出來。通行密碼有否加密並不會改變認證方法的性質。因此，本會認為，當局現時就保安的要求所作的考慮或許存在瑕疵，而且有關所選的認證方法是否足夠的問題，應與傳送資料時用以保障資料的方法，分開評估。

2. 現時使用通行密碼的認證方法

通行密碼在網上銀行業務上廣泛使用，並不代表有關的做法妥當。事實上，當銀行開始推行網上服務時，尚未有穩健成熟的公匙基礎設施支援此等措施。其後，銀行若要提升已存在的多套互聯網系統，以支援電子證書的使用，所涉及的成本卻十分高昂，加上其他技術及運作方面的原因，以致網上銀行至今仍廣泛使用通行密碼。

此外，其他國家的網上銀行系統亦曾因為黑客故意入侵或保安設計上的漏洞而出現嚴重的保安問題。英國的稅務當局亦曾因保安出現問題而暫停使用網上報稅系統。因此，當局應不斷評估系統的保安需要，然後選用適當的保安措施。

3. 使用電話網絡

雖然黑客可能難以入侵電話系統，但自動電話交換系統事實上普遍容易洩露資料。此外，當局只顧及資料會因外來侵襲而洩露，考慮並不周全。入侵者很多時可能旨在令電話系統癱瘓。因此，電話系統亦非完全不受影響。

由於納稅人必須在限期屆滿前提交報稅表，有關系統須在較短時間內處理突然增多的傳送量。因此，本會認為，當局需考慮的是，倘若電話網絡或後端系統在處理大量資料時出現故障或長時間的延誤，以致納稅人在限期過後才能報稅，甚至完全不能提交報稅表，有關情況對納稅人構成的影響。當局應在此等情況發生前預先作好準備，以及在事前清楚訂定稅務局、電子化計劃及個別納稅人分別應負上的責任。

4. 特定的保安設計

本會極不贊成以人手選擇任何加密匙，因為透過此種方法選取的加密匙，難免會在保安水平方面比由系統產生的密碼脆弱。

5：系統保安的檢討

本會支持當局在電話報稅及電子化計劃的系統內加入監管接達的功能，以及定期覆核該等接達及交易紀錄。有關的系統最好由獨立的第三方定期進行保安方面的檢討。

附錄2：就《2001年稅務(修訂)(第2號)條例草案》提出的修訂建議

本會現就擬議條例草案提出下述修訂建議，以澄清條例草案現時使用的部分技術用語的涵義。

第2條

2(a) 釋義

"通行密碼"指由任何人挑選並~~獲局長批准~~符合局長就稅務局指定的系統中使用所訂明的政策及標準、目的是在該人與局長通訊時認證該人身份的字母、字樣、數目字或其他符號的任何組合；

第8條

(6) 局長可藉憲報公告指明對以下各項的規定——

(a) 產生或發出電子紀錄或任何按規定須與電子紀錄一併提交的附件的形式；

(b) 如何使用~~將~~數碼簽署或通行密碼或任何其他~~形式的簽署~~認證方法~~附於~~認證根據本條提交的報稅表；及

(c) 關於任何按規定須與電子紀錄一併提交的附件的軟件及通訊。

(7) 局長可就任何為本條例的目的而與局長作出的通訊，~~批准任何~~就通行密碼訂明政策及標準及指定任何系統。

其他建議

此外，當簽訂合約的雙方同意使用某些認證方法，以支援電子業務交易，雙方事實上已贊同對方作出的一項特定假設，即：如其中一方接獲的電子訊息符合先前協定的特定要求，即在沒有相反證據的情況下，接獲訊息的一方有權把訊息視為另一方授權的證明，在商業上對雙方均具約束力。因此，當局宜於條例草案中清楚訂明此等假設。

M3859