(立法會秘書處撮譯本，只供參考用)

資訊保安及鑑證公會就《2001年稅務(修訂)(第2號)條例草案作出的聲明

本會的前提：

資訊保安及鑑證公會(下稱"本會")是由電腦保安及鑑證專業人士組成的協會。本會認為，由於資訊保安基建是透過利用數碼證書作為認可及法律上接納的簽署工具而確立的，稅務局除接納數碼證書所產生的數碼簽署外，亦接納以通行密碼及任何簽署工具簽署報稅表的做法，令整個基建受到削弱。

這項修訂會帶來兩個問題。首先，這意味著通行密碼及任何簽署方式均可產生與使用數碼證書具同樣保安水平的認可數碼簽署，而這在技術上是不正確的。其次，由於在稅務局報稅表系統中使用的通行密碼屬稅務局局長及擁有人本身共有的秘密，利用通行密碼簽署的訊息不能達到不容推翻的目的。

因此，本會不贊同稅務局在《2001年稅務(修訂)(第2號)條例草案》中所提出的修訂。

本會的意見：

1. 修訂的方向及動機均屬正確。

2. 對非電腦用戶來說，透過電話報稅是上選。

3. 通行密碼、個人辨認號碼或稅務編號均可用作認證納稅人在稅務局網站上的身份。然而，由於有一位人士或以上能取得納稅人的通行密碼，上述密碼不能用作證明報稅表的真確性。

數碼證書／數碼簽署可用作認證及不容推翻。然而，通行密碼、個人辨認號碼或稅務編號只可達到**識別及認證身份的目的，而不能達到不容推翻的目的**。

根據稅務局建議的計劃，稅局密碼匙的持有人及通行密碼的擁有人，均可產生同樣的密碼雜湊。因此，若通行密碼持有人聲稱稅務局所出示的報稅表曾作出修改，稅務局便不能在法律訴訟中以密碼雜湊作為保障。這是因為並無不容推翻的保證。

通行密碼除可用作確定及認證身份外，亦可用作產生密碼雜湊及數碼簽署。然而，與公匙密碼加密法不同，通行密碼產生的數碼

簽署及認證計劃不能達到不容推翻的目的。目前，根據香港法例，公匙密碼加密計算法是唯一能用作查證電子文件是否不容推翻的計劃。

4. 在稅務局建議的報稅制度中，通行密碼、個人辨認號碼或稅務編號的設計均並不安全。根據條例草案所作的修訂，稅務局局長有取得及覆核納稅人所選通行密碼的特權。此外，在傳統的共用通行密碼系統中，發信人及收信人若使用共同密碼，將會產生密碼核對和，因此，其他人可知悉納稅人所使用的密碼。

此外，Itsik Mantin、Adi Shamir及Scott Fluhrer 已在其文章內指出，強化加密技術(RC4)有內在的弱點。據他們的文章所載，RC4較適用於密碼匙會在信息每次進行加密後便更新的連串資料保障。因此，稅務局在推行利用RC4的加密計劃時應特別小心。

5. 稅務局在條例草案中所建議的提交報稅表簽署程序**並無清楚界定和並不清晰**。在條例草案擬稿中，稅務局擬把"...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本條提交的報稅表內..."一句加入法例之內。然而，此處並無清楚述明報稅表的簽署如何產生及送交稅務局。

這句甚至意味著通行密碼是附於根據本條所提交的報稅表。本會建議修改條例草案的措詞，以免產生混淆。

6. 根據傳統，通行密碼是以雜湊的方式保存，以防止其他人取得密碼匙解開所有通行密碼。在稅務局建議的報稅系統中，通行密碼將以對稱密碼計劃保存，任何人只要擁有加密匙及加密的檔案，即可檢索檔案上的所有密碼。因此，稅務局局長及納稅人均可在該系統內獲認證其納稅人身份。在出現爭議時，這會削弱稅務局向法庭所提出的證供。

m3856