

Ref: HQ309/405/22C

Mr LEUNG Siu-cheong
Chairman
Professional Information Security Association
Unit 610, Lippo Sun Plaza
28 Canton Road
Tsimshatsui, Kln

13 February 2003

Dear Mr Leung,

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

Thank you for your letter of 10 February 2003. I am pleased to provide below our response to the various points raised by you.

Interface with ETO and statutory support for the use of password/PIN

The Electronic Transactions Ordinance (ETO) was enacted to facilitate electronic transactions and drive e-business development by providing electronic records and digital signatures with the same legal status as that of their paper-based counterparts. While the ETO is designed to provide a generic framework that can be applied to various legislation, it should not prevent other Government bureaux and departments from amending or introducing their own legislation to cater for the specific needs and requirements for implementing electronic services.

We do not consider that the ETO should be interpreted as giving an exclusive legal recognition to digital signature. It has in fact followed a 'Technology Neutral' approach and provided legal recognition for digital signature and other forms of electronic signature. Section 14 of the ETO provides that if an Ordinance accepts an electronic process or the authentication of information by **an electronic signature** for the purposes of that Ordinance 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. Password is a form of electronic signature as referred to in the above provision.

We understand that one of the major issues examined in the ETO Review in 2002 was whether in addition to digital signature legal recognition should be extended to cover other forms of electronic signature, including password. Though it has not been proposed in the Review to make a general amendment in the ETO on the use of password for satisfying a signature requirement under the law, the Administration remains of the view that password

should be introduced for services where the level of security offered by it is commensurate with the risk of the services involved. Where the use of password is appropriate in any government service, the Administration will deal with it by specific amendments to relevant legislation, so that the implications of the legislative amendment and the security concern of that proposal can be fully examined by the Legislative Council and the community. We consider tax return filing to be one of the specific cases where password can be accepted as sufficiently secure for the purpose.

As to your comment regarding the adverse impact of the Bill on the ETO, we would state that the proposed amendment merely allows the use of password as **an alternative means** to satisfy the signature requirement for return filing purpose and IRD will continue to accept the use of digital certificates. There is thus no question of the Bill bypassing the ETO or having any adverse impact on the ETO.

Will the Bill set a precedent for use of PIN in other Government services

We wish to re-iterate that the purpose of the Bill is not to give password the same status as digital signature in all situations or extend the possible methodologies for effecting e-transactions in a general way. As mentioned above, since the legal amendments for using password / PIN in other government services are subject to the scrutiny of the Legislative Council and the community, we do not think that the Bill will set an unwarranted precedent for other Ordinances.

Security measures of the proposed system

We fully share your comment that preserving the confidentiality of taxpayers' information is of utmost importance. We also acknowledge that there is a difference in the level of security between using password and using digital signature. However, we consider that with our proposed system security design (details of which have already been elaborated in our letter of 11 January 2002 in reply to yours of 7 January 2002) and the tight administrative measures, a password can be accepted as sufficiently secure for tax return filing purpose.

Whether security measures need be provided in the Bill

We wish to advise that the Department has always been obliged to ensure the security of its systems, whether for tax returns filed in the conventional way or through the proposed electronic means. Furthermore, the existing legislations, such as the Personal Data (Privacy) Ordinance and the secrecy provision in section 4 of the Inland Revenue Ordinance have already provided a comprehensive legal framework on IRD's responsibility and accountability in the handling and protection of personal information collected from the public. This position will not be changed with the proposed use of password for return filing purposes. We therefore do not consider it necessary to introduce specific provisions in the Bill to benchmark the system security requirements for handling electronic tax returns.

Suggestions for additional system controls

We thank you for your suggestions regarding the controls to be added to the system. In this regard, we would state that the Department always attaches great importance to IT security policy and has established strict guidelines and procedures for information and data handling. Tight security control measures will be implemented under the tax return filing system to protect the integrity, confidentiality and availability of taxpayer's data. It is also the Department's policy to conduct regular audit review on system security to keep in pace with technology development. Administrative measures will also be put in place to remind the public of sound password practices. In relation to your comments on the higher risk features on the functions of "Default data display on the next entry" and "Data review and modification", we have already planned to commission an independent consultant to review the security design of these functions before their implementation.

Appeal for support

Finally, I think you would agree that there is no such thing as a perfect security system or of a system with perfect security. A balance would have to be struck between attaining the highest level of security at all costs and affording convenience to the customers at reasonable security level. We believe that we have carefully balanced the two sides in the proposed system being offered. For now, the most important thing is for the IRD to be given the green light to go ahead so that she can take the steps forward and towards realizing the desired goal.

Once again, I would like to thank you for your valuable comments and look forward to your continued support in this matter.

Yours sincerely,

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

cc The Hon Eric LI Ka-cheung, JP, Chairman, Bills Committee
 The Hon. SIN Chung-kai
 Secretary for Financial Services and the Treasury (Attn: Mr Ivanhoe Chang)
 Clerk to Bills Committee