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 invoked and demonstrated. Non-repudiability 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 all 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)