立法會
Legislative Council

LC Paper No. CB(1) 2273/01-02

Ref : CB2/BC/12/01

Background brief on
Inland Revenue (Amendment) (No. 2) Bill 2001

Purpose

This paper gives a summary of major issues considered by members of the Panel on Financial Affairs (FA Panel) in respect of the Inland Revenue (Amendment) (No. 2) Bill 2001.

Objective of the Bill

2. At present, electronic filing of Tax Returns - Individuals and Property Tax returns with the use of digital signatures under the Government Electronic Service Delivery (ESD) Scheme and the filing of Profits Tax returns in e-Forms are provided for in the Electronic Transactions Ordinance (ETO) (Cap. 553). The Inland Revenue Department (IRD) proposes to provide alternative means for tax return filing, i.e. filing of tax returns by telephones and the use of a password for filing of tax returns under the ESD Scheme. There are however no provisions, in either the ETO or the Inland Revenue Ordinance (Cap. 112) for these alternative means.

3. The Bill seeks to provide a legal basis for -

(a) the use of password for authentication and fulfillment of signature requirement for tax returns filed under the ESD Scheme; and

(b) the filing of tax returns by telephones.

Deliberation of the Panel

4. When the Bill was considered by the House Committee on 23 November 2001, some Members raised concern about the security of information contained in the tax returns in the course of filing the return by the proposed new means. Members decided that the policy aspects of the Bill, including the security aspect, should first be considered by the FA Panel before a decision was made on whether a Bills Committee should be formed to study the Bill.

5. The major issues considered by members of the FA Panel at the meeting on 7 January 2002 are summarized below.

Security aspects

6. According to the Administration, the level of system integrity required or desired in an IT system has to be determined having due regard to the risk involved. The Information Technology Services Department has studied the proposal for allowing the filing of a return under the ESD Scheme by using a password and concluded that such a system will attain a high level of security in the transmission of tax data by meeting the "strong encrytion" 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.

7. The Administration has also pointed out that the use of a password for authentication is widely adopted in the internet especially for most internet banking services, and internet filing of tax returns with the use of a password for authentication has also been implemented in many other tax jurisdictions such as the United States, Canada and Singapore.

8. As regards the submission of tax returns by telephone, the Administration has advised that the public telephone network is considered to be a "trusted network" and is widely used by banks and public utilities companies for conducting electronic transactions. It is extremely difficult to hack into a telephone network system, and having regard to the nature of data transmitted through the telephone lines, the chance of security risk should be remote. Again, telefiling has been adopted by other tax jurisdictions including the United States, Canada, Australia and Singapore.

9. Some Panel members have expressed support for providing taxpayers with the proposed new channels for filing tax returns, which is consistent with Government policy of using information technology to improve Government services. They consider that although the use of passwords for authentication in electronic transactions does not provide the same level of security as the use of digital certificates, the use of passwords for internet filing of tax returns is acceptable given the technology available to ensure data security and the measures put in place by the Administration. They also consider that given the proven experience of overseas tax jurisdictions in the use of passwords for authentication, and provided that the Administration exercises prudent monitoring of the systems, the proposed new filing channels should not give rise to security problems.

Cost-effectiveness and efficiency of the proposed new means of tax return filing

10. Some members have expressed concern about the cost-effectiveness of establishing and maintaining a telefiling system, in consideration that the system would probably be used by individual taxpayers once a year only, and that the utilization of this system among taxpayers may turn out to be low.

11. The Administration estimates that 800,000 taxpayers would meet the eligibility criteria for telefiling. While the initial take-up rate may not be high, the Administration expects the rate to gradually increase over time (perhaps 5% in the longer term). The total cost of implementing the telefiling project is about $4.8 million while a staff saving of $0.9 million a year could be achieved as a result of the lesser demand on manual filing and data input.

Efficiency of the telefiling system

12. The Panel has noted that on average, it would take about five minutes for telefiling a Salary Tax return and about four minutes for a Property Tax return. The telefiling system will record and store the data captured during the whole return fling process in digitized format. Taxpayers may lodge a written request to IRD for a copy of the print-out of the data stored in their own tax files.

Interface with the Electronic Transactions Ordinance

13. The Panel has raised concern on how the Bill would interface with the ETO and whether the Administration would extend the use of passwords to other electronic government service applications. The Panel has noted the following relevant views of the Hong Kong Society of Accountants (HKSA), as conveyed by Hon Eric LI -

(a) HKSA in principle supports the early implementation of proposed new services as additional channels to facilitate the submission of tax returns;

(b) For the integrity of the legal framework governing electronic transactions, HKSA considers it preferable to have provided for in the ETO the changes sought to be effected by the Bill;

(c) However, HKSA accepts that internet filing and telefiling of tax returns with the use of a password warrant specific arrangement as provided for under section 14 of ETO; and

(d) The Administration should review the ETO as a matter of priority to examine whether and how the ETO should cater for the specific arrangements for electronic transactions provided for in other ordinances but not yet in the ETO. In the course of the review of the ETO, any inadequacies in the IRO in relation to electronic transactions should also be addressed.

14. According to the Administration, the ETO provides a generic legal framework for electronic transactions. Section 14 of the ETO specifies 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. It is not Government's policy intention to put all legislative provisions concerning electronic transactions in the ETO, as such an approach may not be possible or practical. The Bill seeks to provide a self-contained and comprehensive legal framework to facilitate internet filing and telefiling with the use of a password for authentication.

15. At the FA Panel meeting, the Administration advised that it had published a public consultation paper on the review of the ETO in March 2002. The consultation period ended on 30 April 2002. The Panel on Information Technology and Broadcasting was briefed on the consultation paper on 11 March 2002. The Administration highlights that with proper management, personal identification number (PIN) can be considered for acceptance as a form of electronic signatures for satisfying the signature requirement under law in specified cases. The proposal of using a password for tax return filing in the Bill is cited as an example of such specified cases. The Administration recommends that the ETO be amended and a new schedule be added so that the Secretary for Information Technology and Broadcasting *(see note 1)* may, by subsidiary legislation, specify in the new schedule legal provisions under which the use of PIN will be accepted for satisfying the signature requirement.

Powers conferred on the Commissioner of Inland Revenue's under the Bill

16. The Panel has raised concern about the availability of checks on the additional powers conferred on C of IR by the Bill. According to the Administration, the powers to be conferred on C of IR under the Bill only cover routine and operational matters, which may change from time to time. These matters do not carry any significant policy implications. The relevant tax authorities in overseas jurisdictions are given similar powers in making regulations or specifications in respect of eligibility criteria, the form and manner as well as the signature requirements of furnishing an electronic return.

Letters from professional bodies and drafting issues

17. The Panel noted that HKSA and the Professional Information Security Association had written to the Commissioner of Inland Revenue (C of IR) on the Bill, and C of IR had replied on 11 January 2002. The correspondence was attached in **Appendix IV**.

18. Referring to the points raised in these correspondence, a member has requested the Administration to review the practical arrangements for C of IR to approve a user's password and the propriety of using the term “affix” in proposed section 51AA(6)(b) of clause 8. The member has also queried the necessity of including "any other signing device" in this proposed section, as this may add uncertainties to the scope of powers conferred on C or IR with regard to the specification of devices for authentication in relation to filing of tax returns.

19. According to the Administration, the Department of Justice's advice is that the wordings of "affixed" and "approved by the Commissioner" used in the Bill are appropriate. The proposed wordings of HKSA are adequate in supporting the functions that a "password" is required to perform on tax returns as a "signature".

---

1 The statutory functions previously exercisable by the Secretary for Information Technology and Broadcasting under the ETO have been transferred to the Secretary for Commerce, Industry and Technology with effect from 1 July 2002.

The ordinary meaning of the word "affix" includes "adding something" and "attaching something", so a "password" can be "affixed" to tax returns. The Administration however agrees to move a Committee Stage Amendment to remove "any other signing device" from clause 8 of the Bill.

Relevant papers

20. The following related papers are attached -

LC Paper No. CB(1)716/01-02(03) dated 3 January 2002	- Administration's paper on "Security aspects on the use of password in electronic filing of tax returns" provided for the FA Panel meeting on 7 January 2002 (**Appendix I**)
LC Paper No. CB(1)1120/01-02	- Minutes of meeting of FA Panel on 7 January 2002
LC Paper No. CB(1)767/01-02	- Report of FA Panel on "Submission of tax returns by electronic means and by telephone with the use of a password" for the House Committee meeting on 11 January 2002 (**Appendix II**)
LC Paper Nos. CB(1)797/01-02 and CB(1)831/01-02 dated 11 & 17 January 2002 respectively	- Letter dated 11 January 2002 from the Secretary for the Treasury (**Appendix III**) to the Chairman of FA Panel
LC Paper Nos. CB(1)749/01-02(02) & (03) and CB(1)805/01-02 dated 8 &14 January 2002 respectively	- Correspondence between C of IR and HKSA and the Professional Information Security Association (**Appendix IV**)
LC Paper No. CB(1)1239/01-02 dated 5 March 2002	- Administration's consultation paper on "Review of the Electronic Transactions Ordinance" provided for the Panel on Information Technology and Broadcasting (an extract in **Appendix V**)

Legislative Council Secretariat
12 July 2002

For meeting on
7 January 2002

LEGISLATIVE COUNCIL PANEL ON FINANCIAL AFFAIRS

SECURITY ASPECTS ON THE USE OF PASSWORD IN ELECTRONIC FILING OF TAX RETURNS

PURPOSE

This paper briefs Members on the technical and administrative measures that the Inland Revenue Department (IRD) will adopt to ensure that electronic filing of tax returns by using passwords will be conducted in a secure manner.

BACKGROUND

2. On 21 November 2001, the Secretary for the Treasury introduced into the Legislative Council the Inland Revenue (Amendment) (No.2) Bill 2001. This amendment Bill seeks to provide a legal basis for:

- the use of password for authentication and fulfillment of signature requirement for tax returns filed under the Government Electronic Service Delivery (ESD) Scheme; and
- the filing of tax returns through telephones.

3. In response to the Legislative Council House Committee Members' request, this paper addresses the security aspects on the use of passwords in electronic filing of tax returns and on telefiling, and sets out the technical and administrative measures that IRD will take to ensure the security of information submitted by the above new means.

TECHNICAL MEASURES

Transmission of tax return data through ESD platform by password

4. Internet filing by using a password is as secure as in the case of using digital certificate. Except that the electronic submission will be signed by applying the taxpayer's password, the system can achieve the same level of security for the data transmitted over the internet because of the use of strong encryption technology. Due to the use of encryption technology, information on the tax return will be end-to-end encrypted on the one hand, meaning the information will be encrypted from the point the return is sent to the point when the return is received by the department by a group of numbers randomly generated by the browser (commonly known as the session key) and IRD's public key. On the other hand, the taxpayer's password will also be encrypted by a different set of randomly generated numbers and IRD's public key for better security control.

5. The Information Technology Services Department (ITSD) has earlier on looked into the security aspect of the two options, viz. filing of a return under the ESD Scheme by using a password vis-a-vis digital certificate. The department concluded that both options attain the same level of security by meeting the "strong encryption" requirements and protecting the session key against third party access. The use of a password as a signing device will not downgrade the degree of security.

6. As a matter of fact, the use of a password for authentication is widely adopted in the internet especially for most internet banking services. The design of the ESD system to use passwords for authentication would adopt similar security standard as in the commercial sector for e-commerce and internet banking services.

7. Internet filing with the use of a password for authentication has also been implemented in other tax jurisdictions such as the United States, Canada and Singapore.

Transmission of tax return through telephone

8. The public telephone network is considered to be a "trusted network" and

is indeed widely used by banks and public utilities companies for conducting electronic transactions. Wiretapping of telephone requires physical access to the telephone lines and special decoding equipment to be set up. This makes it extremely difficult to hack into a telephone network system. Having regard to the nature of data transmitted through the telephone lines, the chance of security risk should be remote.

9. 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 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. According to the U.S. Internal Revenue Service, in the U.S., about 5 million returns were filed through telephone in 2000. In the light of other countries' experience, we believe that transmitting tax return data through telephone network is unlikely to pose a security concern.

ADMINISTRATIVE MEASURES

Authorization and Authentication Control

10. A registration mechanism will also be put in place so that the service is only accessible by authorized users after proper authentication. All persons intending to file a tax return electronically by using a password have to register with IRD in advance to obtain a Taxpayer Identification Number (TIN) and an Access Code which will be despatched to them under separate cover. To complete the registration process, the taxpayer has to access the telefiling system using both the TIN and the Access Code and to register a password of his own choice. The TIN and the password will be used for authentication purposes in all subsequent electronic transactions.

11. Checking will be built into the telefiling and ESD systems to guard against unauthorized access. In the event that the number of unsuccessful attempts to gain access to a TIN record exceeds 5, the relevant password will be revoked. The taxpayer has to apply for the Access Code again before he can use the service.

12. All password information will be stored in encrypted format. The generation of the encrypted password from its 6-digit format involves the use of a strong encryption algorithm with a 128-bit encryption key. The encryption key will be specified by a Deputy Commissioner of Inland Revenue and no person other than him knows this encryption key.

System Security Control

13. The telefiling and ESD systems are designed with an access control feature which only allows authorized persons to use the system. All access will be logged for security control and audit trail purpose.

Custody of Password

14. The terms and conditions for use of the password will be clearly set out for the attention of all registered users of the service. Users will be advised to keep their passwords strictly confidential, to change them periodically and to report to IRD any incident of the passwords having been lost or compromised.

Review of Transactions Log

15. All access and updating transactions will be logged by the system and IRD will conduct a daily review of the transactions log to ensure that all transactions have been properly authorized.

CONCLUSION

16. The foregoing paragraphs set out the tight administrative and system control IRD will exercise in an attempt to ensure the security of the data transmitted via electronic and telephonic means. In designing the telefiling system and the use of passwords for tax returns furnished under the ESD Scheme, IRD has made extensive reference to the standard adopted by the commercial sector and other tax jurisdictions. The continuing practice in the commercial sector and overseas experience indicate that telefiling and the use of a password are secure means of conducting electronic transactions. Conducting tax-related businesses through telephone networks or the use of password should not pose any security concerns.

ADVICE SOUGHT

17. Members are requested to note the above technical and administrative measures to be adopted by IRD to ensure that electronic filing of tax returns by using passwords is conducted in a secure manner. We hope that Members would support the Inland Revenue (Amendment) (No.2) Bill 2001, which seeks to provide greater convenience for taxpayers by providing a legal basis for filing of tax returns through the use of passwords and telefiling.

Inland Revenue Department
December 2001

立法會
Legislative Council

LC Paper No. CB(1) 767/01-02

Ref : CB1/PL/FA

Paper for the House Committee meeting
on 11 January 2002

Report of the Panel on Financial Affairs
Submission of tax returns by electronic means and by telephone
with the use of a password

Purpose

This paper reports on the deliberation of the Panel on the submission of tax returns by electronic means and by telephone with the use of a password at the Panel meeting held on 7 January 2002.

Background

2. At the House Committee meeting on 23 November 2001, when members considered the Inland Revenue (Amendment) (No. 2) Bill 2001 (the Bill), which was introduced to the Council on 21 November 2001, members noted that the Bill sought to provide the legal framework for submission of tax returns by electronic means and by telephone with the use of a password. Some members raised concern about the security of information contained in the tax returns in the course of filing the returns by these new means. Members agreed that as the policy aspects of the Bill had not been discussed by the relevant Panel prior to its introduction into the Council, the subject might first be considered by the Panel on Financial Affairs, before a decision was made on whether a Bills Committee should be formed to study the Bill.

Deliberation of the Panel

Security aspects

3. According to the Administration, internet filing by using a password is as secure as in the case of using a digital certificate, due to the use of strong encryption technology for end-to-end encryption. The use of a password as a signing device will not downgrade the degree of security. The Administration has also pointed out that the use of a password for authentication is widely adopted in the internet especially for most internet banking services, and internet filing of tax returns with the use of a password for authentication has also been implemented in other tax jurisdictions such as the United States, Canada and Singapore.

4. As regards the submission of tax returns by telephone, the Administration has advised that the public telephone network is considered to be a "trusted network" and is widely used by banks and public utilities companies for conducting electronic transactions. It is extremely difficult to hack into a telephone network system, and having regard to the nature of data transmitted through the telephone lines, the chance of security risk should be remote. Again, telefiling has been adopted by other tax jurisdictions including the United States, Canada, Australia and Singapore.

5. Members have also taken note of the administrative measures put in place by the Inland Revenue Department (IRD) to ensure data security.

6. Some members have expressed support for providing taxpayers with the proposed new channels for filing tax returns, which is consistent with Government policy of using information technology to improve Government services. Their views were as follows-

(a) Although the use of passwords for authentication in electronic transactions does not provide the same level of security as the use of digital certificates, the use of passwords for internet filing of tax returns is acceptable given the technology available to ensure data security and the measures put in place by the Administration;

(b) Given the proven experience of overseas tax jurisdictions in the use of passwords for authentication, and provided that the Administration exercises prudent monitoring of the systems, the proposed new filing channels should not give rise to security problems.

7. The Commissioner of Inland Revenue (C of IR) has advised that the Administration does not intend to equate the legal status of digital signatures with passwords. However, the Administration is confident that with the relevant technical and administrative measures put in place, using passwords for authentication can achieve a comparable standard of security as using digital signatures.

Cost-effectiveness

8. Some members have expressed concern about the cost-effectiveness of establishing and maintaining a telefiling system, in consideration that the system would probably be used by individual taxpayers once a year only, and that the utilization of this system among taxpayers may turn out to be low.

9. According to C of IR, the Administration cannot at this stage provide a precise estimate of the utilization rate of the telefiling system. While the utilization rate may be low during the initial implementation period as in the case of other Government electronic services, implementation of the proposed new services is an important step forward in enhancing IRD's services. IRD is

implementing a five-year programme to enhance its services through the use of information technology. The proposed new channels for filing tax returns form part of a comprehensive package of new electronic services to be launched by IRD. The use of a password for authentication is also applicable to other electronic services of IRD including the interactive tax enquiry services on the Internet.

10. As regards staffing implications of the proposed new services, C of IR has advised that upon completion of the five-year programme, it is envisaged that there would be manpower savings in IRD. There is no plan to create any additional directorate post in IRD to implement the proposed new services.

Efficiency of the telefiling system

11. Regarding the normal time required for telefiling a tax return, the Panel has noted that on average, it would take about five minutes for telefiling a Salary Tax return and about four minutes for a Property Tax return. IRD would be issuing a guidance note to taxpayers who have registered with IRD for the new service to facilitate their use of the service. The Administration has been requested to provide information on whether there is any way for a taxpayer who has used the telephone to file a tax return to review and verify the accuracy of the information he has submitted.

Interface with other electronic transactions - related legislations

12. The Panel has also examined the interface between the Bill and other legislations, such as the Electronic Transactions Ordinance (Cap. 553) (ETO) and the recently-introduced Import and Export (Electronic Transactions) Bill 2001.

13. According to the Administration, the ETO provides a generic legal framework for electronic transactions. Section 14 of the ETO provides scope for specific situations to be dealt with in a "self-contained" manner in another ordinance. While the use of a password for authentication may not be broadly applicable to all types of electronic transactions, it can be suitably applied to electronic filing of tax returns provided that there are proper measures in place to ensure data security. The Bill seeks to provide a self-contained and comprehensive legal framework to facilitate internet filing and telefiling with the use of a password for authentication.

14. The Panel has also noted that a review of the ETO is being undertaken and a relevant public consultation paper will be published in one to two months.

15. As regards the consistency between the Bill and the Import and Export (Electronic Transactions) Bill 2001, the Administration has undertaken to provide information in this respect.

Views of professional bodies

16. The Panel has noted two letters addressed to C of IR from the Hong Kong Society of Accountants (HKSA) and the Professional Information Security Association setting out their concerns and views on the submission of tax returns with the use of a password.

17. Mr Eric LI has advised the Panel of the position of the HKSA with regard to the proposed new services. In gist -

(a) HKSA in principle supports the early implementation of proposed new services as additional channels to facilitate the submission of tax returns;

(b) For the integrity of the legal framework governing electronic transactions, HKSA considers it preferable to have provided for in the ETO the changes sought to be effected by the Bill;

(c) However, HKSA accepts that internet filing and telefiling of tax returns with the use of a password warrant specific arrangement as provided for under section 14 of ETO; and

(d) The Administration should review the ETO as a matter of priority to examine whether and how the ETO should cater for the specific arrangements for electronic transactions provided for in other ordinances but not yet in the ETO. In the course of the review of the ETO, any inadequacies in the IRO in relation to electronic transactions should also be addressed.

18. Taking note of the views of the two organizations, a member pointed out the need to review the practical arrangements for C of IR to approve a user's password and the propriety of using the term “affix” in proposed section 51AA(6)(b) of Clause 8, which provides that C of IR may by notice published in the Gazette specify requirements as to how a digital signature or password or any other signing device is to be affixed to a return furnished under this section. The member also queried the necessity of including "any other signing device" in this proposed section, as this may add uncertainties to the scope of powers conferred on C or IR with regard to the specification of devices for authentication in relation to filing of tax returns. The Administration has undertaken to further review the drafting of the Bill taking into account members' comments and the views of professional bodies.

Other issues

19. The Panel has also invited the Administration to brief members on the availability of checks on the additional powers conferred on C of IR by the Bill. According to C of IR the relevant tax authorities in overseas jurisdictions are given similar powers in electronic filing and telefiling of tax returns. The powers

conferred on C of IR are administrative in nature and pertinent to the implementation of the proposed new services. The existing legal framework under the IRO has already provided adequate checks on C of IR's powers. As regards the timing for launching the proposed new services, while some members has considered it appropriate to launch the new services in April 2002 as currently scheduled, there was also a view among members that the relevant issues should be thoroughly considered to ensure propriety of the proposed legal framework and the security and reliability of the technical infrastructure.

Advice sought

20. Members are invited to take note of the deliberation of the Panel in considering whether a Bills Committee should be formed to scrutinize the Bill.

Council Business Division 1
Legislative Council Secretariat
10 January 2002

Appendix III

Fax No. : 2530 5921
Tel No. : 2810 2310
Our Re£ FIN 43/5/144
Your Ref. :

11 January 2002

Hon Ambrose Lau Hon-chuen
Chairman of the Legislative Council
Panel on Financial Affairs
Legislative Council Building
8 Jackson Road, Central
Hong Kong

Dear Mr Lau,

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

Thank you for giving us an opportunity on 7 January 2002 to explain to Members the objectives of the Inland Revenue (Amendment) (No.2) Bill 2001 and the security aspects on the proposals contained therein (i.e. filing of a return under the Electronic Service Delivery (ESD) Scheme by using a password, and the use of passwords in telefiling). We are grateful that Members were in general supportive of the policy of introducing the use of passwords in electronic filing of tax return, and of implementing telefiling. We understand that Members were in general satisfied with the security aspects of the systems. We also note that some Members would like to have these new services introduced as scheduled (which will be the second quarter of this year).

2. To facilitate Members' further consideration of the Amendment Bill, we provide hereunder our detailed response to and supplementary information on the questions/concerns Members raised at the meeting.

Security of the use of passwords in filing of tax returns

3. The paper we issued to the Financial Affairs Panel has set out in detail the measures the Inland Revenue Department (IRD) would put in place to ensure that the systems enabling the use of passwords to file tax returns electronically and through telephone are secure.

4. As noted by some Members at the Panel meeting, 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, the Information Technology Services Department (ITSD) has earlier on studied and endorsed the security of this proposal. ITSD's conclusion is that such a 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.

5. The use of a password is now widely adopted in the internet especially for most internet banking services. Internet filing of tax returns with the use of a password has been implemented in many other tax jurisdictions (including the United States, Canada and Singapore). The proposed introduction of this new means of electronic tax filing service by IRD is a move in line with these general trends of e-commerce development.

Telefiling Process

6. Some Members asked what would be the usage of telefiling and what would be the procedures. The telefiling process is summarised in ***Annex***. Before performing the filing, a taxpayer may put down all the information required in the tax return on the ``Telefiling Record Sheet", which will be provided by IRD. The Sheet serves as a checklist and assists taxpayers in the filing process. After a filing has been performed, the system will repeat automatically the relevant tax return data keyed in by the taxpayer for his confirmation. He may then check the accuracy

of the inputted data against the record on the "Telefiling Record Sheet" and make changes to the data inputted if necessary. It will take a taxpayer around 4 to 5 minutes to complete the filing. The telefiling system will record and store the data captured during, the whole return filing process in digitized format. Taxpayers may lodge a written request to IRD for a copy of the print-out of the data stored their own tax files.

7. We estimate that 800,000 taxpayers would meet the eligibility criteria for telefiling. In view of the fact that this will be a new service and that taxpayers may take some time to get used to it, the initial take-up rate may not be too high, but we expect the rate to gradually increase over time (perhaps 5% in the longer term). In other tax jurisdictions, the telefiling take-up rates range between 3% to 9% (4.1% for USA, 2.9% for Canada and 8.5% for Singapore). IRD will launch massive publicity activities to promote this new service upon enactment of the legislation.

8. The total cost of implementing the telefiling project is about $4.8 million ($4.2 million in non-recurrent expenditure and $0.6 million non-recurrent staff cost). We also estimate that a staff saving of $0.9 million a year could be achieved as a result of the lesser demand on manual filing and data input.

Interface with the Electronic Transactions Ordinance

9. Some Members would like to know how the Inland Revenue (Amendment) (No.2) Bill 2001 would interface with the Electronic Transactions Ordinance (ETO) and whether the Administration would extend the use of passwords to other electronic government service applications.

10. 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. The Ordinance provides a generic framework that can be applied to other legislation. However, this does not preclude dealing with specific situations in the relevant ordinances in a self-contained manner. It is for

this purpose that section 14 of the ETO specifies 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. It is not our policy intent to put all legislative provisions concerning electronic transactions in the ETO, as such a approach may not be possible or practical.

11. A Member asked us to ensure that consistent terminologies would be used in different ordinance and quoted the Import and Export (Electronic Transactions) Bill 2001 as an example. 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 focus of the Inland Revenue (Amendment) (No. 2) Bill 2001 is to provide an alternative to the mode of authentication in satisfying the signature requirement in filing tax returns and the necessary legislative backing for the use of passwords in filing tax returns electronically. These two Bills contain provisions which cater for electronic processing in their own specific and different situations. Both are consistent with the policy intent and sprint of the ETO.

12. 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 use of passwords in filing tax returns and telefiling, as proposed in the Amendment Bill in order to drive the development of E-government in Hong Kong,. ITBB will consider whether or not the use of passwords should be widely adopted in other electronic processes. It will consult the public on the issue shortly in the context of the coming ETO review.

Commissioner of Inland Revenue's power in relation to specification

13. Members asked about the Commissioner of Inland Revenue (CIR)'s power under the Amendment Bill. In clause 8 of the Amendment Bill, the Commissioner is empowered to specify certain cases where the furnishing of a return by electronic filing and the use of the telefiling system are applicable, to specify technical or other details concerning an electronic record or any attachment required to be furnished with an electronic record, and to approve a password. These eligibility criteria and form and manner of the returns are routine an operational matters, and may change from time to time. As these matters do not carry any significant policy implications, we propose to allow the Commissioner to deal with them.

14. In other tax jurisdictions like USA, Singapore, United Kingdom, Australia and Canada their CIR equivalents are also given the power to make regulation or specifications in respect of eligibility criteria, the form and manner as well as the signature requirements of furnishing an electronic return.

Specific Drafting Issues

15. Some Members referred us to the specific drafting suggestions forwarded by the Hong Kong Society of Accountants (ref. Appendix to the Society's letter to CTR dated 4 January) and urged us to review our position.

16. We have carefully examined the Society's suggestions. The Department of Justice's advice is that the wordings of “affixed” and “approved by the Commissioner” used in our Bill are appropriate. The Society’s proposed wordings are inadequate in supporting the functions that a “password” is required to perform on tax returns as a “signature”. The ordinary meaning of the word “affix” includes “adding something” and “attaching something”, so a “password” can be “affixed” to tax returns. CIR has set out detailed comments in her reply dated 11 January 2002 to the Society.

17. The Society also suggests that we remove "any other signing device" from clause 8 of the Amendment Bill. This clause was included to cater for future technological development, such that when there is some signing device other than electronic signature and password, which attains the same level of security, the legislation would not have to be amended. We note the Society's and Members' concern about the uncertainty this clause could give rise to. Having reviewed our position, we are prepared to move a Committee Stage Amendment to delete this clause.

18. We hope our position as set out above would help allay any concern Members may have about the drafting of the Bill. We look forward to Members' support of the Amendment Bill.

Yours sincerely,

(Miss Erica Ng)
for Secretary for the Treasury

Encl.

c.c. Members of the LegCo Panel on Financial Affairs

Internal

CIR (Attn: Mrs Alice Lau Mak Yee-ming)
SITB (Attn: Miss Adeline Wong)
D of J (Attn: Mr MY Cheung)
Law Draftsman (Attn: Ms Lonnie Ng)

Annex

Telefiling Process

(i) First, the taxpayer has to enter his Taxpayer identification Number (TIN). With this TIN, the telefiling system will check whether there is any outstanding tax return for the taxpayer before he is allowed to proceed further.

(ii) Then, the taxpayer will be asked to state the details of his income and claim for allowances for the relevant year of assessment. During this process, the system will also check whether the taxpayer's return is acceptable to be filed through telephone. If the taxpayer's information indicates that he does not fulfill the criteria (for example the taxpayer has income from business), the system will advise the taxpayer that his return is not suitable for telefiling.

(iii) After the taxpayer has inputted the required information, the system will repeat the relevant tax return data again for the taxpayer's confirmation. The taxpayer can amend the data if necessary.

(iv) If the taxpayer confirms that the information is in order, he will then be required to since the tax return by inputting his password.

(v) After verifying the taxpayer's password, the system will generate an Acknowledgement Reference Number to acknowledge that the return has been received. The taxpayer is advised to jot down this Number on the Tax Record Sheet, which can serve as an acknowledgement of receipt by IRD. This Number will also facilitate the taxpayer in case he wishes to obtain a copy of the return data as he would do in the case of a paper return.

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)

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

Appendix V

Proposals

Legal recognition' of other forms of electronic signatures

6. The ETO addresses the concerns in electronic transactions by giving legal recognition to electronic records and digital signatures[2] supported by recognized certificates. We encourage Government bureaux and departments to review whether signature requirement in law under their portfolio can be removed in order to facilitate electronic transactions. But for those cases where the signature requirement has to be maintained, it is timely now to consider whether legal recognition should be extended to cover other forms of electronic signatures[3], in addition to digital signature, in order to stimulate e-business development.

7. Different electronic authentication technologies and means have been developed and adopted by governments and business communities around

---

[2] Under the ETO, a "digital signature" means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine whether the transformation was generated using the private key that corresponds to the signer's public key, and whether the initial electronic record has been altered since the transformation was generated.

[3] Under the ETO, an "electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purpose of authenticating or approving the electronic record. Digital signature is one form of electronic signatures.

the world. To give the public a wider choice and to facilitate e-business and E-government development, we should examine whether legal recognition should be given to other means of electronic authentication.

8. The use of personal identification number (PIN) is an authentication means which should be examined for recognition under the ETO. It is commonly used in banking transactions nowadays as well as in some E-government transactions overseas, e.g. filing of tax return in Australia, Singapore, the UK and the USA, renewal of driving licences in some states in the USA, etc. It is convenient to users as they do not have to rely on other tools or devices to identify themselves electronically. The use of PIN for authentication has been widely tested in various types of market applications. With proper management, it can be considered for acceptance as a form of electronic signatures for satisfying the signature requirement under law in specified cases[4] where the level of security offered by it is commensurate with the risk of the service involved, e.g. where there is already established relationship between the parties involved so that the PIN could be securely issued, used and verified; and where a secure system like the Electronic Service Delivery Scheme which provides strong encryption services for data transmission is used for making the electronic transaction. The use of PIN should be provided as an option in addition to the use of digital signature and hand-written signature. It should be up to individual users to opt for the means which suits them best. **We, therefore, consider that there is a case for the ETO to be amended and a new schedule added so that the Secretary for Information Technology and Broadcasting (the Secretary) may, by subsidiary legislation, specify in the new schedule legal provisions under which the use of PIN will be accepted for satisfying the signature requirement.** What provisions will eventually be included in the schedule will be subject to normal legislative procedure.

9. We have also considered other means of authentication like using biometrics. While these means may be sound technologically and have been deployed in internal applications of some organisations, there is currently no institutional arrangement in place which can support their application on a community-wide basis. It is not anticipated that an independent and trusted

---

[4] The Inland Revenue (Amendment)(No. 2) Bill 2001 has been introduced into the Legislative Council which, inter alia, provides that a password can be used for authentication and fulfillment of signature requirement for tax returns filed to the Inland Revenue Department under the Inland Revenue Ordinance (Cap. 112).

third party which collects the biometrics of subscribers on a community-wide basis for the purpose of authenticating the identity of the subscribers in electronic transactions would emerge in the short future. Nor would this be a situation which has already gained wide acceptance in the community. Moreover, few parties in the community (including Government departments) may now have the technical capability to deal with biometrics of outside parties for the purpose of authentication in electronic transactions on a communitywide basis. **We, therefore, consider that other means of authentication including biometrics should be examined at a later stage when they become more mature, and when related institutional support emerges in the market.**