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.