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