

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