LC Paper No. CB(2) 310/02-03(01)

Bills Committee on Inland Revenue (Amendment) (No. 2) Bill 2001

Administration's Response to Issues Raised at the Bills Committee Meeting on 23 October 2002

Introduction

At the second meeting of the Bills Committee held on 23 October 2002, the Administration was requested to provide the following information -

(a) scope of the current review of the ETO and the proposed Electronic Transactions (Amendment) Bill, e.g. whether it covered the use of a personal identification number (PIN) for authentication;

(b) the Commerce, Industry and Technology Bureau (CITB) to explain at the meeting of the Panel on Information Technology and Broadcasting on 7 November 2002 -

  (i) the interface of the Inland Revenue (Amendment) (No. 2) Bill 2001 (the Bill) with the ETO; and

  (ii) the experience of overseas jurisdictions where PIN was used for authentication of documents filed with the government, e.g. whether any difficulties were encountered in meeting the security requirements;

(c) examples of "reasonable excuse" as a defence against the imposition of criminal responsibility for an incorrect tax return filed using a password, given the vulnerability of a password-based system ;

(d) statistics on the use of digital signature in submitting tax returns, and the estimated number of taxpayers who would file tax returns by telephone ;

(e) the costs and benefits of providing a telefiling system for tax returns, e.g. the amounts of capital investment and recurrent costs ;

(f) the plans for public education and publicity to increase public awareness of the proposed new means of submitting tax returns by telephone, and the differences in the level of security between using PIN and digital signature for filing tax returns ;

(g) a comparison between using contract law and the Bill to authenticate the use of passwords ; and

(h) the reasons for suspending the tax e-filing system from May to July 2002 in the UK.

2. The following paragraphs set out the Administration's response.

Scope of the ETO review and the proposed ETO (Amendment) Bill

3. The major issues examined in the ETO review include –

(a) whether, in addition to digital signature, legal recognition should be extended to cover other forms of electronic signature, including PIN;

(b) whether the requirement of "delivery by post or in person" under certain specified legal provisions should be construed as covering "delivery by electronic means" as well;

(c) withdrawal of certain exemptions from the application of the ETO; and

(d) the operation of the voluntary recognition scheme for certification authorities.

4. Regarding item (a) above, CITB proposed in the public consultation paper published in March this year to accept PIN as a form of electronic signature to satisfy the signature requirement under law in specified cases where the level of security offered by it is commensurate with the risk of the service involved. To give this legal effect, CITB proposed in the consultation paper to amend the ETO and add a new schedule so that the Secretary for Commerce, Industry and Technology may, by subsidiary legislation, specify in the new schedule legal provisions with signature requirement for which the use of PIN would be accepted as satisfying the signature requirement.

5. While some respondents supported this proposal, many were opposed to or had reservations about it. Some expressed concern about the security level offered by PIN, as it is less secure than digital signature and is a shared secret between the user and the application/service provider. They also considered that the proposed recognition of PIN would weaken the incentive for the public to adopt digital signature, and the introduction of less secure alternatives would reduce the public's confidence in electronic transactions. Some further suggested that PIN could not satisfy the non-repudiation function expected of a signature, which digital signature could.

6. While CITB remains of the view that PIN should be introduced for services

where the level of security offered by it is commensurate with the risk of the services involved so that users may have a wider choice, having considered the comments received during the public consultation CITB is of the view that there may not be a case to make a general and sweeping amendment to the ETO for the purpose. The Administration should make specific amendments to relevant legislation so that the implications of each amendment can be fully examined by the Legislative Council and the community.

7. The telefiling proposal under discussion is a good example of the type of service where the introduction of PIN would widen user choice and upgrade the Government's service to the public while at the same time, the level of security offered by it is commensurate with the risk of the service involved. The Administration is of the view that the specific legislation, i.e. the Inland Revenue Ordinance, should be amended to enable the provision of the service.

Interface of the Bill with the ETO and experience of overseas jurisdictions on using PIN for authentication in government services

8. As requested by the Bills Committee, CITB has explained the issues set out in paragraph 1(b) above at the meeting of the Panel on Information Technology and Broadcasting on 7 November, 2002.

Examples of "reasonable excuse" for incorrect tax return filed using password

9. There would be cases in which, having regard to all the relevant circumstances and the available evidence, it is doubtful whether the incorrect tax return was filed by the taxpayer. In such cases, the benefit of the doubt would be given to the taxpayer. A few examples of such cases are given below –

(a) The records of the Inland Revenue Department (IRD) show that the taxpayer has already reported to IRD that his password might have been inadvertently disclosed to a third party, and such report was made before or shortly after the incorrect return was filed to IRD.

(b) The taxpayer, having received the tax return for the year, did not complete the return but finds that an incorrect return had been submitted allegedly by him, e.g. upon receiving the tax assessment. He immediately raised the matter with IRD.

(c) Two tax returns for the same year were received by IRD, one of which was the incorrect return.

Statistics on the Use of Digital Signatures in Submitting Tax Returns

10. The use of digital signature in submitting tax returns was launched in January 2001 through the Electronic Service Delivery (ESD) platform. Few returns were filed using this means during the period to March 2001. For the year ended 31 March 2002, some 2,300 returns out of a total of 2.2 million eligible returns were filed by such means while the figure for the period from 1 April 2002 to 31 October 2002 was about 1,900.

Expected Take Up Rate for Telefiling

11. 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 high. Nevertheless, we expect the rate to increase gradually over time (perhaps up to 5% in the longer term). As a reference point, the telefiling take-up rates in other tax jurisdictions range between 3% and 9% for the year 2000, i.e. 4.1% for USA (launched in 1992), 2.9% for Canada (launched in 1998) and 8.5% for Singapore (launched in 1995).

Cost and Benefits of Providing the Telefiling System

12. The total cost of implementing the telefiling system 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 for manual filing and data input. Besides staff saving, the proposed telefiling system will also bring forth intangible benefits such as instant data validation and transmission, as well as providing taxpayers with another convenient option for filing tax returns.

Publicity Plan

13. IRD will launch widespread publicity to promote the new electronic filing service upon enactment of the legislation. Publicity items would include, among others, the issue of publicity leaflets, advertisement in newspapers, and announcement on television and radio. The publicity leaflets will set out the eligibility criteria for furnishing the different types of returns, and will draw taxpayers' attention to the difference in the level of security between using PIN and digital signature for filing tax returns. Taxpayers will also be advised that they have the choice of filing a paper return or an electronic return. The leaflets will be sent to all taxpayers along with the Tax Returns for Individuals and Property Tax Returns.

Contract Law versus Legislation

14. In the private sector, passwords are being used to authenticate the identity of

the contracting parties in transactions between them upon their mutual agreement. Both parties are bound by the terms of the agreement to which the law of contract applies. However, such transactions are invariably matters which are civil in nature.

15. In the context of return filing, apart from identifying himself by the use of a password, a taxpayer has to shoulder the legal consequences of filing any incorrect return which is criminal in nature. In the absence of statutory authority, the Commissioner has no power to impose criminal liability on a taxpayer, by mutual agreement or otherwise. Therefore, it is necessary to introduce a statutory provision to provide a legal basis for accepting the use of passwords as satisfying the signature requirement in furnishing a tax return, so that criminal sanctions would flow from the filing of an incorrect return.

The UK Incident

16. The UK Inland Revenue shut down its Internet Service for Self-Assessment (SA Online) on 27 May 2002 following reports from some customers that they had seen information relating to other persons. Nevertheless, the cause of the incident was identified and the service resumed after 1 month on 28 June 2002.

17. According to the UK Inland Revenue, the incident was a system fault due to a combination of internal and external factors (the UK Revenue's statement is at Annex A). The problem lies with the way in which the Internet "session cookie" identifying the user was managed and it could, in certain rare circumstances, be presented to another user. That is how some users saw information relating to another person.

18. We have made further enquiries to the UK Inland Revenue on the cause of the incident and its implications. In their most recent response, they confirmed that (i) the security incident referred to was the result of a combination of unusual circumstances; (ii) none of those circumstances were relevant to the use of PIN/password as the authentication/signing token; and (iii) they have never had any security or confidentiality problems from the use of PIN/password.

19. In Hong Kong, IRD's tax filing application under the ESD system is of a different design. No user application data including passwords will be stored in the session cookies and the data will be end to end encrypted. Only IRD has the decryption key for access to the data. Thus, the UK incident should not be repeated in the Hong Kong tax filing system.

Financial Services and the Treasury Bureau
November 2002

SA Online

We are pleased to announce that the SA Online service (the electronic tax return provided by us) is now available again. The service was temporarily withdrawn on 27 May following reports from some customers that they had seen information relating to another person. The Internet filing service itself has remained available throughout and we have continued to receive returns from customers using alternative electronic tax returns

Confidentiality of customer information is of paramount importance to us and that is why we withdrew the service pending a thorough investigation. We have now completed that investigation.

We have been able to identify the precise causes of this regrettable incident, which was a combination of internal and external factors. The way in which the "session cookie" identifying the user was managed meant that it could, in certain rare circumstances, be presented to another user. That is how some users saw information relating to another person. Our identification of the causes has been verified by independent Internet security experts and they have also endorsed the changes we have made to ensure it does not happen again. As we withdrew only the SA Online service there have been suggestions that EzGov, who produce the SA Online form for us, must have been at fault. We wish to make it clear that EzGov were not at fault in any way.

We want to provide reassurance to all our customers so we have also undertaken a comprehensive examination of the logs which record all the activity on our Internet filing service to be sure we identified any customers who may have been affected. That is one reason it has taken some time to restore the SA Online service. We are now able to say that for 27,967 of the SA Online users since 6 April we can eliminate the possibility that another person saw their information. However, there are 47 users where the entries in our logs suggest that another person may have seen their information. In addition, there are 665 users where, although it is unlikely their information was seen by anyone else, we cannot completely eliminate the possibility. We are writing to all those who may have been affected to apologise and explain what we are doing.

We very much regret this incident. Although the number of people known to have been affected is small and the information seen was generally very limited, we place the highest importance on protecting the confidentiality of customer information.

We hope our thorough and independently endorsed investigation will give our customers confidence

about using the service in future.

Home **Top** | **Menu**