LC Paper No. CB(2) 172/02-03(01)

Bills Committee on Inland Revenue (Amendment) (No. 2) Bill 2001
Administration's Response to
Summary of concerns raised in submissions
(As at 22 October 2002)

Organisation	Concern	Administration's Response
1. Hongkong Post [LC Paper No. CB(2) 4/02-03(02)]	- do not have any comments on the provision of necessary legal framework for the use of passwords and telephones in furnishing tax returns - has provided the charges for digital certificates issued by Hongkong Post Certificate Authority	- Noted.
2. Office of the Privacy Commissioner for Personal Data [LC Paper No. CB(2) 4/02-03(03)]	- suggests that the proposed arrangement should include adequate safeguards for the data transmitted	- IRD will adopt tight technical and administrative measures to ensure the security and confidentiality of the returns data submitted with the use of password.
3. Information Security and Forensics Society [LC Paper No. CB(2) 4/02-03(04)]	- does not support the proposed amendment in the Bill, although the proposal is on the right track - considers that the use of password, Taxpayer Identification Number (TIN) and Personal Identification Number (PIN) in the proposed tax return system was not securely designed. TIN and PIN can only achieve the purpose	- Noted. - Non-repudiation is always one of IRD's major concerns. The overall design of our return filing system must ensure that the electronic records will be handled in such a way that the principle of non-repudiation can be invoked and demonstrated.

	of identification and authentication, but not non-repudiation. Passwords on the encrypted file can be retrieved with the possession of the encryption key	- For the purpose, IRD will adopt tight system and administrative control measures to protect electronic records from unauthorized access, including – – registration mechanism; – allotment of Taxpayer Identification Number (TIN) and Access Code, issued by separate notices; – self-selected password to ensure only the taxpayer himself knows the password; – access control features to restrict the use of system to authorized users; – all access and transactions are logged for security control and audit trail; – users are reminded to keep strict confidentiality of their passwords; - IRD will not use the password alone to achieve non-repudiation. Non-repudiation would be addressed in the following manner - – A person joining IRD's electronic filing services shall keep his password confidential. This is an express condition under the "Terms and Conditions for use of password" to which the user must agree before he is allowed to use the services. – By virtue of the proposed s.2(5) and existing s.51(5) of the IRO, a person signing a return with his password electronically shall be deemed to be cognizant of the contents thereof unless the contrary is proved. – In lawsuits, IRD will seek to establish to the Court that the taxpayer has used his password to furnish an electronic return and that these details have not been tampered with

		according to its internal control and administrative measures. The Court will then decide whether or not it accepts that the non-repudiation averred should be accepted or rejected.
	- <u>suggests</u> defining clearly in the Bill the process of furnishing tax return with the use of digital certificates, password or any other signing device	- Specifications of technical details in furnishing electronic records for tax return filing purpose have been catered for in the Bill. Clause 8 of the Bill empowers the Commissioner to specify by notice in Gazette the technical details for the form and manner of furnishing an electronic record for tax filing purpose and how the tax return signature is to be affixed to the return. The Commissioner will set out these details by notice in Gazette after the Bill is enacted. (Please refer to the draft details in Annex A & B of the Information Paper for Bills Committee).
4. Professional Information Security Association [LC Paper No. CB(2) 4/02-03(05)]	– <u>considers</u> that: (a) the Electronic Transactions Ordinance (ETO) recognizes digital signature as the <u>only</u> proven technology that satisfied the authentication and security requirements. The Government should not try to bypass ETO to use another technology option like PIN, before the ETO is revised	- The ETO stipulates that, if a rule of law requires the signature of a person, a digital signature supported by a recognised digital certificate issued by a certification authority recognised under the ETO satisfies the requirement. Nevertheless, section 14 of the ETO provides that if an Ordinance permits or requires **the authentication of information by an electronic signature** for the purposes of that Ordinance 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. There is thus no question of the Inland Revenue (Amendment) (No.2) Bill 2001 bypassing the ETO. - The ETO is a generic legal framework with the aim of facilitating the use of electronic transactions. However, we have not ruled out that there may be circumstances where provisions for electronic transactions could be set out in specific

		legislation.
	(b) PIN is less secure than digital signature, and cannot fulfil the requirement of non-repudiation. PIN-based system is not suitable for Inland Revenue Department (IRD) Tax Return Filing System. IRD should continue to use digital signature for tax returns	- Whether password-based system is sufficiently secure or not in individual cases depends very much on the risk involved in the application and whether the security offered by the system is commensurate with the risk concerned. We consider that with the proposed system security design and administrative measures, a password can be accepted as sufficiently secure for the tax return filing purpose.
	(c) Telephone filing is not realistic. Taxpayers would rather fill in a paper form, if they would have to fill in a Telefiling record sheet	- Telefiling service provides additional benefits like data validation and instant transmission. Besides, it avoids paper handling and possible postal delay. - Telefiling has been proved acceptable in other tax jurisdictions like USA, Canada and Singapore since the early nineties. Some 5 million US taxpayers filed their return through telephone in the year 2000.
	- <u>concerns</u> about the implementation of the e-filing system, e.g. the RC4 encryption algorithm adopted by IRD is vulnerable to attacks and there are severe security and management problems with a PIN-based system	- All stored passwords are encrypted using strong encryption algorithm. The encryption key consists of 16-digits half of which is specified separately by each of the two Deputy Commissioners of Inland Revenue. - The technical design of IRD's system will ensure that the password database can only be accessed by the login program of the system but the Deputy Commissioners do not have access to the login program. Therefore, even though the Deputy Commissioners combined can have knowledge of the encryption key, they cannot retrieve the passwords. No single person at all in the IRD can retrieve the passwords. - There is also a further access control feature in the system. In

		the event that the number of unsuccessful attempts to gain access to a record with incorrect password exceeds five, the relevant password will be revoked, thus barring any further attacks on the system. - There is strict security policy requiring the encryption key to be changed from time to time. Besides, all access will be logged for security control and audit trail purposes. IRD will conduct a daily review of the transactions logged to ensure that all transactions have been properly authorized.
	- concerns about the operational limits of the system, i.e. to handle huge volume of submissions before the deadline	- Sufficient capacity will be provided to handle the peak submission volume. - IRD will closely monitor the usage rate and the system capacity after the service is launched. The systems will be scalable and can be expanded if circumstances required. - In the event of system failure or long delays / unavailability leading to returns being received beyond the deadlines, the Commissioner may exercise her discretion to extend the return filing deadline.
	- proposes establishing an authority to develop and adopt security assessment for government services in the event that the ETO review considers PIN a acceptable technology	- The Commerce, Industry and Technology Bureau (CITB) has received similar comments during the public consultation on the review of the ETO. CITB will look into this proposal in the context of the ETO review, if the proposal to accept PIN as a form of electronic signature as satisfying signature requirement under law in specified cases is to be pursued.
5. Hong Kong Society of Accountants	- supports in principle IRD's initiative to encourage greater use of electronic services	- Noted and welcomed.

[LC Paper No. CB(2) 4/02-03(06)]	- <u>expresses concerns</u> about the following : (a) interface of the Bill with ETO; (b) the lack of specific legal backing for adopting methods of authentication other than digital certificates;	- See reply to para. 4(a). - The purpose of the Bill is not to give a password the same status as digital signature in all situations or extend the possible methodologies for effecting e-transactions in a general way. It merely allows the use of a password as **an alternative means** of authentication and to satisfy the signature requirement for return filing purpose. Taxpayers can determine themselves whether the password option should be used, or whether the digital signature or physical option should be adopted. - CITB, which is the policy bureau for the promotion of e-business in Hong Kong and for the operation of the ETO, supports this proposal.
	(c) given the inherent vulnerability of a system based on passwords rather than digital certificates, the proposal to treat the submission of a tax return through the use of a password as the legal equivalent of signing a return will put users of the system at a disadvantage; and	- It is not possible for IRD to haphazardly enforce the penal provisions under the IRO. Section 80(2) of the IRO provides that any person, who without "reasonable excuse" makes an incorrect return, commits an offence. A penalty, whether levied by the Courts, or whether imposed by the Commissioner in the form of additional tax under Section 82A is only applicable if the taxpayer has no "reasonable excuse". If the case is to be prosecuted, clear evidence is required from IRD to prove beyond reasonable doubt that the taxpayer had the intent to make an incorrect return or, as the case may be, the "wilful intent to evade tax". The standard of proof required is obviously very high. - In doubtful cases, the taxpayer will be given the benefit of the doubt under our legal system. IRD never prosecutes a taxpayer simply because the filed data are prima facie incorrect.

		- If a taxpayer is not comfortable with the filing of a return electronically using a password, he can simply choose to file the paper return.
	(d) the references in the Bill to the CIR "approving" a password is inappropriate and these should be reviewed	- The approval processes in setting up a password involve the selection of numbers by the taxpayer that conform to requirements prescribed by the Commissioner as well as the successful transmission, verification, validation and recording of the selected numbers in IRD's computer system. The Bill has collectively embodied all processes as "approved by the Commissioner". We consider these wordings adequate and appropriate.
6. Information Systems Audit and Control Association (Hong Kong Chapter) [LC Paper No. CB(2) 4/02-03(07)]	– supports in principle the proposals made in the Bill	- Noted and welcomed.
	– mainly concerns about the security controls of the proposed electronic transaction mechanism, specifically the proposed use of password	
	– considers :	
	(a) the question of whether the means of authentication chosen is adequate should be assessed separately from the method used to protect data during transmission;	- Agreed. Given the tight security and administrative measures in the proposed system (see response at 3rd bullet in item 3 above for details), the use of password for the purpose of return filing is adequate.
	(b) the use of password, though widely adopted, does not imply that it is good practice, and hence constant review of security needs of a system should be carried out; and	- Agreed. IRD attaches great importance to IT security policy and has established strict guidelines and procedures for information and data handling. An information security risk assessment for IRD conducted by an independent consultant was completed in February 2002. Periodic security assessment and

		review by independent party will also be conducted to ensure the effectiveness of the security measures and to keep abreast of the technology development.
		- Using a password for electronic filing of a tax return will be implemented as one of the ESD applications. The ESD scheme has satisfactorily passed through an independent security audit before its launch. Security audit will be conducted periodically by independent consultants. IRD will undertake all necessary periodic security review to cover its systems that handle submission of tax return using PIN in addition to the ESD.
	(c) the implications of failure or long delay of telephone network in handling the transaction volume.	- See remarks to the same concern raised by Professional Information Security Association.
	- <u>suggests</u> adopting a system generated encryption key, rather than a manually selected key and regular security review by an independent third party	- Even though the 16-digit encryption key is manually selected, the key has been specified by the two Deputy Commissioners separately. This administrative measure should be able to achieve a comparable level of security as offered by a system generated key.
	- <u>proposes</u> the following amendments to the Bill :	
	(a) to spell out more clearly the definition of "password" (clause 2);	- See remarks to item (d) of concerns raised by Hong Kong Society of Accountants.
	(b) to replace "signing device" and "affixed" by "means of authentication" and "used to authenticate" respectively in the relevant provisions (clause 8(6));	- We understand that the concern on the proposed terminology of “affixed” is to restrict the use of password for authentication purpose only. However, the Adminstration’s 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 IRO 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 the Administration's policy intention and fulfill the functions mentioned above, we consider it appropriate to retain the word "affix".
	(c) to prescribe the password policies and standards in the Bill (clause 8(7)); and	- For the time being, the password is simply any combination of 6 numerics chosen by the taxpayer which is then validated, recorded and approved by the Commissioner. It is not necessary to prescribe the password policies and standards in the Bill.
	(d) to state clearly the presumption that, in the absence of evidence to the contrary, the receiving party has the right to accept the message as proof of the other party's authorisation, i.e. along the line of the provisions in Schedule 1 to the Import and Export Ordinance [Cap. 60].	- The stated presumption is clear. The proposed s.2(5) would extend a reference to the act of signing a return to that of adopting a password to a return. Thus, the person signing a return electronically by means of his password shall be deemed to be cognizant of the contents thereof, i.e. he shall be taken as having authorized the submission of the return, unless the contrary is proved.
7. Digi-Sign Certification Services Limited [LC Paper No. CB(2) 70/02-03(01)]	– <u>considers</u> (a) the use of PIN's to satisfy the signature requirement would depend on proper management and the use of a secure system; and	- Agreed. IRD will adopt tight technical and administrative measures to ensure the security and confidentiality of the returns data submitted with the use of password.

	(b) the Government should focus on the promotion of Public Key Infrastructure, and leave the use of PIN's for satisfying the signature requirement as a contractual matter between the PIN user and the relying party	- The Government will continue to promote the Public Key Infrastructure. - The use of PIN cannot be left as merely a contractual matter. This is because legal amendment is required to deem the adoption of the password as constituting a signature for the purposes of the IRO so that legal consequences would ensue.