Bills Committee on Inland Revenue (Amendment) (No. 2) Bill 2001
Summary of concerns raised in submissions

(As at 16 October 2002)

Organisation	Concern	Remarks
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	
2. Office of the Privacy Commissioner for Persona Data [LC Paper No. CB(2) 4/02-03(03)]	- suggests that the proposed arrangement should include adequate safeguards for the data transmitted	
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 of identification and authentication, but not non-repudiation. Passwords on the encrypted file can be retrieved with the possession of the encryption key - suggests defining clearly in the Bill the process of furnishing tax return with the use of digital certificates, password or any other signing device	

4. Professional Information Security Association [LC Paper No. CB(2) 4/02-03(05)]	- considers that : (a) the Electronic Transactions Ordinance (ETO) recognises digital signature as the only 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 (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 (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 - concerns 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 - concerns about the operational limits of the system, i.e. to handle a huge volume of submissions before the 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	

5. Hong Kong Society of Accountants [LC Paper No. CB(2) 4/02-03(06)]	- supports in principle IRD's initiative to encourage greater use of electronic services - expresses concerns 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; (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 (d) the references in the Bill to the CIR "approving" a password is inappropriate and these should be reviewed	HKSA's letter dated 4 January 2002 to the Commissioner of Inland Revenue (CIR) concerning the proposals in the Bill is attached to its submission. CIR's reply is at LC Paper No. CB(1) 805/01-02(02)
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 - 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;	

	(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 (c) the implications of failure or long delay of telephone network in handling the transaction volume. - <u>suggests</u> adopting a system generating encryption key, rather than a manually selected key and regular security review by an independent third party - <u>proposes</u> the following amendments to the Bill : (a) to spell out more clearly the definition of "password" (clause 2); (b) to replace "signing device" and "affixed" by "means of authentication" and "used to authenticate" respectively in the relevant provisions (clause 8(6)); (c) to prescribe the password policies and standards in the Bill (clause 8(7)); and (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.	

7. Digi-Sign Certification Services Limited [LC Paper No. CB(2) 70/02-03(01)]	- considers : (a) the use of PIN's to satisfy the signature requirement would depend on proper management and the use of a secure system; and (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	

Council Business Division 2
Legislative Council Secretariat
17 October 2002