



Mrs. Carrie Yau
Secretary for Information Technology and Broadcasting
2/F Murray Building
Garden Road
Hong Kong

April 30, 2002

Dear Mrs. Yau,

Comment on the Review of the Electronic Transaction Ordinance (Cap. 533)

Professional Information Security Association (PISA) is a not-for-profit organization for local information security professionals. We concern about the development of information security of Hong Kong. We have witnessed the development of a more secure platform in electronic transaction after the publishing of the ETO in year 2000. We have noted and appreciate the effort of the HKSAR Government in moving towards the electronic Government. We would like to state that system security and public trust are still major considerations for success of this direction. We as well would like to express our opinions on the Electronic Transaction Ordinance (ETO) Review.

The major concern of PISA in the ETO Review falls on the legal recognition of personal identification number (PIN) as a form satisfying the signature requirement. While we are positive to the proposal to allow the use of PIN in some less sensitive application system to promote the concept of electronic submission and paperless registration to government service, we have reservation in the way PIN is recognized legally as equivalent to digital signature.

PIN cannot be used to sign an electronic document as a digital signature

In the current ETO 2000, digital signature which is based on the public key infrastructure, is recognized as the only one proven technology among other known electronic signatures that satisfies the requirements of authentication, confidentiality, integrity and non-repudiation. This understanding had been reconfirmed in the several replies of the government to the public during the consultation of



the ETO in 2000.

The current proposal in the ETO review clearly indicates the government has made a change of policy. However, there is no clear justification in the consultation document for such move. Are there any study or survey, or change of technology that caused the Government to make a conclusion that PIN once could not be accepted in satisfying the signature requirement, now can meet the requirement?

In our view, PIN cannot be used to sign a document as what the digital signature or manuscript signature can do. Firstly, the fact that PIN cannot provide non-repudiation has been well established in the theory of cryptography. PIN is weak enough to be reproduced by all kinds of password cracking and social engineering attacks, and then be used right away. It is only “something you know” while digital signature provides “something you have” in addition to its strength against reproduction. Secondly, unlike digital signature based systems which bases on the asymmetric key pairs, for the PIN-based systems, the service provider is keeping a copy of the PIN stored in either encrypted or unencrypted form. When there is a legal dispute, the non-repudiation of the transaction is in doubt.

Users must be clearly told the risks of adopting PIN

Users adopting PIN and digital or manuscript signature have to bear very different levels of security risk. If any PIN based system is installed, users must be informed of the risk induced and they have to accept the risk in order to enter the system, and that users must be given alternatives to work with the system other than using PIN. The notice must be clearly stated in visual or audio form and bear the language of the users’ choice.

The Review does not address the infrastructure provision for the coexistence of PIN based and PKI based systems.

In the current ETO 2000, digital signature is the only accepted technology so everything is clear-cut. In the ETO Review, however, the government is proposing a coexistence of both digital signature



based and PIN based systems. In the proposal, we cannot find any paragraph mentioning the approach to deal with such coexistence. Without this, the public would get confused with the applicability of each type of technology to various types of e-Business.

How does the government identify to the public the difference of risk associated with PIN based and Digital Signature based systems, so as not to mislead un-educated business users or un-concerned business people to use system of inappropriate level of security (because of easier cost justification or other reason) to cause fraud and distrust to e-Business. Would the government publish guidelines and process for the risk assessment for governmental application services to apply technology of appropriate security level? Would there be a party to carry out or approve the validity of the risk assessment, or the government would let each department justify by their own without monitoring? Would the government propose a workable risk assessment model for business or let it run in unregulated mode?

We appreciate your attention to the above opinions and look forward to your reply and clarification. We also think that a face-to-face meeting can facilitate the communication to clarify our concerns. Please contact me at telephone 8104-6800 or email: sc.leung@pisa.org.hk.

Yours faithfully,

Mr. LEUNG Siu Cheong
Chairperson
Professional Information Security Association

Cc: Legislative Councillors