Letter from
the Hon. Sin Chung-kai dated 3 December 1999

Introduction

This paper addresses the issues raised by the Hon. Sin Chung-kai in his letter to the Administration dated 3 December 1999.

Mechanism for Appeal

2. Clause 27 of the Electronic Transactions Bill stipulates that the Secretary for Information Technology and Broadcasting (the Secretary) may confirm, vary or reverse the decision of the Director of Information Technology Services (the Director) under Clauses 20, 21, 22, 23 or 26 of the Bill with regard to a certification authority upon appeal. We consider the proposed arrangements for handling appeals appropriate for the following reasons :

(a) the Secretary is not involved in any way in the Director's decision making process. In considering an appeal, the Secretary will act in an entirely impartial manner, taking account of all relevant factors. The appellant will receive a fair hearing and the Secretary will consider the case strictly on merits;

(b) the decision of the Secretary on appeal is subject to judicial review. This would safeguard the interest of the concerned certification authority;

(c) there is a need to arrive at a decision on the appeal expeditiously in the interest of the certification authority concerned, the subscribers and other parties who may rely on the recognised certificates issued by the certification authority concerned; and

(d) we have undertaken to review the operation of the Electronic Transactions Ordinance 18 months after its enactment in the light of operational experience. We recommend that our proposed appeal mechanism be

adopted and be reviewed as part of this broader review exercise.

Advisory Committee on Code of Practice for Recognised Certification Authorities

3. The Director will set up an advisory committee to oversee the implementation of the code of practice for recognised certification authorities. The proposed terms of reference and membership of the advisory committee are set out in the Annex. We shall establish the advisory committee after the enactment of the Bill and shall review the consultation mechanism for the code of practice 18 months after the enactment of the Bill.

Responsibility of a Revoked Certification Authority

4. Under Clause 38A of the Bill, a recognised certification authority must maintain or cause to be maintained an on-line and publicly accessible repository. Under Clause 27C of the Bill, the Director has to give notice about the revocation or suspension of a recognition of a certification authority in the relevant certification authority disclosure record maintained for that certification authority.

5. In accordance with the draft code of practice for recognised certification authorities, a recognised certification authority has to contain in its repository its certification authority disclosure record. Therefore, its clients will be able to obtain information about the suspension or revocation of the recognition of that certification authority either through the certification authority disclosure record maintained by the Director or through the disclosure record contained in the repository of that certification authority.

6. Separately, we have also stipulated in the code of practice that a recognised certification authority has to publish in its repository notices of the suspension, revocation or non-renewal of the recognition granted by the Director.

7. Clause 43 of the Bill further stipulates that it is an offence to make a false claim that a person is a recognised certification authority.

8. There are thus adequate provisions to require the recognised certification authority to notify its clients of the suspension or revocation of its recognition. We, therefore, do not consider that there is a need to make further stipulations in this regard in the Bill.

Disclosure Record

9. The certification authority disclosure record to be maintained by the Director under Clause 27B of the Bill for each recognised certification authority will contain the following information -

(a) the name and contact details of the certification authority;

(b) the validity period of the recognition granted to the certification authority by the Director under Clause 20(5)(b) of the Bill and conditions, if any, attached by the Director to the recognition under Clause 20(5)(a) of the Bill;

(c) the particular certificate, or types, classes or description of certificates issued by the certification authority that are recognised by the Director;

(d) the certificate of the certification authority itself which contains its own public key;

(e) the location of the certification authority's certification practice statements and the method for them to be accessed;

(f) various notices to be given by the Director under Clause 27C of the Bill, such as those relating to the revocation, suspension or reinstatement after suspension of the recognition granted to the certification authority;

(g) the date and material information of the assessment reports which the certification authority has to furnish to the Director under Clause 37 of the Bill;

(h) details of any incidents which the certification authority has notified the Director and which have material effect on the ability of the certification authority to operate in a trustworthy manner or on the validity or reliability of the recognised certificates issued by that certification authority; and

(i) any other relevant information concerning the certification authority which the Director considers appropriate to be disclosed so as to maintain the integrity of and public confidence in the voluntary recognition scheme.

Given the long list of information to be contained in the disclosure record and the need for some flexibility for the Director, we do not propose to enumerate in the Bill the entire list of information to be contained in the disclosure record to be maintained by the Director for individual recognised certification authorities.

Information Technology and Broadcasting Bureau
December 1999

Annex

Advisory Committee on Code of Practice for Recognised Certification Authorities

Proposed Terms of Reference

To advise the Director of Information Technology Services on matters relating to the code of practice for recognised certification authorities issued under the Electronic Translations Ordinance, in particular in respect of -

(1) the review of the principles, technical standards and procedures set out in the code of practice for the operation of recognised certification authorities to take account of operational experience as well as technological and other relevant developments;

(2) the consideration of amendments to the code of practice in the light of the outcome of the review referred to in (1) above and the related consultation arrangements; and

(3) any other matters which are conducive to improving the operation of the voluntary recognition scheme for certification authorities in Hong Kong.

Tentative Membership

Chairman

Director of Information Technology Services

Members

A Legislative Councillor

Selected representative(s) of recognised certification authorities

Selected representative(s) of business users of certification services

Selected representative(s) from the related professions (IT, legal, accounting, etc.)

Selected representative(s) from academic institutions

Selected representative(s) from other related bodies (e.g. Office of the Privacy Commissioner for Personal Data)

Representative of Information Technology and Broadcasting Bureau