

**Proposed Amendment to  
Guidance Note on Compliance Assessment of Certification Authorities  
regarding the Assessment of the Management of Liabilities  
by a Certification Authority**

**Introduction**

This paper briefs Members on a proposed amendment to the Guidance Note on Compliance Assessment of Certification Authorities in respect of the assessment of the management of liabilities by a certification authority (CA).

**Background**

2. Section 21(4) of the Electronic Transactions Ordinance (Cap. 553) (ETO) sets out the matters that the Director of Information Technology Services (the Director) shall take into account in determining whether an applicant CA is suitable for recognition under the ETO. Among other things, the Director shall consider the arrangements put in place by the applicant to cover any liability that may arise from its activities relevant for the purposes of the ETO.

3. In accordance with section 20(3)(b) of the ETO, a CA applying for recognition must furnish to the Director a report which contains an assessment as to whether the applicant is capable of complying with the provisions of the ETO and the Code of Practice for Recognized Certification Authorities. The Guidance Note on Compliance Assessment of Certification Authorities (Guidance Note) published by the Director provides guidelines in respect of the scope and conduct of an assessment of a CA.

4. Paragraph 22 of the Guidance Note states that the assessor should, in respect of the CA's management of its potential liabilities, express an opinion as to the reasonableness of the assertions made by the CA that it has implemented and maintained effective procedures to determine and manage its potential liabilities.

5. The Hong Kong Society of Accountants (HKSA) published its Practice Note 870 "The Assessments of Certification Authorities under the Electronic Transactions Ordinance" (Practice Note) in December 2000. The

Practice Note provides guidance to members of HKSA acting as assessors on the scope, conduct and reporting requirements of an assessment of a CA under the ETO.

6. The requirement as set out in paragraph 22 of the Guidance Note is reflected in paragraphs 47 and 68 of the Practice Note.

### **Feedback from An Assessor**

7. We received feedback from an assessor, who had prepared an assessment report on a CA, that it was unreasonable to expect a CA to provide an assertion that the CA's procedures were effective in determining the potential liabilities in relation to the issuance of certificates. The assessor was also of the view that there would be practical difficulty for it to form an opinion on such an assertion, even if it was made by a CA. The assessor's concern was with the requirement of "effectiveness" of the procedures of a CA in determining potential liabilities, as "effectiveness" implies expectation that the CA will carry out the procedures in a manner leading to the achievement of the objectives for which the procedures are designed. The assessor opined that, while the design of the procedures could be assessed, the result of the execution of the procedures by the CA would not be something to be assured.

8. We consulted the HKSA with regard to the above feedback from the assessor who is a member of the HKSA. The HKSA advised that there were grounds for the concerns of the assessor and considered that the threshold of "appropriateness" instead of "effectiveness" would be more reasonable.

9. After further consultation between the HKSA and the Information Technology Services Department, the HKSA revised its Practice Note in July 2001 by replacing the word "effective" with "appropriate" in paragraphs 47 and 68 therein and in the example engagement letter and assessment report attached to the Practice Note.

### **Proposed amendments to the Guidance Note**

10. In connection with the advice of the HKSA and its revision of the Practice Note as described in paragraph 9 above, we intend to amend paragraph 22 of the Guidance Note as follows:

"22. The assessor should, in respect of the CA's management of its potential liabilities, express an opinion as to the reasonableness of the assertions made by the CA that it has implemented and

maintained appropriate procedures to determine and manage its potential liabilities."

11. The above proposed amendment should take immediate effect upon its publication in the Guidance Note.

### **Advice Sought**

12. Members' views are herewith invited.

**Information Technology Services Department  
August 2001**