ACCOP Paper No. 4/2001

Proposed Amendment to Code of Practice for Recognized Certification Authorities regarding Publication by Director of Information Technology Services of Information Submitted by a Recognized Certification Authority

Introduction

This paper briefs Members on a proposed amendment to the Code of Practice for Recognized Certification Authorities (the Code of Practice). The amendment is in respect of the publication by the Director of Information Technology Services (the Director) of information submitted by a recognized certification authority (RCA) under the Electronic Transactions Ordinance (Cap. 553) (ETO) or the Code of Practice.

Background

2. In accordance with section 31(1) of the ETO, the Director must maintain for each RCA an on-line and publicly accessible record, i.e. the disclosure record. Section 31(2) specifies that the Director must publish in the disclosure record of a RCA information regarding that RCA relevant for the purposes of the ETO.

3. In accordance with section 43(1) of the ETO, at least once in every 12 months, a RCA must furnish the Director with a report containing an assessment as to whether the RCA has complied with the provisions of the ETO and the Code of Practice. Section 43(3) stipulates that the Director must publish in the disclosure record for the RCA the date of the assessment report and the material information in the assessment report.

4. In accordance with paragraph 10.3 in the Code of Practice, a RCA is required to submit to the Director half-yearly progress reports containing information such as the number and types of digital certificates issued, performance compared with its stated service level, changes in its organisational structure or systems, etc. Furthermore, paragraph 10.6 in the Code of Practice specifies that a RCA shall report any incident that materially and adversely affects its operation to the Director immediately.

5. In accordance with paragraph 10.4 in the Code of Practice, the Director may also call for a progress report or other information from a RCA relevant under the ETO at any time by giving a reasonable notice to the RCA.

6. In cases where the Director considers that any information received from a RCA or from other sources should be published for the benefit of the public in so far as the operation of the RCA relevant under the ETO is concerned, the Director will publish such information in the disclosure record of the RCA in accordance with section 31(2) or 43(3) of the ETO.

Possible Attempt to Stop the Director from Publishing Information

7. With regard to the publication by the Director of information submitted by a RCA, there is a possibility that the RCA might try to prevent the publication by claiming confidentiality or copyright protection in respect of the information concerned.

8. We have sought legal advice on the extent of the authorities conferred to the Director by the ETO over any possible claim of confidentiality or copyright by a RCA with regard to a piece of information submitted by the RCA. According to our legal advice, although the ETO has authorised the Director to publish information of a RCA by way of sections 31(1) and 43(3) therein, there is no certainty that such statutory authorities will in all cases provide a defence in respect of a claim of breach of confidentiality. Furthermore, the ETO does not authorise the Director copying from a report submitted by a RCA.

Proposed Amendment to the Code of Practice

9. To address the above issue, we intend to amend the Code of Practice by adding two new paragraphs under Section 10 (Disclosure of Information) as follows:

> "10.7 On submission by a recognized CA of any report or information under the Ordinance or the Code of Practice, the recognized CA shall be deemed to have granted a licence to the Director for the Director to reproduce and publish the whole or any part of the report or information for the purpose of the relevant provisions under the Ordinance. The recognized CA shall ensure that it has the necessary rights over such report or information so that it can grant the aforesaid licence to the Director. The recognized CA agrees to the disclosure of any such report or information by the

Director as the Director thinks fit for the purpose of the relevant provisions under the Ordinance.

10.8 A recognized CA shall not attempt in any way to prevent the Director from publishing information for the purpose of the relevant provisions under the Ordinance. ”

10. The requirements proposed in the two new paragraphs should take immediate effect upon their publication in the Code of Practice.

Undertaking from a Qualified Person

11. The assessment report submitted by a RCA to the Director at least once in every 12 months is prepared by a qualified person under section 43(2) of the ETO. It is possible that the qualified person, or a member of the assessment team working for the qualified person, might try to stop the Director from publishing information from an assessment report by claiming confidentiality or copyright protection in respect of the information therein.

12. To prevent such a possible situation, we have inserted requirements similar to those set out in paragraph 9 above in the document entitled "Documents and Information Required for Application to Engage A Qualified Person under the Electronic Transactions Ordinance (Cap. 553)" which is published on our web site (http://www.itsd.gov.hk/itsd/caro/sub7.htm). A copy of the document is at the Annex. Paragraphs 2(a)(vii) and (viii) therein are the relevant undertakings required from a potential assessor (i.e. the qualified person), the responsible individual and members of the assessment team who work for the potential assessor.

Advice Sought

13. We welcome Members' views, in particular on the proposed arrangements in paragraphs 9-12 above.

Information Technology Services Department
August 2001

Annex

Documents and Information Required for Application to Engage A Qualified Person under the Electronic Transactions Ordinance (Cap. 553)

Section 20(3)(b) of the Electronic Transactions Ordinance (Cap. 553) (the Ordinance) specifies that a certification authority (CA) seeking recognition must furnish to the Director of Information Technology Services (the Director) a report prepared by a person acceptable to the Director for giving the report. The report must provide an assessment as to whether the CA is capable of complying with the provisions of the Ordinance applicable to a recognized CA and the Code of Practice for Recognized Certification Authorities (Code of Practice). Sections 43(1) and (2) of the Ordinance specify that at least once in every 12 months, a recognized CA must furnish to the Director a report containing an assessment as to whether the recognized CA has complied with the provisions of the Ordinance applicable to a recognized CA and the Code of Practice during the period for which the report is prepared. The report must be prepared by a person approved by the Director as being qualified to make such a report.

2. A CA shall apply in writing to the Director for approval that the person whom the CA intends to engage for the preparation of an assessment report is a qualified person under section 20(3)(b) or section 43(2). The CA shall furnish the Director with the following documents and information in respect of the application:

(a) An original statement jointly signed by the person who wishes to be a qualified person (the Potential Assessor) and by the individual (the Responsible Individual) who will sign the assessment report, stating that:

   i) the Responsible Individual together with members of the assessment team acting or working for the Potential Assessor will prepare the assessment report;

   ii) the Responsible Individual together with members of the assessment team meet the qualifications set out in paragraph 12.2 of the Code of Practice (*the Responsible Individual and members of the assessment team are all included as paragraph 12.3 of the*

Code of Practice specifies that a qualified person may be an organisation comprising individuals that collectively possess all the requirements set out in paragraph 12.2);

iii) the Responsible Individual meets the requirements and shall bear the responsibilities set out in paragraph 12.3 of the Code of Practice;

iv) the Responsible Individual will ensure that the assessment report is prepared in accordance with the Guidance Note on Compliance Assessment of Certification Authorities;

v) the information provided in the statement is, to the best of the knowledge and belief of the Potential Assessor and the Responsible Individual, true and accurate up to the moment the Potential Assessor and the Responsible Individual sign the statement;

vi) the Potential Assessor and the Responsible Individual have read and understood section 47 of the Ordinance in respect of the consequences of making or furnishing any declaration, return, certificate or other document or information which is untrue, inaccurate or misleading;

vii) the Potential Assessor, the Responsible Individual and members of the assessment team agree to grant a licence to the Director, where they have the right to grant such licence, for the Director to reproduce and publish the whole or any part of the contents of the assessment report for the purpose of the relevant provisions under the Ordinance; and

viii) the Potential Assessor, the Responsible Individual and members of the assessment team agree to the disclosure of any information in the assessment report by the Director as the Director thinks fit for the purpose of the relevant provisions under the Ordinance.

Certified copies of the statement are not accepted.

(b) An original letter from the professional organisation or association, which the Responsible Individual belongs to, confirming that the

Responsible Individual is a member of the organisation or association with good standing and that the Responsible Individual is currently holding the relevant practising certificate. The letter should be issued by the organisation or association within one month from the date of application for approval as a qualifier person. Certified copies are not accepted.

(c) A list of members of the assessment team which will prepare the assessment report and their individual experiences and qualifications relevant for the preparation of the assessment report, with particular regards to the skills requirements set out in paragraph 12.2 of the Code of Practice. The experiences of members of the assessment team should be presented on a project-by-project basis, including without limitation:

i) a brief description of each project, preferably with the name of the client;

ii) the role and responsibility of each member of the assessment team in each project; and

iii) duration of involvement by each member of the assessment team in each project.

(d) For performing the financial review as part of the assessment, the team member concerned should be a registered member holding the relevant practising certificate of a professional organisation or association in the accounting discipline which meets the requirements as set out in 12.5 of the Code of Practice with documentary proof.

(e) A description of the methodology and standards to be adopted for the purpose of performing the assessment.

(f) If the Potential Assessor is a company incorporated under the Companies Ordinance (Cap. 32), a certified true copy of the certificate of incorporation and the business registration certificate of the Potential Assessor.

(g) If the Potential Assessor is a partnership, a certified true copy of the business registration certificate of the Potential Assessor.

(h) A certified true copy of the business registration certificate or its equivalent of the CA who submits the application for the Potential Assessor to be approved as qualified to prepare an assessment report.

(i) If any of the above particulars and documents are to be certified, the particular and document shall be certified by an independent solicitor, commissioner for oaths or a notary public.

(Please note:

- a reference to a solicitor is a reference to a person who is a solicitor qualified to act as such under the Legal Practitioners Ordinance (Cap. 159);

- commissioner for oaths means a commissioner for oaths duly appointed by the Chief Justice under any enactment in force in Hong Kong; and

- notary public, in relation to Hong Kong, means a notary public registered by the Registrar of the High Court under section 40 of the Legal Practitioners Ordinance (Cap 159), and in relation to a place outside Hong Kong, means a person duly authorized to take declarations under the laws of that place).

(j) If any of the particulars and documents are submitted via electronic mail, the submission would be governed by the provisions of the Electronic Transactions Ordinance (Cap. 553) and should be sent to the email address: caro@itsd.gov.hk.

Information Technology Services Department

August 2001