PRACTICE NOTE 870
THE ASSESSMENTS OF CERTIFICATION AUTHORITIES UNDER THE ELECTRONIC TRANSACTIONS ORDINANCE

(Issued December 2000; revised July 2001; February 2002 and September 2004 (name change))

Contents *Paragraphs*

PRACTICE NOTE 870
THE ASSESSMENTS OF CERTIFICATION AUTHORITIES UNDER THE ELECTRONIC TRANSACTIONS ORDINANCE

The purpose of Practice Notes issued by the Hong Kong Institute of Certified Public Accountants (HKICPA) is to assist auditors in applying Auditing Standards of general application to particular circumstances and industries.

They are persuasive rather than prescriptive. However they are indicative of good practice and have similar status to the explanatory material in Statements of Auditing Standards (SASs), even though they may be developed without the full process of consultation and exposure used for SASs. Auditors should be prepared to explain departures when called upon to do so.

Supplement One forms part of this Practice Note.

Introduction

Purpose of Practice Note

1. The purpose of this Practice Note is to provide guidance to members acting as assessors on the scope, conduct and reporting requirements of an assessment of Certification Authorities ("CAs") pursuant to the requirement under section 20(3)(b) or section 43(1) of the Electronic Transactions Ordinance. Section 20(3)(b) of the Electronic Transactions Ordinance states that a CA applying for recognition under section 20(1) must furnish to the Director of Information Technology Services ("Director") a report containing an assessment as to whether the CA is capable of complying with the provisions of the Ordinance applicable to a recognized CA ("RCA") and the "Code of Practice for Recognized Certification Authorities" issued by the Director under section 33 of the Ordinance ("Code of Practice"). Section 43(1) of the Electronic Transactions Ordinance states that at least once in every 12 months, RCAs must furnish to the Director a report containing an assessment as to whether the RCA has complied with the provisions of the Ordinance applicable to a RCA and the Code of Practice during the report period.

2. This Practice Note has been prepared in consultation with the Information Technology Services Department ("ITSD") of the Hong Kong SAR Government, and it has been agreed that the scope of work and reporting by members under this PN would meet the requirements of an assessment of a CA pursuant to the requirement under section 20(3)(b) or section 43(1) of the Electronic Transactions Ordinance.

3. In this Practice Note all the sections referred to below are in respect of the Electronic Transactions Ordinance ("Ordinance") unless otherwise stated. A Glossary of Terms is included at the end of this Practice Note.

4. This Practice Note is based on the provisions of the Ordinance applicable to a RCA effective as at January 2000, as well as the requirements set out in the Code of Practice which was published in January 2000 and updated in March 2001.

5. Every care has been taken in the preparation of this Practice Note. However, this Practice Note should be used in conjunction with the Ordinance, the Code of Practice and the "Guidance Note on Compliance Assessment of Certification Authorities" published by the ITSD in January 2000 and updated in February 2001.

6. The terms "comply with" and "compliance with" can be taken to mean "capable of complying with" (section 20(3)(b)) and "has complied with" (section 43(1)) throughout this Practice Note. The term "RCA" can be taken to mean "applicant CA" (section 20(3)(b)) and "recognized CA" (section 43(1)) throughout this Practice Note. The actual meaning of the terms will be dependent upon the context in which they are used.

7. Except as otherwise specified, the terms in this Practice Note common to the Ordinance and the Code of Practice carry the same meaning as those defined in the Ordinance and the Code of Practice. Reference would need to be made to the Ordinance and the Code of Practice, where necessary.

Overview of legislative framework

8. The Ordinance was enacted on 7 January 2000. The purpose of the Ordinance is to give electronic transactions and records the same legal status as paper-based records, as well as to establish a legal framework needed to support a public key infrastructure (PKI). The Ordinance sets out specific provisions relating to the legal recognition and admissibility of electronic records, the presentation and retention of information electronically, the use of digital signatures, formation of electronic contracts, recognition of CAs and certificates, and regulations concerning RCAs and recognized certificates. The Postmaster General is a RCA for the purpose of the Ordinance.

9. The Ordinance empowers the Director to recognize CAs (section 21) and/or certificates issued by RCAs (section 22), and to renew the recognition of RCAs (section 27). The regulatory framework established under the Ordinance for CAs and certificates is of a voluntary nature; an organisation can still offer CA services without seeking recognition from the Director.

10. In accordance with section 33, the Director has published a Code of Practice to specify the standards and procedures for carrying out the functions of RCAs. Failure to comply with the Ordinance or the Code of Practice may result in a CA not being approved for recognition or having its recognition suspended or revoked, as the case may be.

11. Prior to recognizing a CA under section 21 or renewing the recognition of a RCA under section 27, the Director is required to consider the areas specified under section 21(4), including:

    a. whether the RCA has the appropriate financial status for operating as a RCA in accordance with the Ordinance and the Code of Practice;

    b. the arrangements put in place or proposed to be put in place by the RCA to cover any liability that may arise from its activities relevant for the purposes of the Ordinance;

    c. the systems, procedures, security arrangements and standards used or proposed to be used by the RCA to issue certificates to subscribers;

    d. the conclusions of the assessment report prepared in accordance with section 20(3)(b);

    e. whether the RCA and the responsible officers are fit and proper persons; and

    f. the reliance limits set or proposed to be set by the RCA for its certificates.

    This Practice Note only provides guidance in relation to the assessment which covers points a. to d. noted above. This is further elaborated in paragraphs 17 to 49 below.

12. The Director may recognize certificates issued by the RCA as recognized certificates, upon application by the RCA. Before recognizing a class, type or description of certificate under section 22, the Director is required to satisfy himself that the RCA has satisfactorily met the criteria specified under section 22(5), including:

    a. whether the certificates are issued in accordance with the Certification Practice Statement(s) ("CPS(s)") ;

    b. whether the certificates are issued in accordance with the Code of Practice;

    c. the reliance limit set or proposed to be set for that type, class or description or the particular certificate; and

    d. the arrangements put in place or proposed to be put in place by the RCA to cover any liability that may arise from the issue of that type, class or description or the particular certificate.

Role of the assessors

13. The role of the assessors would be to conduct assessments pursuant to the requirement under section 20(3)(b) or section 43(1) in accordance with this Practice Note and provide an assessment report to the RCA.

14. Prior to the RCA engaging a member to act as an assessor, the RCA is required to seek approval of the member by the Director, in accordance with section 12 of the Code of Practice. The list of eligibility criteria is set out in section 12 of the Code of Practice.

15. Members acting as assessors should be, and be seen to be, free in the assessments they undertake of any interest which might detract from objectivity. Members would also ensure that they take reasonable care to avoid giving any impression that the assessment report is the sole factor that the Director would consider in the granting or renewal of a CA's recognition status. Furthermore, members would do or say nothing to encourage the management of the RCA, third parties or the public to place a mistaken degree of reliance on the assessment.

16. A significant part of the assessment is of a technical nature, and members would ensure that they possess or have available the technical expertise in information technology and other areas needed to conduct the assessment. Members are reminded that one of the Fundamental Principles established in Professional Ethics Statement 1.200 "Explanatory foreword" is that a member should not undertake or continue professional work which he is not himself competent to perform unless he obtains such advice and assistance as will enable him to carry out his task competently. Members should also refer to the Professional Risk Management Bulletin PRMB1, "Managing the professional liability of accountants", issued on 15 July 1999 for further guidance.

Scope of the assessments

17. The objective of the assessment is to draw a conclusion for the purposes of section 20(3)(b) or section 43(1), as to whether, in all material respects, the RCA under assessment has complied with the provisions of the Ordinance applicable to a RCA and the Code of Practice.

18. Members would obtain from the management of the RCA an assertions letter that states that the RCA has complied with the provisions of the Ordinance applicable to a RCA and the Code of Practice, and attach it to the assessment report. In the preparation of the assertions letter, reference may be made to Appendix 3.

19. Members would review the reasonableness of management assertions by appying the procedures in paragraphs 20 to 49 below.

20. The assessment comprises three parts:

    a. the review of the reasonableness of the assertions by the management of the RCA in respect of its compliance with the provisions of the Ordinance applicable to a RCA and the Code of Practice. Specifically, the following RCA practices would be considered:

        i. the RCA's disclosure of its business practices in its CPS(s) and the provision of its services in accordance with its disclosed business practices;

        ii. the RCA's compliance with the requirements in respect of the use of a trustworthy system to support its operations; and

        iii. the RCA's compliance with the requirements in respect of the recognition of its certificates;

    b. the review of the RCA's half yearly financial projections prepared by the RCA for the next 12 months in respect of the RCA's operations relevant under the Ordinance; and

    c. the review of the arrangements proposed to be put in place or put in place by the RCA to cover any liability that may arise from its activities that fall within the scope of the Ordinance and the Code of Practice.

RCA practices

21. Members would design and carry out appropriate procedures to assess and conclude on the RCA's assertions made in respect of paragraph 20(a) above. In this respect, it is considered that members would normally regard the RCA's compliance with sections 36 to 45 and the Code of Practice as their normal scope of review to enable them to assess and conclude on the RCA's assertions made in respect of paragraph 20(a) above. Sections 36 to 45 are:

    a. Section 36: Publication of issued and accepted certificates;

    b. Section 37: Recognized certification authority to use trustworthy system;

    c. Section 38: Presumption as to correctness of information;

    d. Section 39: Representations upon issuance of recognized certificate;

    e. Section 40: Representations upon publication of recognized certificate;

    f. Section 41: Reliance limit;

    g. Section 42: Liability limits for recognized certification authorities;

    h. Section 43: Recognized certification authority to furnish report on compliance with Ordinance and code of practice;

    i. Section 44: Recognized certification authority to issue a certification practice statement;

    j. Section 45: Recognized certification authority to maintain repository.

22. However, where members become aware, during the assessment, of any knowledge or information of non-compliance by the RCA with other sections of the Ordinance, members would have to consider the implications thereof on the scope of their review and would perform additional procedures, as considered appropriate.

23. The requirements under sections 36 to 45 are elaborated in the Code of Practice which provides guidance on the standards and procedures to be adopted by RCAs in carrying out their functions. It is the view of the Director that RCAs are required to comply with all sections of the Code of Practice.

24. While members would need to assess whether the RCA has complied with the entire Code of Practice, certain requirements specified in the Code of Practice are general in nature, such as requiring a RCA to comply with all applicable ordinances and regulations regarding the privacy of personal information (paragraph 3.6 of the Code of Practice). Members may find it difficult to design effective procedures that would provide positive assurance on the RCA's compliance with such requirements.

25. Appendix 3 allocates the sections of the Code of Practice into three Parts: 3A, 3B and 3C. The first part, Part 3A, lists the sections of the Code of Practice where members would provide a positive assurance on the RCA's compliance. Members would exercise professional judgement to determine the extent of procedures that need to be performed to support the positive assurance on the RCA's compliance with these requirements.

26. The second part, Part 3B, lists the sections of the Code of Practice which are general in nature, as discussed in paragraph 24, where members would provide a negative assurance on the RCA's compliance. It is not envisaged that members would be expected to conduct tests to assess the RCA's compliance with these sections, however, they would be expected to highlight any non-compliance with such requirements should any such incidents come to their attention during the course of the assessment.

27. The third part of Appendix 3, Part 3C, lists the explanatory material contained in the Code of Practice. These sections provide additional explanations and would be read in conjunction with Parts 3A and 3B. These sections are statements of fact, and members would not be expected to provide any assurance on the RCA's compliance with them.

28. When performing the assessment, members would be expected, as a minimum, to design and carry out appropriate procedures to assess the RCA's compliance with the requirements set out in Parts 3A and 3B of Appendix 3.

Disclosure of CA business practices and provision of its services

29. Section 4 of the Code of Practice requires the RCA to define in the CPS(s) its policies and practices, including details of services intended to be provided or provided in relation to the types, classes or descriptions of recognized certificates that it issues. The CPS is required to be maintained and updated for changes in the RCA's policies and practices under section 44.

30. The minimum standards which the Director expects the RCA to adopt and comply with when issuing its CPS(s) are set out in the Code of Practice's appendix, "Standards and Procedures regarding the Contents of Certification Practice Statements". Members would refer to this appendix when performing the assessment.

31. Members would assess whether the RCA has implemented a process to issue and maintain an up to date CPS(s) and whether the CPS(s) issued by the RCA meets the minimum standards as set out in the appendix to the Code of Practice. Members would design and perform tests to obtain reasonable assurance that the RCA discloses all relevant policies and business practices in its CPS(s) and adheres to the business practices disclosed. In designing the procedures to be performed, members would ensure that, as a minimum, the requirements set out in Parts 3A-2 and 3A-12 of Appendix 3 are addressed.

Assessment of systems, procedures, security arrangements and standards

32. Section 37 requires a RCA to use a trustworthy system in performing its services. Under section 5 of the Code of Practice, the term "system" refers to the system itself, i.e. hardware and software, as well as those control and operational procedures (both manual and automated) that are designed to ensure that the system will perform its intended functions in a consistent, reliable and dependable manner.

33. In the assessment of a trustworthy system, members would obtain an understanding of the technical setup of the RCA's systems, and design and carry out procedures to cover as a minimum the requirements set out in Part 3A-3 of Appendix 3.

34. Where a RCA specifically states in its CPS(s) matters concerning the underlying technical configuration of its systems, such as stating that its cryptographic module conforms to a specific security standard (e.g. FIPS 140-1, level 2), members would perform appropriate procedures to obtain reasonable assurance concerning the validity of such statements. It is however not envisaged that members would have the capability to independently validate such statements as such validation is usually conducted in technical laboratories over an extended period of time.

Certificate life cycle management

35. Members would only be expected to perform work in this area if the RCA issues certificates that are recognized by the Director under section 22 or there are the designated certificates issued by The Postmaster General, or is seeking to obtain recognition of some or all of the classes of certificates that it issues.

36. Members would design and carry out appropriate procedures to obtain reasonable assurance that the certificates are issued in accordance with the RCA's CPS(s), as well as in compliance with the requirements set out in Part 3A-4 of Appendix 3.

37. Members would also assess the reasonableness of management assertions that it has established procedures to determine and manage its potential liability in relation to the issue of recognized or unrecognized certificates. This aspect is elaborated further in paragraphs 47 to 49 below.

Other obligations of RCAs

38. Members would design and carry out procedures to assess the RCA's compliance with other sections detailed in Part 3A of Appendix 3 which do not fall within the scope of the three areas described in paragraphs 29 to 37 above.

39. In relation to the requirements set out in Part 3B of Appendix 3, members would be expected to highlight any non-compliance with these sections should any such incidents come to their attention during the course of the assessment.

Review of financial projections

40. Members would review the financial projections prepared by the RCA to assess whether the accounting policies upon which the financial projections are based are consistent with those normally adopted by the RCA and conform with generally accepted accounting principles adopted in Hong Kong or International Accounting Standards, and whether the projections have been properly compiled based on assumptions made by management. In reviewing the financial projections, members would have regard to the information disclosed in the RCA's latest audited financial statements, where appropriate, and also the RCA's management accounts for the period between the latest audited financial statements and the financial projections.

41. The financial projections would include half yearly cashflow projections and financial position forecasts in respect of the RCA's operations relevant under the Ordinance. The financial projections would be based on assumptions about events that may occur in the future and possible actions by the RCA. The financial projections should cover a period of no less than 12 months. The RCA would need to confirm the period covered by the financial projections with the Director, which will form the basis of the assessment.

42. Members would ascertain which accounting policies have been adopted by the RCA in its annual financial statements so as to assess whether they conform with the generally accepted accounting principles adopted in Hong Kong or International Accounting Standards, and have been consistently applied in the preparation of the RCA's financial projections.

43. Where the RCA's accounting policies do not appear to be in conformity with the generally accepted accounting principles adopted in Hong Kong or International Accounting Standards, members would include an appropriate comment in the assessment report.

44. It is the responsibility of the members acting as assessors to consider whether the financial projections have been properly compiled on the basis of the assumptions made by the management of the RCA. This would include checking the arithmetical accuracy of the financial projections and the supporting information.

45. While evidence may be available to support the assumptions on which the financial projections are based, such evidence is itself generally future oriented and speculative in nature, and therefore cannot be relied upon to the same extent as information derived from the audited financial statements for prior accounting periods. Members are therefore not in a position to report upon the assumptions or to report on the prospect of the RCA achieving the financial projections. However, if an assumption is made which appears to be unrealistic or inappropriate (or one is omitted which appears to be important), members would comment on this matter in the assessment report.

46. It is, therefore, important that members take reasonable care in the wording of their report to avoid giving any impression that they are in any way confirming, guaranteeing or otherwise accepting responsibility for the ultimate accuracy and realisation of projections. Moreover, members would do or say nothing to encourage the management of RCAs, third parties or the public to place a mistaken degree of reliance on statements as to future projections, the achievement of which must always be subject to uncertainty.

Ascertaining potential liabilities

47. Members would assess the reasonableness of the assertions made by the RCA that it has implemented and maintained appropriate procedures to determine and manage its potential liabilities in relation to the certificates, both recognized and unrecognized, that it has issued or planned to issue, including:

    a. potential claims arising out of any error or omission on the part of the RCA, its directors, officers, employees or agents; and

    b. potential liabilities arising from the reliance limits specified on its certificates.

48. In assessing the reasonableness of the above assertions made by the RCA, members would obtain an understanding of the procedures the RCA has in place to determine and manage its potential liabilities.

49. Members would ascertain the information from management of the RCA in respect of the following areas and reproduce such information as an attachment to their assessment report:

    a. potential liabilities of the RCA in relation to issued certificates at the time of the review;

    b. details of insurance cover or other appropriate forms of cover for the RCA's potential liabilities in relation to issued certificates as at the time of the assessment including details of insurers such as the insurer's registration name and address;

    c. any claims the RCA has received from subscribers and/or relying parties since the date of the last assessment and the status of these claims; and

    d. any claims which have been filed against the insurance policies of the RCA since the date of the last assessment.

    Members are under no obligation to perform procedures to confirm the completeness of the above information nor to provide an assurance on its reasonableness.

Planning considerations

50. Members would plan and perform the assessment with an attitude of professional scepticism recognizing that circumstances may exist which may cause material exceptions in the RCA's compliance with the provisions of the Ordinance applicable to a RCA and the Code of Practice.

51. In planning an assessment of the RCA, members would also consider the following matters:

    a. Conditions attached by the Director in granting or renewing recognition under section 21 or section 27

       Members would obtain an understanding of the conditions attached by the Director, and would seek management assertions on compliance with these conditions as appropriate. Additional procedures would be designed as appropriate to assess the RCA's compliance with these conditions.

    b. Additional requirements on assessment issued by the Director

       As a general principle, the engagement for the assessment is between the RCA and the member. Members would ensure that any additional requirements issued by the Director to the RCA in relation to the assessment are specifically detailed in the engagement letter.

       Where members are unable to address the additional requirements due to a limitation of scope or for other reasons, members would notify the RCA of the inability to meet the additional requirements. Members would ensure that such limitations are clearly set out in both the engagement letter and the assessment report.

    c. Significant parts of the RCA's operations being outsourced to third parties

       The Ordinance and the Code of Practice allow RCAs to outsource parts of their operations to third parties. Where parts of the RCA's operations are outsourced, members would use their professional judgement to assess the significance of such functions and to consider extending the assessment procedures as appropriate to include relevant parts of the third party operations. Examples of significant functions that may be outsourced include certificate issuance and repository maintenance.

    d. The expertise required for technical areas assessment

       In the assessment of a trustworthy system, members would apply relevant technical skills and knowledge when assessing the following areas:

       i. technical setup of the RCA's systems including operating system, network, application and database configuration and security management;

       ii. controls and procedures over generation of keys and their management; and

       iii. controls and procedures over security of repositories and certificate revocation list.

Given the technical nature of the subject matter, members may involve as appropriate experts in carrying out the assessment.

When using work performed by an expert or the RCA's internal audit, members should consider the requirements of SAS 520 "Using the work of an expert" and SAS 500 "Considering the work of internal auditing". Members should ensure that the work performed by the expert provides sufficient appropriate evidence to support the members' conclusions.

e. Implications of section 47 for members

Section 47 states that it is an offence if a person knowingly or recklessly makes, orally or in writing, signs or furnishes any declaration, return, certificate or other document or information required under the Ordinance which is untrue, inaccurate or misleading. The Director requires that the assessors should be aware of the implications of section 47 as it is relevant to the assessment report.

Members would therefore take all possible steps to ensure that the assessment report is factually accurate, for example by requiring the RCA under assessment to provide written confirmation on the factual accuracy of the information provided to members for the purpose of this assessment. The management's confirmation that it is aware of and has complied with this section would be included in the engagement letter and the management representations letter.

Responsibilities of RCAs

52. The management of the RCA is responsible for ensuring that the RCA has complied with the provisions of the Ordinance applicable to a RCA and the Code of Practice, and with the policies and business practices specified in the RCA's CPS(s) as they relate to the activities of a RCA. These responsibilities include:

    a. disclosure of its business practices in its CPS(s) in accordance with the Ordinance and the Code of Practice and provision of its services in accordance with its disclosed business practices;

    b. the design, implementation and maintenance of a trustworthy system and the overall control framework surrounding the trustworthy system to support its operations; and

    c. compliance with the requirements in respect of the recognition of its certificates.

53. Management of the RCA also has the sole responsibility for the preparation and presentation of the financial projections, including the assumptions upon which the financial projections are based, and the information regarding the potential liabilities of the RCA provided to the members acting as assessors.

Engagement letter

54. The basic principles applicable to drafting engagement letters as set out in SAS 140 "Engagement letters" are applicable to the assessment of RCAs. Members should agree the terms of the engagement with the RCA. The agreed terms should be recorded in an engagement letter or other suitable form such as a contract. An example of an engagement letter is included in Appendix 1.

55. Specific matters in relation to the assessment that would be included in the engagement letter include:

    a. the objective of the assessment;

    b. the assessment will be performed in accordance with this Practice Note;

    c. the responsibilities of the RCA;

    d. a reference to the need for management representations;

    e. an explanation of the inherent limitations of the work, including the fact that the assessment cannot be relied upon to disclose all non-compliance, errors, illegal acts or other irregularities, for example, fraud or defalcations that may exist, and the financial projections cannot be relied on to the same extent as information derived from the audited financial statements for prior accounting periods as they are future oriented and may be affected by unforeseen events;

f. a reminder to management of its responsibility under section 47;

g. any agreed upon limitations of the liability of the member; and

h. the form of any reports or other communication of results of the engagement.

Management representations

56. In addition to obtaining from the management of the RCA an assertions letter that states that the RCA has complied with the provisions of the Ordinance applicable to a RCA and the Code of Practice (see paragraph 18 above), members are recommended to obtain written confirmation of representations made by management in the course of the assessment, on matters material to the assessment when those representations are necessary to obtaining sufficient appropriate evidence.

57. Matters on which written management representations may be sought by members include:

a. a statement that management has disclosed to the member acting as assessor all significant changes in procedures;

b. a statement that management has disclosed to the member acting as assessor details of any fraud or illegal acts, irregularities or uncorrected errors attributable to the RCA's directors, its officers, employees or agents that came to its attention;

c. a statement that management has informed the member acting as assessor of all instances, of which it is aware, when procedures had not operated as designed;

d. a statement that all claims received from and all claims filed against insurance policies have been disclosed to the member acting as assessor; and

e. a statement regarding awareness of and compliance with section 47.

58. Further guidance on management representations is set out in SAS 440 "Representations by management".

Reporting

59. Members would prepare a written assessment report addressed to the RCA on the results and findings of the assessment. Members would state clearly in the report the findings of the assessment including sufficient details of material exceptions, such as incidents of non-compliance with the provisions of the Ordinance applicable to a RCA and the Code of Practice (see paragraphs 70 to 72 below).

60. The form and content of the assessment report by members will depend on the specific terms and conditions agreed with the management. However, such assessment reports would normally be expected to contain:

a. a statement that the report is intended solely for filing with the Director in accordance with the Ordinance and for no other purposes;

b. the objective of the assessment;

c. the period covered by the assessment report;

d. the responsibilities of the RCA;

e. a statement that all control systems have inherent limitations and accordingly errors or irregularities may occur and not be detected. Also, a statement that the assessment may not identify all material exceptions or significant weaknesses and should not be relied upon to disclose all such material exceptions or fraud, system control weaknesses, errors or instances of non-compliance which may exist;

f. a statement that the purpose of the engagement is to conduct an assessment of the RCA's compliance with the provisions of the Ordinance applicable to a RCA and the Code of Practice. Also a statement that accordingly, no assurance can be provided on the design or operational effectiveness of the control procedures that management of the RCA has in place, other than their compliance with the provisions of the Ordinance applicable to a RCA and the Code of Practice.

g. a statement that the projection of any conclusions to future periods is subject to the risk that changes will be made to systems and/or controls to allow for changes in business or other requirements and that the validity of projecting any conclusions in light of the possibility of such changes must be considered;

h. the basis of conclusion in respect of the assessment; and

i. the conclusions reached for the assessment as discussed below.

61. An example report is set out in Appendix 2.

RCA practices

62. Members would provide an assurance as to whether or not, in all material respects, the assertions by the management of the RCA under assessment in respect of its compliance with the sections of the Code of Practice set out in Part 3A of Appendix 3 are reasonable. In providing this assurance, members would specifically provide their assurance on the following matters:

a. whether or not the RCA discloses its business practices in its CPS(s) in accordance with the Ordinance and the Code of Practice and provides its services in accordance with its disclosed business practices;

b. whether or not the RCA complies with the requirements in respect of the use of a trustworthy system to support its operations in accordance with section 37 and the Code of Practice; and

c. whether or not the RCA complies with the requirements in respect of the recognition of its certificates in accordance with sections 36, 38, 39 and 40 and the Code of Practice.

63. Members would also state whether any information has come to their attention during the course of the assessment that would indicate that the assertions made by management of the RCA in respect of its compliance with the sections of the Code of Practice set out in Part 3B of Appendix 3 are not reasonable.

64. Based on the conclusions drawn in paragraphs 62 and 63 above, members would provide an assurance as to whether or not, in all material respects, the management assertions in respect of the RCA's compliance with the provisions of the Ordinance applicable to a RCA and the Code of Practice are reasonable.

Review of financial projections

65. With respect to the RCA's financial projections, members would state:

a. the period covered by the financial projections;

b. whether, in the members' opinion, the accounting policies upon which the projections are based are consistent in all material respects with those normally adopted by the RCA and conform with the generally accepted accounting principles adopted in Hong Kong or International Accounting Standards; and

c. whether, in the members' opinion, the financial projections have been properly compiled in all material respects in accordance with the assumptions made by the RCA.

66. Where the RCA's accounting policies do not appear to be in compliance with the generally accepted accounting principles adopted in Hong Kong or International Accounting Standards, members would include an appropriate comment in the assessment report.

67. Members would also include an appropriate comment in the assessment report if any of the assumptions made, or omitted to be made, by the RCA appears to the members to be unrealistic or inappropriate based on the members' experience and professional judgement.

Ascertaining potential liabilities

68. Members would provide an assurance as to the reasonableness of the assertions made by the RCA that it has implemented and maintained appropriate procedures to determine and manage its potential liabilities in relation to the issue of certificates.

69. Members would reproduce as an attachment to the assessment report the information ascertained from management of the RCA in respect of:

    a. potential liabilities of the RCA in relation to issued certificates at the time of the review;

    b. details of insurance cover or other appropriate forms of cover for the RCA's potential liabilities in relation to issued certificates as at the time of the assessment including details of the insurer such as the insurer's registration name and address;

    c. any claims the RCA has received from subscribers and/or relying parties since the date of the last assessment and the status of these claims; and

    d. any claims which have been filed against the insurance policies since the date of the last assessment.

    Members are under no obligation to perform procedures to confirm the completeness of the above information nor to provide an assurance on its reasonableness.

Material exceptions

70. Members would exercise professional judgement to assess the severity of any noted exceptions or deficiencies, based on the results of the work performed in each of the areas under assessment. All incidents of non-compliance with the provisions of the Ordinance applicable to a RCA and the Code of Practice would be presented in their assessment report.

71. Regardless of whether the RCA has reported such exceptions to the Director during the assessment period, members would nevertheless present those exceptions in their assessment report. Members would also consider whether those exceptions identified in previous periods reoccurred during the period being reported on.

72. Where members have identified opportunities for enhancements to the control procedures implemented by the management of the RCA, they may consider communicating their recommendations to management on these matters.

Publication by the Director of the material information in an assessment report

73. It should be noted that under section 43(3), the Director must publish in the certification authority disclosure record for the RCA the date of the assessment report and the material information in the assessment report, and that under section 31(2), the Director must publish in the certification authority disclosure record information regarding that certification authority relevant for the purposes of the Ordinance.

74. From the perspective of sound risk management, the assessors are advised to encourage the Director to publish the assessment report in full. However, under the Ordinance, the Director has the ultimate authority and full discretion as to what constitutes "material information" in the assessment report to be published by him.

74A. In the event that only extracts from an assessment report but not the full assessment report are published by the Director under section 31(2) or 43(3), the Director has confirmed to the HKICPA that he shall make a statement accompanying the extracts from an assessment report that the full assessment report is not being published.

Confidentiality and copyright of an assessment report

74B. The HKICPA has obtained the following legal advice:

    a. the RCA enjoys the right of confidentiality to an assessment report as it is produced by members at the request and expense of the RCA and is addressed to the RCA, and the RCA is therefore the relevant party to grant a waiver of confidentiality to the Director enabling him to publish the material information in an assessment report pursuant to section 31(2) or 43(3); and

    b. the RCA enjoys an exclusive licence to use the copyright of an assessment report including for the purpose of providing it to the Director, and the RCA is therefore the relevant party to grant a copyright licence to the Director enabling him to publish the material information in an assessment report pursuant to section 31(2) or 43(3).

SUPPLEMENT ONE TO PRACTICE NOTE 870 THE ASSESSMENTS OF CERTIFICATION AUTHORITIES UNDER THE ELECTRONIC TRANSACTIONS ORDINANCE

(Issued July 2001)

This Supplement forms part of Practice Note 870 and should be used in conjunction with the Practice Note.

This Supplement will become effective on 7 August 2001.

Introduction

75. The terms and abbreviations used in this Supplement carry the same meanings as those in Practice Note 870.

76. This Supplement is issued to provide guidance on the additional requirements as stipulated in the "Second Supplementary Note to the Guidance Note on Compliance Assessment of Certification Authorities under the Electronic Transactions Ordinance" issued by the ITSD on 7 February 2001 (Second Supplementary Note). The Second Supplementary Note will become effective on 7 August 2001.

Additional reporting requirements

77. The Second Supplementary Note requires the assessment of RCAs pursuant to the requirement under section 20(3)(b) or section 43(1) of the Ordinance to be expanded to include:

    a. a review of the RCA's 90-day projection of operating costs; and

    b. an ascertainment of details of insurance cover arranged by the RCA.

Review of 90-day projection of operating costs

78. The assessors would compare the following as ascertained from the RCA:

    a. the amount of net current assets as shown in the accounts, which may be in the form of unaudited management accounts, of the RCA for the period ended on a specified date which is the start date of the 12-month financial projection prepared by the RCA (see paragraph 41 above); and

    b. a projection of operating costs for 90 days in respect of the RCA's operations relevant under the Ordinance, which should start from a date as specified in paragraph 78(a) above.

79. In respect of the 90-day projection of operating costs, the assessors would consider:

    a. whether the accounting policies upon which the projection is based are consistent in all material respects with those normally adopted by the RCA and conform with the generally accepted accounting principles adopted in Hong Kong or International Accounting Standards; and

    b. whether the projection has been properly compiled in all material respects in accordance with the assumptions made by the RCA. If any of the assumptions made, or omitted to be made, by the RCA appears to the assessors to be unrealistic or inappropriate, the assessors would include an appropriate comment in the assessment report.

80. The net current assets referred to in paragraph 78(a) above means current assets less current liabilities.

81. The assessors would present the result of the comparison as stated in paragraph 78 above in the assessment report, and state any comments as a result of the considerations in respect of paragraph 79 above.

82. The accounts and the 90-day projection of operating costs of the RCA, as ascertained from the RCA and referred to in paragraph 78 above, are required to be attached as appendices to the assessment report.

Insurance cover

83. In addition to ascertaining from the RCA the information as set out in paragraph 49 above, the assessors would ascertain the following information from the RCA:

a. whether the RCA has arranged for liability cover with an amount no less than the reliance limit set on the recognized certificates that it issues. The RCA may provide the liability cover by insurance or in other forms; and

b. whether the RCA has acquired insurance cover against claims arising from error or omission of the RCA, with a minimum limit of indemnity in relation to each and every single claim during the period of insurance of not less than:

i. 10 times the reliance limit specified by the RCA on its certificates; or

ii. $200,000

whichever is higher. Moreover, the total insurance cover for aggregate claim amount in any one insurance period of 12 months should be set at 10 times the amount of (i) or (ii) whichever is higher. Such liability cover should be in place at all times and should be arranged for each type, class or description of recognized certificates issued by the RCA. Should the RCA choose to put in place other forms of liability cover, the same minimum limit of indemnity should be provided for.

84. The assessors would report the information as detailed in paragraph 83 above.

GLOSSARY

This glossary outlines the key terms discussed in this Practice Note. Reference should be made to the Ordinance and the Code of Practice for a full list of terms.

Certificate: A record which

a. is issued by a CA for the purpose of supporting a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;

b. identifies the CA issuing it;

c. names or identifies the person to whom it is issued;

d. contains the public key of the person to whom it is issued; and

e. is signed by a responsible officer of the CA issuing it.

Certification authority or CA: A person who issues a certificate to a person (who may be another CA).

Certification practice statement or CPS: A statement issued by a CA to specify the practices and standards that the CA employs in issuing certificates.

Certificate revocation list: A list maintained and published by a CA to specify the certificates that are issued by it and that have been revoked.

Recognized certificate:

a. a certificate recognized under section 22 of the Ordinance;

b. a certificate of a type, class or description of certificate recognized under section 22 of the Ordinance; or

c. a certificate designated as a recognized certificate and issued by the Postmaster General.

Recognized Certification Authority or RCA: A CA recognized under section 21 or the Postmaster General.

Repository: An information system for storing and retrieving certificates and other information relevant to certificates.

Subscriber: A person who

a. is named or identified in a certificate as the person to whom the certificate is issued;

b. has accepted that certificate; and

c. holds a private key which corresponds to a public key listed in that certificate.

Trustworthy system: Computer hardware, software and procedures that

a. are reasonably secure from intrusion and misuse;

b. are at a reasonable level in respect of availability, reliability and ensuring a correct mode of operations for a reasonable period of time;

c. are reasonably suitable for performing their intended function; and

d. adhere to generally accepted security principles.

Appendix 1 : Example engagement letter for engagements under either section 20(3)(b) or section 43(1) of the Electronic Transactions Ordinance

(revised and effective from 26 February 2002)

The following letter is for use as a guide in conjunction with the considerations outlined in paragraph 55 of this Practice Note and will need to be varied according to individual requirements and circumstances. The example wording in respect of a general limitation of liability under the "Limitation of liability" section of the example engagement letter is for general guidance only and does not constitute legal advice. If you are in any doubt as to understanding the statutory requirements and legal implications of the Control of Exemption Clauses Ordinance, you should seek legal advice.

[The Board of Directors]
[Name of CA]
[Address of CA]

[Date]
Our ref:

Dear Sirs

Assessment of [name of CA] under [section 20(3)(b)] [section 43(1)] of the Electronic Transactions Ordinance

This letter is to confirm our understanding of the terms and objective of our engagement to perform an assessment of [name of CA] under [section 20(3)(b)] [section 43(1)] of the Electronic Transactions Ordinance ("Ordinance") and the nature and limitations of such an assessment.

Objective of our assessment

1.1 The objective of the assessment is to enable us to draw a conclusion for the purposes of [section 20(3)(b)] [section 43(1)] of the Ordinance, as to whether, in all material respects, [name of CA] [is capable of complying with] [has complied with] the provisions of the Ordinance applicable to a recognized Certification Authorities (CA) and the "Code of Practice for Recognized Certification Authorities" issued by the Director of Information Technology Services ("Director") under section 33 of the Ordinance ("Code of Practice") published in January 2000 and updated in March 2001 [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx].

Use of the assessment report by [name of CA]

2.1 We will issue an assessment report which is intended solely for [name of CA] to file with the Director in accordance with [section 20(3)] [section 43] of the Ordinance. The assessment report may not be provided by [name of CA] to third parties for any other purpose without our prior written consent.

2.2 It is acknowledged that, under section 43(3) of the Ordinance, the Director must publish in the certification authority disclosure record for [name of CA] the date of the assessment report and the material information in the assessment report, and under section 31(2) of the Ordinance, the Director must publish in the certification authority disclosure record information regarding [name of CA] relevant for the purposes of the Ordinance. It is also acknowledged that, accordingly, [name of CA] may be asked by the Director to grant him an express waiver of confidentiality and an express copyright licence enabling him to publish the material information in the assessment report. We acknowledge that [name of CA] has the right to grant such a waiver of confidentiality and copyright licence to the Director, and that there is no breach of any duty of confidence owed by [name of CA] to us and no infringement of our copyright of the assessment report by [name of CA] if [name of CA] grants such a waiver of confidentiality and copyright licence to the Director for the purpose of section 31(2) or 43(3) of the Ordinance.

Responsibilities of management

3.1 As management of [name of CA], for the purposes of [its application for recognition] [its continuing/renewal of recognition] as a recognized CA as defined under the Ordinance, you are responsible for ensuring that [name of CA] [is capable of complying with] [has been complying with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice, and with the policies and business practices specified in [name of CA]'s Certification Practice Statement(s) ("CPS(s)") as they relate to the activities of a recognized CA. These responsibilities include:

a. disclosure of [name of CA]'s business practices in its CPS(s) in accordance with the Ordinance and the Code of Practice and provision of its services in accordance with its disclosed business practices;

b. the design, implementation and maintenance of a trustworthy system and the overall control framework surrounding the trustworthy system to support [name of CA]'s operations; and

c. compliance with the requirements in respect of the recognition of [name of CA]'s certificates.

3.2 You also have the sole responsibility for the preparation of [name of CA]'s financial projections in respect of the CA's operations relevant under the Ordinance, including cashflow projections and financial position forecasts prepared in half-yearly intervals for the next 12 months, and a projection of operating costs for the next 90 days from the commencement date of the above cashflow projections and financial position forecasts. The accounting policies upon which the financial projections are based should be consistent with those normally adopted by [name of CA] and conform with generally accepted accounting principles adopted in Hong Kong or International Accounting Standards, and the projections should be properly compiled based on your assumptions.

3.3 You are responsible to provide us with the information regarding the potential liabilities of [name of CA] in relation to the issue of certificates at the time of the review, details of insurance cover or other appropriate cover for the liabilities including details of insurers such as the insurer's registration name and address, any claims [name of CA] has received from subscribers and/or relying parties since the date of the last assessment and the status of these claims, and any claims which have been filed against the insurance policies of [name of CA] since the date of the last assessment.

3.4 It is your responsibility to provide us with a management assertions letter that [name of CA] [is capable of complying with] [has complied with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice.

3.5 In accordance with the "Guidance Note on Compliance Assessment of Certification Authorities under the Electronic Transactions Ordinance" published by the Information Technology Services Department ("ITSD") in January 2000 and updated in February 2001, you should make available to us, as and when required, the following:

a. information on [name of CA] regarding:

i. policies and business practices, including details of services [to be provided] [provided];

ii. the systems [to be used] [used] to perform the services;

iii. key management and certificate life cycle controls; and

iv. the potential liabilities in relation to the issue of certificates of [name of CA] at the time of the review, details of insurance cover or other appropriate cover for the liabilities including details of insurers such as the insurer's registration name and address, any claims [name of CA] has received from subscribers and/or relying parties since the date of the last assessment and the status of these claims, and any claims which have been filed against the insurance policies of [name of CA] since the date of the last assessment;

b. financial projections in respect of the CA's operations relevant under the Ordinance, including cashflow projections and financial position forecasts prepared in half-yearly intervals for the next 12 months, and a projection of operating costs for the next 90 days from the commencement date of the above cashflow projections and financial position forecasts;

c. [name of CA]'s latest audited financial statements, and unaudited management accounts for the period between the latest audited financial statements and the financial projections; and

d. other relevant records and related information of [name of CA] that may be needed to support our assurance provided on [name of CA]'s [capability to comply with] [compliance with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice.

Scope of assessment

4.1 Our assessment will be conducted in accordance with Practice Note 870 "The assessments of Certification Authorities under the Electronic Transactions Ordinance" issued by the Hong Kong Institute of Certified Public Accountants.

4.2 The assessment will comprise three parts:

RCA practices

a. the review of the reasonableness of your assertions in respect of [name of CA]'s [capability to comply with] [compliance with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx]. Specifically, the following RCA practices would be considered:

i. [name of CA]'s [capability to disclose] [disclosure of] its business practices in its CPS(s) and [capability to provide] [provision of] its services in accordance with its disclosed business practices;

ii. [name of CA]'s [capability to comply with] [compliance with] the requirements in respect of the use of a trustworthy system to support its operations; and

iii. [name of CA]'s [capability to comply with] [compliance with] the requirements in respect of the recognition of its certificates;

Financial projections

b. the review of [name of CA]'s financial projections in respect of its operations relevant under the Ordinance prepared by you, including half-yearly cashflow projections and financial position forecasts for the next 12 months, and a projection of operating costs for the next 90 days from the commencement date of the above cashflow projections and financial position forecasts;

c. the comparison of the following as ascertained from [name of CA]:

i. the amount of net current assets (i.e. current assets less current liabilities) as shown in the [audited financial statements/unaudited management accounts] of [name of CA] for the [year/period] ended xx/xx/xxxx; and

ii. the projection of operating costs in respect of [name of CA]'s operations relevant under the Ordinance for the next 90 days from xx/xx/xxxx being the start date of the 12-month financial projections prepared by [name of CA]; and

Potential liabilities

d. the review of the arrangements [to be put in place] [put in place] by [name of CA] to cover any liability that may arise from its activities that fall within the scope of the Ordinance and the Code of Practice.

4.3 We shall carry out procedures designed to obtain such appropriate evidence as we consider sufficient to enable us to draw reasonable conclusions therefrom. The nature and extent of our procedures may vary according to our assessment of [name of CA]'s systems and controls and may cover any aspects of the business operations that we consider appropriate.

4.4 In order to assist us with the assessment, we shall request sight of records, documents or statements of [name of CA], including any correspondence with the Director relating to the areas covered in our assessment.

Reporting requirements

5.1 We will provide a written report to you on the results and findings of the assessment.

RCA practices

5.2 We will report to you whether in our opinion, in all material aspects, the assertions made by you in respect of [name of CA]'s [capability to comply with] [compliance with] the sections of the Code of Practice set out in Part 3A of Appendix 3 to Practice Note 870 [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx] are reasonable. In particular, we will provide our assurance on whether or not [name of CA] [is capable of] [has]:

a. [disclosing] [disclosed] its business practices in its CPS(s) in accordance with the Ordinance and the Code of Practice and [providing] [provided] its services in accordance with its disclosed business practices;

b. [complying with] [complied with] the requirements in respect of the use of a trustworthy system to support its operations in accordance with section 37 of the Ordinance and the Code of Practice; and

c. [complying with] [complied with] the requirements in respect of the recognition of its certificates in accordance with sections 36, 38, 39 and 40 of the Ordinance and the Code of Practice.

5.3 We will also state whether any information came to our attention during the course of the assessment that would indicate that the assertions made by you in respect of [name of CA]'s [capability to comply with] [compliance with] the sections of the Code of Practice set out in Part 3B of Appendix 3 to Practice Note 870 [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx]are not reasonable.

5.4 Based on the conclusions drawn in 5.2 and 5.3 above, we will report to you whether the assertions made by you in respect of [name of CA]'s [capability to comply with] [compliance with] the provisions of the Ordinance applicable to a recognized CA [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx] are reasonable.

5.5 We will attach a copy of the management assertions letter provided to us as an appendix to our assessment report.

Financial projections

5.6 We will report on [name of CA]'s financial projections, including half- yearly cashflow projections and financial position forecasts for the next 12 months, and a projection of operating costs for the next 90 days from the commencement date of the above cashflow projections and financial position forecasts, which will have been prepared by you, particularly stating:

a. the period covered by the financial projections;

b. whether in our opinion the accounting policies upon which the financial projections are based are consistent in all material respects with those normally adopted by [name of CA] and conform with [generally accepted accounting principles adopted in Hong Kong] [International Accounting Standards]; and

c. whether in our opinion the financial projections have been properly compiled on the basis of the assumptions made by you.

5.7 We will include an appropriate comment in our assessment report if, based on our experience and professional judgement, any assumptions made, or omitted to be made, by you appear to be unrealistic or inappropriate.

5.8 We will attach a copy each of the financial projections prepared by you as an appendix to our assessment report.

5.9 We will present in our assessment report the result of the comparison of the following as ascertained from [name of CA]:

a. the amount of net current assets (i.e. current assets less current liabilities) as shown in the [audited financial statements/unaudited management accounts] of [name of CA] for the [year/period] ended xx/xx/xxxx; and

b. the projection of operating costs in respect of [name of CA]'s operations relevant under the Ordinance for the next 90 days from xx/xx/xxxx being the start date of the 12-month financial projections prepared by [name of CA].

5.10 We will attach a copy of the [audited financial statements/unaudited management accounts] of [name of CA] for the [year/period] ended xx/xx/xxxx provided to us by [name of CA] as an appendix to our assessment report.

[5.11 We will not carry out any verification work on the unaudited management accounts of [name of CA] for the [year/period] ended xx/xx/xxxx.]

Potential liabilities

5.12 We will provide an assurance as to the reasonableness of your assertions that you [will implement and maintain] [have implemented and maintained] appropriate procedures to determine and manage [name of CA]'s potential liabilities in relation to the issue of certificates.

5.13 We will reproduce as an appendix to our assessment report the information ascertained from you in respect of:

a. potential liabilities of [name of CA] in relation to issued certificates at the time of the review;

b. details of insurance cover or other appropriate cover for the liabilities including details of the insurer such as the insurer's registration name and address;

c. any claims [name of CA] has received from subscribers and/or relying parties since the date of the last assessment and the status of these claims; and

d. any claims which have been filed against the insurance policies of [name of CA] since the date of the last assessment.

We are under no obligation to perform procedures to confirm the completeness of the above information nor to provide an assurance on its completeness.

Management representations

6.1 As part of our assessment procedures, we may request you to provide written confirmation of certain oral representations which we may receive from you and your staff during the course of the assessment on matters having a material effect on our assessment report. In connection with representations and the supply of information to us generally, you are responsible for the accuracy and completeness of any information or documentation provided to us. We bring to your attention that it is an offence under section 47 of the Ordinance for a person to knowingly or recklessly make, orally or in writing, sign or furnish any declaration, return, certificate or other document or information required under the Ordinance which is untrue, inaccurate or misleading.

Limitation of work

7.1 Control procedures designed to address specific management assertions are subject to inherent limitations, and accordingly, errors, irregularities or system control weaknesses may occur and not be detected. Although we will plan our assessment so that we will have a reasonable expectation of detecting material exceptions such as incidents of non-compliance with the provisions of the Ordinance applicable to a recognized CA and the Code of Practice (including those resulting from fraud, errors or non-compliance with law or regulations), our assessment should not be relied upon to disclose all such material exceptions including fraud, errors, system control weaknesses and instances of non-compliance which may exist.

7.2 The purpose of this engagement is to conduct an assessment of [name of CA]'s [capability to comply with] [compliance with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice. Accordingly, we will not provide an assurance on the design or operational effectiveness of the control procedures that you have in place, other than their [capability to comply with] [compliance with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice.

7.3 You are responsible for the preparation of the projections and forecasts and for ensuring the reasonableness of the underlying assumptions. Where we suggest making adjustments to these forecasts and projections, these relate solely to errors we have noted, or to contingencies or amendments which we consider appropriate and shall in no way reduce your overall responsibility. Further, you will retain the right to decide on whether or not to accept any of our recommendations.

7.4 Financial projections and the assumptions upon which the projections are based are future oriented and may be affected by unforeseen events. Therefore, the projections cannot be relied upon to the same extent as information derived from the audited financial statements for prior accounting periods, and we can provide no assurance as to how closely the actual outcome will correspond to the forecasts and projections.

7.5 Furthermore our assurance will be based on historical information, and the projections of any information or conclusions contained in our assessment report to any future periods are subject to the risk that changes in procedures or circumstances may alter their validity.

Limitation of liability

8.1 We will not be liable for any loss or damage caused by, or arising from, any fraudulent acts, misrepresentation or wilful default on the part of [name of CA], its directors, employees or agents.

8.2 *Members would set out any general limitation of liability [Insert members' guidance]. For example:*

Any liability of the Firm, its [Partners] [Directors] and staff from actions found against us to pay damages for losses arising as a direct result of breach of contract or negligence on our part in respect of services provided in connection with or arising out of the engagement set out in this letter (or any variation of addition thereto), whether in contract, negligence or otherwise shall in no circumstances exceed $[ ] in aggregate: such amount including all legal and other costs which we may incur in defending any actions against us. The foregoing shall not exclude or restrict liability (if it would otherwise but for the foregoing have arisen) for death or personal injury caused by the negligence (as defined in section 2 of the Control of Exemption Clauses Ordinance) of the Firm, its [Partners][Directors] or staff.

Fees

9.1 Our fees will be based on the degree of skill involved, the experience of staff engaged and the time necessarily occupied in the work, plus out-of-pocket expenses.

Agreement of terms

10.1 We shall be grateful if you could confirm in writing your agreement to these terms by signing and returning the enclosed copy of this letter, or inform us if they are not in accordance with your understanding of the terms of engagement.

Yours faithfully
ABC & Co.

_____

We agree to the terms of this letter.

.....
[Director, for and on behalf of the board of [name of CA]]
[Date]

Appendix 2 : Example assessment report for engagements under either section 20(3)(b) or section 43(1) of the Electronic Transactions Ordinance

(revised and effective from 26 February 2002)

[The Board of Directors]
[Name of CA]
[Address of CA]

[Date]
Our ref:

Dear Sirs

Assessment Report of [name of CA] under [section 20(3)(b)] [section 43(1)] of the Electronic Transactions Ordinance

Objective of our assessment

1.1 The objective of the assessment is to enable us to draw a conclusion for the purposes of [section 20(3)(b)] [section 43(1)] of the Electronic Transactions Ordinance ("Ordinance"), as to whether, in all material respects, [name of CA] [is capable of complying with] [has complied with] the provisions of the Ordinance applicable to a recognized Certification Authority ("CA") and the "Code of Practice for Recognized Certification Authorities" issued by the Director of Information Technology Services ("Director") under section 33 of the Ordinance ("Code of Practice") published in January 2000 and updated in March 2001 [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx].

Use of this report by [name of CA]

2.1 This report is intended solely for [name of CA] to file with the Director in accordance with [section 20(3)] [section 43] of the Ordinance. This report may not be provided by [name of CA] to third parties for any other purpose without our prior written consent.

2.2 It is acknowledged that, under section 43(3) of the Ordinance, the Director must publish in the certification authority disclosure record for [name of CA] the date of this report and the material information in this report, and under section 31(2) of the Ordinance, the Director must publish in the certification authority disclosure record information regarding [name of CA] relevant for the purposes of the Ordinance. It is also acknowledged that, accordingly, [name of CA] may be asked by the Director to grant him an express waiver of confidentiality and an express copyright licence enabling him to publish the material information in this report. We acknowledge that [name of CA] has the right to grant such a waiver of confidentiality and copyright licence to the Director, and that there is no breach of any duty of confidence owed by [name of CA] to us and no infringement of our copyright of this report by [name of CA] if [name of CA] grants such a waiver of confidentiality and copyright licence to the Director for the purpose of section 31(2) or 43(3) of the Ordinance.

Responsibilities of management

RCA practices

3.1 As management of [name of CA], for the purposes of [its application for recognition] [its continuing/renewal of recognition] as a recognized CA as defined under the Ordinance, you are responsible for ensuring that [name of CA] [is capable of complying with] [has been complying with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice, and with the policies and business practices specified in [name of CA]'s Certification Practice Statement(s) ("CPS(s)"). These responsibilities include:

a. disclosure of [name of CA]'s business practices in its CPS(s) in accordance with the Ordinance and the Code of Practice and provision of its services in accordance with its disclosed business practices;

b. the design, implementation and maintenance of a trustworthy system and the overall control framework surrounding the trustworthy system to support [name of CA]'s operations; and

c. compliance with the requirements in respect of the recognition of [name of CA]'s certificates

3.2 It is also your responsibility to provide us with a management assertions letter that [name of CA] [is capable of complying with] [has complied with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice.

Financial projections

3.3 You are also responsible for preparing [name of CA]'s financial projections in respect of the CA's operations relevant under the Ordinance, including cashflow projections and financial position forecasts prepared in half-yearly intervals for the next 12 months, and a projection of operating costs for the next 90 days from the commencement date of the above cashflow projections and financial position forecasts.

Potential liabilities

3.4 It is your responsibility to provide us with the information regarding the potential liabilities of [name of CA] in relation to the issue of certificates at the time of the review, details of insurance cover or other appropriate cover for the liabilities including details of insurers such as the insurer's registration name and address, any claims [name of CA] has received from subscribers and/or relying parties since the date of the last assessment and the status of these claims, and any claims which have been filed against the insurance policies since the date of the last assessment.

Basis of conclusion

4.1 Our assessment has been conducted in accordance with Practice Note 870 "The assessments of Certification Authorities under the Electronic Transactions Ordinance" issued by the Hong Kong Institute of Certified Public Accountants.

4.2 This assessment comprises three parts:

RCA practices

a. the review of the reasonableness of the management assertions in respect of [name of CA]'s [capability to comply with] [compliance with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx], which have been attached as appendix [w] to this assessment report. Specifically, the following RCA practices have been considered:

i. [name of CA]'s [capability to disclose] [disclosure of] its business practices in its CPS(s) and [capability to provide] [provision of] its services in accordance with its disclosed business practices;

ii. [name of CA]'s [capability to comply with] [compliance with] the requirements in respect of the use of a trustworthy system to support its operations; and

iii. [name of CA]'s [capability to comply with] [compliance with] the requirements in respect of the recognition of its certificates;

Financial projections

b. the review of [name of CA]'s financial projections in respect of its operations relevant under the Ordinance prepared by management, including half-yearly cashflow projections and financial position forecasts for the next 12 months, and a projection of operating costs for the next 90 days from the commencement date of the above cashflow projections and financial position forecasts, which are attached as appendix [x] to this assessment report;

c. the comparison of the following as ascertained from [name of CA]:

i. the amount of net current assets (i.e. current assets less current liabilities) as shown in the [audited financial statements/unaudited management accounts] of [name of CA] for the [year/period] ended xx/xx/xxxx; and

ii. the projection of operating costs in respect of [name of CA]'s operations relevant under the Ordinance for the next 90 days from xx/xx/xxxx being the start date of the 12-month financial projections prepared by [name of CA]; and

Potential liabilities

d. the review of the arrangements [to be put in place] [put in place] by [name of CA] to cover any liability that may arise from its activities that fall within the scope of the Ordinance and the Code of Practice.

Inherent limitations

5.1 Control procedures designed to address specific management assertions are subject to inherent limitations, and accordingly, errors, irregularities or system control weaknesses may occur and not be detected. Although we planned our assessment so that we had a reasonable expectation of detecting material exceptions such as incidents of non-compliance with the provisions of the Ordinance applicable to a recognized CA and the Code of Practice (including those resulting from fraud, errors or non-compliance with law or regulations), our assessment should not be relied upon to disclose all such material exceptions including fraud, errors, system control weaknesses and instances of non-compliance which may exist.

5.2 In addition to this, the projection of any conclusions, based on our findings [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx], to future periods is subject to the risk that changes will be made to systems and/or controls to allow for changes in business or other requirements. The validity of projecting any conclusions in light of the possibility of such changes must be considered.

5.3 The cashflow projections, financial position forecasts, projection of operating costs and information regarding potential liabilities in relation to the issue of certificates of [name of CA] were prepared by and are the responsibility of management. These projections relate to future events and are based on management's assumptions which may not remain valid throughout the period of the projections. Consequently, the projections cannot be relied upon to the same extent as information derived from the audited financial statements for prior accounting periods. For these reasons, we provide no assurance as to how closely the actual cashflows, financial positions and operating costs achieved will correspond to the projections.

5.4 The purpose of this engagement is to conduct an assessment of [name of CA]'s [capability to comply with] [compliance with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice. Accordingly, we will not provide an assurance on the design or operational effectiveness of the control procedures that you have in place, other than their [capability to comply with] [compliance with] the provisions of the Ordinance applicable to a recognized CA and the Code of Practice.

Exceptions

6.1 Members would set out any exceptions noted during the assessment including incidents of non-compliance with the provisions of the Ordinance applicable to a recognized CA and the Code of Practice. A detailed discussion of the exceptions may be included as an appendix to the assessment report.

Conclusions

RCA practices

7.1 [Except for the exceptions noted above], in our opinion, in all material respects,

a. the management assertions in respect of [name of CA]'s [capability to comply with] [compliance with] the sections of the Code of Practice set out in Part 3A of Appendix 3 to Practice Note 870 [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx] are reasonable. In particular, [name of CA] [is capable of] [has]:

i. [disclosing] [disclosed] its business practices in its CPS(s) in accordance with the Ordinance and the Code of Practice and [providing] [provided] its services in accordance with its disclosed business practices;

ii. [complying with] [complied with] the requirements in respect of the use of a trustworthy system to support its operations in accordance with section 37 of the Ordinance and the Code of Practice; and

iii. [complying with] [complied with] the requirements in respect of recognition of its certificates in accordance with sections 36, 38, 39 and 40 of the Ordinance and the Code of Practice;

b. no information came to our attention during the course of the assessment that would indicate that the management assertions in respect of [name of CA]'s [capability to comply with] [compliance with] the sections of the Code of Practice set out in Part 3B of Appendix 3 to Practice Note 870 [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx] are not reasonable; and

c. based on the conclusions drawn in 7.1a. and b. above, the management assertions in respect of [name of CA]'s [capability to comply with] [compliance with] the provisions of the Ordinance applicable to a recognized CA [as at the date of assessment, xx/xx/xxxx] [for the period xx/xx/xxxx to xx/xx/xxxx] are reasonable.

Financial projections

7.2 [Except for the exceptions noted above], in our opinion, in all material respects, the accounting policies upon which [name of CA]'s cashflow projections and financial position forecasts for the period xx/xx/xxxx to xx/xx/xxxx, and projection of operating costs for the period xx/xx/xxxx to yy/yy/yyyy, in respect of the CA's operations relevant under the Ordinance are based, are consistent with those normally adopted by [name of CA] and conform with [generally accepted accounting principles adopted in Hong Kong] [International Accounting Standards], and the financial projections have been properly compiled on the basis of the assumptions made by management of [name of CA].

7.3 It has been ascertained from [name of CA] that the amount of net current assets (i.e. current assets less current liabilities) as shown in the [audited financial statements/unaudited management accounts] of [name of CA] for the [year/period] ended xx/xx/xxxx *(the commencement date of the cashflow projections and financial position forecasts referred to in paragraph 7.2 above)* was $X.

7.4 It has been ascertained from [name of CA] that the 90-day projection of operating costs referred to in paragraph 7.2 above was $Y.

7.5 A comparison of the figures in paragraphs 7.3 and 7.4 above reveals that $X [exceeds/does not exceed] $Y.

[7.6 We have not carried out any verification work on the unaudited management accounts of [name of CA] for the [year/period] ended xx/xx/xxxx].

7.7 Copies of the [audited financial statements/unaudited management accounts] and the 90-day projection of operating costs of [name of CA] referred to in paragraphs 7.3 and 7.4 above respectively are attached in appendices [x] and [z] to this assessment report.

Potential liabilities

7.8 [Except for the exceptions noted above], in our opinion, in all material respects, the management assertions that [name of CA] [will implement and maintain] [has implemented and maintained] appropriate procedures to determine and manage its potential liabilities in relation to the issue of certificates are reasonable.

Information obtained

8.1 The information relating to potential liabilities in relation to the issue of certificates by [name of CA], details of insurance cover or other appropriate cover for the liabilities including details of insurers such as the insurer's registration name and address, any claims [name of CA] has received from subscribers and/or relying parties since the date of the last assessment and the status of these claims, and any claims which have been filed against the insurance policies of [name of CA] since the date of the last assessment as was ascertained from management of [name of CA] is reproduced as appendix [y] to this assessment report. We do not provide an assurance on this information as we have not verified its accuracy or completeness.

ABC & Co.
Certified Public Accountants (Practising) [or Certified Public Accountants]
Hong Kong

Appendix [x]: Financial projections of [name of CA]

A. Cashflow projections

	CA operations projections 6 months to xx/xx/xxxx	CA operations projections 6 months to xx/xx/xxxx
	HK$'000	HK$'000
Operating activities		
Net cash inflow from CA business	x	x
Returns on investments and servicing of finance		
Interest received	x	x
Interest paid	(x)	(x)
Interest element of finance lease rental payments	(x)	(x)
Net cash outflow from returns on investments and servicing of finance	(x)	(x)
Taxation		
Hong Kong profits tax paid	(x)	(x)
Investing activities		
Purchase of fixed assets	(x)	(x)
Sale of fixed assets	x	x
Payment for deferred development costs	(x)	(x)
Net cash outflow from investing activities	(x)	(x)
Net cash outflow before financing	(x)	(x)
Financing		
Repayments of amounts borrowed	(x)	(x)
Capital element of finance lease rental payments	(x)	(x)
Net cash outflow from financing	(x)	(x)
Increase/(decrease) in cash and cash equivalents	x	(x)
Cash and cash equivalents at xx/xx/xxxx	x	x
Cash and cash equivalents at xx/xx/xxxx	x	x

Analysis of the balances of cash and cash equivalents:

Bank balances and cash	x	x
Bank overdrafts	(x)	(x)
	x	x

B. Financial position forecasts

	CA operations forecasts as at xx/xx/xxxx	CA operations forecasts as at xx/xx/xxxx
	HK$'000	HK$'000
Non-current assets		
Property, plant and equipment	x	x
Deferred development costs	x	x
Current assets		
Trade and other receivables	x	x
Bank balances and cash	x	x
	x	x
Current liabilities		
Trade and other payables	x	x
Taxation payable	x	x
Bank loans and overdrafts	x	x
	x	x
Net current assets	x	x
Total assets less current liabilities	x	x
Non-current liabilities	x	x
Net assets	x	x
Capital and reserves		
Share capital	x	x
Reserves	x	x
	x	x

C. 90-day projection of operating costs

*
*
*
*
*
*

D. Principal assumptions for the cashflow projections and financial position forecasts

Note: This is not an exhaustive list of assumptions. Members would include assumptions made in additional areas as appropriate.

			Management assumptions for the first six months	Management assumptions for the second six months
Gross Revenue		- Certificates - Other		
Costs	- staff - occupancy - insurance - equipment / systems - maintenance - other costs - interest			
Unusual or infrequently occurring items				
Discontinuing operations				
Trade debtors				
Trade creditors				
Sundry debtors & creditors				
Taxation				
Investments				
Fixed assets				
Loans & finance leases				

*
*
*
*
*
*

E. Principal assumptions for the 90-day projection of operating costs

*
*
*
*
*
*

Appendix [y]: Information obtained from [name of CA] relating to potential liabilities in relation to the issue of certificates and insurance cover

*
*
*
*
*
*

Appendix [z]: [audited financial statements/unaudited management accounts] of [name of CA] for the [year/period] ended xx/xx/xxxx provided by [name of CA]

*
*
*
*
*
*

Appendix 3 Requirements of the Code of Practice

This appendix provides a summary of the requirements with which members are required to provide a positive, negative or no assurance on the RCA's compliance. Members are recommended to refer to the Code of Practice for the complete requirements.

A. Sections of the Code of Practice where a positive assurance is provided

Members would obtain management assertions and provide a positive assurance on the RCA's compliance with the following requirements:

Applicable sections	Descriptions	Requirements
A-1 General responsibilities of a RCA		
3.1	General responsibilities of a RCA	A RCA shall comply with the conditions attached by the Director of Information Technology Services ("the Director") to the recognition granted under section 21 or renewed under section 27 of the Ordinance.
3.2	General responsibilities of a RCA	A RCA may appoint agents or subcontractors to carry out some or all of its operations provided that: ■ the agents or subcontractors are equally capable of complying with the Code of Practice relevant to their operations, and ■ the RCA is and remains responsible for the activities of its agents or subcontractors in the performance or purported performance by them of the functions, powers, rights and duties of the RCA under the Ordinance.
3.4	General responsibilities of a RCA	A RCA shall furnish the Director with a copy of its certification authority certificate (CA certificate) which the Director shall publish in the certification authority disclosure record maintained by the Director for that CA.
3.5	General responsibilities of a RCA	Where the Code of Practice requires a RCA to log, record, retain or archive information and records, the RCA shall do so for a period of at least 7 years or such longer or shorter period as may be specified by the Director and in a manner that ensures the security, integrity and accessibility of the information and records for retrieval and inspection.
3.8	General responsibilities of a RCA	If a RCA issues to the public both recognized certificates and certificates not recognized by the Director, the RCA shall publicize the fact that it issues these two categories of certificates.
A-2 Certification practice statement (CPS)		
4.1	CPS	A RCA shall publish for public knowledge and maintain one or more up to date CPS for the types, classes or descriptions of recognized certificates that it issues.

4.2	CPS	A RCA shall state in its CPS(s) the liabilities, limitations on liability, rights and obligations of the RCA, its subscribers and persons who rely on the certificates issued by the RCA, and the significance of its reliance limit on its certificates. A RCA shall: ■ specify separately as appropriate such information in any contract with its subscribers; and ■ make such information available, both in printed form and in electronic form via an on-line and publicly accessible means.
4.3	CPS	A RCA shall provide up to date information in its CPS(s) concerning the recognition status of the types, classes or descriptions of recognized certificates that the RCA issues.
4.4	CPS	A RCA shall draw the attention of its subscribers and persons who may rely upon those of its certificates which are not recognized certificates to the significance of using and relying upon those certificates.
4.5	CPS	A RCA shall draw the attention of its subscribers to the extent that their personal information will become public information when such information is incorporated in recognized certificates issued by the RCA to the subscribers and published in a repository of the RCA. Its CPS(s) shall state clearly the contents of the relevant recognized certificates.
4.6	CPS	A RCA shall submit a copy of its CPS(s) to the Director upon publication of the CPS(s), and notify the Director in writing of any subsequent changes to the CPS(s) as soon as practicable. A RCA must also record all changes made to the CPS(s) together with the effective date of each change as soon as practicable.
4.8	CPS	A RCA shall retain a copy of each version of the CPS(s) it has issued, together with the date the CPS(s) come into effect and the date the CPS(s) cease to have effect if applicable.
4.9	CPS	A RCA shall, when issuing a type, class or description of recognized certificates, comply with the CPS for that type, class or description of recognized certificates.
4.10	CPS	A RCA shall ensure that its CPS(s) are readily available in its on-line and publicly accessible repository. The repository shall be promptly updated when there are changes to the CPS(s).
4.12	CPS	The RCA shall consult the Director in respect of the effect of the intended material change to its CPS on the recognition status of the types, classes or descriptions of recognized certificates that the RCA issues. Examples of material change to a CPS include without limitation: (a) changes in the identification process that weaken the reliability of the recognized certificates; (b) changes in the reliance limit of the recognized certificates; or (c) changes in the key generation, storage, or usage procedures.

4.13	CPS	A RCA shall notify any incident that adversely and materially affects the validity of the whole or any part of its CPS to the irector, its subscribers and relying parties immediately. The RCA shall take immediate action to address the incident. The esolutions in respect of the incident shall be reflected as soon as practicable in the CPS, published on-line on the RCA's epository and reported to the Director.
A-3 Trustworthy system		
5.1	Trustworthy system	A RCA shall use a trustworthy system in performing its services, including the generation and management of its keys, the generation and management of subscribers' keys if appropriate, the issuance, renewal, suspension or revocation of recognized certificates, the giving of notice of the issuance, renewal, suspension or revocation of recognized certificates, the provision of a repository, and the publication of recognized certificates and other information in the repository.
5.6	Trustworthy system	In relation to security sensitive functions, the RCA is expected to adopt systems and procedures that meet such standards as are widely accepted or recognized world-wide. In addition, a RCA shall perform structured assessments to ascertain the underlying risks of its operations, and implement appropriate counter-measures for managing, mitigating and monitoring such risks.
5.7	Trustworthy system	A RCA operating in a public key infrastructure (PKI) shall make use of any hardware, software and cryptographic components. These components shall be supported by appropriate security policies and procedures in order to ensure that the RCA operates in a secure environment.
5.9	Generally accepted security principles	A RCA shall develop, establish, maintain and update documented and approved policies, procedures and practices over its operational environment, including but not limited to the areas discussed in the following sub-paragraphs.
5.9.1	Generally accepted security principles	A RCA shall develop, establish, maintain, update and enforce adequate and proper security control over its operation in accordance with generally accepted security principles which must cover the aspects set out in the sub-sections below as a minimum.
5.9.1(a)(i)	Asset classification and management	A RCA shall classify its assets properly and identify the owner(s) of its major assets. The RCA shall maintain an up to date and complete inventory of its assets, and establish procedures to safeguard its assets.
5.9.1(a)(ii)	Asset classification and management	The RCA shall treat the information that it maintains as one of its assets and classify such information in accordance with the degree of importance to the business operations. Appropriate controls shall be established to secure such information from unauthorised access or damage.
5.9.1(b)(i)	Personnel security	A RCA shall develop, establish, maintain and update effective controls over personnel security including: ■ defining roles and responsibilities within formal job descriptions; ■ performing verification checks on its personnel; and ■ incorporating confidentiality or similar clauses in employment contracts.

5.9.1(b)(ii)	Personnel security	A RCA shall provide appropriate and adequate training to its personnel to maintain their competency and ensure effective implementation of and compliance with its security policies. Training may include: ■ appropriate technical training; ■ organisational policies and procedures; and ■ defined procedures to deal with security incidents.
5.9.1(b)(iii)	Personnel security	A RCA shall establish appropriate controls to monitor the performance of its personnel including: ■ regular performance reviews; ■ formal disciplinary procedures; and ■ formal termination procedures.
5.9.1(c)	Physical and environmental security	A RCA shall maintain effective physical and environmental security controls including: ■ identifying and defining secure areas, and implementing security controls; ■ establishing formal procedures for staff and visitors' access; ■ establishing access monitoring mechanisms; ■ establishing environmental controls; ■ establishing general security controls; and ■ ensuring maintenance and review of environmental controls.
		Where a RCA relies on services provided by third parties for the protection of physical and environmental security, such services shall be stated in formal service agreements established with these third party suppliers.
5.9.1(d)	Management over systems access	A RCA shall develop, establish, maintain and update effective controls and procedures over access to its information and application systems including: ■ establishing proper business requirements for controlling access to systems; ■ establishing formal user responsibilities; ■ establishing formal procedures for the management of user identification profiles and monitoring of access to its systems; ■ establishing proper controls over access to networks, operating and applications systems; ■ establishing controls over the monitoring of system access and usage; ■ establishing controls over mobile computing and teleworking; ■ establishing controls against unauthorised or illegal usage of software; and ■ establishing procedures to deal with access security incidents.

5.9.2	Operational management	A RCA shall maintain effective controls and procedures in respect of its day-to-day operations. Operational policies and standard operating procedures shall be formalised and documented including: ■ clear definition of duties and responsibilities of its operational personnel; ■ regular capacity monitoring procedures; ■ proper procedures to protect its computer infrastructure against malicious programs; ■ proper procedures over systems and network management; ■ proper procedures over the handling, distribution, storage and disposal of electronic information and media; and ■ proper procedures for handling and resolving operational problems.
5.9.3	Development and maintenance of computer systems	A RCA shall develop, establish, maintain and update effective controls and procedures over system development and maintenance activities including: ■ establishing proper internal standards to ensure uniformity of development work; ■ procedures to ensure segregation of the production and development environments; ■ procedures to ensure segregation of duties between operational and development personnel; ■ controls over access to data and systems held in its production and development environments; ■ controls over change control process, including emergency changes to systems and/or data; and ■ procedures for the proper management in respect of the acquisition of equipment and services.
5.9.4	Continuity of business perations	A RCA shall develop, establish, maintain and update a business continuity plan that covers all critical aspects of its operations.
5.9.5	Continuity of business operations	The continuity plan shall be tested vigorously on a regular basis, involving relevant key personnel detailed in the plan.
5.9.6	Continuity of business operations	The continuity plan shall cover contingencies such as recovery from a compromise or suspected compromise of the RCA's private key used to sign subscriber certificates, or recovery from major failure of the RCA's systems or any of the components of the RCA's systems.
5.9.7	Maintenance of appropriate event journals	A RCA shall maintain adequate event journals, which includes the retention of documents related to the issuing and managing of recognized certificates by the RCA.
5.9.8	Maintenance of appropriate event journals	A RCA shall archive such event journals. The RCA shall also regularly review the event journals and take action against any exceptions identified.

5.9.9	Maintenance of appropriate event journals	A RCA shall maintain journals relating to all major events including: ■ access to materials and equipment used for key generation; ■ in respect of keys and certificates, their generation, issuance, distribution, storage, backup, suspension, revocation, withdrawal, archival, destruction, and other related events; ■ security incidents, including key compromise; and ■ procurement, installation, implementation, decommission and retirement of cryptographic devices.
5.9.10	Compliance monitoring and assurance	A RCA shall develop, establish, maintain and update appropriate controls to ensure compliance with applicable legal, regulatory and technical requirements including: ■ establishing an appropriate function to monitor all aspects of the operations of the RCA; ■ ensuring that its compliance monitoring function meets the current industrial standards and practices; and ■ arranging for appropriate review to be conducted over its operational systems.
5.10	Good Practices Specific to Functions of a RCA	A RCA shall develop, establish, maintain and update formal documented and approved policies, procedures and practices over specific functions of a RCA, without limitation the areas discussed in the sub-sections below.
5.10.1	Management of CPS(s)	A RCA shall disclose its business practices in its CPS(s) and maintain effective controls over its CPS(s) including without limitation: ■ forming a management committee with the authority and responsibility for determining and approving the contents of CPS(s),including any certificate policy or policies that are adopted by the RCA; ■ establishing effective procedures for the on-going review and updating of the CPS(s); and ■ making the CPS(s) available to its subscribers and persons who may rely on the recognized certificates issued by that RCA.
5.10.2	Legal and regulatory monitoring and compliance	A RCA shall maintain effective procedures to monitor and ensure compliance with all legal and regulatory requirements, including relevant provisions in the the Regulations thereunder and Ordinance, and the Code of Practice.
5.10.3	Key management	A RCA shall maintain effective procedures and controls over the generation, storage, backup, recovery, distribution, use, destruction, and archiving of the RCA's own keys including: ■ controls over the use of cryptographic modules for key generation; ■ operational controls over key generation; ■ controls over key storage, backup and recovery ■ controls over security for the key distribution process; ■ controls over the usage of the key; ■ controls to ensure the safe destruction of key pairs and any related devices; and

		■ controls for ensuring the archived keys meet the security and operational requirements stated in the CPS.
5.10.4	Management of key generating devices	A RCA shall maintain effective procedures and controls over the procurement, receipt, installation, acceptance tests, commissioning, usage, repair, maintenance, and retirement of key generating devices. Control examples include: ■ procedures for ensuring the integrity of the cryptographic module; ■ procedures for ensuring that the handling of key generating device is under proper supervision by authorised personnel; and ■ procedures for ensuring that the strength of keys generated using the cryptographic modules is of the appropriate strength.
5.10.5	Key management services provided by the RCA (where appropriate)	A RCA shall maintain effective procedures and controls over key management services, if any, provided by the RCA to its subscribers, such as key generation,storage, backup, recovery, destruction and archival. Such procedures and controls shall be consistent with the principles set out in sub-sections 5.10.3 and 5.10.4 of the Code of Practice above.
5.10.6	Lifecycle management of tokens (where appropriate)	A RCA shall maintain effective procedures and controls over the preparation, activation, usage, distribution, and termination of any tokens, such as smart cards, used by the RCA.
5.10.7	Certificate management	A RCA shall maintain effective procedures and controls over the management of certificates including: ■ verification of the identity of the person and the uniqueness of the person's distinguished name; ■ notification of the need for renewal of certifications; ■ open and common interface for the issuance of its recognized certificates; ■ performance monitoring against service levels; and ■ complaints handling.
5.10.8	Management of certificate revocation list	A RCA shall maintain effective procedures and controls over the management of its certificate revocation list. For example: ■ a RCA shall update its certificate revocation list in accordance with the policies, procedures and arrangements stated in its CPS; and ■ there shall be procedures to ensure that only authorised personnel have access to the repository and the certificate revocation list for their maintenance.
5.11	Key generation using a trustworthy system and keeping of records	A RCA shall provide a trustworthy system to generate the RCA's own and the subscriber's key pair.
5.12	Key generation using a trustworthy system and keeping of records	A RCA shall separately keep its own private key and the activation data (e.g. PINs, passwords, etc.) in a secure manner.

5.13	Key generation using a trustworthy system and keeping of records	A RCA shall make and retain records in respect of: ■ activities relating to the issuance, renewal, suspension and revocation of recognized certificates (including the identification documents of any person applying for a recognized certificate from the RCA); ■ the certificate revocation list; ■ the documents relating to the generation of the RCA's own key pair; ■ the documents relating to the generation of the subscriber's key pairs; and ■ the administration of the RCA's computer facilities.
5.14	Key generation using a trustworthy system and keeping of records	A RCA shall archive all recognized certificates issued by it and maintain mechanisms to access such certificates.
5.15	Digital signatures	The technical implementation for the creation of a digital signature shall be such that: (a) the digital signature shall only be created under the direction of the person to whom the digital signature relates; and (b) no other person can reproduce the digital signature and thereby create a valid digital signature without the involvement or the knowledge of the person to whom the digital signature relates.
5.19	Security and risk management	A RCA shall adopt a security policy in accordance with generally accepted security principles.
5.20	Security and risk management	A RCA shall establish a comprehensive security incident reporting and handling procedure, and disaster recovery set-up and procedure for its operation.
5.21	Security and risk management	A RCA shall adequately identify and establish procedures to deal with the risks associated with its operation. The RCA shall implement a risk management plan that will provide for the management of, including without limitation, the following incidents: ■ key compromise; ■ security breach of the system or network of the RCA; ■ unavailability of the infrastructure of the RCA; and ■ unauthorised generation of certificates and of certificate suspension and revocation information.
A-4 Certificates and recognized certificates		
6.1	Certificates and recognized certificates	A RCA may issue certificates recognized by the Director under section 22 of the Ordinance or certificates not recognized by the Director. Where a RCA issues both recognized and unrecognized certificates, it shall use separate private keys to sign the recognized and unrecognized certificates respectively.
6.2	Certificates and recognized certificates	Recognized certificates shall contain the necessary information to facilitate subscribers and persons who rely on the certificates to locate the associated CPS during the conduct of electronic transactions.

6.3	Issuance of certificates	A RCA may issue a recognized certificate to a person only after the CA: (a) has received a request for issuance of the recognized certificate from the person applying for such a certificate; and (b) has complied with all of the practices and procedures set out in the CPS including procedures regarding identity verification of the person in respect of that type, class or description of recognized certificates.
6.4	Issuance of certificates	A RCA shall provide a reasonable opportunity for the subscriber to verify the contents of the recognized certificate before accepting the certificate.
6.5	Issuance of certificates	A RCA shall publish recognized certificates that it issues and that are accepted by its subscribers in the on-line and publicly accessible repositories maintained by it or maintained for it by third parties.
6.6	Issuance of certificates	A RCA shall obtain the consent of the subscriber in respect of any personal information of the subscriber which the RCA intends to include in the certificate that is to be issued to the subscriber and to be listed in an on-line and publicly accessible repository.
6.7	Issuance of certificates	Once a recognized certificate has been issued by the RCA and accepted by the subscriber, the RCA shall notify the subscriber through all reasonable channels within a reasonable time of any fact known to the RCA that affects the validity or reliability of the recognized certificate.
6.8	Issuance of certificates	A recognized certificate shall state when its validity expires.
6.10	Issuance of certificates	All transactions related to the issuance of a recognized certificate including the date and time shall be recorded.
6.11	Suspension and revocation of recognized certificates	A RCA shall be able to revoke and may also be able to suspend recognized certificates in accordance with the following paragraph.
6.12	Suspension and revocation of recognized certificates	A recognized certificate shall contain or incorporate by reference necessary information to locate or identify the repository or repositories in which suspension or revocation notices of the recognized certificate will be published.
6.13	Suspension and revocation of recognized certificates	Unless a RCA and its subscriber otherwise agree, the RCA that issues a recognized certificate to the subscriber shall suspend or revoke the certificate within a reasonable time after receiving a request from: (a) the subscriber named or identified in the recognized certificate; or (b) a properly authorised person.
6.14	Suspension and revocation of recognized certificates	Within a reasonable time following suspension or revocation of a recognized certificate by a RCA, the RCA shall publish a signed notice of the suspension or revocation (e.g. certificate revocation list) in a repository maintained by it or by an outside organisation for the RCA.

6.15	Suspension and revocation of recognized certificates	The exact time of the revocation or suspension by the RCA as well as the allocation of liability for transactions using the certificate in the period between the receipt of the request for revocation or suspension and the time when the certificate is revoked or suspended shall be agreed between the RCA and the subscriber.
6.16	Suspension and revocation of recognized certificates	A RCA may temporarily suspend a recognized certificate that it has issued if the RCA has reasonable grounds to believe that the recognized certificate is unreliable, regardless of whether the subscriber consents to the suspension; but the RCA shall complete its investigation regarding the reliability of the recognized certificate and decide within a reasonable time period whether to reinstate the certificate or to revoke the certificate.
6.17	Suspension and revocation of recognized certificates	If the RCA considers that an immediate revocation of a recognized certificate issued by it is justified in the light of all the information available to it, the certificate shall be revoked, regardless of whether the subscriber has given consent to the revocation.
6.18	Suspension and revocation of recognized certificates	In the case of suspension requested by the subscriber or a properly authorised person, the RCA shall check with the subscriber or that properly authorised person whether the recognized certificate to be suspended shall be revoked or reinstated after suspension. The relevant CPS shall state the action to be taken in the event that it is not possible for the RCA to contact the subscriber or the properly authorised person for his instruction of whether the suspended certificate shall be revoked or reinstated after suspension.
6.19	Suspension and revocation of recognized certificates	Whenever a RCA suspends or revokes a recognized certificate which is issued by it, the RCA shall, within a reasonable time, notify the suspension or revocation of the recognized certificate and provide a record to the subscriber of the recognized certificate or the properly authorized person.
6.20	Suspension and revocation of recognized certificates	A RCA shall provide hotline or other facilities for subscribers to report to the RCA incidents affecting their certificates or private keys, for example, keys having been lost or compromised.
6.21	Suspension and revocation of recognized certificates	All transactions, including the date and time, in relation to suspension or revocation of certificates shall be recorded.
6.22	Renewal of recognized certificates	A recognized certificate is subject to renewal upon expiry of its validity at the request of the subscriber and the discretion of the RCA.
6.23	Renewal of recognized certificates	All transactions including the date and time in relation to the renewal of a recognized certificate shall be recorded.
A-5 Verification of subscriber's identity		
7.1	Verification of subscriber's identity	A RCA shall specify in the relevant CPS that corresponds to a particular type, class or description of recognized certificates the procedure to verify the identity of a person who applies for such a recognized certificate from the RCA.
7.2	Verification of subscriber's identity	A RCA shall retain copies of the documentary evidence that identifies its subscribers.

A-6 Reliance limit		
8.1	Reliance limit	In issuing a type, class or description of recognized certificates to subscribers, a RCA may specify in the relevant CPS that corresponds to that type, class or description of certificates a reliance limit on the certificates. The RCA shall specify in the relevant CPS the significance of the reliance limit on the use of the recognized certificates.
8.2	Reliance limit	A RCA shall arrange suitable insurance or other forms of cover to ensure that it is capable of covering its liability for claims up to the reliance limit set for the recognized certificates that it issues.
A-7 Repositories		
9.1	Repositories	A RCA shall make available at least one on-line and publicly accessible repository for the publication of recognized certificates and related information. The RCA shall ensure that its repository or repositories are implemented through trustworthy systems. The RCA shall state in its CPS(s) the service levels in respect of the operation of its repository or repositories.
9.3	Repositories	A repository of a RCA shall contain : ■ recognized certificates issued by the RCA; ■ suspension or revocation notices of its recognized certificates (including certificate revocation lists as appropriate); ■ the CA disclosure record for that RCA; and ■ other information as specified by the Director.
9.5	Repositories	A RCA shall keep in its repository an archive of recognized certificates that have been suspended or revoked, or that have expired within at least the previous seven years.
A-8 Disclosure of information		
10.1	Disclosure of information	A RCA shall publish in its repository or repositories: (a) its CA certificate that contains the public key corresponding to the private key used by the RCA to digitally sign recognized certificates it issues; (b) the suspension, revocation or non-renewal notice of its CA certificate or recognition granted by the Director; and (c) any other fact that materially and adversely affects either the reliability of a recognized certificate that the RCA has issued or its ability to perform its services relevant under the Ordinance.
10.2	Disclosure of information	A RCA shall inform the Director of any changes in the appointment of responsible officers or any person who performs functions equivalent to that of a responsible officer within 3 working days from the date of appointment of that person.
10.3	Disclosure of information	A RCA shall submit progress reports to the Director at 6-month intervals containing information with regard to: (a) the number of its subscribers classified by type, class or description of certificates; (b) the number of certificates issued, suspended, revoked, expired and renewed by type, class or description of certificates;

		(c) its performance compared with its stated service levels; (d) new types, classes or descriptions of certificates issued; (e) changes in its organisational structure or systems; (f) actions taken by the RCA to address recommendation(s) made in the assessment report which is prepared and submitted to the Director under section 20(3)(b) or 43(1) of the Ordinance; and (g) any changes related to the above items since the preceding progress report was submitted or since the application for recognition or renewal as a RCA
A-9 Termination of service		
11.1	Termination of service	A RCA shall submit to the Director a termination plan when the RCA applies for recognition as a RCA or renewal of its recognition.
11.2	Termination of service	The termination plan shall specify the arrangements for the termination of the of service RCA's service, especially the arrangement for its records, including the certificates which it has issued and its CA certificate, to be archived for not less than 7 years.
11.3	Termination of service	The termination plan shall cover both voluntary and involuntary termination of the RCA's service including the expiry or revocation of the recognition granted by the Director to the RCA. The termination plan shall also include measures to ensure that the interests of the subscribers are safeguarded upon termination of the RCA's service.
11.4	Termination of service	Any CPS published by a RCA must refer to the termination plan of the RC
A-10 Assessment of compliance with the Ordinance and the Code of Practice		
12.1	Assessment of compliance with the Ordinance and the Code of Practice	At least once in every 12 months, a RCA shall submit to the Director a report containing an assessment as to whether the RCA has complied with the provisions of the Ordinance applicable to a RCA and the Code of Practice.
12.6	Assessment of compliance with the Ordinance and the Code of Practice	A copy of the assessment report shall be submitted to the Director by the RCA within 4 weeks of the completion of the assessment, together with management's response to any recommendation raised by the assessor to the RCA as a result of the assessment. In the event that a RCA applies for renewal of recognition to the Director, the RCA shall submit a complete report of such assessment which is completed within three months prior to the date of the application for renewal by the RCA.
A-11 Inter-operability		
14.2	Inter-operability	A RCA shall state in its CPS(s) the open and common interfaces that it supports and any inter-operability that it has established with other CAs.
A-12 Appendix		
All sections	Appendix	Standards and procedures regarding the contents of CPS.
The assessor would review the RCA's CPS to assess whether it complies with the minimum requirements specified in the appendix to the Code of Practice.		

B. Sections of the Code of Practice where a negative assurance may be provided

Members would obtain management assertions for the RCA's compliance with the requirements below. A negative assurance may be provided on the RCA's compliance with the following sections of the Code of Practice:

Applicable sections	Requirements
B-1 General responsibilities of a RCA	
3.3	A RCA shall take all reasonable care in issuing certificates to its subscribers and shall take all reasonable care to persons who may rely upon these certificates.
3.6	A RCA shall comply with all applicable regulations regarding the privacy of personal information.
3.7	A RCA shall refrain from engaging in restrictive practices that impair economic efficiency or free trade.
3.9	A RCA shall take care of the needs of persons with disabilities in the provision of its services in accordance with all applicable ordinances and regulations regarding the prevention of any discriminatory practice against any person with disabilities.
B-2 Trustworthy system	
5.16	If there is an incident which materially and adversely affects a RCA's trustworthy system or the integrity of its recognized certificates, the RCA shall: ■ inform the Director immediately in respect of the incident; ■ use all reasonable endeavours to notify all persons who are or who will be affected by that incident; and ■ act in accordance with the procedures, if any, specified in the CPS governing such an incident.
5.17	RCAs shall ensure that all its personnel possess the necessary knowledge, technical qualifications and expertise to effectively carry out their duties.
5.18	RCAs shall ensure that all its responsible officers and those officers with trusted roles such as security officers, CA administrators, privileged system operators, registration personnel, and any other personnel that have access to key material, cryptographic modules, or activity event logs shall be fit and proper persons.
B-3 Repositories	
9.2	A RCA, in maintaining and managing a repository, shall not carry out any activity in a manner that creates an unreasonable risk to persons relying on the recognized certificates or other information contained in the repository.
9.4	A repository of a RCA shall not contain any information which the RCA knows to be inaccurate or unreliable.
B-4 Disclosure of information	
10.4	The RCA shall report to the Director immediately any material changes in the information set out in section 10.3 (see Part A-8).
10.5	A RCA shall report to the Director immediately when the RCA realises there is an event which may or will lead to potential conflict of interest in respect of the operation of the RCA.
10.6	A RCA shall report any incident that materially and adversely affects its operation to the Director immediately.

B-5 Termination of service	
11.5	Before a RCA's service is terminated, the RCA shall (a) inform the Director of its intention to terminate service at least 90 days before the termination of its service; (b) inform all its subscribers of its intention at least 60 days before the termination of its service; (c) advertise such intention in one English language daily newspaper and one Chinese language daily newspaper in circulation in the Hong Kong Special Administrative Region for at least three consecutive days at least 60 days before the termination of its service; (d) if considered necessary by the Director, make arrangements to revoke all certificates which remain not revoked or expired, regardless of whether the subscribers have requested for the revocation, when it terminates its service; and (e) make appropriate arrangements to effect an orderly transfer of information contained in the RCA's repository, including details of certificates issued by the RCA and the RCA's public key(s).
B-6 Adoption of standards and technology	
13.1	A RCA shall continuously review and, where appropriate, improve and update its standards and technology in order to uphold the confidence that its subscribers place in it and to protect the interests of the subscribers.
B-7 Inter-operability	
14.1	To reduce barriers for digital signatures supported by recognized certificates to be widely accepted, a RCA shall, wherever applicable, adopt an open and common interface to facilitate the verification by others of digital signatures supported by its recognized certificates.
B-8 Consumer protection	
15.1	The advertisement of services by a RCA shall be decent, honest and truthful. Comparative advertising shall be fair and not misleading. All claims shall be capable of independent substantiation.

C - Sections of the Code of Practice where no assurance is provided

This part lists the explanatory material contained in the Code of Practice. These sections provide additional explanations and would be read in conjunction with Parts A and B. These sections are statements of fact, and members would not provide any assurance on the RCA's compliance with them.

Applicable sections	Requirements
C-1 Introduction All sections in Introduction.	
C-2 Definition of terms All sections in Definition of terms.	
C-3 Certification Practice Statement	
4.7	If a RCA issues a type, class, or description of recognized certificates that are specified in a certificate policy, then the certificate policy will be considered as part of the CPS.
4.11	The standards and procedures regarding the contents of a CPS are set out in the appendix to the Code of Practice.
C-4 Trustworthy system	
5.2	The term 'system' refers to the system itself, i.e. hardware and software, as well as those control and operational procedures (both manual and automated) that are designed to ensure that the system will perform its intended functions in a consistent, reliable and dependable manner.
5.3	For a system to be accepted as trustworthy, a RCA shall demonstrate that the mechanisms, procedures, and conditions under which the system operates are adequate for the performance of its intended functions.
5.4	There is no absolute measure of trustworthiness. It can only be assessed against a specific context.
5.5	In accordance with the technology-neutral and minimalist regulatory approach adopted under the Ordinance, a RCA is free to determine the technical solutions to support its operations.
5.8	The manner in which a RCA achieves its objective in maintaining a trustworthy system may vary, depending on the kind of services to be provided by the RCA, the state of technology and the business environment. A RCA shall adhere to the generally accepted good practices in section 5.9.
C-5 Certificates and recognized certificates	
6.9	By issuing a recognized certificate, a RCA represents to any person who reasonably relies on the recognized certificate or a digital signature verifiable by a public key listed in the recognized certificate that the RCA has issued the recognized certificate in accordance with its applicable CPS.
C-6 Assessment of compliance with the Ordinance and the Code of Practice	
12.2	The RCA shall ensure that the report is prepared, at the expense of the RCA, by a qualified person approved by the Director for this purpose. In order to be considered as being qualified for preparing the assessment report, the person shall be: ■ independent of the RCA under assessment; ■ accredited by a recognized professional organisation or association; and ■ proficient in: - the assessment of public key infrastructure and related technologies, such as digital signature and certificate, etc;

	- applying information security tools and techniques; - performing financial reviews; - performing security reviews; and - performing third-party reviews.
12.3	The qualified person may be an individual possessing all of the above requirements, or a partnership of an organisation comprising individuals that collectively possess all of the above requirements. The individual signing the assessment report shall: ■ be a registered member of the recognized professional organisation or association, e.g. holding a valid practising certificate or attaining a similar status; ■ have overall responsibility for ensuring that the person(s) performing the assessment possess sufficient knowledge of the subject matter, such as digital signature and certificate, public key infrastructure, financial matters, etc.; and ■ have overall responsibility for ensuring the quality of the assessment and adherence to any standards or practices adopted for the purpose of performing such assessments.
12.4	For illustrative purposes, a Certified Public Accountant, i.e. a professional accountant with practising certificate issued under the Professional Accountants Ordinance (Cap. 50) who possesses or has available the technical expertise in information technology as set out in section 12.2, or alternatively a professional in the field of information technology who possess or has available technical expertise as set out in section 12.2, is considered acceptable for approval by the Director as the person to conduct the assessment. The Director is also prepared to assess the suitability of other persons as being qualified to conduct the assessment.
12.5	The professional organisation or association referred to in section 12.2 must have an established system to properly admit and regulate its members. The key features of such a system shall include without limitation: ■ rules and regulations that govern membership admission requirements, such as in respect of training, competency testing, fitness for membership; ■ rules and regulations that govern professional and ethical standards and guidelines to members that govern the performance of their professional services, such as in respect of conflict of interest, undertaking and accepting instructions; ■ mechanism for enforcing the professional and ethical standards and monitoring the conduct of members including without limitation formal disciplinary procedures, quality assurance measures such as peer reviews; and ■ mandatory continuing professional education requirement.
12.7	Failure to meet the requirements as stated in the Ordinance, the Regulations thereunder and the Code of Practice may be a ground for suspending or revoking the recognition granted by the Director to a RCA or for rejecting a RCA's application for renewal of its recognition by the Director.