# Guidance Note on Compliance Assessment of Certification Authorities under the Electronic Transactions Ordinance (Cap. 553)

**Published in July 2012**

**(Version 3.0)**

Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region

# Introduction

1. The information contained in this guidance note (version 3.0) does not form part of the Code of Practice for Recognized Certification Authorities ("Code of Practice") and it is not intended to affect your rights and obligations. It is not intended to be relied upon as a statement of the legal position and you should consult your legal adviser before acting upon the information. This guidance note (version 3.0) supersedes version 2.0 of the same document published in July 2004.

2. Under the Electronic Transactions Ordinance (Cap. 553) ("Ordinance"), assessment reports shall be furnished to the Government Chief Information Officer ("GCIO") in the following circumstances:

   (a) In accordance with section 20(3)(b) of the Ordinance, a certification authority ("CA") seeking recognition must furnish to the GCIO a report which contains an assessment as to whether the CA is capable of complying with such provisions of the Ordinance and of the Code of Practice as are specified in the Code of Practice (such provisions are specified under paragraph 1 of Appendix 2 of the Code of Practice);

   (b) In accordance with section 27(5A)(b) of the Ordinance, a recognized CA applying for renewal of recognition must furnish to the GCIO a report which contains an assessment as to whether the recognized CA is and is capable of complying with such provisions of the Ordinance and of the Code of Practice as are specified in the Code of Practice (such provisions are specified under paragraph 1 of Appendix 2 of the Code of Practice);

   (c) In accordance with section 43(1)(a) of the Ordinance, at least once in every 12 months, a recognized CA must furnish to the GCIO a report which contains an assessment as to whether the recognized CA has, for the period to which the report relates, complied with such provisions of the Ordinance and of the Code of Practice as are specified in the Code of Practice (such provisions are specified under paragraph 1 of Appendix 2 of the Code of Practice); and

   (d) In accordance with section 43A(1)(c) of the Ordinance, the GCIO may, in relation to major changes of a recognized CA, require the recognized CA to furnish to the GCIO a report which contains an assessment as to–

      – whether**,** having regard to the major changes that have occurred, the recognized CA is and is capable of complying; or

      – whether, having regard to the major changes that will occur, the recognized CA is capable of complying

      with such provisions of the Ordinance and of the Code of Practice as are specified in the Code of Practice (such provisions are specified under paragraph 3 of Appendix 2 of the Code of Practice).

Any such report must be prepared by a person approved by the GCIO as being qualified to make the report.

3. This document provides guidance on the scope and conduct of the assessment required under sections 20(3)(b), 27(5A)(b), 43(1)(a) or 43A(1)(c) of the Ordinance of a CA intending to seek recognition and a CA already recognized respectively, and is primarily aimed at:

   - the person referred to in sections 20(3)(b)(ii), 27(5A)(b)(ii), 43(1)(a)(ii) or 43A(1)(c)(ii) of the Ordinance who will prepare the assessment report;

   - recognized CAs who must furnish to the GCIO a report containing an assessment required under sections 27(5A)(b), 43(1)(a) or 43A(1)(c) of the Ordinance; and

   - CAs that are considering to apply for recognition under section 20(1) of the Ordinance.

   The ensuing paragraphs apply to an assessment required under sections 20(3)(b), 27(5A)(b) or 43(1)(a) of the Ordinance. In respect of an assessment required under section 43A(1)(c) of the Ordinance, the scope of the assessment will depend on the specific circumstances of the major changes that a recognized CA will make or has made to its systems, operation, controls and procedures. The ensuing paragraphs apply to an assessment required under section 43A(1)(c) of the Ordinance where they are relevant having regard to the scope of the assessment concerned.

## Scope of Assessment

4. The objective of the assessment is to determine:

   - whether, in all material respects, the CA under assessment is capable of, or has been complying with the requirements under relevant provisions of the Ordinance and the Code of Practice, as the case may be; and

   - whether, in all material respects, the CA has complied with the policies and business practices specified in its certification practice statement(s) ("CPS").

5. The assessment should cover the assertions made by the CA concerned on the CA's capability to comply or actual compliance with the relevant provisions under the Ordinance and the Code of Practice.

6. The assessor should cover the following key areas in the assessment:

   - obtain an understanding of the CA's policies and business practices, and assess whether such information has been properly disclosed;

- assess the CA's compliance with the requirements concerning the use of a trustworthy system to support its operations;

- assess the CA's compliance with the requirements regarding the recognition of certificates in accordance with the CA's CPS(s) and the Code of Practice ; and

- review specific information relating to the CA's financial projection and ascertain and review specific information relating to cover against potential liabilities arising from the issue of certificates by the CA.

## Disclosure of CA Policies and Business Practices

7. The assessor should obtain an understanding of the policies and practices defined by the CA. It is envisaged that such information, including details of the services provided or intended to be provided by the CA, will be incorporated into the CPS(s) issued and maintained by the CA.

8. Where the CA supports one or more certificate policies (CP), including any associated with a mutual recognition scheme for certificates as defined in the Code of Practice, the assessor should understand the requirements specified in each policy and its linkage with the CA's associated CPS(s). The assessor should ascertain that the CA has made appropriate disclosures in such CPS(s) regarding their status of compliance with the supported CP(s).

9. The assessor should design and carry out appropriate tests as considered necessary to assess the reasonableness of management's assertions that the policies and business practices are stated and disclosed in accordance with the requirements set out in the Ordinance and the Code of Practice, and if applicable, the CP(s) associated with a mutual recognition scheme for certificates as defined in the Code of Practice.

## Assessment of Systems, Procedures, Security Arrangements and Standards

10. Section 37 of the Ordinance requires a recognized CA to use a trustworthy system in performing its services. The CA under assessment must demonstrate that its systems can adequately fulfil this requirement as well as those requirements set out in its CPS(s). Section 5 of the Code of Practice provides guidelines on the assessment of a trustworthy system.

11. The assessor should design and carry out appropriate tests as considered necessary to assess the reasonableness of management's assertions that the CA has implemented and maintained a trustworthy system in performing its services.

## Assessment of Certificate Life Cycle Controls

12. A CA seeking recognition of its certificates should demonstrate that:

    - the certificates are issued in accordance with the CA's CPS(s) as well as in compliance with the requirements set out in the Code of Practice; and

    - the CA's arrangements for ensuring liability cover are consistent with the context of its business.

13. The assessor should design and carry out appropriate tests as considered necessary to assess the reasonableness of management's assertions that effective controls, as defined under the Code of Practice and the CA's CPS(s), are implemented and maintained by the CA over the certificate life cycle.

## Compliance Assessment against any CP(s) associated with the Mutual Recognition Scheme for Certificates as defined in the Code of Practice

14. A CA issuing or applying to issue certificates under the mutual recognition scheme for certificates as defined in the Code of Practice should demonstrate that the certificates are issued in accordance with the CA's CPS(s) that are associated and in compliance with any CP(s) associated with such mutual recognition scheme for certificates.

15. Where applicable, the assessor should design and carry out appropriate tests that are additional to the tests described under paragraphs 12 and 13 above and as considered necessary to assess the reasonableness of management's assertions with respect to the CA's compliance with any CP(s) associated with the mutual recognition scheme for certificates as defined in the Code of Practice.

## Review of Financial Projection

16. The assessor should review the CA's financial projection prepared by the CA for the next 12 months in respect of the CA's operation relevant under the Ordinance. In reviewing the financial projections, the assessor should consider the relevant aspects of the CA's business including without limitation:

    - the nature and background of the CA's business, such as its recent history, and other relevant information which could impact its operations;

    - the accounting policies normally followed by the CA, and whether or not these are consistent with the generally accepted accounting principles employed in the Hong Kong Special Administrative Region or equivalent principles accepted internationally, and have been consistently applied in the preparation of the financial projection;

- the assumptions upon which the financial projection is based, and whether or not the financial projection has been compiled on the basis of these assumptions; and

- the procedures followed by the CA in preparing the financial projection.

17. Such financial projection for the next 12 months should include cashflow projection and financial position forecasts prepared in semi-annual intervals.

18. The assessor should compare the following as ascertained from the CA:

    (a) the amount of net current assets as shown in the accounts, which may be in the form of unaudited management accounts, of the CA as at the date specified in paragraph 19 below; and

    (b) a projection of operating costs for 90 days in respect of the CA's operation relevant under the Ordinance, which should start from the same date as specified in paragraph 19 below.

19. As part of the assessment of a CA, the assessor should review the CA's financial projection prepared by the CA for the next 12 months in respect of the CA's operation relevant under the Ordinance. The CA would need to confirm the period covered by the financial projection with the GCIO. The date referred to in paragraph 18 above should be the same as the start date of the 12-month financial projection prepared by the CA.

20. In respect of the 90-days projection of operating costs, the assessor should consider:

    - whether the accounting policies upon which the projection is based are consistent in all material respects with those normally adopted by the CA and conform with the generally accepted accounting principles employed in the Hong Kong Special Administrative Region or equivalent principles accepted internationally; and

    - whether the projection has been properly compiled in all material respects in accordance with the assumptions made by the CA. If any of the assumptions made, or omitted to be made, by the CA appears to the assessor to be unrealistic or inappropriate based on the assessor's experience and professional judgement and, where applicable, having regard to the information as disclosed in the latest audited financial statements of the CA, the assessor should include an appropriate comment in the assessment report.

21. The net current assets referred to in paragraph 18 should mean current assets less current liabilities.

## Ascertaining Potential Liabilities

22. Based on the information provided by the CA, the assessor should ascertain the arrangements that have been established by the CA to determine and manage its potential liabilities in relation to the recognized certificates that it has issued or planned to issue, including:

    - potential claims arising out of any error or omission on the part of the CA, its officers, employees or agents; and

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

23. Where a CA intends to apply for recognition but has not yet commenced operation, the projected number of certificates that it will issue over the next 12 months could be used as the basis of calculating the potential liabilities.

24. For the purpose of paragraph 22, the assessor should perform appropriate procedures to:

    - ascertain details of insurance cover or other appropriate forms of cover for the CA's potential liabilities in relation to issued certificates as at the time of the review, and perform appropriate procedures to assess the CA's compliance with paragraphs 8.2 to 8.4 of the Code of Practice with regard to liability cover;

    - ascertain whether the CA has received any claims from subscribers and/or relying parties since the date of the last assessment and the status of these claims; and

    - ascertain whether claims have been filed against the insurance polices since the date of the last assessment.

## Reporting

25. The assessor should prepare a formal written report addressed to the CA, on the results and findings of the assessment. The assessor should state clearly in the report the specific procedures agreed with the CA and performed as part of the assessment, as well as findings of the assessment including sufficient details of material exceptions, such as incidents of non-compliance with relevant provisions in the Ordinance or the Code of Practice.

26. The assessor should provide an opinion as to whether or not, in all material aspects, the assertions by the management of the CA under assessment in respect of its capability to comply or actual compliance with relevant provisions in the Ordinance and the Code of Practice are reasonable. In reaching this opinion, the assessor should specifically consider the following aspects:

- whether or not the CA discloses its business practices in its CPS(s) in accordance with the relevant provisions in the Ordinance and the Code of Practice and provides its services in accordance with its disclosed business practices;

- whether or not the CA complies with the requirements in respect of the use of a trustworthy system to support its operations in accordance with the relevant provisions in the Ordinance and the Code of Practice; and

- whether or not the CA complies with the requirements in respect of the recognition of its certificates including key management and certificate life cycle management in accordance with the relevant provisions in the Ordinance and the Code of Practice.

27. Where applicable, the assessor should provide an opinion as to whether or not, in all material aspects, the assertions by the management of the CA under assessment in respect of:

- compliance between its CPS(s) and relevant provisions in any CP(s) associated with the mutual recognition scheme for certificates as defined in the Code of Practice are reasonable; and
- its capability to comply or actual compliance with relevant provisions in any CP(s) associated with the mutual recognition scheme for certificates as defined in the Code of Practice are reasonable.

28. The assessor should, in respect of the CA's financial projection, state:

- the period covered by the financial projection;

- whether the accounting policies upon which the projection is based are consistent in all material respects with those normally adopted by the CA and conform with the generally accepted accounting principles employed in the Hong Kong Special Administrative Region or equivalent principles accepted internationally; and

- whether the financial projection has been properly compiled in all material respects in accordance with the assumptions made by the CA. If any of the assumptions made, or omitted to be made, by the CA appears to the assessor to be unrealistic or inappropriate based on the assessor's experience and professional judgement and, where applicable, having regard to the information as disclosed in the latest audited financial statements of the CA company, the assessor should include an appropriate comment in the assessment report.

29. The assessor should, in addition to the items reported as set out in paragraph 28, present the result of the comparison as set out in paragraph 18 and state any comments as a result of the consideration in respect of paragraph 20. The accounts and the 90-days

projection of operating costs of the CA, as ascertained from the CA and referred to in paragraph 18, should be attached as appendices to the assessment report.

30. The assessor should, in respect of the CA's management of its potential liabilities, express an opinion as to the reasonableness of the assertions made by the CA that it has implemented and maintained appropriate procedures to determine and manage its potential liabilities.

31. The assessor should ascertain and report the information gathered as a result of performing the procedures set out in paragraph 24 in respect of (1) the potential liabilities of the CA; (2) insurance or other appropriate forms of cover for the liabilities; and (3) claims received by the CA or filed against the CA's insurance policies.

32. The assessor should, in addition to the items reported as set out in paragraph 31, report the result of performing procedures to assess the CA's compliance with paragraphs 8.2 to 8.4 of the Code of Practice.

## Reliance on Work Performed by Internal Audit

33. Where appropriate, the assessor should consider the extent to which the CA's internal audit activities may be relied upon to modify the nature, timing and extent of assessment performed by the assessor. If reliance on the internal audit function is planned, the assessor should consider:

- the competence and objectivity of the internal audit function;
- the extent to which the internal audit activities cover the specific certification practices under assessment; and
- the follow up of the issues identified and the status of the resolution of the issues.

## Conduct of the Assessment

34. The assessor should perform the assessment in accordance with appropriate standards and practices relating to the performance of such work (where applicable) established by the professional organisation or association to which the assessor is a member.

35. The assessor should consider the severity of any noted exceptions or deficiencies, based on the results of the work performed in each of the areas under the assessment.

36. The assessor should design and execute tests to validate that the appropriate requirements set out in the CA's CPS(s), and any relevant CP(s) that is supported by the CPS(s), are adequately reflected in the operations, technology and/or documentation of the CA. The tests performed by the assessor is expected to include:

- analysis of the information obtained;
- re-computation, comparison and other accuracy check;
- observation of the CA's operation;
- inspection of relevant documents and logs; and
- other tests deemed appropriate by the assessor, such as verification of system settings, obtaining confirmations, etc.

37. Notwithstanding the above, the assessor should apply due professional judgement in determining the nature, timing and extent of testing procedures to be performed during the assessment.

## References

38. In performing the compliance assessment, the assessor should consider generally accepted control principles that may apply to the CA's operation. The related body of knowledge that is currently available includes:

- Institute of Internal Auditors' Systems Auditability and Control Report;
- Information Systems Audit and Control Association and Foundation, Control Objectives for Information and Related Technology (CobiT);
- ANSI (American National Standards Institute) X9.79-2001, Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework;
- AICPA/CICA CATrust Principles and Criteria;
- Evaluation Criteria for Information Technology Security (Common Criteria);
- IETF PKIX Drafts and Requests for Comment; and
- CSPP - Guidance for COTS Security Protection Profiles (Formerly: CS2-Protection Profile Guidance for Near-term COTS), National Institutes of Standards and Technology, Department of Commerce, USA.