Guidance Note on Recognition of Certification Authorities and Certificates under the Electronic Transactions Ordinance (Cap. 553)

Published in January 2010

(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. A certification authority ("CA") seeking recognition from the Government Chief Information Officer ("GCIO") should be capable of complying with all relevant provisions applicable to a recognized CA under the Electronic Transactions Ordinance (Cap. 553) ("Ordinance"), Regulations thereunder and the Code of Practice. A recognized CA may also apply to the GCIO for recognition of its certificates.

3. This guidance note outlines the conditions and the process for the recognition of CAs and certificates.

Recognition of Certification Authorities

4. In accordance with section 21(4) of the Ordinance, in determining whether an applicant is suitable for recognition, the GCIO shall consider, in addition to any other relevant matters, the following matters:

   (a) whether the applicant has the appropriate financial status for operating as a recognized CA 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 applicant to cover any liability that may arise from its activities relevant for the purposes of the Ordinance;

   (c) the system, procedure, security arrangements and standards used or proposed to be used by the applicant to issue certificates to subscribers;

   (d) the report prepared by a person approved by the GCIO as being qualified to make such a report which contains an assessment as to whether the applicant is capable of complying with the provisions of the Ordinance and of the Code of Practice as are specified under paragraph 1 of Appendix 2 of the Code of Practice, or the statutory declaration made by a responsible officer of the applicant which states whether the applicant is capable of complying with the provisions of the Ordinance and of the Code of Practice as are specified under paragraph 2 of Appendix 2 of the Code of Practice;

   (e) whether the applicant and the responsible officers are fit and proper persons; and

   (f) the reliance limits set or proposed to be set by the applicant on its certificates.

Financial Considerations

5. Items (a), (b) and (f) in section 21(4) of the Ordinance all relate to the financial aspects of the applicant's operation.

6. The applicant should provide evidence that:

   (a) it has assessed the business and financial risks that will arise or have arisen from its operation as a CA; that it has made adequate arrangements covering itself for its operation and against potential claims arising from the certificates that it has issued or plans to issue. Where the CA issues certificates with specific reliance limits, the liability cover, such as by obtaining insurance, should be sufficient to meet the potential liabilities of the CA in respect of the reliance limits. More specific requirements in respect of liability cover are set out in section 8 of the Code of Practice; and

   (b) it intends to be, and will remain, a going concern. Such intention can be demonstrated in various ways, including without limitation:

   – maintaining adequate finance to support its operation;

   – having installed, or contracted to install systems and equipment which support the operation of a CA and having made necessary financial arrangements; and

   – having adequate and appropriate personnel, both in terms of quality (skill level) and quantity (number of staff), to support a CA's operation and having made the necessary financial arrangements.

Systems, Procedures, Security Arrangements and Standards

7. The GCIO shall only grant recognition to those CAs which meet a standard acceptable to the GCIO. To meet the acceptable standard, the applicant should ensure that its systems, procedures, security arrangements and standards form a trustworthy system which the applicant uses to issue certificates to subscribers and carry out related services.

8. Guidelines on a trustworthy system are described in section 5 of the Code of Practice.

9. To facilitate accessibility of its web site by persons with disabilities, a CA shall refer to the "Web Content Accessibility Guidelines" (www.w3.org/TR/WAI-WEBCONTENT) issued by the World Wide Web Consortium.

Assessment Report

10. The applicant must furnish to the GCIO a report containing an assessment as to whether the applicant is capable of complying with the provisions of the Ordinance

and of the Code of Practice as are specified under paragraph 1 of Appendix 2 of the Code of Practice.

11. The applicant should ensure that the report is prepared by a person approved by the GCIO as being qualified to make such a report. Qualifications of the person are set out in section 12 of the Code of Practice. Before preparing the assessment report required under section 20(3)(b) of the Ordinance, the applicant should ensure that the person to prepare the report is approved by the GCIO as being qualified to make such a report.

12. The assessment report shall be prepared by a qualified person in accordance with the Guidance Note on Compliance Assessment of Certification Authorities published by the GCIO.

Statutory Declaration

13. The applicant must furnish to the GCIO a statutory declaration stating whether the applicant is capable of complying with the provisions of the Ordinance and of the Code of Practice as are specified under paragraph 2 of Appendix 2 of the Code of Practice.

14. The statutory declaration shall be made by a responsible officer of the applicant.

Fit and Proper Person

15. As required in section 21(4)(e), the applicant and its responsible officers should be fit and proper persons. The criteria for determining whether a person is a fit and proper person are set out in section 21(5) of the Ordinance. The applicant's responsible officer(s) should make statutory declarations that they are fit and proper persons. Moreover, for verification purpose, the applicant and its responsible officer(s) should authorise the Commissioner of Police of the Hong Kong Special Administrative Region or his equivalent counterpart in the overseas jurisdiction to disclose the criminal records, if any, of the applicant and the responsible officer(s) of the applicant to the GCIO.

Validity Period of Recognition of a CA

16. The validity period for the recognition of a recognized CA will normally be 2 years. The recognized CA may apply to the GCIO for renewal of the recognition at least 30 days before but not earlier than 60 days before the expiry of the validity of the recognition.

Recognition of Certificates

17. A recognized CA may apply to the GCIO for recognition of some or all of its certificates. If the CA is not yet a recognized CA, the CA can submit an application of recognition both for itself as well as for its certificates. The recognition of the certificates will be considered after the GCIO has granted recognition to the CA concerned.

18. In general, so long as a CA maintains its recognition status, the recognition status of a certificate issued by the CA will not change provided that the relevant certification practice statement ("CPS"), including the relevant certificate policy that governs the recognized certificate, has not materially changed.

19. Material changes that may affect the recognition status of the certificate may include without limitation :

    (a) changes in the identification process that weaken the reliability of the certificate;

    (b) changes in the reliance limit of the certificate; or

    (c) changes in the key generation, storage, or usage requirements.

20. Before a recognized CA effects any intended material change to its operation or CPS that corresponds to one or more types, classes or descriptions of recognized certificates that the recognized CA issues, the recognized CA shall inform details of the change in writing to the GCIO. The GCIO will consider whether the intended material change complies with relevant provisions of the Ordinance and this Code of Practice.

Certificate Recognition Criteria

21. For the recognition of a particular certificate or a type, class or description of certificates, a recognized CA should demonstrate that:

    (a) the certificate(s) are issued in accordance with the recognized CA's CPS;

    (b) the certificate(s) are issued in accordance with the Code of Practice; and

    (c) the arrangements put in place or proposed to be put in place by the recognized CA to cover any liability that may arise from the issue of that particular certificate, or that type, class or description of certificates are sufficient.

Application Form

22. The application form for seeking recognition of CA or certificates can be obtained from -

Certification Authority Recognition Office
Office of the Government Chief Information Officer
15-16/F, Wanchai Tower,
12 Harbour Road,
Wan Chai,
Hong Kong.
(Fax : 2845 5516)

The application form is also available on the web site of the Office of the Government Chief Information Officer (http://www.ogcio.gov.hk/eng/caro/esub7.htm).

23. When the completed application form is submitted to the GCIO, the applicant should ensure that the completed application form is accompanied by the assessment report, the statutory declaration, the application fee(s) and any relevant documents or information which may be required by the GCIO for the purpose of the application.

24. The GCIO may request for further documents or information in connection with the application.

Relevant Documents or Information Required

25. Section 30 of the Ordinance states that the GCIO must specify by notice published in the Gazette any particulars and documents to be furnished in support of the application made under sections 20(3)(a), 22(2) and (10) and 27(5A) of the Ordinance.