ACCOP Paper No. 6/2003

Review of the Code of Practice for Recognized Certification Authorities

Purpose

This paper calls for input for the review of the Code of Practice for Recognized Certification Authorities ("Code of Practice").

Background

2. At the 8th meeting of the Advisory Committee on Code of Practice for Recognized Certification Authorities ("ACCOP") held on 17 January 2003, it was decided that the Information Technology Services Department would proceed to conduct a review of the Code of Practice.

3. In March and April 2003, we circulated ACCOP Paper No. 4/2003 to Members setting out the proposed consultation arrangements in respect of the review of the Code of Practice. A number of comments were received from Members including their expressed support to the proposed consultation arrangements as well as a suggestion regarding the list of target respondent organisations. Accordingly, the list of target respondent organisations for the consultation has been revised as at Annex I.

Proposed amendments to the Code of Practice

4. In ACCOP Paper No. 4/2003, we suggested to distribute a set of proposals for improving the Code of Practice to the target respondents to seek their comments. Such proposals are set out at Annex II that are based on our experience of implementing the requirements stipulated in the Code of Practice since its publication in January 2000. Target respondents may also provide comments on any other aspects of the Code of Practice which is available at www.itsd.gov.hk/itsd/english/caro/esub3.htm.

Electronic Transactions (Amendment) Bill 2003

5. The Electronic Transactions (Amendment) Bill 2003 ("the Bill"), which seeks to update and improve the Electronic Transactions Ordinance (Cap. 553), was published in the Gazette on 13 June 2003. Parts of the provisions set out in the Bill may consequentially lead to amendments to the

Code of Practice. However, we have not reflected any of such potential amendments in the proposals at Annex II because passage of the Bill through the Legislative Council is still in progress. Nevertheless, we have taken care to ensure that the proposals at Annex II are not inconsistent with the provisions set out in the Bill. The Bill is available for viewing by the public at http://www.info.gov.hk/itbb/english/it/eto.htm.

Advice sought

6. Members' comments are invited in respect of the proposals at Annex II. Members may also provide comments on any other aspects of the Code of Practice.

7. We would also like to seek Members' assistance to solicit comments on the same subjects as set out in the preceding paragraph from the organizations with which Members are respectively affiliated (please refer to Part (A) of Annex I). A separate consultation paper will be provided to Members for distribution to those organizations. We will consult the organizations individually listed under Parts (B) and (C) of Annex I.

Submission of comments

8. All comments should be sent to Mr Raymond Chow, Secretary of the ACCOP, on or before **28 July 2003** by fax (2573 7113), e-mail (**rclchow@itsd.gov.hk**) or by post to the address at 19/F, Wu Chung House, 213 Queen's Road East, Wan Chai, Hong Kong.

Enquiry

9. For enquiries about the review of the Code of Practice including information contained in this paper, please contact Mr Raymond Chow at 2961 8206 or via e-mail.

Information Technology Services Department
June 2003

Annex I

Target Respondent Organisations To Be Consulted in respect of the Review of the Code of Practice

(A) Organisations with which ACCOP members are affiliated

1. City University of Hong Kong
2. Hong Kong Computer Society
3. Hong Kong General Chamber of Commerce
4. Hong Kong Institution of Engineers
5. Hong Kong Jockey Club
6. Hong Kong PKI Forum
7. Hong Kong Society of Accountants
8. Law Society of Hong Kong
9. Office of the Privacy Commissioner for Personal Data
10. Tradelink Electronic Commerce Limited

(B) Recognized CAs

11. Digi-Sign Certification Services Limited
12. HiTRUST.COM (HK) Incorporated Limited
13. Hongkong Post CA
14. Joint Electronic Teller Services Limited

(C) Other organisations

15. Hong Kong Article Numbering Association
16. Hong Kong International Arbitration Centre[1]
17. ESD Services Limited
18. Information Security and Forensics Society
19. Information Systems Audit and Control Association
20. Professional Information Security Association

[1] Newly included as suggested by an ACCOP member during the consultation in March/April 2003.

Annex II

Code of Practice for Recognized Certification Authorities
Proposed Amendments

Section	Proposed Amendment	Remark
1.7	On the 2nd last line, "that will be set up and" is to be deleted.	Since the ACCOP has been set up, the phrase "that will be set up" should not be necessary.
2.1	"fit and proper person" (i) In point (a), remove "with deception" on the last line. (ii) In points (c) and (d), "within the 5 years preceding the date of the application for recognition as a recognized CA or for the renewal of such a recognition" is to be replaced by "within 5 preceding years".	(i) To align with the criteria of "fit and proper person" as set out in section 21(5)(a) of ETO. (ii) To render points (c) and (d) also applicable for the period of time after recognition or renewal of recognition is granted to a CA.
3.6	To replace “personal information” by “personal data”. Similar amendment as appropriate will apply to all relevant sections of the Code of Practice where reference to “personal information” appears.	“Personal information” is replaced by “personal data” as the Personal Data (Privacy) Ordinance (Cap. 486) has defined the term “personal data” but not “personal information”.
3.8	(i) To replace "certificates not recognized by the Director" by "certificates which are not recognized certificates". (ii) To add “in its certification practice statement(s) and repository” after “the recognized CA shall publicize”.	(i) Recognition of certificates is not all under the authority of the Director. For the case of Postmaster General, recognized certificates are designated by the Postmaster General under the ETO. (ii) To provide clearer requirement as to where a recognized CA shall publicize the fact that it issues two categories of certificates, i.e. recognized as well as not recognized.

Section	Proposed Amendment	Remark
4.5	The 2 instances of "subscribers" are to be replaced by "applicants for certificates". Similar amendment as appropriate will apply to all relevant sections of the Code of Practice where reference to "subscriber" appears.	Before an applicant for a certificate accepts the certificate, the applicant has not yet become a subscriber. It is the applicant (rather than in the capacity of a subscriber) whose attention should be drawn to the extent that his personal data will become public information.
4.12	(i) In the 1st sentence, to add "its operation or" before "its CPS'. (ii) In the 1st sentence, to replace "the recognized CA shall consult the Director in respect of the effect of the intended material change on the recognition status of the types, classes or descriptions of recognized certificates concerned" by "the recognized CA shall inform details of the change in writing to the Director.". To replace the 2nd sentence by "The Director will consider whether the intended material change complies with relevant provisions of the Ordinance and this Code of Practice." (iii) To remove the 3rd sentences. (iv) In the 4th sentence, to replace "a CPS" by "the operation of the recognized CA or its CPS.	(i) A major change may affect the CA's operation or its CPS. (ii) To set out more clearly that a recognized CA shall inform details of the material change in writing to the Director. The Director will then consider the material change with reference to relevant provisions of the ETO and the Code of Practice. (iii) The 3rd sentence describes a decision of a recognized CA and should not be necessary in the Code of Practice. (iv) See (i) above.
5.10.3	To move the last sub-bullet point under the 2nd bullet point to the end of section 5.10.5.	The sub-bullet point is about key generation by a recognized CA for subscribers and should be placed under section 5.10.5.

Section	Proposed Amendment	Remark
5.10.8	To expand the meaning of all occurrences of "certificate revocation list" to include "and any other means of publishing revocation information". Similar amendment as appropriate will apply to all relevant sections of the Code of Practice where reference to "certificate revocation list" appears.	To cater for the use of means other than certificate revocation list for the publication of certificate revocation information.
5.11	To replace "A recognized CA shall provide a trustworthy system to generate…" by "A recognized CA shall ensure that a trustworthy system is used to generate…".	To cater for the situation that an applicant for a certificate uses his own system, rather than using a system provided by the recognized CA, to generate keys.
6.1	i) To revise the 1st sentence as: "A recognized CA may issue recognized certificates and certificates which are not recognized certificates.". ii) In the 2nd sentence, replace "certificates not recognized by the Director" by "certificates which are not recognized certificates".	i) & ii) Recognition of certificates is not all under the authority of the Director. For the case of the Postmaster General, recognized certificates are designated by the Postmaster General under the ETO.
6.4	To revise the section as: "A recognized CA shall provide a reasonable opportunity to the applicant for a certificate to verify the personal data of the applicant that are placed or to be placed into the certificate."	The revision is mainly to replace "subscriber" by "applicant for a certificate" (please refer to remark for section 4.5 above) and to clarify that the verification is on personal data of the applicant.

Section	Proposed Amendment	Remark
8.2	(i) To revise the section as: "A recognized CA shall arrange suitable insurance or other forms of cover to ensure that it is capable of covering potential liabilities arising from or related to issuance and use of recognized certificates. Specifically, the recognized CA shall provide evidence that it has acquired insurance cover against claims arising from its error or omission, with a minimum limit of indemnity in relation to each and every single claim during the period of insurance of not less than – (a) 10 times the reliance limit specified by the recognized CA in its certification practice statement(s) in relation to its certificates; or (b) $200,000; whichever is higher. Moreover, the total insurance cover for aggregate claim amount in any one insurance period of 12 months shall be set at 10 times the amount of (a) or (b) whichever is higher. Such liability cover shall be in place at all times and shall cover all type, class or description of recognized certificates issued by the recognized CA. Should the recognized CA choose to put in place other forms of liability cover, the same minimum limit of indemnity shall be provided for. Any such other forms of liability cover shall be administered by an independent third party."	(i) To incorporate requirements of liability cover basically following similar requirements currently specified in the "Guidance Note on Recognition of Certification Authorities and Certificates" published by the Director.

Section	Proposed Amendment	Remark
	(ii) To add the requirements that an insurance policy acquired by a recognized CA shall be: (a) issued by an insurer authorized to carry out the pertinent insurance business in HKSAR under the Insurance Companies Ordinance (Cap. 41), including Lloyd's; and (b) governed by and construed in accordance with laws of HKSAR. In addition, both the recognized CA and the insurer agree to submit to the non-exclusive jurisdiction of the courts of HKSAR as regards any claim or matter arising under the insurance policy.	(ii) To ensure that an insurance policy acquired by a recognized CA is issued by an authorized insurer and is subject to local jurisdiction.
10.3(f)	To add "or exception(s) or deficiency(ies) identified" after "recommendation(s) made".	To also request a recognized CA to report its actions to address exceptions and deficiencies identified in an assessment report.
11.1	In the 2nd sentence, to replace "a termination plan" by "an updated termination plan", and to add "or when requested by the Director by the time specified in a notice issued by Director to the recognized CA" at the end of the sentence.	To allow the Director to request an updated termination plan from a recognized CA by giving a notice to the CA.
11.5(e)	Add the following text at end of the sub-section: "The transfer of information shall be made to a custodian who is to maintain the information for not less than 7 years from the	To provide more specific requirements on the transfer of the CA's information upon its termination of service.

Section	Proposed Amendment	Remark
	date on which the recognized CA terminates its service or the transfer of information is effected whichever is later. The public shall be informed of the means and procedures to access the information."	
12.4	To replace the section as follows: "For illustrative purpose, the following person who meets the requirements set out in sections 12.2 and 12.3 above may apply to the Director for approval as the person qualified to conduct the assessment: (a) a Certified Public Accountant, i.e. a professional accountant with a practising certificate issued under the Professional Accountants Ordinance (Cap. 50); or (b) a Corporate Member in the Information Discipline of the Hong Kong Institution of Engineers who is also a Registered Professional Engineer under the Engineers Registration Ordinance (Cap. 409) in the same discipline. The Director may also approve applications submitted by other persons as being qualified to conduct the assessment."	To reflect that Corporate Members of the Hong Kong Institution of Engineers who are also Registered Professional Engineers are eligible for consideration by the Director to serve as a qualified person to prepare an assessment report on a CA.
Appendix		
2.2.2	To replace the 1st and 2nd sentences by: "A recognized CA shall provide the appropriate object identifier(s) of its CPS(s) if available. Where the	To more clearly set out requirements for the publication of object identifiers and certificate policies where appropriate.

Section	Proposed Amendment	Remark
	recognized CA supports specific certificate policies (CPs) for recognized certificates issued under the CPS(s), the recognized CA shall identify those CPs and provide the appropriate object identifiers of the CPs if available in this section of the CPS".	
2.2.4	To replace the 1st occurrence of "subscribers" by "subscribers and relying parties".	To also include "relying parties" as in the case of the 2nd sentence of the section in which both subscribers and relying parties are mentioned.
4.1	To replace "end entity" by "applicant for a certificate".	"Applicant for a certificate" is more appropriate and precise than "end entity".
4.1.7	To replace "the name on a certificate corresponds to the person being issued the certificate" by "the name of the subscriber appeared on a certificate is the name of the applicant for a certificate to whom the certificate will be issued".	To set out more clearly the requirement in respect of the name that should appear in a certificate.
5.1	In the 1st sentence, to replace "subscribers to obtain new certificates" by "applicants for certificates to apply for new certificates".	Before an applicant for a certificate accepts the certificate, the applicant has not yet become a subscriber. Therefore, it is more appropriate to use "applicant" instead of "subscriber", and to use "apply" instead of "obtain".
5.3	2nd bullet point and last sentence To replace "contents of the certificates" by "contents of their personal data in their certificates".	To clarify that "contents" refer to personal data of the applicants.
5.4.2	(i) *(*Page *12)* 1st bullet point To replace "user certificate" by "certificate". (ii) *(Page 12)* 2nd bullet *point*	(i) To avoid using different terms for "certificate". (ii) To avoid using different terms for "subscriber".

Section	Proposed Amendment	Remark
	To replace "certificate subject" by "subscriber".	
5.4.3	(i) In the 1st paragraph, to replace “identify unexpired certificates that are no longer valid” by “specify the certificates that are issued by a recognized CA and that have been revoked”	(i) To align with the definition of certificate revocation list in section 2 of the Code of Practice.
	(ii) In the 1st paragraph, to replace “give the reason” by “may give the reason”.	(ii) To reflect the fact that reasons may not always be available for the revocation of a certificate.