

**Proposed Responses to Comments Received  
in respect of the Review of the Code of Practice  
for Recognized Certification Authorities**

**Purpose**

This paper sets out the proposed responses to the comments received during the consultation in respect of the review of the Code of Practice for Recognized Certification Authorities (“Code of Practice”).

**Background**

2. At the 8<sup>th</sup> meeting of the Advisory Committee on Code of Practice for Recognized Certification Authorities (“ACCOP”) held in 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/April 2003, we circulated ACCOP Paper No. 4/2003 to seek Members’ comments on the proposed consultation arrangements in respect of the review of the Code of Practice. In June/July 2003, we conducted the consultation with the following target respondents:

- (a) Members of ACCOP and, through Members, the organizations with which Members are affiliated (ref: ACCOP Paper No. 6/2003 and Paper No. 7/2003);
- (b) recognized certification authorities (“CA”); and
- (c) six other organizations to which the services of CAs and the conduct of secure electronic transactions are relevant.

4. In the consultation, we invited the target respondents to comment on a set of proposed amendments to the Code of Practice, as well as on any other aspects of the Code of Practice.

**Comments Received**

5. During the consultation period, submissions were received from the following 8 individuals and organizations:

- (a) Dr L M Cheng
- (b) HiTRUST.COM (HK) Incorporated Limited
- (c) Hong Kong Article Numbering Association
- (d) Hong Kong International Arbitration Centre
- (e) Hongkong Post
- (f) Information Systems Audit and Control Association
- (g) Privacy Commissioner for Personal Data
- (h) Professional Information Security Association

### **Proposed Responses**

6. We have carefully examined and considered the aforesaid submissions, and have prepared our proposed responses as set out at Annex.

### **Advice sought**

7. Members' comments are invited in respect of the proposed responses at Annex.

8. Subject to Member's comments, we will proceed to amend the Code of Practice accordingly.

**Information Technology Services Department**  
**December 2003**

**Review of Code of Practice for Recognized Certification Authorities**  
**Comments Received and Proposed Responses**

Section	Summary of Comments Received	Proposed Responses
3.6	The proposed amendment is made without making specific reference to the Personal Data (Privacy) Ordinance (“PD(P)O”). It may be desirable to provide a clear definition of the term "personal data" with specific reference to its definition under the PD(P)O.	We will provide a clear definition of the term “personal data” in the Code of Practice for Recognized Certification Authorities (“Code of Practice”) as suggested.
3.8	<p>(a) <u>Regarding point (ii) of the proposed amendments</u>  The requirement is vague. This is a matter of degree and volume of information to be publicized for satisfying the proposed requirement.</p> <p>(b) <u>Regarding point (ii) of the proposed amendments</u>  The term “repository” has a specific meaning - essentially a directory that holds details of issued certificates. Hence, from a pure technical viewpoint, it is not practical to require a CA to publicize such facts in a repository. Instead, the Director may require separate repositories be used to store recognized certificates and certificates that are not recognized certificates.</p>	<p>We will provide further elaboration in section 3.8 to the effect that the fact to be publicized by a recognized certification authority (“RCA”) shall enable relevant parties to clearly identify which types of certificates issued by the RCA are recognized under the Electronic Transactions Ordinance (Cap. 553) (“ETO”) and which types are not.</p> <p>According to section 10 of the Appendix of the Code of Practice, a repository may be implemented using different standards such as LDAP for directories and HTML for web pages. As such, the required facts may be publicized by an RCA in its repository in a form suitable for such publication.</p> <p>We agree with the suggestion that separate repositories shall be used by an RCA to publish certificates that are recognized under the ETO and those that are not.</p>

Section	Summary of Comments Received	Proposed Responses
4.12	(a) The type of reporting format for the material change is not specified which can affect the length of reassessment and decision.	Currently when an RCA notifies the Director of Information Technology Services (“Director”) in respect of an intended material change in the RCA’s operation, the RCA is allowed to use its chosen format to present to the Director information about the material change. So far, such an arrangement works smoothly. Therefore, we are of the view that specification of a reporting format should not be necessary. While we allow the flexibility for RCAs to use their chosen formats for reporting major changes, we endeavor to process the reports by RCAs expeditiously.
	(b) Is there any recommendation in speeding up the process of minor changes?	When we receive a report from an RCA in respect of an intended change in its operation, we will assess whether the intended change is material in affecting the trustworthiness of its operation. We only follow up with the RCA in respect of changes that are material rather than minor changes.
	(c) <i>Regarding point (ii) of the proposed amendments</i> It is recommended that the Director should consider incorporating an appeal or review mechanism in situations where the CA does not concur with the Director’s ruling [ <i>in respect of whether an intended material change in the RCA’s operation complies with the ETO and the Code of Practice</i> ].	In the event that an RCA proceeds to implement a material change in its operation which, in the view of the Director, does not comply with the ETO or the Code of Practice, the Director may revoke or suspend recognition of the RCA under section 23 or 24 of the ETO. In accordance with section 28 of the ETO, the RCA may appeal to the Secretary for Commerce, Industry and Technology against the decision of the Director. An appeal mechanism has been provided for under the ETO.
5.9.2	There is no requirement for the personal background of the operational personnel. This may impose some potential security risk to the CA. It is suggested that a	There are currently measures to deal with risks in relation to the backgrounds of CA personnel. Under section 21(4) of the ETO with regard to determining whether an applicant CA is suitable for

Section	Summary of Comments Received	Proposed Responses
	<p>similar security screening process adopted for Security Licensing Companies currently run by the Police may be a good benchmarking.</p>	<p>recognition, the Director shall consider, among other matters, whether the applicant and its responsible officers are fit and proper persons. With reference to the criteria of a fit and proper person set out in section 21(5) of the ETO, the Director will enquire with the Commissioner of Police on whether there are any criminal records against the responsible officers concerned. The Director will also check with the Official Receiver to see if there are any bankruptcy cases against the responsible officers. The Director will continue to adopt such measures in considering whether the CA's responsible officers are fit and proper persons.</p> <p>Furthermore, under section 5.9.1(b)(i) of the Code of Practice, an RCA is required to develop and maintain effective controls over personnel security through mechanisms including without limitation verification checks on backgrounds of its personnel in accordance with its security policies and procedures. In the assessment of an RCA by an independent assessor (either for application for recognition or for annual assessment), compliance by the RCA with the Code of Practice including section 5.9.1(b)(i) will be assessed.</p>
5.10.8	<p>Certificate revocation list (CRL) is a universally accepted means of publishing details concerning revoked certificates. There are also international standards on CRLs. There is therefore no need to incorporate "any other means of publishing revocation information", particularly in view of the CA's obligation to adopt industry technology and open standards.</p>	<p>The proposal to include "other means of publishing revocation information" is to cater for the implementation of specific types of digital certificates in respect of which common industry practice has yet to emerge for the publication of certificate revocation information. As soon as any common industry practice in this regard becomes widely accepted, an RCA shall, where applicable, adopt such common industry practice as an open and common</p>

Section	Summary of Comments Received	Proposed Responses
		interface for facilitating interoperability as required under section 14.1 of the Code of Practice. Such a common industry practice could be the traditional CRL or some other new industry standard.
5.11	<p>(a) It is proposed that the RCA’s responsibility is to advise the subscriber to use a “trustworthy” system for the purpose of key pair generation in the situation that the subscriber selects to use his own system to generate keys.</p> <p>(b) From the compliance viewpoint, this is difficult (may even be impossible) for the recognized CA to ensure that the subscriber will use a trustworthy system.</p> <p>(c) In situations where subscribers used their own key generation systems, the CA should provide reasonable guidance and advice in relation to the trustworthiness of the key generation process. In addition, the CA should, if it considers necessary, consider the</p>	<p>With regard to the situation where an applicant for a certificate generates his key pair using his own system, we will revise section 5.11 to the effect that an RCA shall request the applicant to use a trustworthy system for generation of the applicant's key pair. The RCA shall provide guidelines to the applicant and shall take reasonably practicable steps to ascertain the applicant's compliance with the guidelines in relation to the use of a trustworthy system by the applicant for the generation of his key pair. The RCA shall not accept the applicant’s key pair if the RCA considers that the applicant fails to comply with the RCA's guidelines or otherwise fails to use a trustworthy system for the generation of the key pair.</p> <p>With regard to keys generated by the RCA both for itself as well as for certificate applicants, the RCA shall use a trustworthy system.</p> <p>Please see the proposed response for (a) above.</p> <p>Please see the proposed response for (a) above.</p>

Section	Summary of Comments Received	Proposed Responses
	<p>trustworthiness of such key generation systems and reserves the right to reject key pairs generated by systems that are not considered trustworthy.</p>	
6.4	<p>(a) It (<i>i.e. the consultation paper</i>) is proposed to change the verification from certificate content to personal data of the applicant for a certificate. The original paragraph is better as the applicant should have opportunity to verify not only his own personal data, but other information on the certificate, such as validity period, key usage etc.</p>	<p>Besides data supplied by the certificate applicant, the other data on the certificate are created by the RCA (e.g. validity, key usage, signature and cryptographic algorithm IDs, the RCA's signature, etc.). It should be the responsibility of the RCA to ensure accuracy of such data created by it rather than to have them verified by the applicant. Some of the data created by the RCA are technical in nature and may not be easily understood by an average certificate applicant. Therefore, we are of the view that an RCA should only be required under the Code of Practice to provide an opportunity for the certificate applicant to verify data of the applicant that are placed or to be placed in a certificate.</p>
	<p>(b) To be consistent with the requirements of DPP2(1) of the PD(P)O, it may be necessary to consider adding an additional requirement "a recognized CA to take all reasonably practicable steps to ensure accuracy of personal data contained in a certificate".</p>	<p>We will revise section 6.4 to the effect that an RCA shall provide a reasonable opportunity to the certificate applicant to verify the "information on the applicant" that is included or to be included in the certificate. Furthermore, the RCA shall take all reasonably practicable steps to ensure accuracy of the information included or to be included in the certificate.</p> <p>"Information on the applicant" means information supplied by the certificate applicant that the RCA includes or will include in the certificate. Depending on the types of certificates, information on the applicant may include personal data of an individual as defined</p>

Section	Summary of Comments Received	Proposed Responses
	(c) Contents of the certificate does not only include personal data, for example, website URL in the case of server certificate, or organisation name in the case of a corporate certificate. As such, the paragraph should not be restricted to just cover “personal data”.	in section 2 of the Personal Data (Privacy) Ordinance (Cap. 486).  Please see the proposed response for (b) above.
8.2	(a) Should the total insurance cover for aggregate claim amount be proportional to the total number of certificates issued, instead of 10 times the amount of (a) or (b) mentioned on page 4 of the Annex II ( <i>of the consultation paper</i> )?	It is not a common practice in the CA industry worldwide that CAs are required to acquire insurance cover in proportion to the number of certificates issued. We have examined relevant regulatory regimes in some other parts of the world (i.e. Australia, Singapore, UK, a number of States in the USA and others) and found that such regulatory requirement rarely exists. Therefore, we do not intend to adopt such an approach in the Code of Practice.
	(b) What is the rationale of setting the insurance cover to such value?	When we published the existing insurance requirements in February 2001, we made reference to relevant regulatory requirements in other parts of the world (i.e. Singapore, Malaysia and a number of States in the USA and others). We defined the insurance requirements such that they were comparable with international practices.
	(c) <i>Regarding point (i) of the proposed amendments</i> The revisions should be further clarified to indicate if the total insurance cover for aggregate claim amount in an insurance period is calculated based on the number of certificates, or on the number of type/class	Our proposed amendment has set out the criteria for determining the aggregate claim amount in any one insurance period. The criteria do not involve the number of certificates or the number of types, classes or descriptions of certificates. Please also see the proposed response for (a) and (b) above.

Section	Summary of Comments Received	Proposed Responses
	of certificate, or in aggregate.	
	(d) <u>Regarding point (ii) of the proposed amendments</u> Please clarify the meaning of the proposed sentence (i.e. “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.”).	It is a non-exclusive jurisdiction clause. A non-exclusive jurisdiction clause will not restrict a claimant’s choice of forum (e.g. courts and arbitration centre) but raises a strong prima facie case that such jurisdiction is forum convenient. In such event, the court of HKSAR will ordinarily rule on a claim pursuant to the insurance policy concerned, if asked, and if the chosen court is foreign, will refuse to rule on the claim.
	(e) <u>Regarding point (ii) of the proposed amendments</u> Should there be conflict of the words “non-exclusive jurisdiction of the courts of HKSAR” in the Proposed Amendment column against the words “subject to local jurisdiction” in the Remark column.	The note under the “Remark” column is meant to highlight the fact that where a claimant chooses to ask the court of HKSAR to rule on a claim pursuant to the insurance policy concerned, the court of HKSAR will ordinarily rule on the claim.
	(f) <u>Regarding point (ii) of the proposed amendments</u> Insurance cover may be taken out on a group level, so in the case of a global CA, although the HK operations may seek recognition in accordance with HK law, insurance cover may be organized on a global level by the group company. Thus we do not believe that the Director should impose specific restrictions in this respect. In addition, the issue of governing law and legal jurisdiction is a matter of commercial decision. We are certainly aware of commercial contracts that were concluded in one country but were subject to the laws of a different	The proposed amendment is to better protect the interest of local users of the services of an RCA by ensuring that an insurance policy acquired by the RCA is issued by an authorized insurer, governed by the laws of HKSAR and subject to the non-exclusive jurisdiction of the courts of HKSAR. We are of the view that the proposed amendment is appropriate.

Section	Summary of Comments Received	Proposed Responses
	<p>legal jurisdiction. As such, we do not consider the proposed changes being necessary.</p>	
11.5(e)	<p>Unless the transfer of the data to the custodian is for the purpose of continuing the original service provided by the relevant RCA, any use of the data for any other purpose without the prescribed consent of the individuals concerned may constitute a breach of the requirements of DPP3 of the PD(P)O. In this connection, it is advisable to state clearly in this section 11.5(e) the specific purpose(s) for which the data are to be transferred to the custodian.</p>	<p>We will amend section 11.5(e) as suggested.</p>
12.4	<p>It is proposed that other globally recognized professional qualifications in information security are accepted as criteria for accepting a person (<i>i.e. a qualified person to conduct assessment</i>). These qualifications include Certified Information System Security Professional (CISSP) and Certified Information Systems Auditor (CISA). In the amended Legislative Council (Amendment) Bills, people who are full member of Professional Information Security Association holding the CISSP designation for 4 years or more are accepted as eligible voters. So it is recommended to make similar arrangements.</p>	<p>We welcome suggestion from any person or organization for consideration by the Director with regard to serving as a qualified person for preparing an assessment report on a CA under the ETO. The relevant requirements are set out in section 12 of the Code of Practice in respect of a qualified person as well as the professional organization with which the person is a member.</p> <p>Should the Professional Information Security Association (“PISA”) or other professional associations wish their members to become eligible for serving as a qualified person, we encourage them to send us relevant information to substantiate that they and their members meet the requirements set out in section 12 of the Code of Practice. We will consider their cases once we receive such relevant information from them.</p>

Section	Summary of Comments Received	Proposed Responses
Appendix of Code of Practice		
2.2.4	<p>The change is not considered necessary. A CA does not typically have any contractual relationship with relying parties. It is also important to consider that a CPS is public domain information, and can be downloaded by subscribers and non-subscribers alike. There is no need to specifically refer to relying parties, so as to avoid any implied obligations / liabilities between the CA and relying parties in general.</p>	<p>We are of the view that our proposed amendment is appropriate. As described in the 2<sup>nd</sup> sentence of section 2.2.4, an RCA would typically state in the CPS at least a telephone number, postal address and electronic mail address for subscribers and relying parties to contact the RCA. Our proposed amendment to the 1<sup>st</sup> sentence is consistent with the 2<sup>nd</sup> sentence in that contact point of the RCA should be provided to both subscribers and relying parties.</p>
3.4.2	<p>Rather than leaving the provisions of dispute resolution procedures for RCAs to establish, it is suggested that the Information Technology Services Department (“ITSD”) to define the provisions for RCAs to follow. By doing so, it establishes consistency, predictability and above all it protects the interests of the consumer.</p>	<p>Allowing RCAs to establish their own dispute resolution procedures is in line with international practices in the CA industry. We have examined relevant regulatory regimes in some other parts of the world (i.e. Singapore, Malaysia, UK and others) and found no prescribed dispute resolution procedures that have to be followed by CAs in those places. Therefore, we consider that it should not be necessary for ITSD to define any specific dispute resolution procedures for RCAs to follow.</p>
4.1.7	<p>The change is not considered necessary. The original wording should suffice. It is important to consider that in some cases, the certificate is used to identify a server. In which case, the name on the certificate may not be the name of the applicant. The original wordings already spell out the requirement, and the revision is largely superfluous.</p>	<p>We consider that our proposed amendment is necessary for setting out more clearly the requirement that the name of the subscriber in a certificate should be the same as that of the applicant to whom the certificate is issued.</p> <p>To cater for information other than the name of the applicant (such as the identifier of a server system), we will expand the requirement</p>

Section	Summary of Comments Received	Proposed Responses
		under section 4.1.7 to the effect that where an RCA adopts specific procedures for verifying information of the applicant other than the name of the applicant that are placed or to be placed in the certificate, the RCA shall explain such specific procedures in its CPS.
5.3	Same comment as for section 6.4 of the Code of Practice.	Please refer to the proposed response under section 6.4 above.
5.4.3	<p>(a) <u>Regarding point (i) of the proposed amendments</u> The change is not considered necessary. The revisions necessarily restricts a CA making use of a third party validation service, which may contain revoked certificates issued by both recognized and unrecognized CAs. It is not considered necessary to specifically make reference to “recognized CAs”.</p> <p>(b) <u>Regarding point (ii) of the proposed amendments</u> It (<i>i.e. the consultation paper</i>) is proposed to replace “give the reason” by “may give the reason”. The reason of change is that CA may not always know the reasons for the revocation of a certificate. We have reservation about the rationale given. The CA should have reason for the revocation of a certificate and should make it known. The transparency of the CA operation is one of the vital quality to build up the trust and confidence of public to the CA.</p>	<p>The proposed amendment is to align with the corresponding definition in section 2 of the Code of Practice in respect of a certificate revocation list maintained by an RCA, and is not meant to refer to any “third party validation service”. Therefore, we are of the view that the proposed amendment is appropriate.</p> <p>Our proposed amendment is in line with international practices in the CA market. We have conducted survey on a number of CAs in some other parts of the world (<i>i.e.</i> Singapore, Malaysia, Australia, UK and others). Most of the CAs do not publish specific reasons for the revocation of their certificates. Therefore, we are of the view that our proposed amendment is appropriate.</p> <p>Besides, the critical piece of information to be published in the CRL is that a certificate has been revoked and should not be relied upon, irrespective of whether the reason of revocation is available.</p>