Comments Received in the Public Consultation Exercise on the Draft Code of Practice for Recognised Certification Authorities

Introduction

The draft Code of Practice (COP) for recognized certification authorities (CAs) to be issued by the Director of Information Technology Services (DITS) under Clause 39 of the Electronic Transactions Bill was published for public consultation between 25 October 1999 and 15 November 1999. As at 23 November 1999, we received written comments from the following :

- British Computer Society (Hong Kong Section);
- Cable & Wireless HKT;
- Consumer Council;
- Hong Kong Bar Association;
- Hong Kong Computer Society;
- Hong Kong Institute of Engineers (IT Division);
- Tradelink Electronic Commerce Limited; and
- An individual.

2. We have also received verbal comments from other bodies when we exchanged views with them on the draft COP.

3. Major comments which we have received on the draft COP and our initial response are summarised in the Annex.

Information Technology and Broadcasting Bureau
November 1999

Annex

Comments on the Draft COP and the Administration's Initial Response

General Responsibilities of a Recognized Certification Authority

Comments on the draft COP	The Government's Response
● The requirement for recognized CAs to keep records in respect of their operations for 7 years may impose a heavy administrative burden on the CAs.	● The records required to be retained under the COP are related to the essential business activities of a recognized CA. Their retention will facilitate the verification of the validity of recognised certificates previously issued by that CA and of the digital signatures supported by these certificates. ● There are similar requirements under other Ordinances for record keeping. For instance, under the Companies Ordinance (Cap.32), there is a requirement for the keeping of books of account.
● Recognized CAs should fully comply with the provisions of the Personal Data (Privacy) Ordinance.	● This is already covered in the draft COP.

Trustworthiness

Comments on the draft COP	The Government's Response
● Specific standards or guidelines should be provided in the COP to more clearly define the term "trustworthy".	● The DITS will issue guidelines in respect of a trustworthy system along the line set out in the Enclosure.

Comments on the draft COP	**The Government's Response**
● A recognized CA should ensure that keys are distributed in a trustworthy manner.	● There is already a requirement in the COP that a recognized CA shall provide a trustworthy system for the generation of its own and the subscribers' key pairs. Where the key pairs are generated by the CA the keys shall be distributed to subscribers in a trustworthy manner.
● Recognized CAs should establish 24-hour hotlines or Internet reporting facilities for subscribers to report lost or compromised keys.	● The COP will require recognised CAs to provide a reliable means for certificate holders to report lost or compromised keys in a timely manner.

Reliance Limit

Comments on the draft COP	**The Government's Response**
● The meaning of "reliance limit" should be clarified.	● The term has been clearly defined in the Electronic Transactions Bill.

Disclosure of Information

Comments on the draft COP	**The Government's Response**
● The COP specifies that a recognized CA shall submit progress report to DITS at a frequency to be specified by DITS. The frequency to be set by DITS should take into consideration possible administrative burden on the recognized CAs and disruption to their business activities.	● We intend to ask recognized CAs to submit progress reports at stipulated internals. Such information would enable us to monitor, upon the introduction of recognised certification services in Hong Kong, the extent of acceptance of such services in Hong Kong. In turn, we can consider whether we need to step up efforts to encourage a higher take-up so as to facilitate secure electronic transactions.

Suspension and Revocation of Certificates

Comments on the draft COP	The Government's Response
● The meaning of "reasonable time for a recognized CA to suspend or revoke a certificate upon request from the subscriber" is not clear. The issue of liability should be clarified in respect of transactions made in the period between the time when a customer has made the request and the time when the suspension or revocation actually takes effect.	● The time required for a recognized CA to revoke or suspend a certificate upon request from the subscriber as well as the allocation of liability is essentially a matter to be determined between the CA and the subscriber. We will stipulate in the COP that these matters should be set out in the certification practice statement.
● Recognized CAs should be required to check with the subscriber whose certificate has been suspended at the subscriber's request whether the suspended certificate should be revoked or reinstated within a reasonable time.	● The COP will require the recognized CA to set out in its certification practice statement the time within which it will check with the subscriber concerned as to whether a certificate suspended should be revoked or reinstated after suspension.

Inter-operability

Comments on the draft COP	The Government's Response
● The requirement to adopt an open and common interface could be difficult to meet in the case where more than one open and common interface standards exist in the market. Guidelines on inter-operability of recognized CAs may have to be issued.	● We will closely monitor the development of standards in this regard and will consider the need for guidelines if warranted.

Auditing *

Comments on the draft COP	The Government's Response
● The qualification of the person to be approved by DITS to prepare the annual report of recognised CAs should be specified.	Our initial view is that Certified Public Accountants (CPAs), i.e. professional accountants with practicing certificates issued under the Professional Accountants Ordinance (Cap. 50), supported by technical expertise on IT aspects as necessary, should have the qualification, training and professional skill to prepare the report

* The term "audit" will be deleted when we revise the COP.

Repositories

Comments on the draft COP	The Government's Response
● It will provide a more open and less "regulated" environment if recognized CAs can publish certificates in other repositories rather than mandating that they maintain their own repositories.	● We will allow a recognized CA to maintain its own repository or out-source the maintenance work to others. However, the concerned CA will be ultimately responsible for the repository.

Consumer Protection and Competition

Comments on the draft COP	The Government's Response
● There is no stipulation in the COP on the standards of conduct in respect of service promotion by the CAs and their interaction with competitors. It was considered that the best way to achieve some form of business and consumer safeguards against misleading and deceptive conduct by CAs is to include some basic guidelines in the COP.	● We will add in the COP the requirement that advertising of services by recognized CAs shall be clear, honest and truthful; that comparative advertising should be fair, reasonable and not misleading; and that claims should be capable of substantiation.
● The COP should specify whether a recognized CA is required to obtain insurance for incidental losses.	● One of the factors that the DITS will consider when granting recognition to a CA is whether there are arrangements in place to cover the liability that may arise from CA activities. We, therefore, do not consider it necessary to further specify in the COP that a recognized CA must obtain insurance for incidental losses.
● A recognized CA should be required to take out a bond to ensure its satisfactory performance.	● Under the voluntary recognition scheme, if a recognized CA fails to comply with the relevant provisions under the Bill or the COP, DITS can revoke or suspend its recognition. We, therefore, do not consider it necessary to require a recognized CA to take out a bond to ensure its satisfactory performance.

Comments on the draft COP	**The Government's Response**
● The contestability of the Hong Kong market for authentication services may be impeded because of the absence of any competition oversight, particularly in the early stages of development in this immature market. The COP should require recognized CAs to refrain from restrictive practices that would impair economic efficiency or free trade.	● We consider that market force should be sufficient to ensure that there is fair competition.

Duties of DITS

Comments on the draft COP	**The Government's Response**
● Consideration should be given to the establishment of an Advisory Council comprising representatives from Government, recognized CAs, local professional IT bodies and other interested parties to act as the authority to enforce the COP.	● We do not consider the establishment of an Advisory Council necessary.
● There should be flexibility for DITS to deal with situations in which a locally recognized CA that also operates overseas is in breach of legislation outside Hong Kong.	● In determining whether to renew, revoke or suspend the recognition of a CA, DITS will consider all relevant factors, including whether the CA has breached legislation in a place outside Hong Kong.

Miscellaneous

Comments on the draft COP	The Government's Response
● The COP should specify clearly the criteria for granting recognition to certification authorities.	● The major criteria for recognition have been set out in the Electronic Transactions Bill. We shall elaborate in the COP, where appropriate, on the practical requirements under these criteria for recognition.
● Guidelines for mutual recognition with overseas CAs should be set out in the COP to facilitate the development of cross-border e-commerce.	● We will actively explore with other Governments, either on a bilateral or multilateral basis, arrangements for cross-recognition of CAs. There is no need to stipulate such matter in the COP.
● The COP should expressly state that it is applicable to Hongkong Post as well as to other recognized CAs on a non-discriminatory basis.	● Hongkong Post is only exempted from Part VII of the Electronic Transactions Bill. As a statutory requirement, it must comply with all other requirements applicable to recognized CAs in the Bill, including compliance with the COP.
● Recognized CAs should be allowed to issue only recognized certificates.	● This should be a business decision to be taken by the recognised CAs. We see no need to set any restriction in this regard.
● Recognized CAs should be required to accept public keys submitted by subscribers.	● This is a matter to be decided between recognised CAs and their customers.

Enclosure

Guidelines on Trustworthy System

General interpretation

1 The Electronic Transactions Bill (ETB) defines a "*trustworthy system*" as 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.

2 It is important to emphasise that the term 'system' refers not just to computer hardware and software, but also to the supporting procedures, both manual and automated, as well as the overall environment within which the system operates.

3 A *trustworthy system* is a system that offers sufficient assurances that it will perform the intended functions in a consistent, reliable, and dependable manner. For a system to be accepted as trustworthy, the certification authorities (CAs) concerned must be able to demonstrate that the mechanisms, procedures, and conditions under which the system operates are adequate for the performance of its intended functions.

4 There is no absolute measure of trustworthiness; it can only be assessed against a specific context. "Reasonableness" will be assessed as fit and appropriate to the end in view, having regard to all the relevant circumstances.

Guiding principles

5 The aim of the ETB is to adopt a technology-neutral and minimalist regulatory approach. In adherence to this principle, it is the intention of Government to allow recognised CAs to determine themselves the specific technical solutions that they wish to implement in order to support their operations.

6 However, where the risk of specific aspects of a CA's operation is high, such as in relation to security sensitive functions, CAs are expected to adopt systems and procedures that adhere to standards widely accepted or recognized worldwide. In addition, as a matter of good practice, CAs should perform structured assessments of the underlying risks of their operations, and implement appropriate counter-measures for managing, mitigating and monitoring such risks.

Specific areas for consideration

7 A CA operating under a public key infrastructure (PKI) will make use of a complex integration of hardware, software and cryptographic components. These components need to be supported by appropriate security policies and procedures in order to give assurance that the CA operates in a secure environment.

8 The manner in which a CA achieves the objective of maintaining a trustworthy system may vary, depending on the specific services to be provided by the CA, the state of available technology and the situations which the CA faces. However, it is expected that all CAs should adhere to the following good practices :

Generally accepted industry good practices

- Establish formal policies, procedures and practices over the CA's operational environment, including but not limited to the following areas:
  - security management over assets;
  - personnel security;
  - physical and environmental security;

- management over systems access;
- operational management;
- development and maintenance of computer systems;
- continuity of business operations;
- maintenance of appropriate audit trails; and
- mechanism for monitoring and ensuring compliance to such policies, procedures and practices.

Good practices specific to CA functions

- Establish formal policies, procedures and practices over specific CA functions, including but not limited to the following areas:
  - management of certification practice statement;
  - legal and regulatory monitoring and compliance in respect of the CA functions;
  - key management, including the generation, storage, backup, recovery, distribution, use, destruction, and archiving of the CA's own keys;
  - management of key generating devices;
  - where appropriate, management over the range of key management services provided by the CA, such as key generation, storage, backup, recovery, destruction, archival, etc. to subscribers;
  - where appropriate, lifecycle management of tokens such as smart cards;
  - certificate management, including but not limited to the generation, issue, renewal, rekey, distribution, suspension, and revocation of certificates; and
  - management of the processing and publication of the certification revocation lists.

9 In establishing the control mechanisms, the CA should consider both the appropriateness and effectiveness of such mechanisms in relation to the specific circumstances of the CA’s services.