For Discussion **ACCOP Paper No. 2/2007**
on 9 November 2007

Advisory Committee on Code of Practice for Recognized Certification Authorities (ACCOP)

Review of The Voluntary CA Recognition Scheme and The Code of Practice

Purpose

This paper seeks Members' views for enhancing the operation of the voluntary certification authority ("CA") recognition scheme and the Code of Practice for Recognized Certification Authorities ("Code of Practice") in order to drive the adoption of digital certificates and sustain the development of e-commerce in Hong Kong.

Voluntary CA Recognition Scheme

2. The Electronic Transactions Ordinance (Cap. 553) ("ETO") was enacted in 2000 and updated in 2004 to provide a legal framework for the conduct of secure e-transactions. Under the ETO, a voluntary CA recognition scheme was established to protect consumer interests and enhance public confidence in e-transactions.

3. Under the voluntary recognition scheme, CAs may apply to the Government for recognition on a voluntary basis. The ETO empowers the Government Chief Information Office ("GCIO") to grant recognition to CAs and digital certificates. In determining whether a CA is suitable for recognition, the GCIO will take into account of the following:

i) whether the CA has the appropriate financial status for operating as a recognized CA;

ii) the arrangements to cover any liability arising from the recognized CA's business;

iii) the system, procedure, security arrangements and standards used by the recognized CA;

iv) an assessment report and a statutory declaration on the recognized CA's capability of complying with the ETO and the Code of Practice;

v) whether the CA and its responsible officers are fit and proper persons; and

vi) the reliance limits set by the CA for its digital certificates.

The Code of Practice

4. The GCIO has published a Code of Practice that specifies the standards and procedures for recognized CAs to carry out their functions relevant under the ETO. The latest version of the Code of Practice was published in 2004. Major measures to better protect the interests of users of CA services are summarized below. Full text of the Code of Practice is available at http://www.ogcio.gov.hk/eng/caro/esub3.htm.

Monitoring of Recognized CAs

5. To monitor the compliance of recognized CAs with the ETO and the Code of Practice:

i) a recognized CA is required to furnish to the GCIO an assessment report and a statutory declaration at least once in every 12 months;

ii) a recognized CA is required to furnish to the GCIO an assessment report and/or a statutory declaration when deemed necessary by the GCIO (e.g. major changes in the systems used by a recognized CA); and

iii) a recognized CA is required to submit progress reports to the GCIO at 6-month intervals regarding its operation during the report periods.

Use of Trustworthy Systems by Recognized CAs

6. A recognized CA is required to deliver secure and reliable services by using a trustworthy system. It shall enforce security control measures, carry out risk management and perform proper documentation.

Other Measures

7. A recognized CA is required to comply with all applicable ordinances and regulations regarding the privacy of personal data. It shall draw the attention of its certificate applicants that their personal data to be incorporated in their certificates will become public information and obtain consents from applicants in order to complete the application process.

8. A recognized CA is required to take care of the needs of persons with disabilities in the provision of its services in accordance with all applicable ordinances and regulations regarding the prevention of any discriminatory practice against any person with disabilities.

Current Situation and Challenges

9. Public key infrastructure ("PKI"), being the underlying technology of digital certificates, is still recognized by the IT industry as the most mature technology that can meet the full range of requirements of secure e-transactions including confidentiality, authentication, integrity and non-repudiation. For example, PKI has been adopted as one of the technologies to mitigate the emerging security risks of phishing and identity theft. The Government will also publish a Risk Assessment and Electronic Authentication Framework in 2007 to facilitate the public and businesses to determine the appropriate assurance level and security requirements for different electronic transactions.

10. There are two recognized CAs under the ETO in Hong Kong, namely Hongkong Post Certification Authority and Digi-Sign Certification Services Limited. They issue digital certificates to both individuals and organizations. Digital certificates are being used in a range of e-Government services (e.g. Electronic Tendering System and Government Electronic Trading Services), online banking, online securities trading, online betting, electronic trade declarations, electronic document exchange, etc.

11. The commonly perceived deterrent factors for the adoption of digital certificates include insufficient user-friendliness and user awareness, which are considered as the cause of the lack of general interest and business investments in developing 'killer applications' to generate greater user needs.

12. The Government has created a critical mass of digital certificate users through the free digital certificate option offered under the smart ID card replacement exercise. To further expand the user base of digital certificate and create more incentives for the market to develop e-business applications in fostering the development of cross-border e-Commerce, the forthcoming "Digital 21" Strategy will include the initiative of

cross-recognition of digital certificates between Hong Kong and the Mainland, which aims at attaining legal status in both places for digital certificates. To take forward this initiative, it is necessary to consider various aspects and initiate a review of the operation of the voluntary CA recognition scheme and the Code of Practice with a view to facilitating this initiative to proceed smoothly.

Views Sought

13. Members' views are sought for enhancing the operation of the voluntary CA recognition scheme and the Code of Practice in order to meet the challenges mentioned in paragraphs 11 and 12 above and sustain the development of e-commerce in Hong Kong. In particular, Members' views are sought on:

i) whether other factors are applicable when determining the qualifications of a CA for recognition;

ii) whether other measures are needed for monitoring the operation of a recognized CA;

iii) whether there are other specific areas on the protection of personal data of digital certificate subscribers that a recognized CA should be aware of;

iv) whether there are other specific areas on the promotion of equal opportunities that a recognized CA should be aware of when providing CA services to persons with disabilities;

v) any observation of drivers that will further boost the adoption of digital certificates for secure e-commerce and any deterring factors need to be addressed; and

vi) any necessary conditions for achieving cross-border recognition of digital certificates and any issues need to be addressed.

Secretariat of the ACCOP
Office of the Government Chief Information Officer
November 2007