For discussion on
12 December 2005

Legislative Council Panel on Information Technology and Broadcasting

Business Review of the Hongkong Post Certification Authority

PURPOSE

The Government has recently completed a business review of the Hongkong Post Certification Authority (HKPCA). This paper reports the outcome of the review and seeks Members' views on our proposed way forward.

BACKGROUND

2. To facilitate the development of e-commerce by instilling trust in the security and integrity of electronic transactions, the Government undertook in the 1998 Digital 21 Strategy to provide a clear legal framework for the conduct of secure electronic transactions and spearhead the development of a public key infrastructure (PKI)[1] in Hong Kong. Accordingly, the Electronic Transactions Ordinance (ETO) (Cap.553) was enacted in January 2000. The ETO provides for, among other things, a voluntary recognition scheme to ensure the trustworthiness of recognized certification authorities (CAs) and the digital certificates issued by them. At the same time, the Hongkong Post (HKP) was invited by the then Information Technology & Broadcasting Bureau (ITBB) to set up a public CA to issue recognized digital certificates in Hong Kong. To assess the business potential of CA services in Hong Kong, HKP discussed extensively with IT professionals and business analysts, and commissioned a market research by a local university. The prospects of e-commerce development in Hong Kong were found to be optimistic and the demand for CA services was forecast to be high. With Government's policy support, HKP agreed to offer public CA services as a commercial venture under its trading fund operation, and launched the HKPCA in January 2000.

[1] PKI refers to the technical mechanisms, procedures and policies that adopt public key cryptography and certification authority to collectively provide a framework for addressing the requirements of secure internet applications such as confidential e-mail exchange, electronic services delivery, and legally-binding electronic business transactions.

3. HKPCA now issues seven types of recognized digital certificates to individuals and organizations in Hong Kong. Its digital certificates (hereinafter referred to as “e-Certs”) are accepted for close to 70 types of e-government services (e.g. electronic filing of tax returns, online application for renewal of driving and vehicle licences, electronic tendering and electronic stamping) and over 20 types of e-commerce services (e.g. online banking, online securities trading, corporate secure data transmission, online betting and electronic trade declarations). In order to create a critical mass of personal e-Cert users, the Government together with HKPCA have taken the opportunity of the territory-wide smart identity (ID) card replacement programme launched in mid-2003 by the Immigration Department to offer an option of one-year free use of the e-Cert to be embedded in the smart ID card. As at mid-November 2005, HKPCA has issued about 1.47 million personal and organizational e-Certs, including over 1.2 million free personal e-Certs embedded in smart ID cards. The Government is also a major user of HKPCA services, subscribing to about 10,000 organizational e-Certs for use in handling confidential e-mail over the Government internal network.

4. While the Government has established a public CA to spearhead the development of PKI in Hong Kong, it has always been the intention that the number of recognized CAs should be determined by market forces under a voluntary recognition scheme. There are at present two commercial recognized CAs, namely Digi-Sign Certification Services Limited (a subsidiary of Tradelink that is partially owned by the Government) and HiTRUST.COM (HK) Incorporated Ltd. Digi-Sign, which was granted recognized CA status in July 2001, serves mainly the trading community using the services of Tradelink, but has in recent years expanded its services to support other applications such as e-banking, e-betting and e-government services. HiTRUST was granted recognized CA status in June 2002, and has yet to offer recognized certificates to the public.

THE 2005 REVIEW

5. In mid-2005, the Commerce, Industry and Technology Bureau (CITB) conducted a review of the e-Cert scheme and the HKPCA operation. We acknowledge that the HKPCA has supported the Digital 21 Strategy by spearheading the development of a PKI to facilitate the development of e-government and e-commerce in Hong Kong, and helped ensure that a recognized CA was in place to serve the community upon the enactment of the ETO. Through the provision of the e-Cert service, the HKPCA has

also successfully raised the awareness of the community of the importance of conducting e-business transactions in a secure manner. However, despite the efforts made to promote the adoption of e-Certs and the development of e-Cert applications in the past five years, the applications available in the market are not yet sufficient to create a strong and sustainable demand for e-Cert in the wider community and support a self-financing operation of HKPCA. Our views on the current market situation and the business prospects of HKPCA are set out in paragraphs 6-11 below.

A. Low utilization of e-Certs by the general public

6. Around 80% of the 1.47 million e-Certs issued by HKPCA are personal e-Certs embedded in smart ID cards and offered to the holders free of charge. A survey conducted by HKP in November 2004 revealed that among the citizens who obtained their e-Certs embedded in smart ID cards during the period from June to August 2004, only about 10% had used the e-Cert. The major reasons for the low utilization of e-Certs by the general public are -

(a) *Mismatch of security/authentication requirements* - experience shows that digital certificates are more readily used for government to government (G2G), government to business (G2B) and business to business (B2B) transactions that have high security, integrity and authentication requirements[2]. The Government Electronic Trading Services (GETS), a G2B application, is an example where digital certificates have been successfully deployed[3]. On the other hand, for the majority of business to consumer (B2C) and government to citizen (G2C) electronic transactions, there is no absolute need to use digital certificates for meeting the security and authentication requirements. Despite that e-Certs are accepted for over 100 e-government and e-commerce applications, they are used only by a small segment of the population or their use is mostly optional, e.g. as an alternative to PIN; and

[2] Digital certificates are capable of supporting secure electronic transactions in terms of authenticity, confidentiality, integrity of data, and non-repudiation of the transactions. Such certificates can be used in data encryption and digital signature of electronic records.

[3] GETS refer to the electronic submission and processing of six trade-related documents required by the Government, namely, import and export declarations, dutiable commodities permits, cargo manifests (excluding road mode), certificate of origin, production notifications, and textiles notifications under the Textiles Trade Registration Scheme.

(b) *Lack of killer applications* – there is not yet a "killer application" that could drive the adoption of e-Cert by the general public. Authentication for Internet banking was once thought to be a promising B2C killer application in view of the increasing risks of fraudulent websites. Some major banks have nonetheless chosen other means (e.g. one-time password token or Short Message Service (SMS)) to satisfy the "two-factor authentication" requirement of the Hong Kong Monetary Authority. As for e-government services, the Government will first consider the need for and the level of authentication required to verify the identity of the service users; and the general direction is to confine the use of e-Cert to transactions requiring the highest level of security in authentication (e.g. voter registration).

B. Lack of a sustainable business case

7. Up to the end of 2004-05, the Post Office Trading Fund and CITB have put in a total of $208 million[4] (net of revenue) in the commissioning, operation and promotion of the e-Cert scheme. HKPCA incurred a cumulative operating loss of about $89.4 million ($144 million if depreciation is included) as at end March 2005.

8. At present, only about 40,000 of the 1.47 million e-Certs (or about 3%) are valid fee-paying e-Certs. These fees, together with other incomes from the CA operation, cover less than 40% of the annual operating costs incurred by HKPCA. In the absence of killer applications, we do not envisage a massive renewal of the e-Cert embedded in smart ID cards once the holders are required to pay an annual subscription[5]. Moreover, the scope of HKP's business is restricted to those prescribed in its trading fund legislation. Hence, when compared to and competing with its commercial counterparts, HKP has limited flexibility in providing value-added commercial services or bundled services to drive the adoption of e-Certs and in generating other income to support its CA operation.

9. Without a sustainable subscription base and income source, we envisage that it would be difficult for HKPCA to achieve a self-financing operation in the foreseeable future. The alternatives will be for HKP to

[4] The investment comprises $158 million from Post Office Trading Fund and $50 million provided by CITB to support the HKPCA operation during the five-year period.

[5] HKPCA has extended the free use of the e-Certs in Smart ID cards up to March 2006 for holders whose e-Certs should have expired before this date.

continue cross-subsidization from its other trading fund operations, or for the Government to fund the operating deficit.

C. Availability of substitutes

10. While the PKI is still recognized by the IT industry as the most mature technology available to address the full range of authenticity, confidentiality, integrity and non-repudiation issues of electronic transactions as discussed in paragraph 6(a) above, the use of e-Certs in the conduct of online transactions in Hong Kong is still mostly optional.

11. With two commercial recognized CAs operating in Hong Kong that are capable of providing recognized digital certificates to both organizations and members of the public, it will be difficult for the Government to justify financing a public CA indefinitely.

PROPOSED WAY FORWARD

12. In the light of the foregoing analysis, the Government has come to the view that the current mode of operation of the public CA, which requires substantial funding support from the Government and the HKP's cross-subsidization from its postal services, is not sustainable in the longer term. We consider that we should explore possible synergy with the private sector by inviting the latter to participate in running the e-Cert services and to come up with new value-added services/businesses that could engender a self-financing public CA operation. Accordingly, HKP will conduct a Request for Proposal (RFP) exercise in the first half of 2006 to ascertain if any interested parties in the private sector are prepared to run the e-Cert operation for a fixed period (e.g. until 2010/11). Bidders may propose to offer new value-added services or e-commerce applications under separate brands, in addition to running the HKPCA operation. The Postmaster General (PMG) will remain a recognized CA under the ETO[6] and be responsible for the performance of its private sector partner in providing recognized certification services.

13. It is estimated that the RFP exercise will close in June/July 2006. If a successful bidder is identified, HKP would award the contract before end of 2006 to enable the selected bidder to take over its CA operation in early 2007. In the event there is no successful bidder, the Government will support the HKPCA until end March 2008 so as to allow

[6] The ETO provides that the PMG is a recognized CA and that the PMG may by himself or by the officers of HKP perform the functions and provide the services of a CA and services incidental or related to the functions or services of a CA.

sufficient time for the existing subscribers of e-Certs and business partners of HKPCA to complete the necessary transitional arrangements and switch to the service of other recognized CAs or other authentication solutions. The HKPCA will proceed to wind down its operations, save for the residual functions required under the ETO and the Code of Practice issued by the Government Chief Information Officer, before end March 2008.

CONCLUSION

14. The proposed two-stage approach outlined in paragraphs 12-13 above seeks to meet the dual objectives of reducing the longer-term public funding support for the HKPCA through inviting private sector participation in the e-Cert scheme, and providing a suitable transitional period to cater for the operational needs of the existing e-Cert users/business partners.

15. We have also considered the option of terminating the e-Cert operation with effect from 2006-07, but found this infeasible because the Government and some commercial organizations rely solely on the e-Certs to support their internal operations and/or transactions with buyers/suppliers. To minimize the disruption to these operations and the inconvenience to the customers, the HKPCA is obliged to allow 18-24 months for the subscribers/users to switch to alternative service providers/solutions.

ADVICE SOUGHT

16. Members are invited to note the outcome of the Review and comment on the proposed way forward set out in paragraphs 12-13 above.

Office of the Government Chief Information Officer
Commerce, Industry and Technology Bureau
November 2005