Hong Kong Electronic Signature Law and Certification Authority Regulations: Promoting E-commerce in the World's Most Wired City

Stephen E. Blythe

Follow this and additional works at: http://scholarship.law.unc.edu/ncjolt

Part of the Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncjolt/vol7/iss1/14

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Journal of Law & Technology by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
Hong Kong is perhaps the “most wired” city in the world and has one of the best environments for e-commerce. Hong Kong’s e-signature law is a major contributing factor to this environment. The Electronic Transactions Ordinance Act of 2000 (“ETO”) allowed the utilization of only one form of electronic signature—digital. This ran contrary to the trend in global electronic signature law; which encourages nations to give legal recognition to more than one. Accordingly, the ETO was amended in 2004 to allow for: (1) multiple forms of electronic signatures to be used in the private sector, with retention of the digital signature requirement for official electronic communiqués with the government; (2) electronic delivery whenever the law specifies that delivery is to be “by post or in person;” (3) bifurcation of the Annual Report of Compliance Assessment pertaining to certification authorities (“CA”), with one part to be performed by an independent auditor, and the other part to be achieved with submission of a sworn statement from the CA; and (4) a requirement that major changes in the CA’s organization must be reported immediately to the government. Also in 2004, and pursuant to the ETO, the government issued the Code of Practice, a lengthy document meticulously specifying the standards and procedures for carrying out the functions of a CA. The Code of Practice includes detailed requirements for both the CA’s Annual Report of Compliance Assessment, as well as the requirements for the contents of the CA’s Certification Practice Statement. Both of these documents are required to be submitted to the government by

---

1 Ph.D. Candidate (Law), The University of Hong Kong; Ph.D. (Business Administration), University of Arkansas, 1979; J.D. cum laude, Texas Southern University, 1986; LL.M., University of Houston, 1992; LL.M. with distinction, University of Strathclyde (Scotland), 2005. Attorney at Law & C.P.A., Texas.
the CA and play an important role in oversight of their activities. Therefore, while the amended ETO now recognizes the validity of more than one form of electronic signature, it is strengthening the degree of trustworthiness of digital signatures through more stringent regulation of CAs. However, consumer protections remain deficient; the author recommends that the ETO be amended again to rectify this oversight.

I. MADE FOR EACH OTHER: E-COMMERCE AND THE WORLD’S “MOST WIRED” CITY

Hong Kong may be the “most wired” city in the world. With a state-of-the-art telecommunications infrastructure, Internet access is available to every business and household in Hong Kong. More than 90% of all households and business firms have broadband (DSL) connectivity; in early 2004, Hong Kong had about 1.5 million DSL subscribers, more than 35% of the total Internet subscriber base. More than 100 Internet Service Providers do business in Hong Kong, and ten of those are large and very-well-financed organizations. In survey results released by the International Telecommunications Union in 2003, Hong Kong finished in first place in Internet access affordability, with average Internet cost being only 0.19% of per-capita income.

The government of Hong Kong aspires to make its city a global e-commerce leader. After the governor of Hong Kong declared
that Information Technology ("IT") was critical for business success, the number of students enrolled in IT-related programs doubled.\(^9\) The "Digital 21 Initiative" was launched in 1998, a "package of initiatives through which Government, business, industry and academia\(^8\) can work together to make Hong Kong a 'leading digital city in a globally connected world.'\(^11\) Digital 21 includes the following projects: (1) the creation of the "Cyberport" in 2002, the "Silicon Valley" of Hong Kong which contains office and residential space for more than 100 high-tech business firms and their employees;\(^12\) (2) the government's adoption of the multi-application "smart" identity card (using two thumbprints as the biometric identifier) for all Hong Kong citizens and residents—besides being used for "automated immigration clearance at border control points,"\(^13\) it can also store a digital certificate (with free digital signature service available at the Hong Kong Post Office for the first year of use)\(^14\) and can be used as a public library card;\(^15\) and (3) an emphasis on greater electronic delivery of public services ("e-government")—by the end of 2003, most public services amenable to electronic delivery had become available online,\(^16\) with the most popular options being "payment of government bills, marriage appointment booking and submission of trade-related documents."\(^17\)

---

\(^9\) Chun & Griffy-Brown, *supra* note 2, at ¶ 8.

\(^10\) Development of Offshore E-commerce Services in Hong Kong, *supra* note 8. The government of Hong Kong’s Information Technology & Broadcasting Bureau ("ITBB") worked with its advisory group (consisting of representatives from government, business, industry and academia), the Information Infrastructure Advisory Committee, in developing the "Digital 21" programs.


\(^12\) Development of Offshore E-commerce Services in Hong Kong, *supra* note 8.

\(^13\) Fung, *supra* note 7.

\(^14\) Fung, *supra* note 7.

\(^15\) Fung, *supra* note 7.


\(^17\) Development of Offshore E-commerce Services in Hong Kong, *supra* note 8.
All of these thrusts are beginning to pay huge dividends. In April 2005, a worldwide survey sponsored by the Economist Intelligence Unit concluded that Hong Kong has the best e-commerce environment in Asia.\textsuperscript{18} In addition to its stellar infrastructure, Hong Kong's e-signature law is also state-of-the-art, providing a firm foundation for undertaking e-commerce transactions with confidence and assurance.\textsuperscript{19}

II. OBJECTIVES OF THE ARTICLE

The objectives of this article are to: (1) give the reader an appreciation for the impressive success of Hong Kong's creation of a high-tech infrastructure; (2) concisely describe the basic aspects of public key infrastructure technology and digital signatures, and explain its impact on e-commerce transactions; (3) describe Hong Kong's original Electronic Transactions Ordinance, and explain its recent amendments and their justification; (4) describe Hong Kong's recently-adopted regulations pertaining to Certification Authorities and their justification; and (5) make recommendations for improvement of Hong Kong e-commerce law.

III. THE ELECTRONIC TRANSACTIONS ORDINANCE

The Electronic Transactions Ordinance ("ETO")\textsuperscript{20} was enacted on January 5, 2000, and was fully implemented by April of that year.\textsuperscript{21} It was influenced\textsuperscript{22} by the American Bar Association

\textsuperscript{18} Development of Offshore E-commerce Services in Hong Kong, supra note 8.

\textsuperscript{19} Hong Kong tax law has also helped. The Port of Hong Kong is virtually duty-free, with tariffs placed on only a few categories of goods (e.g., alcoholic beverages).

\textsuperscript{20} Electronic Transactions Ordinance ("ETO"), No. 1, (2000) O.H.K.


Digital Signature Guidelines, the Utah Digital Signature Act, the UNCITRAL Model Law on Electronic Commerce, the U.S. Uniform Electronic Transactions Ordinance, and the European Union’s Digital Signature Directive.

A. Legal Recognition of Digital Signatures

In 1995, Utah became the first jurisdiction in the United States to enact a digital signature law. In that statute, Utah recognized only digital signatures; it did not recognize other types of electronic signatures. Although such a law provides for relatively more security in e-commerce transactions, it carries the disadvantage of being too restrictive. Nevertheless, Hong Kong

---


26 UNIF. ELEC. TRANSACTIONS ACT (“UETA”), 7A U.L.A. 252 (2002). UETA is a model law written by the United States National Conference on Commissioners on Uniform State Laws for consideration for enactment by the respective state legislatures. Since its dissemination, UETA has been adopted in almost all of the United States jurisdictions, either in its original form or with amendments.


29 An electronic signature may be defined as “any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with the intent to authenticate a writing.” See infra note 86, at 511. There are many forms of electronic signatures; examples include “a name typed at the end of an e-mail message, a digitized fingerprint, a digitized image of a handwritten signature that is attached to an electronic message, a retinal scan, a pin number, or a digital signature.” See infra, not 86, at 511.
followed the Utah example in its original ETO recognizing only the digital signature, and did not grant recognition to other forms of electronic signatures. In granting recognition to the digital signature, Hong Kong was effectively telling the world that it would treat a digital signature the same as it treated a handwritten, "hard copy" signature.

Under the ETO, "digital signature" was defined similarly to the Utah Act, as follows:

An electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine: (a) whether the transformation was generated using the private key that corresponds to the signer's public key; and (b) whether the initial electronic record has been altered since the transformation was generated.

The original ETO was not "technologically-neutral." Instead, it favored one technology—the digital signature—to the exclusion of other forms of electronic signatures. The need for heightened security seemed to be paramount in the mind's eye of the ETO's creators. However, there are tradeoffs. The attainment of greater security, achieved by only granting recognition to the digital signature, meant that e-commerce participants' choices would be limited. They would be forced to use a technology that offered high security, but one that perhaps also would be more expensive, less convenient, too complicated, and less adaptable to technologies employed by other nations.

---

30 ETO, supra note 20, §§ 2, 6.
31 ETO, supra note 20, §§ 2, 6.
33 It is rude for a writer to divulge the ending in the middle of a story, but the astute (if previously uninformed) reader may now correctly surmise that the ETO was subsequently amended! The changes, resulting in a greater degree of private-sector, technological-neutrality in Hong Kong electronic signature law, will be covered below.
B. Concomitant Effects of Sole Recognition, of the Digital Signature

Sole recognition of the digital signature, to the exclusion of other types of electronic signatures, has these concomitant effects: (1) employment of an asymmetric cryptology; (2) utilization of public key infrastructure ("PKI"); and (3) regulation of Certification Authorities. 34

1. Asymmetric Cryptology

Under the Utah Model, adopted in the original ETO, "digital signatures receive legal protection only if asymmetric key cryptology produced the digital signature." 35 Such a system employs double keys—one key is used to encrypt the message by the sender, and a different, albeit mathematically-related, 36 key is used by the recipient to decrypt the message. 37 The sender has a private key, known only to him/her, 38 used to generate the digital signature, and the recipient uses the public key, often available online, to verify that the proper party created the message and that it has not been altered during transmission. 39 This is a very good system for e-commerce, since two stranger-parties, perhaps living far apart, can confirm each other's identity and thereby reduce the likelihood of fraud in the transaction.

34 Wu, supra note 22.
37 By contrast, "symmetric" cryptology employs one key. The same key is used for both encryption and decryption. Thus, the sender and recipient are using the same key. There are two disadvantages: (1) two stranger-parties using a public network have no way to securely transmit symmetrical keys to be used in subsequent transmissions; and (2) the transfer of a key in such a situation could possibly be intercepted or modified by a third party. See Robin C. Capehart & Mark A. Starcher, Wired, Wonderful West Virginia: Electronic Signatures in the Mountain State, 104 W. VA. L. REV. 303, 311-12 (2002).
38 PKI Assessment Guidelines, supra note 36, at 305.
2. PKI

Before a party can digitally "sign" anything, he/she must first be in possession of a pair of keys—the private key and a related public key.\(^{40}\) The party will apply to a Certification Authority ("CA") to confirm his/her identity and to issue the pair of keys. After the applicant's identity has been confirmed, the CA will issue a certificate as verification of the subscriber's identity. The certificate will be placed in a public repository, most often the CA's website. Whenever the subscriber digitally signs a message, the CA confirms the signature of the sender; whereupon, the CA informs the recipient of the encrypted message which "public key" is necessary to decode the message.\(^{41}\) At that point, the recipient is able to access the public key which is used to decrypt the sender's message.\(^{42}\)

The Utah model prescribes an open PKI system.\(^{43}\) In an open system, unlike a closed one, the same certificate is used for all parties with which the subscriber wants to transact. Accordingly, it is relatively easier to enter into a transaction because it is easier to digitally sign a document.\(^{44}\) However, if the subscriber's private key is lost or compromised, the consequences are potentially much more egregious because there is a greater likelihood that the

---

\(^{40}\) Aristotle Mirzaian, *Electronic Commerce: This is Not Your Father's Oldsmobile*, 26 Rutgers L. Rev. 7, 13 (2002).


\(^{43}\) Wu, *supra* note 22. In a closed PKI system, the user-subscriber must obtain a different certificate for different groups of people with whom they want to conduct transactions. The advantage is that legal liability is potentially more limited, since the CA and members of a certain group may enter into agreements defining their rights and responsibilities toward each other; in an open PKI system, public law defines the rights and responsibilities of the parties. On the other hand, the disadvantage of the closed PKI system is that it is relatively more difficult than the open system to digitally sign a document and to enter into a transaction. Wu, *supra* note 22.

\(^{44}\) Wu, *supra* note 22 (citing D.J. Greenwood, *Risk and Trust Management Techniques For an "Open but Bounded" Public Key Infrastructure*, 38 Jurimetrics J. 277 (1998)).
subscriber may be defrauded.\textsuperscript{45} Notwithstanding the adoption of an open system, the ETO does contain some features which are typical of a closed system, such as: (1) all Recognized CAs must issue annual Certification Practice Statements; and (2) Recognized CAs also have the option of specifying monetary liability limits in the certificates they issue.\textsuperscript{46} Both of these considerations have the effect of reducing the potential legal exposure of the Recognized CA, and this is akin to a closed system. Therefore, it may be said that the Hong Kong System is a “hybrid” one rather than being purely open or purely closed.

3. Regulation of Certification Authorities

The ETO does not require a CA to apply for “recognition.” An “unrecognized” CA may legally operate in Hong Kong. However, the ETO does not apply to an unrecognized CA. As a result, a digital signature issued by an unrecognized CA has no legal recognition, and accordingly, no legal rights and obligations will attach to it that are enforceable in a court of law. Thus, although it is a “voluntary” system,\textsuperscript{47} an unrecognized CA faces tremendous pressure to become “recognized.” In a \textit{de facto} sense, the system is not really voluntary; it is compulsory.

Furthermore, an unrecognized CA has unlimited liability, whereas a Recognized CA (“RCA”) is generally able to limit its liability under the ETO.\textsuperscript{48} For example, an RCA will not be liable for loss incurred due to reliance on a false or forged digital

\textsuperscript{45} Benjamin Wright has argued forcefully that PKI does not result in the elimination or even the reduction of risk; it simply transfers it to the private key. In a PKI system, it is critical for the private key holder to keep it secret and to maintain security over it. Although a sophisticated party involved with “high-end financial deals” may appreciate the advantages of the PKI system, the unsophisticated person may be uncomfortable in being responsible for the all-powerful private key. \textit{See} Symposium, \textit{Cyber Rights, Protection, and Markets}, “Eggs in Baskets: Distributing the Risks of Electronic Signatures,” 32 \textit{UWLA L. REV.} 215, 219–220 (2001).

\textsuperscript{46} Wu, \textit{supra} note 22.

\textsuperscript{47} ETO, \textit{supra} note 20, § 20(1) (stating “[a] certification authority may apply to the Director to become a recognized certification authority for the purposes of this Ordinance”) (emphasis added).

\textsuperscript{48} ETO, \textit{supra} note 20, § 42.
signature supported by its certificate, provided the RCA has complied with all material requirements of the ETO and the Code of Practice. Additionally, the RCA may reduce its exposure by placement of a "cap" on its legal liability, i.e., by stating a "reliance limit." The RCA is afforded limitation of liability because of two reasons: (1) it will speed up the issuance of certificates, since the CA will not have to engage in so much research of the applicant; and (2) it will make the purchase of the digital signature cheaper to the applicant, since the RCA will have less expenses due to diminished need for liability insurance coverage. On the other hand, the ETO has been criticized for shifting "an immense liability burden onto consumers who conduct electronic transactions through the RCA."

But note—the above does not give the RCA carte blanche to be negligent, reckless, or to intentionally deceive. The RCA will be liable for damages incurred due to reliance on erroneous information stated in a certificate or in a repository, if the RCA had a duty to confirm the information according to the Code of Practice or the Certification Practice Statement, but negligently, recklessly or intentionally failed to do so.

The RCA is afforded relatively greater respect and status than its unrecognized counterpart. Subscribers, other interested parties, and the general public place relatively greater trust and reliance in an RCA. This is because RCA status is only granted to those CAs with: (1) a good financial position; (2) good liability insurance coverage; (3) trustworthy systems; (4) good security arrangements; (5) high standards required for issuance of certificates; (6) officers who are "fit and proper persons;" and (7) notice of acceptance reliance limits which are stated in the certificates.

The RCA must be able to show that it uses a trustworthy system of issuing and withdrawing certificates and displaying them

---

49 ETO, supra note 20, § 42(1).
50 ETO, supra note 20, § 42(2).
51 Wu, supra note 22. The author contends that the ETO in its current form is deficient in its consumer protections. Id. See discussion infra Recommendations Section.
52 ETO, supra note 20, § 42(3).
53 ETO, supra note 20, § 22.
in a public repository. The Director of Information Technology issued a Code of Practice for RCAs, which delineates the standards and procedures to be used by RCAs for implementation of the ETO.\textsuperscript{54} Furthermore, every RCA is required to submit a report to the Director of Information Technology Services, a Certification Practice Statement ("CPS"), stating the standards and procedures employed in issuing certificates and in carrying out its other tasks.\textsuperscript{55} The CPS, in turn, is used to determine the legal liability limits of the RCA.

Interestingly, the ETO established the Hong Kong Post Office as an RCA.\textsuperscript{56} Several reasons may account for this. One is that it is simply convenient to go to a local post office in one's neighborhood to find an RCA. Another reason may be that the lawmakers were unsure as to whether private firms\textsuperscript{57} would be

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{54} See infra note 157.
\item \textsuperscript{55} ETO, supra note 20, § 44; see infra note 307 (stating that an up-to-date copy of the CPS must be kept on file with the government and in the RCA's repository).
\item \textsuperscript{56} ETO, supra note 20, §§ 34, 35. This was criticized by the Chamber of Commerce on the ground that it will give the public sector too much influence upon electronic transactions, resulting in a "playing field which is possibly not level" for private CAs. See infra note 96, at 4.
\item \textsuperscript{57} Digi-Sign Certification Services, Ltd., ("Digi-Sign") a wholly-owned subsidiary of Tradelink Electronic Commerce, Ltd., became the first private CA in Hong Kong. By 2004, it had more than 170,000 subscribers. Its website is located at http://www.digi-sig.com. Later, HiTrust became the second private CA in Hong Kong. It is affiliated with the Veri-Sign Trust Network, and its website address is http://www.hitrust.com.hk. On May 18, 2004, Digi-Sign announced it had entered into a cooperative agreement with Guangdong Electronic Certification Authority ("GECA") to jointly issue a "Unified-Cert." The Unified-Cert makes it possible for PRC residents (possessing valid travel documents to Hong Kong, or a Hong Kong Identity Card) to simultaneously obtain, in one application, both the Digi-Sign ID-Cert and the digital certificate of GECA. This service is expected to lead to an increase of online activities between Hong Kong and Guangdong Province. GECA was established by the Guangdong provincial government in 2000 and now has more than 180,000 subscribers. Its website address is http://www.cnca.net. For a brief discussion of the E-commerce regulations of Guangdong Province, see Andrew Zheng, "E-commerce in China—Guangdong Promulgates Comprehensive Legislation," available at http://www.perkinscoie.com/page.cfm?id=51; Digi-Sign and Guangdong Electronic Certification Authority Cooperate on Unified-Cert Service, available at http://www.tradelink.com.hk/eng/ 20040518.html.
\end{itemize}
\end{footnotesize}
interested in becoming a CA and they wanted to ensure that at least one well-known CA was available to get the implementation of the ETO underway.

The Director has a number of enforcement powers which may be exercised against RCAs. Their recognition may be suspended or revoked if they do not: (1) maintain a trustworthy system; or (2) abide by the provisions of the ETO, the Code of Practice, or its own CPS.\(^{58}\)

C. Obligation of Secrecy

In reaction to the public concern over security of private information, the ETO included a provision mandating secrecy. Persons attaining access to confidential data while performing functions covered by the ETO (e.g., the RCA’s attainment of the subscriber’s personal information in an application for a certificate) are prohibited from disclosure to other persons.\(^{59}\) The ETO also forbids the knowing or reckless dissemination of false information whilst engaged in a function under the statute (e.g., giving false information to an RCA in an application for a certificate),\(^{60}\) or for persons pretending to be an RCA.\(^{61}\) Violators may be subject to fine or imprisonment.\(^{62}\)

D. ETO Not Applicable in Certain Specified Situations

The old-fashioned “hard copy” is still mandatory in the creation of the following legal documents: wills, codicils and

---

\(^{58}\) ETO, supra note 20, §§ 23, 24.

\(^{59}\) Exceptions are allowed where it is necessary to carry out a function of the ETO, pursuant to a court order, or for the purpose of implementation or otherwise pertaining to a criminal proceeding in Hong Kong.

\(^{60}\) ETO, supra note 20, § 47.

\(^{61}\) ETO, supra note 20, § 48.

other testamentary documents;\textsuperscript{63} anything to do with the creation, change or revocation of an express trust;\textsuperscript{64} a power of attorney;\textsuperscript{65} documents required to be stamped pursuant to the Stamp Duty Ordinance (Cap. 117);\textsuperscript{66} government grants and leases;\textsuperscript{67} deeds, conveyances, judgments, written instruments, \textit{lis pendens} and documents effecting a floating charge (referred to in sect. 2A) pursuant to the Land Registration Ordinance (Cap. 128);\textsuperscript{68} assignments, mortgages and legal charges under the Conveyancing and Property Ordinance (Cap. 219);\textsuperscript{69} oaths and affidavits;\textsuperscript{70} statutory declarations;\textsuperscript{71} judgments or orders of a court;\textsuperscript{72} warrants issued by a court or a magistrate;\textsuperscript{73} and negotiable instruments.\textsuperscript{74}

Furthermore, in Hong Kong (as in most jurisdictions of the world), forget about using email to file court documents. The ETO is not applicable to matters coming before the following courts, government agencies or government officials: the Court of Final

\textsuperscript{63} ETO, \textit{supra} note 20, sched. 1(1). As evidence that electronic documenting is on the march, even this common exception may be on its way out. \textit{See} Chad Michael Ross, Comment, \textit{Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will}, 35 U. MEM. L. REV. 603 (2005). Tennessee became the first U.S. state to recognize that a computer-generated signature may be used by a testator to "sign" the document. The testator had affixed the electronic signature in the presence of two witnesses. The appellate court found that "[a] computer-generated signature made by a testator comes within the description of 'any other symbol or methodology executed or adopted by a party with intention to authenticate a writing or record,' and if affixed before two or more attesting witnesses, satisfies the requirements for a testator to execute a will." \textit{Id.} at 603.

\textsuperscript{64} ETO, \textit{supra} note 20, sched. 1(2). However, this exclusion does not refer to a resulting, implied or constructive trust.

\textsuperscript{65} ETO, \textit{supra} note 20, sched. 1(3).

\textsuperscript{66} ETO, \textit{supra} note 20, sched. 1(4). However, this exclusion does not refer to a contract note relating to s 5A of the Stamp Duty Ordinance.

\textsuperscript{67} ETO, \textit{supra} note 20, sched. 1(5).

\textsuperscript{68} ETO, \textit{supra} note 20, scheds. 1(6), 1(8).

\textsuperscript{69} ETO, \textit{supra} note 20, sched. 1(7).

\textsuperscript{70} ETO, \textit{supra} note 20, sched. 1(9).

\textsuperscript{71} ETO, \textit{supra} note 20, sched. 1(10).

\textsuperscript{72} ETO, \textit{supra} note 20, sched. 1(11).

\textsuperscript{73} ETO, \textit{supra} note 20, sched. 1(12).

\textsuperscript{74} ETO, \textit{supra} note 20, sched. 1(13).
Appeal;\textsuperscript{75} the Court of Appeal;\textsuperscript{76} the Court of First Instance;\textsuperscript{77} the District Court;\textsuperscript{78} the Mental Health Review Tribunal established pursuant to the Mental Health Ordinance (Cap. 136);\textsuperscript{79} the Lands Tribunal;\textsuperscript{80} a coroner appointed under § 3 of the Coroners Ordinance (Cap. 504);\textsuperscript{81} the Labour Tribunal;\textsuperscript{82} the Obscene Articles Tribunal established under the Control of Obscene and Indecent Articles Ordinance (Cap. 390);\textsuperscript{83} the Small Claims Tribunal;\textsuperscript{84} and magistrates.\textsuperscript{85}

E. Deficiencies of the Original ETO

1. No Mention of Foreign CAs

E-commerce is an international phenomenon.\textsuperscript{86} If a party in Hong Kong engages in a commercial transaction with a party in a foreign country, and the foreign party uses a certificate issued by a foreign CA does the ETO recognize that certificate? That issue was not dealt with in the original ETO.\textsuperscript{87}

2. No Mention of Insolvency of CAs

What if the CA, after issuing the certificate, becomes insolvent and declares bankruptcy? What is the impact of that situation on the legal viability of the certificate generally, and upon the legal

\textsuperscript{75} ETO, supra note 20, sched. 2(a).
\textsuperscript{76} ETO, supra note 20, sched. 2(b).
\textsuperscript{77} ETO, supra note 20, sched. 2(c).
\textsuperscript{78} ETO, supra note 20, sched. 2(d).
\textsuperscript{79} ETO, supra note 20, sched. 2(e).
\textsuperscript{80} ETO, supra note 20, sched. 2(f).
\textsuperscript{81} ETO, supra note 20, sched. 2(g).
\textsuperscript{82} ETO, supra note 20, sched. 2(h).
\textsuperscript{83} ETO, supra note 20, sched. 2(i).
\textsuperscript{84} ETO, supra note 20, sched. 2(j).
\textsuperscript{85} ETO, supra note 20, sched. 2(k).
\textsuperscript{86} For insights into the complexity of conflict of laws rules in international E-commerce, see Jochen Zaremba, International Electronic Transaction Contracts Between U.S. and EU Companies and Customers, 18 Conn. J. Int'l L. 479 (2003).
\textsuperscript{87} Wu, supra note 22.
liability of the CA specifically? This important issue is not addressed in the ETO.88

3. No Mention of Legal Obligations of Subscribers

The ETO devotes a considerable amount of attention to the duties and responsibilities of CAs. In particular, the statute goes to great pains to ensure that the CA uses a "trustworthy" system. However, the original ETO gave scant attention to the duties and responsibilities of subscribers, and to their actions which could undermine the trustworthiness of the system. Subscribers should be held accountable and legally responsible for their actions which reduce the security of the system, e.g.: (1) not maintaining adequate security controls over the private key; (2) committing errors in the creation of the message and the digital signature; and (3) using unreliable hardware or software which could lead to mechanical errors. If the CA has responsibilities, so does the subscriber.89

4. Deficient Consumer Protections

Sometimes, the e-commerce buyer finds herself at the mercy of the predator-seller. Especially, the buyer is in need of protections requiring the seller to prominently display electronic notices pertaining to the sale, and to ensure that the buyer will be able to gain access to those notices.

5. The "Hamstrung" Effect

As mentioned, the original ETO followed the Utah Model and adopted the digital signature as the only recognized technology. This degree of devotion to one technology "locked in" the ETO to the digital signature exclusively and made it less open-minded and considerate of other, potentially better technologies. Technology changes and evolves at a rapid pace indeed. Accordingly, the original ETO had the drawback of becoming passé and out-of-date overnight, just as soon as some new, better form of technology

88 Wu, supra note 22.
89 Wu, supra note 22.
made its appearance.\(^9\) The original ETO was criticized for being too inflexible, and this criticism (and others) led to a number of amendments in the statute.\(^9\)

**IV. THE ITBB’S CONSULTATION PAPER: RECOMMENDED AMENDMENTS TO THE ETO**

In the summer of 2001, the Hong Kong Government’s Information Technology and Broadcasting Bureau (“ITBB”) undertook an internal governmental review of the ETO for the purpose of ensuring that Hong Kong’s e-commerce law remained up-to-date.\(^2\) Toward that end, all Hong Kong governmental departments were consulted and asked to state their views on issues pertaining to the ETO. At the end of the of the consultations, the viewpoints were compiled into a group of preliminary proposals for amendment of the ETO.\(^3\) In March, 2002, the ITBB issued its findings to the public in the *Consultation Paper on the Review of the Electronic Transactions Ordinance* and requested the public to comment on them. A consideration of the specific proposals follows.

**A. Proposals for Legal Recognition of Other Forms of Electronic Signatures**

First, the ITBB stated its view that all governmental departments should review whether the digital signature requirement can be removed, “in order to facilitate electronic

---

\(^9\) This criticism of the Utah Model is viable. However, there is another side to the story. Until a better technology comes along, the digital signature is one of the best—if not the best—for E-commerce transactions. *See* Stephen E. Blythe, *supra* note 26, at 21 (contending that the United Kingdom and the United States are “too 'minimalist' and need to achieve more stringency and standardization in their e-signature laws”).


\(^2\) ITBB, *supra* note 21, at 1.

\(^3\) ITBB, *supra* note 21, at 2-9.
transactions." They proposed that other forms of electronic signatures—besides digital signatures—should be considered for legal recognition.

The Hong Kong General Chamber of Commerce was pleased to see the ITBB’s consideration of other forms of electronic signatures. According to the Chamber of Commerce, this would be consistent with UNCITRAL’s Model Law on Electronic Commerce, which advocated technological-neutrality and a “minimalist” approach with as little regulation as possible. However, the Chamber of Commerce also noted that their concerns were not completely allayed by the government’s proposals stating: “There should thus be no need to confer such sweeping powers, including determination of even the form, manner, and format of electronic record, to the Secretary for Information Technology and Broadcasting . . . . This regulatory approach is too restrictive.”

1. Proposal to Use the Pin As a Substitute for the Digital Signature: Rejected

As previously mentioned, there are a number of electronic signatures available; the digital signature is only one type of electronic signature. Interestingly, the ITBB advocated that the personal identification number (“PIN”) be seriously considered for adoption as an alternative to the digital signature requirement. They observed that the PIN was already used extensively in banking operations around the world and in the implementation of E-government functions in many countries. “With proper management, [the PIN] can . . . satisf[y] the signature requirement . . . where the level of security offered by it is commensurate with the risk of the service involved, e.g. where

---

94 ITBB, supra note 21, at 2.
95 ITBB, supra note 21, at 2.
97 Id. at 3.
98 ITBB, supra note 21, at 3.
there is [an] already established relationship between the parties . . . ." It99 Their argument was that the PIN offered more economy and convenience for the user, albeit with less security, and that the individual user should decide the level of security desired.100

In its response to the government’s Consultation Paper on the Review of the Electronic Transactions Ordinance, the Chamber of Commerce embraced the proposal to grant legal acceptance to PINs as an alternate form of electronic signature.101 Naturally, they took a “pro-market” approach to the issue: “We would emphasize that the aim of electronic signature authentication is to simplify, not complicate electronic commerce.”102 The Chamber of Commerce cited UNCITRAL’s stance that electronic signatures should be presumed to be valid and enforceable, and should not become hamstrung by any specific technical requirements.103 They adopted the ITBB’s economic argument as well: “[I]n a free market different levels of security will be needed by different businesses, at different costs.”104

However, the wholesale acceptance of the PIN as a viable substitute for the digital signature was not to be. This proposal did not become an amendment to the ETO. The serious flaws in the proposal were exposed in a journal article written by a group of law professors at The University of Hong Kong (“HKU”).105 As a

99 ITBB, supra note 21, at 3.
100 ITBB, supra note 21, at 3.
102 Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, supra note 96, at 3.
103 Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, supra note 96, at 3.
104 Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, supra note 96, at 3.
foundation for discussion, the article noted that a signature must satisfy three basic requirements: (1) it must identify the signatory in order to show that the document carries his/her authority—the "authorization" requirement; (2) it must indicate that the signatory has approved the document's contents—the "approval" requirement; and (3) there must be an absence of fraud in that the signature must indeed be that of the signatory and has been applied with her/her consent to the document—the "no fraud" requirement. To comply with the authorization requirement, there must be a confirmation that the signature is that of the signatory; to comply with the approval requirement, the signatory must be able to ensure that the document's contents will not be altered subsequent to the signing; and, to comply with the no fraud requirement, the signature must be sophisticated enough to reasonably ensure that it has not been forged.

A digital signature complies with all three of these requirements. If the hash value computed by the document's recipient is identical to that of the hash value contained in the digital signature, then it can be concluded that: (1) the document has not been altered; (2) the document was created or authorized by the owner of the private key, whose identity is confirmed by the certification authority; and (3) there is virtually no chance of fraud having occurred because it is impossible to mathematically compute the private key using the public key. Hence, all three requirements are fulfilled by the digital signature.

(2002). But see Clement Shum & Sai-hong Ko, The Legal Significance of PINs in Banking, 30 HONG KONG L.J. 194 (2000) (arguing (1) the common law should regard a PIN as a form of electronic signature; (2) the PIN holder owes a duty of care to his bank when using the PIN; (3) a bank should not hold the PIN holder liable for consequential losses emanating from a criminal's use of unconscionable or deceptive means to obtain the PIN; and (4) a bank has a duty to warn its customers of criminal acts which may be used against PIN holders).


107 Pun et al., supra note 105, at 248.

108 Pun et al., supra note 105, at 251.

109 Pun et al., supra note 105, at 251–52.
Does the PIN satisfy the three requirements? No, it satisfies only the authorization requirement—it does not satisfy the approval requirement and the no fraud requirement. A person with illegitimate knowledge of a PIN may use it to fabricate an electronic document and create a session record contending that the document was created by the rightful PIN owner. Furthermore, the culprit who has gained access to a PIN may attach it to a fabricated electronic document at any time, and the fabrication cannot be distinguished from an original document.

In their article, the HKU professors cast a spotlight on PIN technology and drove home the point that, in comparison to digital signature technology, it is relatively primitive and offers significantly less security. Their criticism, coupled with that of others, resulted in the rejection of the ITBB's proposal to grant the PIN full-fledged legal status as an acceptable form of electronic signature.

2. Proposal to Postpone Utilization Of Biometrics: Rejected

The ITBB, although acknowledging that biometrics is technologically sound, decided to call for a postponement of its utilization. They contended there was "currently no institutional arrangement in place which can support their application on a community-wide basis." Furthermore, they stated that they did not foresee the emergence in the near future of an "independent and trusted third party" who could collect biometric data from subscribers on a community-wide basis, or that biometrics would gain wide acceptance in the community. How wrong they were! The best item of evidence indicating wide acceptance of biometrics in Hong Kong is the Hong Kong Identity Card, accepted by the

---

110 Pun et al., supra note 105, at 254.
111 Pun et al., supra note 105, at 254.
112 Pun et al., supra note 105, at 254.
113 Pun et al., supra note 105, at 254.
114 Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, supra note 96, at 3.
115 Id. at 4.
government as well as the general public, and employing two thumb prints as its biometric identifier.\textsuperscript{116}

To its credit, the Hong Kong General Chamber of Commerce took a view contrary to that of the ITBB and had called for “some means of enabling them [biometric identifiers] early within the current legislative framework [to] be examined.”\textsuperscript{117} Their position was that technological development should be market-driven,\textsuperscript{118} not government-driven; the role of government should be “to provide a framework to enable the market to freely develop these, rather than making a judgment as to which types of technology should mature and when.”\textsuperscript{119} It remains to be seen whether biometrics will be employed in private business to the extent that the Hong Kong government has employed it, but the almost-universal tide of acceptance created by the successful I.D. card seems to be overwhelming.\textsuperscript{120}

3. \textit{Proposal to Allow for Electronic “Delivery by Post or in Person:” Accepted.}

Noting that a number of Hong Kong laws allowed for legal notice to be given through “Delivery by Post or in Person,” the ITBB proposed that electronic delivery should be deemed as


\textsuperscript{117} Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, \textit{supra} note 96, at 2.

\textsuperscript{118} On the other hand, a number of good counter-arguments can be made against allowing the marketplace to be the “primary legislator of electronic signatures.” See Jennifer L. Koger, \textit{Note, You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures}, 11 TRANSNAT’L L. & CONTEMP. PROBS. 491 (2001).

\textsuperscript{119} \textit{Id.} at 3.

complying with this requirement. In order to avoid each and every law having to be amended to allow for electronic notice, an amendment to the ETO was proposed allowing that “delivery by post or in person” would be automatically interpreted to so allow. The Chamber of Commerce had no objection, stating “obviously we support extending [the ETO’s] meaning to cover delivery by electronic means.” This amendment was adopted, but a proviso was added to the effect that the recipient must agree to the delivery in electronic form.

4. Proposal to Continue Most Exemptions Under the ETO: Accepted

The ITBB categorized the exemptions under the ETO into five groups: (1) where the matter or document involved is solemn (e.g., electoral process); (2) where there is an operational need (e.g., requirement to produce a document to a Government authority immediately, “on-the-spot”); (3) voluminous and complex submission (e.g., works departments); (4) need for adherence to international practices (e.g., documents to be retained by an international flight crew); and (5) need to ensure that the Government can meet its contractual obligations (e.g., submission requirements pertaining to trade-related documents concerning the franchise of the Tradelink).

The Chamber of Commerce, given its “minimalist” approach to regulation, naturally supported “a more aggressive approach to encourage wider application of electronic means.” It opined that, over time, the need for the exclusions would be reduced.

---

121 ITBB, supra note 21, at 4.
123 ITBB, supra note 21, at 56.
5. Proposed Changes in Regulation of Certification Authorities: Accepted

The ETO provides for a voluntary recognition program for CAs.\textsuperscript{125} CAs are not obliged to apply for recognition. Those who do must present, on an annual basis, evidence to the Director of Information Technology that they provide a trustworthy service.\textsuperscript{126} The ETO requires CAs to hire an independent assessor (e.g., a Certified Public Accountant) to prepare and submit an assessment report to the Director.\textsuperscript{127} In the \textit{Consultation Paper on the Review of the Electronic Transactions Ordinance}, the ITBB recommended that the assessment report be divided into two parts: one part dealing with issues pertaining to the trustworthiness factors, and the other part pertaining to the non-trustworthiness factors.\textsuperscript{128} Furthermore, the ITBB proposed that the independent assessor only be required to address the trustworthiness issues, with the non-trustworthiness issues covered by a declaration made by an authorized agent of the CA.\textsuperscript{129}

Additionally, the ITBB noted that sometimes, extraordinary situations will require a CA to submit a report to the Director in the middle of a reporting period, before the end of the year.\textsuperscript{130} Examples of such situations might be: (1) significant changes in the financial status of the CA; (2) changes in the liability insurance coverage of the CA; or (3) changes pertaining to “the system, procedure, security arrangements and standards used by the CA to issue certificates to its subscribers.”\textsuperscript{131} In such situations, the proposal would give the Director the authority to mandate the CA to prepare a report in mid-year covering only these extraordinary factors.\textsuperscript{132}

\begin{flushright}
\begin{tabular}{ll}
\textsuperscript{125} & ITBB, \textit{supra} note 21, at 6. \\
\textsuperscript{126} & ITBB, \textit{supra} note 21, at 6–7. \\
\textsuperscript{127} & ITBB, \textit{supra} note 21, at 7. \\
\textsuperscript{128} & ITBB, \textit{supra} note 21, at 8. \\
\textsuperscript{129} & ITBB, \textit{supra} note 21, at 8. \\
\textsuperscript{130} & ITBB, \textit{supra} note 21, at 8. \\
\textsuperscript{131} & ITBB, \textit{supra} note 21, at 8. \\
\textsuperscript{132} & ITBB, \textit{supra} note 21, at 9. \\
\end{tabular}
\end{flushright}
The Chamber of Commerce agreed with these two proposals. However, on the issue of regulation of CAs generally, the Chamber of Commerce claimed that the Director of Information Technology Services had a conflict of interest with the Postmaster General, since the Postmaster is a designated CA under the ETO, and the Director and the Postmaster are "two departments under the same policy bureau." Accordingly, the Chamber of Commerce called for the Director to confer with an independent advisory committee, consisting of representatives from other affected parties, in the discharge of its regulatory duties over the Postmaster General.

V. AMENDMENTS TO THE ETO: 2004

Following the dissemination of the ITBB's Consultation Paper on the Review of the Electronic Transactions Ordinance in 2002, and the subsequent responses to it by the Chamber of Commerce and other interested parties, a bill was prepared for consideration by the Hong Kong Legislature. As a result, the Electronic Transactions (Amendment) Ordinance (the "Amendment Ordinance") was enacted and went into effect on 30 June 2004.

133 Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, supra note 96, at 4.
135 Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, supra note 96, at 4.
136 ITBB, supra note 21.
137 Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, supra note 96.
140 Id. at A481.
A. Private Contracts: Electronic Form Allowed, With Technological-Neutrality

One of the amendments grants private parties the right to select the form of electronic signature they desire. No particular form of electronic signature is required in the case of private contracts, subject to certain exceptions pertaining to reliability, appropriateness in specific circumstances, and of course the preferences of the parties. This is commensurate with the worldwide trend toward technological-neutrality and less regulation of electronic signatures.

In private contracts, it is recognized that the private parties themselves should decide the issue of which form of electronic signature to use. One factor in this decision is the economics, i.e., the parties must decide whether to use a more sophisticated, yet more expensive form (i.e., the digital signature) or to use a less sophisticated, yet cheaper form. In the private sector, it is considered unwise to tie the parties to a specific form of electronic signature. Instead, let market forces decide. Furthermore, technological innovation continues at a rapid pace, so better forms of technology may exist tomorrow which are only on the “drawing board” today.

However, the digital signature requirement continues in force for electronic communiqués with the government. This is considered “necessary and defensible” because the focus on one form of electronic signature provides clarity and certainty to citizens, making filing requirements easier to comprehend. This will also be “cost-effective” to the Hong Kong government.

---

141 Amendment Ordinance, supra note 139, § 5 (amending ETO § 6).
142 Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, supra note 96, at 3.
143 Consultation Paper on the Review of the Electronic Transactions Ordinance: Comments by the Hong Kong General Chamber of Commerce, supra note 96, at 3.
144 Amendment Ordinance, supra note 139, § 5 (amending ETO § 6).
145 Legislative Council Brief, supra note 138, at 3.
146 Legislative Council Brief, supra note 138, at 3.
because only one form of electronic signature will have to be dealt with.

B. Electronic Delivery Allowed in Cases of Serving Documents “by Post or in Person”

Many statutes in Hong Kong allow for service of documents “by Post or in Person.” These statutes were enacted before the invention of the computer and before it was possible to send electronic messages. The government and the citizens would be well-served for these laws to allow for the legal recognition of electronic service. For both the government and the relevant parties, electronic service carries the important advantages of being cheaper and more convenient.147

Accordingly, the ETO was amended. It now states that electronic service “to an information system designated by the person” satisfies the requirement for “a document to be served on a person by personal service or by post.”148

This amendment does not apply if an ordinance requires the personal service upon one private party by another private party, where neither is affiliated with the government. In that situation, another amendment is applicable: electronic service will be allowed to fulfill the service requirement only if the recipient gives consent to the utilization of the electronic form.149

C. Voluntary Recognition Program for Certification Authorities: Two Changes

As mentioned, the original ETO provided for “recognition” of CAs.150 It established a program of recognition for CAs that show themselves to be especially trustworthy entities. A CA applying for “recognized” status must submit a report prepared by an approved independent assessor attesting to the applicant’s

147 ITBB, supra note 2.
148 Amendment Ordinance, supra note 139, § 4 (supplementing § 5A of the ETO).
149 Amendment Ordinance, supra note 139, § 10 (amending ETO, § 15).
150 ETO, supra note 20, §§ 20, 21.
adherence to requirements of the ETO and the Code of Practice.\textsuperscript{151} After attainment of recognition, the RCA must continue to submit an assessment report every twelve months and each time it applies for renewal of recognition.\textsuperscript{152}

1. **Bifurcation of the Assessment Report**

The ETO was amended to allow the RCA to submit a sworn statement in regard to its operational aspects (e.g., adherence to non-discrimination against handicapped persons).\textsuperscript{153} The independent assessor is no longer required to address the operational issues; the independent assessor will only address the issues pertaining to trustworthiness of the RCA.\textsuperscript{154}

2. **Major Changes in Mid-Year**

The original ETO did not consider the impact of major changes upon the RCA occurring in mid-year, between the times that the assessment reports are submitted. In 2004, this omission was addressed; the ETO was amended requiring the RCA to inform the Director at once of the occurrence of major changes in its organization which could have a bearing upon its suitability for recognition.\textsuperscript{155}

VI. **THE CODE OF PRACTICE FOR RECOGNIZED CERTIFICATION AUTHORITIES**

Section 33 of the ETO provides that “[t]he Director may issue a code of practice specifying standards and procedures for carrying out the functions of recognized certification authorities.”\textsuperscript{156}

\textsuperscript{151} ETO, supra note 20, § 43.  
\textsuperscript{152} ETO, supra note 20, § 43.  
\textsuperscript{153} Amendment Ordinance, supra note 139, §§ 12, 16, 21 (amending ETO §§ 20, 27, 43).  
\textsuperscript{154} Amendment Ordinance, supra note 139, §§ 12, 16, 21 (amending ETO §§ 20, 27, 43).  
\textsuperscript{155} Amendment Ordinance, supra note 139, § 22 (supplementing § 43A of the ETO).  
\textsuperscript{156} This fact is re-affirmed at COP § 1.1, see infra note 157.
Pursuant to that authority, the Director issued the Code of Practice ("COP") in July 2004. A slightly amended version was issued in December 2004. This document grants insight into the plethora of detailed daily duties that must be carried out by the RCA.

The Government Chief Information Officer ("GCIO") has directed the Certification Authority Recognition Office ("CARO") to "process applications for and renewal of CA recognition," and to monitor whether existing RCAs are in compliance with the ETO and the Code of Practice.

CARO shall consider an applicant-CA's ability to abide by the COP in making its decision as to whether the CA qualifies for recognition. Specific criteria to be considered in the evaluation of a CA's application for recognition include: financial status; arrangements to cover potential liabilities; the proposed system for issuance of certificates; the assessment report made by an external auditor and the applicant's statutory declaration; and whether the applicant and its officers are fit and proper persons. CARO may also take into account a failure to comply with the Code of Practice.

---


158 Code of Practice for Recognized Certification Authorities Published by the Government Chief Information Officer under Section 33 of the Electronic Transactions Ordinance ("COP Amended") (Dec. 2004) (Cap. 553), (H.K.). The amendments consisted only of the following: a revision of § 1.9 in order to update the version numbers; and a revision of § 12.4(a) pertaining to the Professional Accountants (Amendment) Ordinance 2004. Id. See also Office of the GCIO, Information Note on the Advisory Committee on Code of Practice for Recognized Certification Authorities, (July 2004) (reserving the right of the GCIO to amend the Code of Practice). It also established a committee (consisting of representatives of RCA's, business organizations, related professional organizations, academics, and others) to provide advice as to needed amendments to the Code of Practice. Id.

159 Undoubtedly, it will prove to be invaluable to future researchers conducting empirical research pertaining to the activities of the RCA.


161 COP, supra note 157, § 1.3.

162 ETO, supra note 20, § 21(4); Office of the GCIO, Guidance Note on Recognition of Certification Authorities and Certificates Under the Electronic Transactions Ordinance (Cap. 553), (July 2004) at 1.
in a decision whether to suspend, revoke, or not renew a recognition previously granted to a CA. Other potentially disqualifying factors include the CA’s failure to abide by: (a) the ETO; or (b) its own Certification Practice Statement (“CPS”).

A CA that has been refused recognition (either when applying the first time, or when applying for renewal of recognition), or whose recognition has been suspended or revoked, may appeal the Director’s decision to the Secretary of the GCIO.

If the COP conflicts with the ETO, the ETO will prevail. If the English version conflicts with the Chinese version, the English version will prevail.

A. Important Definitions

A certificate is required to contain the following: (1) confirmation of the identity of the person holding a private key; (2) the identity of the CA; (3) identification of the person to whom the private key is issued; (4) the public key of the person to whom the private key is issued; and (5) the CA’s signature.

A common theme running through the COP pertains to trustworthiness of the parties involved with digital signatures, especially that of the CA. The COP requires the persons intimately involved in the digital signature process to be “fit and proper persons.” In determination of whether a person is “fit and proper,” the GCIO must consider the following factors (others may also be considered): (1) the fact that a person has been convicted in the Hong Kong Special Administration Region of a crime consisting of fraud, corruption, or dishonesty; (2) the fact that an individual person has been convicted of a violation of the ETO; (3)

---

163 COP, supra note 157, § 1.5
164 ETO, supra note 20, § 25.
165 ETO, supra note 20, § 28; Office of GCIO, supra note 162.
167 See id. § 1.8.
168 See id. § 2.1.
169 See id. § 5.18.
the fact that the person is an undischarged bankrupt or has entered into a voluntary or involuntary "scheme of arrangement" pursuant to the Bankruptcy Ordinance within the past five years; and (4) the fact that a corporation is in liquidation, the subject of a winding-up order or has a receiver in charge of its finances pursuant to the Bankruptcy Ordinance within the past five years.\(^{170}\)

A "recognized" certificate is one that is: (1) recognized pursuant to ETO, Section 22; (2) a certificate of a type, class, or description of one recognized pursuant to ETO, Section 22, or (3) designated as "recognized" by the Postmaster General.\(^{171}\)

Because CAs must maintain a repository of the certificates they have issued, a definition was necessary. A repository is "an information system for storing and retrieving certificates and other information relevant to certificates."\(^{172}\)

The COP defines a "subscriber" as one who is named in the certificate as the one to whom the certificate is issued.\(^{173}\) To qualify as a subscriber, the person must have accepted the certificate and must be holding a private key corresponding to a public key listed in the certificate.\(^{174}\) The COP provides that a subscriber may also be a CA, i.e., it is acceptable for one CA to issue a certificate to another CA.\(^{175}\)

The concept of "trustworthiness" not only applies to persons involved with digital signatures—it also applies to the equipment that is involved.\(^{176}\) A "trustworthy system" consists of hardware, software and procedures which are reasonably: (1) secure; (2) available and reliable, and ensure a proper mode of operations for a reasonable period of time; (3) suitable for performing their intended function; and (4) in compliance with generally accepted security principles.\(^{177}\)

\(^{170}\) See id. § 2.1.
\(^{171}\) Id.
\(^{172}\) Id.
\(^{173}\) Id.
\(^{174}\) Id.
\(^{175}\) Id.
\(^{176}\) Id.
\(^{177}\) Id.
In order to "verify" a digital signature, one must ensure that: (1) the digital signature was created using the private key corresponding to the public key listed in a certificate; and (2) the digital record was not modified since the creation of the digital signature.  

B. General Responsibilities of a Recognized Certification Authority

The RCA must comply with all conditions which are established by the GCIO at the time of granting or renewal of the recognition.  

Any agents or subcontractors employed by the RCA must be equally capable of performing the duties, and the RCA is responsible for the acts or omissions of the agents or subcontractors.  

An RCA has a duty to exercise reasonable care in its acts which affect the subscribers and others relying upon the certificates.  

The RCA must provide to the GCIO a copy of its certification authority certificate that it uses to sign recognized certificates. This will be published by the GCIO for use by interested parties in verification of the validity of the recognized certificates.  

Information having a retention requirement must be archived for not less than seven years.  

The ETO is concerned with secrecy, i.e., maintaining privacy of personal data. Toward that end, the COP requires the RCA to: (1) publish to applicants and subscribers its privacy policy pertaining to its handling of private, personal information; (2) give a copy of its written Personal Information Collection Statement to

---

178 Id.
179 See id. § 3.1.
180 See id. § 3.2.
181 See id. § 3.3.
182 See id. § 3.4.
183 Id.
184 See id. § 3.5.
185 ETO, supra note 20, § 46.
subjects before collecting private data from them; (3) include a purpose statement in its repository or CPS defining the objective in maintaining the repository and the permitted use of personal data contained there; and (4) on a "regular" basis, or whenever major changes have occurred, conduct a self-assessment pursuant to the "Privacy Compliance Self-Assessment Kit" published by the Office of the Privacy Commissioner for Personal Data.  

RCAs are not allowed to engage in monopolistic activity; antitrust behavior is undesirable because it results in restraint of trade. Competition is desirable in the certification authority industry in order to keep the cost of the service as low as possible and to give the consumer a choice.

It is acceptable for an RCA to issue either a recognized certificate, or a non-recognized one. If both types are issued, the RCA should express that fact in its repository and CPS. In this communiqué, the RCA should pinpoint the particular certificates, or types/classes of certificates, that are recognized and which are not.

C. Trustworthiness of the System

The RCA is mandated to use trustworthy hardware, software and control procedures. There are no absolute measures of trustworthiness; it is a relative term. The RCA must undertake a risk analysis and adopt measures which will enable it to control the risk it is facing. After the enactment of the ETO amendments in 2004, Hong Kong has assumed a "technology-neutral" and supposedly "minimalist" regulatory approach. Accordingly, the

---

186 COP, supra note 157, at § 3.6.
187 See id. § 3.7.
188 See id. § 3.8.
189 Id.
190 Id.
191 See id. §§ 5.1, 5.2.
192 See id. § 5.4.
193 See id. § 5.6.
194 Electronic Transactions (Amendment) Ordinance, supra note 139.
195 COP, supra note 157, § 5.5. However, after being confronted with the stringency and the meticulousness of the regulations in the Code of Practice,
RCA has some latitude in determining the technical solutions it may employ. It is recognized that every private RCA is in a unique situation and that methods used in attainment of a trustworthy system may vary. Nevertheless, all RCAs should strive to adhere to a group of fundamental maxims which serve as a foundation for all—the Generally Accepted Industry Good Practices.

If the RCA finds its system is no longer trustworthy, this should be reported to the GCIO at once.

All responsible officers in trusted roles (i.e., security officers, CA administrators, privileged system operators, registration personnel, or anyone with access to key material cryptographic modules, or activity event logs) are mandated to be “fit and proper persons.”

D. Generally Accepted Industry Good Practices

The RCA should generally follow the “Generally Accepted Industry Good Practices” with respect to:

1. Security Management Factors. Asset classification and management (information should be treated as an asset, with appropriate attention to data privacy), personnel security, physical and environmental security, control of system access, security incident reporting procedure, planning for extraordinary incidents (e.g., key compromise, security breach of the system or network, unavailability of the RCA’s infrastructure, unauthorized

RCAs must wonder what it would be like to be doing business in a “maximalist” jurisdiction!

196 COP, supra note 186, at § 5.5.
197 See id. § 5.9 et seq.
198 See id. § 5.16.
199 See id. § 5.18.
200 See id. § 5.9.1(a).
201 See id. § 5.9.1(b).
202 See id. § 5.9.1(c).
203 See id. § 5.9.1(d).
204 See id. § 5.20.
generation of certificates/certificate suspension and revocation information);\textsuperscript{205}

2. \textit{Operational Management Factors}. Development of effective policies and procedures over everyday operations, delineation of duties of personnel, monitoring system performance to control bottlenecks, protection of computer infrastructure (e.g., against viruses), provision of backup and archiving, and resolution of problems;\textsuperscript{206}

3. \textit{Computer Systems Management Factors}. Establishment of standards for development work, segregation of production and development environments, segregation of duties of operative and development personnel, handling emergency changes to systems, and overseeing acquisition of new equipment;\textsuperscript{207}

4. \textit{Business Operations Continuity Factors}. Making and testing contingency plans in order to cope with anticipated new situations, and recovering from a compromise or suspected compromise of the RCA’s private key;\textsuperscript{208}

5. \textit{Factors in Maintenance of Journals}. Keeping journal records of issuance and management of certificates,\textsuperscript{209} regularly reviewing journals and noting missing entries and following-up,\textsuperscript{210} keeping logs pertaining to keys and security incidents,\textsuperscript{211} and

6. \textit{Compliance Monitoring Factors}. Establishing controls to ensure compliance with all legal, technical and regulatory requirements.\textsuperscript{212}

E. \textit{Good Practices Specific to Functions of an RCA}

The RCA should be cognizant of, and adhere to, the “Good Practices Specific to Functions of a Recognized CA.”\textsuperscript{213} These are concerned with:

\textsuperscript{205} See id. § 5.21.
\textsuperscript{206} See id. § 5.9.2.
\textsuperscript{207} See id. § 5.9.3.
\textsuperscript{208} See id. §§ 5.9.4, 5.9.5, 5.9.6.
\textsuperscript{209} See id. § 5.9.7.
\textsuperscript{210} See id. § 5.9.8.
\textsuperscript{211} See id. § 5.9.9.
\textsuperscript{212} See id. § 5.9.10. 
1. **Management of the CPS.** A committee should be established within the CA organization to prepare the Certification Practice Statement ("CPS").

2. **Monitoring of the RCA’s Functions.** The functions are affected by laws and regulations to ensure that all legal and regulatory requirements are understood and are being complied with.

3. **Key Management.** To ensure control of cryptographic equipment used to generate keys (its procurement, receipt, installation, acceptance tests, commissioning, usage, repair and maintenance, retirement, and destruction), the personnel involved, the keys’ custody (e.g., using “dual access” control) and backup.

4. **Key Management Services Provided by the RCA (if applicable).** If the RCA assists the subscriber in controlling its keys, these services must be monitored and controlled.

5. **Lifecycle Management of Tokens (if applicable).** For example, if smart cards are used by the RCA, control must be established over their “preparation, activation, usage, distribution, and termination.”

6. **Certificate Management.** Verification of the applicant’s identity, notifying the subscriber in a timely manner before the expiration date of the certificate that it is time to renew, adoption of a common format of certificates, ensuring that the CA’s repository meets the standards expressed in the CA’s CPS, and establishment of a complaint-handling procedure; and

7. **Management of the Publication of Certificate Revocation Information.** Ensuring that the relevant CPS policies and procedures regarding revocation are followed, and ensuring that

---

213 See id. § 5.10.
214 See id. § 5.10.1.
215 See id. § 5.10.2.
216 See id. §§ 5.10.3, 5.10.4.
217 See id. § 5.10.5.
218 See id. § 5.10.6.
219 See id. § 5.10.7.
only authorized persons have access to the certificate revocation list.\textsuperscript{220}

F. Key Management: Trustworthy Generation and Good Record-Keeping

Key generation is the "heart and soul" of the RCA’s job. If the applicant generates his/her own keys, the RCA should emphasize to the applicant the importance of using a trustworthy system to do so.\textsuperscript{221} The RCA should provide trustworthiness guidelines to the applicant and take "reasonably practicable steps" to determine whether the applicant has in fact used a trustworthy system to generate the keys.\textsuperscript{222} If the RCA determines that the applicant has not used a trustworthy system or has not obeyed the prescribed guidelines, the RCA should not accept the applicant’s keys.\textsuperscript{223}

The RCA must maintain good security over its own private key.\textsuperscript{224}

Good record-keeping is essential to effective management of keys. Records must be kept of the following activities: (1) issuance, renewal, suspension and revocation of certificates; (2) the publication of information pertaining to revoked certificates (e.g., the certificate revocation list); (3) the creation of the RCA’s own key pair; (4) the creation of the subscribers’ key pairs; (5) its computer facilities;\textsuperscript{225} and (6) all issued certificates should be archived and access to them should be permitted by relying parties.\textsuperscript{226}

G. Digital Signatures

Digital signatures should only be created by the party to whom they relate.\textsuperscript{227}

\textsuperscript{220} See id. § 5.10.8.
\textsuperscript{221} See id. § 5.11.
\textsuperscript{222} Id.
\textsuperscript{223} Id.
\textsuperscript{224} See id. § 5.12.
\textsuperscript{225} See id. § 5.13.
\textsuperscript{226} See id. § 5.14.
\textsuperscript{227} See id. § 5.15(a).
It should be impossible for a digital signature to be reproduced without the assistance or the knowledge of the person to whom the digital signature relates.\textsuperscript{228}

\textbf{H. Issuance of Recognized Certificates}

An RCA may issue both recognized and non-recognized certificates.\textsuperscript{229} If it issues both, separate private keys should be used for the two categories.\textsuperscript{230}

The recognized certificate should indicate to the subscriber, or the relying third party, how to access the RCA's CPS.\textsuperscript{231}

The recognized certificate should only be issued: (1) to applicants for such a certificate; and (2) after compliance with the identity verification procedures listed in the RCA's CPS.\textsuperscript{232} The identity verification procedure must be specified in the recognized certificate, and the verification evidence must be retained by the RCA.\textsuperscript{233}

The RCA will publish certificates that have been issued and accepted in its online repository.\textsuperscript{234} Subscribers must give personal consent to the publication of their personal information.\textsuperscript{235} If both recognized and non-recognized certificates have been issued by the RCA, separate repositories shall be used.\textsuperscript{236} The repository must contain:

1. recognized certificates issued by that RCA (containing the public key corresponding to the private key used by the RCA to digitally sign recognized certificates it issues);\textsuperscript{237}
2. suspension or revocation notices (to include the certificate revocation list);\textsuperscript{238}
3. the disclosure record for that RCA;\textsuperscript{239}
4. other facts which materially and adversely affect

\textsuperscript{228} See id. § 5.15(b).
\textsuperscript{229} See id. § 6.1.
\textsuperscript{230} Id.
\textsuperscript{231} See id. § 6.2.
\textsuperscript{232} See id. § 6.3.
\textsuperscript{233} See id. §§ 7.1, 7.2.
\textsuperscript{234} See id. § 6.5.
\textsuperscript{235} See id. § 6.6.
\textsuperscript{236} See id. § 6.5.
\textsuperscript{237} See id. § 10.1(a).
\textsuperscript{238} See id. §§ 9.3, 10.1(b).
\textsuperscript{239} See id. § 9.3.
the reliability of the certificate, or which materially and adversely affect
the ability of the RCA to perform its services;\textsuperscript{240} and (5) other
information as specified by the GCIO.\textsuperscript{241}

Recognized certificates may be renewed upon expiration of
their validity at the request of the subscriber and at the discretion
of the RCA.\textsuperscript{242}

If the recognized certificate has a reliance limit, it must be
specified in the CPS and the significance of said limit must be
explained in the CPS.\textsuperscript{243}

The RCA must obtain insurance in order to provide coverage
for any potential liabilities arising from issuance of recognized
certificates, and the RCA must provide evidence of such
insurance.\textsuperscript{244} The RCA's amount of insurance coverage must be
not less than: (1) ten times the reliance limit specified by the RCA
in its CPS; or (2) $200,000, whichever is greater.\textsuperscript{245} Additionally,
the minimum total insurance coverage for aggregated claims are
required to be ten times the amount of (1) or (2), whichever is
greater.\textsuperscript{246} The insurance coverage must be administered by an
independent third party.\textsuperscript{247} Furthermore, the insurer must be: (1)
authorized to engage in the insurance business pursuant to the
Insurance Companies Ordinance (Cap. 41), including Lloyd’s,\textsuperscript{248}
and (2) governed by the laws of the Hong Kong SAR.\textsuperscript{249}

The holder of a recognized certificate must be kept informed
by the RCA of any emerging fact which affects the validity of the
certificate.\textsuperscript{250}

The recognized certificate must state its expiration date.\textsuperscript{251}

\textsuperscript{240} See id. § 10.1(c).
\textsuperscript{241} See id. § 9.3.
\textsuperscript{242} See id. § 6.22.
\textsuperscript{243} See id. § 8.1
\textsuperscript{244} See id. § 8.2
\textsuperscript{245} Id.
\textsuperscript{246} Id.
\textsuperscript{247} Id.
\textsuperscript{248} See id. § 8.3(a).
\textsuperscript{249} See id. § 8.3(b).
\textsuperscript{250} See id. § 6.7.
\textsuperscript{251} See id. § 6.8.
The CPS of the RCA is only applicable to recognized certificates; it is not applicable to non-recognized certificates.252

I. Suspension and Revocation of Recognized Certificates

Suspension or revocation must be implemented if the RCA obtains such a request from either: (1) the subscriber named on the face of the certificate; or (2) a "properly authorized person."253

If a certificate is suspended or revoked, notice must be placed in the repository that is identified on the face of the certificate.254 This must be accomplished "within a reasonable time."255

The RCA and the subscriber must reach an agreement as to the exact time of the suspension or revocation, and the allocation of liability for transactions relying upon the certificate between the receipt of the request for revocation or suspension and the exact time of the revocation or suspension.256

The RCA may temporarily suspend a recognized certificate if it has reasonable grounds to believe that it is unreliable; in this situation, the consent of the subscriber is unnecessary.257 Within a reasonable time, the RCA must complete its investigation and with either reinstate, or revoke, the certificate.258

If the RCA decides that an immediate revocation is required, the RCA may do so, and the consent of the subscriber is unnecessary.259

The RCA shall provide an emergency method of communication (i.e., a "hotline") for the subscriber to inform the RCA that the private key has been lost or that its security has been compromised.260

252 See id. § 6.9.
253 See id. § 6.13.
255 See id. § 6.14.
256 See id. § 6.15.
257 See id. § 6.16.
258 Id.
259 See id. § 6.17.
260 See id. § 6.20.
The RCA is required to maintain in its repository an archive of suspended and revoked certificates. It must be maintained for a minimum period of seven years.

J. Disclosure of Information

Every six months, the RCA must report to the GCIA the following information: (1) the number of subscribers in the various categories of certificates; (2) the number of certificates that have been issued, revoked, expired, and renewed by various categories; (3) a comparison of its actual performance level with its stated service levels; (4) new categories of certificates that have recently been issued; (5) changes in its organization structure or systems; and (6) actions taken to address deficiencies previously noted in its most-recently submitted Assessment Report submitted to the GCIO pursuant to ETO sections 20(3)(b), 27(5A)(b) or 43(1)(a) or 43A(1)(c).

Any material changes in the above information must be immediately reported. The GCIO must be advised of personnel changes pertaining to “responsible officers” within three days. Conflicts of interest, or potential conflicts of interest, must be reported immediately. Any “incident that materially and adversely affects” the RCA’s operations must be reported immediately.

Whenever the RCA submits a report or information to the GCIO, it must possess the necessary legal rights over that report or information, and must simultaneously grant a license to the RCA to publish said report or information. The RCA must agree to the publication of any or all of the report or information, and it

---

261 See id. § 9.3.
262 See id. § 9.5.
263 See id. § 10.3.
264 See id. § 10.4.
265 See id. § 10.2.
266 See id. § 10.5.
267 See id. § 10.6.
268 See id. § 10.7.
269 See id. § 10.8.
must not attempt to prevent the publication of the report or information.270

K. Termination of the RCA’s Service

Whenever the RCA applies for recognition or renewal of its recognition, it should also submit a termination plan.271 The termination plan shall contain arrangements for maintenance of the RCA’s records for a period of not less than seven years after the date of termination of its services.272 The termination plan must cover both voluntary and non-voluntary situations, and must provide for the safeguarding of the subscribers’ interests upon the RCA’s termination.273 The CPS must include the termination plan.274

In order for the RCA’s termination to be recognized under the ETO, the RCA must: (1) give a minimum of ninety days’ notice to the GCIO of its intention to terminate its services; (2) inform all subscribers a minimum of sixty days before the termination date; (3) advertise in both Chinese-language and English-language daily Hong Kong newspapers for three consecutive days at least sixty days before the termination; (4) revoke all certificates upon termination of service; and (5) make an orderly transfer of information contained in the RCA’s repository to a custodian who will maintain the information for a minimum of seven years from the date of termination or from the date of transfer of the information, whichever is later. The public should be informed of how to access the information maintained by the custodian.275

270 See id. § 10.9.
271 See id. § 11.1.
272 See id. § 11.2.
273 See id. § 11.3.
274 See id. § 11.4.
275 See id. § 11.5.
L. Annual Report of Compliance Assessment\textsuperscript{276}

1. Independent Assessor’s Compliance Review

Every twelve months after the RCA has attained its status,\textsuperscript{277} or whenever the RCA applies for renewal of its status,\textsuperscript{278} or whenever the RCA has undergone “major changes,”\textsuperscript{279} an independent assessor\textsuperscript{280} must be hired by the RCA to submit a report to the GCIO as to whether the RCA is in compliance with the ETO and with the Code of Practice.\textsuperscript{281} The report must be submitted within four weeks of the completion of the assessment.\textsuperscript{282}

2. RCA’s Statutory Declaration of Compliance

Every twelve months after the RCA has attained its status,\textsuperscript{283} or whenever the RCA applies for renewal of its status,\textsuperscript{284} or whenever the RCA has undergone “major changes,”\textsuperscript{285} the RCA shall submit a statutory declaration to the GCIO as to whether the RCA is in compliance with the ETO and with the Code of Practice.\textsuperscript{286} The statutory declaration must be submitted to the GCIO within four weeks after it was prepared.\textsuperscript{287}

\textsuperscript{276} See generally Office of GCIO, supra note 162.
\textsuperscript{277} COP, supra note 157 at § 12.1(a).
\textsuperscript{278} See id. § 12.1(b).
\textsuperscript{279} See id. § 12.1(c).
\textsuperscript{280} The independent assessor’s required qualifications are explained in COP, supra note 157, §§ 12.212.5.
\textsuperscript{281} COP, supra note 157 at § 12.1. Specific parts of the ETO and the COP to be addressed in the review are given in the COP, Appendix 2, § 1; they are generally concerned with the trustworthiness of the RCA and its system.
\textsuperscript{282} COP, supra note 157 at § 12.6.
\textsuperscript{283} See id. § 13.1(a).
\textsuperscript{284} See id.§ 13.1(b).
\textsuperscript{285} See id. § 13.1(c).
\textsuperscript{286} See id. § 13.1. Specific parts of the ETO and the Code of Practice to be addressed in the declaration are given in the COP, Appendix 2, § 2. They are generally concerned with the operational aspects of the RCA, e.g., compliance with anti-discrimination law. Trustworthiness issues are addressed in the independent assessor’s review, as noted above.
\textsuperscript{287} COP, supra note 157 at § 12.1(a).§ 13.3.
M. Continual Upgrading of Technology, Inter-Operability, and Consumer Protection

RCAs are mandated to continuously upgrade their technology in order to provide good service to subscribers and relying third parties.\footnote{288} Specific policies, procedures and controls regarding upgrading must be established.\footnote{289} They must be assigned to organizational units, and from time to time they must be re-assessed.\footnote{290}

RCAs shall do whatever possible to develop systems which are interoperable.\footnote{291} In other words, the RCA’s systems should be able to interact with systems of other RCAs, “wherever applicable.”\footnote{292} Such development of an “open and common interface” will enable the RCA’s digital signatures and its certificates to be more easily verified by other RCAs.\footnote{293} The RCA’s CPS must express the common interfaces that it supports and the degree of interoperability it has established with other RCAs.\footnote{294}

The RCA’s advertisements must be “decent, honest and truthful.”\footnote{295} Advertising claims must be “fair and not misleading,” and must be “capable of independent substantiation.”\footnote{296}

N. The Certification Practice Statement ("CPS"): Overview

The main body of the COP provides an overview of the CPS. Coverage of detailed standards and procedures in the construction of the CPS is contained in Appendix 1 of the COP,\footnote{297} and are presented in the next section.

\footnote{288} See \textit{id.} § 14.1.  
\footnote{289} See \textit{id.} § 14.1(a).  
\footnote{290} See \textit{id.} §§ 14.1(a), (b).  
\footnote{291} See \textit{id.} §§ 15.1, 15.2.  
\footnote{292} See \textit{id.} § 15.1.  
\footnote{293} Id.  
\footnote{294} See \textit{id.} § 15.2.  
\footnote{295} See \textit{id.} § 16.1.  
\footnote{296} Id.  
\footnote{297} See \textit{id.} § 4.11.
The CPS is only applicable to recognized CAs; it is not applicable to non-recognized CAs.\footnote{See id. § 1.}

There are two types of CPS: ordinary and extraordinary.

1. **Ordinary CPS**

   The CPS will be drafted by the RCA. It will be continually reviewed and revised as necessary. An up-to-date copy will be kept on file in the Office of the GCIO; it will also be posted in the RCA’s online repository for dissemination to subscribers and relying parties.\footnote{See id. § 4.6.} The primary information contained in the CPS will be: (1) liabilities and limitations of liability (including reliance limit),\footnote{See id. § 4.2.} (2) rights and obligations of the RCA, the subscriber, and third parties relying on the certificate;\footnote{Id.} (3) whether the certificates it has issued are recognized or non-recognized, and the types/classes of each category, and the significance of having a non-recognized certificate;\footnote{See id. §§ 4.3, 4.4.} and (4) notice to the applicants for recognized certificates that personal data will become public information after it has been deposited in the RCA’s repository.\footnote{See id. § 4.5.}

2. **Extraordinary CPS: After Material Changes**

   Pursuant to a 2004 amendment of the ETO,\footnote{ETO, (2000) Cap. 553, § 24(43A). (H.K.), available at http://upan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN010238.pdf.} an interim, supplementary CPS may need to be issued to the GCIO (and to subscribers and relying parties) in the middle of a reporting period if material changes occur.\footnote{COP, supra note 157 at § 4.12.} Examples of material changes include: (1) the RCA’s issuance of new types/classes of recognized certificates; (2) changes in the identification process...
that downgrade the reliability of the recognized certificates; and (3) changes in the key generation, storage or usage procedures.  

3. Standards and Procedures Regarding the Contents of a CPS

The Code of Practice, Appendix 1, specifies the minimum standards and procedures expected of an RCA in preparing its CPS.

A common theme applicable to all aspects of the work of the RCA is that, insofar as possible, "widely accepted technical standards and management practices" should be adopted. These standards and practices are to be specified in the CPS, along with details of each, as well as "interface" applications for use of its certificates and services. For example, the standards adopted for the certificate profile, certificate revocation list, and repository shall be published. Adoption and publication of internationally-accepted standards and practices will facilitate the RCA's interaction with other related persons and organizations in all parts of the world. By its very nature, e-commerce is a global phenomenon and the Hong Kong CPS standards and procedures definitely reflect this viewpoint.

The RCA is mandated to disclose the principal attributes of each type, class, or description of certificate that it issues, e.g.: recognition status, reliance limit, and the form of identification required to be submitted by the subscriber. The RCA should describe what recognition means and its importance to all relevant

---

306 COP, supra note 157 at § 4.12.
308 The idea of a CPS emanates from the American Bar Association ("ABA") Digital Signature Guidelines. See supra note 23. The ABA Guidelines define the CPS as "a statement of the practices which a certification authority employs in issuing the certificates." Id. § 1.8.
309 CPS, supra note 307, app. 1 § 10; see also COP, supra note 157, §§ 15.12.
310 Id.
311 CPS, supra note 307, app. 1 § 10.
312 COP, supra note 157 at § 2.1.
parties, and should provide the website address of its repository. The relevant groups or functions it impacts upon (e.g., registration, repository, and target end-users) should be delineated; any outsourcing of functions should be explained. Limitations or restrictions placed on each class of certificate should also be disclosed. Contact information should be given to all interested parties. A detailed description of the types of information to be included in a CPS follows.

O. Obligations of the Parties

1. The RCA's Obligations

These include, but are not limited to, the provision of notice to the subscriber of issuance, suspension or revocation of a certificate. Additionally, the RCA assumes repository responsibilities, e.g., timely publication of certification information pertaining to issuance, suspension or revocation; and ensuring that all interested parties are capable of accessing the repository.

2. The Subscriber's Obligations

These include, but are not limited to: providing accurate information to the RCA when applying for issuance of a certificate; taking care of the private key and doing everything reasonably possible not to lose it or jeopardize its security; abiding by any restrictions placed by the RCA upon the use of the private key; and promptly informing the RCA whenever the private key has been lost or its security has been compromised.

---

313 Id. § 2.2.1.
314 Id. § 2.2.2.
315 Id. § 2.2.3.
316 Id.
317 Id. § 2.2.4.
318 Id. § 3.3.1.
319 Id. § 3.1.2.
3. *The Relying Party’s Obligations*

The relying party has the duty:

[t]o learn the purpose for which the certificate has been issued; to verify the authenticity of the digital signature; to enquire at the RCA’s online repository periodically as to whether the certificate has been suspended or revoked; and to keep informed as to any limitation of the RCA’s liabilities and warranties.\(^\text{320}\)

4. *Liability*

The effect of a reliance limit should be emphasized.\(^\text{321}\) Warranties, and limits on warranties, for each type, class, or description of certificate should be disclosed.\(^\text{322}\) The types of liability assumed (i.e., for direct, indirect, special, consequential, incidental, and liquidated damages) for each type, class or description of certificate should be given, as well as any limitation on liability (or loss limitations, or other exclusions) for each of them.\(^\text{323}\) Additionally, the RCA should explain the assignment of liability for transactions supported by a certificate which occur in-between these two points-in-time: (1) when the subscriber requests suspension or revocation of the certificate and (2) the time of actual suspension or revocation by the RCA.\(^\text{324}\)

5. *Financial Responsibility*

The RCA should include relevant financial information, such as: the existence of any fiduciary relationships among parties related to the certificate; financial responsibility for administrative expenses incurred; financial assurances provided to the subscriber and relying third parties; and miscellaneous financial information, including but not limited to, performance bonds and insurance policies.\(^\text{325}\)

\(^{320}\) *Id.* § 3.1.3.

\(^{321}\) *Id.* § 3.2.

\(^{322}\) *Id.* § 3.2.1.

\(^{323}\) *Id.* § 3.2.2.

\(^{324}\) *Id.* § 3.2.

\(^{325}\) *Id.* § 3.3.
6. **Interpretation and Enforcement**

   The governing law and the jurisdiction for the enforcement of relevant claims shall be stated.\(^{326}\) If dispute resolution procedures have been agreed to, those should also be stated.\(^{327}\)

7. **Fees**

   Costs and fees should be disclosed as they affect both the subscriber and relying third parties.\(^{328}\) Acts serving as the basis for fee assessment include the certificate's issuance, revocation, suspension, retrieval, or verification of status.\(^{329}\)

8. **Repository**

   The means of publication of information pertaining to the issued certificates must be included.\(^{330}\) Ordinarily, this will be the online website; its address must be disclosed so that all interested parties may access it.\(^{331}\) The contents of the repository should be listed, e.g.: all certificates which have been issued and their current recognition status, and a copy of the CPS with all amendments.\(^{332}\) Additionally, the frequency of publication of the information contained in the repository shall be expressed.\(^{333}\)

9. **Compliance Assessments**

   Full details of compliance assessments are also part of the CPS.\(^{334}\) This includes: their frequency of occurrence; their identity and qualifications of the independent auditor (e.g., a Certified Public Accountant); any connections or relationships between the RCA and the auditor (in other words, is the auditor really independent); the scope of the compliance assessment (i.e., the

\(^{326}\) Id. § 3.4.1.  
\(^{327}\) Id. § 3.4.2.  
\(^{328}\) Id. § 3.5.  
\(^{329}\) Id.  
\(^{330}\) Id. § 3.6.  
\(^{331}\) Id.  
\(^{332}\) Id.  
\(^{333}\) Id.  
\(^{334}\) Id. § 3.7.
specific types and categories of information that it focuses on); to whom the compliance report is disseminated to; and the policy concerning follow-up action to resolve any problem areas which have been uncovered and highlighted in the compliance report.\footnote{335}

10. Confidentiality

ETO § 46 emphasizes the importance of secrecy of private information; the RCA is precluded from infringement of the right of privacy of all interested parties. Accordingly, the "Confidentiality Policy" section\footnote{336} is one of the most important parts of the CPS. Specific issues to be addressed includes: categories of information which must be treated confidentially, with special attention paid to the outsourcing component of the RCA’s activities; categories of information that are not confidential; the parties to be informed in the cases of suspension or revocation of certificates; laws and internal policies in regard to release of otherwise-confidential information to law-enforcement authorities or a court of law; the policy on release of records or information to the subscriber, a relying party, or others; and the situations or conditions allowing the RCA to disclose information or records with the owner’s consent.\footnote{337}

11. Identification and Authentication

It is critical for the RCA to use good methods of identification of the parties and authentication of relevant documents.

12. Initial Certification

The naming convention should be expressed, e.g., “X.500 Distinguished Names ("DN").”\footnote{338} Details of all name forms must be given, including prefixes.\footnote{339} Policies used to avoid “name collisions,” (i.e., two or more persons having the same name)
should be included, and it should be stated as to whether each name must be unique.\textsuperscript{340} Also, there should be a name claim dispute resolution procedure.\textsuperscript{341} Consideration should be given as to whether names on the certificate are meaningful.\textsuperscript{342} The method to prove the possession of the private key should be listed.\textsuperscript{343}

One of the most crucial parts of the CPS concerns the specific means of identification of the subscriber.\textsuperscript{344} If specific application procedures are adopted and applied in each and every case, this will enable a prospective subscriber to understand exactly what personal data is required to be submitted in the application; and, it will give the relying third party some notion as to the degree of reliability of the certificates which have been issued under the CPS.\textsuperscript{345}

13. Other Situations

In regard to an application for revocation or suspension of a certificate, it is important for the CPS to express: who may make such a request and in what circumstances; the effect of revocation/suspension; how long after revocation/suspension occurs will the publication occur; the duties of the subscriber to inform the RCA of events which may require revocation/suspension; and protections given to the subscriber after revocation/suspension is requested (to include the allocation of liability between the RCA and the subscriber).\textsuperscript{346}

Stringent identification information also must be required in situations of routine re-key, certificate renewal, and re-key after revocation.\textsuperscript{347}

\textsuperscript{340} Id.
\textsuperscript{341} Id. § 4.1.5.
\textsuperscript{342} Id. § 4.1.2.
\textsuperscript{343} Id. § 4.1.6.
\textsuperscript{344} Id. § 4.1.7.
\textsuperscript{345} Id.
\textsuperscript{346} Id. §§ 4.4, 4.5.
\textsuperscript{347} Id. §§ 4.2, 4.3.
P. Operational Requirements

1. Steps in Application for a Certificate

The established procedure pertaining to application for a certificate should be explained in detail.\textsuperscript{348} The documentation required, personal information to be authenticated, and the means of identification must be expressed.\textsuperscript{349} Any interface requirement must be explained.\textsuperscript{350}

Additionally, the applicant should be explained the responsibilities he/she will be assuming, terms and conditions pertaining to the application, and any representations which may have been made by the RCA.\textsuperscript{351} The recognition status of the certificates must be emphasized in the CPS; if the certificates are not recognized, the implications of that status should be expressed.\textsuperscript{352}

2. Certificate Issuance

The CPS must include the processes employed by the RCA in: the generation of keys,\textsuperscript{353} the delivery of keys,\textsuperscript{354} ensuring that it does not have possession of the subscriber's private keys without their written consent; creation of certificates; delivery of certificates to applicants; and the posting of the certificates in the repository.\textsuperscript{355}

\footnotesize
\begin{itemize}
  \item \textsuperscript{348} Id. § 5.1.
  \item \textsuperscript{349} Id.
  \item \textsuperscript{350} Id.
  \item \textsuperscript{351} Id.
  \item \textsuperscript{352} Id.
  \item \textsuperscript{353} Id. § 5.2.
  \item \textsuperscript{354} Id. If the keys are generated by the applicant, the public key must be delivered to the RCA with the certificate request and the RCA must confirm that the applicant is in possession of the corresponding private key. On the other hand, if the keys are generated by the RCA, the private key must be safely delivered to the applicant, and the RCA must indicate the precautions it takes to ensure the security of keys in its possession.
  \item \textsuperscript{355} Code of Practice for Recognized Certification Authorities Published by the Government Chief Information Officer under Section 33 of the Electronic
3. Certificate Acceptance

The CPS must describe the procedure used to assure that the certificate has been accepted by the subscriber. This includes the necessity for the RCA to explain to the subscriber the significance of their responsibilities. The applicant will be given an opportunity to verify the information on the certificate before accepting. The applicant should be given a chance to either accept the certificate, or reject it. If deciding to accept, the applicant will be issued the certificate.

4. Certificate Suspension

The suspension process shall be expressed in detail, to include: conditions for suspension; who can initiate/stop a suspension; how a suspension is initiated/stopped; time limits for stopping the suspension or moving from suspension to revocation; total time allowed for the suspension to last; allocation of liability during the “in-between period” (between request of suspension and implementation of suspension); how much time is allotted the RCA to check with the subscriber or a relying third party as to whether the suspension should occur; and what the RCA should do if the subscriber or the relying third party cannot be located.

5. Certificate Revocation

The revocation process shall be expressed in detail, to include: conditions for revocation; who can initiate/stop a revocation; how a revocation is initiated/stopped; methods used to give notice of a revocation (e.g., posting, email, certificate revocation list, update to a revocation/validity information server); the amount of time allowed to complete the revocation process; and the allocation of


356 Id. § 5.3.
357 Id. See also responsibilities defined in CPS. Id. § 3.1.2.
358 Id. § 5.3.
359 Id.
360 Id.
361 Id. § 5.4.1.
liability in the "in-between period" (between time of request of revocation and implementation of revocation).362

In order for the revocation request to be valid, the subscriber (or authorized person) must: identify the certificate to be revoked; give the reason for revocation; and attach a digital or a manual signature.363 These requirements reduce the likelihood of an imposter revoking the certificate of a subscriber.

Ordinarily, revocation is required in the following situations: when information in the certificate has changed before its expiration; the subscriber has not complied with the stipulations of the CPS; the subscriber informs the RCA that the private key has either been lost or its security may have been compromised; or the subscriber no longer wants the ability to sign electronic messages.364

The RCA’s Certificate Revocation Lists ("CRLs") identifies the certificates that it has revoked, and the reasons for the revocation.365 The CPS indicates its procedure for distribution of the CRL and how relying parties may access it.366 Ordinarily, it is posted at the RCA’s website, but other means of publication may also be used.367

The RCA must warn subscribers not to rely on a digital signature if the certificate containing the public key has been revoked.368 Additionally, the CPS must address the issue of allocation of liability between the RCA and relying third parties in the following situation: when the third party is temporarily unable to obtain information pertaining to revoked certificates, and the RCA is responsible for the third party's inability to obtain the information.369

362 Id. § 5.4.2.
363 Id.
364 Id.
365 Id. § 5.4.3.
366 Id.
367 Id.
368 Id. § 5.4.4.
369 Id.

   a. Utilization of Event Logs. In order to maintain a secure environment, the RCA needs to list in the CPS the types of events which must be “logged” in: any “suspicious network activity;” (e.g., an unusual amount of unsuccessful attempts to gain access to the network); events pertaining to the network installation, modification and configuration of the network; and events pertaining to privileged access to any part of the RCA’s network.370

   Also, the following events pertaining to management of certificates need to be recorded: revocation and suspension requests; actual issuance, revocation, and suspension; actual renewals; additions made to the repository; creation and publication of revocation and suspension information; the RCA’s generation of keys, and rollover operations; the RCA’s generation of key pairs for the subscriber; creation of backups and their safekeeping; and recovery from emergencies.371

   The frequency of making entries in the event logs needs to be noted,372 as well as the frequency of consolidation and review of the logs.373 Specification needs to be made of the retention period for the logs,374 the means of safeguarding the logs,375 and the provision of backup procedures for the logs.376

   b. Archived Records. A general maxim regarding records retention is that the RCA should maintain records with sufficient enough detail so as to allow the validation of a certificate and the past “proper operation” of the certificate.377 Accordingly, the following are typical data to be considered by the RCA for record-keeping: data pertaining to initialization of the RCA’s equipment (e.g., configuration files, assessment reviews, CPS, and contracts to which the RCA is a party), and data pertaining to the RCA’s

370 Id. § 5.5.1.
371 Id.
372 Id. § 5.5.2.
373 Id.
374 Id. § 5.5.3.
375 Id. § 5.5.4.
376 Id. § 5.5.5.
377 Id. § 5.6.
operations (e.g., updates made to any of the aforementioned items, all certificates and their suspension/revocation information, periodic event logs, and other information as necessary).  

The retention period for archived information should be expressed, as well as protection measures, and backup procedures for said information.

7. **Key Changeover and Compromise**

If the RCA routinely engages in changeover of the keys (e.g., as a security precaution), the changeover procedure should be included in the CPS as well as details pertaining to how the subscribers will be so informed.

Because of the ever-present possibility of key compromise or disaster, it is necessary for the RCA to have a response plan ready in the event of those contingencies. In planning for the compromise of the computer system, the following factors, at a minimum, need to be considered in the CPS: how to re-establish a secure environment after it has been tainted; how to make a decision as to which certificates need to be revoked, if any; how to decide if the RCA should revoke its own key; the procedure to be employed in re-certification of the subscribers; and how the RCA’s new public key will be delivered to the subscribers.

If a key compromise has taken place, or is strongly suspected, subscribers and relying parties must be so informed. Additionally, procedures pertaining to re-establishment of trustworthiness need to be implemented.

During or following a natural disaster, the facility’s exceptional security measures need to be implemented during the period before normal security has been fully reinstated. For example,
exceptional security procedures would need to be implemented in order to protect sensitive materials at a damaged location.  

8. *The RCA’s Termination Plan*

Such a plan shall contain the steps to be taken in the winding-up of the CA’s service. Part of said plan will consist of notifying the subscribers and the relying third parties. The future location of the archived records, and the identity of their custodian, needs to be conveyed. The arrangements for termination of service are required to be in compliance with the requirements expressed in section 11 of the Code of Practice.  

Q. *Physical, Procedural and Personnel Security Controls*

The RCA must also explain how the non-technical operational controls help to ensure that its business is being conducted in a trustworthy manner. These controls include physical, procedural and personnel controls.  

1. *Physical Security*

Physical security controls should be described. The RCA must have security over its buildings and offices. Secure areas must be identified and control must be established over their access. Environmental hazards (e.g., fire, humidity, water, etc.) must be dealt with. Storage and disposal of media must be properly carried out.  

2. *Procedural Controls Over the RCA’s Managers*

Trusted roles need to be identified. The role in need of the greatest degree of trust is the RCA’s Administrator. This person will supervise the issuance of certificates, organization of

---

386 *Id.*
387 *Id.* § 5.9.
388 *Id.* § 6.
389 *Id.* § 6.1.
390 A trusted role is one “where the incumbent performs functions that can introduce security problems if not carried out properly.” *Id.* § 6.2.
operations, and record-keeping. The Administrator must be especially cognizant of the organization’s stipulations in its CPS, and do everything possible to ensure that they are met.

Another trusted role is that of Key Recovery Agent. This person will supervise the “more specific functions related to the maintenance of key recovery material or systems.”

Other trusted roles may also be established by the RCA. In order to promote trustworthiness and integrity of the system, a good management control tool is to separate the duties of the principal officers. This separation of powers and responsibilities is good management because it results in a system of “checks and balances” and helps to prevent any one of the officers from violating the integrity and trustworthiness of the system, which is so crucial to the success of the RCA’s organization.

3. Control of Non-Managerial Personnel

In the RCA organization, use of good personnel management methods is even more important than in the ordinary business firm, and pay big dividends. In an RCA firm, relatively more attention must be devoted to: (1) background checks and security clearances when recruiting personnel; (2) employee training to ensure that all understand the importance of maintaining a trustworthy system, and how to perform their job functions efficiently and correctly; (3) utilization of job rotation to reduce the likelihood that an employee will be able to totally control one of the functions of the RCA; (4) meticulous methods of performance appraisal, and stringent discipline and punishment for infraction of work rules pertaining to unauthorized acts; (5) heightened control over contractor personnel and obtaining indemnification agreements before they begin work in the RCA organization; and (6) provision of manuals to the personnel explaining operational procedures and the specific details of their jobs.

\[\text{id.} \S 6.2.\]
\[\text{id.}\]
\[\text{id.}\]
\[\text{id.}\]
\[\text{id.} \S 6.3.\]
R. Technical Security Controls

1. Control of Keys

One of the most important factors pertaining to trustworthiness concerns security of the keys. Issues to be addressed in the CPS include: who is responsible for generation of the key pair; methods used to attain secure delivery of the keys to the subscriber/certificate user; size of the key to be adopted; quality controls over public key parameters; requirements concerning the type and quality of cryptographic modules used; and the key’s usage and purpose (i.e., mapping under the X.509 PKI Certificate Profile version 3 and CRL Profile version 2 standards).

With respect to the issue of protection of the private keys, the following issues are worthy of consideration in the CPS: technical standards of the key generation module that is employed by the RCA (e.g., the ISO 15782-1/FIPS 140-1 Security Requirements for Cryptographic Modules); requiring more than one person to approve a transaction pertaining to a private key; the type of back-up established for private keys and security controls over it; the security controls of the location at which the private keys are archived; security controls over the keys’ activation, usage, deactivation and destruction; and the length of the usage period for private keys.

2. Control of Activation Data

In addition to attainment of control over the keys themselves, it is equally important to attain control over the activation data (e.g., passwords and PIN numbers) used for the keys; this applies throughout the life cycle of such data, from their creation to their distribution, utilization, archival, and eventual destruction. Issues in this regard which may be covered in the CPS include: computer security controls (e.g., controls used to prevent

---

396 Id. § 7.
397 Id.
398 Id.
399 Id.
unauthorized access to the system—reference may be made to a computer security rating framework standard, such as ISO 15408:1999; system development life cycle controls (e.g., developing the hardware and software for the initial configuration to prevent tampering); network security controls (e.g., use of a firewall to protect the system from outside "invasion," or monitoring of unauthorized access attempts; and cryptographic module engineering controls (an appropriate standard may be referenced, such as ISO 15782-1/FIPS 140-1, Security Requirements for Cryptographic Modules).400

S. Certificate and CRL Profiles

The CPS shall include the format used for its certificates and certificate revocation list ("CRL").401 Although not specifically mandated to be used, it is "generally envisaged" that the format of the certificate will be ITU X.509 v3, and the format of the CRL will be ITU X.509 v2 CRL.402 Utilization of these standard formats will facilitate the interaction of a particular RCA’s certificates403 and CRL’s404 with other organizations throughout the world.

T. Procedures Pertaining to Posting and Amendment of the CPS

The CPS must specify the repository or other means used to disseminate the CPS.405 The repository may be located at the

400 Id.
401 Id. § 8.
402 Id. These are standards developed by the International Telecommunications Union.
403 More specific information pertaining to the certification format includes: the version number supported; certificate extensions; cryptographic algorithm object identifiers; name forms and constraints; certificate policy object identifier; whether the policy constraints extension is employed; syntax and semantics of policy qualifiers; and processing semantics of the critical certificate policy extension. Id.
404 More specific information pertaining to the CRL includes: version numbers supported; details regarding the entry extensions; and other media used to publish notice of revocation and how to access them. Id.
405 Id. § 9.2.
RCA’s website. The CPS must inform the subscribers and the relying third parties the location of the repository and how to access the CPS.

The CPS should also include the procedure adopted for amending the CPS. Means of notification of interested parties (i.e., the subscriber, the relying third parties, and the GCIO) should be stated. If the repository is used to notify the changes, the posting to the repository should be made before, or very soon after, the changes have been made. The CPS may also indicate the types of changes, if any, that do not require prior notification to the parties.

VII. THE SECRETARY’S EXECUTIVE ORDER OF 2005

Section 11(2) of the ETO provides that: “The Secretary may, in relation to an Ordinance to which this Ordinance applies, specify by notice published in the Gazette (a) the manner and format in which information in the form of an electronic record is to be given, presented or retained for the purposes of that Ordinance . . . .” Accordingly, in January of 2005, Secretary Francis Ho issued an executive order specifying the required format for the submission of documents in electronic form to the Hong Kong government. This executive order went into effect on 1 March 2005. The order is applicable to electronic documents filed with the government, but does not apply to

---

406 Id.
407 Id.
408 Id. § 9.1.
409 Id.
410 Id.
411 Id.
413 Id.
electronic documents transmitted to private, non-governmental parties. Private parties determine their own format requirements.\footnote{Id. For example: (1) if English characters are used, they must be coded in either ASCII or ISO 10646-1:2000; (2) if English characters are coded in ASCII, then Chinese characters shall be coded in Big 5; (3) if electronic records are compressed, then one of the following compression standards shall be used: Zip file (.zip), or GNU zip file (.gz); (4) one of the following file formats must be used: TXT, RTF, HTML, or PDF; and (5) graphics must employ one of these graphic file formats: EPSF, TIFF, PNG, GIF, or JPEG. \textit{Id.}}

VIII. CONCLUSIONS AND RECOMMENDATIONS

A. Conclusions

Hong Kong is perhaps the “most wired” city in the world and has one of the best environments for e-commerce. Hong Kong’s e-signature law is a major contributing factor to this environment.

The Electronic Transactions Ordinance (“ETO”) was enacted in 2000 and provided for legal recognition of the digital signature in private e-commerce transactions and in official communications with the Hong Kong government. A digital signature was given the same legal effect as if were a handwritten one. This removal of the legal impediments toward electronic “signing” facilitated the development of e-commerce (and E-government) in Hong Kong. With the adoption of the digital signature, Hong Kong concomitantly began to utilize asymmetric cryptology, public key infrastructure, and a system of regulation of certification authorities.

However, the original ETO allowed only one form of electronic signature—digital. This ran contrary to the trend in global electronic signature law, which encourages nations to take a “technologically neutral” approach and not to grant a “monopoly” to only one form of electronic signature. Accordingly, the ETO was amended in 2004 to allow for: (1) other forms of electronic signatures to be acceptable in the private sector, with retention of the digital signature requirement for communiqués with the government; (2) electronic delivery whenever an ordinance specifies that delivery is to be “by post or in person;” (3)
bifurcation of the Annual Report of Compliance Assessment pertaining to certification authorities ("CA"), with one part to be performed by an independent auditor, and the other part to be achieved with submission of a sworn statement from the CA; and (4) a requirement that certain types of major changes in the CA's organization or status must be reported immediately to the government, in the middle of the reporting period.

Hong Kong has a "voluntary" system of regulation of CA's; it is not compulsory for CAs to apply for, or to achieve, recognized status. However, the advantage in doing so is that the recognized certification authority ("RCA") is able to provide more overall security for the subscriber than a non-recognized one, and the subscriber may be willing to pay more for the RCA's services as a result. Pursuant to the ETO, the Government Chief Information Officer ("GCIO") issued the Code of Practice, a handbook of regulations pertaining to RCAs, in 2004. The Code of Practice meticulously specifies the standards and procedures for carrying out the functions of an RCA, and includes detailed requirements pertaining to these two documents: (1) the RCA's Annual Report of Compliance Assessment; and (2) the RCA's Certification Practice Statement. These two documents, both of which must be periodically submitted by the RCA to the GCIO, play an important role in the attainment of governmental oversight over the activities of RCAs. Therefore, whilst the amended ETO now recognizes the validity of more than one form of electronic signature, simultaneously it is strengthening the degree of trustworthiness of digital signatures through more stringent regulation of RCAs.

However, one criticism of the government's promulgation of so many minute regulations of RCAs is that this runs counter to a basic trend in worldwide electronic signature law—minimalization of regulatory control by the government. The "minimalists" argue that digital signatures should be controlled more by market forces than by governmental regulations. One of the counter-arguments to this point of view, however, is that the digital signature is not required in the private sector; it is only mandatory when electronically communicating with the government of Hong Kong. Thus, in a private sector transaction, the transacting party is not confined to utilization of the digital signature, and is free to choose
another form of electronic signature and avoid altogether the rather stringent regulatory rules adopted for CAs. A party “opting out” of the digital signature, though, may later regret that decision because he/she will then ordinarily have a relatively less secure environment than that afforded by the digital signature. Trade-offs, always tradeoffs . . . we can never avoid them.

B. Recommendations

So far, the ETO seems to be doing a good job in protecting the consumer-subscriber from the unscrupulous or incompetent RCA. The RCA faces a colossal amount of regulation, making it difficult indeed for that party to engage in illegal, unethical, or incompetent behavior. Besides the technical regulations, the RCA is also mandated to employ fair advertising methods.

However, the greatest potential threat to the online consumer is neither the RCA nor the computer hacker—it is the online seller! The original ETO and its amendments do not provide enough protection of the naïve consumer-buyer from the unscrupulous cyber-seller. To fill this vacuum, the ETO should be amended again; a new section should be added pertaining to the online seller’s required disclosures to the buyer. The new section should be modeled after the consumer disclosures section of the U.S. Electronic Signatures in Global and National Commerce Act (“E-Sign”). The following provisions (paraphrased from the E-Sign Act) need to be included:

1. If the seller is already required to give information to the consumer in writing, provision of the information in electronic form is only allowed if:
   i. the buyer consents to the electronic form (and has not withdrawn consent); and
   ii. prior to the consent, the consumer was informed in a “clear and conspicuous statement.”

---

416 Id. § 101(c)(1).
417 Id. § 101(c)(1)(A).
418 Id. § 101(c)(1)(B) (emphasis added). The “clear and conspicuous” requirement means just what it says—this notice should be in plain view, not
iii. that he/she is not mandated to accept the electronic form, he/she may refuse to accept it, and he/she was informed of the right to withdraw the consent (and any penalties incurred because of withdrawal of consent);\(^{419}\)

iv. whether the consent applies only to the particular transaction currently under consideration, or other transactions as well;\(^{420}\)

v. how to withdraw consent and how to electronically update contact information of the buyer;\(^{421}\)

vi. how the buyer may obtain a paper copy of an electronic record, and the amount of fee (if any) charged for the copy;\(^{422}\) and the consumer\(^{423}\) before consenting, was given a statement of the required computer hardware and software necessary to access the electronic records;\(^{424}\)

vii. consented electronically, "in a manner that reasonably demonstrates" that the consumer possesses enough computer knowledge and understanding to be able to "access information in the electronic form that will be used to provide the information that is the subject of the consent;"\(^{425}\) and

viii. after consent has been given, if a change in the hardware or software required to access electronic records leads to a "material risk" that the consumer won't be able to obtain access in the future, or to retain an electronic document in the future, then the seller must:\(^{426}\)

ix. provide the buyer a statement of the revised hardware and software requirements, with notice that the buyer may now withdraw the consent previously given without imposition of a fee or a penalty;\(^{427}\) and

x. again comply with (c), above.\(^{428}\)

2. These provisions do not affect or replace any other disclosures to the consumer which may be required under another statute, regulation or rule of law.\(^{429}\)
3. Withdrawal of consent in (1), above, does not affect the legal validity of electronic records provided to the buyer before the consent was withdrawn. The buyer's withdrawal of consent is effective "within a reasonable period of time" after receipt of the withdrawal by the seller. The buyer may elect to treat a failure of the seller to comply with (1)(d), above, as a withdrawal of consent.\textsuperscript{430}

C. A Final Thought

Law, by its very nature, is not "cast in stone." It is always a work in process, a stage in the evolutionary process. Hong Kong's Electronic Transactions Ordinance is no exception. The amendments of 2004 significantly improved it and, in all likelihood, more "fine tuning" of the ETO will occur in the future. Expect Hong Kong to continue to be in the vanguard of world e-commerce law and to uphold its reputation as one of the world's "most wired" cities.

\textsuperscript{430} Id. § 101(c)(4).