BSA *Business Software Alliance*

November 12, 1999

Miss Salumi Chan
Clerk to Bills Committee
Legislative Council
Legislative Council Building
8 Jackson Road
Central
Hong Kong

Dear Miss Chan,

Thank you for sending us the points you made to the Legislative Council in reply to BSA's original comments on the draft Electronic Transactions Bill.

We read your response with great interest, and feel encouraged by your willingness to respond to our concerns. It is in this constructive perspective that we would like to further discuss several remaining aspects of your response:

General Concerns:

(1) BSA agrees that legal certainty is of fundamental importance to the development of electronic commerce. BSA also agrees that the goal of providing legal certainty should be central to the Electronic Transactions Bill. We follow the lines of UNCITRAL, the National Conference of Commissioners on Uniform State Law, the European Commission and others in the belief that this legal certainty is obtained by removing any uncertainty about the legal recognition of electronic signatures. Virtually all the most recently adopted laws and ongoing regulatory activities are promoting the principle of non-discrimination. The fundamental article of any regulation aimed at providing legal recognition of electronic signatures should embody the principle that an electronic signature can not be denied legal effect exclusively on the basis that it is in electronic format or that it has not been generated using a particular technology.

BSA however does not see the reinforcing link between the use of current security measures and legal certainty. Legal certainty can be obtained by establishing, to the greatest extent possible, the equivalency of electronic signatures and manual signatures. The purpose is to overcome unwarranted biases against electronic methods of signing and authenticating records, without putting requirements on them which never existed for manual signatures. Security measures can create user confidence if they provide the adequate level of security for the right price, depending on the underlying transaction. They will not automatically create legal certainty, especially if the framework which should provide them legal recognition is unclear.

.../Page 2

(2) By not adopting a non-discrimination clause, the Bill denies any legal certainty to certificates which have not been recognized. In addition, according to the bill, a non-recognized certification authority cannot create legally recognized certificates. However, as the draft Bill is based on Public Key Infrastructure and only foresees the recognition of specific certificates and certificate authorities, will not be able to cover existing and upcoming transactions in need of legal certainty. It excludes any form of biometrics, a click of the "I agree" button or any future technology that will be developed. Though of course signatures and certification authorities need to be reliable, this can be addressed by qualitative criteria. In addition, this can be addressed by minimum criteria rather than licensing procedures, which are known to often be a slow and non-transparent approval mechanism.

In addition, any criteria used to determine legal recognition will only give legal certainty if they are explicate and verifiable.

Moreover, by linking the license regime to legal recognition, the HK government is creating a de-facto mandatory license regime. Though CAs are allowed to operate without license, none of the certificates they produce will be legally recognized. A de-facto licensing system cannot be considered to emulate market forces. An industry or government certification or seal system could be set up to provide additional trust to the less experienced user, but this should not result in a denial of legal recognition to non certified certificates.

(3) International experience has shown that technical standards developed by governments, especially in fast-changing areas such as the Internet, are usually outdated before they are adopted. Standardization efforts should be handed over to industry. The term "code of practice" is misleading, as this term traditionally points to an industry consensus or self-regulation, which is clearly not the case here. BSA has the firm intention of commenting on the code in a separate note, but nevertheless feels that certain fundamental issues of the Bill need to be addressed first, before addressing more detailed aspects.

Public Key Infrastructure (PKI), as the term indicates, is not technology neutral. On this issue, study made recently by the law firm Steptoe and Johnson for the Internet Law and Policy Forum says: "As recently as 1995, when legislative initiatives began to emerge in the United States, the use of asymmetric, or "public key," cryptography as a means of creating "digital signatures" was widely perceived as the nearly-universal foundation for all electronic authentication. Indeed, it is safe to say that this perception continued well into 1997, both in the United States and abroad, and remains influential today. More recently, however, there has been growing recognition that other means of electronic authentication, including biometrics and dynamic signature analysis, will take on equal or greater importance in the years ahead. In fact, some of these techniques - and particularly those that are based on biometrics features - may prove to be more reliable and less susceptible to compromise than digital signatures." They go on to conclude that not one technology will prevail as a sole means of authentication.

Neither authentication service providers nor users will be served by a premature designation of technologies or rules which are created for the sole purpose of erecting a uniform framework.

.../Page 3

(4) As mentioned above, the Hong Kong government should anticipate that authentication means (including both the use of business practices and technology solutions) will change over time in response to technological developments and market demands. It should avoid any action likely, directly or indirectly, to preclude or discourage innovation in authentication technologies or new applications for those technologies. In particular, when a government acts as participants in the marketplace, engaging in transactions with citizens and other parties, it should not "lock in" particular electronic authentication means through the force of its presence in the marketplace, but rather should allow for changing market standards and applications for existing and future technologies.

The pace of the policy making and adoption is inherently slow, especially compared to the fast pace of technological change of the Internet. This is why governments around the world have already emphasized the need for flexible and technology neutral legislation to foster electronic commerce. Building a legal framework around a currently available technology in the fast moving environment of e-commerce risks isolating Hong Kong from the mainstream of technological and legislative developments internationally. Without the Bill, government departments and all other parties in the community would have the contractual freedom to demand certain types of signatures and/or signatures providing specific levels of security in their dealings with other parties. Governments should not determine for users other than themselves what the appropriate technology, level of security and related cost is of the authentication method users want to associate with their transaction. It is important that governments avoid discriminating against electronic signatures by applying stricter rules to them than to handwritten signatures. Aside from the current Electronic Transactions Bill, it seems unclear which "various rules of law" oblige the government and other users to use digital signatures rather than any other forms of electronic signatures. Again, in this respect, BSA feels that denying legal recognition to electronic signatures other than those approved by the government creates a de-facto barrier to their use, by denying them the legal certainty given to recognized certificates.

Though it is mentioned in the response that recognition of signatures other than digital signature would be governed by the common law, it is not always clear whether or not existing laws or regulations impose legal barriers to the recognition of electronic signatures or not. The main goal of legislation in this area should be the removal of this uncertainty.

(5) As mentioned above, a voluntary licensing scheme linked to the granting of legal recognition can be seen as a de-facto mandatory licensing scheme. In this scenario, the number of certification authorities will not be decided by the market but by the Hong Kong government.

(6) As mentioned above, the pace of the policy making and adoption is inherently slow, especially compared to the fast pace of technological change of the Internet. If the Hong Kong government can already foresee now that it will have to amend the electronic Transactions Ordinance in reaction to the development of new technologies, it is clear that it will never be a law which promotes innovation. The law does really risk isolating Hong Kong from the mainstream of technological and legislative developments internationally.

.../Page 4

(7) Here again, BSA is of the position that the denial of legal certainty is a restriction. If it were not, the Hong Kong government would not be drawing up an electronic transactions bill aimed at providing legal recognition for a specific type of digital signatures.

The Bill establishes overly-restrictive conditions for legal recognition

(1) The government as a user can demand specific characteristics for the signatures it wants to use in its dealings with its business partners, though even then it would be advisable not to do it in a way which would foreclose the market. The government would certainly not be forced to be able to accept and handle electronic records prepared using any type of software just because they are not being discriminated against. Specific requirements of the governments as a user should, however, not effect the general conditions for legal recognition of electronic signatures used by all other users.

Other Concerns:

(1) Though article 20 (3) goes in the right direction of setting objective and verifiable criteria for the Director to follow, the purpose of the clause is undermined by the first sentence of 20(3), which states that the Director is able to take decisions based on "any other matter the Director considers relevant". In addition, though Article 19 speaks of a "prescribed manner" and a "prescribed fee" to submit an application, the director may wave "any requirements" and "part or whole of the prescribed fee". "Specific conditions" and the "period of validity" may be determined by the Director, without any reference to any verifiable criteria on which these decisions should be made. The same comments are valid for the recognition of certificates, which the Director seems to be allowed to grant at wish (Art.21(1)"The Director MAY recognize [....]"). A slight worry regarding the possibility of appeal is that appeal is only possible with the Secretary of Information Technology and Broadcasting. The question arises whether a more independent body would not be more appropriate.

(2) BSA is grateful to the DITS for sending us the Draft "Code of Practice", and will be submitting comments on the "Code" in a separate note. However, we do feel that it is essential for the Bill to be of the highest quality from the start, and would therefore prefer to await the DITS' reaction to some of our fundamental concerns regarding the Bill itself before reacting on the "Code" intended to implement it.

(3) It remains unclear to the members of BSA why the Hong Kong Post does not have to comply with the same criteria for its recognition as a Certification Authority and for the recognition of its certificates as any other certification authority looking for its own recognition and that of its certificates.

(4) BSA still feels that it is unnecessary and premature to deal with the liability issue at this stage. Though it is true that some countries, such as Singapore, Malaysia and Utah (some of the fist digital signature legislations around) have limitation of liability clauses, most of the more recent laws do not.

.../Page 5

(5) The Hong Kong government should recognize that their actions with respect to electronic authentication can create barriers to trade. As mentioned earlier, denying legal certainty is a barrier, and even a discriminating barrier if it is combined with the granting of legal recognition under very restrictive conditions. Electronic commerce is global, and the mutual recognition between electronic signatures between countries will need to be ensured for electronic commerce to take off. The universally recognized work of UNCITRAL in this area was initiated explicitly to ensure that this mutual recognition could take place. If the Hong Kong Bill were used as a model in other countries, electronic commerce would not be possible across national borders, as no country would legally recognize the electronic signatures generated in the other countries. For an economy with a trading capacity so inversely proportional to its size, it would seem a very curious precedent to set.

Sincerely,

Tom Robertson
Vice President