立法會 CB(1)443/99-00(04)號文件
LC Paper No. CB(1) 443/99-00(04)

Comments on the Responses made by the Government on

Electronic Transactions Bill and Code of Practice

By

Information Technology Division, Hong Kong Institution of Engineers

Date: 22-Nov-1999

Your Ref.: LC Paper No. CB(1) 409/99-00(02)

On Standards for Certification Authority and Code of Practice

- *We note the comments on the code of practice for recognised certification authorities. It is the intention of the Director of Information Technology Services to provide more detailed guidelines on the criteria for the recognition of certification authorities as well as the operation of recognised certification authorities.*

Our comments:

We never have any doubt that it is always the intention of the DITS to prepare more detailed guidelines on the criteria for the recognition of the certification authorities. However, if this is the genuine "intention", it was not evidently shown in the recent Code of Practice issued by the ITSD. In fact, before the enactment of the ETB, the public should be given a whole set of the regulatory framework for the Certification Authorities as covered in the ETB, so that the public can discuss and debate on the contents as openly and freely as possible.

By deferring the release of these "detailed guidelines", and decoupling these "detailed guidelines" from the Code of Practice, the public is deprived of the chance to comment on the regulatory framework as a whole and to give an overall view on what needs to be done. We are fully aware of the complexity of this framework, as the ETB, COP, regulations (Section 44 refers) and conditions (Section 20(5) refers) for the CA are all closely inter-linked with each other.

If the Government plans to release these "detailed guidelines" at a later stage (for instance after the ETB is passed), they should assure the public of an open and transparent consultation exercise when such "detailed guidelines" are being developed. The Government should promise the public that a working task force (or similar arrangement) would be formed to develop such "detailed guidelines".

On Termination of Certification Authority Services

- *We note the comments on the termination of certification authority services. The Director of Information Technology Services will continue to maintain the certification authority disclosure record of the recognised certification authority after it has terminated its services. The disclosure record will contain the public key of the*

recognised certification authority which can be used to verify certificates previously issued by the recognised certification authority before its termination of services. It is also the intention of the Director of Information Technology Services to stipulate in the code of practice for recognised certification authorities that the termination plan of recognised certification authorities should cover not only the archiving of records but also the archiving of the public key of the recognised certification authority after its termination of service.

Our comments:

According to the ETB, the "disclosure record" is explicitly required to contain information about

- Revocation
- Suspension
- Renewal
- Audit date and result

As to whether other information such as the public key of the [once] recognized CA who has already terminated its business will be contained in the disclosure record, it is not explicitly mentioned in the ETB. So we doubt the validity of the approach suggested by the Government unless such a provision is explicitly mentioned in the ETB. The problem is about the legal status of the information contained in the disclosure record. If the DITS hands out a copy of the public key of the [once] recognized CA, does the public key still have the legal status to support the certificates this CA has issued and signed in the past? Since the ETB has no mention about the legal status of the public key of a [once] recognized CA handed out by the DITS, we cannot take it for granted that such a public key can have the same legal status as the one obtained from the recognized repository for the purpose of supporting the certificates this [once] recognized CA has issued in the past.

On Encryption

- *We do not see a need to specifically provide encrypted documents with legal status. Whether certain data messages need to be encrypted, and if so the particular encryption technology to be used, is to be decided by the sender and the recipient. We do not consider it appropriate to deal with this matter by law.*

Our Comments

Encryption (confidentiality) is as important as digital signature, we think that it should be given legal status in any legislation for Electronic Transactions. One only needs to study what other countries (Australia, Canada, UK, USA) have done to realize its importance. It is a pity that confidentiality has been given up by the Government at this important stage of legislation for Electronic Transactions. How many people would like to have their contracts flown across the public Internet in clear text form?

The use of encryption could not be a sole matter between the sender and the receiver if we are considering e-Commerce, e-Business, and Electronic Transactions as a whole. We are concerned that under the proposed legal framework, encrypted messages might be denied of legal status and hence no one could afford to use it. In relation to our concern, we would like the Government to provide clarification to following scenario:

- When someone encrypts an electronic record, can it be treated as being "*retained in the form in which it was originally generated"*?

- If an electronic record is encrypted, is it true or otherwise that "*the information contained in the electronic record is accessible so as to be usable for subsequent reference*"?

- If in the course of an electronic transaction, Alice signs a contract by applying her private key to encrypt the whole contract, and then sends it to the relying party Bob. Bob can use Alice's certificate and public key to verify the contract's integrity and authenticity. Can this be treated as an acceptable digital signature?

- If in the course of an electronic transaction between Alice and Bob, Alice

    1. signs the contract by applying Bob's public key to encrypt the whole contract;

    2. applies her private key to encrypt the encrypted contract; and then

    3. sends the doubly encrypted contract to the relying party Bob.

  Can this be treated as an acceptable method of generating a signature?

Without recognition for encryption by the ETB, we are worried that e-Business, e-Commerce, or Electronic Transactions as a whole cannot really flourish in Hong Kong, and will surely lag behind other countries who have already enacted law to support encryption.

On Public/Private Key Generation

- *Section 3.3.2b of the draft code of practice for recognised certification authorities stipulates that a recognised certification authority shall make and keep in a trustworthy manner the records of documents relating to the generation of its own and the subscribers' key pairs, not the actual key pairs of the subscribers. Section 3.3.4 stipulates that a recognised certification authority shall provide a trustworthy system for the generation of its own and the subscribers' key pairs, e.g. the recognised certification authority may provide trustworthy software for the subscriber to generate his own public/private keys. There is no mandatory requirement that the recognised certification authority must generate the private key for the subscribers.*

Our Comments

If the Government can confirm that the "*records of documents*" do not apply to subscribers' private keys, this should be stated clearly and unambiguously in the Code of Practice. On the other hand, if a recognized CA really keeps records of both the public key and private key of the subscribers, can it be treated as a violation of the Code of Practice?

We are amazed that the clause "*a recognised certification authority shall provide **a** trustworthy system for the generation of its own **and** the subscribers' key pairs*" can be interpreted by the Government as "to provide the subscriber with a trustworthy system, e.g. a [piece of] trustworthy software". Clearly the original clause means that the

recognised CA shall provide **a** trustworthy system for the generation of its own **and** the subscribers' key pairs simultaneously. This must be a trustworthy system for the CA's own use, not something to be provided to the subscriber.

We think that a *trustworthy system* must be a system as a whole, not only a single piece of software in its isolation. The system normally includes the hardware, the software, the environment, the security policy, and the personnel. We wonder how such a trustworthy system can be provided by the recognized CA to its subscribers to generate the subscribers' own key pairs. If this is a piece of "trustworthy software" for the subscriber to take home and run, will it still be trustworthy if it is run, say, in a careless manner, in a poorly controlled environment, or by an average user who does not have any training about information security? We find it hard to understand on what basis can the Government equate a trustworthy system to a piece of trustworthy software. We sincerely hope that such an interpretation of trustworthy system will not be used in the assessment of the CA who is applying for recognition in the future.

Since the Government maintains that "*there is no mandatory requirement that the recognised certification authority must generate the private key for the subscribers*", we think the public should be guaranteed by law the rights to submit only the public key to the recognized CA for the purpose of applying for a recognized certificate. If this cannot be incorporated in the ETB, at least the Code of Practice should spell out clearly these rights.

- *Whether a recognised certification authority should accept a subscriber's submission of his own public key for registration is a matter of commercial decision to be taken by the certification authority concerned, not by the Government. It is a matter for the clients to decide how their key pairs should be generated. There is no stipulation in the code of practice. We do not consider that there would be doubt or dispute over this matter between the recongised certification authority and the subscribers.*

Our Comments

Since a recognized CA is granted the legal status to generate recognized certificates for its subscribers, its operation should be regulated by law and that is the purposes of the ETB and the Code of Practice. Without a clear indication in the Code of Practice, (although such would have appeared in the regulations and conditions to the CA) we are concerned that if every recognized CA will not accept public key only, or if they charge a high price for that, there will not be any choice for the consumers. By that time the public are virtually forced to submit both the public and the private keys. If the Government maintains that this situation will not happen because of market forces, can the Government tell the public whether Hongkong Post, the first recongised CA, will accept public key only, for purposes of subscribers applying for recognised certificates?