Bangkok Post The world's window on Thailand

CORPORATE COUNSELLOR

Understanding signing documents electronically

0
Share Tweet

Published: 13/01/2012 at 12:00 AM
Newspaper section: Business

Clients often ask about the use of electronic signatures. However, when we delve further into their questions, we tend to find there is a misunderstanding as to precisely what this means. Often what they really mean to ask is whether they can sign a contract with a pen and then fax it, or scan and email it, and whether the copy that is printed at the other end will be effective in the same way as an original. This is something altogether different from an electronic signature.

Thailand has established an excellent framework enabling the use of electronic documents for legal purposes. The primary legislation on this topic is the Electronic Transactions Act (ETA) of 2001. Subject to a few narrow exceptions, the ETA takes the general approach that an offer and acceptance may be expressed in the form of a data message, and that a contract shall not be denied legal effect on the sole ground that the offer or acceptance with respect to that contract was made in the form of a data message. The concept of "data messages" includes information generated, sent, received, stored or processed by electronic means such as electronic data interchange, electronic mail, telegram, telex or facsimile. So this framework offers considerable latitude and does not explicitly require the use of any particular system.

Regarding documents that must be in writing, a data message is deemed to constitute a written document if the information is accessible and usable for subsequent reference without alteration of its meaning. Similarly, when a signature is actually required on a particular document, the ETA provides it will be deemed signed if the electronic method used is capable of identifying the signatory and indicating the signatory approved the information in the data message as his/her own, and if such method is reliable and appropriate, having regard to the parties' agreement in addition to the surrounding circumstances.

The ETA defines "electronic signature" as a letter, character, number, sound or any other symbol created in electronic form and affixed to a data message in order to establish the association between a person and a data message for purposes of identifying the signatory and showing the signatory has approved the information contained therein. An electronic signature is considered reliable if the signature creation data are, within the context in which they are used, linked to the signatory and no other person; if the signature creation data were, at the time of signing, under the control of the signatory and no other person; if any post-signing alteration is detectable; and if where the signature is meant to indicate that the signatory attests to the completeness and integrity of the information, any alteration to such information is detectable. However, the law is clear that these criteria should not function to limit other possible ways of proving whether an electronic signature is reliable.

It is important to bear in mind the law sets certain legal obligations for electronic signatories. Among these, they must exercise reasonable care to avoid unauthorised use of their signature creation data. In addition, one must quickly notify any person who may reasonably be expected to act in reliance on the electronic signature and/or the electronic signature service provider if the signatory knows or should have known that the signature creation data has been lost, damaged, compromised, unduly disclosed or known in a manner inconsistent with its purpose, or if the signatory becomes aware there is a substantial risk that the signature creation data may have been lost, damaged, compromised, unduly disclosed or known in a manner inconsistent with its purpose. Finally, where a certificate is issued to support the electronic signature, a signatory must exercise reasonable care to ensure the accuracy and completeness of all the signatory's material representations which are relevant to the certificate, throughout its validity.

Regarding legal proceedings, the ETA also makes express provisions for establishing the reliability and verifiability of data messages _ quite relevant if there is potential for their use as evidence in court. Primarily, this has implications for the system by which data messages are maintained so as to evidence transmission and acceptance thereof. On this issue, the ETA provides that in assessing the evidential weight of a data message so as to conclude whether and to what extent it is reliable, regard shall be had to the reliability of the method by which the data message was generated, stored and/or communicated and the methods by which the integrity of the information was maintained and by which its originator was identified or indicated, as well as all relevant circumstances. Thus, when using electronic documents, it is necessary to deploy a system that will capture, store and ultimately be able to present each one in a way that proves reliable, particularly regarding the identity of the signers.

In brief, the ETA has set the framework to provide for an approach that does not require the use of any particular system. Rather, the ETA has established requirements based on capability and appropriateness. These are further developed in ministerial regulations promulgated under the ETA. Electronic commerce is certainly an area of growth in Thailand, and we can only look forward to further developments in electronic signatures.

This article was prepared by David Duncan, a consultant in the Corporate and Commercial Department at Tilleke & Gibbins. Please send comments to Andrew Stoutley at andrew.s@tilleke.com