E-ASEAN REFERENCE FRAMEWORK FOR ELECTRONIC COMMERCE LEGAL INFRASTRUCTURE

ASEAN SECRETARIAT
2001

Published by the ASEAN Secretariat

ACKNOWLEDGMENTS

The publishers would like to thank the following for their contribution and assistance to this publication:

Brunei
Kasmirhan Tahir, AG Chambers, Brunei

Cambodia
Koy Kim Sea, Under Secretary of State, MPT, Cambodia

Indonesia
Arrianto Mukti Wibowo, Business Development Manager, Indosign
Rahmat Banuhampu, Liaison Officer, Embassy of the Republic of Indonesia

Malaysia
Izzam Ibrahim, Legal Advisor, MSC Trustgate
Khaw Lake Tee, Senior Manager, Legal Unit, MDC
Low Wee Liam, Manager, Information Risk Management

Myanmar
Thaung Tin, Managing Director, IT Education and PC Distribution

Philippines
Teresa Hatta, Managing Director, Banko Sentral ng Pilipinas
Claro Parlade, Parlade Law Office, Philippines
Enrique Domingo, Bank Attorney, Office of the General Counsel, Banko Sentral ng Pilipinas
Eugene C. Reyes, Foreign Trade Officer, Philippines

Singapore
William Hioe, Senior Director, IDA Singapore
Tan Ken Hwee, Senior Counsel, Attorney-General's Chambers
Lena Kua, Senior Manager, IDA Singapore
Lawrence Tan, Manager, IDA Singapore
Isa Seow, Assistant Manager, IDA Singapore

Thailand
Surangkana Kaewjumnong, Chief of IT Law Development Project, NECTEC
Danai Milindavanij, Ph.D, Acting Head Network Technology Laboratory, NECTEC
Orada Teppayayon, Legal Researcher, NECTEC

Finally, but not least, the publishers would like to thank Drew & Napier for giving its consent to use extracts from its publication entitled, "Your Guide to e-Commerce Law in Singapore".

CONTENTS

I. Purpose	**1**
II. Basic Concepts and Definitions	**2**
III. General Principles of e-Commerce Laws	**5**
IV. Scope and Legal Effects of e-Commerce Laws	**6**
V. Provisions of e-Commerce Laws	**7**
VI. Presumptions of e-Commerce Laws	**9**
VII. Implementation of e-Commerce Laws	**12**
VIII. Other Related Legislation	**14**
IX. Cross-Border Issues to be Addressed	**15**

I Purpose

1. This reference framework provides a guide for:

   a. Helping ASEAN member states that do not have any e-commerce laws in place to accelerate the timeline to draft their own;

   b. Helping ASEAN member states that already have e-commerce laws in place to facilitate cross-border e-commerce and the cross-recognition/cross-certification of digital certificates/digital signatures.

2. This reference framework is developed based on the following e-commerce laws of ASEAN member states, and in consultation with the legal experts from the governments of these member states:

   a. Electronic Transactions Act (ETA) of Singapore
   b. Digital Signature Act (DSA) of Malaysia
   c. Electronic Commerce Act (ECA) of Philippines
   d. Electronic Transactions Order (ETO) of Brunei
   e. Draft Electronic Transactions Bill (ETB) of Thailand

3. These e-commerce laws are in turn based largely on UNCITRAL's[1] Model Law on Electronic Commerce and Draft Model Law on Electronic Signatures, as well as the e-commerce and electronic signature laws of the US (e.g. Utah, Illinois) and Europe (e.g. Germany).

[1] UNCITRAL (United Nations Commission on International Trade Law) is the core legal body within the United Nations tasked by the UN General Assembly to further the progressive harmonisation and unification of international trade law, including international e-commerce law.

II Basic Concepts and Definitions

E-commerce

4. e-Commerce as used in the context of this reference framework refers to electronic transactions on the Internet or any other open networks. Such transactions can be divided into two categories:

a. Those that involve the sale of physical goods and services;

b. Those that involve the direct, on-line transfer of information and digital goods and services (e.g. software, music-on-demand, video-on-demand).

5. In the first category, the Internet or any other open network is used as the medium for order placement, acceptance and even payment, but the delivery of goods and services to the consumer is via the traditional physical mode.

6. In the second category, the Internet or any other open network is used as the medium of communication as well as the medium of exchange.

7. Because e-commerce takes place on the Internet or any other open network in a 'face-less' manner (i.e. the buyer and seller do not see each other face-to-face), it is necessary to have e-commerce laws to protect both the merchant and the customer.

Electronic Contracting

8. In law, a contract is said to come into being when an offer is accepted in unequivocal terms and with an intention to create legal relations. The contract must be supported by consideration, very often the price of the product or service purchased. In addition, the contracting parties must have legal capacity to enter into the contract that has sufficiently certain terms and conditions.

9. When a person makes an offer, he is expressing a desire to enter into a contract on the understanding that if the other party accepts his offer, there will be a binding agreement between the parties.

10. If an offer is to be accepted, the unequivocal acceptance of that offer must be communicated to the person who made that offer.

11. An offer can be revoked at any time before it is accepted (or deemed to be accepted). It can also lapse after a specified time (or a reasonable time, if unspecified) or on the occurrence of a specified event.

12. In electronic contracting, the offer and acceptance are communicated electronically.

Electronic Record

13. According to UNCITRAL's definition, an electronic record refers to "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy".

Electronic Signature / Digital Signature

14. UNCITRAL defines an electronic signature as "data in electronic form affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message".

15. A digital signature, on the other hand, is an "electronic signature consisting of a transformation of an 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 accurately determine (a) whether the transformation was created 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 made". A digital signature is thus more secure and tamper-proof than an electronic signature.

Public Key Infrastructure (PKI)

16. A public key infrastructure makes use of a cryptography system in which messages encrypted with one key can only be decrypted with a second key. The PKI gets its name from the concept that the user will make one key known to the public ('public key') but keep the other one secret ('private key'). The public can use the public key to send messages that only the private key owner can read. The private key can be used to send messages that could only have been sent by the private key owner.

17. The PKI also allows the user to create a digital signature which is unique to the private key and the length and contents of the message being sent. Anyone who has the user's public key can then verify the integrity of the signature and thus ascertain whether the message sent has been tampered with.

Digital Certificate and Certification Authority

18. Due to the 'face-less' nature of electronic communications, there is no independent means to verify that a message sent is really from the person alleged or from an impostor. A trusted third party, in the form of a certification authority (CA), is required to attest that a person issuing a digital signature may be presumed to be who he says he is. The CA is charged with issuing digital certificates to users. A digital certificate, which is stored on a smart card, functions like a secure electronic identification card. The digital certificate, which contains the user's identity, public and private keys, purpose and scope

of usage of the keys, can be used to generate the user's unique digital signatures.

III General Principles of e-Commerce Laws

19. The general principles of e-commerce laws are:

a. They should conform to international standards such as UNCITRAL's Model Law on Electronic Commerce and Draft Model Law on Electronic Signatures so as to be interoperable with similar laws of other countries;

b. They should be transparent and predictable so that there is no legal ambiguity between transacting parties in an electronic transaction;

c. They should be technology neutral, i.e. no discrimination between different types of technology;

d. They should be media neutral, i.e. paper-based commerce and e-commerce are to be treated equally by law.

IV Scope and Legal Effects of e-Commerce Laws

20. e-Commerce legislation is enacted with the purpose of providing predictability and certainty in areas where existing laws fall short. It is meant to encourage business and consumer confidence in e-commerce as well as provide legal recognition of electronic transactions, electronic records and electronic signatures. The legal effects are:

a. A contract can be formed electronically, unless otherwise agreed between the parties;

b. No record should be denied any legal effect just because it is a form of electronic record;

c. Where a rule of law requires information to be in writing, an electronic record would satisfy that rule if it is accessible for subsequent reference;

d. Electronic signatures meet all existing requirements for hand-written signatures.

21. In Singapore's implementation, some types of contracts are specifically excluded from the ETA at this point in time. This is because the notion of electronic contracts is fairly new to Singaporeans and the Singapore government wants to adopt a cautious approach first.

22. Contracts that must still be made in writing and signed by the contracting parties include:

a. Contracts for the sale or other disposition of immovable property or any interest in immovable property;

b. Powers of attorney;

c. Wills;

d. Negotiable instruments;

e. Documents of title.

23. Brunei's ETO, which is modelled closely after Singapore's ETA, also has similar limiting scope. In addition, Brunei's ETO also excludes the creation of any legal instrument or document under any written law relating to Islamic law. Thailand's ETB also has such limiting scope but is not spelt out explicitly, except as "prescribed in the Royal Decree". Philippines' ECA does not have such limiting scope.

V Provisions of e-Commerce Laws

24. e-Commerce laws should at least include the following features:

Electronic Transactions

25. Provisions clarifying that the normal rules of contract apply equally to transactions conducted online:

a. The legal recognition of an expression of offer and acceptance through an electronic record, including a declaration of will or notice and other statements associated with the formation of an electronic contract;

b. The rules to attribute an electronic record sent by an authorised sender or an automated system, and the circumstances in which a recipient of an electronic record is entitled to presume that a particular electronic record is from a particular sender;

c. The rules on acknowledging the receipt of an electronic record;

d. The rules determining the time and place an electronic record is considered as having been sent to, or received from, another person.

26. Provisions governing the legal effects of using electronic records and electronic signatures/digital signatures:

a. Information given in an electronic record should not be denied any legal effect merely on the basis that it is in electronic form;

b. A reliable electronic record should be legally valid and enforceable, subject to reasonable exceptions;

c. A reliable electronic record should satisfy certain legal requirements for information to be in written form or presented in writing, subject to reasonable exceptions;

d. A reliable electronic signature should satisfy any law that requires a signature for a document, subject to reasonable exceptions;

e. There should be rules to prove an electronic signature.

27. Provisions governing presumptions regarding reliable electronic records and electronic signatures/digital signatures:

a. There should be rules to govern the circumstances under which electronic records and electronic signatures/digital signatures are treated

as reliable records and signatures, and the rebuttal presumptions applicable to them.

Trusted Third Parties/Certification Authorities

28. Provisions governing the duties of trusted third parties (TTPs)/ certification authorities (CAs).

29. Provisions governing the duties between subscribers and their TTPs/CAs, including the issuance, management, suspension and revocation of digital certificates.

30. Provisions governing the regulation and licensing of TTPs/CAs, including the appointment of a controller of TTPs/CAs.

31. The following is not mandatory but is included in Singapore's ETA to define explicitly the rules governing the roles and responsibilities of service providers:

Service Providers

32. Provisions governing the extent of legal liability of service providers. Network service providers should be exempted from any criminal or civil liability for merely providing access to third-party online content over which they have no editorial control.

33. Details of the above provisions, including a comparison of the e-commerce laws of UNCITRAL, Singapore, Malaysia, Thailand, Philippines and Brunei, are given in the Annex.

VI Presumptions of e-Commerce Laws

34. These presumptions come into operation when the issues are not dealt with explicitly in the contract. They are meant to dispel uncertainty concerning the legal effect, transmission and receipt of electronic records[2].

There is no difference between electronic records and paper documents.
35. There should be no distinction in form between intangible electronic records and tangible paper documents. The form in which electronic records are presented or retained (e.g. utilising digital bits and bytes) cannot be used as the only reason to deny them legal effect, validity or enforceability.

An electronic record can replace a written document.
36. In the physical world, a written document has the status of being the cornerstone of reliability, traceability and inalterability of any transactions evidenced by that document. This is brought over into the virtual world where an electronic record satisfies any rule of law making provision for information to be written as long as the electronic record is accessible. To ensure that the record is accessible, the software required to make it accessible will also need to ensure it can be retained.

Parties can contract electronically.
37. There should be no ambiguity that an offer to contract and acceptance of that offer can be expressed electronically. Therefore, no party can attempt to evade his/her obligations by arguing that the transaction is invalid or is otherwise unforeseeable on the basis it was carried out electronically.

38. However, it is important to note that the provisions concerning electronic contracts:

a. Operate as a default rule i.e. it does not override any existing arrangement between the parties in relation to the way that a contract will be formed;

b. Do not automatically establish the validity of that electronic transaction. It merely provides that the electronic form of the transaction does not make it invalid (in this context, validity is intended to include legal effect and enforceability).

Electronic records are admissable as evidence in court.
39. In order to interpret the intention of the parties or a particular clause in a written contract evidencing the transaction between the parties, a court may refer to external evidence, e.g. correspondences or minutes of negotiations between parties. In this regard, e-commerce laws can ensure that e-mails or

[2] Extracted from Drew & Napier Your Guide to e-Commerce Law in Singapore

records stored electronically can be admitted as evidence of the parties' intentions as to the transaction between them.

If the electronic record is sent, the recipient is entitled to act on the record.

40. A recipient of an electronic record will be entitled to assume that the record was sent by the sender and to act on it if:

a. He/she has applied an agreed procedure to ascertain the authenticity of that record; or

b. The electronic record can be attributed to the actions of a person whose relationship with the sender would enable that person to access the sender's computer systems such that the record appears to the recipient to originate from the sender.

41. So where the parties have not agreed on any attribution rules for electronic communications, a person purporting to be the originator of an electronic record could only be bound to that record if in fact the record was sent by him or with his authority. This means that an e-merchant could, by the actions of his employee, be bound to a contract he may not be aware of, on account of his having provided his employee an e-mail address, which originates from his computer system.

42. However, his presumption is rebuttable, in that the recipient would not be entitled to rely on this presumption if it would be unreasonable for him to do so, e.g. the sender had already notified the recipient and the recipient had "reasonable time" to act accordingly (e.g. not to complete the transaction). The meaning of "reasonable time" would depend on the circumstances in each case, e.g. in the case of just-in time supply, the recipient should be notified before he adjusts his production process or activates the supply chain.

43. Further, if the recipient knew or could have discovered, had he exercised reasonable care that the electronic record did not originate from the sender, the recipient would not be entitled to rely on this presumption.

If the sending of an electronic record is conditional upon acknowledgement of receipt, the record is not sent until the acknowledgement has been received.

44. The sender can inform the recipient that sending of the e-mail is conditional upon receipt by means of that e-mail itself. If the sender has not indicated the method of acknowledgement, acknowledgement may be given by a method of communication or by conduct indicating that the e-mail has been received (e.g. sending the purchase order).

When a sender receives the recipient's acknowledgement of receipt, the electronic record is deemed received by the recipient.

45. If a sender receives an acknowledgement of receipt from the recipient, it is presumed, unless otherwise proved, that the record has been received by the recipient. This presumption, however, does not imply that the content of the electronic record corresponds to that which was sent. If any inconsistency exists between the text of the electronic record as sent and received, the text as received prevails, unless the recipient is not entitled to rely on presumption above.

46. This presumption merely clarifies when an acknowledgement of receipt occurs. It does not deal with the legal consequences that may flow either from the electronic record or from the acknowledgement of its receipt. It also does not deal with whether the record is useable or intelligible to the recipient.

An electronic record is sent when it enters a computer server/router outside the sender's control. An electronic record is received when it enters the addressee's computer/router.

47. There is a default rule to determine when an electronic record is sent and when it is received. This provision will only apply where such matters have not been agreed between the parties.

48. The time of dispatch of that electronic record will depend on whether or not the recipient has told the sender to send the record to a designated information system. If specified directions have been given and the electronic record is so transmitted, the record will be received when it enters the designated information system. In all other cases, the record will be received when it comes to the attention of the recipient.

An electronic record is sent from the sender's place of business and received at the recipient's place of business.

49. The distinction between this presumption and the one before is the issue of time and place of receipt. The presumption above determines time of dispatch and receipt, while this presumption determines place of dispatch and receipt of the electronic record.

50. The computer server may be located in a jurisdiction other than where the recipient is located. Nevertheless, the solution is to make the location of the computer server irrelevant and to replace it with an objective criterion, namely the party's place of business. Dispatch of an electronic record will be deemed to occur from the sender's place of business (or residence where there is no place of business). Similarly, receipt of that record will be deemed at the recipient's place of business. If a party has more than one place of business, the place of dispatch or receipt will be the place of business having the nearest connection with the underlying transaction.

VII Implementation of e-Commerce Laws

51. In this section, we highlight the differences in the implementation of e-commerce laws among ASEAN member states.

Electronic Transactions Legislation

52. Malaysia is the only one out of the five ASEAN member states with e-commerce laws that does not have a comprehensive electronic transactions legislation. It has chosen the path of enacting the DSA to take care of digital signatures, leaving the other components of electronic transactions to existing laws, including common law, instead.

Electronic Signatures/Digital Signatures

53. While the e-commerce laws of Singapore, Brunei, Thailand and Philippines have presumptions relating to electronic signatures, Malaysia's DSA pertains strictly to presumptions relating to digital signatures. In Malaysia's DSA, the digital signature must be "verified by reference to the public key listed in a valid certificate issued by a licensed certification authority". Singapore's ETA and Brunei's ETO also make distinction of **secure** electronic signatures, which must fulfil three requirements: (a) a prescribed security procedure, (b) a commercially reasonable security procedure agreed to by both transacting parties, and (c) must be verifiable as unique to a person, identify him/her and must have been "created through means that are under the full control of the signer"[3].

Licensing of CAs

54. Singapore has opted for a voluntary licensing scheme for CAs. This is because the Singapore government does not want to stifle the development and growth of the fledgling CA industry in Singapore by subjecting the CAs to the stringent regulations pertaining to licensees. This policy may be reviewed later when the CA industry matures.

55. Under Singapore's regime, a licensed CA enjoys three benefits compared to a non-licensed CA:

a. A licensed CA will enjoy the benefits of evidentiary presumption for digital signatures generated from the digital certificate it issues. Without such a presumption, a party that intends to rely on a digital signature must produce enough evidence to convince the court that the signature has been created under conditions that will render it trustworthy. With the presumption, the party relying on the digital signature merely has to show that the signature has been correctly verified, and the onus is on the other party disputing the signature to prove otherwise.

[3] Extracted from Tan Ken Hwee Breaking New Ground Asia Business Law Review No 23, Jan 1999

b. The liability of the CA will be limited under the ETA. The CA will not be liable for any loss caused by the reliance on a false or forged digital certificate of a subscriber so long as the CA has complied with the requirements under the ETA. If the licensed CA fails to observe some of its obligations, the CA will only be liable up to the reliance limit specified in the digital certificate.

c. The licensing of a CA by the Controller is an indication that the CA has met the stringent regulatory requirements established. It is an indication to the public that the CA is trustworthy and deserving of consumer confidence. Together with the ease of proof in using digital signatures, there can be greater reliance on such CAs.

56. Although Singapore's ETA does not require CAs to be licensed, it does impose a number of requirements on CAs without regard to whether they are licensed or not. For example, all CAs, licensed or unlicensed, must either issue a Certification Practice Statement or abide by the statutorily-prescribed requirements for issuing a digital certificate. Additionally, all CAs must comply with statutory standards for disclosing material information about a digital certificate and the procedures for revoking or suspending a certificate.

57. Brunei also has a voluntary licensing scheme. Thailand's regime is one of "voluntary unless otherwise directed". Malaysia, on the other hand, has implemented a "mandatory unless otherwise exempted" licensing scheme under its DSA. For Malaysian licensed CAs, they are also not liable for "punitive or exemplary damages", and "damages for pain or suffering".

Liability of Service Providers

58. As mentioned in an earlier section, Singapore's ETA has special provisions on the legal liabilities of service providers.

VIII Other Related Legislation

59. It should be noted that while e-commerce laws enable electronic transactions to take place with trust, confidence and certainty in cyberspace, they have to be complemented by other related legislation to ensure the interests of businesses and consumers are protected. Relevant legislation, regulations or codes of practice include:

a. Data privacy and protection
b. Consumer protection
c. Computer crimes/computer misuse
d. Copyright, trademarks, intellectual property rights
e. Admissibility of computer output as evidence in court
f. Internet code of practice
g. Advertising code of practice

60. Where these legislation, regulations or codes of practice are inadequate or inapplicable to cyberspace, they will have to be amended and updated.

IX Cross-Border Issues to be Addressed

61. In cross-border e-commerce, some of the issues that need to be addressed are:

a. Jurisdiction – Which court may hear and resolve the dispute between contracting parties from two different countries? Which law to use? Whether the court judgement obtained in one jurisdiction is enforceable in another jurisdiction?

b. Taxation – Where should the source(s) of income be if the electronic transaction occurs in multiple countries? Which tax regime should be used? Which jurisdiction should the taxes accrue to?

62. These issues are beyond the scope of this reference framework but are highlighted here for future studies.