A.M. No. 01-7-01-SC

RULES ON ELECTRONIC EVIDENCE

Acting on the Memorandum dated 18 June 2001 of the Committee on the Revision of the Rules of Court to Draft the Rules on E-Commerce Law [R.A. No. 8792] submitting the Rules on Electronic Evidence for this Court's consideration and approval, the Court Resolved to APPROVED the same.

The Rules on Electronic Evidence shall apply to cases pending after their effectivity. These Rules shall take effect on the first day of August 2001 following thier publication before the 20th of July in two newspapers of general circulation in the Philippines

17th July 2001.

RULES ON ELECTRONIC EVIDENCE

Rule 1

COVERAGE

Section 1. *Scope.* – Unless otherwise provided herein, these Rules shall apply whenever an electronic document or electronic data message, as defined in Rule 2 hereof, is offered or used in evidence.

Section 2. *Cases covered.* – These Rules shall apply to all civil actions and proceedings, as well as quasi-judicial and administrative cases.

Section 3. *Application of other rules on evidence.* – In all matters not specifically covered by these Rules, the Rules of Court and pertinent provisions of statutes containing rules on evidence shall apply.

Rule 2

DEFINITION OF TERMS AND CONSTRUCTION

Section 1. *Definition of terms.* – For purposes of these Rules, the following terms are defined, as follows:

(a) "Asymmetric or public cryptosystem" means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key for verifying the digital signature.

(b) "Business records" include records of any business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit, or for legitimate or illegitimate purposes.

(c) "Certificate" means an electronic document issued to support a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair.

(d) "Computer" refers to any single or interconnected device or apparatus, which, by electronic, electro-mechanical or magnetic impulse, or by other means with the same function, can receive, record, transmit, store, process, correlate, analyze, project, retrieve and/or produce information, data, text, graphics, figures, voice, video, symbols or other modes of expression or perform any one or more of these functions.

(e) "Digital signature" refers to an electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer's public key can accurately determine:

i. whether the transformation was created using the private key that corresponds to the signer's public key; and

ii. whether the initial electronic document had been altered after the transformation was made.

(f) "Digitally signed" refers to an electronic document or electronic data message bearing a digital signature verified by the public key listed in a certificate.

(g) "Electronic data message" refers to information generated, sent, received or stored by electronic, optical or similar means.

(h) "Electronic document" refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically. It includes digitally signed documents and any print-out or output, readable by sight or other means, which accurately reflects the electronic data message or electronic document. For purposes of these Rules, the term "electronic document" may be used interchangeably with "electronic data message".

(i) "Electronic key" refers to a secret code which secures and defends sensitive information that crosses over public channels into a form decipherable only with a matching electronic key.

(j) "Electronic signature" refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedure employed or adopted by a person and executed or adopted by such person with the intention of authenticating, signing or approving an electronic data message or electronic document. For purposes of these Rules, an electronic signature includes digital signatures.

(k) "Ephemeral electronic communication" refers to telephone conversations, text messages, chatroom sessions, streaming audio, streaming video, and other electronic forms of communication the evidence of which is not recorded or retained.

(l) "Information and communication system" refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar devices by or in which data are recorded or stored and any procedure related to the recording or storage of electronic data messages or electronic documents.

(m) "Key pair" in an asymmetric cryptosystem refers to the private key and its mathematically related public key such that the latter can verify the digital signature that the former creates.

(n) "Private key" refers to the key of a key pair used to create a digital signature.

(o) "Public key" refers to the key of a key pair used to verify a digital signature.

Section 2. *Construction.* – These Rules shall be liberally construed to assist the parties in obtaining a just, expeditious, and inexpensive determination of cases.

The interpretation of these Rules shall also take into consideration the international origin of Republic Act No. 8792, otherwise known as the Electronic Commerce Act.

Rule 3
ELECTRONIC DOCUMENTS

Section 1. *Electronic documents as functional equivalent of paper-based documents.* – Whenever a rule of evidence refers to the term writing, document, record, instrument, memorandum or any other form of writing, such term shall be deemed to include an electronic document as defined in these Rules.

Section 2. *Admissibility.* – An electronic document is admissible in evidence if it complies with the rules on admissibility prescribed by the Rules of Court and related laws and is authenticated in the manner prescribed by these Rules.

Section 3. *Privileged communication.* – The confidential character of a privileged communication is not lost solely on the ground that it is in the form of an electronic document.

Rule 4
BEST EVIDENCE RULE

Section 1. *Original of an electronic document.* – An electronic document shall be regarded as the equivalent of an original document under the Best Evidence Rule if it is a printout or output readable by sight or other means, shown to reflect the data accurately.

Section 2. *Copies as equivalent of the originals.* – When a document is in two or more copies executed at or about the same time with identical contents, or is a counterpart produced by the same impression as the original, or from the same matrix, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original, such copies or duplicates shall be regarded as the equivalent of the original.

Notwithstanding the foregoing, copies or duplicates shall not be admissible to the same extent as the original if:

(a) a genuine question is raised as to the authenticity of the original; or

(b) in the circumstances it would be unjust or inequitable to admit the copy in lieu of the original.

Rule 5
AUTHENTICATION OF ELECTRONIC DOCUMENTS

Section 1. *Burden of proving authenticity.* – The person seeking to introduce an electronic document in any legal proceeding has the burden of proving its authenticity in the manner provided in this Rule.

Section 2. *Manner of authentication.* – Before any private electronic document offered as authentic is received in evidence, its authenticity must be proved by any of the following means:

(a) by evidence that it had been digitally signed by the person purported to have signed the same;

(b) by evidence that other appropriate security procedures or devices as may be authorized by the Supreme Court or by law for authentication of electronic documents were applied to the document; or

(c) by other evidence showing its integrity and reliability to the satisfaction of the judge.

Section 3. Proof of electronically notarized document. – A document electronically notarized in accordance with the rules promulgated by the Supreme Court shall be considered as a public document and proved as a notarial document under the Rules of Court.

Rule 6
ELECTRONIC SIGNATURES

Section 1. *Electronic signature.* – An electronic signature or a digital signature authenticated in the manner prescribed hereunder is admissible in evidence as the functional equivalent of the signature of a person on a written document.

Section 2. *Authentication of electronic signatures.* – An electronic signature may be authenticated in any of the following manner:

(a) By evidence that a method or process was utilized to establish a digital signature and verify the same;

(b) By any other means provided by law; or

(c) By any other means satisfactory to the judge as establishing the genuineness of the electronic signature.

Section 3. *Disputable presumptions relating to electronic signatures.* – Upon the authentication of an electronic signature, it shall be presumed that:

(a) The electronic signature is that of the person to whom it correlates;

(b) The electronic signature was affixed by that person with the intention of authenticating or approving the electronic document to which it is related or to indicate such person's consent to the transaction embodied therein; and

(c) The methods or processes utilized to affix or verify the electronic signature operated without error or fault.

Section 4. *Disputable presumptions relating to digital signatures.* – Upon the authentication of a digital signature, it shall be presumed, in addition to those mentioned in the immediately preceding section, that:

(a) The information contained in a certificate is correct;

(b) The digital signature was created during the operational period of a certificate;

(c) No cause exists to render a certificate invalid or revocable;

(d) The message associated with a digital signature has not been altered from the time it was signed; and,

(e) A certificate had been issued by the certification authority indicated therein.

Rule 7
EVIDENTIARY WEIGHT OF ELECTRONIC DOCUMENTS

Section 1. *Factors for assessing evidentiary weight.* – In assessing the evidentiary weight of an electronic document, the following factors may be considered:

(a) The reliability of the manner or method in which it was generated, stored or communicated, including but not limited to input and output procedures, controls, tests and checks for accuracy and reliability of the electronic data message or document, in the light of all the circumstances as well as any relevant agreement;

(b) The reliability of the manner in which its originator was identified;

(c) The integrity of the information and communication system in which it is recorded or stored, including but not limited to the hardware and computer programs or software used as well as programming errors;

(d) The familiarity of the witness or the person who made the entry with the communication and information system;

(e) The nature and quality of the information which went into the communication and information system upon which the electronic data message or electronic document was based; or

(f) Other factors which the court may consider as affecting the accuracy or integrity of the electronic document or electronic data message.

Section 2. *Integrity of an information and communication system.* – In any dispute involving the integrity of the information and communication system in which an electronic document or electronic data message is recorded or stored, the court may consider, among others, the following factors:

(a) Whether the information and communication system or other similar device was operated in a manner that did not affect the integrity of the electronic document, and there are no other reasonable grounds to doubt the integrity of the information and communication system;

(b) Whether the electronic document was recorded or stored by a party to the proceedings with interest adverse to that of the party using it; or

(c) Whether the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not act under the control of the party using it.

Rule 8
BUSINESS RECORDS AS EXCEPTION TO THE HEARSAY RULE

Section 1. *Inapplicability of the hearsay rule.* – A memorandum, report, record or data compilation of acts, events, conditions, opinions, or diagnoses, made by electronic, optical or other similar means at or near the time of or from transmission or supply of information by a person with knowledge thereof, and kept in the regular course or conduct of a business activity, and such was the regular practice to make the memorandum, report, record, or data compilation by electronic, optical or similar means, all of which are shown by the testimony of the custodian or other qualified witnesses, is excepted from the rule on hearsay evidence.

Section 2. *Overcoming the presumption.* – The presumption provided for in Section 1 of this Rule may be overcome by evidence of the untrustworthiness of the source of information or the method or circumstances of the preparation, transmission or storage thereof.

Rule 9
METHOD OF PROOF

Section 1. *Affidavit evidence.* – All matters relating to the admissibility and evidentiary weight of an electronic document may be established by an affidavit stating facts of direct personal knowledge of the affiant or based on authentic records. The affidavit must affirmatively show the competence of the affiant to testify on the matters contained therein.

Section 2. *Cross-examination of deponent.* – The affiant shall be made to affirm the contents of the affidavit in open court and may be cross-examined as a matter of right by the adverse party.

Rule 10
EXAMINATION OF WITNESSES

Section 1. *Electronic testimony.* – After summarily hearing the parties pursuant to Rule 9 of these Rules, the court may authorize the presentation of testimonial evidence by electronic means. Before so authorizing, the court shall determine the necessity for such presentation and prescribe terms and conditions as may be necessary under the circumstances, including the protection of the rights of the parties and witnesses concerned.

Section 2. *Transcript of electronic testimony.* – When examination of a witness is done electronically, the entire proceedings, including the questions and answers, shall be transcribed by a stenographer, stenotypist or other recorder authorized for the purpose, who shall certify as correct the transcript done by him. The transcript should reflect the fact that the proceedings, either in whole or in part, had been electronically recorded.

Section 3. *Storage of electronic evidence.* – The electronic evidence and recording thereof as well as the stenographic notes shall form part of the record of the case. Such transcript and recording shall be deemed prima facie evidence of such proceedings.

Rule 11
AUDIO, PHOTOGRAPHIC, VIDEO, AND EPHEMERAL EVIDENCE

Section 1. *Audio, video and similar evidence.* – Audio, photographic and video evidence of events, acts or transactions shall be admissible provided it shall be shown, presented or displayed to the court and shall be identified, explained or authenticated by the person who made the recording or by some other person competent to testify on the accuracy thereof.

Section 2. *Ephemeral electronic communications.* – Ephemeral electronic communications shall be proven by the testimony of a person who was a party to the same or has personal knowledge thereof. In the absence or unavailability of such witnesses, other competent evidence may be admitted.

A recording of the telephone conversation or ephemeral electronic communication shall be covered by the immediately preceding section.

If the foregoing communications are recorded or embodied in an electronic document, then the provisions of Rule 5 shall apply.

Rule 12
EFFECTIVITY

Section 1. *Applicability to pending cases.* – These Rules shall apply to cases pending after their effectivity.

Section 2. *Effectivity.* – These Rules shall take effect on the first day of August 2001 following their publication before the 20th of July 2001 in two newspapers of general circulation in the Philippines.