The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the Drafting Committee. They do not necessarily reflect the views of the Conference and its Commissioners and the Drafting Committee and its Members and Reporters. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.

DRAFTING COMMITTEE ON
UNIFORM ELECTRONIC TRANSACTIONS ACT

PATRICIA BRUMFIELD FRY, University of North Dakota, School of Law, P.O. Box 9003, Grand Forks, ND  58201, Chair
STEPHEN Y. CHOW, One Beacon Street, 30th Floor, Boston, MA  02108
KENNETH W. ELLIOTT, Suite 630, 119 N. Robinson Avenue, Oklahoma City, OK  73102
HENRY DEEB GABRIEL, JR., Loyola University, School of Law, 526 Pine Street, New Orleans, LA  70118
BION M. GREGORY, Office of Legislative Counsel, State Capitol, Suite 3021, Sacramento, CA 95814-4996
JOSEPH P. MAZUREK, Office of Attorney General, P.O. Box 201401, 215 N. Sanders, Helena, MT  59620
PAMELA MEADE SARGENT, P.O. Box 846, Abingdon, VA  24212
D. BENJAMIN BEARD, University of Idaho, School of Law, 6th and Rayburn Streets, Moscow, ID  83844-2321, Reporter

EX OFFICIO

GENE N. LEBRUN, P.O. Box 8250, 9th Floor, 909 St. Joseph Street, Rapid City, SD  57709, President
HENRY M. KITTLESON, P.O. Box 32092, 92 Lake Wire Drive, Lakeland, FL  33802-2092, Division Chair

AMERICAN BAR ASSOCIATION ADVISORS

C. ROBERT BEATTIE, 150 S. 5th Street, Suite 3500, Minneapolis, MN  55402, Business Law Section
AMELIA H. BOSS, Temple University, School of Law, 1719 N. Broad Street, Philadelphia, PA 19122, Advisor
THOMAS J. SMEDINGHOFF, 500 W. Madison Street, 40th Floor, Chicago, IL  60661-2511, Science and Technology Section

EXECUTIVE DIRECTOR

FRED H. MILLER, University of Oklahoma, College of Law, 300 Timberdell Road, Norman, OK  73019, Executive Director
WILLIAM J. PIERCE, 1505 Roxbury Road, Ann Arbor, MI  48104, Executive Director Emeritus

Copies of this Act may be obtained from:
NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS
211 E. Ontario Street, Suite 1300
Chicago, Illinois  60611
312/915-0195
# TABLE OF DISPOSITION OF SECTIONS IN SEPTEMBER 18, 1998 DRAFT

<table>
<thead>
<tr>
<th>September 18, 1998 Draft Section</th>
<th>January 25, 1999 Draft Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>101.</td>
<td>.101</td>
</tr>
<tr>
<td>102.</td>
<td>.102</td>
</tr>
<tr>
<td>103.(a)</td>
<td>.103(a)</td>
</tr>
<tr>
<td>104(a).</td>
<td>.103(b)</td>
</tr>
<tr>
<td>104(b).</td>
<td>.103(c)</td>
</tr>
<tr>
<td>104(c).</td>
<td>.103(b)(7)</td>
</tr>
<tr>
<td>104(d).</td>
<td>.108</td>
</tr>
<tr>
<td>104(e).</td>
<td>.103(d)</td>
</tr>
<tr>
<td>105.</td>
<td>.104</td>
</tr>
<tr>
<td>106.</td>
<td>.105</td>
</tr>
<tr>
<td>107.</td>
<td>.Deleted</td>
</tr>
<tr>
<td>108.</td>
<td>.Deleted</td>
</tr>
<tr>
<td>109.</td>
<td>.Deleted</td>
</tr>
<tr>
<td>110.</td>
<td>.107</td>
</tr>
<tr>
<td>201(a).</td>
<td>.106(a)</td>
</tr>
<tr>
<td>201(b).</td>
<td>.106(c)</td>
</tr>
<tr>
<td>201(c).</td>
<td>.106(e)</td>
</tr>
<tr>
<td>202.</td>
<td>.109</td>
</tr>
<tr>
<td>203.</td>
<td>.110</td>
</tr>
<tr>
<td>204.</td>
<td>.116(a and d)</td>
</tr>
<tr>
<td>205(a).</td>
<td>.113(a and e)</td>
</tr>
<tr>
<td>205(b).</td>
<td>.Deleted</td>
</tr>
<tr>
<td>206.</td>
<td>.113(b, c, d, and f)</td>
</tr>
<tr>
<td>301(a).</td>
<td>.106(a)</td>
</tr>
<tr>
<td>301(b).</td>
<td>.106(d)</td>
</tr>
<tr>
<td>301(c).</td>
<td>.106(e)</td>
</tr>
<tr>
<td>302.</td>
<td>.111(a and c)</td>
</tr>
<tr>
<td>303(a).</td>
<td>.116(b)</td>
</tr>
<tr>
<td>303(b).</td>
<td>.111(b)</td>
</tr>
<tr>
<td>304.</td>
<td>.112</td>
</tr>
<tr>
<td>401(a).</td>
<td>.116(c)</td>
</tr>
<tr>
<td>401(b).</td>
<td>.115</td>
</tr>
<tr>
<td>401(c).</td>
<td>.106(b)</td>
</tr>
<tr>
<td>402.</td>
<td>.117(a-e)</td>
</tr>
<tr>
<td>403(a).</td>
<td>.Deleted</td>
</tr>
<tr>
<td>403(b).</td>
<td>.117(f)</td>
</tr>
<tr>
<td>404.</td>
<td>.114</td>
</tr>
<tr>
<td>405.</td>
<td>.118</td>
</tr>
<tr>
<td>501.</td>
<td>.201</td>
</tr>
<tr>
<td>502.</td>
<td>.202</td>
</tr>
<tr>
<td>503.</td>
<td>.Deleted</td>
</tr>
<tr>
<td>504.</td>
<td>.203</td>
</tr>
</tbody>
</table>
## UNIFORM ELECTRONIC TRANSACTIONS ACT

### TABLE OF CONTENTS

### PART 1

**GENERAL PROVISIONS**

**NON-GOVERNMENTAL RECORDS AND SIGNATURES**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>SHORT TITLE.</td>
</tr>
<tr>
<td>102</td>
<td>DEFINITIONS.</td>
</tr>
<tr>
<td>103</td>
<td>SCOPE.</td>
</tr>
<tr>
<td>104</td>
<td>SCOPE—EXCLUSIONS AND LIMITATIONS.</td>
</tr>
<tr>
<td>105</td>
<td>VARIATION BY AGREEMENT.</td>
</tr>
<tr>
<td>106</td>
<td>APPLICATION AND CONSTRUCTION.</td>
</tr>
<tr>
<td>107</td>
<td>MANIFESTING ASSENT.</td>
</tr>
<tr>
<td>108</td>
<td>OPPORTUNITY TO REVIEW.</td>
</tr>
<tr>
<td>109</td>
<td>DETERMINATION OF REASONABLE SECURITY PROCEDURE.</td>
</tr>
<tr>
<td>110</td>
<td>LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES AND ELECTRONIC CONTRACTS.</td>
</tr>
<tr>
<td>111</td>
<td>EFFECT OF REQUIRING UNREASONABLE SECURITY PROCEDURE.</td>
</tr>
<tr>
<td>112</td>
<td>PROVISION OF INFORMATION IN WRITING.</td>
</tr>
</tbody>
</table>

### PART 2

**ELECTRONIC RECORDS**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>202</td>
<td>ATTRIBUTION OF ELECTRONIC RECORD TO PARTY.</td>
</tr>
<tr>
<td>203</td>
<td>DETECTION OF CHANGES AND ERRORS.</td>
</tr>
<tr>
<td>204</td>
<td>INADVERTENT ERROR.</td>
</tr>
<tr>
<td>205</td>
<td>EFFECT OF ELECTRONIC SIGNATURES.</td>
</tr>
<tr>
<td>206</td>
<td>OPERATIONS OF ELECTRONIC DEVICES.</td>
</tr>
<tr>
<td>207</td>
<td>NOTARIZATION AND ACKNOWLEDGMENT.</td>
</tr>
<tr>
<td>208</td>
<td>ORIGINALS—INFORMATION ACCURACY.</td>
</tr>
<tr>
<td>209</td>
<td>RETENTION OF ELECTRONIC RECORDS; ORIGINALS.</td>
</tr>
<tr>
<td>210</td>
<td>ADMISSIBILITY INTO EVIDENCE.</td>
</tr>
<tr>
<td>211</td>
<td>FORMATION OF CONTRACT AND VALIDITY.</td>
</tr>
<tr>
<td>212</td>
<td>OPERATIONS OF ELECTRONIC AGENT; AUTOMATED TRANSACTIONS.</td>
</tr>
<tr>
<td>213</td>
<td>TIME AND PLACE OF SENDING AND RECEIPT.</td>
</tr>
<tr>
<td>214</td>
<td>ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.</td>
</tr>
<tr>
<td>215</td>
<td>CONTROL OF TRANSFERABLE RECORDS.</td>
</tr>
</tbody>
</table>
PART 3

ELECTRONIC SIGNATURES

SECTION 301. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES.
SECTION 302. EFFECT OF ELECTRONIC SIGNATURES.
SECTION 303. OPERATIONS OF ELECTRONIC DEVICES.
SECTION 304. NOTARIZATION AND ACKNOWLEDGMENT.

PART 4

ELECTRONIC CONTRACTS AND COMMUNICATIONS

SECTION 401. FORMATION AND VALIDITY.
SECTION 402. TIME AND PLACE OF SENDING AND RECEIPT.
SECTION 403. ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.
SECTION 404. ADMISSIBILITY INTO EVIDENCE.
SECTION 405. TRANSFERABLE RECORDS.

PART 5

GOVERNMENTAL ELECTRONIC RECORDS

SECTION 501. CREATION AND RETENTION OF ELECTRONIC RECORDS AND CONVERSION OF WRITTEN RECORDS BY GOVERNMENTAL AGENCIES.
SECTION 502. RECEIPT AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.
SECTION 503. [DESIGNATED STATE OFFICER] TO ADOPT STATE STANDARDS.
SECTION 504. INTEROPERABILITY.

PART 6

MISCELLANEOUS PROVISIONS

SECTION 601. SEVERABILITY.
SECTION 602. EFFECTIVE DATE.
SECTION 603. SAVINGS AND TRANSITIONAL PROVISIONS.
PART 1

GENERAL PROVISIONS

SECTION 101. SHORT TITLE. This [Act] may be cited as the Uniform Electronic Transactions Act.

SECTION 102. DEFINITIONS.

(a) In this [Act] [unless the context otherwise requires]:

(1) "Agreement" means the bargain of the parties in fact as found in their language or inferred from other circumstances, and rules, regulations, and procedures given the effect of agreements under rules of law otherwise applicable to a particular transaction. [Whether an agreement has legal consequences is determined by this [Act], if applicable, or otherwise by other applicable rules of law.]

(2) "Automated transaction" means a transaction formed or performed, in whole or in part, by electronic means or electronic records in which the acts or records of one or both parties are not reviewed by an individual as an ordinary step course in forming a contract, performing under an existing contract, or fulfilling any obligation required by the transaction.

(3) "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result. The term does not include informational content.

(4) “Consumer” means an individual involved in a transaction primarily for personal, family, or household purposes.
(5) “Consumer transaction” means a transaction in which a consumer is involved.

(46) "Contract" means the total legal obligation resulting from the parties' agreement as affected by this [Act] and other applicable rules of law.

(57) "Electronic" means of or relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(68) "Electronic agent device" means a computer program, or other electronic, or other automated means configured and enabled by a person used to initiate or respond to electronic records or performances in whole or in part without review by an individual.

(79) "Electronic record" means a record created, stored, generated, received, or communicated by electronic means.

(810) "Electronic signature" means a signature in electronic form, attached to or logically associated with an electronic record.

(911) "Governmental agency" means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a state or of any county, municipality, or other political subdivision of a state.

(1012) "Information" means data, text, images, sounds, codes, computer programs, software, databases, or the like.
"Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or otherwise processing information.

"Informational content" means information that in its ordinary use is intended to be communicated to or perceived by a person in the ordinary use of the information.

"Notify" means to communicate, or make available, information to another person in a form and manner appropriate or required under the circumstances.

“Organization” means a person other than an individual.

"Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, two or more persons having a joint or common interest, governmental agency, government, governmental subdivision, agency, instrumentality, or public corporation, or any other legal or commercial entity.

"Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

"Rule of law" means a statute, regulation, ordinance, common-law rule, court decision, or other law enacted, established, or promulgated by in this State, or by any governmental agency, commission, department, court, or other authority or political subdivision of this State.
(18) "Security procedure," means a procedure or method, [established by law or agreement, or knowingly adopted by each party,] employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the informational content of an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, callback or other acknowledgment procedures; or any other procedures that are reasonable under the circumstances.

(19) "Sign" means to execute or adopt a signature.

(20) "Signature" means an identifying symbol, sound, or process; or encryption of a record in whole or in part, that is attached to or associated with a record and executed or adopted by a person to associate the person with the record, as part of a record.

(21) "Term" means that portion of an agreement which relates to a particular matter.

(22) "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business or governmental affairs. taken by a person which relate to or involve another person or persons.

(23) "Transferable record" means a record, other than a writing, that would be a note under [Article 3 of the Uniform Commercial Code], an instrument or chattel paper under [Article 9 of the Uniform Commercial Code], or a document of title under [Article 1 of the Uniform Commercial Code], if the record were in writing.
(263) "Writing" includes printing, typewriting, and any other intentional
reduction of a record to tangible form. "Written" has a corresponding meaning.

(b) Other definitions applying to this [Act] or to specified sections thereof, and the
sections in which they appear are:

"Inadvertent error". Section 204
"Requiring party". Section 110

Sources: Definitions in this Act have been derived from Uniform Commercial Code
definitions, Article 2B drafts, and from other models, specifically the UNCITRAL Model
Law, Illinois Model, Oklahoma Model and Massachusetts Model.

Reporter’s Note: The qualification to the introductory clause has been deleted based on
comments from the Committee on Style that it is unnecessary and creates ambiguity.

1. "Agreement"

Committee Votes:
1. To delete the concept of manifestation of assent from the definition - By
   consensus (no formal vote) (Sept. 1997)
2. To delete course of performance, course of dealing and usage of trade: Committee
   4 Yes - 2 No; Observers 6 Yes - 1 No. (Jan. 1998)

Revised to conform to language in Article 2B.
At the September, 1997 Meeting the definition of agreement which included terms to
which a party manifested assent was rejected. The consensus of both the Committee and
observers was that there was no need to separate manifestations of assent from the
language and circumstances which comprise the bargain in fact of the parties as part of
the definition of agreement. Rather the Reporter was directed to return to the definition
of agreement in the Uniform Commercial Code. Accordingly, the definition in the
November, 1997 Draft was taken from the most recent revision to Article 1.

At the January, 1998 Meeting, the Committee more specifically defined the policy
guiding this Act: the Act is a procedural act providing for the means to effectuate
transactions accomplished via an electronic medium, and, unless absolutely necessary
because of the unique circumstances of the electronic medium, the Act should leave all
questions of substantive law to law outside this Act. In light of this principle the prior
references to usage evidence as informing the content of an agreement was considered
substantive, and therefore, best left to other law outside this Act.

The need for a definition of agreement arises because the existence of a security
procedure often depends on the agreement of the parties. However, the facts and
evidence which establish an agreement are left to other law, e.g., the Uniform Commercial Code, common law, etc.

Whether the parties have reached an agreement is determined by their express language and surrounding circumstances. The Restatement of Contracts §3 provides that "An agreement is a manifestation of mutual assent on the part of two or more persons. A bargain is an agreement to exchange promises or to exchange a promise for a performance or to exchange performances."

The Uniform Commercial Code specifically includes in the circumstances from which an agreement may be inferred "course of performance, course of dealing and usage of trade..." as defined in the UCC.

The provisions in the last clause of the first sentence are intended to include circumstances where the law deems agreements to exist as a matter of a rule, regulation or otherwise. For example, Article 4 (Section 4-103(b)) provides that Federal Reserve regulations and operating circulars and clearinghouse rules have the effect of agreements. Such agreements by law are properly included in the definition in this Act.

The existence and content of an agreement under this Act are determined by the parties' language and surrounding circumstances. The relevant surrounding circumstances and the context of the transaction will inform the precise terms of any agreement. The second sentence of this definition makes clear that the substantive law applicable to an electronic transaction effectuated by this Act must be applied to determine those circumstances relevant in establishing the precise scope and meaning of the parties' agreement. THE STYLE COMMITTEE VIEWS THE PROVISION AS SUBSTANTIVE AND CONTENDS THAT IT SHOULD NOT BE INCLUDED IN THE DEFINITION. Considering the source of this provision is the UCC, which has a 40-50 year history of construction, THE PROVISION HAS BEEN RETAINED FOR DISCUSSION BY THE DRAFTING COMMITTEE AT ITS NEXT MEETING.

The comment to this definition will make clear that, though derived from the UCC definition, there is no intent to affect the meaning of the term under the UCC or any other applicable law.

2. "Automated Transaction."

Committee Vote: To delete references to governmental and commercial: Committee 4 Yes (Chair broke tie) - 3 No; Observers 19 Yes - 1 No. (Jan. 1998)

Article 2B has conformed its terminology with this Act by adopting "automated transaction" in place of "electronic transaction." The definitions in each are conceptually the same. The definition in this Act is broader, going beyond contract formation to performances under a contract and other obligations accomplished by electronic means in a transaction, because of the diversity of transactions to which this Act may apply.

As with electronic agents, this definition addresses the circumstance where electronic records may result in action or performance by a party although no human review of the electronic records is anticipated. Section 116 provides specific contract formation rules where one or both parties do not review the electronic records.
3. "Computer program." This definition is derived from Article 2B. The term is used principally with respect to the definition of "electronic agent" and "information."

4. “Consumer.” This definition has been added in order to provide a means to limit the effect of Sections 107 and 108, should the Drafting Committee so choose.

5. “Consumer transaction.” This definition has been added in order to provide a means to limit the effect of Sections 107 and 108, should the Drafting Committee so choose.

6. "Electronic." This definition serves to assure that the Act will be applied broadly as new technologies develop. While not all technologies listed are technically "electronic" in nature (e.g., optical fiber technology), the need for a recognized, single term warrants the use of "electronic" as the defined term.

7. "Electronic agent." This Act used the term "electronic device" (rather than “electronic agent” used in Article 2B) in order to avoid connotations of agency. However, in Article 2B and in other contexts the term “electronic agent” has come to be recognized as a near term of art. The term “electronic device” has not been widely hailed as a significant improvement. Accordingly, the Chair and Reporter of UETA agreed in the coordination meeting to adopt “electronic agent” in order to be consistent with Article 2B. (Article 2B will adopt the language in the definition and the only point of difference will be the phrase “in whole or in part” after the word “performances” which will not be included in Article 2B.) Comments made at UETA Drafting Committee meetings from members of the Committee and observers highlight that the key aspect of this term is its function as a tool of a party. As the term “electronic agent” has come to be recognized, it is limited to the tool function.

   The definition has been revised to reflect comments that, for purposes of the definition, it is irrelevant who employs the agent. Rather the definition establishes that an electronic agent is a machine. The effect on the party using the agent is addressed in the operative provisions of the Act (e.g., Section 116(b))

   An electronic agent, such as a computer program or other automated means employed by a person, is a tool of that person. As a general rule, the employer of a tool is responsible for the results obtained by the use of that tool since the tool has no independent volition of its own. However, an electronic agent by definition is capable, within the parameters of its programming, of initiating, responding or interacting with other parties or their electronic agents once it has been activated by a party, without further attention of that party. This Act (Section 116(b)) provides that a person is responsible for actions taken and accomplished through electronic agents in the absence of human intervention.

   While this Act proceeds on the paradigm that an electronic agent is capable of performing only within the technical strictures of its preset programming, it is conceivable that, within the useful life of this Act, electronic agents may be created with the ability to act autonomously, and not just automatically. That is, through developments in artificial intelligence, a computer may be able to "learn through
experience, modify the instructions in their own programs, and even devise new
25 (Winter, 1996). If such developments occur, courts may construe the definition of
electronic agent accordingly, in order to recognize such new capabilities.

8. "Electronic record." An electronic record is a subset of the broader defined term
"record." Unlike the term "electronic message" used in Article 2B, the definition is not
limited to records intended for communication, but extends to any information contained
or transferred in an electronic medium. It is also used in this Act as a limiting definition
in those provisions in which it is used.

Electronic means for creating, storing, generating, receiving or communicating
electronic records include information processing systems, computer equipment and
programs, electronic data interchange, electronic mail, or voice mail, facsimile, telex,
telecopying, scanning, and similar technologies.

9. "Electronic signature." As with electronic record, this definition is a subset of the
broader defined term "signature." The purpose of the separate definition is principally one
of clarity in extending the definition of signature to the electronic environment.

The key aspect of this definition lies in the necessity that the electronic signature
be linked or logically associated with the electronic record. For example, in the paper
world, it is assumed that the symbol adopted by a party is attached to or located
somewhere in the same paper that is intended to be authenticated. These tangible
manifestations do not exist in the electronic environment, and accordingly, this definition
expressly provides that the symbol must in some way be linked to, or associated with, the
electronic record being signed. This linkage is consistent with the regulations
promulgated by the Food and Drug Administration. 21 CFR Part 11 (March 20, 1997).

A digital signature using public key encryption technology would qualify as an
electronic signature, as would the mere appellation of one's name at the end of an e-mail
message - so long as in each case the signer executed or adopted the symbol and it
identified the signer.

10. "Governmental agency."
Committee Vote: To include legislative and judicial agencies - 3 Yea - 0 Nay (October,
1998)
This definition is important in the context of Part 2. The reference to legislative and
judicial agencies has been included per the vote of the Committee in Rapid City. The
definition has also been expanded to be a generic description unrelated to any particular
State. This was necessitated by the use of the term in Section 203 on Interoperability.
Where governmental agencies of the enacting state are relevant this has been clarified in
the operative provisions.

11. "Information processing system." This term is used in Section118 regarding the
time and place of receipt of an electronic record. It has been revised to conform with
Article 2B.
12. "Informational Content." This definition has been added to differentiate information in an electronic record, which includes all data forming part of an electronic record, with the informational content of an electronic record which is the portion of the electronic record intended actually to be used by a human being. An example from Article 2B establishing this distinction is the Westlaw user who uses the search program to retrieve a case. The search program would be information, but only the case retrieved would be informational content. It has been revised to conform with Article 2B.

13. "Notify." This definition has been deleted since there are no longer any references in the Act.

14. “Organization.” This definition has been deleted since there are no longer any references in the Act.

15. “Person.” This definition has been clarified by incorporating the definition of governmental agency.

16. "Record." This is the standard Conference formulation for this definition.

17. "Rule of Law." The definition is drafted broadly. IT HAS BEEN BRACKETED IN RECOGNITION OF THE STYLE COMMITTEE’S RECOMMENDATION THAT IT BE DELETED AND THE UNDEFINED TERM "LAW" BE SUBSTITUTED. IT HAS BEEN RETAINED FOR DRAFTING COMMITTEE CONSIDERATION.

The only provision in the Act addressing the effect of security procedures in a given transaction is Section 107.

The key aspects of a security procedure include verification of an electronic signature in addition to verification of the identity of the sender, and assurance of the informational integrity, of an electronic record. The definition does not identify any particular technology. This permits the use of procedures which the parties select or which are established by law. It permits the greatest flexibility among the parties and allows for future technological development.

18. "Security procedure." It was suggested at the Annual Meeting that the way in which a security procedure becomes applicable should be referenced in the substantive rule and not set forth as part of the definition. Accordingly, this clause has been deleted and the definition revised for clarity and to more closely parallel Article 2B.

The only provision in the Act addressing the effect of security procedures in a given transaction is Section 107.

19. Signature." As part of the coordination meeting regarding Article 2B, the differences between the definition of authentication in 2B (and revised Article 9) and UETA were noted. It was suggested that the UETA consider adopting a definition of “signature” which deferred to the applicable definition of signature provided by the substantive law applicable to a given transaction or in the alternative, that UETA not define the term. THIS IDEA IS NOTED FOR CONSIDERATION BY THE COMMITTEE.
At the September, 1997 Drafting Meeting, the consensus of the Committee and observers was to go back to the definition of signature, and to delete the definition of "authenticate." Given the purpose of this Act to equate electronic signatures with written signatures, the sense was that retaining signature as the operative word would better accomplish that purpose. However, the idea of fleshing out the concept of authenticate present in the existing UCC definition of signature was thought to be wise. Therefore, the definitional concepts set forth in the definition of authenticate in Article 2B were carried into the definition of signature.

At the April 1998 meeting a good deal of discussion related to the propriety of delineating the specific functions of a signature. The Committee deleted from former Section 302 a provision establishing the specific effects of an electronic signature. The one critical aspect of a signature that was recognized was its purpose of identifying a person. Accordingly, the definition has been revised to reflect the principal function of a signature as an identifying mark. In addition, some volition must attach to application of a mark and this is noted by the requirement that the mark be "executed or adopted" by a person. This draft also requires that the mark, etc, be executed or adopted for the purpose of associating the person with the record, in order to distinguish a signature from a mere autograph.

At the Annual Meeting it was suggested that an unrecorded statement over the phone might qualify as a signature under this broadened definition. In order to address this concern the definition now indicates that the symbol or sound must be attached to or associated with the record. The effect of the signature is left to the underlying substantive law in light of the facts and circumstances. See Section 111. In short, the definition here reflects the bare minimum as to the function of a signature, with the substantive effect being treated in Section 111 and the substantive law underlying the transaction.

20. "Term." This definition has been deleted since it is not used in the Act in any way requiring definition.

21. “Transaction.” This definition has been revised for clarity and specificity in light of comments made at the October, 1998 meeting that it was too broad. Accordingly, it is now limited to actions between people taken in the context of commercial or governmental activities.

22. "Transferable record." This definition is necessary in the event the Drafting Committee decides to retain Section 118. It has been revised to limit its applicability solely to promissory notes under Article 3, consistent with the exclusion of “orders” from the scope of the Act.

23. "Writing." This definition reflects the current UCC definition.
SECTION 103. SCOPE. (a) Except as otherwise provided in subsection (b), this [Act] applies to electronic records and electronic signatures that relate to any transaction.

SECTION 104. SCOPE—EXCLUSIONS AND LIMITATIONS.

(b a) This [Act] does not apply to electronic records and electronic signatures related to a transaction to the extent that the transaction is governed by:

1. a rules of law governing the creation and execution of wills and codicils;

2. a rules of law governing the creation and execution of personal testamentary trusts created and executed in connection with wills and codicils;

3. [Articles 4, 5, and 8 of the Uniform Commercial Code];

4. [Article 4A of the Uniform Commercial Code except that the requirement of a written agreement in the following sections may be satisfied with electronic records and signatures:....]

5. a rules of law governing the issuance, transfer, negotiation, or enforcement of orders as defined in [Article 3 of the Uniform Commercial Code];

6. a rule of law which expressly authorizes the use of other than written records or manual signatures in satisfaction of the rule provides for the method and manner under which electronic records and electronic signatures may be used in satisfaction of the rule;
(47) Other transactions identified by ETA Task Force on excluded transactions;

(8) other transactions, if any, identified by State; and

(§ 9) Transactions specifically excluded by any governmental agency of this State under Part 25.

(c) In a statute, rule, or regulation containing a rule of law described in subparagraph (a)(36), any express requirement elsewhere in that statute, rule, or regulation that a record be in writing shall not be affected by this Act if the court determines that application of this Act would be contrary to the purpose of the requirement.

(d) Except as otherwise specifically provided in Subsection (d), this Act does not apply to a provision in a requirement in a rule of law relating to a specific mode of delivery or display of information.

(d) If a rule of law requires a person to provide information in writing to another person that requirement is satisfied if the information is provided in an electronic record which is

(1) provided in an electronic record which is under the control of the person to which it is provided; and

(2) capable of retention for subsequent reference. [Substance moved to section 108]

(e) A transaction subject to this Act is also subject to other applicable substantive rules of law, which substantive rules of law must be construed
whenever reasonable as consistent with this [Act]. If such a construction is unreasonable, the substantive rule of law governs.

**Source:** UETA Sections 103 and 104 (Sept., 1998 Draft); Section 103 of Revised Draft of Article 1.

**Committee Votes:**
1. In former Section 103:
   a. To delete references to commercial and governmental transactions - Committee 4 Yes - 3 No (Chair broke tie) Observers 19 Yes - 1 No (Jan. 1998).
   b. To incorporate supplemental principles as part of Scope section - Committee Yes Unanimous Observers 12 Yes - 0 No (Jan. 1998).
   c. To delete reference to supplemental principles (April 1998)
2. In former Section 104 to delete "repugnancy" language, and provide that Act will apply except for specific exclusions. Committee 4 Yes - 1 No Observers 14 Yes - 1 No (with a number of abstentions) (Jan. 1998)

**Reporter's Note to This Draft:**
1. Former Sections 103 and 104 have been combined into a single scope section per comments of the Style Committee. Subsection (b) has been revised to make the scope and exclusion provisions parallel in applicability to electronic records and electronic signatures related to transactions.
2. The language in subsection (b)(2) has been revised for clarity. Use of the term "testamentary trusts" is a known term of art.
3. The relationship of this Act to the Uniform Commercial Code remains, perhaps, the most difficult question of scope. In the course of the revision projects of the last decade developments with electronic media have been considered to a greater or lesser degree in each of the revised Articles. The revisions of Articles 5 and 8 provide for significant media neutrality and should not be affected by this Act.

   Article 4A could be wholly excluded, with minimal effect. However, the level of consideration of electronic media throughout the entire statute was not as thorough as with Article 5 and Article 8. For example, the provisions for agreements regarding commercially unreasonable security procedures must be in writing, and it is not clear that such agreements could not as well be accomplished electronically. Determining which sections are to be included within UETA will require care. The Reporter will prepare such exceptions for the April meeting of the Committee, if the Committee determines that this is the appropriate method for addressing Article 4A.

   Although Article 4 specifically authorized electronic presentment and check truncation, the check collection system remains predominantly paper based. Discussions with representatives of the Federal Reserve have demonstrated significant concerns about this Act having any impact on the current system of check collection. Accordingly, the definition of, and provisions regarding, transferable records in Section 118 have been limited to promissory note equivalents, and orders under Article 3 have been eliminated from the Scope of this Act. Considering the highly regulated and largely closed nature of
the check collection system, exclusion of Article 4 from the Act seems a reasonable
approach.  
The principal reason for retaining applicability of the UETA to the UCC relates to
the status of enactment for revised Articles 2, 2A, and 9 and proposed Article 2B. Upon
promulgation, these revisions will clearly fall within the exception in subparagraph (6)
because they will contain provisions for the use of electronic media, and under subsection
(c) will be unified entitling under which application of this Act to specific requirements
for writings will be contrary to the purpose of such requirements. However, until the
enactment of these revised Articles, the UETA has definite applicability in assuring that
sales, leases, licenses and secured transactions under the non-revised articles, will be
valid if done electronically. Accordingly, a broad exclusion for the UCC from the
UETA, as has been suggested by some, would be ill-advised.

In the same vain, other statutes where the use of electronic media was a conscious
part of the drafting process are also addressed by the interaction of subsection (b)(6) and
(c). Subsection (c) can be viewed as a limited “repugnancy” provision. That is, in a
statute which has specific provisions on electronic media, when the statute elsewhere
provides for a writing, this Act will not apply upon an affirmative finding by the court
that application of this Act would be contrary to the purpose of that writing requirement.

4. Subparagraph (8) preserves a space for individual states to exclude other
transactions which might be of particular concern in a given jurisdiction. Transactions
such as statutory powers of attorney, health powers, and perhaps even real estate
transactions might be excluded.

5. The exclusion in subsection (d) for rules of law calling for particular methods for
delivering or displaying information is intended to preserve such delivery/display
requirements regardless of the media used. If a notice must be displayed at a place of
business that requirement does not change simply because the notice may now be
electronic. However, the ability to properly display the notice, if it is only in electronic
form, may necessitate the use of paper. Similarly, if a rule of law requires delivery by US
postal service, this Act will not affect that requirement of the rule, and delivery by post of
a disc with the information on it would be required. This may in turn be subject to the
rule in Section 108 regarding provision of information in writing.

**Reporter's Note:**

1. The scope of the Act is limited to electronic records and electronic signatures.
The underlying premise of this section is that this Act applies to all electronic records and
signatures unless specifically excluded.

2. At the May, 1997 meeting, the Drafting Committee expressed strong reservations
about applying this Act to all writings and signatures, as is contemplated in the Illinois,
Massachusetts and other models. These same reservations were again raised at the
September, 1997 Meeting. An attempt was made in the Nov. 1997 draft to address those
concerns by limiting applicability of the Act to only those records and signatures arising
in the context of a "commercial transaction" or "governmental transaction," as therein
defined. However, the view of a majority of the committee and most observers was that
defining the terms "commercial transactions" and "governmental transactions" was not
possible with any degree of precision. Rather, a specific delineation of excluded
transactions was considered preferable to an attempt to redefine commercial and
governmental transactions.
3. In order to identify the specific transactions and transaction types to be excluded,
a Task Force comprised of a number of observers and the Chair and Reporter for the
Committee was formed under the leadership of R. David Whittaker. This Task Force was
charged with reviewing selected statutory compilations (Massachusetts and Illinois being
two states where significant work had already been started) to determine the types of
transactions requiring writings and manual signatures which should be excluded from the
coverage of this Act.
4. The Task Force Report was completed at the end of September and was
extensively discussed at the October, 1998 meeting. Subsection (b) sets forth specific
exclusions and limitations to the coverage of this Act based on the Task Force Report, the
discussions at the October 1998 meeting and subsequent meetings and comments with
other interested parties.

SECTION 104-105. VARIATION BY AGREEMENT.

(a) This [Act] does not require that records or signatures be generated, stored,
sent, received, or otherwise processed or used by electronic means or in electronic form.
(b) Except as otherwise provided in subsections 107 and 108 (c) and (d), as
between parties involved in generating, storing, sending, receiving, or otherwise
processing or using electronic records or electronic signatures, the provisions of this [Act]
may be varied by agreement. The presence in certain provisions of this [Act] of the words
"unless otherwise agreed", or words of similar import, does not imply that the effect of
other provisions may not be varied by agreement.
(c) The determination of reasonableness in Section 109 may not be varied by
agreement:
(d) The effect of requiring an unreasonable security procedure stated in Section
110 may not be varied by agreement.
The presence in certain provisions of this Act of the words "unless otherwise agreed", or words of similar import, does not imply that the effect of other provisions may not be varied by agreement under subsection (a).

Source: UCC Section 1-102(3); Illinois Model Section 103.
Committee Vote: To move former subsection (c) to the end of subsection (b). Yea-3 Nay-0 (October, 1998)

Reporter’s Note to this Draft:
The only provisions of the Act which may not be varied by agreement are those in Sections 107 and 108 regarding the effect of security procedures and the provision of information in writing. In each case, the Drafting Committee may seek to limit the effect of those sections to consumer transactions.

Reporter’s Note:
1. Subsection (a) makes clear that this Act is intended to permit the use of electronic media, but does not require any person to use electronic media. For example, if Chrysler Corp. were to issue a recall of automobiles via its internet website, it would not be able to rely on this Act to validate that notice in the case of a person who never logged on to the website, or indeed, had no ability to do so. The provisions in Section 106 permitting a person to establish reasonable forms for electronic records and signatures assumes a pre-existing relationship between parties to a transaction, in which one party places reasonable limits on the records and signatures, electronic or otherwise, which will be acceptable to it.
2. Given the principal purpose of this Act to validate and effectuate the use of electronic media, it is important to preserve the ability of the parties to establish their own requirements concerning the method of generating, storing and communicating with each other. This Act affects substantive rules of contract law in very limited ways by giving effect to actions done electronically. Even in those cases, the parties remain free to alter the timing and effect of their communications.

SECTION 105 106. APPLICATION AND CONSTRUCTION. This Act must be construed and applied consistently with reasonable practices under the circumstances and to facilitate electronic transactions, promote its purposes and policies.

Source: UCC Section 1-102
Committee Vote: To delete “liberally” and substitute “facilitate electronic transactions”. Yea-3 Nay-0 (October, 1998)

Reporter’s Note to this Draft. The Style Committee still believes that this section smacks of a general purposes clause, creates ambiguity, and should be deleted.

Reporter’s Note:
The purposes and policies of this Act are
a) to facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and electronic signatures;
b) to eliminate barriers to electronic commerce and governmental transactions resulting from uncertainties relating to writing and signature requirements;
c) to simplify, clarify and modernize the law governing commerce and governmental transactions through the use of electronic means;
d) to permit the continued expansion of commercial and governmental electronic practices through custom, usage and agreement of the parties;
e) to promote uniformity of the law among the states (and worldwide) relating to the use of electronic and similar technological means of effecting and performing commercial and governmental transactions;
f) to promote public confidence in the validity, integrity and reliability of electronic commerce and governmental transactions; and
g) to promote the development of the legal and business infrastructure necessary to implement electronic commerce and governmental transactions.

SECTION 201 106. LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES AND ELECTRONIC CONTRACTS.

(a) A record or signature may not be denied legal effect, validity, or enforceability solely because it is an in electronic form record.

(b) A contract may not be denied legal effect, validity, or enforceability solely because an electronic record was used in its formation.

(bc) If a rule of law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies the rule of law requirement.

(d) If a rule of law requires a signature, or provides consequences in the absence of a signature, the rule of law is satisfied with respect to an electronic record if the electronic record includes an electronic signature.

(ce) In any transaction, a person may establish reasonable requirements regarding the type of records or signatures acceptable to it.

Source: UETA Sections 201, 301 and 401(a) (Sept. 1998 Draft).
Reporters Note to this Draft:

1. Subsections (a and b) have been revised to delete the words “validity and enforceability”. This makes the sections more parallel with Article 2B without altering the meaning of the section.

2. This section reflects the significant reorganization from the September 1998 draft. There are now only 18 sections regarding private electronic transactions and they all appear in Part 1. Part 2 sets forth the provisions encouraging governmental agencies to “go electronic.” This section combines the general effectiveness provisions for electronic records and signatures and contracts taken from the noted sections of the prior draft.

3. At the September, 1998 meeting consideration of the annual meeting comment that these rules should be stated in the positive rather than the negative confirmed that the rules must be stated in the negative. This Act is only eliminating one ground for denying validity to records, signatures and contracts. Accordingly it provides that the medium cannot be the only ground for such a denial, and leaves to other law other grounds for denying such validity.

Reporters Note:

1. Under different provisions of substantive law the legal effect of an electronic record may be separate from the issue of whether the record contains a signature. For example, where notice must be given as part of a contractual obligation, the effectiveness of the notice will turn on whether the party provided the notice regardless of whether the notice was signed. An electronic record attributed to a party under Section 109 would suffice in that case, notwithstanding that it may not contain a signature.

2. Subsections (a) and (b) establish the fundamental premise of this Act: That the form in which a record, signature or contract is generated, presented, communicated or stored may not be the only reason to deny it legal recognition. On the other hand, subsections (a) and (b) should not be interpreted as establishing the legal effectiveness of any given record, signature or contract. For example, where a rule of law requires that the record contain minimum substantive content, the legal effect will depend on whether the record meets the substantive requirements. However, the fact that the information is set forth in an electronic, as opposed to paper record, is irrelevant.

3. Subsections (c and d) are particularized applications of subsection (a). The purpose is to validate and effectuate electronic records and signatures as the equivalent of writings, subject to all of the rules applicable to the efficacy of a writing, except as such other rules are modified by the more specific provisions of this Act.

Illustration 1: A sends the following e-mail to B: "I hereby offer to buy widgets from you, delivery next Tuesday. /s/ A." B responds with the following e-mail: "I accept your offer to buy widgets for delivery next Tuesday. /s/ B." The e-mails may not be denied effect solely because they are electronic. In addition, the e-mails do qualify as records under the Statute of Frauds. However, because there is no quantity stated in either record, the parties' agreement would be unenforceable under existing UCC Section 2-201(1).
**Illustration 2:** A sends the following e-mail to B: "I hereby offer to buy 100 widgets for $1000, delivery next Tuesday. /s/ A." B responds with the following e-mail: "I accept your offer to purchase 100 widgets for $1000, delivery next Tuesday. /s/ B." In this case the analysis is the same as in Illustration 1 except that here the records otherwise satisfy the requirements of UCC Section 2-201(1). The transaction may not be denied legal effect solely because there is not a pen and ink "writing" or "signature".

The purpose of the section is to validate electronic records and signatures in the face of legal requirements for paper writings and manual signatures. Where no legal requirement of a writing or signature is implicated, electronic records and electronic signatures are subject to the same proof issues as any other evidence.

5. Subsection (e) is a particularized application of Section 104, to make clear that parties retain control in determining the types of records to be used and accepted in any given transaction. For example, if the Chrysler recall hypothetical referred to in Note 2 to Section 104, although Chrysler cannot unilaterally require recall notices to be effective under this Act, it may indicate the method of recall in a purchase agreement with a customer. If the customer objects, the customer would have the right to establish reasonable requirements for such notices.

**SECTION 107. MANIFESTING ASSENT.** In a transaction governed by this Act, the following rules apply:

(1) A person, acting in person, by its agent or through its electronic device, manifests assent to a record or term if, acting with knowledge of, or after having an opportunity to review, the record or term it intentionally engages in conduct it knows or has reason to know will cause the other party to infer assent.

(2) Unless the substantive rules of law governing the transaction provide otherwise, mere retention of information or a record without objection is not a manifestation of assent.

(3) If assent to a particular term is required by the substantive rules of law governing the transaction, a person, acting in person, by its agent or through its electronic
device, does not manifest assent to the term unless there was an opportunity to review the
term and the manifestation of assent relates specifically to the term:

—____(4) A manifestation of assent may be proved in any manner, including showing
that a procedure existed by which a person, acting in person, by its agent or through its
electronic device must have engaged in conduct or operations that manifested assent to the
record or term in order to proceed further in the transaction.}]

Reporter’s Note to this Draft. The Committee voted unanimously at the September,
1998 meeting to delete this section as unnecessary. Since the concept is not used
elsewhere in the statute, and since the provision was intended to merely track the
Restatement concepts of mutual assent, the Committee considered the provision
superfluous.

[SECTION 108. OPPORTUNITY TO REVIEW. A person or electronic device
has an opportunity to review a record or term only if it is made available in a manner that:

—____(1) would call it to the attention of a reasonable person and permit review; or
—____(2) in the case of an electronic device, would enable a reasonably configured
electronic device to react to it.]

Reporter's Note to this Draft: See Note to deleted section 107 above.

SECTION 109. DETERMINATION OF REASONABLE SECURITY
PROCEDURE:

—____[(a) The reasonableness of a security procedure is determined by the court as a
matter of law.]
—____(b) In determining the reasonableness of a security procedure, the following rules
apply:
(1) A security procedure established by law is reasonable for the purposes for which it was established.

(2) A security procedure established by an organization for use in transactions among its members, or between other persons and the organization or its members is reasonable for the purposes for which it was established.

(3) Except as otherwise provided in paragraphs (1) and (2), reasonableness is determined in light of the purposes of the procedure and the circumstances at the time the parties agreed to or adopted the procedure, including the nature of the transaction, sophistication of the parties, volume of similar transactions engaged in by either or both of the parties, availability of alternatives offered to but rejected by a party, cost of alternative procedures, and procedures in general use for similar transactions.

(4) A reasonable security procedure may require the use of any security measures that are reasonable under the circumstances.

**Reporter’s Notes to this Draft.** This section was deleted as no longer relevant in light of the changes to section 107 below.

**SECTION 107 140. EFFECT OF REQUIRING UNREASONABLE SECURITY PROCEDURE.**

**ALTERNATIVE 1**

(a) [In a consumer transaction] If a person (the "requiring party") imposes; as a condition of entering into a transaction with [a consumer] [another person], or otherwise is responsible for a particular security procedure being used in a transaction a requirement
that the parties expressly agree to be bound by the results of a security procedure that is not reasonable, the following rules apply:

(1) (A) If the [consumer] [other party] reasonably relies to its detriment on an electronic record or electronic signature purporting to be that of the requiring party and;

(B) application of the security procedure verified

(i) the source of the electronic record or electronic signature;

or

________________________ (ii) the integrity of the informational content of the electronic record,

the requiring party may not deny the source, or integrity of the informational content, of the electronic record or electronic signature to which the security procedure was applied.

(2) If the requiring party relies on an electronic record or electronic signature purporting to be that of the [consumer] [other party], the [consumer] [other party] retains the right to deny the source of the electronic record or electronic signature, or the integrity of the informational content of the electronic record.

ALTERNATIVE 2

(a) An agreement to be bound by the results of a security procedure is unenforceable [in a consumer transaction].

END OF ALTERNATIVES

(b) The provisions of this section may not be varied by agreement.
(b) A person does not impose a security procedure under subsection (a) if it makes reasonable alternative security procedures available to the other person, together with information which enables the other person to make an informed selection from among the offered procedures.

Source: New

Reporter's Note to this Draft. This section has been drafted in response to the Committee's direction to prepare a provision which casts the risk of misattribution, and informational error on the party that is responsible for a particular security procedure being used in a transaction. One immediate difficulty in such a case is that the security procedure being used may not have been injected into the transaction by either party, or it may be virtually impossible to determine which party "required" the security procedure. For example, the parties may be relying on a security procedure built into the software of one or the other party, e.g., netscape's security procedure. In such a case it may be that neither party is responsible for the security procedure because neither party consciously selected the procedure. At the very least, the question of whether a party was responsible for the use of the procedure may be difficult to determine.

Alternative 1 is a revision of the former section 110 stripped of the issue of the reasonableness of the security procedure. Under this draft, regardless of the reasonableness of a security procedure, the party not responsible for bringing the security procedure into the transaction retains rights to deny attribution and content integrity of records received by the requiring party, thereby putting the requiring party to its proof. At the same time the provision binds the responsible party to records and signatures verified by the security procedure and reasonably relied upon by the other party. These provisions cannot be varied by agreement, and are no longer predicated on an agreement to be bound by the results of the security procedure. If neither party was responsible for the use of the security procedure this section would be inapplicable and the parties would be left to prove the transaction in any reasonable manner.

Alternative 2 is more straightforward. It simply provides that an agreement to be bound by the results of a security procedure regardless of the veracity of those results, is not enforceable. Without such an agreement the parties will be left to prove the attribution or content integrity of a record/signature by showing the efficacy of the security procedure. An agreement to be bound to results obviates the necessity for the relying party to convince the trier of fact that the security procedure is good and so establishes the identity of the other party or content of the message. Instead all that need be shown is that the security procedure was applied properly and that the result indicated the other party was the sender and the content was as stated. The other party is then effectively denied the ability to challenge the efficacy of the record/signature. If that agreement to be bound to the results is denied effect, then the relying party must still prove the validity and quality of the security procedure and the other party retains the ability to challenge the quality of the procedure. If the parties do not expressly agree to be bound by the results of the
procedure, this alternative would not be applicable, and the proponent of the electronic
record or signature would be required to establish the validity of the record/signature.

Illustration 1. General Motors advises its franchisees that GM has established a
security procedure for ordering goods and that all parties must agree to be bound
by the results of the procedure. Through no fault of franchisee, bad guy sends an
electronic record which, upon application of the security procedure shows
franchisee as the buyer. Under Alternative 1, since GM was responsible for this
procedure being used, the franchisee would retain the right to deny that it is the
source of the order, and GM would be required to prove that the record was in fact
that of the franchisee under section 109. The agreement to be bound would be an
impermissible variation of the provisions of alternative 1.

If the underlying agreement as to the procedure were controlling, the franchisee
would bear the loss, since the electronic record would be attributable to the
franchisee. Under Alternative 2, that agreement is unenforceable (unless limited to
consumer transactions) and the franchisee retains the right to deny that it sent the
electronic record. GM would be put to its proof regarding the efficacy of the
security procedure or otherwise prove the order came from franchisee.

Illustration 2. Same facts as Illustration 1. If the bad guy is an employee of the
franchisee the result, in this case, would be no different. The franchisee remains
entitled to challenge the efficacy of the order placed by its employee, and GM
would have to establish attribution in fact under Section 109.

Illustration 3. GM advises its suppliers that GM has established a security
procedure for ordering goods and that all parties must agree to be bound by the
results of the procedure. Bad guy sends an order showing GM as the orderer of
$50,000 of parts. Supplier relies on the order and ships the goods. Bad guy
intervenes and takes the goods. In Supplier's claim for payment, under Alternative
1, GM will be bound by the order so long as the security procedure was properly
applied and the supplier reasonably relied on it. Under Alternative 2, GM would
be allowed to deny that it sent the order because the agreement to be bound by the
results of the security procedure is unenforceable.

In a consumer context the general result will be that a vendor receiving an order will bear
the risk that the order did not come from the purported sender. If a security procedure is
proposed by the vendor, alternative 1 would make the vendor the requiring party. The
consumer would likely adopt the procedure in order to complete the transaction. If a
trustworthy procedure is used the vendor would be able to prove the efficacy of the
security procedure in order to establish consumer was the source of the order and should
be bound. If the security procedure was not trustworthy, the vendor would likely be
unable to establish consumer as the source of the record and would bear the loss. If the
consumer had agreed to be bound to the results of the procedure, alternative 2 would
preserve the consumer’s ability to challenge the vendor’s claims by making the agreement unenforceable.

In transactions where neither party is responsible for the use of a particular security procedure, as in the case of a consumer ordering from a web vendor under the netscape security procedure residing on the consumer’s computer, the parties are left to prove their respective cases without aid of this section. Since the security procedure would be adopted by the use of both parties without either party injecting it into the transaction, Alternative 1 would not apply. Alternative 2 would be inapplicable since there would be no agreement to be bound by the results.

In the event that a transaction is accomplished without any security procedure, this Act, while validating the electronic records and signatures implemented in transactions falling within the Scope of this Act, does not address whether such records and signatures are otherwise legally binding or effective.

Among other commenters, the Bank Working Group has expressed its view that the UETA should not include any rule which would provide a specific effect for a security procedure. Rather, the use or non-use of security procedures would simply be one element in a party’s proof of records and signatures accomplished electronically. The Group’s letter to the Chair and Reporter has been distributed with this draft. WHETHER THE UETA SHOULD LEAVE THE EFFECT OF SECURITY PROCEDURES TO OTHER LAW IS A QUESTION THE COMMITTEE WILL NEED TO ADDRESS.

The draft provides an option to limit the alternative provisions to consumer transactions. Given the function of these alternatives as protective, the draft provides that, regardless of the alternative, this section may not be varied by agreement. THESE ARE CRITICAL ISSUES FOR THE COMMITTEE’S CONSIDERATION.

SECTION 108. PROVISION OF INFORMATION IN WRITING.

(a) If a rule of law requires a person to provide information in writing to another person, that requirement is satisfied if the information is provided in an electronic record that is

(1) under the control of the person to which it is provided; and

(2) capable of retention for subsequent reference by the person to which it is provided.

(b) The provisions of this section may not be varied by agreement in [a consumer transaction].
Source: UETA Section 104(d) *Sept., 1998 Draft); Canadian Draft Uniform Electronic Commerce Act

Reporter’s Note to this Draft. This is a new section, previously a part of former Section 104 Exclusions from Scope. It is included in response to suggestions made in the Report of the Task Force on State Law Exclusions to protect parties entitled to receipt of notice in writing. The provision allows parties to provide information electronically so long as the recipient has full control of the retention or disposition of the information once received. The concern was prompted by the recognition that electronic information may be given to a person while the person lacks the ability to copy or download the information.

SECTION 202 109. ATTRIBUTION OF ELECTRONIC RECORD TO PERSON.

[ALTERNATIVE 1]

(a) An electronic record is attributable to a person if:

(1) it was in fact the action of the person, a person authorized by it, or the person's electronic device;

(2) another person, in good faith and acting in conformity with a reasonable security procedure for identifying the person to which the electronic record is sought to be attributed, reasonably concluded that it was the act of the other person, a person authorized by it, or the person's electronic device.

(b) Attribution of an electronic record to a person under subsection (a)(2) has the effect provided for by law, regulation or an agreement regarding the security procedure.

[ALTERNATIVE 2]

(a) An electronic record is attributable to a person if the electronic record resulted from the action of the person, acting in person, by its agent, or by its electronic agent device. Attribution may be proven in any manner, including by showing the efficacy of any security procedure applied to determine the person to whom the electronic record was attributable.
(b) Attribution of an electronic record to a person under subsection (a) has the effect provided for by law, regulation, or agreement regarding the security procedure.

Source: UETA Section 202 Alternative 2 (Sept. 1998 Draft); Originally derived from Article 2B.

Committee Vote: To adopt Alternative 2 - Yea - 3 Nay - 0 (October 1998)

Reporter’s Notes: The language change in subsection (a) was made to conform to the language in Article 2B.

Alternative 1 was the provision as appeared in the Annual Meeting Draft. It was the result of the Committee’s votes in April, 1998 to remove presumptions in this Section.

This draft retains the idea of attribution, including attribution to a person acting through an agent or electronic agent. It also indicates that the use of a security procedure will be an important aspect in establishing attribution. However, it does not set forth any rule of attribution under particular circumstances.

SECTION 203 110. DETECTION OF CHANGES AND ERRORS. If the parties act in conformity with a reasonable security procedure, established by law, regulation, or agreement, to detect changes or errors in the informational content of an electronic record, between the parties, the following rules apply:

(1) If a sender has conformed to the security procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the sender is not bound by the change or error.

(2) If the other party notifies the sender in a manner required by the security procedure which describes the informational content of the record as received, the sender shall review the notification and report in a reasonable manner any change or error detected by it. Failure so to review and report any change or error binds the sender to the informational content of the record as received.

Source: UETA Section 203 (Sept. 1998 Draft) - Originally derived from Article 2B.
**Reporter’s Note:** No change from the September, 1998 Draft has been made except that the requirement that the security procedure be reasonable and the qualification that a security procedure must be established by law or agreement have each been deleted as unnecessary.

This section allocates the risk of errors and changes in transmission to the party that could have best detected the error or change through the proper application and use of a security procedure. If it is shown that application of the security procedure would have detected the error, the failure to apply the security procedure likely will result in the relying party bearing any resulting loss since the originating party will not be bound by the error. If it is shown that the security procedure would not have detected the error, subsection (1) will be inapplicable and the effect of any error will be determined under the applicable substantive law. If the security procedure requires the parties to communicate and one party fails to do so, that party will bear any loss under subsection (2). These results properly obtain regardless of the reasonableness of the procedure (since it must be effective to trigger the rule in (1)), or the manner in which the procedure was created.

THE COMMITTEE MAY WISH TO CONSIDER WHETHER SUBSECTION (2) ADDS ANYTHING TO THE SECTION. If the security procedure requires particular actions, subsection (1) requires both parties to comply. Subsection (2) is a specific application of subsection (1) since the actions contemplated under subsection (2) are the result of requirements under the security procedure. Subsection (1) could be redrafted as a single stand alone default rule.

**SECTION 204. INADVERTENT ERROR.** [Moved to Section 116(a and d)]

**SECTION 302 111. EFFECT OF ELECTRONIC SIGNATURES.**

[ALTERNATIVE 1]

- (a) Except as provided in subsection (b), the effect of an electronic signature shall be determined from the context and surrounding circumstances at the time of its execution or adoption.

- (b) As between parties to an agreement, the following rules apply:

  - (1) An electronic signature shall have the effect provided in the agreement.

  - (2) An electronic record containing an electronic signature is signed as a matter of law if the electronic signature is verified in conformity with a commercially reasonable security procedure for the purpose of verification of electronic signatures.
(a) An electronic signature may be proven in any manner, including by showing that the electronic signature was signed in conformity with a security procedure for validating electronic signatures, or that a procedure existed by which the person, acting in person, by its agent, or by its electronic agent device, must have engaged in conduct or operations that signed the record or term in order to proceed further in the processing of the transaction.

[(b) A person bound by the operations of an electronic agent under Section 116 is deemed to have signed an electronic record produced by the agent on its behalf, whether or not the operations result in the attachment or application of an electronic signature to the electronic record].

(bc) The effect of an electronic signature must be determined from the context and surrounding circumstances at the time of its execution or adoption.

**Source:** Subsections (a and c) from UETA Section 302 Alternative 2 (Sept. 1998 Draft); Subsection (b) from UETA Section 303 (Sept. 1998 Draft).

**Committee Vote:** To adopt Alternative 2 - Yea - 3 Nay - 0 (October 1998)

**Reporter's Note to this Draft.** The language change in subsection (a) was made to conform to the language in Article 2B.

1. Alternative 1 reflected the provision as it appeared in the Annual Meeting Draft. Alternative 2, adopted by the Committee in October, 1998, removes any statutory effect of an electronic signature verified by a security procedure. Instead, an electronic signature is proven in any reasonable manner, and it is likely that the efficacy of a security procedure will be critical in this proof. However, the effect of the signature is left to the context under subsection (c).
2. Subsection (b) has been moved to this section from former Section 303 because it relates to the existence of a signature. Its purpose is to establish that by programming an electronic agent, a party assumes responsibility for electronic records and operations "executed" by the program. While the electronic agent may or may not execute a symbol representing an electronic signature, the party programming the electronic agent has indicated its authentication of records and operations produced by the electronic agent within the parameters set by the programming. Accordingly, the party should be deemed
to have signed the records of the electronic agent. The effect of such a signature is left to other law or agreement under subsection (c). **THE PROVISION HAS BEEN BRACKETED FOR THE COMMITTEE’S CONSIDERATION REGARDING WHETHER IT IS APPROPRIATE TO DEEM A RECORD SIGNED UNDER THE CIRCUMSTANCES SET FORTH IN SUBSECTION (b).**

**Reporter's Note:** An electronic signature is any identifying symbol executed or adopted by a person. This Act had included in the definition of signature the attributes normally associated with a pen and ink signature in order to make clear what a signer intends by signing a document, i.e., to identify oneself, adopt the terms of the signed record, and verify the integrity of the informational content of the record which is signed. At the April, 1998 meeting concern was expressed that these attributes were too exclusive because signatures may be used for other purposes as well. Consequently, the effect of the signature is left to agreement or other law.

**SECTION 303. OPERATIONS OF ELECTRONIC DEVICES.** [Substance moved to Section 116(b) and Section 111(b)]

(a) A person that configures and enables an electronic device is bound by operations of the device:

(b) A person bound by the operations of an electronic device under subsection (a) is deemed to have signed an electronic record produced by the device on its behalf, whether or not the operations result in the attachment or application of an electronic signature to the electronic record:

**SECTION 304 112. NOTARIZATION AND ACKNOWLEDGMENT.**

If a rule of law requires that a signature be notarized or acknowledged, or provides consequences in the absence of a notarization or acknowledgment, the requirement rule of law is satisfied with respect to an electronic signature if a security procedure was applied to the electronic signature which establishes by clear and convincing evidence the identity of the person signing the electronic record [and that the electronic record has not been altered since it was electronically signed].

**Source:** New
**Reporter's Note:** This provision has been added in response to the Task Force Report. The last clause has been bracketed because there is a question whether notarization and acknowledgment have the purpose of assuring content integrity. The clear and convincing standard has been deleted based on concerns raised at the October 1998 meeting that this standard is too stringent. The purpose of a notary is generally one of identification, and so long as a security procedure establishes identity by the normal preponderance of the evidence standard, that was considered to be sufficient.

**SECTION 205. ORIGINALS: ACCURACY OF INFORMATION.** [COMBINED WITH FORMER 206 IN NEXT SECTION]

(a) If a rule of law [or a commercial practice] requires a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that rule of law requirement is satisfied met by an electronic record if [the electronic record is shown to reflect accurately] [there exists a reliable assurance as to the integrity of] the information set forth in the electronic record after it was first generated in its final form, as an electronic record or otherwise:

(b) The integrity and accuracy of the information in an electronic record are determined by whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change arising in the normal course of communication, storage, and display. The standard of reliability required must be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

**SECTION 206 113. RETENTION OF ELECTRONIC RECORDS.**

(a) If a rule of law requires that certain documents, records, or information be retained, that requirement is met by retaining an electronic records of the information in
the record, if the electronic record is shown to reflect accurately the information set forth
in the record after it was first generated in its final form as an electronic record or
otherwise.

(b) An electronic record reflects accurately the information in a record under
subsection (a), if:

(1) the information contained in the electronic record remains accessible
for later reference;

(2) the electronic record is retained in the format in which it
originally was generated, stored, sent, or received, or in a format that can be demonstrated
to reflect accurately the information as originally generated, stored, sent, or received; and

(3) the information, if any, is retained in a manner that enables the
identification of the source of origin and destination of the record, the authenticity and
integrity of the information in the record, an electronic record and the date and time it the
record was sent or received,

(bc) A requirement to retain documents, records, or information in accordance
with subsection (a) does not apply extend to any information whose sole purpose is to
enable the record to be sent or received.

(ed) A person satisfies subsection (a) by using the services of any other person; if
the conditions set forth in subsection (a) are met.

(e) If a rule of law [or a commercial practice] requires a record to be presented or
retained in its original form, or provides consequences if the record is not presented or
retained in its original form, that rule of law [or commercial practice] is satisfied by an
electronic record retained in accordance with subsection (a).

(df) A record retained as an electronic record in accordance with subsection (a)
satisfies rules of law requiring a person[, other than a governmental agency,] to retain
records for evidentiary, audit, or like purposes, until a governmental agency of this State
adopts rules of law specifically prohibiting the use of electronic records for specified
purposes within the jurisdiction of the governmental agency. However, this section does
not preclude a federal or state governmental agency of this State from specifying
additional requirements for the retention of records, either written or electronic, subject to
the agency's jurisdiction.

Source: UETA Sections 205 and 206 (Sept. 1998 Draft); Uncitral Model Articles 8 and
10; Illinois Model Sections 204 and 206.
Reporter's Notes to This Draft: Former sections 205 - Originals and 206 - Retention of
Records, overlapped in significant ways. This draft combines these provisions. The
general standard for retention in subsection (a) is derived from the former 205(a) standard
for an original. Subsection (b) provides a safe harbor for meeting the standard in
subsection (a), and is the provision for retention of electronic records from former section
206(a). Subsections (c and d) are from former section 206(b and c). Subsection (e) is
from former section 205(a) and makes records retained in accordance with the standard in
subsection (a) valid as originals. Finally, subsection (f) is an expansion of former section
206(d) which is necessary to assure that governmental agencies are required to accept
records retained electronically for evidentiary, audit and similar record retention functions,
unless the agency specifically requires another medium.
Reporter's Note: This section deals with the serviceability of electronic records as
retained records and originals. As was noted at the May, 1997 meeting, the concept of an
original electronic document is problematic. For example, as I draft this Act the question
may be asked what is the "original" draft. My answer would be that the "original" is either
on a disc or my hard drive to which the document has been initially saved. Since I
periodically save the draft as I am working, the fact is that at times I save first to disc then
to hard drive, and at others vice versa. In such a case the "original" may change from the
information on my disc to the information on my hard drive. Indeed, as I understand
computer operations, it may be argued that the "original" exists solely in RAM and, in a
sense, the original is destroyed when a "copy" is saved to a disc or to the hard drive. In any
event, the concern focuses on the integrity of the information, and not with its "originality."

A second question raised at the May, 1997 meeting related to when the law requires an "original." Except in the context of paper tokens such as documents of title and negotiable instruments, most requirements for "originals" derive from commercial practice where the assurance of informational integrity is a concern. The comment to Illinois Model Law Section 204 (derived largely from Uncitral Model Law Summary Paragraph 62) identifies some of these situations as follows:

The requirement that a document be "an original" occurs in a variety of contexts for a variety of reasons. Documents of title and negotiable instruments, for example, typically require the endorsement and presentation of an original. But in many other situations it is essential that documents be transmitted unchanged (i.e., in their "original" form), so that other parties, such as in international commerce, may have confidence in their contents. Examples of such documents that might require an "original" are trade documents such as weight certificates, agricultural certificates, quality/quantity certificates, inspection reports, insurance certificates, etc. Other non-business related documents which also typically require an original form include birth certificates and death certificates. When these documents exist on paper, they are usually only accepted if they are "original" to lessen the chance that they have been altered, which would be difficult to detect in copies.

Since requirements for "originals" are often the result of commercial practice and not an actual rule of law, the section includes the bracketed language regarding requirements derived from commercial practice. As a policy matter it is not at all clear that legislation should override established commercial practice. **THIS PROVISION (now in subsection (e)) REMAINS BRACKETED AS A QUESTION WHICH MUST BE RESOLVED BY THE DRAFTING COMMITTEE.**

So long as there exists reliable assurance that the electronic record accurately reproduces the information, this section continues the theme of establishing the functional equivalence of electronic and paper-based records. This is consistent with Fed.R.Evid. 1001(3) and Unif.R.Evid. 1001(3) (1974) which provide:

> If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."

This draft adopts as the appropriate standard that noted in the rules of evidence.

Another issue relates to the use of originals for evidentiary purposes. In this context the concern principally relates to the "best evidence" or "original document" rule. The use of electronic records in evidence is addressed in the next Section and its notes.

At the May, 1997 meeting concern was expressed that retained records may become unavailable because the storage technology becomes obsolete and incapable of reproducing the information on the electronic record. Subsection (b)(1) addresses this concern by requiring that the information in the electronic record "remain" accessible, and
subsection (b)(2) addresses the need to assure the integrity of the information when the format is updated or changed. This section would permit parties to convert original written records to electronic records for retention so long as the requirements of subsection (a) are satisfied. Accordingly, in the absence of specific requirements to retain written records, written records may be destroyed once saved as electronic records satisfying the requirements of this section.

SECTION 404 114. ADMISSIBILITY INTO EVIDENCE.

(a) In any legal proceeding, evidence of an electronic record or electronic signature may not be excluded:

(1) on the sole ground that it is an electronic record or electronic signature;

or

(2) on the ground that it is not in its original form or is not an original.

[ (b) In assessing the evidentiary weight of an electronic record or electronic signature, the trier of fact shall consider the manner in which the electronic record or electronic signature was generated, stored, communicated, or retrieved, the reliability of the manner in which the integrity of the electronic record or electronic signature was maintained, the manner in which its originator was identified or the electronic record was signed, and any other relevant circumstances.]

Source: UETA Section 404 (Sept. 1998 Draft); Uncitral Model Article 9; Illinois Model Section 205.

Reporter's Note: Like section 106, subsection (a)(1) prevents the nonrecognition of electronic records and signatures solely on the ground of the media in which information is presented. Subsection (a)(2) also precludes inadmissibility on the ground an electronic record is not an original.

Nothing in this section relieves a party from establishing the necessary foundation for the admission of an electronic record.

Subsection (b) gives guidance to the trier of fact in according weight to otherwise admissible electronic evidence. IT HAS BEEN BRACKETED FOR THE DRAFTING COMMITTEE’S CONSIDERATION in light of the questionable propriety of statutorily directing a court in the manner of consideration of evidence.
SECTION 401 115. FORMATION OF CONTRACT AND VALIDITY.

(a b) If an electronic record initiated by a person, or by its party or an electronic agent device, evokes an electronic record in response a contract is formed in the same manner and with the same effect as if the electronic records were not electronic. A contract is formed, if at all:

(1) when the response signifying acceptance is received; or

(2) if the response consists of electronically performing performance of the requested consideration in whole or in part, when the requested consideration, to be performed electronically, is received unless the initiating electronic record prohibited that form of response.

(b 3) The terms of a contract are determined by the substantive rules of law applicable to the particular contract.

(a) In an automated transaction, the following rules apply: [COMPARE SECTION 116(c) INFRA]

(1) A contract may be formed by the interaction of electronic devices of the parties, even if no individual was aware of or reviewed the electronic device's actions or the resulting terms and agreements. A contract is formed if the interaction results in the electronic devices' engaging in operations that confirm the existence of a contract or indicate agreement, such as engaging in performing the contract, ordering or instructing performance, accepting performance, or making a record of the existence of a contract:

(2) A contract may be formed by the interaction of an person's electronic device and an individual. A contract is formed by the interaction if the individual
performs actions that the individual knows or reasonably should know will cause the
device to complete the transaction or performance, or which are clearly indicated to be an
acceptance, regardless of other expressions or actions by the individual to which the
individual cannot reasonably expect the electronic device to react.

(3) The terms of a contract resulting from an automated transaction
include:

(A) terms of the parties' agreement;

(B) terms that the electronic device could take into account;

and

(C) to the extent not covered by subparagraph (1A) or (2B), terms
provided by law.

c. Unless otherwise agreed, a contract may not be denied legal effect, validity, or
enforceability solely because an electronic record was used in its formation:

Source: UETA Section 401(b) and (a)(3) (Sept. 1998 Draft); Article 2B Draft Section
2B-204; Uncitral Model Article 11.

Reporter's Note: The language in subsection (a) has been revised to conform with the
parallel provisions in Article 2B.

This section has been significantly revised. The provisions in former section 401
relating to automated transactions have been moved to the next section. The subsection
addressing the efficacy of electronic contracts has been moved to section 106 regarding
general efficacy of electronic records, signatures and contracts.

The balance of the section now simply provides that contract formation and
determination of resulting terms are a function of the law underlying the transaction. The
only change wrought by this section is to provide that the timing of the contract is based
on receipt and not sending, reversing the mailbox rule.

SECTION 116. OPERATIONS OF ELECTRONIC AGENTS;

AUTOMATED TRANSACTIONS. (a) In this section, "inadvertent error" means an
error by an individual made in dealing with an electronic agent of another person if the
electronic agent of the other person did not allow for the prevention or correction of the error.

(b) Operations of an electronic agent are the acts of a person if the person used the electronic agent for such purposes.

(c) In an automated transaction, the following rules apply:

(1) A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agent's actions or the resulting terms and agreements.

(2) A contract may be formed by the interaction of a person’s electronic agent and an individual. A contract is formed by the interaction if the individual performs actions that it is free to refuse to perform which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.

(d) In an automated transaction involving an individual, the individual is not responsible for an electronic record that the individual did not intend but which was caused by an inadvertent error if, on learning of the other person’s reliance on the erroneous electronic record, the individual:

(1) promptly notifies the other person of the error and that the individual did not intend the electronic record received by the other person;

(2) takes reasonable steps, including steps that conform to the other person’s reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and
(3) has not used or received the benefit or value of the consideration, if any, received from the other person.

**Source:** UETA Sections 204, 303(a) and 401(a)(Sept. 1998 Draft) - Originally derived from Article 2B Draft.

**Reporter’s Notes to This Draft:** This section brings together all provisions from the September, 1998 Draft which deal with the use of Electronic agents. It provides for the effectiveness of actions taken through the operations of electronic agents, clarifies that contracts can be entered.
into by machines, and addresses the idea of inadvertent error when an individual is dealing
with a machine.

Former Section 303(a) has been revised to make the operations of electronic agents
the acts of the person using the agent for the purposes accomplished. This makes the
section parallel to the provision in Article 2B, and addresses concerns of the ABA
Electronic Agents Task Force regarding the strict liability aspect of the former provision.
By equating the operations with acts of a person, the legal effect of a person’s acts,
accomplished through the operations of an electronic agent, are left to the substantive law
governing the transaction.

Former section 204 has been included without substantive change. The second
sentence of former section 401(a)(1) has been deleted based on comments at the last
meeting that it was unnecessary. Based on the same concerns, minor changes for
clarification to former section 401(a)(2) have been made.

Reporters Notes:

1. Operations of Electronic agents. Formerly Section 303(b).

   Formerly Section 303(b).

   Section 116(b) makes clear that the party that sets operations of an electronic agent
   in motion is responsible for the records and signatures resulting from such operations. A
   party is bound by the actions of a computer program designed to act without human
   intervention, as well as electronic and automated means such as telecopy and facsimile
   machines used by a party.

   A Task Force of the ABA Committee on the Law of Cyberspace considered the
   issue of electronic agents at the mid-winter working meeting in Atlanta, January 15-16,
   1998. A proposed alternative based on that meeting has been included in the Reporters
   Memorandum for this draft.

2. Automated Transactions. Formerly section 401(a).

   A. Subsection (c) addresses those transactions not involving human review by one
   or both parties and provides rules to expressly validate contract formation when electronic
   agents are involved. It sets forth the circumstances under which formation will occur in a
   fully automated transaction and under an automated transaction where one party is an
   individual.

   B. Subsection (c)(2) addresses the circumstance of an individual dealing with an
   electronic agent.

   As noted in a number of comments at the January, 1998 meeting, whether one
   knows that one is dealing with an electronic agent should be irrelevant, so long as the
   individual proceeds with actions it knows or reasonably should know will result in
   accomplishment of the ends desired. Concerns previously expressed by observers that
   individuals may not know what contemporaneous statements made by the individual
   would be given effect because of the possibility of contemporaneous or subsequent human
   review, have been addressed by limiting those actions of the individual which may result
   in a contract to those which the individual would reasonably expect to result in a contract.
   This will provide the party employing an electronic agent with an incentive to make clear
   the parameters of the agent's ability to respond. If the party employing the electronic
   agent provides such information, the individual's act of proceeding on the basis of
   contemporaneous actions or expressions not within the parameters of the agent would be
unreasonable and such actions and expressions could not be the basis for contract
formation.
3. **Inadvertent Error.** Formerly section 204.

This section attempts to address the issue of human error in the context of an
automated transaction. The reason for attempting to address this issue is that inadvertent
errors, such as a single keystroke error, do occur, and are difficult, if not impossible to
retrieve, given the speed of electronic communications. However, the definition of
"inadvertent error" would allow a vendor to provide an opportunity for the individual to
confirm the information to be sent, in order to avoid the operation of this provision. By
providing an opportunity to an individual to review and confirm the information initially
sent, the other party can eliminate the possibility of the individual defending on the
grounds of inadvertent error since the electronic agent, through confirmation, allowed for
correction of the error.

**SECTION 402 117. TIME AND PLACE OF SENDING AND RECEIPT.**

(a) Unless otherwise agreed between the sender and the recipient, an electronic
record is sent when it the information is addressed or otherwise directed properly to the
recipient and enters an information processing system outside the control of the sender or
of a person that sent the electronic record on behalf of the sender.

(b) Unless otherwise agreed between the sender and the recipient, an electronic
record is received when the electronic record enters an information processing system in a
form capable of being processed by that system that the recipient uses or has designated
for the purpose of receiving electronic records or information and from which the recipient
is able to retrieve the electronic record. In a form capable of being processed by that
system, if the recipient uses or has designated that system for the purpose of receiving
such an electronic record or information. An electronic record is also received when the
recipient learns of its content from a record.
(c) Subsection (b) applies even if the place the information processing system is located is different from the place the electronic record is considered to be received under subsection (d).

(d) Unless otherwise agreed between the sender and the recipient, an electronic record is deemed to be sent from the sender's place of business and is deemed to be received at the recipient's place of business. For the purposes of this subsection, the following rules apply:

(1) If the sender or recipient has more than one place of business, the place of business of that person is that which has the closest relationship to the underlying transaction or, if there is no underlying transaction, the principal place of business.

(2) If the sender or the recipient does not have a place of business, the place of business is the sender's or recipient's residence, as the case may be.

(e) Subject to Section 403, An electronic record is effective when received even if no individual is aware of its receipt.

[f] Receipt of an electronic acknowledgment establishes that a record was received but, in itself, does not establish that the content sent corresponds to the content received.

Source: UETA Sections 402 and 403(b) (Sept. 1998 Draft); Uncitral Model Article 15.

Reporter’s Note to this Draft. This section has been revised for clarity and to incorporate former subsection 403(b) in light of the deletion of the balance of former section 403.

Reporter's Note:
1. This section provides default rules regarding when an electronic record is sent and when and where an electronic record is received. This section does not address the efficacy of the record that is received. That is, whether a record is unintelligible or unusable by a recipient is a separate issue from whether that record was received.
2. Subsection (a) now requires that information be properly addressed or otherwise directed to the recipient before it will be considered sent.

3. Subsection (b) provides simply that when a record enters the system which the recipient has designated or uses and to which it has access, in a form capable of being processed by that system, it is received. Unless the parties have agreed otherwise, entry into any system to which the recipient has access will suffice. By keying receipt to a system which is accessible by the recipient, the issue of leaving messages with a server or other service is removed. However, the issue of how the sender proves the time of receipt is not resolved by this section. The last sentence provides the ultimate fallback by providing that in all events a record is received when the recipient has knowledge of it.

4. Subsections (c) and (d) provide default rules for determining where a record will be considered to have been received. The focus is on the place of business of the recipient and not the physical location of the information processing system. As noted in paragraph 100 of the commentary to the Uncitral Model Law

   It is not uncommon for users of electronic commerce to communicate from one State to another without knowing the location of information systems through which communication is operated. In addition, the location of certain communication systems may change without either of the parties being aware of the change.

Accordingly, where the place of sending or receipt is an issue, the relevant location should be the location of the sender or recipient and not the location of the information processing system.

5. Subsection (e) rejects the mailbox rule and provides that electronic records are effective on receipt. This approach is consistent with Article 4A and, as to electronic records, Article 2B.

6. Subsection (f), from former section 403, provides that receipt of an acknowledgment does not establish the content of the message, but simply that it was received. It is a holdover from former Section 403 and HAS BEEN BRACKETED FOR THE COMMITTEE’S CONSIDERATION WHETHER IT IS NECESSARY.

SECTION 403. ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.

(a) If the sender of a record requests or agrees with the recipient of the record that receipt of the record must be acknowledged electronically, the following rules apply:

(1) If the sender indicates in the record or otherwise that the record is conditional on receipt of an electronic acknowledgment, the record does not bind the
sender until acknowledgment is received, and the record is no longer effective if
acknowledgment is not received within a reasonable time after the record was sent:

(2) If the sender does not indicate that the record is conditional on
electronic acknowledgment and does not specify a time for receipt, and electronic
acknowledgment is not received within a reasonable time after the record is sent, the
sender, upon notifying the other party, may:

(A) treat the record as being no longer effective; or
(B) specify a further reasonable time within which electronic

acknowledgment must be received and, if acknowledgment is not received within that
time, treat the record as being no longer effective.

(3) If the sender specifies a time for receipt and receipt does not occur
within that time, the sender may treat the record as no longer being effective.

(b) Receipt of electronic acknowledgment establishes that the record was received
but, in itself, does not establish that the content sent corresponds to the content received.

Source: Uncitral Model Article 14; Article 2B.
Reporter's Note: This section was deleted by vote of the Committee Yea- 3 Nay - 0 at the
October 1998 meeting. Subsection (b) was moved to section 117(f).

SECTION 405 118. CONTROL OF TRANSFERABLE RECORDS. If the
identity of the person entitled to enforce a transferable record can be reliably determined
from the record itself or from a method employed for recording, registering, or otherwise
evidencing the transfer of interests in such records, the person entitled to enforce the
record is deemed to be in possession of the record.
(a) A person having control of a transferable record is deemed to be [in possession] [the holder] of the transferable record.

(b) A person has control of a transferable record if the record itself or a method employed for recording, registering, or otherwise evidencing the transfer of interests in such records reliably establishes that person as the person with the right to enforce the transferable record.

(c) A person has control of a transferable record under subsection (b) if the record or records comprising the transferable record are created, stored, and assigned in such a manner that:

(1) a single authoritative copy of the record or records exists which is unique, identifiable, and except as otherwise provided in paragraphs (4), (5), and (6), unalterable;

(2) the authoritative copy identifies the person asserting control as the assignee of the record or records:

(3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(4) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(5) each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

(6) any revision of the authoritative copy is readily identifiable as an authorized or unauthorized revision.
Source: Subsection (b) derived from Oklahoma Model Section III.B.2; subsection (c)
Revised Article 9, Section 9-105.

Reporter's Note: This section has been retained for discussion by the Drafting
Committee on whether such documents should be covered by this Act.

The focus of this section has been clarified and sharpened. Like Revised Article 9
section 9-105 (from which subsection (c) is taken), this provision is intended to provide an
analog to possession of a tangible instrument. "Control" is intended to serve as the
functional equivalent of possession of a written token. If control of the transferable record
can be established, then it is possible to invoke the rules of Article 3 (if the transferable
record is the unwritten equivalent of a note) to establish one's rights as a holder in due
course. The question of the necessity to also provide imputation of indorsements is
continuing to be discussed, and may be necessary. The question of indorsements can be
mooted by adopting the provision making the person in control the "holder", since then all
indorsements will necessarily be imputed.

At the ABA Committee on the Law of Cyberspace working meeting in Atlanta
January 15-16, discussions about the proper formulation for including electronic tokens in
the UETA were had with members of the CLC committee including representatives from
the Federal Reserve. The memorandum from Professors Jane Winn and Paul Shupack to
the Chair and Reporter will be available for the Committee's consideration in Richmond.

PART 3
ELECTRONIC SIGNATURES

PART 4
ELECTRONIC CONTRACTS AND COMMUNICATIONS

PART 5 2
GOVERNMENTAL ELECTRONIC RECORDS

SECTION 5 201. CREATION AND RETENTION OF ELECTRONIC
RECORDS AND CONVERSION OF WRITTEN RECORDS BY
GOVERNMENTAL AGENCIES.

[Unless expressly prohibited by statute, each] [Each] governmental agency of this State
shall determine if, and the extent to which, it will create and retain electronic records
instead of written records and convert written records to electronic records. [The
[designated state officer] shall adopt rules governing the disposition of written records after conversion to electronic records.]

Source: Massachusetts Electronic Records and Signatures Act Section 3 (Draft - November 4, 1997)

Reporter's Note: See Notes following Section 203.

SECTION 5 202. RECEIPT ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.

(a) Except as otherwise provided in Section 113(f), [Except as expressly prohibited by statute each] [each] governmental agency of this State shall determine whether, and the extent to which, it will send and receive accept electronic records and electronic signatures to and from other persons, and otherwise create, use, store, and rely upon electronic records and electronic signatures.

(b) In a case governed by subsection (a), the governmental agency, by appropriate regulation giving due consideration to security, [may] [shall] specify:

(1) the manner and format in which the electronic records must be created, sent, received, and stored[, and the systems established for such purposes];

(2) if electronic records must be electronically signed, the type of electronic signature required, and the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process;
(3) control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records; and

(4) any other required attributes for electronic records which are currently specified for corresponding non-electronic records, or reasonably necessary under the circumstances.

(e) All regulations adopted by a governmental agency must conform to the applicable requirements established by [designated state officer] pursuant to Section 503.

(d c) Except as otherwise provided in Section 113(f), this [Act] does not require any governmental agency of this State to use or permit the use of electronic records or electronic signatures.

Source: Illinois Model Section 801; Florida Electronic Signature Act, Chapter 96-324, Section 7 (1996).

Reporter’s Note: See Notes following Section 203.

SECTION 5 203. [DESIGNATED STATE OFFICER] TO ADOPT STATE STANDARDS. The [designated state officer] may adopt regulations setting forth rules, standards, procedures, and policies for the use of electronic records and electronic signatures by governmental agencies. If appropriate, those regulations must specify differing levels of standards from which implementing governmental agencies may choose in implementing the most appropriate standard for a particular application.

SECTION 504 203. INTEROPERABILITY. To the extent practicable under the circumstances, regulations adopted by [designated state officer] or a governmental agency relating to the use of electronic records or electronic signatures must be drafted in a
manner Regulations adopted by a governmental agency of this State pursuant to Section 202 must be designed to encourage and promote consistency and interoperability with similar requirements adopted by other governmental agencies of this and other States and the federal government, and non-governmental persons interacting with governmental agencies of this State. If appropriate, those regulations must specify differing levels of standards from which implementing governmental agencies of this State may choose in implementing the most appropriate standard for a particular application.

Source: Illinois Model Section 803.

Reporter’s Notes to Part 2. This Part addresses the expanded scope of this Act.

Committee Votes: To delete bracketed provisions in sections 201, 202 and to delete former section 503. Yea - 3 Nay - 0 (October, 1998)

1. Section 201 is derived from former subsection 501(a) and authorizes state agencies to use electronic records and electronic signatures generally for intra-governmental purposes, and to convert written records and manual signatures to electronic records and electronic signatures. By its terms it leaves the decision to use electronic records or convert written records and signatures to the governmental agency. It also authorizes the destruction of written records after conversion to electronic form. The bracketed language requiring the appropriate state officer to issue regulations governing such conversions was deleted by the Committee at the October, 1998 meeting. The Committee also deleted former section 503 because it was considered inappropriate to provide for a single mechanism for promulgation of regulations in every state.

2. Section 202 has been revised along the model of the pending Illinois legislation and broadly authorizes state agencies to send and receive electronic records and signatures in dealing with non-governmental persons. Again, the provision is permissive and not obligatory (see subsection (d)). However, it has been clarified to provide that with respect to electronic records used for evidentiary purposes, Section 113 will apply unless a particular agency expressly opts out.

3. Section 203 requires regulating authorities to take account of consistency in applications and interoperability to the extent practicable when promulgating regulation. This section is critical in addressing the concerns of many at our meetings that inconsistent applications may promote barriers greater than currently exist.

PART 6 3

MISCELLANEOUS PROVISIONS
SECTION 6.301. SEVERABILITY CLAUSE. If any provision of this [Act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [Act], which can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

Source: Article 1 Draft Section 1-106.

SECTION 6.302. EFFECTIVE DATE. This [Act] takes effect....

Source:

SECTION 6.303. SAVINGS AND TRANSITIONAL PROVISIONS.

Source: