

# House Study Bill 650

## Bill Text

PAG LIN

1 1 DIVISION I  
1 2 SUBCHAPTER 1  
1 3 GENERAL  
1 4 Section 101. NEW SECTION. 554C.101 SHORT TITLE.  
1 5 This chapter shall be known and may be cited as the "Iowa  
1 6 Electronic Commerce Security Act".  
1 7 Sec. 102. NEW SECTION. 554C.102 PURPOSES AND  
1 8 CONSTRUCTION.  
1 9 This chapter shall be construed consistently with what is  
1 10 commercially reasonable under the circumstances and to  
1 11 effectuate all of the following purposes:  
1 12 1. Facilitate electronic communications by means of  
1 13 reliable electronic records.  
1 14 2. Facilitate and promote electronic commerce, by  
1 15 eliminating barriers resulting from uncertainties over writing  
1 16 and signature requirements, and promoting the development of  
1 17 the legal and business infrastructure necessary to implement  
1 18 secure electronic commerce.  
1 19 3. Facilitate electronic filing of documents with state  
1 20 and local government agencies and promote efficient delivery  
1 21 of government services by means of reliable electronic  
1 22 records.  
1 23 4. Minimize the incidence of forged electronic records,  
1 24 intentional and unintentional alteration of records, and fraud  
1 25 in electronic commerce.  
1 26 5. Establish uniformity of rules, regulations, and  
1 27 standards regarding the authentication and integrity of  
1 28 electronic records.  
1 29 6. Promote public confidence in the integrity,  
1 30 reliability, and legality of electronic records and electronic  
1 31 commerce.  
1 32 Sec. 103. NEW SECTION. 554C.103 VARIATION BY AGREEMENT  
1 33 USE OF ELECTRONIC MEANS OPTIONAL.  
1 34 1. As between parties involved in generating, sending,  
1 35 receiving, storing, or otherwise processing electronic  
2 1 records, the provisions of this chapter may be varied by  
2 2 agreement of the parties. However, an agreement shall not  
2 3 vary requirements provided in section 554C.203, subsection 2;  
2 4 section 554C.204, subsection 4; section 554C.305, subsection  
2 5 2; sections 554C.422, 554C.423, 554C.424, and 554C.442; and  
2 6 section 554C.444, subsection 2.  
2 7 2. This chapter shall not be construed to require a person  
2 8 to create, store, transmit, accept, or otherwise use or  
2 9 communicate information, records, or signatures by electronic  
2 10 means or in electronic form.  
2 11 SUBCHAPTER 2  
2 12 ELECTRONIC RECORDS AND SIGNATURES GENERALLY  
2 13 Sec. 104. NEW SECTION. 554C.201 DEFINITIONS.  
2 14 As used in this chapter, unless the context otherwise  
2 15 requires:  
2 16 1. "Commissioner" means the commissioner of insurance  
2 17 appointed pursuant to section 505.2.  
2 18 2. "Consumer transaction" means a transaction by an  
2 19 individual for personal, household, or family use.  
2 20 3. "Electronic" includes electrical, digital, magnetic,  
2 21 optical, electromagnetic, or any other form of technology that

2 22 entails capabilities similar to these technologies.  
2 23 4. "Electronic record" means a record generated,  
2 24 communicated, received, or stored by electronic means for use  
2 25 in an information system or for transmission from one  
2 26 information system to another.  
2 27 5. "Electronic signature" means a signature in electronic  
2 28 form attached to or logically associated with an electronic  
2 29 record.  
2 30 6. "Government agency" means any executive, legislative,  
2 31 or judicial agency, department, board, commission, authority,  
2 32 institution, or instrumentality of this state or of any  
2 33 county, city, or other political subdivision of this state.  
2 34 7. "Information" includes but is not limited to data,  
2 35 text, images, sound, codes, computer programs, software, and  
3 1 databases.  
3 2 8. "Party" means a person involved in an electronic  
3 3 transaction governed by the provisions of this chapter.  
3 4 9. "Record" means information that is inscribed, stored,  
3 5 or otherwise fixed on a tangible medium or that is stored in  
3 6 an electronic or other medium and is retrievable in  
3 7 perceivable form.  
3 8 10. "Rule of law" means any statute, rule of or order by a  
3 9 government agency, regulation, ordinance, common law rule, or  
3 10 court decision enacted, adopted, established, or rendered by  
3 11 the general assembly, government agency, court, political  
3 12 subdivision of, or other authority of, this state.  
3 13 11. "Security procedure" means a methodology or procedure  
3 14 for the purpose of doing any of the following:  
3 15 a. Verifying that an electronic record is the record of a  
3 16 specific person.  
3 17 b. Detecting an error or alteration in the communication,  
3 18 content, or storage of an electronic record since a specific  
3 19 point in time. A security procedure may require the use of  
3 20 algorithms or codes, identifying words or numbers, encryption,  
3 21 answer back, acknowledgment procedures, or similar security  
3 22 devices.  
3 23 12. "Signed" or "signature" includes any symbol executed  
3 24 or adopted, or any security procedure employed or adopted,  
3 25 including by use of electronic means, by or on behalf of a  
3 26 person with a present intention to authenticate a record.  
3 27 Definitions used in any part of this chapter shall apply in  
3 28 all other parts of this chapter.  
3 29 Sec. 105. NEW SECTION. 554C.202 LEGAL RECOGNITION.  
3 30 Information shall not be denied legal effect, validity, or  
3 31 enforceability solely on the grounds that it is in the form of  
3 32 an electronic record or an electronic signature.  
3 33 Sec. 106. NEW SECTION. 554C.203 ELECTRONIC RECORDS.  
3 34 1. Where a rule of law requires information to be written  
3 35 or in writing or provides for certain consequences if it is  
4 1 not, an electronic record satisfies that rule of law  
4 2 requirement.  
4 3 2. The provisions of this section shall not apply to any  
4 4 of the following:  
4 5 a. When its application involves a construction of a rule  
4 6 of law that is clearly inconsistent with the manifest intent  
4 7 of the body imposing the requirement or repugnant to the  
4 8 context of the same rule of law. However, the mere  
4 9 requirement that information be in writing, written, or  
4 10 printed shall not by itself be sufficient to establish an  
4 11 intent which is inconsistent with the requirement of this  
4 12 section.  
4 13 b. To any rule of law governing the creation or execution  
4 14 of a will or trust, living will, a general, durable, or  
4 15 healthcare power of attorney, or a voluntary, involuntary, or  
4 16 standby guardianship or conservatorship.  
4 17 c. To any record that serves as a unique and transferable  
4 18 physical expression of rights and obligations including,

4 19 without limitation, negotiable instruments and other  
4 20 instruments of title wherein possession of the instrument is  
4 21 deemed to confer title in a consumer transaction.  
4 22 d. To any record that grants a legal or equitable interest  
4 23 in real property, including a mortgage, deed of trust, pledge,  
4 24 security interest, or other lien or encumbrance in a consumer  
4 25 transaction.

4 26 Sec. 107. NEW SECTION. 554C.204 ELECTRONIC SIGNATURES.

4 27 1. Where a rule of law requires a signature, or provides  
4 28 for certain consequences if a document is not signed, an  
4 29 electronic signature satisfies that requirement.

4 30 2. An electronic signature may be proved in any manner,  
4 31 including by showing that a procedure exists by which a person  
4 32 must of necessity have executed a symbol or security procedure  
4 33 for the purpose of verifying that an electronic record is the  
4 34 record of that person in order to proceed further with a  
4 35 transaction.

5 1 3. Absent an agreement to the contrary, the recipient of a  
5 2 signed electronic record is entitled to establish reasonable  
5 3 requirements to ensure that the symbol or security procedure  
5 4 adopted as an electronic signature by the person signing is  
5 5 authentic.

5 6 4. The provisions of this section shall not apply to any  
5 7 of the following:

5 8 a. When its application would involve a construction of a  
5 9 rule of law that is clearly inconsistent with the manifest  
5 10 intent of the body imposing the requirement or repugnant to  
5 11 the context of the same rule of law. However, the mere  
5 12 requirement that information be in writing, written, or  
5 13 printed shall not by itself be sufficient to establish an  
5 14 intent which is inconsistent with the requirement of this  
5 15 section.

5 16 b. To any rule of law governing the creation or execution  
5 17 of a will or trust, living will, a general, durable, or  
5 18 healthcare power of attorney, or a voluntary, involuntary, or  
5 19 standby guardianship or conservatorship.

5 20 c. To any record that serves as a unique and transferable  
5 21 physical expression of rights and obligations including, but  
5 22 is not limited, to negotiable instruments and other  
5 23 instruments of title wherein possession of the instrument is  
5 24 deemed to confer title in a consumer transaction.

5 25 d. To any record that grants a legal or equitable interest  
5 26 in real property, including a mortgage, deed of trust, pledge,  
5 27 security interest, or other lien or encumbrance in a consumer  
5 28 transaction.

5 29 Sec. 108. NEW SECTION. 554C.205 REQUIREMENT FOR ORIGINAL  
5 30 INFORMATION.

5 31 1. Where a rule of law requires information to be  
5 32 presented or retained in its original form, or provides  
5 33 consequences for information not being presented or retained  
5 34 in its original form, that rule of law is satisfied by an  
5 35 electronic record if there exists reliable assurance as to the  
6 1 integrity of the information from the time when it was first  
6 2 generated in its final form, as an electronic record or  
6 3 otherwise.

6 4 2. The criteria for assessing the integrity of information  
6 5 shall be whether the information has remained complete and  
6 6 unaltered, apart from the addition of any endorsement and any  
6 7 change that arises in the normal course of communication,  
6 8 storage, and display. The standard of reliability required  
6 9 shall be assessed in the light of all relevant circumstances,  
6 10 including but not limited to the purpose for which the  
6 11 information was generated.

6 12 3. The provisions of this section do not apply to any  
6 13 record that serves as a unique and transferable physical  
6 14 expression of rights and obligations including, but not  
6 15 limited to, negotiable instruments and other instruments of

6 16 title wherein possession of the instrument is deemed to confer  
6 17 title.

6 18 Sec. 109. NEW SECTION. 554C.206 ADMISSIBILITY INTO  
6 19 EVIDENCE.

6 20 1. In any legal proceeding, nothing in the application of  
6 21 the rules of evidence shall apply so as to deny the  
6 22 admissibility of an electronic record or electronic signature  
6 23 into evidence based on any of the following:

6 24 a. On the sole ground that it is an electronic record or  
6 25 electronic signature.

6 26 b. On the grounds that it is not in its original form or  
6 27 is not an original.

6 28 2. Information in the form of an electronic record shall  
6 29 be given due evidential weight by the trier of fact. In  
6 30 assessing the evidential weight of an electronic record or  
6 31 electronic signature where its authenticity is in issue, the  
6 32 trier of fact may consider all relevant information or  
6 33 circumstances, including but not limited to the manner in  
6 34 which it was generated, stored, or communicated, the  
6 35 reliability of the manner in which its integrity was  
7 1 maintained, the manner in which its originator was identified,  
7 2 and the manner in which the electronic record was signed.

7 3 Sec. 110. NEW SECTION. 554C.207 RETENTION OF ELECTRONIC  
7 4 RECORDS.

7 5 1. a. Where a rule of law requires that certain  
7 6 documents, records, or information be retained, that  
7 7 requirement is met by retaining electronic records of the  
7 8 information, provided that all of the following conditions are  
7 9 satisfied:

7 10 (1) The electronic record and the information contained in  
7 11 the electronic record must be accessible so as to be usable  
7 12 for subsequent reference at all times when such information  
7 13 must be retained.

7 14 (2) The information must be retained in the format in  
7 15 which it was originally generated, sent, or received; or in a  
7 16 format that can be demonstrated to represent accurately the  
7 17 information originally generated, sent, or received.

7 18 (3) Data is retained which enables the identification of  
7 19 the origin and destination of the information, the  
7 20 authenticity and integrity of the information, and the date  
7 21 and time when it was generated, sent, or received.

7 22 b. An obligation to retain documents, records, or  
7 23 information in accordance with this subsection does not extend  
7 24 to any data the sole purpose of which is to enable the record  
7 25 to be sent or received.

7 26 2. Nothing in this section shall preclude any federal or  
7 27 government agency from specifying additional requirements for  
7 28 the retention of records that are subject to the jurisdiction  
7 29 of such agency.

7 30 SUBCHAPTER 3  
7 31 SECURE ELECTRONIC RECORDS AND SIGNATURES

7 32 Sec. 111. NEW SECTION. 554C.301 SECURE ELECTRONIC  
7 33 RECORD.

7 34 1. Subject to the provisions of section 554C.303, if, by  
7 35 the application of a qualified security procedure, it can be  
8 1 verified that an electronic record has not been altered since  
8 2 a specified point in time, such electronic record shall be  
8 3 considered to be a secure electronic record from such  
8 4 specified point in time to the time of verification.

8 5 2. For purposes of this subchapter, a qualified security  
8 6 procedure is a security procedure to detect changes in content  
8 7 that is any of the following:

8 8 a. Authorized by, and implemented in accordance with the  
8 9 requirements of, this chapter.

8 10 b. Previously agreed to by the parties, and implemented in  
8 11 accordance with the terms of such agreement.

8 12 c. Certified by the commissioner as providing reliable

8 13 evidence that an electronic record has not been altered, and  
8 14 implemented in a manner specified by the certification.

8 15 Sec. 112. NEW SECTION. 554C.302 SECURE ELECTRONIC  
8 16 SIGNATURE.

8 17 1. Subject to the provisions of section 554C.303, if, by  
8 18 the application of a qualified security procedure, it can be  
8 19 authenticated that an electronic signature is the signature of  
8 20 a specific person, the electronic signature shall be  
8 21 considered to be a secure electronic signature at the time of  
8 22 verification.

8 23 2. A qualified security procedure for purposes of this  
8 24 section is a security procedure for identifying a party that  
8 25 is any of the following:

8 26 a. Authorized by, and implemented in accordance with the  
8 27 requirements of, this chapter.

8 28 b. Previously agreed to by the parties to an agreement,  
8 29 and implemented in accordance with the terms of the agreement.

8 30 c. Certified by the commissioner as being capable of  
8 31 creating an electronic signature that meets all of the  
8 32 following conditions:

8 33 (1) Is unique to the signer within the context in which it  
8 34 is used.

8 35 (2) Can be used to promptly, objectively, and  
9 1 automatically identify the person signing the electronic  
9 2 record.

9 3 (3) Was reliably created by such identified person.

9 4 (4) Is linked to the electronic record to which it relates  
9 5 in a manner which ensures that if the record or signature is  
9 6 changed the electronic signature is invalidated, provided that  
9 7 the security procedure is implemented in a manner required by  
9 8 the certification.

9 9 Sec. 113. NEW SECTION. 554C.303 COMMERCIALY REASONABLE  
9 10 RELIANCE.

9 11 1. An electronic record or electronic signature that  
9 12 qualifies for secure status pursuant to section 554C.301,  
9 13 554C.302, 554C.412, or 554C.413 shall not be considered secure  
9 14 unless the proponent establishes all of the following:

9 15 a. Use of the applicable security procedure was  
9 16 commercially reasonable.

9 17 b. The security procedure was implemented in a trustworthy  
9 18 manner or, where applicable, in a manner specified by this  
9 19 chapter or the commissioner, to the extent such information is  
9 20 within the knowledge of the proponent.

9 21 c. Reliance on the security procedure was reasonable and  
9 22 in good faith in light of all the circumstances known to the  
9 23 proponent at the time of the reliance, having due regard for  
9 24 all of the following:

9 25 (1) Information that the proponent knew or had notice of  
9 26 at the time of reliance, including all facts, statements, and  
9 27 limitations contained in any statement by any third party  
9 28 involved in the authentication process.

9 29 (2) The value or importance of the electronic record  
9 30 signed with the secure electronic signature, if known.

9 31 (3) Any course of dealing between the proponent and the  
9 32 purported sender and the available indicia of reliability or  
9 33 unreliability apart from the secure electronic signature.

9 34 (4) Any usage of trade, particularly trade conducted by  
9 35 trustworthy systems or other computer-based means.

10 1 (5) Whether the authentication was performed with the  
10 2 assistance of an independent third party.

10 3 (6) Any other evidence relating to facts of which the  
10 4 proponent was aware that would suggest that reliance was or  
10 5 was not reasonable.

10 6 2. The commercial reasonableness of a security procedure  
10 7 is to be determined by the trier of fact in light of the  
10 8 purposes of the procedure and the commercial circumstances at  
10 9 the time the procedure was used, including but not limited to

10 10 the nature of the transaction, sophistication of the parties,  
10 11 volume of similar transactions engaged in by either or both of  
10 12 the parties, availability of alternatives offered to but  
10 13 rejected by either of the parties, cost of alternative  
10 14 procedures, and procedures in general use for similar types of  
10 15 transactions.

10 16 Sec. 114. NEW SECTION. 554C.304 PRESUMPTIONS.

10 17 1. In resolving a civil dispute involving a secure  
10 18 electronic record, it shall be rebuttably presumed that the  
10 19 electronic record has not been altered since the specific  
10 20 point in time to which the secure status relates.

10 21 2. In resolving a civil dispute involving a secure  
10 22 electronic signature, all of the following shall be rebuttably  
10 23 presumed:

10 24 a. The secure electronic signature is the signature of the  
10 25 person to whom it correlates.

10 26 b. The secure electronic signature was affixed by that  
10 27 person with the intention of signing the electronic record.

10 28 3. The effect of the presumptions provided in this section  
10 29 is to place on the party challenging the integrity of a secure  
10 30 electronic record or challenging the genuineness of a secure  
10 31 electronic signature both the burden of going forward with  
10 32 evidence to rebut the presumption and the burden of persuading  
10 33 the trier of fact that the falsity of the presumed fact is  
10 34 more probable than the truth of its existence.

10 35 4. In the absence of a secure electronic record or a  
11 1 secure electronic signature, nothing in this chapter shall  
11 2 change existing rules regarding legal or evidentiary rules  
11 3 regarding the burden of proving the authenticity and integrity  
11 4 of an electronic record or an electronic signature.

11 5 Sec. 115. NEW SECTION. 554C.305 ATTRIBUTION OF SIGNATURE  
11 6 TO A PARTY.

11 7 1. Except as provided by another applicable rule of law,  
11 8 and subject to the provisions of section 554C.304, a secure  
11 9 electronic signature is attributable to the person to whom it  
11 10 correlates, whether or not authorized, if all of the following  
11 11 apply to the electronic signature:

11 12 a. The signature resulted from acts of a person who  
11 13 obtained the access numbers, codes, computer programs, or  
11 14 other information necessary to create the signature from a  
11 15 source under the control of the alleged signer, creating the  
11 16 appearance that it came from the person to whom it correlates.

11 17 b. The access occurred under circumstances constituting a  
11 18 failure to exercise reasonable care by the person to whom it  
11 19 correlates.

11 20 c. The recipient reasonably relied to the recipient's  
11 21 detriment on the apparent source of the electronic record,  
11 22 taking into account the factors provided in section 554C.303.

11 23 2. The provisions of this section shall not apply to  
11 24 consumer transactions, including but not limited to credit  
11 25 card and automatic teller machines, except to the extent  
11 26 allowed by applicable consumer law.

11 27 Sec. 116. NEW SECTION. 554C.306 CERTIFICATION BY THE  
11 28 COMMISSIONER.

11 29 1. A security procedure may be certified by the  
11 30 commissioner as meeting the requirements of section 554C.301  
11 31 or 554C.302, following an appropriate investigation or review,  
11 32 if all of the following apply:

11 33 a. The technology utilized by the security procedure is  
11 34 completely open and fully disclosed to the public in order to  
11 35 facilitate a comprehensive evaluation of its suitability for  
12 1 its intended purpose.

12 2 b. The certification is in accordance with the rules  
12 3 adopted by the commissioner pursuant to chapter 17A.

12 4 c. The certification specifies at least all of the  
12 5 following:

12 6 (1) A full and complete identification of the security

12 7 procedure.

12 8 (2) A specification of one or more acceptable trustworthy  
12 9 methods by which the security procedure may be implemented  
12 10 consistent with the certification.

12 11 (3) A term for the certification which shall not exceed  
12 12 five years.

12 13 2. At the end of the term for each certified security  
12 14 procedure, or earlier as determined by the commissioner, the  
12 15 security procedure may be reevaluated in light of then-current  
12 16 technology and recertified or decertified as appropriate.

#### 12 17 SUBCHAPTER 4

### 12 18 DIGITAL SIGNATURES

#### 12 19 PART 1

#### 12 20 DEFINITIONS

12 21 Sec. 117. NEW SECTION. 554C.401 DEFINITIONS.

12 22 As used in this subchapter, unless the context otherwise  
12 23 requires:

12 24 1. "Asymmetric cryptosystem" means a computer-based system  
12 25 capable of generating and using a key pair, consisting of a  
12 26 private key for creating a digital signature, and a public key  
12 27 to verify the digital signature.

12 28 2. "Certificate" means a record that at a minimum provides  
12 29 all of the following:

12 30 a. Identifies the certification authority issuing the  
12 31 certificate.

12 32 b. Names or otherwise identifies its subscriber.

12 33 c. Contains a public key that corresponds to a private key  
12 34 under the control of the subscriber.

12 35 d. Identifies its operational period.

13 1 e. Is digitally signed by the certification authority  
13 2 issuing the certification.

13 3 3. "Certification authority" means a person who authorizes  
13 4 and causes the issuance of a certificate.

13 5 4. "Certification practice statement" means a statement  
13 6 published by a certification authority or person operating a  
13 7 repository that specifies the policies or practices that the  
13 8 certification authority employs in issuing, suspending, and  
13 9 revoking certificates, and providing access to a certificate.

13 10 5. "Correspond" means to belong to the same key pair.

13 11 6. "Digital signature" means a type of an electronic  
13 12 signature consisting of a transformation of an electronic  
13 13 record using a message digest function that is encrypted with  
13 14 an asymmetric cryptosystem using the signer's private key in a  
13 15 manner providing that any person having the initial  
13 16 untransformed electronic record, the encrypted transformation,  
13 17 and the signer's public key may accurately determine all of  
13 18 the following:

13 19 a. Whether the transformation was created using the  
13 20 private key that corresponds to the signer's public key.

13 21 b. Whether the initial electronic record has been altered  
13 22 since the transformation was made. A digital signature is a  
13 23 security procedure.

13 24 7. "Key pair" means, in an asymmetric cryptosystem, two  
13 25 mathematically related keys, having the properties that  
13 26 provide all of the following:

13 27 a. One key can encrypt a message which only the other key  
13 28 can decrypt.

13 29 b. Even knowing one key, it is computationally infeasible  
13 30 to discover the other key.

13 31 8. "Message digest function" means an algorithm that maps  
13 32 or translates the sequence of bits comprising an electronic  
13 33 record into another, generally smaller, set of bits, referred  
13 34 to as the message digest, without requiring the use of any  
13 35 secret information such as a key, in a manner which provides  
14 1 all of the following:

14 2 a. A record yields the same message digest every time the  
14 3 algorithm is executed using such record as input.

14 4 b. It is computationally infeasible that any two  
14 5 electronic records can be found or deliberately generated that  
14 6 would produce the same message digest using the algorithm  
14 7 unless the two records are identical.

14 8 9. "Operational period of a certificate" means a period  
14 9 beginning and ending as follows:

14 10 a. The period begins on the date and at the time the  
14 11 certificate is issued by a certification authority or on a  
14 12 later date and at a time certain if stated in the certificate.

14 13 b. The period ends on the date and at the time the  
14 14 certificate expires as noted in the certificate or on an  
14 15 earlier date if the certificate is revoked or suspended in  
14 16 accordance with this chapter.

14 17 10. "Private key" means the key of a key pair used to  
14 18 create a digital signature.

14 19 11. "Public key" means the key of a key pair used to  
14 20 verify a digital signature.

14 21 12. "Repository" means a system for storing and retrieving  
14 22 certificates or other information relevant to certificates.

14 23 13. "Revoke a certificate" means to permanently end the  
14 24 operational period of a certificate from a specified time  
14 25 forward.

14 26 14. "Subscriber" means a person to whom all of the  
14 27 following applies:

14 28 a. The person is the subject named or otherwise identified  
14 29 in a certificate issued to the person.

14 30 b. The person controls a private key that corresponds to  
14 31 the public key listed in that certificate.

14 32 c. The digitally signed messages verified by reference to  
14 33 the certificate are to be attributed to the person.

14 34 15. "Suspend a certificate" means to temporarily suspend  
14 35 the operational period of a certificate for a specified time  
15 1 period or from a specified time forward.

15 2 16. "Trustworthy system" means a system of computer  
15 3 hardware, software, and procedures that satisfies all of the  
15 4 following:

15 5 a. Is reasonably secure from intrusion and misuse.

15 6 b. Provides a reasonable level of availability,  
15 7 reliability, and correct operation.

15 8 c. Is reasonably suited to performing the system's  
15 9 intended functions.

15 10 d. Adheres to generally accepted security procedures.

15 11 e. Meets or exceeds the requirements of rules adopted by  
15 12 the commissioner.

15 13 17. "Valid certificate" means a certificate that meets the  
15 14 following conditions:

15 15 a. The certificate has been issued by a certification  
15 16 authority.

15 17 b. The subscriber listed in the certificate has accepted  
15 18 the certificate in accordance with this chapter.

15 19 18. "Verify a digital signature" means to use the public  
15 20 key listed in a certificate, together with an appropriate  
15 21 message digest function and public key algorithm, to evaluate  
15 22 a digitally signed electronic record in order to determine all  
15 23 of the following:

15 24 a. That the digital signature was created using the  
15 25 private key corresponding to the public key listed in the  
15 26 certificate.

15 27 b. The electronic record has not been altered since its  
15 28 digital signature was created.

#### 15 29 PART 2

#### 15 30 EFFECT OF A DIGITAL SIGNATURE

15 31 Sec. 118. NEW SECTION. 554C.411 SECURE ELECTRONIC  
15 32 RECORD.

15 33 Subject to the provisions of section 554C.303, an  
15 34 electronic record or any portion thereof that is signed with a  
15 35 digital signature shall be considered to be a secure

16 1 electronic record if the digital signature was created during  
16 2 the operational period of a valid certificate and is verified  
16 3 by reference to the public key listed in such certificate.

16 4 Sec. 119. NEW SECTION. 554C.412 SECURE ELECTRONIC  
16 5 SIGNATURE.

16 6 Subject to the provisions of section 554C.303, when all or  
16 7 any portion of an electronic record is signed with a digital  
16 8 signature, the digital signature shall be considered a secure  
16 9 electronic signature with respect to all or that portion of  
16 10 the record, if all of the following apply:

16 11 1. The digital signature was created during the  
16 12 operational period of a valid certificate, was used within any  
16 13 limits specified or incorporated by reference in the  
16 14 certificate, and can be verified by reference to the public  
16 15 key listed in the certificate.

16 16 2. The certificate shall be considered trustworthy, if one  
16 17 of the following is determined by the trier of fact:

16 18 a. The certificate was issued by a certification authority  
16 19 in accordance with standards, procedures, and other  
16 20 requirements specified by rule of the commissioner.

16 21 b. A trier of fact independently finds one of the  
16 22 following:

16 23 (1) That the certificate was issued in a trustworthy  
16 24 manner by a certification authority that properly  
16 25 authenticated the subscriber and the subscriber's public key.

16 26 (2) The material information set forth in the certificate  
16 27 is true.

16 28 3. The process and systems utilized to create and verify a  
16 29 digital signature are considered trustworthy because one of  
16 30 the following applies:

16 31 a. They comply with standards, procedures, and other  
16 32 requirements specified by the commissioner.

16 33 b. A trier of fact independently finds that they are  
16 34 trustworthy.

16 35 Sec. 120. NEW SECTION. 554C.413 COMMISSIONER AUTHORITY TO  
17 1 ADOPT RULES.

17 2 1. The commissioner may adopt rules applicable to the  
17 3 public or private sector which define when a certificate and a  
17 4 digital signature is considered sufficiently trustworthy in  
17 5 order to ensure that a digital signature verified by reference  
17 6 to the certificate will qualify as a secure electronic  
17 7 signature. The rules may include but are not limited to any  
17 8 of the following:

17 9 a. Establishing or adopting standards applicable to  
17 10 certification authorities or certificates. Compliance with  
17 11 the standards may be measured by obtaining a voluntary  
17 12 certification from the commissioner or becoming accredited by  
17 13 one or more independent accrediting entities recognized by the  
17 14 commissioner.

17 15 b. Establishing or adopting standards applicable to the  
17 16 digital signature creation or verification process.

17 17 2. In adopting rules as provided in this section, the  
17 18 commissioner shall consult with the office of the attorney  
17 19 general and representatives of the division of information  
17 20 technology services of the department of general services.  
17 21 The commissioner shall adopt rules that will provide maximum  
17 22 flexibility in the implementation of digital signature  
17 23 technology and the business models necessary to support it,  
17 24 establish a clear basis for the recognition of certificates  
17 25 issued by foreign certification authorities, and, to the  
17 26 extent reasonably possible, maximize the opportunities for  
17 27 uniformity with the laws of other jurisdictions, both within  
17 28 the United States and internationally.

17 29 PART 3

17 30 DUTIES GENERALLY

17 31 Sec. 121. NEW SECTION. 554C.421 RELIANCE ON  
17 32 CERTIFICATES.

17 33 A person relying on a digital signature may also rely on a  
17 34 valid certificate containing the public key by which the  
17 35 digital signature can be verified.

18 1 Sec. 122. NEW SECTION. 554C.422 RESTRICTIONS ON  
18 2 PUBLICATION OF CERTIFICATE.

18 3 A person shall not publish a certificate, or otherwise make  
18 4 it available to anyone known by that person to be in a  
18 5 position to rely on the certificate or on a digital signature  
18 6 that is verifiable with reference to the public key listed in  
18 7 the certificate, if that person knows that any of the  
18 8 following apply:

18 9 1. The certification authority listed in the certificate  
18 10 has not issued the certificate.

18 11 2. The subscriber listed in the certificate has not  
18 12 accepted the certificate.

18 13 3. The certificate has been revoked or suspended, unless  
18 14 the publication is for the purpose of verifying a digital  
18 15 signature created prior to such suspension or revocation.

18 16 Sec. 123. NEW SECTION. 554C.423 FRAUDULENT PURPOSE.

18 17 A person shall not knowingly create, publish, alter, or  
18 18 otherwise use a certificate for a fraudulent or other unlawful  
18 19 purpose. A person convicted of violating this section is  
18 20 guilty of a serious misdemeanor. A person convicted of a  
18 21 second or subsequent violation is guilty of a class "D"  
18 22 felony.

18 23 Sec. 124. NEW SECTION. 554C.424 FALSE OR UNAUTHORIZED  
18 24 REQUEST.

18 25 A person shall not knowingly misrepresent the person's  
18 26 identity or authorization in requesting or accepting a  
18 27 certificate or in requesting suspension or revocation of a  
18 28 certificate. A person convicted of violating this section is  
18 29 guilty of a serious misdemeanor. A person convicted of a  
18 30 second or subsequent violation is guilty of a class "D"  
18 31 felony.

#### 18 32 PART 4

18 33 DUTIES OF CERTIFICATION AUTHORITIES AND REPOSITORIES

18 34 Sec. 125. NEW SECTION. 554C.431 TRUSTWORTHY SYSTEM.

18 35 A certification authority and a person maintaining a  
19 1 repository shall utilize a trustworthy system in performing  
19 2 their services.

19 3 Sec. 126. NEW SECTION. 554C.432 DISCLOSURE.

19 4 1. For each certificate it issues, a certification  
19 5 authority must publish to relying parties all of the  
19 6 following:

19 7 a. Its certification practice statement, if the authority  
19 8 has one.

19 9 b. Its certification authority certificate that identifies  
19 10 the certification authority as a self-certifying subscriber  
19 11 and that contains the public key corresponding to the private  
19 12 key used by that certification authority to digitally sign the  
19 13 certificate.

19 14 c. Notice of a revocation or suspension of its  
19 15 certification authority certificate, and any other fact  
19 16 material relating to either the reliability of a certificate  
19 17 that it has issued or its ability to perform its services.

19 18 2. In the event of an occurrence that materially and  
19 19 adversely affects a certification authority's trustworthy  
19 20 system or its certification authority certificate, the  
19 21 certification authority must do all of the following:

19 22 a. Use reasonable efforts to notify persons who are known  
19 23 to be or foreseeably will be affected by that occurrence.

19 24 b. Act in accordance with procedures governing this type  
19 25 of occurrence specified in its certification practice  
19 26 statement.

19 27 3. If a certification authority certifies itself as a  
19 28 certification authority, it shall disclose to all relying  
19 29 parties that it is self-certified. The certification

19 30 authority shall publish a copy of its own certification  
19 31 authority certificate that is verifiable by reference to a  
19 32 public key listed in a certificate issued by the certification  
19 33 authority.

19 34 Sec. 127. NEW SECTION. 554C.433 ISSUANCE OF A  
19 35 CERTIFICATE.

20 1 A certification authority may issue a certificate to a  
20 2 prospective subscriber for the purpose of verifying digital  
20 3 signatures only after the certification authority does all of  
20 4 the following:

20 5 1. Receives a request for the issuance from the  
20 6 prospective subscriber.

20 7 2. Does either of the following:

20 8 a. Complies with all of the practices and procedures set  
20 9 forth in its applicable certification practice statement,  
20 10 including procedures regarding identification of the  
20 11 perspective subscriber.

20 12 b. In the absence of a certification practice statement,  
20 13 confirms one of the following:

20 14 (1) The prospective subscriber is the person to be listed  
20 15 in the certificate to be issued.

20 16 (2) The information in the certificate to be issued is  
20 17 accurate.

20 18 (3) The prospective subscriber rightfully holds a private  
20 19 key capable of creating a digital signature, and the public  
20 20 key to be listed in the certificate can be used to verify a  
20 21 digital signature affixed by such private key.

20 22 Sec. 128. NEW SECTION. 554C.434 REPRESENTATIONS UPON  
20 23 ISSUANCE OF CERTIFICATE.

20 24 By issuing a certificate, a certification authority  
20 25 represents to any person who reasonably relies on the  
20 26 certificate or a digital signature verifiable by the public  
20 27 key listed in the certificate, that the certification  
20 28 authority has issued the certificate in accordance with any  
20 29 applicable certification practice statement stated or  
20 30 incorporated by reference in the certificate, or of which the  
20 31 relying person has notice, and the requirements and  
20 32 representations imposed by the law under which it was issued.  
20 33 In the absence of a certification practice statement or law,  
20 34 the certification authority represents that as of the time the  
20 35 certificate is issued it has confirmed all of the following:

21 1 1. The certification authority has complied with all  
21 2 applicable requirements of this chapter in issuing the  
21 3 certificate, and if the certification authority has published  
21 4 the certificate or otherwise made it available to a relying  
21 5 person, that the subscriber identified in the certificate has  
21 6 accepted it.

21 7 2. The subscriber identified in the certificate,  
21 8 rightfully holds the private key corresponding to the public  
21 9 key listed in the certificate.

21 10 3. The subscriber's public key and private key constitute  
21 11 a functioning key pair.

21 12 4. All information in the certificate is accurate as of  
21 13 the date it was issued, unless the certification authority has  
21 14 stated in the certificate or incorporated by reference in the  
21 15 certificate a statement that the accuracy of specified  
21 16 information is not confirmed.

21 17 5. To the knowledge of the certification authority, there  
21 18 are no known material facts omitted from the certificate which  
21 19 would, if known, adversely affect the reliability of the  
21 20 representations required to be provided by the certification  
21 21 authority under this section.

21 22 Sec. 129. NEW SECTION. 554C.435 SUSPENSION OF A  
21 23 CERTIFICATE.

21 24 The certification authority that issues a certificate, and  
21 25 any person maintaining a repository where the certificate is  
21 26 published, shall suspend the certificate pursuant to any of

21 27 the following:

21 28 1. The receipt of an order issued by a court of competent  
21 29 jurisdiction.

21 30 2. In accordance with the policies and procedures  
21 31 governing suspension specified in its certification practice  
21 32 statement. In the absence of policies and procedures  
21 33 governing suspension, the certificate shall be suspended as  
21 34 soon as possible after receiving a request by a person whom  
21 35 the certification authority or person maintaining a repository  
22 1 reasonably believes to be any of the following:

22 2 a. The subscriber listed in the certificate.

22 3 b. A person duly authorized to act for that subscriber.

22 4 c. A person acting on behalf of that subscriber, who is  
22 5 unavailable.

22 6 Sec. 130. NEW SECTION. 554C.436 REVOCATION OF A  
22 7 CERTIFICATE.

22 8 The certification authority that issues a certificate, and  
22 9 any person maintaining a repository where the certificate is  
22 10 published, shall revoke the certificate pursuant to any of the  
22 11 following:

22 12 1. Upon receipt of an order issued by a court of competent  
22 13 jurisdiction.

22 14 2. In accordance with the policies and procedures  
22 15 governing revocation specified in its certification practice  
22 16 statement. In the absence of policies and procedures  
22 17 governing revocation, the certificate shall be revoked as soon  
22 18 as possible after one of the following occurs:

22 19 a. Receipt of a request for revocation by the subscriber  
22 20 named in the certificate, if the certification authority or  
22 21 repository confirms that the person requesting the revocation  
22 22 is the subscriber or is an agent of the subscriber with  
22 23 authority to request the revocation.

22 24 b. Receipt of a certified copy of an individual  
22 25 subscriber's death certificate, or upon confirmation by other  
22 26 reliable evidence that the subscriber is dead.

22 27 c. Presentation of documents effecting a dissolution of a  
22 28 corporate subscriber, or upon confirmation by other evidence  
22 29 that the subscriber has been dissolved or has ceased to exist.

22 30 d. Confirmation by the certification authority that one of  
22 31 the following applies:

22 32 (1) A material fact represented in the certificate is  
22 33 false.

22 34 (2) A material prerequisite to issuance of the certificate  
22 35 was not satisfied.

23 1 (3) The certification authority's private key or  
23 2 trustworthy system was compromised in a manner materially  
23 3 affecting the certificate's reliability.

23 4 (4) The subscriber's private key or trustworthy system was  
23 5 compromised.

23 6 Upon effecting a revocation, the certification authority  
23 7 shall promptly notify the subscriber listed in the revoked  
23 8 certificate of the revocation.

23 9 Sec. 131. NEW SECTION. 554C.437 NOTICE OF SUSPENSION OR  
23 10 REVOCATION.

23 11 Upon suspending or revoking a certificate, a person  
23 12 maintaining a repository where the certificate is published  
23 13 shall do all of the following:

23 14 1. Promptly publish notice of the suspension or revocation  
23 15 if the certificate was published.

23 16 2. Disclose the fact of suspension or revocation on  
23 17 inquiry by a relying party.

23 18 PART 5

23 19 DUTIES OF SUBSCRIBERS

23 20 Sec. 132. NEW SECTION. 554C.441 GENERATING THE KEY PAIR.

23 21 If the subscriber generates the key pair whose public key  
23 22 is to be listed in a certificate issued by a certification  
23 23 authority and accepted by the subscriber, the subscriber must

23 24 generate that key pair and maintain and store the private key  
23 25 using a trustworthy system.

23 26 Sec. 133. NEW SECTION. 554C.442 OBTAINING A CERTIFICATE.

23 27 All material representations made by the subscriber to a  
23 28 certification authority for purposes of obtaining a  
23 29 certificate must be accurate and complete.

23 30 Sec. 134. NEW SECTION. 554C.443 ACCEPTANCE OF A  
23 31 CERTIFICATE.

23 32 1. A person accepts a certificate that names a person as a  
23 33 subscriber by publishing it to one or more persons, depositing  
23 34 the certificate in a repository, or demonstrating approval of  
23 35 the certificate, while knowing or having notice of its  
24 1 contents.

24 2 2. By accepting a certificate, the subscriber listed in  
24 3 the certificate represents to all who reasonably rely on the  
24 4 information contained in the certificate that all of the  
24 5 following apply:

24 6 a. The subscriber rightfully holds the private key  
24 7 corresponding to the public key listed in the certificate.

24 8 b. All representations made by the subscriber to the  
24 9 certification authority and material to the information listed  
24 10 in the certificate are true.

24 11 c. All information in the certificate that is within the  
24 12 knowledge of the subscriber is true.

24 13 Sec. 135. NEW SECTION. 554C.444 CONTROL OF THE PRIVATE  
24 14 KEY.

24 15 1. Except as otherwise provided by another applicable rule  
24 16 of law, by accepting a certificate issued by a certification  
24 17 authority the subscriber identified in the certificate assumes  
24 18 a duty to persons who reasonably rely on the certificate to  
24 19 exercise reasonable care to retain control of the private key  
24 20 corresponding to the public key listed in the certificate and  
24 21 to prevent its disclosure to a person not authorized to create  
24 22 the subscriber's digital signature. The requirements of this  
24 23 subsection shall continue during the operational period of the  
24 24 certificate.

24 25 2. The provisions of this section do not apply to consumer  
24 26 transactions.

24 27 Sec. 136. NEW SECTION. 554C.445 INITIATING SUSPENSION OR  
24 28 REVOCATION.

24 29 Except as otherwise provided by another applicable rule of  
24 30 law, if the private key corresponding to the public key listed  
24 31 in a certificate is compromised during the operational period  
24 32 of the certificate, a subscriber who has accepted the  
24 33 certificate shall do one of the following:

24 34 1. Request the issuing certification authority, and all  
24 35 independent repositories in which the subscriber has  
25 1 authorized the certificate to be published, to suspend or  
25 2 revoke the certificate.

25 3 2. Provide reasonable notice to all relying parties that  
25 4 the public key listed in the certificate was compromised  
25 5 during the operational period of the certificate.

25 6 PART 6  
25 7 GOVERNMENT AGENCY USE OF ELECTRONIC RECORDS AND SIGNATURES

25 8 Sec. 137. NEW SECTION. 554C.451 GOVERNMENT AGENCY USE OF  
25 9 ELECTRONIC RECORDS.

25 10 1. Each government agency shall determine if, and the  
25 11 extent to which, it will send and receive electronic records  
25 12 and electronic signatures to and from other persons.

25 13 2. In any case where a government agency decides to send  
25 14 or receive electronic records, or to accept document filings  
25 15 by electronic records, the government agency may, by rule,  
25 16 giving due consideration to security, specify any of the  
25 17 following:

25 18 a. The manner and format in which electronic records must  
25 19 be sent, received, and stored, including interoperability  
25 20 requirements.

25 21 b. If electronic records must be signed, the type of  
25 22 electronic signature required including, if applicable, a  
25 23 requirement that the sender use a digital signature or other  
25 24 secure electronic signature, the manner and format in which  
25 25 the electronic signature must be affixed to the electronic  
25 26 record, and the identity of or criteria that must be met by a  
25 27 certification authority used by the person filing the  
25 28 document.

25 29 c. Control processes and procedures which are appropriate  
25 30 to ensure adequate integrity, security, confidentiality, and  
25 31 auditability of electronic records.

25 32 d. Any other required attributes for electronic records  
25 33 that are currently specified for corresponding paper  
25 34 documents, or reasonably necessary under the circumstances.

25 35 3. All rules adopted by a government agency shall be  
26 1 consistent with the rules adopted by the commissioner.

26 2 Sec. 138. NEW SECTION. 554C.452 COMMISSIONER TO ADOPT  
26 3 STATE STANDARDS.

26 4 1. The commissioner, in consultation with the office of  
26 5 the attorney general and the division of information  
26 6 technology services of the department of general services,  
26 7 shall adopt rules setting forth standards, procedures, and  
26 8 policies for the use of electronic records and electronic  
26 9 signatures by government agencies. Where appropriate, the  
26 10 rules shall specify different levels of standards from which  
26 11 implementing government agencies can select the standard most  
26 12 appropriate for a particular application.

26 13 2. The commissioner shall specify appropriate procedural  
26 14 and technical security requirements to be implemented and  
26 15 followed by government agencies for all of the following:

26 16 a. The generation, use, and storage of key pairs.

26 17 b. The issuance, acceptance, use, suspension, and  
26 18 revocation of certificates.

26 19 c. The use of digital signatures.

26 20 3. Each government agency shall have the authority to  
26 21 issue, or contract for the issuance of, certificates to all of  
26 22 the following:

26 23 a. Its employees and agents.

26 24 b. Persons conducting business or other transactions with  
26 25 the government agency. The government agency may take other  
26 26 actions consistent with this authority, including the  
26 27 establishment of repositories and the suspension or revocation  
26 28 of issued certificates, provided that actions by the  
26 29 government agency are conducted in accordance with all rules,  
26 30 procedures, and policies specified by the commissioner. The  
26 31 commissioner may adopt rules, procedures, and policies under  
26 32 which government agencies may issue or contract for the  
26 33 issuance of certificates, or restrict or prohibit their  
26 34 issuance.

26 35 4. The commissioner may specify appropriate standards and  
27 1 requirements that must be satisfied by a certification  
27 2 authority before any of the following occur:

27 3 a. The services of a certification authority are used by a  
27 4 government agency for the issuance, publication, suspension,  
27 5 or revocation of certificates to the government agency,  
27 6 including its employees or agents, for official use only.

27 7 b. The certificates that the certification authority  
27 8 issues are accepted for purposes of verifying digitally signed  
27 9 electronic records sent to any government agency by any  
27 10 person.

27 11 Sec. 139. NEW SECTION. 554C.453 INTEROPERABILITY.

27 12 To the extent reasonable under the circumstances, rules  
27 13 adopted by the commissioner or a government agency relating to  
27 14 the use of electronic records or electronic signatures shall  
27 15 be drafted in a manner designed to encourage and promote  
27 16 consistency and interoperability with similar requirements  
27 17 adopted by government agencies of other states and the federal

27 18 government.

27 19

DIVISION II

27 20

CONFORMING PROVISIONS

27 21 Sec. 201. Section [22.7](#), Code Supplement 1997, is amended  
27 22 by adding the following new subsection:

27 23 NEW SUBSECTION. 38. a. Records containing information  
27 24 that would disclose, or might lead to the disclosure of,  
27 25 private keys as provided in section 554C.

27 26 b. Records which if disclosed might jeopardize the  
27 27 security of an issued certificate or a certificate to be  
27 28 issued pursuant to chapter 554C.

27 29 Sec. 202. COMMISSIONER REQUIRED TO ADOPT RULES. The  
27 30 commissioner of insurance shall adopt rules as required by  
27 31 this Act not later than July 1, 1999.

27 32

EXPLANATION

27 33 This bill relates to electronic commerce security.

27 34 The bill creates a new Code chapter relating to electronic  
27 35 commerce referred to as new Code chapter 554C.

28 1 New Code section 554C.101 provides the short title for the  
28 2 chapter, referred to as the "Iowa Electronic Commerce Security  
28 3 Act".

28 4 New Code section 554C.102 provides for the purposes and  
28 5 construction of the chapter. The bill provides that the  
28 6 chapter must be construed consistently with what is  
28 7 commercially reasonable under the circumstances to effectuate  
28 8 electronic communications by means of reliable electronic  
28 9 records; facilitate and promote electronic commerce by  
28 10 eliminating certain present barriers; facilitate the  
28 11 electronic filing of documents with state and local government  
28 12 agencies; minimizing the incidence of forged electronic  
28 13 records; establishing uniformity of regulations and standards;  
28 14 promoting public confidence in the integrity, reliability, and  
28 15 legality of electronic records and electronic commerce.

28 16 New Code section 554C.103 provides for variation by  
28 17 agreement between parties involved in generating, sending,  
28 18 receiving, storing, or otherwise processing electronic  
28 19 records. The bill provides certain exceptions. It also  
28 20 provides that the bill is not to be construed to require a  
28 21 person to engage in electronic commerce.

28 22 New Code section 554C.201 provides for definitions as used  
28 23 in the chapter, including the definitions for electronic  
28 24 record and electronic signature. An "electronic record" is  
28 25 defined to mean a record generated, communicated, received,  
28 26 or stored by electronic means. An "electronic signature"  
28 27 means a signature in electronic form attached to or logically  
28 28 associated with an electronic record.

28 29 New Code section 554C.202 provides that information cannot  
28 30 be denied legal effect solely on the grounds that it is in the  
28 31 form of an electronic record or an electronic signature.

28 32 New Code section 554C.203 provides that where a rule of law  
28 33 requires information to be written, or in writing, an  
28 34 electronic record satisfies that rule of law. This  
28 35 requirement does not apply to the construction of a rule of  
29 1 law that would be inconsistent with its purpose.

29 2 New Code section 554C.204 provides that where a rule of law  
29 3 requires a signature, an electronic signature satisfies that  
29 4 rule of law. This requirement does not apply to defeat an  
29 5 expressed purpose of a rule of law; the creation or execution  
29 6 of a will or trust, living will, general, durable, or  
29 7 healthcare power of attorney, a voluntary, involuntary, or  
29 8 standby guardianship or conservatorship; any record that  
29 9 serves as a unique and transferable physical expression of  
29 10 rights and obligations in consumer transactions; or any record  
29 11 that grants a legal or equitable interest in real property in  
29 12 consumer transactions.

29 13 New Code section 554C.205 provides that where a rule of law  
29 14 requires information to be presented or retained in its

29 15 original form that rule of law is satisfied by an electronic  
29 16 record if there exists reliable assurance as to the integrity  
29 17 of the information.

29 18 New Code section 554C.206 provides that in any legal  
29 19 proceeding, nothing in the application of the rules of  
29 20 evidence shall apply to deny the admissibility of an  
29 21 electronic record or electronic signature into evidence based  
29 22 on the sole ground that it is an electronic record or  
29 23 electronic signature or it is not in its original form with  
29 24 some exceptions. The section provides that information in the  
29 25 form of an electronic record must be given due evidential  
29 26 weight by the trier of fact.

29 27 New Code section 554C.207 provides that where a rule of law  
29 28 requires that certain documents, records, or information be  
29 29 retained that requirement is met by retaining electronic  
29 30 records of the information.

29 31 New Code section 554C.301 provides for securing electronic  
29 32 records by utilizing a qualified security procedure which  
29 33 detects changes in the information's content.

29 34 New Code section 554C.302 provides for secure electronic  
29 35 signatures. It provides that an electronic signature shall be  
30 1 considered to be a secure electronic signature if executed  
30 2 utilizing a qualified security procedure.

30 3 New Code section 554C.303 provides additional requirements  
30 4 for secure status information. It provides requirements for  
30 5 proving that an electronic record or electronic signature  
30 6 qualifies for secure status, including providing for special  
30 7 procedures. The bill provides that the security procedure  
30 8 must be commercially reasonable, as determined by the trier of  
30 9 fact.

30 10 New Code section 554C.304 provides for a rebuttable  
30 11 presumption when resolving a civil dispute involving a secure  
30 12 electronic record. The bill provides for a rebuttable  
30 13 presumption relating to alterations of an electronic record  
30 14 and the legitimacy of an electronic signature. The effect of  
30 15 the presumption is to place on the party challenging the  
30 16 integrity of a secure electronic record or challenging the  
30 17 genuineness of a secure electronic signature both the burden  
30 18 of going forward with evidence to rebut the presumption and  
30 19 the burden of persuading the trier of fact that the falsity of  
30 20 the presumed fact is more probable than the truth of its  
30 21 existence.

30 22 New Code section 554C.305 provides that a secure electronic  
30 23 signature is attributable to the person to whom it correlates.  
30 24 The attribution may apply whether or not authorized, when the  
30 25 access occurred under circumstances constituting a failure to  
30 26 exercise reasonable care and the recipient reasonably relied  
30 27 to the recipient's detriment on the apparent source of the  
30 28 electronic record. Consumer transactions are excluded from  
30 29 this provision.

30 30 New Code section 554C.306 provides that a security  
30 31 procedure may be certified by the commissioner of insurance if  
30 32 the technology utilized by the security procedure is  
30 33 completely open and fully disclosed to the public, the  
30 34 certification is in accordance with the rules adopted by the  
30 35 commissioner, and the certification complies with requirements  
31 1 relating to its trustworthiness.

31 2 New Code section 554C.401 provides a number of special  
31 3 definitions which apply to digital signatures.

31 4 New Code section 554C.411 provides that an electronic  
31 5 record that is signed with a digital signature is considered  
31 6 to be a secure electronic record if the digital signature was  
31 7 created during the operational period of a valid certificate  
31 8 issued by the commissioner.

31 9 New Code section 554C.412 provides that when an electronic  
31 10 record is signed with a digital signature, the digital  
31 11 signature is considered a secure electronic signature if it

31 12 meets certain requirements. It must have been created during  
31 13 the period when a valid certificate was issued by a  
31 14 certification authority in accordance with standards,  
31 15 procedures, and other requirements specified by rule of the  
31 16 commissioner of insurance, or found to be trustworthy by the  
31 17 findings of a trier of fact.

31 18 New Code section 554C.413 provides that the commissioner of  
31 19 insurance may adopt rules applicable to the public or private  
31 20 sector which define when a certificate and a digital signature  
31 21 are considered sufficiently trustworthy.

31 22 New Code section 554C.421 provides that a person relying on  
31 23 a digital signature may also rely on a valid certificate  
31 24 containing a public key by which the digital signature can be  
31 25 verified.

31 26 New Code section 554C.422 prohibits a person from  
31 27 publishing or making available a certificate if that person  
31 28 knows that the certification authority listed in the  
31 29 certificate has not issued the certificate, the subscriber  
31 30 listed in the certificate has not accepted the certificate, or  
31 31 the certificate has been revoked or suspended.

31 32 New Code section 554C.423 prohibits a person from knowingly  
31 33 creating, publishing, altering, or otherwise using a  
31 34 certificate for a fraudulent or other unlawful purpose. A  
31 35 person convicted of violating this section is guilty of a  
32 1 serious misdemeanor. A person convicted of a second or  
32 2 subsequent violation is guilty of a class "D" felony.

32 3 New Code section 554C.424 prohibits a person from knowingly  
32 4 misrepresenting the person's identity or authorization in  
32 5 requesting or accepting a certificate or in requesting  
32 6 suspension or revocation of a certificate. A person convicted  
32 7 of violating this section is guilty of a serious misdemeanor.  
32 8 A person convicted of a second or subsequent violation is  
32 9 guilty of a class "D" felony.

32 10 New Code section 554C.431 provides that a person designated  
32 11 as a certification authority and a person maintaining a  
32 12 repository must utilize a trustworthy system in performing  
32 13 their services.

32 14 New Code section 554C.432 provides for disclose to parties  
32 15 relying upon a certification, a certification practice  
32 16 statement, a certification authority certification, and a  
32 17 notice of a revocation or suspension of its certification  
32 18 authority certificate.

32 19 New Code section 554C.433 provides for the issuance of a  
32 20 certificate to a prospective subscriber for the purpose of  
32 21 verifying digital signatures.

32 22 New Code section 554C.434 provides that by issuing a  
32 23 certificate, a certification authority represents to any  
32 24 person who reasonably relies on the certificate or a digital  
32 25 signature verifiable by the public key listed in the  
32 26 certificate, that the certification authority has issued the  
32 27 certificate in accordance with any applicable certification  
32 28 practice statement. The statement shall provide that the  
32 29 certification authority has complied with all applicable  
32 30 requirements of the bill and that all information in the  
32 31 certificate is accurate.

32 32 New Code section 554C.435 provides for the suspension of a  
32 33 certificate by the certification authority that issues a  
32 34 certificate.

32 35 New Code section 554C.436 provides that the certification  
33 1 authority that issues a certificate, and any person  
33 2 maintaining a repository where the certificate is published,  
33 3 must revoke the certificate upon receipt of an order issued by  
33 4 a court of competent jurisdiction or in accordance with the  
33 5 policies and procedures governing revocation specified in its  
33 6 certification practice statement.

33 7 New Code section 554C.437 provides for a notice of  
33 8 suspension or revocation.

33 9 New Code section 554C.441 provides that if a subscriber  
33 10 generates the key pair whose public key is to be listed in a  
33 11 certificate issued by a certification authority and accepted  
33 12 by the subscriber, the subscriber must generate that key pair  
33 13 and maintain and store the private key using a trustworthy  
33 14 system.

33 15 New Code section 554C.442 provides that all material  
33 16 representations made by the subscriber to a certification  
33 17 authority for purposes of obtaining a certificate must be  
33 18 accurate and complete.

33 19 New Code section 554C.443 provides that a person accepts a  
33 20 certificate that names a person as a subscriber by publishing  
33 21 it to one or more persons, depositing the certificate in a  
33 22 repository, or demonstrating approval of the certificate,  
33 23 while knowing or having notice of its contents.

33 24 New Code section 554C.444 provides that by accepting a  
33 25 certificate issued by a certification authority the subscriber  
33 26 identified in the certificate assumes a duty to persons who  
33 27 reasonably rely on the certificate to exercise reasonable care  
33 28 to retain control of the private key corresponding to the  
33 29 public key listed in the certificate and to prevent its  
33 30 disclosure to an unauthorized person. The provisions of this  
33 31 section do not apply to consumer transactions.

33 32 New Code section 554C.445 provides that if a private key  
33 33 corresponding to the public key listed in a certificate is  
33 34 compromised during the operational period of the certificate,  
33 35 a subscriber who has accepted the certificate must take  
34 1 security actions to protect relying parties.

34 2 New Code section 554C.451 provides that each government  
34 3 agency must determine if, and the extent to which, it will  
34 4 send and receive electronic records and electronic signatures  
34 5 to and from other persons.

34 6 New Code section 554C.452 provides that the commissioner of  
34 7 insurance, in consultation with the office of the attorney  
34 8 general and the division of information technology services of  
34 9 the department of general services, shall adopt rules setting  
34 10 forth standards, procedures, and policies for the use of  
34 11 electronic records and electronic signatures by government  
34 12 agencies.

34 13 New Code section 554C.453 provides that rules adopted by  
34 14 the insurance commissioner or a government agency relating to  
34 15 the use of electronic records or electronic signatures must be  
34 16 drafted in a manner designed to encourage and promote  
34 17 consistency and interoperability with similar requirements  
34 18 adopted by government agencies of other states and the federal  
34 19 government.

34 20 The bill provides conforming amendments. The bill requires  
34 21 that the commissioner of insurance adopt rules as required by  
34 22 the bill not later than July 1, 1999.

34 23 LSB 3386XL 77

34 24 da/jw/5