

# REPRINTED

FEB 26 1998  
Place On Calendar

HOUSE FILE 2474  
BY COMMITTEE ON COMMERCE  
AND REGULATION

(SUCCESSOR TO HSB 650)

Passed House, <sup>(R 604)</sup> Date 3/11/95  
Vote: Ayes 71 Nays 25  
Approved \_\_\_\_\_

Passed Senate, Date \_\_\_\_\_  
Vote: Ayes \_\_\_\_\_ Nays \_\_\_\_\_

## A BILL FOR

1 An Act relating to electronic commerce security, and providing  
2 penalties.

3 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22

HF 2474

DIVISION I

SUBCHAPTER 1

GENERAL

Section 101. NEW SECTION. 554C.101 SHORT TITLE.

This chapter shall be known and may be cited as the "Iowa Electronic Commerce Security Act".

Sec. 102. NEW SECTION. 554C.102 PURPOSES AND CONSTRUCTION.

This chapter shall be construed consistently with what is commercially reasonable under the circumstances and to effectuate all of the following purposes:

1. Facilitate electronic communications by means of reliable electronic records.

2. Facilitate and promote electronic commerce, by eliminating barriers resulting from uncertainties over writing and signature requirements, and promoting the development of the legal and business infrastructure necessary to implement secure electronic commerce.

3. Facilitate electronic filing of documents with state and local government agencies and promote efficient delivery of government services by means of reliable electronic records.

4. Minimize the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce.

5. Establish uniformity of rules, regulations, and standards regarding the authentication and integrity of electronic records.

6. Promote public confidence in the integrity, reliability, and legality of electronic records and electronic commerce.

Sec. 103. NEW SECTION. 554C.103 VARIATION BY AGREEMENT -- USE OF ELECTRONIC MEANS OPTIONAL.

1. As between parties involved in generating, sending, receiving, storing, or otherwise processing electronic

1 records, the provisions of this chapter may be varied by  
2 agreement of the parties. However, an agreement shall not  
3 vary requirements provided in section 554C.203, subsection 2;  
4 section 554C.204, subsection 4; section 554C.305, subsection  
5 2; sections 554C.422, 554C.423, 554C.424, and 554C.442; and  
6 section 554C.444, subsection 2.

7 2. This chapter shall not be construed to require a person  
8 to create, store, transmit, accept, or otherwise use or  
9 communicate information, records, or signatures by electronic  
10 means or in electronic form.

11 SUBCHAPTER 2

12 ELECTRONIC RECORDS AND SIGNATURES GENERALLY

13 Sec. 104. NEW SECTION. 554C.201 DEFINITIONS.

14 As used in this chapter, unless the context otherwise  
15 requires:

16 1. "Commissioner" means the commissioner of insurance  
17 appointed pursuant to section 505.2.

18 2. "Consumer transaction" means a transaction by an  
19 individual for personal, household, or family use.

20 3. "Electronic" includes electrical, digital, magnetic,  
21 optical, electromagnetic, or any other form of technology that  
22 entails capabilities similar to these technologies.

23 4. "Electronic record" means a record generated,  
24 communicated, received, or stored by electronic means for use  
25 in an information system or for transmission from one  
26 information system to another.

27 5. "Electronic signature" means a signature in electronic  
28 form attached to or logically associated with an electronic  
29 record.

30 6. "Government agency" means any executive, legislative,  
31 or judicial agency, department, board, commission, authority,  
32 institution, or instrumentality of this state or of any  
33 county, city, or other political subdivision of this state.

34 7. "Information" includes but is not limited to data,  
35 text, images, sound, codes, computer programs, software, and

1 databases.

2 8. "Party" means a person involved in an electronic  
3 transaction governed by the provisions of this chapter.

4 9. "Record" means information that is inscribed, stored,  
5 or otherwise fixed on a tangible medium or that is stored in  
6 an electronic or other medium and is retrievable in  
7 perceivable form.

8 10. "Rule of law" means any statute, rule of or order by a  
9 government agency, regulation, ordinance, common law rule, or  
10 court decision enacted, adopted, established, or rendered by  
11 the general assembly, government agency, court, political  
12 subdivision of, or other authority of, this state.

13 11. "Security procedure" means a methodology or procedure  
14 for the purpose of doing any of the following:

15 a. Verifying that an electronic record is the record of a  
16 specific person.

17 b. Detecting an error or alteration in the communication,  
18 content, or storage of an electronic record since a specific  
19 point in time. A security procedure may require the use of  
20 algorithms or codes, identifying words or numbers, encryption,  
21 answer back, acknowledgment procedures, or similar security  
22 devices.

23 12. "Signed" or "signature" includes any symbol executed  
24 or adopted, or any security procedure employed or adopted,  
25 including by use of electronic means, by or on behalf of a  
26 person with a present intention to authenticate a record.

27 Definitions used in any part of this chapter shall apply in  
28 all other parts of this chapter.

29 Sec. 105. NEW SECTION. 554C.202 LEGAL RECOGNITION.

30 Information shall not be denied legal effect, validity, or  
31 enforceability solely on the grounds that it is in the form of  
32 an electronic record or an electronic signature.

33 Sec. 106. NEW SECTION. 554C.203 ELECTRONIC RECORDS.

34 1. Where a rule of law requires information to be written  
35 or in writing or provides for certain consequences if it is

1 not, an electronic record satisfies that rule of law  
2 requirement.

3 2. The provisions of this section shall not apply to any  
4 of the following:

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

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

17 c. To any record that serves as a unique and transferable  
18 physical expression of rights and obligations including,  
19 without limitation, negotiable instruments and other  
20 instruments of title wherein possession of the instrument is  
21 deemed to confer title in a consumer transaction.

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

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

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

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

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

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

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

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

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

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

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

31 1. Where a rule of law requires information to be  
32 presented or retained in its original form, or provides  
33 consequences for information not being presented or retained  
34 in its original form, that rule of law is satisfied by an  
35 electronic record if there exists reliable assurance as to the

1 integrity of the information from the time when it was first  
2 generated in its final form, as an electronic record or  
3 otherwise.

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

12 3. The provisions of this section do not apply to any  
13 record that serves as a unique and transferable physical  
14 expression of rights and obligations including, but not  
15 limited to, negotiable instruments and other instruments of  
16 title wherein possession of the instrument is deemed to confer  
17 title.

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

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

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

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

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

1 maintained, the manner in which its originator was identified,  
2 and the manner in which the electronic record was signed.

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

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

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

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

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

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

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

30 SUBCHAPTER 3

31 SECURE ELECTRONIC RECORDS AND SIGNATURES

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

34 1. Subject to the provisions of section 554C.303, if, by  
35 the application of a qualified security procedure, it can be



1 verified that an electronic record has not been altered since  
2 a specified point in time, such electronic record shall be  
3 considered to be a secure electronic record from such  
4 specified point in time to the time of verification.

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

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

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

12 c. Certified by the commissioner as providing reliable  
13 evidence that an electronic record has not been altered, and  
14 implemented in a manner specified by the certification.

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

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

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

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

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

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

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

35 (2) Can be used to promptly, objectively, and

1 automatically identify the person signing the electronic  
2 record.

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

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

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

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

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

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

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

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

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

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

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

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

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

6 2. The commercial reasonableness of a security procedure  
7 is to be determined by the trier of fact in light of the  
8 purposes of the procedure and the commercial circumstances at  
9 the time the procedure was used, including but not limited to  
10 the nature of the transaction, sophistication of the parties,  
11 volume of similar transactions engaged in by either or both of  
12 the parties, availability of alternatives offered to but  
13 rejected by either of the parties, cost of alternative  
14 procedures, and procedures in general use for similar types of  
15 transactions.

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

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

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

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

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

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

35 4. In the absence of a secure electronic record or a

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

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

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

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

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

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

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

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

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

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

1 its intended purpose.

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

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

6 (1) A full and complete identification of the security  
7 procedure.

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

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

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

17 SUBCHAPTER 4

18 DIGITAL SIGNATURES

19 PART 1

20 DEFINITIONS

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

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

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

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

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

32 b. Names or otherwise identifies its subscriber.

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

35 d. Identifies its operational period.

- 1 e. Is digitally signed by the certification authority  
2 issuing the certification.
- 3 3. "Certification authority" means a person who authorizes  
4 and causes the issuance of a certificate.
- 5 4. "Certification practice statement" means a statement  
6 published by a certification authority or person operating a  
7 repository that specifies the policies or practices that the  
8 certification authority employs in issuing, suspending, and  
9 revoking certificates, and providing access to a certificate.
- 10 5. "Correspond" means to belong to the same key pair.
- 11 6. "Digital signature" means a type of an electronic  
12 signature consisting of a transformation of an electronic  
13 record using a message digest function that is encrypted with  
14 an asymmetric cryptosystem using the signer's private key in a  
15 manner providing that any person having the initial  
16 untransformed electronic record, the encrypted transformation,  
17 and the signer's public key may accurately determine all of  
18 the following:
- 19 a. Whether the transformation was created using the  
20 private key that corresponds to the signer's public key.
- 21 b. Whether the initial electronic record has been altered  
22 since the transformation was made. A digital signature is a  
23 security procedure.
- 24 7. "Key pair" means, in an asymmetric cryptosystem, two  
25 mathematically related keys, having the properties that  
26 provide all of the following:
- 27 a. One key can encrypt a message which only the other key  
28 can decrypt.
- 29 b. Even knowing one key, it is computationally infeasible  
30 to discover the other key.
- 31 8. "Message digest function" means an algorithm that maps  
32 or translates the sequence of bits comprising an electronic  
33 record into another, generally smaller, set of bits, referred  
34 to as the message digest, without requiring the use of any  
35 secret information such as a key, in a manner which provides

1 all of the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

34 15. "Suspend a certificate" means to temporarily suspend  
35 the operational period of a certificate for a specified time

1 period or from a specified time forward.

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

5 a. Is reasonably secure from intrusion and misuse.

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

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

10 d. Adheres to generally accepted security procedures.

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

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

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

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

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

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

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

29 PART 2

30 EFFECT OF A DIGITAL SIGNATURE

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

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



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

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

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

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

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

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

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

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

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

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

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

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

35 Sec. 120 NEW SECTION. 554C.413 COMMISSIONER AUTHORITY TO

## 1 ADOPT RULES.

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

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

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

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

## 29 PART 3

## 30 DUTIES GENERALLY

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

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



1 repository shall utilize a trustworthy system in performing  
2 their services.

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

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

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

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

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

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

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

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

27 3. If a certification authority certifies itself as a  
28 certification authority, it shall disclose to all relying  
29 parties that it is self-certified. The certification  
30 authority shall publish a copy of its own certification  
31 authority certificate that is verifiable by reference to a  
32 public key listed in a certificate issued by the certification  
33 authority.

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

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

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

7 2. Does either of the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 reasonably believes to be any of the following:

- 2 a. The subscriber listed in the certificate.
- 3 b. A person duly authorized to act for that subscriber.
- 4 c. A person acting on behalf of that subscriber, who is
- 5 unavailable.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18

PART 5

19

DUTIES OF SUBSCRIBERS

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

21 If the subscriber generates the key pair whose public key  
22 is to be listed in a certificate issued by a certification  
23 authority and accepted by the subscriber, the subscriber must  
24 generate that key pair and maintain and store the private key  
25 using a trustworthy system.

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

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

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

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



1 contents.

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

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

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

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

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

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

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

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

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

34 1. Request the issuing certification authority, and all  
35 independent repositories in which the subscriber has

1 authorized the certificate to be published, to suspend or  
2 revoke the certificate.

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

6 PART 6

7 GOVERNMENT AGENCY USE OF ELECTRONIC RECORDS AND SIGNATURES

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

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

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

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

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

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

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

35 3. All rules adopted by a government agency shall be

1 consistent with the rules adopted by the commissioner.

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

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

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

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

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

19 c. The use of digital signatures.

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

23 a. Its employees and agents.

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

35 4. The commissioner may specify appropriate standards and

1 requirements that must be satisfied by a certification  
2 authority before any of the following occur:

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

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

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

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

19 DIVISION II

20 CONFORMING PROVISIONS

21 Sec. 201. Section 22.7, Code Supplement 1997, is amended  
22 by adding the following new subsection:

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

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

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

32 EXPLANATION

33 This bill relates to electronic commerce security.

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

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

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

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

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

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

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

1 law that would be inconsistent with its purpose.

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

13 New Code section 554C.205 provides that where a rule of law  
14 requires information to be presented or retained in its  
15 original form that rule of law is satisfied by an electronic  
16 record if there exists reliable assurance as to the integrity  
17 of the information.

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

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

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

34 New Code section 554C.302 provides for secure electronic  
35 signatures. It provides that an electronic signature shall be

1 considered to be a secure electronic signature if executed  
2 utilizing a qualified security procedure.

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

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

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

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

1 relating to its trustworthiness.

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

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

9 New Code section 554C.412 provides that when an electronic  
10 record is signed with a digital signature, the digital  
11 signature is considered a secure electronic signature if it  
12 meets certain requirements. It must have been created during  
13 the period when a valid certificate was issued by a  
14 certification authority in accordance with standards,  
15 procedures, and other requirements specified by rule of the  
16 commissioner of insurance, or found to be trustworthy by the  
17 findings of a trier of fact.

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

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

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

32 New Code section 554C.423 prohibits a person from knowingly  
33 creating, publishing, altering, or otherwise using a  
34 certificate for a fraudulent or other unlawful purpose. A  
35 person convicted of violating this section is guilty of a



1 serious misdemeanor. A person convicted of a second or  
2 subsequent violation is guilty of a class "D" felony.

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

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

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

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

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

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

35 New Code section 554C.436 provides that the certification

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

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

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

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

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

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

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

1 security actions to protect relying parties.

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

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

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

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

23

24

25

26

27

28

29

30

31

32

33

34

35

HOUSE FILE 2474  
FISCAL NOTE

---

The estimate for House File 2474 is hereby submitted as a fiscal note pursuant to Joint Rule 17 and as a correctional impact statement pursuant to Section 2.56, Code of Iowa. Data used in developing this fiscal note and correctional impact statement are available from the Legislative Fiscal Bureau to members of the Legislature upon request.

---

House File 2474 creates Chapter 554C, Code of Iowa relating to electronic commerce security including the definition of electronic signature, establishing penalties for misrepresentation, and other provisions.

**ASSUMPTIONS**

1. Charge, conviction, and sentencing patterns will remain stable.
2. Penalties proposed in this Bill are less than current law. Prosecutors would have the discretion of which charges to bring.

**CORRECTIONAL IMPACT**

There is no correctional impact of HF 2474.

**FISCAL IMPACT**

There is no fiscal impact of HF 2474.

**SOURCE**

Criminal and Juvenile Justice Planning Division,  
Department of Human Rights  
Department of Commerce  
Department of Corrections  
Department of Justice  
Information Technology Services

(LSB 3386hv, CIB)

FILED MARCH 5, 1998

BY DENNIS PROUTY, FISCAL DIRECTOR

H-8281

1 Amend House File 2474 as follows:

- 2 1. Page 4, line 23, by inserting before the word  
3 "mortgage" the following: "deed,".  
4 2. Page 5, line 26, by inserting before the word  
5 "mortgage" the following: "deed,".  
6 3. Page 22, line 28, by inserting after the word  
7 "subscriber" the following: "or other legal entity".  
8 4. Page 22, line 29, by inserting after the word  
9 "subscriber" the following: "or other legal entity".  
10 5. Page 27, line 20, by striking the word  
11 "CONFORMING" and inserting the following:  
12 "MISCELLANEOUS".  
13 6. Page 27, by inserting after line 31 the  
14 following:

15 "Sec. \_\_\_\_ . CONSIDERATION OF MODEL LEGISLATION. It  
16 is the intent of the general assembly that if the  
17 national conference of commissioners on uniform state  
18 laws proposes a uniform electronic commerce act, the  
19 general assembly shall consider the proposed uniform  
20 act during the session in which the proposed uniform  
21 law is submitted to the states for consideration or  
22 during its next regular session if the proposed  
23 uniform act is submitted to the states during a period  
24 in which the general assembly is not in session."

By JACOBS of Polk

H-8281 FILED MARCH 10, 1998

*Adapted*  
3/11/98  
(P. 604)

HOUSE FILE **2474**  
BY COMMITTEE ON COMMERCE  
AND REGULATION

(SUCCESSOR TO HSB 650)

(As Amended and Passed by the House, March 11, 1998)

Passed House, Date \_\_\_\_\_ Passed Senate, Date \_\_\_\_\_  
Vote: Ayes \_\_\_\_\_ Nays \_\_\_\_\_ Vote: Ayes \_\_\_\_\_ Nays \_\_\_\_\_  
Approved \_\_\_\_\_

**A BILL FOR**

1 An Act relating to electronic commerce security, and providing  
2 penalties.

3 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

4

5

6

New Language \_\_\_\_\_

7

8

9

10

11

12

13

14

15

16

17

18

19

## 1 DIVISION I

## 2 SUBCHAPTER 1

## 3 GENERAL

4 Section 101. NEW SECTION. 554C.101 SHORT TITLE.5 This chapter shall be known and may be cited as the "Iowa  
6 Electronic Commerce Security Act".7 Sec. 102. NEW SECTION. 554C.102 PURPOSES AND  
8 CONSTRUCTION.9 This chapter shall be construed consistently with what is  
10 commercially reasonable under the circumstances and to  
11 effectuate all of the following purposes:12 1. Facilitate electronic communications by means of  
13 reliable electronic records.14 2. Facilitate and promote electronic commerce, by  
15 eliminating barriers resulting from uncertainties over writing  
16 and signature requirements, and promoting the development of  
17 the legal and business infrastructure necessary to implement  
18 secure electronic commerce.19 3. Facilitate electronic filing of documents with state  
20 and local government agencies and promote efficient delivery  
21 of government services by means of reliable electronic  
22 records.23 4. Minimize the incidence of forged electronic records,  
24 intentional and unintentional alteration of records, and fraud  
25 in electronic commerce.26 5. Establish uniformity of rules, regulations, and  
27 standards regarding the authentication and integrity of  
28 electronic records.29 6. Promote public confidence in the integrity,  
30 reliability, and legality of electronic records and electronic  
31 commerce.32 Sec. 103. NEW SECTION. 554C.103 VARIATION BY AGREEMENT  
33 -- USE OF ELECTRONIC MEANS OPTIONAL.34 1. As between parties involved in generating, sending,  
35 receiving, storing, or otherwise processing electronic

1 records, the provisions of this chapter may be varied by  
2 agreement of the parties. However, an agreement shall not  
3 vary requirements provided in section 554C.203, subsection 2;  
4 section 554C.204, subsection 4; section 554C.305, subsection  
5 2; sections 554C.422, 554C.423, 554C.424, and 554C.442; and  
6 section 554C.444, subsection 2.

7 2. This chapter shall not be construed to require a person  
8 to create, store, transmit, accept, or otherwise use or  
9 communicate information, records, or signatures by electronic  
10 means or in electronic form.

11 SUBCHAPTER 2

12 ELECTRONIC RECORDS AND SIGNATURES GENERALLY

13 Sec. 104. NEW SECTION. 554C.201 DEFINITIONS.

14 As used in this chapter, unless the context otherwise  
15 requires:

16 1. "Commissioner" means the commissioner of insurance  
17 appointed pursuant to section 505.2.

18 2. "Consumer transaction" means a transaction by an  
19 individual for personal, household, or family use.

20 3. "Electronic" includes electrical, digital, magnetic,  
21 optical, electromagnetic, or any other form of technology that  
22 entails capabilities similar to these technologies.

23 4. "Electronic record" means a record generated,  
24 communicated, received, or stored by electronic means for use  
25 in an information system or for transmission from one  
26 information system to another.

27 5. "Electronic signature" means a signature in electronic  
28 form attached to or logically associated with an electronic  
29 record.

30 6. "Government agency" means any executive, legislative,  
31 or judicial agency, department, board, commission, authority,  
32 institution, or instrumentality of this state or of any  
33 county, city, or other political subdivision of this state.

34 7. "Information" includes but is not limited to data,  
35 text, images, sound, codes, computer programs, software, and



1 databases.

2 8. "Party" means a person involved in an electronic  
3 transaction governed by the provisions of this chapter.

4 9. "Record" means information that is inscribed, stored,  
5 or otherwise fixed on a tangible medium or that is stored in  
6 an electronic or other medium and is retrievable in  
7 perceivable form.

8 10. "Rule of law" means any statute, rule of or order by a  
9 government agency, regulation, ordinance, common law rule, or  
10 court decision enacted, adopted, established, or rendered by  
11 the general assembly, government agency, court, political  
12 subdivision of, or other authority of, this state.

13 11. "Security procedure" means a methodology or procedure  
14 for the purpose of doing any of the following:

15 a. Verifying that an electronic record is the record of a  
16 specific person.

17 b. Detecting an error or alteration in the communication,  
18 content, or storage of an electronic record since a specific  
19 point in time. A security procedure may require the use of  
20 algorithms or codes, identifying words or numbers, encryption,  
21 answer back, acknowledgment procedures, or similar security  
22 devices.

23 12. "Signed" or "signature" includes any symbol executed  
24 or adopted, or any security procedure employed or adopted,  
25 including by use of electronic means, by or on behalf of a  
26 person with a present intention to authenticate a record.

27 Definitions used in any part of this chapter shall apply in  
28 all other parts of this chapter.

29 Sec. 105. NEW SECTION. 554C.202 LEGAL RECOGNITION.

30 Information shall not be denied legal effect, validity, or  
31 enforceability solely on the grounds that it is in the form of  
32 an electronic record or an electronic signature.

33 Sec. 106. NEW SECTION. 554C.203 ELECTRONIC RECORDS.

34 1. Where a rule of law requires information to be written  
35 or in writing or provides for certain consequences if it is

1 not, an electronic record satisfies that rule of law  
2 requirement.

3 2. The provisions of this section shall not apply to any  
4 of the following:

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

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

17 c. To any record that serves as a unique and transferable  
18 physical expression of rights and obligations including,  
19 without limitation, negotiable instruments and other  
20 instruments of title wherein possession of the instrument is  
21 deemed to confer title in a consumer transaction.

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

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

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

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

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

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

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

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

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

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

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

31 1. Where a rule of law requires information to be  
32 presented or retained in its original form, or provides  
33 consequences for information not being presented or retained  
34 in its original form, that rule of law is satisfied by an  
35 electronic record if there exists reliable assurance as to the

1 integrity of the information from the time when it was first  
2 generated in its final form, as an electronic record or  
3 otherwise.

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

12 3. The provisions of this section do not apply to any  
13 record that serves as a unique and transferable physical  
14 expression of rights and obligations including, but not  
15 limited to, negotiable instruments and other instruments of  
16 title wherein possession of the instrument is deemed to confer  
17 title.

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

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

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

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

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

1 maintained, the manner in which its originator was identified,  
2 and the manner in which the electronic record was signed.

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

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

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

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

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

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

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

30

### SUBCHAPTER 3

31

### SECURE ELECTRONIC RECORDS AND SIGNATURES

32

Sec. 111. NEW SECTION. 554C.301 SECURE ELECTRONIC

33 RECORD.

34 1. Subject to the provisions of section 554C.303, if, by  
35 the application of a qualified security procedure, it can be

1 verified that an electronic record has not been altered since  
2 a specified point in time, such electronic record shall be  
3 considered to be a secure electronic record from such  
4 specified point in time to the time of verification.

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

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

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

12 c. Certified by the commissioner as providing reliable  
13 evidence that an electronic record has not been altered, and  
14 implemented in a manner specified by the certification.

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

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

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

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

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

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

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

35 (2) Can be used to promptly, objectively, and

1 automatically identify the person signing the electronic  
2 record.

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

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

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

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

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

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

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

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

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

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

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

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

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

6 2. The commercial reasonableness of a security procedure  
7 is to be determined by the trier of fact in light of the  
8 purposes of the procedure and the commercial circumstances at  
9 the time the procedure was used, including but not limited to  
10 the nature of the transaction, sophistication of the parties,  
11 volume of similar transactions engaged in by either or both of  
12 the parties, availability of alternatives offered to but  
13 rejected by either of the parties, cost of alternative  
14 procedures, and procedures in general use for similar types of  
15 transactions.

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

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

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

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

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

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

35 4. In the absence of a secure electronic record or a



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

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

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

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

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

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

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

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

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

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

1 its intended purpose.

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

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

6 (1) A full and complete identification of the security  
7 procedure.

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

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

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

17 SUBCHAPTER 4

18 DIGITAL SIGNATURES

19 PART 1

20 DEFINITIONS

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

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

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

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

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

32 b. Names or otherwise identifies its subscriber.

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

35 d. Identifies its operational period.

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

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

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

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

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

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

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

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

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

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

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

1 all of the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

34 15. "Suspend a certificate" means to temporarily suspend  
35 the operational period of a certificate for a specified time

1 period or from a specified time forward.

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

5 a. Is reasonably secure from intrusion and misuse.

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

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

10 d. Adheres to generally accepted security procedures.

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

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

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

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

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

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

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

29

#### PART 2

30

#### EFFECT OF A DIGITAL SIGNATURE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

35 Sec. 120 NEW SECTION. 554C.413 COMMISSIONER AUTHORITY TO

## 1 ADOPT RULES.

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

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

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

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

29

## PART 3

30

## DUTIES GENERALLY

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

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





1 repository shall utilize a trustworthy system in performing  
2 their services.

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

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

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

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

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

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

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

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

27 3. If a certification authority certifies itself as a  
28 certification authority, it shall disclose to all relying  
29 parties that it is self-certified. The certification  
30 authority shall publish a copy of its own certification  
31 authority certificate that is verifiable by reference to a  
32 public key listed in a certificate issued by the certification  
33 authority.

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

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

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

7 2. Does either of the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 reasonably believes to be any of the following:

- 2 a. The subscriber listed in the certificate.
- 3 b. A person duly authorized to act for that subscriber.
- 4 c. A person acting on behalf of that subscriber, who is
- 5 unavailable.

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

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

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

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

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

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

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

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

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

35 (2) A material prerequisite to issuance of the certificate

1 was not satisfied.

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

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

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

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

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

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

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

19

#### PART 5

20

#### DUTIES OF SUBSCRIBERS

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

22 If the subscriber generates the key pair whose public key  
23 is to be listed in a certificate issued by a certification  
24 authority and accepted by the subscriber, the subscriber must  
25 generate that key pair and maintain and store the private key  
26 using a trustworthy system.

27 Sec. 133. NEW SECTION. 554C.442 OBTAINING A CERTIFICATE.

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

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

33 1. A person accepts a certificate that names a person as a  
34 subscriber by publishing it to one or more persons, depositing  
35 the certificate in a repository, or demonstrating approval of

1 the certificate, while knowing or having notice of its  
2 contents.

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

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

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

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

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

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

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

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

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

35 1. Request the issuing certification authority, and all

1 independent repositories in which the subscriber has  
2 authorized the certificate to be published, to suspend or  
3 revoke the certificate.

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

7 PART 6

8 GOVERNMENT AGENCY USE OF ELECTRONIC RECORDS AND SIGNATURES

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

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

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

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

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

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

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

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

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

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

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

17 a. The generation, use, and storage of key pairs.

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

20 c. The use of digital signatures.

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

24 a. Its employees and agents.

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



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

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

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

12 Sec. 139. NEW SECTION. 554C.453 INTEROPERABILITY.

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

20 DIVISION II

21 MISCELLANEOUS PROVISIONS

22 Sec. 201. Section 22.7, Code Supplement 1997, is amended  
23 by adding the following new subsection:

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

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

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

33 Sec. 203. CONSIDERATION OF MODEL LEGISLATION. It is the  
34 intent of the general assembly that if the national conference  
35 of commissioners on uniform state laws proposes a uniform

1 electronic commerce act, the general assembly shall consider  
2 the proposed uniform act during the session in which the  
3 proposed uniform law is submitted to the states for  
4 consideration or during its next regular session if the  
5 proposed uniform act is submitted to the states during a  
6 period in which the general assembly is not in session.

7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35

Jacobs, Ch  
Sukup  
Osterhaus

HSB 650  
COMMERCE AND REGULATION

SENATE/HOUSE FILE <sup>30</sup> ~~171~~ 2474  
BY (PROPOSED GOVERNOR'S BILL)

Passed Senate, Date \_\_\_\_\_ Passed House, Date \_\_\_\_\_  
Vote: Ayes \_\_\_\_\_ Nays \_\_\_\_\_ Vote: Ayes \_\_\_\_\_ Nays \_\_\_\_\_  
Approved \_\_\_\_\_

**A BILL FOR**

1 An Act relating to electronic commerce security, and providing  
2 penalties.  
3 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25

1 DIVISION I  
2 SUBCHAPTER 1  
3 GENERAL

4 Section 101. NEW SECTION. 554C.101 SHORT TITLE.

5 This chapter shall be known and may be cited as the "Iowa  
6 Electronic Commerce Security Act".

7 Sec. 102. NEW SECTION. 554C.102 PURPOSES AND  
8 CONSTRUCTION.

9 This chapter shall be construed consistently with what is  
10 commercially reasonable under the circumstances and to  
11 effectuate all of the following purposes:

12 1. Facilitate electronic communications by means of  
13 reliable electronic records.

14 2. Facilitate and promote electronic commerce, by  
15 eliminating barriers resulting from uncertainties over writing  
16 and signature requirements, and promoting the development of  
17 the legal and business infrastructure necessary to implement  
18 secure electronic commerce.

19 3. Facilitate electronic filing of documents with state  
20 and local government agencies and promote efficient delivery  
21 of government services by means of reliable electronic  
22 records.

23 4. Minimize the incidence of forged electronic records,  
24 intentional and unintentional alteration of records, and fraud  
25 in electronic commerce.

26 5. Establish uniformity of rules, regulations, and  
27 standards regarding the authentication and integrity of  
28 electronic records.

29 6. Promote public confidence in the integrity,  
30 reliability, and legality of electronic records and electronic  
31 commerce.

32 Sec. 103. NEW SECTION. 554C.103 VARIATION BY AGREEMENT  
33 -- USE OF ELECTRONIC MEANS OPTIONAL.

34 1. As between parties involved in generating, sending,  
35 receiving, storing, or otherwise processing electronic

1 records, the provisions of this chapter may be varied by  
2 agreement of the parties. However, an agreement shall not  
3 vary requirements provided in section 554C.203, subsection 2;  
4 section 554C.204, subsection 4; section 554C.305, subsection  
5 2; sections 554C.422, 554C.423, 554C.424, and 554C.442; and  
6 section 554C.444, subsection 2.

7 2. This chapter shall not be construed to require a person  
8 to create, store, transmit, accept, or otherwise use or  
9 communicate information, records, or signatures by electronic  
10 means or in electronic form.

11 SUBCHAPTER 2

12 ELECTRONIC RECORDS AND SIGNATURES GENERALLY

13 Sec. 104. NEW SECTION. 554C.201 DEFINITIONS.

14 As used in this chapter, unless the context otherwise  
15 requires:

16 1. "Commissioner" means the commissioner of insurance  
17 appointed pursuant to section 505.2.

18 2. "Consumer transaction" means a transaction by an  
19 individual for personal, household, or family use.

20 3. "Electronic" includes electrical, digital, magnetic,  
21 optical, electromagnetic, or any other form of technology that  
22 entails capabilities similar to these technologies.

23 4. "Electronic record" means a record generated,  
24 communicated, received, or stored by electronic means for use  
25 in an information system or for transmission from one  
26 information system to another.

27 5. "Electronic signature" means a signature in electronic  
28 form attached to or logically associated with an electronic  
29 record.

30 6. "Government agency" means any executive, legislative,  
31 or judicial agency, department, board, commission, authority,  
32 institution, or instrumentality of this state or of any  
33 county, city, or other political subdivision of this state.

34 7. "Information" includes but is not limited to data,  
35 text, images, sound, codes, computer programs, software, and

1 databases.

2 8. "Party" means a person involved in an electronic  
3 transaction governed by the provisions of this chapter.

4 9. "Record" means information that is inscribed, stored,  
5 or otherwise fixed on a tangible medium or that is stored in  
6 an electronic or other medium and is retrievable in  
7 perceivable form.

8 10. "Rule of law" means any statute, rule of or order by a  
9 government agency, regulation, ordinance, common law rule, or  
10 court decision enacted, adopted, established, or rendered by  
11 the general assembly, government agency, court, political  
12 subdivision of, or other authority of, this state.

13 11. "Security procedure" means a methodology or procedure  
14 for the purpose of doing any of the following:

15 a. Verifying that an electronic record is the record of a  
16 specific person.

17 b. Detecting an error or alteration in the communication,  
18 content, or storage of an electronic record since a specific  
19 point in time. A security procedure may require the use of  
20 algorithms or codes, identifying words or numbers, encryption,  
21 answer back, acknowledgment procedures, or similar security  
22 devices.

23 12. "Signed" or "signature" includes any symbol executed  
24 or adopted, or any security procedure employed or adopted,  
25 including by use of electronic means, by or on behalf of a  
26 person with a present intention to authenticate a record.

27 Definitions used in any part of this chapter shall apply in  
28 all other parts of this chapter.

29 Sec. 105. NEW SECTION. 554C.202 LEGAL RECOGNITION.

30 Information shall not be denied legal effect, validity, or  
31 enforceability solely on the grounds that it is in the form of  
32 an electronic record or an electronic signature.

33 Sec. 106. NEW SECTION. 554C.203 ELECTRONIC RECORDS.

34 1. Where a rule of law requires information to be written  
35 or in writing or provides for certain consequences if it is

650

1 not, an electronic record satisfies that rule of law  
2 requirement.

3 2. The provisions of this section shall not apply to any  
4 of the following:

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

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

17 c. To any record that serves as a unique and transferable  
18 physical expression of rights and obligations including,  
19 without limitation, negotiable instruments and other  
20 instruments of title wherein possession of the instrument is  
21 deemed to confer title in a consumer transaction.

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

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

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

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

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

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

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

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

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

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

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

31 1. Where a rule of law requires information to be  
32 presented or retained in its original form, or provides  
33 consequences for information not being presented or retained  
34 in its original form, that rule of law is satisfied by an  
35 electronic record if there exists reliable assurance as to the



1 integrity of the information from the time when it was first  
2 generated in its final form, as an electronic record or  
3 otherwise.

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

12 3. The provisions of this section do not apply to any  
13 record that serves as a unique and transferable physical  
14 expression of rights and obligations including, but not  
15 limited to, negotiable instruments and other instruments of  
16 title wherein possession of the instrument is deemed to confer  
17 title.

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

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

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

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

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

1 maintained, the manner in which its originator was identified,  
2 and the manner in which the electronic record was signed.

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

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

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

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

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

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

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

30

### SUBCHAPTER 3

31

### SECURE ELECTRONIC RECORDS AND SIGNATURES

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

34 1. Subject to the provisions of section 554C.303, if, by  
35 the application of a qualified security procedure, it can be

650

1 verified that an electronic record has not been altered since  
2 a specified point in time, such electronic record shall be  
3 considered to be a secure electronic record from such  
4 specified point in time to the time of verification.

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

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

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

12 c. Certified by the commissioner as providing reliable  
13 evidence that an electronic record has not been altered, and  
14 implemented in a manner specified by the certification.

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

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

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

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

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

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

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

35 (2) Can be used to promptly, objectively, and

1 automatically identify the person signing the electronic  
2 record.

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

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

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

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

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

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

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

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

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

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

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

650

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

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

6 2. The commercial reasonableness of a security procedure  
7 is to be determined by the trier of fact in light of the  
8 purposes of the procedure and the commercial circumstances at  
9 the time the procedure was used, including but not limited to  
10 the nature of the transaction, sophistication of the parties,  
11 volume of similar transactions engaged in by either or both of  
12 the parties, availability of alternatives offered to but  
13 rejected by either of the parties, cost of alternative  
14 procedures, and procedures in general use for similar types of  
15 transactions.

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

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

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

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

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

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

35 4. In the absence of a secure electronic record or a

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

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

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

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

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

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

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

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

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

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

650

1 its intended purpose.

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

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

6 (1) A full and complete identification of the security  
7 procedure.

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

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

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

17 SUBCHAPTER 4

18 DIGITAL SIGNATURES

19 PART 1

20 DEFINITIONS

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

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

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

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

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

32 b. Names or otherwise identifies its subscriber.

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

35 d. Identifies its operational period.

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

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

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

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

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

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

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

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

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

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

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



1 all of the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

34 15. "Suspend a certificate" means to temporarily suspend  
35 the operational period of a certificate for a specified time

1 period or from a specified time forward.

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

5 a. Is reasonably secure from intrusion and misuse.

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

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

10 d. Adheres to generally accepted security procedures.

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

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

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

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

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

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

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

29 PART 2

30 EFFECT OF A DIGITAL SIGNATURE

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

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

650

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

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

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

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

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

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

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

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

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

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

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

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

35 Sec. 120 NEW SECTION. 554C.413 COMMISSIONER AUTHORITY TO

1 ADOPT RULES.

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

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

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

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

29 PART 3

30 DUTIES GENERALLY

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

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



1 repository shall utilize a trustworthy system in performing  
2 their services.

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

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

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

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

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

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

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

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

27 3. If a certification authority certifies itself as a  
28 certification authority, it shall disclose to all relying  
29 parties that it is self-certified. The certification  
30 authority shall publish a copy of its own certification  
31 authority certificate that is verifiable by reference to a  
32 public key listed in a certificate issued by the certification  
33 authority.

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

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

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

7 2. Does either of the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



1 reasonably believes to be any of the following:

- 2 a. The subscriber listed in the certificate.
- 3 b. A person duly authorized to act for that subscriber.
- 4 c. A person acting on behalf of that subscriber, who is
- 5 unavailable.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18 PART 5

19 DUTIES OF SUBSCRIBERS

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

21 If the subscriber generates the key pair whose public key  
22 is to be listed in a certificate issued by a certification  
23 authority and accepted by the subscriber, the subscriber must  
24 generate that key pair and maintain and store the private key  
25 using a trustworthy system.

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

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

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

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

1 contents.

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

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

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

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

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

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

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

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

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

34 1. Request the issuing certification authority, and all  
35 independent repositories in which the subscriber has

1 authorized the certificate to be published, to suspend or  
2 revoke the certificate.

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

6 PART 6

7 GOVERNMENT AGENCY USE OF ELECTRONIC RECORDS AND SIGNATURES

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

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

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

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

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

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

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

35 3. All rules adopted by a government agency shall be

1 consistent with the rules adopted by the commissioner.

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

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

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

- 16 a. The generation, use, and storage of key pairs.
- 17 b. The issuance, acceptance, use, suspension, and
- 18 revocation of certificates.
- 19 c. The use of digital signatures.

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

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

35 4. The commissioner may specify appropriate standards and

1 requirements that must be satisfied by a certification  
2 authority before any of the following occur:

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

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

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

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

19 DIVISION II

20 CONFORMING PROVISIONS

21 Sec. 201. Section 22.7, Code Supplement 1997, is amended  
22 by adding the following new subsection:

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

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

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

32 EXPLANATION

33 This bill relates to electronic commerce security.

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

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

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

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

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

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

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

1 law that would be inconsistent with its purpose.

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

13 New Code section 554C.205 provides that where a rule of law  
14 requires information to be presented or retained in its  
15 original form that rule of law is satisfied by an electronic  
16 record if there exists reliable assurance as to the integrity  
17 of the information.

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

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

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

34 New Code section 554C.302 provides for secure electronic  
35 signatures. It provides that an electronic signature shall be



1 considered to be a secure electronic signature if executed  
2 utilizing a qualified security procedure.

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

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

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

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

1 relating to its trustworthiness.

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

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

9 New Code section 554C.412 provides that when an electronic  
10 record is signed with a digital signature, the digital  
11 signature is considered a secure electronic signature if it  
12 meets certain requirements. It must have been created during  
13 the period when a valid certificate was issued by a  
14 certification authority in accordance with standards,  
15 procedures, and other requirements specified by rule of the  
16 commissioner of insurance, or found to be trustworthy by the  
17 findings of a trier of fact.

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

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

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

32 New Code section 554C.423 prohibits a person from knowingly  
33 creating, publishing, altering, or otherwise using a  
34 certificate for a fraudulent or other unlawful purpose. A  
35 person convicted of violating this section is guilty of a

650

1 serious misdemeanor. A person convicted of a second or  
2 subsequent violation is guilty of a class "D" felony.

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

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

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

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

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

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

35 New Code section 554C.436 provides that the certification

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

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

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

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

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

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

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

1 security actions to protect relying parties.

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

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

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

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

23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35