

MAR 10 1999

COMMERCE AND REGULATION

HOUSE FILE  
BY JACOBS

3/15/99 Do Pass  
5-3/23/99 Commerce  
5-3/30/99 Amend/Do Pass  
w/53195

624

Passed House, Date 3/23/99 (P. 189) Passed Senate, Date 4/12/99 (P. 1047)  
Vote: Ayes 96 Nays 0 Vote: Ayes 47 Nays 2

Approved 5/19/99  
Repassed 4/15/99  
votes - 90-0

(P. 1351)

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:

HOUSE FILE 624

S-3195

1 Amend House File 624, as passed by the House, as  
2 follows:

3 1. Page 2, line 12, by inserting after the word  
4 "signature" the following: ", except as otherwise  
5 provided by a rule of law".

6 2. Page 2, line 34, by striking the word "any"  
7 and inserting the following: "the".

8 3. Page 2, line 35, by inserting after the word  
9 "branch" the following: ", or an".

By COMMITTEE ON COMMERCE  
JOHN W. JENSEN, Chairperson

adopted 4/12/99 (P. 1047)

S-3195 FILED MARCH 30, 1999

SENATE AMENDMENT TO HOUSE FILE 624

H-1541

1 Amend House File 624, as passed by the House, as  
2 follows:

3 1. Page 2, line 12, by inserting after the word  
4 "signature" the following: ", except as otherwise  
5 provided by a rule of law".

6 2. Page 2, line 34, by striking the word "any"  
7 and inserting the following: "the".

8 3. Page 2, line 35, by inserting after the word  
9 "branch" the following: ", or an".

RECEIVED FROM THE SENATE

H-1541 FILED APRIL 12, 1999

House Concurred 4/15/99 (P. 1350)

HF 624

DIVISION I  
SUBCHAPTER I  
GENERAL

Section 1. NEW SECTION. 554C.101 SHORT TITLE.

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

Sec. 2. 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. 3. 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 records, the provisions of this chapter may be varied by

1 agreement of the parties. However, an agreement shall not  
2 vary requirements provided in section 554C.203, subsection 2;  
3 section 554C.204, subsection 4; section 554C.305, subsection  
4 2; sections 554C.422, 554C.423, 554C.424, and 554C.442; and  
5 section 554C.444, subsection 2.

6 2. This chapter shall not be construed to require a person  
7 to create, store, transmit, accept, or otherwise use or  
8 communicate information, records, or signatures by electronic  
9 means or in electronic form. A government agency shall not  
10 require electronic filing of an electronic record or an  
11 electronic signature as the only means of filing such record  
12 or signature.

13 SUBCHAPTER II

14 ELECTRONIC RECORDS AND SIGNATURES GENERALLY

15 Sec. 4. NEW SECTION. 554C.201 DEFINITIONS.

16 As used in this chapter, unless the context otherwise  
17 requires:

18 1. "Commissioner" means the commissioner of insurance  
19 appointed pursuant to section 505.2.

20 2. "Consumer" means an individual engaged in a transaction  
21 for personal, family, or household purposes.

22 3. "Consumer transaction" means a transaction by an  
23 individual for personal, household, or family use.

24 4. "Electronic" includes electrical, digital, magnetic,  
25 optical, electromagnetic, or any other form of technology that  
26 entails capabilities similar to these technologies.

27 5. "Electronic record" means a record generated,  
28 communicated, received, or stored by electronic means for use  
29 in an information system or for transmission from one  
30 information system to another.

31 6. "Electronic signature" means a signature in electronic  
32 form attached to or logically associated with an electronic  
33 record.

34 7. "Government agency" means any executive, legislative,  
35 or judicial branch agency, department, board, commission,

1 authority, institution, or instrumentality of this state or of  
2 any county, city, or other political subdivision of this  
3 state.

4 8. "Information" includes but is not limited to data,  
5 text, images, sound, codes, computer programs, software, and  
6 databases.

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

9 10. "Record" means information that is inscribed, stored,  
10 or otherwise fixed on a tangible medium or that is stored in  
11 an electronic or other medium and is retrievable in  
12 perceivable form.

13 11. "Rule of law" means any statute, rule of or order by a  
14 government agency, regulation, ordinance, common law rule, or  
15 court decision enacted, adopted, established, or rendered by  
16 the general assembly, government agency, court, political  
17 subdivision of, or other authority of, this state or the  
18 federal government.

19 12. "Security procedure" means a methodology or procedure  
20 for the purpose of doing any of the following:

21 a. Verifying that an electronic record is the record of a  
22 specific person.

23 b. Detecting an error or alteration in the communication,  
24 content, or storage of an electronic record since a specific  
25 point in time. A security procedure may require the use of  
26 algorithms or codes, identifying words or numbers, encryption,  
27 answer back, acknowledgment procedures, or similar security  
28 devices.

29 13. "Signed" or "signature" includes any symbol executed  
30 or adopted, or any security procedure employed or adopted,  
31 including by use of electronic means, by or on behalf of a  
32 person with a present intention to authenticate a record.

33 Definitions used in any part of this chapter shall apply in  
34 all other parts of this chapter.

35 Sec. 5. NEW SECTION. 554C.202 LEGAL RECOGNITION.

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

4 A transaction subject to this chapter is also subject to  
5 other applicable substantive rules of law. Other substantive  
6 rules of law, whenever reasonable, shall be construed to be  
7 consistent with this chapter. If such construction is  
8 unreasonable, such other substantive rule of law governs.

9 Sec. 6. NEW SECTION. 554C.203 ELECTRONIC RECORDS.

10 1. Where a rule of law requires information to be written  
11 or in writing or provides for certain consequences if it is  
12 not, an electronic record satisfies that rule of law  
13 requirement.

14 2. The provisions of this section shall not apply to any  
15 of the following:

16 a. When its application involves a construction of a rule  
17 of law that is clearly inconsistent with the manifest intent  
18 of the body imposing the requirement or repugnant to the  
19 context of the same rule of law. However, the mere  
20 requirement that information be in writing, written, or  
21 printed shall not by itself be sufficient to establish an  
22 intent which is inconsistent with the requirement of this  
23 section.

24 b. A rule of law governing the creation or execution of a  
25 will or trust, living will, a general, durable, or healthcare  
26 power of attorney, or a voluntary, involuntary, or standby  
27 guardianship or conservatorship.

28 c. A record that serves as a unique and transferable  
29 physical expression of rights and obligations including,  
30 without limitation, negotiable instruments and other  
31 instruments of title wherein possession of the instrument is  
32 deemed to confer title in a consumer transaction.

33 d. A record that grants a legal or equitable interest in  
34 real property, including a deed, mortgage, deed of trust,  
35 pledge, security interest, or other lien or encumbrance.

1 e. A disclosure required in a consumer transaction,  
2 including but not limited to, disclosures required in chapter  
3 13C, sections 321.69 and 321.71, chapters 516D, 523B, 523E,  
4 523G, 533D, 537, 537B, 538A, 552, 552A, 555A, 557A, 557B,  
5 558A, and 562A, section 714.16, and chapter 714B, or an  
6 administrative rule adopted pursuant to such sections and  
7 chapters.

8 Sec. 7. NEW SECTION. 554C.204 ELECTRONIC SIGNATURES.

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

12 2. An electronic signature may be proved in any manner,  
13 including by showing that a procedure exists by which a person  
14 must of necessity have executed a symbol or security procedure  
15 for the purpose of verifying that an electronic record is the  
16 record of that person in order to proceed further with a  
17 transaction.

18 3. Absent an agreement to the contrary, the recipient of a  
19 signed electronic record is entitled to establish reasonable  
20 requirements to ensure that the symbol or security procedure  
21 adopted as an electronic signature by the person signing is  
22 authentic.

23 4. The provisions of this section shall not apply to any  
24 of the following:

25 a. When its application would involve a construction of a  
26 rule of law that is clearly inconsistent with the manifest  
27 intent of the body imposing the requirement or repugnant to  
28 the context of the same rule of law. However, the mere  
29 requirement that information be in writing, written, or  
30 printed shall not by itself be sufficient to establish an  
31 intent which is inconsistent with the requirement of this  
32 section.

33 b. To any rule of law governing the creation or execution  
34 of a will or trust, living will, a general, durable, or  
35 healthcare power of attorney, or a voluntary, involuntary, or

1 standby guardianship or conservatorship.

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

7 d. To any record that grants a legal or equitable interest  
8 in real property, including a deed, mortgage, deed of trust,  
9 pledge, security interest, or other lien or encumbrance.

10 Sec. 8. NEW SECTION. 554C.205 REQUIREMENT FOR ORIGINAL  
11 INFORMATION.

12 1. Where a rule of law requires information to be  
13 presented or retained in its original form, or provides  
14 consequences for information not being presented or retained  
15 in its original form, that rule of law is satisfied by an  
16 electronic record if there exists reliable assurance as to the  
17 integrity of the information from the time when it was first  
18 generated in its final form, as an electronic record or  
19 otherwise.

20 2. The criteria for assessing the integrity of information  
21 shall be whether the information has remained complete and  
22 unaltered, apart from the addition of any endorsement and any  
23 change that arises in the normal course of communication,  
24 storage, and display. The standard of reliability required  
25 shall be assessed in the light of all relevant circumstances,  
26 including but not limited to the purpose for which the  
27 information was generated.

28 3. The provisions of this section do not apply to any  
29 record that serves as a unique and transferable physical  
30 expression of rights and obligations including, but not  
31 limited to, negotiable instruments and other instruments of  
32 title wherein possession of the instrument is deemed to confer  
33 title.

34 Sec. 9. NEW SECTION. 554C.206 ADMISSIBILITY INTO  
35 EVIDENCE.

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

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

7 b. On the grounds that it is not in its original form or  
8 is not an original.

9 2. Information in the form of an electronic record shall  
10 be given due evidential weight by the trier of fact. In  
11 assessing the evidential weight of an electronic record or  
12 electronic signature where its authenticity is in issue, the  
13 trier of fact may consider all relevant information or  
14 circumstances, including but not limited to the manner in  
15 which it was generated, stored, or communicated, the  
16 reliability of the manner in which its integrity was  
17 maintained, the manner in which its originator was identified,  
18 and the manner in which the electronic record was signed.

19 Sec. 10. NEW SECTION. 554C.207 RETENTION OF ELECTRONIC  
20 RECORDS.

21 1. a. Where a rule of law requires that certain  
22 documents, records, or information be retained, that  
23 requirement is met by retaining electronic records of the  
24 information, provided that all of the following conditions are  
25 satisfied:

26 (1) The electronic record and the information contained in  
27 the electronic record must be accessible so as to be usable  
28 for subsequent reference at all times when such information  
29 must be retained.

30 (2) The information must be retained in the format in  
31 which it was originally generated, sent, or received; or in a  
32 format that can be demonstrated to represent accurately the  
33 information originally generated, sent, or received.

34 (3) Data is retained which enables the identification of  
35 the origin and destination of the information, the



1 authenticity and integrity of the information, and the date  
2 and time when it was generated, sent, or received.

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

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

11 SUBCHAPTER III

12 SECURE ELECTRONIC RECORDS AND SIGNATURES

13 Sec. 11. NEW SECTION. 554C.301 SECURE ELECTRONIC RECORD.

14 1. Subject to the provisions of section 554C.303, if, by  
15 the application of a qualified security procedure, it can be  
16 verified that an electronic record has not been altered since  
17 a specified point in time, such electronic record shall be  
18 considered to be a secure electronic record from such  
19 specified point in time to the time of verification.

20 2. For purposes of this subchapter, a qualified security  
21 procedure is a security procedure to detect changes in content  
22 that is any of the following:

23 a. Authorized by, and implemented in accordance with the  
24 requirements of, this chapter.

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

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

30 Sec. 12. NEW SECTION. 554C.302 SECURE ELECTRONIC  
31 SIGNATURE.

32 1. Subject to the provisions of section 554C.303, if, by  
33 the application of a qualified security procedure, it can be  
34 authenticated that an electronic signature is the signature of  
35 a specific person, the electronic signature shall be

1 considered to be a secure electronic signature at the time of  
2 verification.

3 2. A qualified security procedure for purposes of this  
4 section is a security procedure for identifying a party that  
5 is any of the following:

6 a. Authorized by, and implemented in accordance with the  
7 requirements of, this chapter.

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

10 c. Certified by the commissioner as being capable of  
11 creating an electronic signature that meets all of the  
12 following conditions:

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

15 (2) Can be used to promptly, objectively, and  
16 automatically identify the person signing the electronic  
17 record.

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

19 (4) Is linked to the electronic record to which it relates  
20 in a manner which ensures that if the record or signature is  
21 changed the electronic signature is invalidated, provided that  
22 the security procedure is implemented in a manner required by  
23 the certification.

24 Sec. 13. NEW SECTION. 554C.303 COMMERCIALY REASONABLE  
25 -- RELIANCE.

26 1. An electronic record or electronic signature that  
27 qualifies for secure status pursuant to section 554C.301,  
28 554C.302, 554C.411, or 554C.412 shall not be considered secure  
29 unless the proponent establishes all of the following:

30 a. Use of the applicable security procedure was  
31 commercially reasonable.

32 b. The security procedure was implemented in a trustworthy  
33 manner or, where applicable, in a manner specified by this  
34 chapter or the commissioner, to the extent such information is  
35 within the knowledge of the proponent.

1 c. Reliance on the security procedure was reasonable and  
2 in good faith in light of all the circumstances known to the  
3 proponent at the time of the reliance, having due regard for  
4 all of the following:

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

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

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

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

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

18 (6) Any other evidence relating to facts of which the  
19 proponent was aware that would suggest that reliance was or  
20 was not reasonable.

21 2. The commercial reasonableness of a security procedure  
22 is to be determined by the trier of fact in light of the  
23 purposes of the procedure and the commercial circumstances at  
24 the time the procedure was used, including but not limited to  
25 the nature of the transaction, sophistication of the parties,  
26 volume of similar transactions engaged in by either or both of  
27 the parties, availability of alternatives offered to but  
28 rejected by either of the parties, cost of alternative  
29 procedures, and procedures in general use for similar types of  
30 transactions.

31 Sec. 14. NEW SECTION. 554C.304 PRESUMPTIONS.

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

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

4        a. The secure electronic signature is the signature of the  
5 person to whom it correlates.

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

8        3. The effect of the presumptions provided in this section  
9 is to place on the party challenging the integrity of a secure  
10 electronic record or challenging the genuineness of a secure  
11 electronic signature both the burden of going forward with  
12 evidence to rebut the presumption and the burden of persuading  
13 the trier of fact that the falsity of the presumed fact is  
14 more probable than the truth of its existence.

15       4. In the absence of a secure electronic record or a  
16 secure electronic signature, nothing in this chapter shall  
17 change existing rules regarding legal or evidentiary rules  
18 regarding the burden of proving the authenticity and integrity  
19 of an electronic record or an electronic signature.

20       Sec. 15. NEW SECTION. 554C.305 ATTRIBUTION OF SIGNATURE  
21 TO A PARTY.

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

27       a. The signature resulted from acts of a person who  
28 obtained the access numbers, codes, computer programs, or  
29 other information necessary to create the signature from a  
30 source under the control of the alleged signer, creating the  
31 appearance that it came from the person to whom it correlates.

32       b. The access occurred under circumstances constituting a  
33 failure to exercise reasonable care by the person to whom it  
34 correlates.

35       c. The recipient reasonably relied to the recipient's

1 detriment on the apparent source of the electronic record,  
2 taking into account the factors provided in section 554C.303.

3 2. The provisions of this section shall not apply to  
4 consumer transactions, including but not limited to credit  
5 card and automatic teller machines, except to the extent  
6 allowed by applicable consumer law.

7 Sec. 16. NEW SECTION. 554C.306 CERTIFICATION BY THE  
8 COMMISSIONER.

9 1. This chapter shall not limit the technology which may  
10 qualify as a security procedure under section 554C.301 or  
11 554C.302 if the technology meets all of the criteria in  
12 subsections 2 and 3.

13 2. A security procedure may be certified by the  
14 commissioner as meeting the requirements of section 554C.301  
15 or 554C.302, following an appropriate investigation or review,  
16 if all of the following apply:

17 a. The technology utilized by the security procedure is  
18 completely open and fully disclosed to the public in order to  
19 facilitate a comprehensive evaluation of its suitability for  
20 its intended purpose.

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

23 c. The certification specifies at least all of the  
24 following:

25 (1) A full and complete identification of the security  
26 procedure.

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

30 (3) A term for the certification which shall not exceed  
31 five years.

32 3. At the end of the term for each certified security  
33 procedure, or earlier as determined by the commissioner, the  
34 security procedure may be reevaluated in light of then-current  
35 technology and recertified or decertified as appropriate.

1 4. A person, upon submitting a written request that  
2 includes a complete explanation of a proposed technology which  
3 meets the requirements of this section together with a  
4 proposed draft of administrative rules applicable to such  
5 technology, may request the commissioner to review the  
6 proposed technology and practices. The commissioner shall  
7 review the proposal and may adopt rules in accordance with  
8 section 554C.413 with respect to the proposed technology and  
9 practices. The commissioner may adopt rules establishing  
10 procedures and requirements for the filing of proposals to  
11 review proposed technology and practices.

12 SUBCHAPTER IV

13 DIGITAL SIGNATURES

14 PART 1

15 DEFINITIONS

16 Sec. 17. NEW SECTION. 554C.401 DEFINITIONS.

17 As used in this subchapter, unless the context otherwise  
18 requires:

19 1. "Asymmetric cryptosystem" means a computer-based system  
20 capable of generating and using a key pair, consisting of a  
21 private key for creating a digital signature, and a public key  
22 to verify the digital signature.

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

25 a. Identifies the certification authority issuing the  
26 certificate.

27 b. Names or otherwise identifies its subscriber.

28 c. Contains a public key that corresponds to a private key  
29 under the control of the subscriber.

30 d. Identifies its operational period.

31 e. Is digitally signed by the certification authority  
32 issuing the certification.

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

35 4. "Certification practice statement" means a statement

1 published by a certification authority or person operating a  
2 repository that specifies the policies or practices that the  
3 certification authority employs in issuing, suspending, and  
4 revoking certificates, and providing access to a certificate.

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

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

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

16 b. Whether the initial electronic record has been altered  
17 since the transformation was made. A digital signature is a  
18 security procedure.

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

22 a. One key can encrypt a message which only the other key  
23 can decrypt.

24 b. Even knowing one key, it is computationally infeasible  
25 to discover the other key.

26 8. "Message digest function" means an algorithm that maps  
27 or translates the sequence of bits comprising an electronic  
28 record into another, generally smaller, set of bits, referred  
29 to as the message digest, without requiring the use of any  
30 secret information such as a key, in a manner which provides  
31 all of the following:

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

34 b. It is computationally infeasible that any two  
35 electronic records can be found or deliberately generated that

1 would produce the same message digest using the algorithm  
2 unless the two records are identical.

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

5 a. The period begins on the date and at the time the  
6 certificate is issued by a certification authority or on a  
7 later date and at a time certain if stated in the certificate.

8 b. The period ends on the date and at the time the  
9 certificate expires as noted in the certificate or on an  
10 earlier date if the certificate is revoked or suspended in  
11 accordance with this chapter.

12 10. "Private key" means the key of a key pair used to  
13 create a digital signature.

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

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

18 13. "Revoke a certificate" means to permanently end the  
19 operational period of a certificate from a specified time  
20 forward.

21 14. "Subscriber" means a person to whom all of the  
22 following applies:

23 a. The person is the subject named or otherwise identified  
24 in a certificate issued to the person.

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

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

29 15. "Suspend a certificate" means to temporarily suspend  
30 the operational period of a certificate for a specified time  
31 period or from a specified time forward.

32 16. "Trustworthy system" means a system of computer  
33 hardware, software, and procedures that satisfies all of the  
34 following:

35 a. Is reasonably secure from intrusion and misuse.



1 b. Provides a reasonable level of availability,  
2 reliability, and correct operation.

3 c. Is reasonably suited to performing the system's  
4 intended functions.

5 d. Adheres to generally accepted security procedures.

6 e. Meets or exceeds the requirements of rules adopted by  
7 the commissioner.

8 17. "Valid certificate" means a certificate that meets the  
9 following conditions:

10 a. The certificate has been issued by a certification  
11 authority.

12 b. The subscriber listed in the certificate has accepted  
13 the certificate in accordance with this chapter.

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

19 a. That the digital signature was created using the  
20 private key corresponding to the public key listed in the  
21 certificate.

22 b. The electronic record has not been altered since its  
23 digital signature was created.

24 PART 2

25 EFFECT OF A DIGITAL SIGNATURE

26 Sec. 18. NEW SECTION. 554C.411 SECURE ELECTRONIC RECORD.

27 Subject to the provisions of section 554C.303, an  
28 electronic record or any portion thereof that is signed with a  
29 digital signature shall be considered to be a secure  
30 electronic record if the digital signature was created during  
31 the operational period of a valid certificate and is verified  
32 by reference to the public key listed in such certificate.

33 Sec. 19. NEW SECTION. 554C.412 SECURE ELECTRONIC

34 SIGNATURE.

35 Subject to the provisions of section 554C.303, when all or

1 any portion of an electronic record is signed with a digital  
2 signature, the digital signature shall be considered a secure  
3 electronic signature with respect to all or that portion of  
4 the record, if all of the following apply:

5 1. The digital signature was created during the  
6 operational period of a valid certificate, was used within any  
7 limits specified or incorporated by reference in the  
8 certificate, and can be verified by reference to the public  
9 key listed in the certificate.

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

12 a. The certificate was issued by a certification authority  
13 in accordance with standards, procedures, and other  
14 requirements specified by rule of the commissioner.

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

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

20 (2) The material information set forth in the certificate  
21 is true.

22 3. The process and systems utilized to create and verify a  
23 digital signature are considered trustworthy because one of  
24 the following applies:

25 a. They comply with standards, procedures, and other  
26 requirements specified by the commissioner.

27 b. A trier of fact independently finds that they are  
28 trustworthy.

29 Sec. 20. NEW SECTION. 554C.413 COMMISSIONER AUTHORITY TO  
30 ADOPT RULES.

31 1. The commissioner may adopt rules applicable to the  
32 public or private sector which define when a certificate and a  
33 digital signature is considered sufficiently trustworthy in  
34 order to ensure that a digital signature verified by reference  
35 to the certificate will qualify as a secure electronic

1 signature. The rules may include but are not limited to any  
2 of the following:

3 a. Establishing or adopting standards applicable to  
4 certification authorities or certificates. Compliance with  
5 the standards may be measured by obtaining a voluntary  
6 certification from the commissioner or becoming accredited by  
7 one or more independent accrediting entities recognized by the  
8 commissioner.

9 b. Establishing or adopting standards applicable to the  
10 digital signature creation or verification process.

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

23 PART 3

24 DUTIES GENERALLY

25 Sec. 21. NEW SECTION. 554C.421 RELIANCE ON CERTIFICATES.

26 A person relying on a digital signature may also rely on a  
27 valid certificate containing the public key by which the  
28 digital signature can be verified.

29 Sec. 22. NEW SECTION. 554C.422 RESTRICTIONS ON  
30 PUBLICATION OF CERTIFICATE.

31 A person shall not publish a certificate, or otherwise make  
32 it available to anyone known by that person to be in a  
33 position to rely on the certificate or on a digital signature  
34 that is verifiable with reference to the public key listed in  
35 the certificate, if that person knows that any of the

1 following apply:

2 1. The certification authority listed in the certificate  
3 has not issued the certificate.

4 2. The subscriber listed in the certificate has not  
5 accepted the certificate.

6 3. The certificate has been revoked or suspended, unless  
7 the publication is for the purpose of verifying a digital  
8 signature created prior to such suspension or revocation.

9 Sec. 23. NEW SECTION. 554C.423 FRAUDULENT PURPOSE.

10 A person shall not knowingly create, publish, alter, or  
11 otherwise use a certificate for a fraudulent or other unlawful  
12 purpose. A person convicted of violating this section is  
13 guilty of a serious misdemeanor. A person convicted of a  
14 second or subsequent violation is guilty of a class "D"  
15 felony.

16 Sec. 24. NEW SECTION. 554C.424 FALSE OR UNAUTHORIZED  
17 REQUEST.

18 A person shall not knowingly misrepresent the person's  
19 identity or authorization in requesting or accepting a  
20 certificate or in requesting suspension or revocation of a  
21 certificate. A person convicted of violating this section is  
22 guilty of a serious misdemeanor. A person convicted of a  
23 second or subsequent violation is guilty of a class "D"  
24 felony.

25 Sec. 25. NEW SECTION. 554C.425 CIVIL REMEDY.

26 A person who suffers a loss by reason of a violation of  
27 section 554C.423 or 554C.424, in a civil action against the  
28 violator, may obtain appropriate legal and equitable relief.  
29 In a civil action under this section, the court may award the  
30 prevailing party its reasonable attorney fees and other  
31 litigation expenses. However, if the plaintiff is a consumer,  
32 the court may award reasonable attorney fees and other  
33 litigation expenses only to a prevailing plaintiff.

34

PART 4

35 DUTIES OF CERTIFICATION AUTHORITIES AND REPOSITORIES

1     Sec. 26. NEW SECTION. 554C.431 TRUSTWORTHY SYSTEM.

2     A certification authority and a person maintaining a  
3 repository shall utilize a trustworthy system in performing  
4 their services.

5     Sec. 27. NEW SECTION. 554C.432 DISCLOSURE.

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

9     a. Its certification practice statement, if the authority  
10 has one.

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

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

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

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

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

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

1     Sec. 28. NEW SECTION. 554C.433 ISSUANCE OF A  
2 CERTIFICATE.

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

7     1. Receives a request for the issuance from the  
8 prospective subscriber.

9     2. Does either of the following:

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

14    b. In the absence of a certification practice statement,  
15 confirms one of the following:

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

18     (2) The information in the certificate to be issued is  
19 accurate.

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

24     Sec. 29. NEW SECTION. 554C.434 REPRESENTATIONS UPON  
25 ISSUANCE OF CERTIFICATE.

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

1 the certification authority represents that as of the time the  
2 certificate is issued it has confirmed all of the following:

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

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

12 3. The subscriber's public key and private key constitute  
13 a functioning key pair.

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

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

24 Sec. 30. NEW SECTION. 554C.435 SUSPENSION OF A  
25 CERTIFICATE.

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

30 1. The receipt of an order issued by a court of competent  
31 jurisdiction.

32 2. In accordance with the policies and procedures  
33 governing suspension specified in its certification practice  
34 statement. In the absence of policies and procedures  
35 governing suspension, the certificate shall be suspended as

1 soon as possible after receiving a request by a person whom  
2 the certification authority or person maintaining a repository  
3 reasonably believes to be any of the following:

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

8 Sec. 31. NEW SECTION. 554C.436 REVOCATION OF A  
9 CERTIFICATE.

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

14 1. Upon receipt of an order issued by a court of competent  
15 jurisdiction.

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

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

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

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

33 d. Confirmation by the certification authority that one of  
34 the following applies:

35 (1) A material fact represented in the certificate is



1 false.

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

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

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

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

12 Sec. 32. NEW SECTION. 554C.437 NOTICE OF SUSPENSION OR  
13 REVOCATION.

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

17 1. Promptly publish notice of the suspension or revocation  
18 if the certificate was published.

19 2. Disclose the fact of suspension or revocation on  
20 inquiry by a relying party.

21 PART 5

22 DUTIES OF SUBSCRIBERS

23 Sec. 33. NEW SECTION. 554C.441 GENERATING THE KEY PAIR.

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

29 Sec. 34. NEW SECTION. 554C.442 OBTAINING A CERTIFICATE.

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

33 Sec. 35. NEW SECTION. 554C.443 ACCEPTANCE OF A  
34 CERTIFICATE.

35 1. A person accepts a certificate that names a person as a

1 subscriber by publishing it to one or more persons, depositing  
2 the certificate in a repository, or demonstrating approval of  
3 the certificate, while knowing or having notice of its  
4 contents.

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

9 a. The subscriber rightfully holds the private key  
10 corresponding to the public key listed in the certificate.

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

14 c. All information in the certificate that is within the  
15 knowledge of the subscriber is true.

16 Sec. 36. NEW SECTION. 554C.444 CONTROL OF THE PRIVATE  
17 KEY.

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

28 2. The provisions of this section do not apply to consumer  
29 transactions.

30 Sec. 37. NEW SECTION. 554C.445 INITIATING SUSPENSION OR  
31 REVOCATION.

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

1 certificate shall do one of the following:

2 1. Request the issuing certification authority, and all  
3 independent repositories in which the subscriber has  
4 authorized the certificate to be published, to suspend or  
5 revoke the certificate.

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

9

PART 6

10 GOVERNMENT AGENCY USE OF ELECTRONIC RECORDS AND SIGNATURES

11 Sec. 38. NEW SECTION. 554C.451 GOVERNMENT AGENCY USE OF  
12 ELECTRONIC RECORDS.

13 1. Each government agency shall determine if, and the  
14 extent to which, it will send and receive electronic records  
15 and electronic signatures to and from other persons. This  
16 section shall not be interpreted as varying the requirements  
17 of chapter 22.

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

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

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

34 c. Control processes and procedures which are appropriate  
35 to ensure adequate integrity, security, confidentiality, and

1 auditability of electronic records.

2 d. Any other required attributes for electronic records  
3 that are currently specified for corresponding paper  
4 documents, or reasonably necessary under the circumstances.

5 3. All rules adopted by a government agency shall be  
6 consistent with the rules adopted by the commissioner.

7 Sec. 39. NEW SECTION. 554C.452 COMMISSIONER TO ADOPT  
8 STATE STANDARDS.

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

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

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

22 b. The issuance, acceptance, use, suspension, and  
23 revocation of certificates.

24 c. The use of digital signatures.

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

28 a. Its employees and agents.

29 b. Persons conducting business or other transactions with  
30 the government agency. The government agency may take other  
31 actions consistent with this authority, including the  
32 establishment of repositories and the suspension or revocation  
33 of issued certificates, provided that actions by the  
34 government agency are conducted in accordance with all rules,  
35 procedures, and policies specified by the commissioner. The

1 commissioner may adopt rules, procedures, and policies under  
2 which government agencies may issue or contract for the  
3 issuance of certificates, or restrict or prohibit their  
4 issuance.

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

8 a. The services of a certification authority are used by a  
9 government agency for the issuance, publication, suspension,  
10 or revocation of certificates to the government agency,  
11 including its employees or agents, for official use only.

12 b. The certificates that the certification authority  
13 issues are accepted for purposes of verifying digitally signed  
14 electronic records sent to any government agency by any  
15 person.

16 Sec. 40. NEW SECTION. 554C.453 INTEROPERABILITY.

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

24 Sec. 41. NEW SECTION. 554C.501 REPEAL.

25 This chapter is repealed effective July 1, 2004.

26 SUBCHAPTER V

27 REPEAL

28 DIVISION II

29 MISCELLANEOUS PROVISIONS

30 Sec. 42. Section 4.1, subsection 39, unnumbered paragraph  
31 1, Code 1999, is amended to read as follows:

32 The words "written" and "in writing" may include any mode  
33 of representing words or letters in general use, and includes  
34 an electronic record as defined in section 554C.201. A  
35 signature, when required by law, must be made by the writing

1 or markings of the person whose signature is required.

2 "Signature" includes an electronic or digital signature as  
3 defined in section 554C.201. If a person is unable due to a  
4 physical disability to make a written signature or mark, that  
5 person may substitute either of the following in lieu of a  
6 signature required by law:

7 Sec. 43. Section 22.7, Code 1999, is amended by adding the  
8 following new subsection:

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

12 b. Records which if disclosed might jeopardize the  
13 security of an issued certificate or a certificate to be  
14 issued pursuant to chapter 554C.

15 Sec. 44. COMMISSIONER REQUIRED TO ADOPT RULES. The  
16 commissioner of insurance shall adopt rules as required by  
17 this Act not later than July 1, 2000.

18 Sec. 45. CONSIDERATION OF MODEL LEGISLATION. It is the  
19 intent of the general assembly that if the national conference  
20 of commissioners on uniform state laws proposes a uniform  
21 electronic commerce act, the general assembly shall consider  
22 the proposed uniform act during the session in which the  
23 proposed uniform law is submitted to the states for  
24 consideration or during its next regular session if the  
25 proposed uniform act is submitted to the states during a  
26 period in which the general assembly is not in session.

27 EXPLANATION

28 This bill relates to electronic commerce security.

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

31 New Code section 554C.101 provides the short title for the  
32 chapter, referred to as the "Iowa Electronic Commerce Security  
33 Act".

34 New Code section 554C.102 provides for the purposes and  
35 construction of the chapter. The bill provides that the

1 chapter must be construed consistently with what is  
2 commercially reasonable under the circumstances to effectuate  
3 electronic communications by means of reliable electronic  
4 records; facilitate and promote electronic commerce by  
5 eliminating certain present barriers; facilitate the  
6 electronic filing of documents with state and local government  
7 agencies; minimizing the incidence of forged electronic  
8 records; establishing uniformity of regulations and standards;  
9 promoting public confidence in the integrity, reliability, and  
10 legality of electronic records and electronic commerce.

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

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

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

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

32 New Code section 554C.204 provides that where a rule of law  
33 requires a signature, an electronic signature satisfies that  
34 rule of law. This requirement does not apply to defeat an  
35 expressed purpose of a rule of law; the creation or execution

1 of a will or trust, living will, general, durable, or  
2 healthcare power of attorney, a voluntary, involuntary, or  
3 standby guardianship or conservatorship; any record that  
4 serves as a unique and transferable physical expression of  
5 rights and obligations in consumer transactions; or any record  
6 that grants a legal or equitable interest in real property in  
7 consumer transactions.

8 New Code section 554C.205 provides that where a rule of law  
9 requires information to be presented or retained in its  
10 original form that rule of law is satisfied by an electronic  
11 record if there exists reliable assurance as to the integrity  
12 of the information.

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

22 New Code section 554C.207 provides that where a rule of law  
23 requires that certain documents, records, or information be  
24 retained that requirement is met by retaining electronic  
25 records of the information.

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

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

33 New Code section 554C.303 provides additional requirements  
34 for secure status information. It provides requirements for  
35 proving that an electronic record or electronic signature



1 qualifies for secure status, including providing for special  
2 procedures. The bill provides that the security procedure  
3 must be commercially reasonable, as determined by the trier of  
4 fact.

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

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

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

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

34 New Code section 554C.411 provides that an electronic  
35 record that is signed with a digital signature is considered

1 to be a secure electronic record if the digital signature was  
2 created during the operational period of a valid certificate  
3 issued by the commissioner.

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

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

17 New Code section 554C.421 provides that a person relying on  
18 a digital signature may also rely on a valid certificate  
19 containing a public key by which the digital signature can be  
20 verified.

21 New Code section 554C.422 prohibits a person from  
22 publishing or making available a certificate if that person  
23 knows that the certification authority listed in the  
24 certificate has not issued the certificate, the subscriber  
25 listed in the certificate has not accepted the certificate, or  
26 the certificate has been revoked or suspended.

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

33 New Code section 554C.424 prohibits a person from knowingly  
34 misrepresenting the person's identity or authorization in  
35 requesting or accepting a certificate or in requesting

1 suspension or revocation of a certificate. A person convicted  
2 of violating this section is guilty of a serious misdemeanor.  
3 A person convicted of a second or subsequent violation is  
4 guilty of a class "D" felony.

5 New Code section 554C.431 provides that a person designated  
6 as a certification authority and a person maintaining a  
7 repository must utilize a trustworthy system in performing  
8 their services.

9 New Code section 554C.432 provides for disclosure to  
10 parties relying upon a certification, a certification practice  
11 statement, a certification authority certificate, and a notice  
12 of a revocation or suspension of its certification authority  
13 certificate.

14 New Code section 554C.433 provides for the issuance of a  
15 certificate to a prospective subscriber for the purpose of  
16 verifying digital signatures.

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

27 New Code section 554C.435 provides for the suspension of a  
28 certificate by the certification authority that issues a  
29 certificate.

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

1 certification practice statement.

2 New Code section 554C.437 provides for a notice of  
3 suspension or revocation.

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

10 New Code section 554C.442 provides that all material  
11 representations made by the subscriber to a certification  
12 authority for purposes of obtaining a certificate must be  
13 accurate and complete.

14 New Code section 554C.443 provides that a person accepts a  
15 certificate that names a person as a subscriber by publishing  
16 it to one or more persons, depositing the certificate in a  
17 repository, or demonstrating approval of the certificate,  
18 while knowing or having notice of its contents.

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

27 New Code section 554C.445 provides that if a private key  
28 corresponding to the public key listed in a certificate is  
29 compromised during the operational period of the certificate,  
30 a subscriber who has accepted the certificate must take  
31 security actions to protect relying parties.

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

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

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

15 New Code section 554C.501 repeals Code chapter 554C  
16 effective July 1, 2004.

17 The bill provides conforming amendments. The bill requires  
18 that the commissioner of insurance adopt rules as required by  
19 the bill not later than July 1, 2000.

20 The bill provides that it is the intent of the general  
21 assembly that if the national conference of commissioners on  
22 uniform state laws proposes a uniform electronic commerce act,  
23 the general assembly shall consider the proposed uniform act  
24 during the session in which it is submitted to the states for  
25 consideration or during the next regular session if the  
26 proposed uniform act is submitted to the states during a  
27 period in which the general assembly is not in session.

28

29

30

31

32

33

34

35

**HOUSE FILE 624  
FISCAL NOTE**

---

A fiscal note for House File 624 is hereby submitted pursuant to Joint Rule 17. Data used in developing this fiscal note is available from the Legislative Fiscal Bureau to members of the Legislature upon request.

---

House File 624 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 would be no significant correctional impact associated with House File 624.

**FISCAL IMPACT**

House File 624 would have no significant General Fund impact.

**SOURCES**

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

(LSB 2172hh, SLS)

FILED MARCH 16, 1999

BY DENNIS PROUTY, FISCAL DIRECTOR

AN ACT  
RELATING TO ELECTRONIC COMMERCE SECURITY, AND PROVIDING  
PENALTIES.

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

DIVISION I  
SUBCHAPTER I

GENERAL

Section 1. NEW SECTION. 554C.101 SHORT TITLE.

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

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

2. This chapter shall not be construed to require a person to create, store, transmit, accept, or otherwise use or communicate information, records, or signatures by electronic means or in electronic form. A government agency shall not require electronic filing of an electronic record or an electronic signature as the only means of filing such record or signature, except as otherwise provided by a rule of law.

SUBCHAPTER II

ELECTRONIC RECORDS AND SIGNATURES GENERALLY

Sec. 4. NEW SECTION. 554C.201 DEFINITIONS.

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

1. "Commissioner" means the commissioner of insurance appointed pursuant to section 505.2.
2. "Consumer" means an individual engaged in a transaction for personal, family, or household purposes.
3. "Consumer transaction" means a transaction by an individual for personal, household, or family use.
4. "Electronic" includes electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies.

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

6. "Electronic signature" means a signature in electronic form attached to or logically associated with an electronic record.

7. "Government agency" means the executive, legislative, or judicial branch, or an agency, department, board, commission, authority, institution, or instrumentality of this state or of any county, city, or other political subdivision of this state.

8. "Information" includes but is not limited to data, text, images, sound, codes, computer programs, software, and databases.

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

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

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

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

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

b. Detecting an error or alteration in the communication, content, or storage of an electronic record since a specific point in time. A security procedure may require the use of algorithms or codes, identifying words or numbers, encryption,

answer back, acknowledgment procedures, or similar security devices.

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

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

Sec. 5. NEW SECTION. 554C.202 LEGAL RECOGNITION.

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

A transaction subject to this chapter is also subject to other applicable substantive rules of law. Other substantive rules of law, whenever reasonable, shall be construed to be consistent with this chapter. If such construction is unreasonable, such other substantive rule of law governs.

Sec. 6. NEW SECTION. 554C.203 ELECTRONIC RECORDS.

1. Where a rule of law requires information to be written or in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law requirement.

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

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

b. A rule of law governing the creation or execution of a will or trust, living will, a general, durable, or healthcare power of attorney, or a voluntary, involuntary, or standby guardianship or conservatorship.



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

d. A record that grants a legal or equitable interest in real property, including a deed, mortgage, deed of trust, pledge, security interest, or other lien or encumbrance.

e. A disclosure required in a consumer transaction, including but not limited to, disclosures required in chapter 13C, sections 321.69 and 321.71, chapters 516D, 523B, 523E, 523G, 533D, 537, 537B, 538A, 552, 552A, 555A, 557A, 557B, 558A, and 562A, section 714.16, and chapter 714B, or an administrative rule adopted pursuant to such sections and chapters.

Sec. 7. NEW SECTION. 554C.204 ELECTRONIC SIGNATURES.

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

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

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

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

a. When its application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the body imposing the requirement or repugnant to

the context of the same rule of law. However, the mere requirement that information be in writing, written, or printed shall not by itself be sufficient to establish an intent which is inconsistent with the requirement of this section.

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

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

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

Sec. 8. NEW SECTION. 554C.205 REQUIREMENT FOR ORIGINAL INFORMATION.

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

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

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

Sec. 9. NEW SECTION. 554C.206 ADMISSIBILITY INTO EVIDENCE.

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

- a. On the sole ground that it is an electronic record or electronic signature.
- b. On the grounds that it is not in its original form or is not an original.

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

Sec. 10. NEW SECTION. 554C.207 RETENTION OF ELECTRONIC RECORDS.

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

- (1) The electronic record and the information contained in the electronic record must be accessible so as to be usable

for subsequent reference at all times when such information must be retained.

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

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

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

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

SUBCHAPTER III

SECURE ELECTRONIC RECORDS AND SIGNATURES

Sec. 11. NEW SECTION. 554C.301 SECURE ELECTRONIC RECORD.

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

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

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

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

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

Sec. 12. NEW SECTION. 554C.302 SECURE ELECTRONIC SIGNATURE.

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

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

- a. Authorized by, and implemented in accordance with the requirements of, this chapter.
- b. Previously agreed to by the parties to an agreement, and implemented in accordance with the terms of the agreement.
- c. Certified by the commissioner as being capable of creating an electronic signature that meets all of the following conditions:

- (1) Is unique to the signer within the context in which it is used.
- (2) Can be used to promptly, objectively, and automatically identify the person signing the electronic record.
- (3) Was reliably created by such identified person.
- (4) Is linked to the electronic record to which it relates in a manner which ensures that if the record or signature is changed the electronic signature is invalidated, provided that the security procedure is implemented in a manner required by the certification.

Sec. 13. NEW SECTION. 554C.303 COMMERCIALY REASONABLE -- RELIANCE.

1. An electronic record or electronic signature that qualifies for secure status pursuant to section 554C.301, 554C.302, 554C.411, or 554C.412 shall not be considered secure unless the proponent establishes all of the following:

- a. Use of the applicable security procedure was commercially reasonable.
- b. The security procedure was implemented in a trustworthy manner or, where applicable, in a manner specified by this chapter or the commissioner, to the extent such information is within the knowledge of the proponent.
- c. Reliance on the security procedure was reasonable and in good faith in light of all the circumstances known to the proponent at the time of the reliance, having due regard for all of the following:

- (1) Information that the proponent knew or had notice of at the time of reliance, including all facts, statements, and limitations contained in any statement by any third party involved in the authentication process.
- (2) The value or importance of the electronic record signed with the secure electronic signature, if known.
- (3) Any course of dealing between the proponent and the purported sender and the available indicia of reliability or unreliability apart from the secure electronic signature.
- (4) Any usage of trade, particularly trade conducted by trustworthy systems or other computer-based means.
- (5) Whether the authentication was performed with the assistance of an independent third party.
- (6) Any other evidence relating to facts of which the proponent was aware that would suggest that reliance was or was not reasonable.

2. The commercial reasonableness of a security procedure is to be determined by the trier of fact in light of the purposes of the procedure and the commercial circumstances at the time the procedure was used, including but not limited to the nature of the transaction, sophistication of the parties,

volume of similar transactions engaged in by either or both of the parties, availability of alternatives offered to but rejected by either of the parties, cost of alternative procedures, and procedures in general use for similar types of transactions.

Sec. 14. NEW SECTION. 554C.304 PRESUMPTIONS.

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

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

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

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

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

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

Sec. 15. NEW SECTION. 554C.305 ATTRIBUTION OF SIGNATURE TO A PARTY.

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

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

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

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

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

Sec. 16. NEW SECTION. 554C.306 CERTIFICATION BY THE COMMISSIONER.

1. This chapter shall not limit the technology which may qualify as a security procedure under section 554C.301 or 554C.302 if the technology meets all of the criteria in subsections 2 and 3.

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

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

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

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

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

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

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

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

4. A person, upon submitting a written request that includes a complete explanation of a proposed technology which meets the requirements of this section together with a proposed draft of administrative rules applicable to such technology, may request the commissioner to review the proposed technology and practices. The commissioner shall review the proposal and may adopt rules in accordance with section 554C.413 with respect to the proposed technology and practices. The commissioner may adopt rules establishing procedures and requirements for the filing of proposals to review proposed technology and practices.

SUBCHAPTER IV  
DIGITAL SIGNATURES

PART 1  
DEFINITIONS

Sec. 17. NEW SECTION. 554C.401 DEFINITIONS.

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

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

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

a. Identifies the certification authority issuing the certificate.

b. Names or otherwise identifies its subscriber.

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

d. Identifies its operational period.

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

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

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

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

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

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

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

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

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

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

8. "Message digest function" means an algorithm that maps or translates the sequence of bits comprising an electronic

record into another, generally smaller, set of bits, referred to as the message digest, without requiring the use of any secret information such as a key, in a manner which provides all of the following:

- a. A record yields the same message digest every time the algorithm is executed using such record as input.
- b. It is computationally infeasible that any two electronic records can be found or deliberately generated that would produce the same message digest using the algorithm unless the two records are identical.

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

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

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

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

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

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

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

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

- a. The person is the subject named or otherwise identified in a certificate issued to the person.
- b. The person controls a private key that corresponds to the public key listed in that certificate.

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

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

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

- a. Is reasonably secure from intrusion and misuse.
- b. Provides a reasonable level of availability, reliability, and correct operation.
- c. Is reasonably suited to performing the system's intended functions.
- d. Adheres to generally accepted security procedures.
- e. Meets or exceeds the requirements of rules adopted by the commissioner.

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

- a. The certificate has been issued by a certification authority.

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

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

- a. That the digital signature was created using the private key corresponding to the public key listed in the certificate.
- b. The electronic record has not been altered since its digital signature was created.

## PART 2

## EFFECT OF A DIGITAL SIGNATURE

Sec. 18. NEW SECTION. 554C.411 SECURE ELECTRONIC RECORD.

Subject to the provisions of section 554C.303, an electronic record or any portion thereof that is signed with a digital signature shall be considered to be a secure electronic record if the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate.

Sec. 19. NEW SECTION. 554C.412 SECURE ELECTRONIC SIGNATURE.

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

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

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

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

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

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

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

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

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

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

Sec. 20. NEW SECTION. 554C.413 COMMISSIONER AUTHORITY TO ADOPT RULES.

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

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

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

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

PART 3

DUTIES GENERALLY

Sec. 21. NEW SECTION. 554C.421 RELIANCE ON CERTIFICATES.

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

Sec. 22. NEW SECTION. 554C.422 RESTRICTIONS ON PUBLICATION OF CERTIFICATE.

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

1. The certification authority listed in the certificate has not issued the certificate.
2. The subscriber listed in the certificate has not accepted the certificate.
3. The certificate has been revoked or suspended, unless the publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

Sec. 23. NEW SECTION. 554C.423 FRAUDULENT PURPOSE.

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

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

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

Sec. 25. NEW SECTION. 554C.425 CIVIL REMEDY.

A person who suffers a loss by reason of a violation of section 554C.423 or 554C.424, in a civil action against the violator, may obtain appropriate legal and equitable relief. In a civil action under this section, the court may award the prevailing party its reasonable attorney fees and other litigation expenses. However, if the plaintiff is a consumer, the court may award reasonable attorney fees and other litigation expenses only to a prevailing plaintiff.

PART 4

DUTIES OF CERTIFICATION AUTHORITIES AND REPOSITORIES

Sec. 26. NEW SECTION. 554C.431 TRUSTWORTHY SYSTEM.

A certification authority and a person maintaining a repository shall utilize a trustworthy system in performing their services.

Sec. 27. NEW SECTION. 554C.432 DISCLOSURE.

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

- a. Its certification practice statement, if the authority has one.
- b. Its certification authority certificate that identifies the certification authority as a self-certifying subscriber and that contains the public key corresponding to the private key used by that certification authority to digitally sign the certificate.

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

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

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



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

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

Sec. 28. NEW SECTION. 554C.433 ISSUANCE OF A CERTIFICATE.

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

1. Receives a request for the issuance from the prospective subscriber.
2. Does either of the following:
  - a. Complies with all of the practices and procedures set forth in its applicable certification practice statement, including procedures regarding identification of the prospective subscriber.
  - b. In the absence of a certification practice statement, confirms one of the following:
    - (1) The prospective subscriber is the person to be listed in the certificate to be issued.
    - (2) The information in the certificate to be issued is accurate.
    - (3) The prospective subscriber rightfully holds a private key capable of creating a digital signature, and the public key to be listed in the certificate can be used to verify a digital signature affixed by such private key.

Sec. 29. NEW SECTION. 554C.434 REPRESENTATIONS UPON ISSUANCE OF CERTIFICATE.

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

1. The certification authority has complied with all applicable requirements of this chapter in issuing the certificate, and if the certification authority has published the certificate or otherwise made it available to a relying person, that the subscriber identified in the certificate has accepted it.
2. The subscriber identified in the certificate, rightfully holds the private key corresponding to the public key listed in the certificate.
3. The subscriber's public key and private key constitute a functioning key pair.
4. All information in the certificate is accurate as of the date it was issued, unless the certification authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed.
5. To the knowledge of the certification authority, there are no known material facts omitted from the certificate which would, if known, adversely affect the reliability of the representations required to be provided by the certification authority under this section.

Sec. 30. NEW SECTION. 554C.435 SUSPENSION OF A CERTIFICATE.

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

1. The receipt of an order issued by a court of competent jurisdiction.
2. In accordance with the policies and procedures governing suspension specified in its certification practice statement. In the absence of policies and procedures governing suspension, the certificate shall be suspended as soon as possible after receiving a request by a person whom the certification authority or person maintaining a repository reasonably believes to be any of the following:
  - a. The subscriber listed in the certificate.
  - b. A person duly authorized to act for that subscriber.
  - c. A person acting on behalf of that subscriber, who is unavailable.

Sec. 31. NEW SECTION. 554C.436 REVOCATION OF A CERTIFICATE.

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

1. Upon receipt of an order issued by a court of competent jurisdiction.
2. In accordance with the policies and procedures governing revocation specified in its certification practice statement. In the absence of policies and procedures governing revocation, the certificate shall be revoked as soon as possible after one of the following occurs:
  - a. Receipt of a request for revocation by the subscriber named in the certificate, if the certification authority or repository confirms that the person requesting the revocation is the subscriber or is an agent of the subscriber with authority to request the revocation.

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

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

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

- (1) A material fact represented in the certificate is false.
- (2) A material prerequisite to issuance of the certificate was not satisfied.
- (3) The certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability.
- (4) The subscriber's private key or trustworthy system was compromised.

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

Sec. 32. NEW SECTION. 554C.437 NOTICE OF SUSPENSION OR REVOCATION.

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

1. Promptly publish notice of the suspension or revocation if the certificate was published.
2. Disclose the fact of suspension or revocation on inquiry by a relying party.

PART 5

DUTIES OF SUBSCRIBERS

Sec. 33. NEW SECTION. 554C.441 GENERATING THE KEY PAIR.

If the subscriber generates the key pair whose public key is to be listed in a certificate issued by a certification

authority and accepted by the subscriber, the subscriber must generate that key pair and maintain and store the private key using a trustworthy system.

Sec. 34. NEW SECTION. 554C.442 OBTAINING A CERTIFICATE.

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

Sec. 35. NEW SECTION. 554C.443 ACCEPTANCE OF A CERTIFICATE.

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

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

- a. The subscriber rightfully holds the private key corresponding to the public key listed in the certificate.
- b. All representations made by the subscriber to the certification authority and material to the information listed in the certificate are true.
- c. All information in the certificate that is within the knowledge of the subscriber is true.

Sec. 36. NEW SECTION. 554C.444 CONTROL OF THE PRIVATE KEY.

1. Except as otherwise provided by another applicable rule of law, by accepting a certificate issued by a certification authority the subscriber identified in the certificate assumes a duty to persons who reasonably rely on the certificate to exercise reasonable care to retain control of the private key corresponding to the public key listed in the certificate and to prevent its disclosure to a person not authorized to create the subscriber's digital signature. The requirements of this

subsection shall continue during the operational period of the certificate.

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

Sec. 37. NEW SECTION. 554C.445 INITIATING SUSPENSION OR REVOCATION.

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

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

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

PART 6

GOVERNMENT AGENCY USE OF ELECTRONIC RECORDS AND SIGNATURES

Sec. 38. NEW SECTION. 554C.451 GOVERNMENT AGENCY USE OF ELECTRONIC RECORDS.

1. Each government agency shall determine if, and the extent to which, it will send and receive electronic records and electronic signatures to and from other persons. This section shall not be interpreted as varying the requirements of chapter 22.

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

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

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

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

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

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

Sec. 39. NEW SECTION. 554C.452 COMMISSIONER TO ADOPT STATE STANDARDS.

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

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

- a. The generation, use, and storage of key pairs.
- b. The issuance, acceptance, use, suspension, and revocation of certificates.
- c. The use of digital signatures.

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

- a. Its employees and agents.
- b. Persons conducting business or other transactions with the government agency. The government agency may take other actions consistent with this authority, including the establishment of repositories and the suspension or revocation of issued certificates, provided that actions by the government agency are conducted in accordance with all rules, procedures, and policies specified by the commissioner. The commissioner may adopt rules, procedures, and policies under which government agencies may issue or contract for the issuance of certificates, or restrict or prohibit their issuance.

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

- a. The services of a certification authority are used by a government agency for the issuance, publication, suspension, or revocation of certificates to the government agency, including its employees or agents, for official use only.
- b. The certificates that the certification authority issues are accepted for purposes of verifying digitally signed electronic records sent to any government agency by any person.

Sec. 40. NEW SECTION. 554C.453 INTEROPERABILITY.

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

SUBCHAPTER V  
REPEAL

Sec. 41. NEW SECTION. 554C.501 REPEAL.

This chapter is repealed effective July 1, 2004.

DIVISION II

MISCELLANEOUS PROVISIONS

Sec. 42. Section 4.1, subsection 39, unnumbered paragraph 1, Code 1999, is amended to read as follows:

The words "written" and "in writing" may include any mode of representing words or letters in general use, and includes an electronic record as defined in section 554C.201. A signature, when required by law, must be made by the writing or markings of the person whose signature is required. "Signature" includes an electronic or digital signature as defined in section 554C.201. If a person is unable due to a physical disability to make a written signature or mark, that person may substitute either of the following in lieu of a signature required by law:

Sec. 43. Section 22.7, Code 1999, is amended by adding the following new subsection:

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

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

Sec. 44. COMMISSIONER REQUIRED TO ADOPT RULES. The commissioner of insurance shall adopt rules as required by this Act not later than July 1, 2000.

Sec. 45. CONSIDERATION OF MODEL LEGISLATION. It is the intent of the general assembly that if the national conference of commissioners on uniform state laws proposes a uniform electronic commerce act, the general assembly shall consider the proposed uniform act during the session in which the proposed uniform law is submitted to the states for consideration or during its next regular session if the proposed uniform act is submitted to the states during a period in which the general assembly is not in session.

---

RON J. CORBETT  
Speaker of the House

---

MARY E. KRAMER  
President of the Senate

I hereby certify that this bill originated in the House and is known as House File 624, Seventy-eighth General Assembly.

---

ELIZABETH ISAACSON  
Chief Clerk of the House

Approved 5/19, 1999

---

THOMAS J. VILSACK  
Governor