House Study Bill 650

Bill Text

PAG LIN

DIVISION I
SUBCHAPTER 1
GENERAL

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

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

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

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

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

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

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

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

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

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

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

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

SUBCHAPTER 2
ELECTRONIC RECORDS AND SIGNATURES GENERALLY

Sec. 104. 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 transaction" means a transaction by an individual for personal, household, or family use.

3. "Electronic" includes electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that

entails capabilities similar to these technologies.

4. "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.

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

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

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

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

9. "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.

10. "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.

11. "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.

12. "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. 105. 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.

Sec. 106. 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. 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,

without limitation, 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 mortgage, deed of trust, pledge, security interest, or other lien or encumbrance in a consumer transaction.

Sec. 107. 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 mortgage, deed of trust, pledge, security interest, or other lien or encumbrance in a consumer transaction.

Sec. 108. 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. 109. 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. 110. 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 3

SECURE ELECTRONIC RECORDS AND SIGNATURES

Sec. 111. 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. 112. 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. 113. NEW SECTION. 554C.303 COMMERCIALLY REASONABLE RELIANCE.

1. An electronic record or electronic signature that qualifies for secure status pursuant to section 554C.301, 554C.302, 554C.412, or 554C.413 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. 114. 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. 115. 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. 116. NEW SECTION. 554C.306 CERTIFICATION BY THE COMMISSIONER.

1. 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.

2. 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.

SUBCHAPTER 4
DIGITAL SIGNATURES
PART 1
DEFINITIONS

Sec. 117. 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. 118. 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. 119. 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. 120 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. 121. 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. 122. 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. 123. 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. 124. 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.

PART 4

DUTIES OF CERTIFICATION AUTHORITIES AND REPOSITORIES

Sec. 125. 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. 126. 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. 127. 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 perspective 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. 128. 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. 129. 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. 130. 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 upon confirmation by other evidence that the subscriber 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. 131. 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. 132. 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. 133. 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. 134. 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. 135. 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. 136. 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. 137. 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.

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. 138. 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. 139. 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.

DIVISION II

CONFORMING PROVISIONS

Sec. 201. Section 22.7, Code Supplement 1997, 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. 202. COMMISSIONER REQUIRED TO ADOPT RULES. The commissioner of insurance shall adopt rules as required by this Act not later than July 1, 1999.

EXPLANATION

This bill relates to electronic commerce security.

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

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

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

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

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

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

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

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

New Code section 554C.205 provides that where a rule of law requires information to be 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.

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

New Code section 554C.207 provides that 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.

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

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

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

New Code section 554C.304 provides for a rebuttable presumption when resolving a civil dispute involving a secure electronic record. The bill provides for a rebuttable presumption relating to alterations of an electronic record and the legitimacy of an electronic signature. The effect of the presumption 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.

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

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

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

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

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

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

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

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

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

New Code section 554C.423 prohibits a person from knowingly creating, publishing, altering, or otherwise using 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.

New Code section 554C.424 prohibits a person from knowingly misrepresenting 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.

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

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

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

New Code section 554C.434 provides that 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. The statement shall provide that the certification authority has complied with all applicable requirements of the bill and that all information in the certificate is accurate.

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

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

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

New Code section 554C.441 provides that if a 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.

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

New Code section 554C.443 provides that 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.

New Code section 554C.444 provides that 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 an unauthorized person. The provisions of this section do not apply to consumer transactions.

New Code section 554C.445 provides that if a 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 must take security actions to protect relying parties.

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

New Code section 554C.452 provides that the commissioner of insurance, 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.

New Code section 554C.453 provides that rules adopted by the insurance commissioner or a government agency relating to the use of electronic records or electronic signatures must 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.

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

LSB 3386XL 77
da/jw/5