

SECOND REGULAR SESSION

SENATE BILL NO. 708

89TH GENERAL ASSEMBLY

INTRODUCED BY SENATOR FLOTRON.

Read 1st time January 12, 1998, and 1,000 copies ordered printed.

TERRY L. SPIELER, Secretary.

L2990.011

AN ACT

Relating to digital signatures, with penalty provisions.

Be it enacted by the General Assembly of the State of Missouri, as follows:

Section 1. Sections 1 to 27 of this act are known as the "Missouri Digital Signatures Act."

Section 2. Sections 1 to 27 of this act shall be construed consistent with what is commercially reasonable under the circumstances and to effectuate the following purposes:

- (1) To facilitate commerce by means of reliable electronic messages;**
- (2) To minimize the incidence of forged digital signatures and fraud in electronic commerce;**
- (3) To implement legally the general import of relevant standards, such as X.509 of the International Telecommunication Union (formerly International Telegraph and Telephone Consultative Committee or CCITT); and**
- (4) To establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages.**

Section 3. For the purposes of sections 1 to 27 of this act, unless the context expressly indicates otherwise, the following terms shall mean:

- (1) "Accept a certificate":**
 - (a) To manifest approval of a certificate, while knowing or having notice of its contents; or**
 - (b) To apply to a licensed certification authority for a certificate, without canceling or revoking the application, if the certification authority subsequently issues a certificate based on the application;**
- (2) "Asymmetric cryptosystem", an algorithm or series of algorithms which**

provide a secure key pair;

(3) "Certificate", a computer-based record which:

(a) Identifies the certification authority issuing it;

(b) Names or identifies its subscriber;

(c) Contains the subscriber's public key; and

(d) Is digitally signed by the certification authority issuing it;

(4) "Certification authority", a person who issues a certificate;

(5) "Certification authority disclosure record", an on-line, publicly accessible record which concerns a licensed certification authority and is kept by the division. A certification authority disclosure record has the contents specified by rule of the division pursuant to section 4 of this act;

(6) "Certification practice statement", a declaration of the practices which a certification authority employs in issuing certificates generally, or employs in issuing a material certificate;

(7) "Certify", the declaration of material facts by the certification authority regarding a certificate;

(8) "Confirm", to ascertain through appropriate inquiry and investigation;

(9) "Correspond", with reference to keys, to belong to the same key pair;

(10) "Digital signature", a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether:

(a) The transformation was created using the private key that corresponds to the signer's public key; and

(b) The message has been altered since the transformation was made;

(11) "Division", the commission's division of the office of secretary of state for the state of Missouri;

(12) "Forge a digital signature", either:

(a) To create a digital signature without the authorization of the rightful holder of the private key; or

(b) To create a digital signature verifiable by a certificate listing as subscriber a person who either:

a. Does not exist; or

b. Does not hold the private key corresponding to the public key listed in the certificate;

(13) "Hold a private key", to be able to use a private key;

(14) "Incorporate by reference", to make one message a part of another message by identifying the message to be incorporated and expressing the intention that it be incorporated;

(15) "Issue a certificate", the acts of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate;

(16) "Key pair", a private key and its corresponding public key in an asymmetric cryptosystem, keys which have the property that the public key can verify a digital signature that the private key creates;

(17) "Licensed certification authority", a certification authority to whom a license has been issued by the division and whose license is in effect;

(18) "Message", a digital representation of information;

(19) "Notify", to communicate a fact to another person in a manner reasonably likely under the circumstances to impart knowledge of the information to the other person;

(20) "Operative personnel", one or more natural persons acting as a certification authority or its agent, or in the employment of or under contract with a certification authority, and who have:

(a) Managerial or policy-making responsibilities for the certification authority;

or

(b) Duties directly involving the issuance of certificates, creation of private keys, or administration of a certification authority's computing facilities;

(21) "Person", a human being or any organization capable of signing a document, either legally or as a matter of fact;

(22) "Private key", the key of a key pair used to create a digital signature;

(23) "Public key", the key of a key pair used to verify a digital signature;

(24) "Publish", to record or file in a repository;

(25) "Qualified right to payment", an award of damages against a licensed certification authority by a court having jurisdiction over the certification authority in a civil action for violation of sections 1 to 27 of this act;

(26) "Recipient", a person who receives or has a digital signature and is in a position to rely on it;

(27) "Recognized repository", a repository recognized by the division pursuant to section 25 of this act;

(28) "Recommended reliance limit", the limitation on the monetary amount recommended for reliance on a certificate pursuant to subsection 1 of section 17 of this act;

(29) "Repository", a system for storing and retrieving certificates and other information relevant to digital signatures;

(30) "Revoke a certificate", to make a certificate ineffective permanently from a specified time forward. Revocation is effected by notation or inclusion in a set of

revoked certificates, and does not imply that a revoked certificate is destroyed or made illegible;

(31) "Rightfully hold a private key", to be authorized to use a private key:

(a) Which the holder or the holder's agents have not disclosed to any person in violation of subsection 1 of section 13 of this act; and

(b) Which the holder has not obtained through theft, deceit, eavesdropping or other unlawful means;

(32) "Signer", a person who creates a digital signature for a message;

(33) "Subscriber", a person who:

(a) Is the subject listed in a certificate;

(b) Accepts the certificate; and

(c) Holds a private key which corresponds to a public key listed in that certificate;

(34) (a) "Suitable guaranty", either a surety bond executed by a surety authorized by the department of insurance to do business in this state, or an irrevocable letter of credit issued by a financial institution authorized to do business in this state by the division of finance in the department of economic development, which, in either event, satisfies all of the following requirements, that it:

a. Is issued payable to the division for the benefit of persons holding qualified rights of payment against the licensed certification authority named as the principal of the bond or customer of the letter of credit;

b. Is in an amount specified by rule of the division pursuant to section 4 of this act;

c. States that it is issued for filing pursuant to the provisions of sections 1 to 27 of this act;

d. Specifies a term of effectiveness extending at least as long as the term of the license to be issued to the certification authority; and

e. Is in a form prescribed by rule of the division;

(b) A suitable guaranty may also provide that the total annual liability on the guaranty to all persons making claims based on it may not exceed the face amount of the guaranty;

(c) A financial institution acting as a certification authority may satisfy the requirements of this subsection from its assets or capital, to the extent of its lending limit as provided by law;

(35) "Suspend a certificate", to make a certificate ineffective temporarily from a specified time forward;

(36) "Time-stamp", either:

(a) To append or attach to a message, digital signature or certificate a digitally

signed notation indicating at least the date and time the notation was appended or attached, and the identity of the person appending or attaching the notation; or

(b) The notation thus appended or attached;

(37) "Transactional certificate", a valid certificate incorporating by reference one or more digital signatures;

(38) "Trustworthy system", computer hardware and software which:

(a) Are reasonably secure from intrusion and misuse;

(b) Provide a reasonable level of availability, reliability and correct operation;

and

(c) Are reasonably suited to performing their intended functions;

(39) (a) "Valid certificate", a certificate which:

a. A licensed certification authority has issued;

b. The subscriber listed in it has accepted;

c. Has not been revoked or suspended; and

d. Has not expired;

(b) A transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference;

(40) "Verify a digital signature", in relation to a given digital signature, message and public key, to determine accurately that:

(a) The digital signature was created by the private key corresponding to the public key; and

(b) The message has not been altered since its digital signature was created.

Section 4. 1. The division may be a certification authority, and may issue, suspend and revoke certificates in the manner prescribed for licensed certification authorities in sections 1 to 27 of this act.

2. The division shall maintain a publicly accessible database containing a certification authority disclosure record for each licensed certification authority. The division shall publish the contents of the database in at least one recognized repository.

3. The division shall promulgate such rules as are necessary to effectuate the provisions of sections 1 to 27 of this act, including rules:

(1) Governing licensed certification authorities, their practice and the termination of a certification authority's practice;

(2) Determining an amount appropriate for a suitable guaranty, in light of:

(a) The burden a suitable guaranty places upon licensed certification authorities; and

(b) The assurance of financial responsibility it provides to persons who rely on certificates issued by licensed certification authorities;

(3) For reviewing software for use in creating digital signatures and publish

reports concerning software;

(4) Specifying reasonable requirements for the form of certificates issued by licensed certification authorities, in accordance with generally accepted standards for digital signature certificates;

(5) Specifying reasonable requirements for recordkeeping by licensed certification authorities;

(6) Specifying reasonable requirements for the content, form and sources of information in certification authority disclosure records, the updating and timeliness of such information, and other practices and policies relating to certification authority disclosure records; and

(7) Specifying the form of certification practice statements.

4. Any rule or portion of a rule, as that term is defined in section 536.010, RSMo, that is promulgated pursuant to the authority delegated in sections 1 to 27 of this act shall become effective only if it has been promulgated pursuant to the provisions of chapter 536, RSMo. All rulemaking authority delegated prior to the effective date of this section is of no force and effect and repealed; however, nothing in this section shall be interpreted to repeal or affect the validity of any rule filed or adopted prior to the effective date of this section if it fully complied with the provisions of chapter 536, RSMo. This section and chapter 536, RSMo, are nonseverable and if any of the powers vested with the general assembly pursuant to chapter 536, RSMo, to review, to delay the effective date or to disapprove and annul a rule are subsequently held unconstitutional, then the grant of rulemaking authority and any rule proposed or adopted after the effective date of this section shall be invalid and void.

Section 5. 1. To obtain or retain a license a certification authority shall:

(1) Be the subscriber of a certificate published in a recognized repository;

(2) Employ as operative personnel only persons who have not been convicted of a felony or a crime involving fraud, false statement or deception;

(3) Employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of sections 1 to 27 of this act;

(4) File with the division a suitable guaranty, unless the certification authority is the governor, a department or division of state government, the attorney general, state auditor, state treasurer, the supreme court, a city, a county or the legislature or its staff offices provided that:

(a) Each of such governmental entities may act through designated officials authorized by ordinance, rule or statute to perform certification authority functions; and

(b) One of such governmental entities is the subscriber of all certificates issued by the certification authority;

(5) Have the right to use a trustworthy system, including a secure means for controlling usage of its private key;

(6) Present proof to the division of having working capital reasonably sufficient, according to rules of the division, to enable the applicant to conduct business as a certification authority;

(7) Comply with all other licensing requirements established by division rule.

2. The division shall issue a license to a certification authority which:

(1) Is qualified pursuant to subsection 1 of this section;

(2) Applies in writing to the division for a license; and

(3) Pays the required filing fee.

3. (1) The division may classify and issue licenses according to specified limitations, such as a maximum number of outstanding certificates, cumulative maximum of recommended reliance limits in certificates issued by the certification authority, or issuance only within a single firm or organization;

(2) A certification authority acts as an unlicensed certification authority when issuing a certificate exceeding the limits of the license.

4. (1) The division may revoke or suspend a certification authority's license for failure to comply with sections 1 to 27 of this act, or for failure to remain qualified pursuant to subsection 1 of this section;

(2) The division's actions pursuant to this subsection are subject to the procedures for adjudicative proceedings in chapter 621, RSMo.

5. The division may recognize by rule the licensing or authorization of certification authorities by other governmental entities, provided that those licensing or authorization requirements are substantially similar to those of this state. If licensing by another governmental entity is so recognized:

(1) Sections 19 to 24 of this act, which relates to presumptions and legal effects, applies to certificates issued by the certification authorities licensed or authorized by that governmental entity in the same manner as it applies to licensed certification authorities of this state; and

(2) The liability limits of section 17 of this act apply to the certification authorities licensed or authorized by that governmental entity in the same manner as they apply to licensed certification authorities of this state.

6. Unless the parties provide otherwise by contract between themselves, the licensing requirements in this section do not affect the effectiveness, enforceability or validity of any digital signature except that sections 19 to 24 of this act do not apply to a digital signature which cannot be verified by a certificate issued by a licensed certification authority. Further, the liability limits of section 17 of this act do not apply to unlicensed certification authorities.

Section 6. 1. A certified public accountant having expertise in computer security, or an accredited computer security professional, shall audit the operations of each licensed certification authority at least once each year to evaluate compliance with sections 1 to 27 of this act. The division may specify qualifications for auditors in greater detail by rule.

2. (1) Based on information gathered in the audit, the auditor shall categorize the licensed certification authority's compliance as one of the following:

(a) Full compliance, which means the certification authority appears to conform to all applicable statutory and regulatory requirements;

(b) Substantial compliance, which means the certification authority generally appears to conform to all applicable statutory and regulatory requirements; however, one or more instances of noncompliance or inability to demonstrate compliance were found in the audited sample, but were likely to be inconsequential;

(c) Partial compliance, which means the certification authority appears to comply with some statutory and regulatory requirements, but was found not to have complied or not to be able to demonstrate compliance with one or more important safeguards; or

(d) Noncompliance, which means the certification authority complies with few or none of the statutory and regulatory requirements, fails to keep adequate records to demonstrate compliance with more than a few requirements, or refused to submit to an audit;

(2) The auditor shall report the date of the audit of the licensed certification authority and resulting categorization to the division;

(3) The division shall publish in the certification authority disclosure record it maintains for the certification authority, the date of the audit and the resulting categorization of the certification authority.

3. (1) The division may exempt a licensed certification authority from the requirements of subsection 1 of this section if:

(a) The certification authority to be exempted requests exemption in writing;

(b) The most recent performance audit, if any, of the certification authority resulted in a finding of full or substantial compliance; and

(c) The certification authority declares under oath or affirmation that one or more of the following is true with respect to the certification authority:

a. The certification authority has issued fewer than six certificates during the past year and the total of the recommended reliance limits of all such certificates does not exceed ten thousand dollars;

b. The aggregate lifetime of all certificates issued by the certification authority during the past year is less than thirty days and the total of the recommended reliance

limits of all such certificates does not exceed ten thousand dollars; or

c. The recommended reliance limits of all certificates outstanding and issued by the certification authority total less than one thousand dollars;

(2) If the certification authority's declaration pursuant to subdivision (1) of subsection 3 of this section falsely states a material fact, the certification authority shall have failed to comply with the performance audit requirement of this subsection;

(3) If a licensed certification authority is exempt pursuant to this subsection, the division shall publish in the certification authority disclosure record it maintains for the certification authority a statement that the certification authority is exempt from the performance audit requirement.

Section 7. 1. The division may investigate the activities of a licensed certification authority material to its compliance with this chapter and issue orders to a certification authority to further its investigation and ensure compliance with sections 1 to 27 of this act.

2. As provided in section 5 of this act, the division may restrict a certification authority's license for its failure to comply with an order of the division, or may suspend or revoke the license of a certification authority.

3. Any person who knowingly or intentionally violates an order of the division issued pursuant to this section or section 8 of this act is subject to a civil penalty of not more than five thousand dollars per violation or ninety percent of the recommended reliance limit of a material certificate, whichever is less.

4. The division may order a certification authority in violation of sections 1 to 27 of this act to pay the costs incurred by the division in prosecuting and adjudicating proceedings relative to, and in enforcement of, the order.

5. Administrative proceedings undertaken pursuant to this section shall be conducted pursuant to chapter 536, RSMo.

Section 8. 1. A certification authority, whether licensed or not, may not conduct its business in a manner that creates an unreasonable risk of loss to subscribers of the certification authority, to persons relying on certificates issued by the certification authority, or to a repository.

2. (1) The division may publish in one or more recognized repositories brief statements advising subscribers, persons relying on digital signatures, and repositories about any activities of a licensed or unlicensed certification authority, of which the division has actual knowledge, which create a risk prohibited by subsection 1 of this section;

(2) The certification authority named in a statement as creating such a risk may protest the publication of the statement by filing a brief, written defense. Upon receipt of such a protest, the division shall:

- (a) Publish the written defense along with the division's statement;**
- (b) Publish notice that a hearing has been scheduled to determine the facts and to decide the matter; and**
- (c) Promptly give the protesting certification authority notice and a hearing as provided in chapter 536, RSMo;**
- (3) Following the hearing, the division shall:**
 - (a) Rescind the advisory statement if its publication was unwarranted pursuant to this section;**
 - (b) Cancel the advisory statement if its publication is no longer warranted;**
 - (c) Continue or amend the advisory statement if it remains warranted; or**
 - (d) Take further legal action to eliminate or reduce a risk prohibited by subsection 1 of this section;**
- (4) The division shall publish its decision in one or more recognized repositories.**

3. Nothing in sections 1 to 27 of this act shall be construed to prevent the division from exercising any and all legal methods to enforce the provisions of sections 1 to 27 of this act. The provisions of this section do not create a right of action in any person other than the division.

Section 9. 1. A licensed certification authority or subscriber shall use only a trustworthy system:

- (1) To issue, suspend or revoke a certificate;**
- (2) To publish or give notice of the issuance, suspension or revocation of a certificate; and**
- (3) To create a private key.**

2. A licensed certification authority shall disclose any material certification practice statement, and any fact material to either the reliability of a certificate which it has issued or its ability to perform its services. A certification authority may require a signed, written and reasonably specific inquiry from an identified person, and payment of reasonable compensation, as conditions precedent to effecting a disclosure required in this subsection.

Section 10. 1. A licensed certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

- (1) The certification authority has received a request for issuance signed by the prospective subscriber; and**
- (2) The certification authority has confirmed that:**
 - (a) The prospective subscriber is the person to be listed in the certificate to be issued;**
 - (b) If the prospective subscriber is acting through one or more agents, the subscriber authorized the agent or agents to have custody of the subscriber's private**

key and to request issuance of a certificate listing the corresponding public key;

(c) The information in the certificate to be issued is accurate after due diligence;

(d) The prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(e) The prospective subscriber holds a private key capable of creating a digital signature; and

(f) The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber;

(3) The requirements of this subsection may not be waived or disclaimed by the licensed certification authority or the subscriber.

2. (1) If the subscriber accepts the issued certificate, the certification authority shall publish a signed copy of the certificate in a recognized repository agreed upon by the certification authority and the subscriber named in the certificate, unless the contract between the certification authority and the subscriber provides otherwise;

(2) If the subscriber does not accept the certificate, a licensed certification authority shall not publish the certificate or shall cancel its publication if the certificate has already been published.

3. Nothing in this section precludes a licensed certification authority from conforming to standards, certification practice statements, security plans, or contractual requirements more rigorous than, but consistent with, sections 1 to 27 of this act.

4. (1) A licensed certification authority which has issued a certificate:

(a) Shall revoke a certificate immediately upon confirming that it was not issued as required by this section; or

(b) May suspend, for a reasonable period of time not to exceed forty-eight hours, a certificate which it has issued in order to conduct an investigation to confirm grounds for revocation pursuant to paragraph (a) of this subdivision;

(2) The certification authority shall give notice of the revocation or suspension to the subscriber as soon as practicable.

5. (1) The division may order the licensed certification authority to suspend or revoke a certificate which the certification authority issued if, after giving the certification authority and subscriber any required notice and opportunity for a hearing in accordance with chapter 536, RSMo, the division determines that:

(a) The certificate was issued without substantial compliance with this section; and

(b) The noncompliance poses a significant risk to persons reasonably relying on the certificate;

(2) The division may suspend a certificate for a reasonable period of time not to

exceed forty-eight hours upon determining that an emergency requires an immediate remedy.

Section 11. 1. (1) By issuing a certificate, a licensed certification authority warrants to the subscriber named in the certificate that:

(a) The certificate contains no information known to the certification authority to be false;

(b) The certificate satisfies all material requirements of sections 1 to 27 of this act; and

(c) The certification authority has not exceeded any limits of its license in issuing the certificate;

(2) The certification authority may not disclaim or limit the warranties of this subsection.

2. Unless the subscriber and certification authority otherwise agree, a certification authority, by issuing a certificate, shall:

(1) Act promptly to suspend or revoke a certificate in accordance with sections 14 and 15 of this act; and

(2) Notify the subscriber within a reasonable time of any facts known to the certification authority which significantly affect the validity or reliability of the certificate once it is issued.

3. By issuing a certificate, a licensed certification authority certifies to all who reasonably rely on the information contained in the certificate that:

(1) The information in the certificate and listed as confirmed by the certification authority is accurate;

(2) All foreseeable information material to the reliability of the certificate is stated or incorporated by reference within the certificate;

(3) The subscriber has accepted the certificate; and

(4) The licensed certification authority has complied with all applicable laws of this state governing issuance of the certificate.

4. By publishing a certificate, a licensed certification authority certifies to the repository in which the certificate is published and to all who reasonably rely on the information contained in the certificate that the certification authority has issued the certificate to the subscriber.

Section 12. 1. By accepting a certificate issued by a licensed certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that:

(1) The subscriber rightfully holds the private key corresponding to the public key listed in the certificate;

(2) All representations made by the subscriber to the certification authority and

material to information listed in the certificate are true;

(3) All material representations made by the subscriber to a certification authority or made in the certificate and not confirmed by the certification authority in issuing the certificate are true.

2. An agent, requesting on behalf of a principal that a certificate be issued naming the principal as subscriber, certifies that the agent:

(1) Holds all authority legally required to apply for issuance of a certificate naming the principal as subscriber; and

(2) Has authority to sign digitally on behalf of the principal, and, if that authority is limited in any way, that adequate safeguards exist to prevent a digital signature exceeding the bounds of the person's authority.

3. A person may not disclaim or contractually limit the application of this section, or obtain indemnity for its effects, if the disclaimer, limitation or indemnity restricts liability for misrepresentation as against persons reasonably relying on the certificate.

4. (1) By accepting a certificate, a subscriber undertakes to indemnify the issuing certification authority for any loss or damage caused by issuance or publication of a certificate in reliance on a false and material representation of fact by the subscriber, or the failure by the subscriber to disclose a material fact if the representation or failure to disclose was made either with intent to deceive the certification authority or a person relying on the certificate or was made with negligence;

(2) If the certification authority issued the certificate at the request of an agent of the subscriber, the agent personally undertakes to indemnify the certification authority pursuant to subdivision (1) of this subsection as if the agent was an accepting subscriber in his or her own right. The indemnity provided in subdivision (1) of this subsection may not be disclaimed or contractually limited in scope, however, a contract may provide consistent, additional terms regarding the indemnification.

5. In obtaining information of the subscriber material to issuance of certificate, the certification authority may require the subscriber to certify the accuracy of relevant information under oath or affirmation of truthfulness and under penalty of criminal prohibitions against false, sworn statements.

Section 13. 1. By accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature.

2. A private key is the personal property of the subscriber who rightfully holds it.

3. If a certification authority holds the private key corresponding to a public key as a fiduciary of the subscriber named in the certificate, and may use that private key only with the subscriber's prior, written approval, unless the subscriber expressly permits the certification authority to hold the private key according to other terms.

Section 14. 1. (1) Unless the certification authority and the subscriber agree otherwise, the licensed certification authority which issued a certificate which is not a transactional certificate shall suspend the certificate for a period not exceeding forty-eight hours:

(a) Upon request by a person identifying himself or herself as the subscriber named in the certificate, or as a person in a position likely to know of a compromise of the security of subscriber's private key, such as an agent, business associate, employee or member of the immediate family of the subscriber; or

(b) By order of the division pursuant to subsection 5 of section 10 of this act;

(2) The certification authority need not confirm the identity or agency of the person requesting suspension pursuant to paragraph (a) of subdivision (1) of this subsection.

2. (1) Unless the certificate provides otherwise or the certificate is a transactional certificate, the division, a court clerk, or county clerk may suspend a certificate issued by a licensed certification authority for a period of forty-eight hours, if:

(a) A person requests suspension and identifies himself or herself as the subscriber named in the certificate or as an agent, business associate, employee or member of the immediate family of the subscriber; and

(b) The requester represents that the certification authority which issued the certificate is unavailable;

(2) The division, court clerk or county clerk may:

(a) Require the person requesting suspension pursuant to subdivision (1) of this subsection to provide evidence, including a statement under oath or affirmation, regarding any information described in subdivision (1) of this subsection; and

(b) Suspend or decline to suspend the certificate in its discretion;

(3) The division, attorney general or county attorney may investigate suspensions by the division, a court clerk or a county clerk for possible wrongdoing by persons requesting suspension pursuant to subdivision (1) of this subsection.

3. (1) Immediately upon suspension of a certificate by a licensed certification authority, the licensed certification authority shall publish notice, signed by the licensed certification authority, of the suspension in any repositories specified in the certificate for publication of notice of suspension. If any repository specified in the certificate no longer exists or refuses to accept publication, or is no longer recognized

pursuant to section 25 of this act, the licensed certification authority shall publish the notice in any recognized repository;

(2) If a certificate is suspended by the division, a court clerk or county clerk, the division or clerk shall give notice as required in subdivision (1) of this subsection for a licensed certification authority, provided that the person requesting suspension pays in advance any fee required by a repository for publication of the notice of suspension.

4. A certification authority shall terminate a suspension initiated by request only:

(1) If the subscriber named in the suspended certificate requests termination of the suspension and the certification authority has confirmed that the person requesting suspension is the subscriber or an agent of the subscriber authorized to terminate the suspension; or

(2) When the certification authority discovers and confirms that the request for the suspension was made without authorization by the subscriber, provided that this subdivision does not require the certification authority to confirm a request for suspension.

5. The contract between a subscriber and a licensed certification authority may limit or preclude requested suspension by the certification authority, or may provide otherwise for termination of a requested suspension. However, if the contract limits or precludes suspension by the division, a court clerk or a county clerk when the issuing certification authority is unavailable, the limitation or preclusion shall be effective only if notice of the limitation or preclusion is published in the certificate.

6. A person may not knowingly or intentionally misrepresent to a certification authority his or her identity or authorization in requesting suspension of a certificate. Violation of this subsection is a class B misdemeanor.

7. While the certificate is suspended, the subscriber is released from the duty to keep the private key secure pursuant to subsection 1 of section 13 of this act.

Section 15. 1. A licensed certification authority shall revoke a certificate which it issued, but which is not a transactional certificate, after:

(1) Receiving a request for revocation by the subscriber named in the certificate; and

(2) Confirming that the person requesting revocation is that subscriber, or is an agent of that subscriber with authority to request the revocation.

2. A licensed certification authority shall confirm a request for revocation and revoke a certificate within one business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity and any agency of the person requesting the suspension.

3. A licensed certification authority shall revoke a certificate which it issued:

(1) Upon receiving a certified copy of the subscriber's death certificate, or upon confirming by other evidence that the subscriber is dead; or

(2) Upon presentation of documents effecting a dissolution of the subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

4. A licensed certification authority may revoke one or more certificates which it issued if the certificates are or become unreliable, regardless of whether the subscriber consents to the revocation.

5. Immediately upon revocation of a certificate by a licensed certification authority, the licensed certification authority shall publish signed notice of the revocation in any repository specified in the certificate for publication of notice of revocation. If any repository specified in the certificate no longer exists or refuses to accept publication, or is no longer recognized pursuant to section 25 of this act, the licensed certification authority shall publish the notice in any recognized repository.

6. A subscriber ceases to certify the information, as provided in section 12 of this act, and has no further duty to keep the private key secure, as required by section 13 of this act, in relation to a certificate whose revocation the subscriber has requested, beginning with the earlier of either:

(1) When notice of the revocation is published as required in subsection 5 of this section; or

(2) Two business days after the subscriber requests revocation in writing, supplies to the issuing certification authority information reasonably sufficient to confirm the request, and pays any contractually required fee.

7. Upon notification as required by subsection 5 of this section, a licensed certification authority is discharged of its warranties based on issuance of the revoked certificate and ceases to certify the information, as provided in section 11 of this act, in relation to the revoked certificate.

Section 16. A certificate shall indicate the date on which it expires. When a certificate expires, the subscriber and certification authority cease to certify the information in the certificate as provided in sections 1 to 27 of this act and the certification authority is discharged of its duties based on issuance of that certificate.

Section 17. 1. By specifying a recommended reliance limit in a certificate, the issuing certification authority and the accepting subscriber recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.

2. Unless a licensed certification authority waives application of this subsection, a licensed certification authority is:

(1) Not liable for any loss caused by reliance on a false or forged digital

signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with all material requirements of sections 1 to 27 of this act;

(2) Not liable in excess of the amount specified in the certificate as its recommended reliance limit for either:

(a) A loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or

(b) Failure to comply with section 10 of this act in issuing the certificate;

(3) Liable only for direct, compensatory damages in any action to recover a loss due to reliance on the certificate, which damages do not include:

(a) Punitive or exemplary damages;

(b) Damages for lost profits, savings or opportunity; or

(c) Damages for pain or suffering.

Section 18. 1. (1) Notwithstanding any provision in the suitable guaranty to the contrary:

(a) If the suitable guaranty is a surety bond, a person may recover from the surety the full amount of a qualified right to payment against the principal named in the bond, or, if there is more than one such qualified right to payment during the term of the bond, a ratable share, up to a maximum total liability of the surety equal to the amount of the bond; or

(b) If the suitable guaranty is a letter of credit, a person may recover from the issuing financial institution the full amount of a qualified right to payment against the customer named in the letter of credit, or, if there is more than one qualified right to payment during the term of the letter of credit, a ratable share, up to a maximum total liability of the issuer equal to the amount of the credit;

(2) Claimants may recover successively on the same suitable guaranty, provided that the total liability on the suitable guaranty to all persons making claims based upon qualified rights of payment during its term may not exceed the amount of the suitable guaranty.

2. To recover a qualified right to payment against a surety or issuer of a suitable guaranty, the claimant shall file written notice of the claim with the division stating the name and address of the claimant, the amount claimed, and the grounds for the qualified right to payment, and any other information required by rule of the division.

3. Recovery of a qualified right to payment from the proceeds of the suitable guaranty shall be forever barred unless:

(1) The claimant substantially complies with subsection 3 of this section; and

(2) Notice of the claim is filed within two years after the occurrence of the violation of any of sections 1 to 27 of this act which is the basis for the claim.

Section 19. 1. Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature if:

(1) That digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

(2) That digital signature was affixed by the signer with the intention of signing the message; and

(3) The recipient has no knowledge or notice that the signer either:

(a) Breached a duty as a subscriber; or

(b) Does not rightfully hold the private key used to affix the digital signature.

2. Nothing in sections 1 to 27 of this act precludes any symbol from being valid as a signature pursuant to other applicable law.

3. This section does not limit the authority of the department of revenue to prescribe the form of tax returns or other documents filed with the department of revenue.

Section 20. Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances. If the recipient determines not to rely on a digital signature pursuant to this section, the recipient shall promptly notify the signer of its determination not to rely on the digital signature.

Section 21. 1. A message is as valid, enforceable and effective as if it had been written on paper, if it:

(1) Bears in its entirety a digital signature; and

(2) That digital signature is verified by the public key listed in a certificate which:

(a) Was issued by a licensed certification authority; and

(b) Was valid at the time the digital signature was created.

2. Nothing in this chapter precludes any message, document or record from being considered written or in writing pursuant to other applicable state law.

Section 22. A copy of a digitally signed message is as effective, valid and enforceable as the original of the message, unless it is evident that the signer designated an instance of the digitally signed message to be a unique original, in which case only that instance constitutes the valid, effective and enforceable message.

Section 23. Unless otherwise provided by law or contract, a certificate issued by a licensed certification authority is an acknowledgement of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgement appear with the digital signature or whether the signer physically appeared before the certification authority when the digital signature was

created, if that digital signature is:

- (1) Verifiable by that certificate; and**
- (2) Affixed when that certificate was valid.**

Section 24. In adjudicating a dispute involving a digital signature, a court of this state shall presume that:

(1) A certificate digitally signed by a licensed certification authority and either published in a recognized repository or made available by the issuing certification authority or by the subscriber listed in the certificate is issued by the certification authority which digitally signed it and is accepted by the subscriber listed in it;

(2) The information listed in a valid certificate, as defined in section 3 of this act, and confirmed by a licensed certification authority issuing the certificate is accurate;

(3) If a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority, it shall have the same force and effect as the use of a manual signature; and

(4) A digital signature was created before it was time stamped by a disinterested person utilizing a trustworthy system.

Section 25. 1. A repository may apply to the division for recognition by filing a written request and providing evidence to the division that the repository meets the requirements of subsection 2 of this section. The division shall determine whether to grant or deny the request in the manner provided for adjudicative proceedings in chapter 536, RSMo.

2. The division shall recognize a repository, after finding that the repository:

(1) Is operated under the direction of a licensed certification authority;

(2) Includes a database containing:

(a) Certificates published in the repository;

(b) Notices of suspended or revoked certificates published by licensed certification authorities or other persons suspending or revoking certificates as provided in sections 14 and 15 of this act;

(c) Certification authority disclosure records for licensed certification authorities;

(d) All orders or advisory statements published by the division in regulating certification authorities; and

(e) Other information as determined by rule of the division;

(3) Operates by means of a trustworthy system;

(4) Contains no significant amount of information which the division finds is known or likely to be untrue, inaccurate or not reasonably reliable;

(5) Contains certificates published by certification authorities required to conform to rules of practice which the division finds to be substantially similar to, or

more stringent toward the certification authorities, than those of this state;

(6) Keeps an archive of certificates that have been suspended or revoked, or that have expired within at least the past three years; and

(7) Complies with other requirements prescribed by rule of the division.

3. The division's recognition of a repository may be discontinued upon the repository's written request for discontinuance filed with the division at least thirty days before discontinuance.

4. The division may discontinue recognition of a repository:

(1) Upon passage of an expiration date specified by the division in granting recognition; or

(2) In accordance with the procedures for adjudicative proceedings prescribed by chapter 536, RSMo, if the division concludes that the repository no longer satisfies the conditions for recognition listed in this section or in rules of the division.

Section 26. 1. Notwithstanding any disclaimer by the repository or any contract to the contrary between the repository, a certification authority, or a subscriber, a repository is liable for a loss incurred by a person reasonably relying on a digital signature verified by the public key listed in a suspended or revoked certificate if:

(1) The loss was incurred more than one business day after receipt by the repository of a request to publish notice of the suspension or revocation; and

(2) The repository had failed to publish the notice of suspension or revocation when the person relied on the digital signature.

2. Unless waived, a recognized repository or the owner or operator of a recognized repository is:

(1) Not liable:

(a) For failure to publish notice of a suspension or revocation, unless the repository has received notice of publication and one business day has elapsed since the notice was received;

(b) For any damages pursuant to subsection 1 of this section in excess of the amount specified in the certificate as the recommended reliance limit;

(c) For misrepresentation in a certificate published by a licensed certification authority;

(d) For accurately recording or reporting information which a licensed certification authority, the division, a county clerk or court clerk has published as provided in sections 1 to 27 of this act, including information about suspension or revocation of a certificate; or

(e) For reporting information about a certification authority, a certificate or a subscriber, if such information is published as provided in sections 1 to 27 of this act or a rule of the division, or is published by order of the division in the performance of

its licensing and regulatory duties pursuant to sections 1 to 27 of this act; and

(2) Liable pursuant to subsection 1 of this section only for direct compensatory damages, which do not include:

- (a) Punitive or exemplary damages;**
- (b) Damages for lost profits, savings or opportunity; or**
- (c) Damages for pain or suffering.**

Section 27. The following governmental entity records are exempt from chapter 610, RSMo, and are not considered public records for the purposes of that chapter:

(1) Records containing information that would disclose, or might lead to the disclosure of private keys, asymmetric cryptosystems or algorithms; or

(2) Records, the disclosure of which might jeopardize the security of an issued certificate or a certificate to be issued.

Unofficial

✓

Bill

Copy