FIRST REGULAR SESSION

SENATE BILL NO. 37

92ND GENERAL ASSEMBLY

INTRODUCED BY SENATORS KLINDT AND KINDER.

Pre-filed December 1, 2002, and 1,000 copies ordered printed.

TERRY L. SPIELER, Secretary.

0421S.01I

AN ACT

To repeal sections 28.600, 28.603, 28.606, 28.609, 28.612, 28.615, 28.618, 28.621, 28.624, 28.627, 28.630, 28.633, 28.636, 28.639, 28.642, 28.645, 28.648, 28.651, 28.654, 28.657, 28.660, 28.663, 28.666, 28.669, 28.672, 28.675, 28.678, and 28.681, RSMo, relating to uniform electronic transactions act, and to enact in lieu thereof seventeen new sections relating to the same subject.

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

Section A. Sections 28.600, 28.603, 28.606, 28.609, 28.612, 28.615, 28.618, 28.621, 28.624, 28.627, 28.630, 28.633, 28.636, 28.639, 28.642, 28.645, 28.648, 28.651, 28.654, 28.657, 28.660, 28.663, 28.666, 28.669, 28.672, 28.675, 28.678, and 28.681, RSMo, are repealed and seventeen new sections enacted in lieu thereof, to be known as sections 432.200, 432.205, 432.210, 432.215, 432.220, 432.225, 432.230, 432.235, 432.240, 432.245, 432.250, 432.255, 432.260, 432.265, 432.270, 432.275, and 432.295, to read as follows:

432.200. Section 432.200 to section 432.295 may be cited as the "Uniform Electronic Transactions Act".

432.205. As used in sections 432.200 to 432.295, the following terms shall mean:

(1) "Agreement", the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction;

(2) "Automated transaction", a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in

forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction;

(3) "Computer program", a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result;

(4) "Contract", the total legal obligation resulting from the parties' agreement as affected by section 432.200 to section 432.295 and other applicable law;

(5) "Electronic", relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities;

(6) "Electronic agent", a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual;

(7) "Electronic record", a record created, generated, sent, communicated, received, or stored by electronic means;

(8) "Electronic signature", an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record;

(9) "Governmental agency", an executive, legislative or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a state or of a county, municipality, or other political subdivision of a state;

(10) "Information", data, text, images, sounds, codes, computer programs, software, databases, or the like;

(11) "Information processing system", an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information;

(12) "Person", an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity;

(13) "Record", information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form;

(14) "Security procedure", a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption or callback, or other acknowledgment procedures;

(15) "State", a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the

jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village, which is recognized by federal law or formally acknowledged by a state;

(16) "Transaction", an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

432.210. 1. Except as otherwise provided in subsection 2, sections 432.200 to 432.295 apply to electronic records and electronic signatures relating to a transaction.

2. Sections 432.200 to 432.295 do not apply to a transaction to the extent it is governed by:

(1) A law governing the creation and execution of wills, codicils, or testamentary trusts; and

(2) The Uniform Commercial Code other than sections 400.1-107, 400.1-206, 400.2-101 to 400.2-725, RSMo, and sections 400.2A-101 to 400.2A-532, RSMo.

3. Sections 432.200 to 432.295 apply to an electronic record or electronic signature otherwise excluded from the application of sections 432.200 to 432.295 under subsection 2 of this section to the extent it is governed by a law other than those specified in subsection 2 of this section.

4. A transaction subject to sections 432.200 to 432.295 is also subject to other applicable substantive law.

432.215. Sections 432.200 to 432.295 apply to any electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after the effective date of sections 432.200 to 432.295.

432.220. 1. Sections 432.200 to 432.295 do not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.

2. Sections 432.200 to 432.295 apply only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

3. A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

4. Except as otherwise provided in sections 432.200 to 432.295, the effect of any of its provisions may be varied by agreement. The presence in certain provisions of sections 432.200 to 432.295 of the words "unless otherwise agreed", or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.

5. Whether an electronic record or electronic signature has legal consequences is determined by sections 432.200 to 432.295 and other applicable law.

432.225. Sections 432.200 to 432.295 must be construed and applied:

(1) To facilitate electronic transactions consistent with other applicable law;

(2) To be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices; and

(3) To effectuate its general purpose to make uniform the law with respect to the subject of sections 432.200 to 432.295 among states enacting it.

432.230. 1. A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

2. A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

3. If a law requires a record to be in writing, an electronic record satisfies the law.

4. If a law requires a signature, an electronic signature satisfies the law.

432.235. 1. If parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.

2. If a law other than sections 432.200 to 432.295 requires a record to be posted or displayed in a certain manner, to be sent, communicated, or transmitted by a specified method, or to contain information that is formatted in a certain manner, the following rules apply:

(1) The record must be posted or displayed in the manner specified in the other law;

(2) Except as otherwise provided in subdivision (2) of subsection 4 of this section, the record must be sent, communicated, or transmitted by the method specified in the other law;

(3) The record must contain the information formatted in the manner specified in the other law.

3. If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

4. The requirements of this section may not be varied by agreement, but:

(1) To the extent a law other than sections 432.200 to 432.295 requires

information to be provided, sent, or delivered in writing but permits that requirement to be varied by agreement, the requirement under subsection 1 of this section that the information be in the form of an electronic record capable of retention may also be varied by agreement; and

(2) A requirement under a law other than sections 432.200 to 432.295 to send, communicate, or transmit a record by first-class mail, postage prepaid, may be varied by agreement to the extent permitted by the other law.

432.240. 1. An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

2. The effect of an electronic record or electronic signature attributed to a person under subsection 1 of this section is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.

432.245. If a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply:

(1) If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record;

(2) In an automated transaction involving an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:

(a) Promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;

(b) Takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and

(c) Has not used or received any benefit or value from the consideration, if any, received from the other person;

(3) If neither subdivision (1) nor subdivision (2) of this section applies, the

change or error has the effect provided by other law, including the law of mistake, and the parties' contract, if any;

(4) Subdivisions (2) and (3) of this section may not be varied by agreement.

432.250. If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.

432.255. 1. If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

(1) Accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

(2) Remains accessible for later reference.

2. A requirement to retain a record in accordance with subsection 1 of this section does not apply to any information the sole purpose of which is to enable the record to be sent, communicated, or received.

3. A person may satisfy subsection 1 of this section by using the services of another person if the requirements of that subsection are satisfied.

4. If a law requires a record to be presented or retained in its original form, or provides consequences if the record is not presented, or retained in its original form, that law is satisfied by an electronic record retained in accordance with subsection 1 of this section.

5. If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with subsection 1 of this section.

6. A record retained as an electronic record in accordance with subsection 1 of this section satisfies a law requiring a person to retain a record for evidentiary, audit or like purposes, unless a law enacted after the effective date of sections 432.200 to 432.295 specifically prohibits the use of an electronic record for the specified purpose.

7. This section does not preclude a governmental agency of this state from specifying additional requirements for the retention of a record subject to the agency's jurisdiction.

432.260. In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

432.265. In an automated transaction, the following rules apply:

(1) A contract may be formed by the interaction of electronic agents of the

parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements;

(2) A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance;

(3) The terms of the contract are determined by the substantive law applicable to it.

432.270. 1. Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it:

(1) Is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;

(2) Is in a form capable of being processed by that system; and

(3) Enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient.

2. Unless otherwise agreed between a sender and the recipient, an electronic record is received when:

(1) It enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and

(2) It is in a form capable of being processed by that system.

3. Subsection 2 of this section applies even if the place the information processing system is located is different from the place the electronic record is deemed to be received under subsection 4 of this section.

4. Unless otherwise expressly provided in the electronic record or agreed between the sender and the recipient, an electronic record is deemed to be sent from the sender's place of business and to be received at the recipient's place of business. For purposes of this subsection, the following rules apply:

(1) If the sender or recipient has more than one place of business, the place of business of that person is the place having the closest relationship to the underlying transaction;

(2) If the sender or the recipient does not have a place of business, the place

of business is the sender's or recipient's residence, as the case may be.

5. An electronic record is received under subsection 2 of this section even if no individual is aware of its receipt.

6. Receipt of an electronic acknowledgment from an information processing system described in subsection 2 of this section establishes that a record was received but, by itself, does not establish that the content sent corresponds to the content received.

7. If a person is aware that an electronic record purportedly sent under subsection 1 of this section, or purportedly received under subsection 2 of this section, was not actually sent or received, the legal effect of the sending or receipt is determined by other applicable law. Except to the extent permitted by the other law, the requirements of this subsection may not be varied by agreement.

432.275. 1. In this section, "transferable record" means an electronic record that:

(1) Would be a note under sections 400.3-101 to 400.3-605, RSMo, or a document under sections 400.7-101 to 400.7-604, RSMo, if the electronic record were in writing; and

(2) The issuer of the electronic record expressly has agreed is a transferable record.

2. A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

3. A system satisfies subsection 2 of this section, and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that:

(1) A single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in subdivisions (4), (5), and (6) of subsection 3 of this section, unalterable;

(2) The authoritative copy identifies the person asserting control as:

(a) The person to which the transferable record was issued; or

(b) If the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;

(3) The authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(4) Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(5) Each copy of the authoritative copy and any copy of a copy is readily

identifiable as a copy that is not the authoritative copy; and

(6) Any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

4. Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in subdivision (20) of section 400.1-201, RSMo, of the uniform commercial code, of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under the uniform commercial code, including, if the applicable statutory requirements under section 400.3-302(a), 400.7-501, or 400.9-308, RSMo, of the uniform commercial code are satisfied, the rights and defenses of a holder in due course, a holder to which a negotiable document of title has been duly negotiated, or a purchaser, respectively. Delivery, possession, and endorsement are not required to obtain or exercise any of the rights under this subsection.

5. Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under the uniform commercial code.

6. If requested by a person against which enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.

432.295. If any provision of sections 432.200 to 432.295 or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of sections 432.200 to 432.295 which can be given effect without the invalid provision or application, and to this end the provisions of sections 432.200 to 432.295 are severable.

[28.600. Sections 28.600 to 28.678 are known as the "Missouri Digital Signatures Act".**]**

[28.603. Sections 28.600 to 28.678 shall be construed to be 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.**]**

[28.606. For the purposes of sections 28.600 to 28.678, 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 28.609;

(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 commissions 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 28.600 to 28.678;

(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 28.672;

(28) "Recommended reliance limit", the limitation on the monetary amount recommended for reliance on a certificate pursuant to subsection 1 of section 28.648;

(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 28.636; 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 or division of credit unions 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 28.609;

c. States that it is issued for filing pursuant to the provisions of sections 28.600 to 28.678;

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 subdivision 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.**]**

[28.609. 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 28.600 to 28.678.

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 28.600 to 28.678, 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 record keeping 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. No rule or portion of a rule promulgated pursuant to the authority of sections 28.600 to 28.678 shall become effective unless it has been promulgated pursuant to the provisions of chapter 536, RSMo.**]**

[28.612. 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 28.600 to 28.678;

(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 28.600 to 28.678, 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 28.654 to 28.669, which relate to presumptions and legal effects, apply to certificates issued by the certification authorities licensed or authorized by that governmental entity in the same manner as they apply to licensed certification authorities of this state; and

(2) The liability limits of section 28.648 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 28.654 to 28.669 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 28.648 do not apply to unlicensed certification authorities.**]**

[28.615. 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 28.600 to 28.678. 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.**]**

[28.618. 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 28.600 to 28.678.

2. As provided in section 28.612, 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 28.621 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 28.600 to 28.678 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.**]**

[28.621. 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 28.600 to 28.678 shall be construed to prevent the division from exercising any and all legal methods to enforce the provisions of sections 28.600 to 28.678. The provisions of this section do not create a right of action in any person other than the division.**]**

[28.624. 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.**]**

[28.627. 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 28.600 to 28.678.

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.**]**

[28.630. 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 28.600 to 28.678; 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 28.639 and 28.642; 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.**]**

[28.633. 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 the issuance of a 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.**]**

[28.636. 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, the certification authority 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.**]**

[28.639. 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 the 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 28.627;

(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 28.672, 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 28.636.**]**

[28.642. 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 28.672, the licensed certification authority shall publish the notice in any recognized repository.

6. A subscriber ceases to certify the information, as provided in section 28.633, and has no further duty to keep the private key secure, as required by section 28.636, 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 28.630, in relation to the revoked certificate.**]**

[28.645. 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 28.600 to 28.678 and the certification authority is discharged of its duties based on issuance of that certificate.**]**

[28.648. 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 28.600 to 28.678;

(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 28.627 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.**]**

[28.651. 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 2 of this section; and

(2) Notice of the claim is filed within two years after the occurrence of the violation of any of sections 28.600 to 28.678 which is the basis for the claim.**]**

[28.654. 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 28.600 to 28.678 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.**]**

[28.657. 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.**]**

[28.660. 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.**]**

[28.663. 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.**]** **[**28.666. Unless otherwise

provided by law or contract, a certificate issued by a licensed certification authority is an acknowledgment of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgment 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.**]**

[28.669. 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 28.606, 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.**]**

[28.672. 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 28.639 and 28.642;

(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.**]**

[28.675. 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

28.600 to 28.678, 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 28.600 to 28.678 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 28.600 to 28.678; 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.**]**

[28.678. 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.**]**

[28.681. 1. Any statement, document or notice required or permitted to be filed with or transmitted by the secretary of state, or any judicial decree requiring the filing of such document, except any document or judicial decree relating to his or her statutory or constitutional duties relating to elections, may be filed, transmitted, stored and maintained in an electronic format prescribed by the secretary of state. No statement, document or notice submitted or filed in an electronic format need be submitted or filed in duplicate. Nothing in this section shall require the secretary of state to accept or transmit any statement, document or notice in an electronic format.

2. Any statutory requirement that a statement, document or notice filed with the secretary of state be signed by any person shall be satisfied by an electronically transmitted identification in a format prescribed by the secretary of state.

3. Any requirement that a statement, document or notice filed with the secretary of state be notarized may be satisfied by a properly authenticated identification in a format prescribed by the secretary of state. The execution of any statement, document or notice pursuant to this subsection constitutes an affirmation under penalty of perjury that the facts stated therein are true and that such person or persons are duly authorized to execute such statement, document or notice, or are otherwise required to file such statement, document or notice.

4. The secretary of state may promulgate rules pursuant to the provisions of section 536.024, RSMo, to effectuate the provisions of this section.**]**

T