WEST VIRGINIA
SECRETARY OF STATE
JOE MANCHIN, III
ADMINISTRATIVE LAW DIVISION

Form #4

Do Not Mark In This Box

FILED

2001 OCT 10 P 3:21

OFFICE WEST VIRGINIA
SECRETARY OF STATE

NOTICE OF RULE MODIFICATION OF A PROPOSED RULE

AGENCY: Secretary of State TITLE NUMBER: 153

CITE AUTHORITY: §39A-3-3

AMENDMENT TO AN EXISTING RULE: YES X NO ___

IF YES, SERIES NUMBER OF RULE BEING AMENDED: 30

TITLE OF RULE BEING AMENDED: ~~Use of Electronic Signatures by State Agencies~~ Use of Digital Signatures, State Certification Authority & State Repository

IF NO, SERIES NUMBER OF RULE BEING PROPOSED: ___

TITLE OF RULE BEING PROPOSED: ___

THE ABOVE PROPOSED LEGISLATIVE RULES, FOLLOWING REVIEW BY THE LEGISLATIVE RULE MAKING REVIEW COMMITTEE, IS HEREBY MODIFIED AS A RESULT OF REVIEW AND COMMENT BY THE LEGISLATIVE RULE MAKING REVIEW COMMITTEE. THE ATTACHED MODIFICATIONS ARE FILED WITH THE SECRETARY OF STATE.

Authorized Signature

$8.40

TITLE 153
LEGISLATIVE RULE
~~JOINT RULE OF THE~~ SECRETARY OF STATE ~~AND STATE AUDITOR~~

SERIES 30
~~USE OF ELECTRONIC SIGNATURES BY STATE AGENCIES~~ USE OF DIGITAL SIGNATURES, STATE CERTIFICATION AUTHORITY AND STATE REPOSITORY

§153-30-1. General.

1.1. Scope. -- This legislative rule establishes the requirements for state agencies intending to use or accept electronic signatures on filings and other messages in electronic form which require the signature of an authorized person.

1.2. Authority. -- W. Va. Code ~~§39-5-4~~ §39A-3-3.

1.3. Filing Date. -- ~~April 1, 1999.~~

1.4. Effective Date. -- ~~April 1, 1999.~~

§153-30-2. Definitions

~~2.4.~~2.1. "Accept an electronic signature" means to accept an electronic record that requires the signature of an authorized person when that electronic record contains an electronic signature in lieu of an original signature.

~~2.1.~~2.2. "Agency" includes any state, county or municipal office, department, division, bureau, board, commission, public corporation or other governmental entity created by the State Constitution, statute, rule or executive order.

~~2.2.~~2.3. "Authorized officer" means the elected or appointed official, or a designee, who has authority to act on behalf of the agency.

2.4. "Certificate" or "digital signature certificate" means a computer-based record that:

2.4.a. Identifies the certification authority issuing it;

2.4.b. Names or identifies its subscriber;

2.4.c. Contains the subscriber's public key; and

2.4.d. Is digitally signed by the certification authority issuing it.

2.5. "Certificate Authority" means an entity issuing a certificate.

2.6. "Certification practice statement" means a declaration of the practices that a certification authority employs in issuing, managing, suspending, and revoking certificates and providing access to them.

2.7. "Corresponding," with reference to keys, means to belong to the same key pair.

~~2.5~~.2.8. "Electronic" means electrical, digital, magnetic, optical, electromagnetic, or any other technology that is similar to these technologies.

~~2.6~~.2.9. "Electronic record" means a record generated, communicated, received, or stored by electronic means.

~~2.3~~.2.10. "Electronic signature" means any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual signature. Electronic signatures include, but are not limited to digital marks and digital signatures:

~~2.3.a. A "digitized signature" which consists of a handwritten signature entered on a recording device utilizing electronic recording software which simultaneously converts the image created to a digital record and attaches it to the electronic document to which it relates;~~

~~2.3.b~~.2.10.a. A "digital mark" which consists of an electronic code indicating approval or confirmation which is entered into a protected digital record following access protocols which identify the user and require a password, personal identification number, encrypted card or other security device which restricts access to one or more authorized individuals; and

~~2.3.c~~.2.10.b. A "digital signature" means an electronic signature consisting of a message transformed using an asymmetric cryptosystem so that a person having the initial message and the signer's public key can accurately determine whether the message was created using the corresponding private key, and whether the initial message has been altered since the message was transformed.

2.10.b.1. A "digitized signature" which may consist of a handwritten signature entered on a recording device utilizing electronic recording software which simultaneously converts the image created to a digital record and attaches it to the electronic document to which it relates or a graphic image file of a person's signature and is attached to the electronic document to which it relates may be used for illustrative purposes and shall not be construed as or considered an "electronic signature" in the context of this legislation.

2.11. "Key pair" means two corresponding keys, referred to as a private key and a public key, which are mathematically related in an asymmetric cryptosystem, where:

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

2.11.b. "Public key" means the key of a key pair used to verify a digital signature; and

2.11.c. The corresponding keys have the properties that:

2.11.c.1. The private key can encrypt a message which only the public key can decrypt; and

2.11.c.2. Even if the public key is known, it is computationally infeasible to discover the private key.

2.12. "Operational period" of a certificate begins on the date and time the certificate is issued by the certification authority (or on a later date and time certain if stated in the certificate) and ends on the date and time it expires as noted in the certificate, or is earlier revoked, but does not include any period during which a certificate is suspended.

~~2.7.~~2.13. "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form, which includes an official record, including but not limited to a message, document, form, return or other instrument which is transmitted electronically from an authorized officer or other person to an agency to meet the requirements of law or to execute an essential transaction. An informal communication ~~will~~ is not ~~be~~ considered an electronic record for purposes of this rule.

2.14. "Repository" means a system for issuing, storing, retrieving, managing, and processing digital signature/mark certificates and any other relevant information, including information relating to the status of a certificate.

2.15. "State certificate processing authority" means an entity with which the State of West Virginia contracts to issue certificates on behalf of the State.

2.16. "Subscriber" means a person who:

2.16.a. Is the subject named or otherwise identified in a certificate;

2.16.b. Controls the private key that corresponds to the public key listed in that certificate; and

2.16.c. Is the person to whom digitally signed messages verified by reference to the certificate are to be attributed.

2.17. "Trustworthy system" means computer hardware, software, and procedures that:

2.17.a. Are reasonably secure from intrusion and misuse;

2.17.b. Provide a reasonably reliable level of availability, reliability, and correct operation;

2.17.c. Are reasonably suited to performing their intended functions; and

2.17.d. Adhere to generally accepted security principles.

§153-30-3. Agency Use of Electronic Records and Electronic Signatures Generally.

3.1. Each agency shall determine if, and the extent to which, it will send and receive electronic records and electronic signatures to and from other persons and otherwise create, use, store, and rely upon electronic records and electronic signatures.

3.2. In any case where an agency decides to send or receive electronic records, or to accept document filings by electronic records, the agency may, giving due consideration to security, specify:

3.2.a. The manner and format in which ~~such~~ the electronic records must be created, sent, received, and stored;

3.2.b. If ~~such~~ the electronic records must be signed, the type of electronic signature that is required or acceptable, the manner and format in which the signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by the sender of the electronic record to facilitate the process;

3.2.c. Control processes and procedures as appropriate to ensure adequate integrity, security, confidentiality, and auditability of the electronic records; and

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

3.3. Whenever any rule of law requires or authorizes the filing of any information, notice, lien, or other document or record with any agency, a filing made by an electronic record has the same force and effect as a filing made on paper in all cases where the agency has authorized or agreed to the electronic filing and the filing is made in accordance with applicable rules or agreement.

3.4. Subject to prior notice by the receiving agency, submission of an electronic record containing an electronic signature record constitutes an agreement by the sender to accept equivalent electronic signature types on return or corresponding electronic records.

§153-30-4. Agency Procedures for Adoption, Modification or Revocation of Electronic Signature Acceptance

4.1. Each agency shall evaluate the types of records received to determine which records can be accepted with electronic signatures, and which form of electronic signature meets the security requirements of the specific transaction.

4.1.a. An electronic record, which requires the signature of a person under oath before an authorized official or with the acknowledgment of a notary public, may ~~not~~ be accepted with an electronic signature. ~~prior to the authorization in law of an electronic attestation.~~

4.1.b. An electronic record, which requires the signature of a person under a self-executing oath, may be accepted with a digital signature or other electronic signature, which is encrypted, capable of verifying the identity of the signer, and capable of discerning any alteration of the message since transformation.

4.2. An agency may accept an electronic record containing an electronic signature only after complying with the procedural requirements of this rule.

4.3. For each type of electronic record on which an agency is willing to accept an electronic signature in satisfaction of a legal signature requirement, the agency shall publish a notice through the Secretary of State which shall specify:

4.3.a. The name of the agency authorizing use of the electronic record;

4.3.b. A description of the type of electronic record;

4.3.c. The type or types of electronic signature that will be accepted on the record;

4.3.d. A description of any restrictions on whom may electronically sign the record;

4.3.e. The date that the electronic record with an electronic signature will first be accepted;

4.3.f. Specifications for any procedures or technology that must be used to create, communicate, or store the electronic signature; and

4.3.g. The name of one or more contacts within the agency who can provide additional information, along with the address, telephone and/or e-mail address of the contact person.

4.4. An agency subject to the Administrative Procedures Act, W. Va. Code Chapter §29A-1-1 et seq., shall comply with the notice requirements of subsection 4.3 of this section prior to acceptance of electronic signatures on electronic records, as follows:

4.4.a. When an agency intends to accept electronic signatures on electronic records sent to or received from employees within the agency or within the department of which the agency is a subdivision, the authorized officer shall give notice as required by subsection 4.3 of this section to the appropriate personnel;

4.4.b. When an agency intends to accept electronic signatures on electronic records sent to or received from other agencies outside the receiving agency's department, the agency shall give notice to the Secretary of State as required by subsection 4.3 of this section, at least thirty (30) days before first acceptance. The Secretary of State shall maintain a database of the agencies and the specific information provided for each type of record;

4.4.c. When an agency intends to use or accept electronic signatures on electronic records received from a person acting on his or her own behalf, or from a person acting on behalf of an entity not subject to the Administrative Procedures Act, or private concerns, the agency shall give notice as required by subsection 4.3 of this section, at least thirty (30) days prior to first acceptance, by publication in the State Register; and

4.4.d. The agency shall make available a summary of procedural information to assist persons desiring to file electronically and utilize electronic signatures.

4.5. An agency not subject to the Administrative Procedures Act, including county and municipal agencies, shall comply with the notice requirements of subsection 4.3 of this section prior to its use or acceptance of electronic signatures on electronic records as follows:

4.5.a. When an agency intends to use or accept electronic signatures on electronic records received from employees within the agency or within the governmental entity of which the agency is a subdivision, the authorized officer shall give notice as required by subsection 4.3 of this section to the appropriate personnel; and

4.5.b. When an agency intends to use or accept electronic signatures on electronic records received from a person acting on his or her own behalf, or from a person acting on behalf of an entity other than the governmental entity of which the agency is a subdivision, or private concerns, the agency shall give notice as required by subsection 4.3 of this section, at least thirty (30) days prior to first acceptance, by publication as a Class I legal advertisement in a qualified newspaper published in the municipality or county where the principal office of the agency is located.

4.6. An agency may modify, suspend, or terminate the acceptance of the electronic signatures after giving notice according to the requirements of this section; provided, that

4.6.a. Notice shall be given as required at least one hundred twenty (120) days prior to the termination of acceptance of a type of electronic signature; and

4.6.b. In an emergency which prevents the acceptance of the electronic signature, an agency may suspend acceptance of electronic signatures and require filings and signatures be provided on paper. The agency shall provide reasonable notice to potential filers.

4.7. Nothing in this rule shall be construed to require an agency to accept electronic signatures in lieu of written signatures.

4.8. Nothing in this rule shall be construed to allow an agency, without the specific authority of statute, to require a person acting on his or her own behalf, or a person acting on behalf of an entity other than a governmental entity to use an electronic signature in order to complete an essential filing.

4.9. All agencies may enter into agreements with other agencies relating to the use and acceptance of electronic signatures on electronic records communicated between those agencies.

§153-30-5. Requirements for Acceptance of Digital Marks.

5.1. An agency which intends to accept digital marks shall establish, at a minimum, the security measures and procedural requirements as provided in this section.

5.2. The agency shall establish a secure registry of persons authorized to sign filings and records, or shall utilize a secure registry for verification of the identity of the signer.

5.2.a. A person who desires to become authorized to file with the agency using a digital mark shall file with the secure registry a signed statement verifying that he or she:

5.2.a.1. Will not share with any other person the password, code or other security key required for use of the mark;

5.2.a.2. Agrees that the use of the mark represents confirmation of a record;

5.2.a.3. Agrees to notify the agency immediately once he or she becomes aware that the security key is compromised; and

5.2.a.4. Understands that the provisions of W. Va. Code §61-3C-10 prescribes the penalties for the unauthorized disclosure of a password, identifying code, personal identification number or other confidential security information.

5.2.b. The agency or secure registry shall issue an authorized person an identifying number and shall enter that number, name and date of authorization into the registry

5.2.c. The appropriate administrator shall revoke the access privileges of the authorized person upon termination of authority.

5.3. Each authorized person shall ~~utilize~~ use a unique number, password or other personal authorization, which shall be encrypted, and which shall indicate the approval of that person.

5.4. The size, frequency of required changes and other elements of the security code shall meet state or agency security policies, if any are in effect. If no policy has been adopted, the elements of the security code shall meet generally acceptable standards for password security.

§153-30-6. Security Requirements for Acceptance of Digital Signature.

~~5.5.~~ 6.1. The agency shall establish the necessary computer hardware and software security, consistent with current generally acceptable standards for secure transactions, to prevent alteration of the electronic

filing and to assure protection of the security key, and shall document that those features and measures are in place.

~~5.5.a.~~ 6.1.a. Information resources shall be protected by use of access control systems. Access control systems can be either internal (passwords, encryption, access control lists, constrained user interfaces) or external (port protection devices, firewalls, host-based authentication).

~~5.5.b~~ 6.1.b. Rules for access to resources (including internal and external telecommunications and networks) shall be established by the information/application owner or manager who is responsible for the resources.

~~5.5.c.~~ 6.1.c. When confidential or sensitive information from one agency is received by another agency in connection with the transaction of official business, the receiving agency shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency.

~~5.5.d.~~ 6.1.d. Pursuant to state security policy, information security and audit controls shall be incorporated into new systems.

~~5.5.e.~~ 6.1.e. Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited, and that violators are subject to criminal prosecution.

~~5.6.~~ 6.2. For filings involving financial transmissions or financial liability, an agency may establish dollar limitations on the amount of a transaction for which a digital signature and digital mark will be accepted.

§153-30-7 Requirements for Acceptance of Digital Signatures

7.1. The Secretary of State, pursuant to legislative rule as required by W. Va. Code ~~§39-5-4~~§39A-3-3, shall establish a certification authority for the registration and issuance of certificates to subscribers for the use of digital signatures, as provided in ~~Secretary of State Rule, Use of Digital Signatures, State Certification Authority and State Repository, 153CSR31.~~ in this rule.

7.2. An agency, which agrees to accept a digital signature in connection with an electronic filing, shall obtain, install and test the essential hardware and software prior to giving notice of the intent to accept digital signatures.

7.3. Any authorized officer or other authorized person who becomes a subscriber to the certification authority maintained by the Secretary of State and who maintains an authorized key pair shall be permitted to use a digital signature on any electronic document which the agency agrees to accept.

§153-30-8. Requirements for Acceptance of Other Forms of Electronic Signatures

8.1. When an agency desires to accept a newly developed form of electronic signature not specifically listed in the definition of electronic signature contained in this rule, the agency shall apply to the Secretary of State for authority to accept the electronic signature.

8.2. To be acceptable as an electronic signature, the technology shall:

8.2.a Allow the receiving agency to verify the identity of the sender; and

8.2.b Allow the receiving agency to determine whether the message received has been altered en route.

8.3. The agency is responsible for assuring the security of the record following its acceptance.

§153-30-9. Selection of State Authority; Eligibility Requirements for Registration and Certificate Management and Authority.

9.1. The Secretary of State shall initiate a procurement process to obtain the services of one or more private vendors, at the discretion of the state, to provide services and systems to enable the Secretary of State to manage and authorize the issuance of digital signature and digital mark certificates.

9.2. The Secretary of State shall initiate a procurement process to obtain the software and systems to serves as the state repository or to obtain the services of one or more private vendors, at the discretion of the Secretary of State, to serve as a state repository.

9.3. The Secretary of State may contract with a vendor for services of a state certification authority and a state repository.

9.4. The state certification authority may issue a certificate that binds a public key to any authorized person for the purpose of verifying a digital signature created by that person on an electronic record in his or her capacity as an agent of the state or any agency in West Virginia, as defined by subsection 2.1. of this rule.

9.5. The state certificate management authority may issue a certificate to any person for the purpose of verifying a digital signature created by that person on an electronic record filed with any agency, as defined by subsection 2.1. of this rule.

9.6. For the duration of the contract, the state certification authority and state repository shall comply with the provisions of this rule.

9.7. To be qualified for selection as a state certification authority and state repository, a vendor shall:

9.7.a. Maintain a system of internal security controls to restrict access to systems and data only to authorized personnel, and conduct appropriate clearances of those personnel to ensure that they have demonstrated knowledge and proficiency in following the requirements of this rule, and have never been convicted of a felony or of any other crime involving fraud or misrepresentation;

9.7.b. File with the secretary of state a corporate surety bond or letter of credit for a term of at least five years, in the amount of fifty thousand dollars ($50,000);

9.7.c. Use a trustworthy system, including a secure means for limiting access to its private key;

9.7.d. Be licensed to do business in the state and registered as a vendor for the state;

9.7.e. Provide the Secretary of State with a copy of an unqualified performance audit performed in accordance with standards set in the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards No. 70 (S.A.S. 70) "Reports on the Processing of Service Transactions by Service Organizations" (1992) to ensure that the certification authority's practices and policies are consistent with the certification authority's stated control objectives. The audit shall include a SAS 70 Type Two audit -- A

Report of Policies and Procedures Placed in Operation and Test of Operating Effectiveness-- receiving an unqualified opinion; and

9.7.f. Meet any other requirements specified in the request for proposal and contract.

§153-30-10. Requirements for State Certificate Management Authority Practice.

10.1. The state certification authority shall provide the Secretary of State at least annually, or upon any significant change in procedures, a certification practice statement detailing the security and procedural steps utilized in the issuance, management, suspension, and revocation of certificates and authentication of the identity of persons named in certificates.

10.2. The Secretary of State shall publish electronically the certification practice statement within thirty (30) days after it is filed.

10.3. The state certification authority shall use only a trustworthy system to:

10.3.a. Issue, suspend, or revoke a certificate;

10.3.b. Publish or give notice of the issuance, suspension, or revocation of a certificate; or

10.3.c. Create and protect private keys.

10.4. Upon a written, signed and reasonably specific inquiry from an identified person, the state certification authority shall disclose any fact material to the reliability of a certificate that it has issued. The certification authority may require payment of reasonable compensation before making this disclosure.

§153-30-11. Requirements for State Repository Practice.

11.1. The state repository shall provide the Secretary of State at least annually, or upon any significant change in procedures, a practice statement detailing the operation of the repository, the conduct of its repository services, the processes for publishing certificates and notices of revocation into the repository, the processes for obtaining copies of certificates and checking certificate status, and all security and procedural steps related to the certificates.

11.2. The Secretary of State shall publish electronically the practice statement within thirty (30) days after it is filed.

11.3. The state repository shall provide all repository services by means of a trustworthy system.

11.4. Upon a written, signed and reasonably specific inquiry from an identified person, the state repository shall disclose any fact material to the reliability of a specific verification transaction. The state repository may require payment of reasonable compensation before making this disclosure.

11.5. The state repository shall provide an online database containing at least:

11.5.a. All valid certificates published into the database by state certification authorities; and

11.5.b. All notices of revocation of the certificates published into the directory by state certification authorities.

11.6. The state repository shall enable state certification authorities to add information, including certificates and notices of certificate revocation, to the database in a prompt, reasonable, and secure manner.

11.7. The state repository shall store certificates issued by state certification authorities that are no longer valid and provide copies of them on request. The state repository shall also store other information regarding certificates, notices of revocation, certification practice statements, and other matters relating to the services provided by state certification authorities, and shall make copies of the information available on request.

11.8. The state repository shall provide any additional information and services specified in its contract with the state.

11.9. The state repository shall make the required Repository Services available via the protocols and methods specified by the state or mutually agreed to by the state and the state repository.

11.10. The state repository shall be available for use online at least 95 percent of the time during business hours. When down time is planned, the state repository shall give reasonable notice before the down time.

11.11. On receipt of a message from a state certification authority requesting publication of a certificate or notice of revocation of a certificate, the state repository shall promptly place the certificate or notice of revocation online in the repository within 24 hours from the time of receipt of the request, if the message is demonstrably authentic, in the required form, and otherwise complies with the applicable specifications for publication into the repository.

11.12. The repository that the state repository provides for the state shall be operationally distinct and separate from any other repository and directory system that the state repository operates.

§153-30-12. Requirements for Issuance of Certificates.

12.1. The state certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

12.1.a. The certification authority has received a request for issuance signed by the prospective subscriber, and if the subscriber is acting in an official capacity, signed by the appropriate officer; and

12.1.b. The certification authority has received sufficient evidence to reasonably determine that:

12.1.b.1. The prospective subscriber is the person to be listed in the certificate to be issued;

12.1.b.2. The information in the certificate to be issued is accurate;

12.1.b.3. The prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate; and

12.1.c. The certification authority has confirmed that:

12.1.c.1. 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; and

12.1.c.2. The certificate provides information sufficient to locate or identify the repository in which notification of the revocation or suspension of the certificate will be listed if the certificate is suspended or revoked.

12.2. The state certification authority may issue a separate certificate to a subscriber as the agent for another officer or authorized person.

12.2.a. The certificate may be issued only upon evidence that:

12.2.a.1. The officer or other authorized person has the authority to designate the prospective subscriber as an agent to act on his or her behalf;

12.2.a.2. The officer or other authorized person files with the state certification authority a statement appointing the prospective subscriber as agent, designating any limitations on his or her authority to act in the official capacity of the officer or appointing person, and requesting issuance of the certificate listing the corresponding public key; and

12.2.a.3. The subscriber agrees in writing to use the certificate only when acting as agent for the officer or other authorized person.

12.2.b. The state certification authority shall clearly identify the subscriber as the holder of the private key corresponding to the public key to be listed in the certificate for the specific purpose of acting on behalf of the officer or authorized person.

12.3. The requirements of subsection 11.1. of this rule may not be waived or disclaimed by either the certification authority, the subscriber, or both.

12.4. In obtaining information of the subscriber material to 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 perjury.

12.5. If the subscriber accepts the issued certificate, the state certification authority shall publish a signed copy of the certificate in the state repository.

12.6. If the subscriber does not accept the certificate, the state certification authority may not publish it, or shall cancel its publication if the certificate has already been published.

§153-30-13. Subscribers; Duties Upon Acceptance of Certificate.

13.1. By accepting a certificate issued by the state certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate during its operational period that:

13.1.a. The subscriber legally holds the private key corresponding to the public key listed in the certificate; and

13.1.b. All representations made by the subscriber to the state certification authority and included in the information listed in the certificate are true.

13.2. By accepting a certificate, a subscriber recognizes that the provisions of W. Va. Code §61-3C-10 prescribe the penalties for the unauthorized disclosure of confidential security information, including the private key.

13.3. A subscriber to whom a certificate is issued in his or her capacity to act on behalf of an agency shall request the revocation of the certificate immediately upon separation from the agency.

13.4. An agency employing a person to whom a certificate is issued to act on behalf of that agency may request the revocation of the certificate upon separation of the employee or disqualification of the employee to act.

§153-30-14. Suspension of Certificate.

14.1. The state certification authority issuing a certificate shall suspend the certificate for a period not to exceed ninety-six hours:

14.1.a. Upon request by a person whom the certification authority reasonably believes to be:

14.1.a.1. The subscriber named in the certificate, or the officer or other authorized person who originally appointed the subscriber to act as agent;

14.1.a.2. a person duly authorized to act for that subscriber;

14.1.a.3. a person acting on behalf of the unavailable subscriber; or

14.1.b. By order of the Secretary of State.

14.2. The certification authority shall require the name, address, and telephone number, of the person requesting suspension, and other evidence of his or her identity.

14.3. Immediately upon suspension of a certificate by the state certification authority, the authority shall give notice of the suspension to the state repository.

14.4. The state certification authority may remove the suspension upon reasonable determination that the suspension was not warranted.

§153-30-15. Revocation of Certificate.

15.1. The state certification authority shall revoke a certificate it has issued within twenty-four hours after receiving:

15.1.a. Confirmation that it was not issued as required by this rule;

15.1.b. A written request for revocation by the subscriber of that certificate or the officer or authorized person originally appointing the subscriber as agent, subject to confirmation of the identity and authority of the person making the request; or

15.1.c. A certified copy of the subscriber's death certificate, or upon confirming the subscriber's death by other evidence.

15.2. The certification authority shall revoke a certificate it has issued upon presentation of documents effecting a dissolution, termination or revocation of the subscriber, or upon other reliable evidence that the subscriber has ceased to exist.

15.3. The certification authority may revoke a certificate that it issued upon evidence that the certificate has become unreliable, regardless of whether the subscriber consents to the revocation.

15.4. Immediately upon revocation of a certificate by the certification authority, the authority shall give notice of the revocation and shall publish the notice in the state repository.

§153-30-16. Expiration of Certificate.

16.1. The term of the certificate is subject to the contract with the state certification authority.

16.2. The certificate is valid for the duration of the term, unless sooner revoked, beginning on the date of issuance.

16.3. A certificate shall indicate the date on which it was issued and on which it expires.

16.4. Upon expiration of a certificate, the certification authority is discharged of its duties with respect to that certificate, except those duties related to the retention of records relating to the certificate.

§153-30-17. Form of Certificates.

17.1. Certificates issued by the state certification authority shall follow the Basic Certificate Field Standards specified in standard ITV-TX.509, Ver. 3, in accordance with certificate profiles issued by the state.

17.2. If certificate extension fields are used, their use shall conform to the required guidelines referenced in X.509 Section 12, and may be displayed on the certificate.

§153-30-18. Record keeping and Retention.

18.1. The state certification authority shall maintain a data file containing the record of each subscriber, including at least:

18.1.a. The name, address, and social security number or other national identification number of the subscriber, and the name of the agency, if the subscriber holds the digital signature certificate as an agency representative;

18.1.b. The name, address, and title of the officer or authorized person on whose behalf the subscriber will act, if the certificate is issued to the subscriber as an agent; and

18.1.c. The date of the issuance and the expiration of the certificate, and certificate number.

18.2. The state repository shall maintain a data file containing every time-stamp issued by the certification authority, with sufficient information to identify the subscriber and the document.

18.3. The state certification authority shall maintain the records necessary to assure compliance with the provisions of W. Va Code §39A-3-3 and this rule, as they pertain to digital signatures and the certificate authority.

18.4. Except for the names and address of subscribers, and the dates of issuance and expiration of their respective certificates, the records of the state certification authority pertaining to subscribers are not subject to public inspection. All records shall be indexed, stored, preserved and reproduced so as to be accurate, complete and accessible to an auditor.

§153-30-19. Compliance Audit.

19.1. The state certification authority may be subject to an annual compliance audit conducted by a reliable certified public accountant in conjunction with a reliable authority on computer security. The audit shall include a SAS 70 Type Two audit as specified in subdivision 3.7.5 of this rule.

19.2. Following an audit, the Secretary of State may require reports as needed to assure problems identified in the audit are corrected.

§153-30-20. Procedure on Discontinuance of Business of State Certification Authority or State Repository.

20.1. If a state certification authority or state repository goes out of business or otherwise discontinues providing the services specified in the contract prior to expiration of the contract, the certification authority or repository shall:

20.1.a. Notify the Secretary of State at least one hundred twenty days before discontinuing services;

20.1.b. Notify all subscribers listed in valid certificates issued by the certification authority at least thirty days before discontinuing services;

20.1.c. Minimize disruption to the subscribers of valid certificates and relying parties;

20.1.d. Refund, on a pro rata basis, fees paid in advance by subscribers for any certificate period in excess of one month from the date of discontinuation; and

20.1.e. Make reasonable arrangements for the preservation of the state certification authority's records.

20.2. The party issuing the corporate surety bond or letter of credit filed with the application shall continue the bond or letter of credit in effect until the expiration of the term specified in the bond or letter of credit.

20.3. The Secretary of State may specify a process by which he or she may, in any combination, receive, administer, or disburse the records of a state certification authority or state repository that discontinues providing services, for the purpose of maintaining access to the records and revoking any previously issued valid certificates in a manner that minimizes disruption to subscribers and relying parties.

20.4. The state may recover the costs of the state incurred in conjunction with the early termination of the contract and the process of obtaining alternative services.

§153-30-21. Fees for Issuance of Certificates.

21.1. The state certification authority may charge the fee for issuance of a certificate which is set by the terms of the state contract in effect at the time of the application by the subscriber.

21.2. The fee for a certificate shall be paid by the subscriber, or in the case of an agency employee, by the agency on whose behalf the subscriber will use the digital signature certificate

DAG

ANALYSIS OF PROPOSED LEGISLATIVE RULES

Agency: Secretary of State

Subject: Use of Electronic Signatures by State Agencies, 153CSR30

PERTINENT DATES

Filed for public comment: June 25, 2001
Public comment period ended: July 26, 2001
Filed following public comment period: July 26, 2001
Filed LRMRC: July 26, 2001
Filed as emergency:

Fiscal Impact: None

ABSTRACT

The proposed rule amends a current legislative rule by incorporating, in its entirety, the provision of the Secretary of State's rule, Use of Digital Signatures, State Certification Authority and State Repository, 153CSR31. There are no changes to the current provisions of that rule.

AUTHORITY

Statutory authority: W.Va. Code, §39A-3-3, which provides, in part, as follows:

> ...(a) The secretary of state shall propose legislative rules for promulgation in accordance with the provisions of article three, chapter twenty-nine-a of this code to establish standards and processes to facilitate the use of electronic signatures in all governmental transactions by state agencies subject to chapter twenty-nine-a of this code. The rules shall include minimum

standards for secure transactions to promote confidence and efficiency in legally binding electronic document transactions. The rules may be amended from time to time to keep the rules current with new developments in technology and improvements in secured transaction processes.

ANALYSIS

I. HAS THE AGENCY EXCEEDED THE SCOPE OF ITS STATUTORY AUTHORITY IN APPROVING THE PROPOSED LEGISLATIVE RULE?

No.

II. IS THE PROPOSED LEGISLATIVE RULE IN CONFORMITY WITH THE INTENT OF THE STATUTE WHICH THE RULE IS INTENDED TO IMPLEMENT, EXTEND, APPLY, INTERPRET OR MAKE SPECIFIC?

Yes.

III. DOES THE PROPOSED LEGISLATIVE RULE CONFLICT WITH OTHER CODE PROVISIONS OR WITH ANY OTHER RULE ADOPTED BY THE SAME OR A DIFFERENT AGENCY?

No.

IV. IS THE PROPOSED LEGISLATIVE RULE NECESSARY TO FULLY ACCOMPLISH THE OBJECTIVES OF THE STATUTE UNDER WHICH THE PROPOSED RULE WAS PROMULGATED?

Yes.

V. IS THE PROPOSED LEGISLATIVE RULE REASONABLE, ESPECIALLY AS IT AFFECTS THE CONVENIENCE OF THE GENERAL PUBLIC OR OF PERSONS AFFECTED BY IT?

Yes.

VI. CAN THE PROPOSED LEGISLATIVE RULE BE MADE LESS COMPLEX OR MORE READILY UNDERSTANDABLE BY THE GENERAL PUBLIC?

No.

VII. WAS THE PROPOSED LEGISLATIVE RULE PROMULGATED IN COMPLIANCE WITH THE REQUIREMENTS OF CHAPTER 29A, ARTICLE 3 AND WITH ANY REQUIREMENTS IMPOSED BY ANY OTHER PROVISIONS OF THE CODE?

Yes.

VIII. OTHER

Counsel has technical modifications to suggest.

TITLE 153
LEGISLATIVE RULE
~~JOINT RULE OF THE~~ SECRETARY OF STATE ~~AND STATE AUDITOR~~

SERIES 30
~~USE OF ELECTRONIC SIGNATURES BY STATE AGENCIES~~ USE OF DIGITAL SIGNATURES, STATE CERTIFICATION AUTHORITY AND STATE REPOSITORY

§153-30-1. General.

1.1. Scope. -- This legislative rule establishes the requirements for state agencies intending to use or accept electronic signatures on filings and other messages in electronic form which require the signature of an authorized person.

1.2. Authority. -- W. Va. Code ~~§39-5-4~~ §39A-3-3.

1.3. Filing Date. -- ~~April 1, 1999.~~

1.4. Effective Date. -- ~~April 1, 1999.~~

§153-30-2. Definitions

~~2.4.~~2.1. "Accept an electronic signature" means to accept an electronic record that requires the signature of an authorized person when that electronic record contains an electronic signature in lieu of an original signature.

~~2.1.~~2.2. "Agency" includes any state, county or municipal office, department, division, bureau, board, commission, public corporation or other governmental entity created by the State Constitution, statute, rule or executive order.

~~2.2.~~2.3. "Authorized officer" means the elected or appointed official, or a designee, who has authority to act on behalf of the agency.

2.4. "Certificate" or "digital signature certificate" means a computer-based record that:

2.4.a. Identifies the certification authority issuing it;

2.4.b. Names or identifies its subscriber;

2.4.c. Contains the subscriber's public key; and

2.4.d. Is digitally signed by the certification authority issuing it.

2.5. "Certificate Authority" means an entity issuing a certificate.

2.6. "Certification practice statement" means a declaration of the practices that a certification authority employs in issuing, managing, suspending, and revoking certificates and providing access to them.

2.7. "Corresponding," with reference to keys, means to belong to the same key pair.

~~2.5.~~2.8. "Electronic" means electrical, digital, magnetic, optical, electromagnetic, or any other technology that is similar to these technologies.

~~2.6.~~2.9. "Electronic record" means a record generated, communicated, received, or stored by electronic means.

~~2.3.~~2.10. "Electronic signature" means any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual signature. Electronic signatures include, but are not limited to digital marks and digital signatures

~~2.3.a. A "digitized signature" which consists of a handwritten signature entered on a recording device utilizing electronic recording software which simultaneously converts the image created to a digital record and attaches it to the electronic document to which it relates;~~

~~2.3.b.~~2.10.a. A "digital mark" which consists of an electronic code indicating approval or confirmation which is entered into a protected digital record following access protocols which identify the user and require a password, personal identification number, encrypted card or other security device which restricts access to one or more authorized individuals; and

~~2.3.c.~~2.10.b. A "digital signature" means an electronic signature consisting of a message transformed using an asymmetric cryptosystem so that a person having the initial message and the signer's public key can accurately determine whether the message was created using the corresponding private key, and whether the initial message has been altered since the message was transformed.

2.10.b.1. ~~Note:~~ A "digitized signature" which may consist of a ~~of~~ handwritten signature entered on a recording device utilizing electronic recording software which simultaneously converts the image created to a digital record and attaches it to the electronic document to which it relates or a graphic image file of a person's signature and is attached to the electronic document to which it relates may be used for illustrative purposes and shall not be construed as or considered an "electronic signature" in the context of this legislation.

2.11. "Key pair" means two corresponding keys, referred to as a private key and a public key, which are mathematically related in an asymmetric cryptosystem, where:

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

2.11.b. "Public key" means the key of a key pair used to verify a digital signature; and

2.11.c. The corresponding keys have the properties that:

2.11.c.1. The private key can encrypt a message which only the public key can decrypt; and

2.11.c.2. Even if the public key is known, it is computationally infeasible to discover the private key.

2.12. "Operational period" of a certificate begins on the date and time the certificate is issued by the certification authority (or on a later date and time certain if stated in the certificate) and ends on the date and time it expires as noted in the certificate, or is earlier revoked, but does not include any period during which a certificate is suspended.

~~2.7.~~2.13. "Record" means information that is inscribed on a tangible medium or that is stored in an

electronic or other medium and is retrievable in perceivable form, which includes an official record, including but not limited to a message, document, form, return or other instrument which is transmitted electronically from an authorized officer or other person to an agency to meet the requirements of law or to execute an essential transaction. An informal communication will not be considered an electronic record for purposes of this rule.

2.14. "Repository" means a system for issuing, storing, retrieving, managing, and processing digital signature/mark certificates and any other relevant information, including information relating to the status of a certificate.

2.15. "State certificate processing authority" means an entity with which the State of West Virginia contracts to issue certificates on behalf of the State.

2.16. "Subscriber" means a person who:

2.16.a. Is the subject named or otherwise identified in a certificate;

2.16.b. Controls the private key that corresponds to the public key listed in that certificate; and

2.16.c. ~~Is the person to whom~~ digitally signed messages verified by reference to the certificate are to be attributed.

2.17. "Trustworthy system" means computer hardware, software, and procedures that:

2.17.a. Are reasonably secure from intrusion and misuse;

2.17.b. Provide a reasonably reliable level of availability, reliability, and correct operation;

2.17.c. Are reasonably suited to performing their intended functions; and

2.17.d. Adhere to generally accepted security principles.

§153-30-3. Agency Use of Electronic Records and Electronic Signatures Generally.

3.1. Each agency shall determine if, and the extent to which, it will send and receive electronic records and electronic signatures to and from other persons and otherwise create, use, store, and rely upon electronic records and electronic signatures.

3.2. In any case where an agency decides to send or receive electronic records, or to accept document filings by electronic records, the agency may, giving due consideration to security, specify:

3.2.a. The manner and format in which such electronic records must be created, sent, received, and stored;

3.2.b. If such electronic records must be signed, the type of electronic signature that is required or acceptable, the manner and format in which the signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by the sender of the electronic record to facilitate the process;

3.2.c. Control processes and procedures as appropriate to ensure adequate integrity, security, confidentiality, and auditability of the electronic records; and

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

3.3. Whenever any rule of law requires or authorizes the filing of any information, notice, lien, or other document or record with any agency, a filing made by an electronic record has the same force and effect as a filing made on paper in all cases where the agency has authorized or agreed to the electronic filing and the filing is made in accordance with applicable rules or agreement.

3.4. Subject to prior notice by the receiving agency, submission of an electronic record containing an electronic signature record constitutes an agreement by the sender to accept equivalent electronic signature types on return or corresponding electronic records.

§153-30-4. Agency Procedures for Adoption, Modification or Revocation of Electronic Signature Acceptance

4.1. Each agency shall evaluate the types of records received to determine which records can be accepted with electronic signatures, and which form of electronic signature meets the security requirements of the specific transaction.

4.1.a. An electronic record, which requires the signature of a person under oath before an authorized official or with the acknowledgment of a notary public, may ~~not~~ be accepted with an electronic signature. ~~prior to the authorization in law of an electronic attestation.~~

4.1.b. An electronic record, which requires the signature of a person under a self-executing oath, may be accepted with a digital signature or other electronic signature, which is encrypted, capable of verifying the identity of the signer, and capable of discerning any alteration of the message since transformation.

4.2. An agency may accept an electronic record containing an electronic signature only after complying with the procedural requirements of this rule.

4.3. For each type of electronic record on which an agency is willing to accept an electronic signature in satisfaction of a legal signature requirement, the agency shall publish a notice through the Secretary of State which shall specify:

4.3.a. The name of the agency authorizing use of the electronic record;

4.3.b. A description of the type of electronic record;

4.3.c. The type or types of electronic signature that will be accepted on the record;

4.3.d. A description of any restrictions on whom may electronically sign the record;

4.3.e. The date that the electronic record with an electronic signature will first be accepted;

4.3.f. Specifications for any procedures or technology that must be used to create, communicate, or store the electronic signature; and

4.3.g. The name of one or more contacts within the agency who can provide additional information, along with the address, telephone and/or e-mail address of the contact person.

4.4. An agency subject to the Administrative Procedures Act, W. Va. Code Chapter §29A-1-1 et seq., shall comply with the notice requirements of subsection 4.3 of this section prior to acceptance of electronic signatures on electronic records, as follows:

4.4.a. When an agency intends to accept electronic signatures on electronic records sent to or received from employees within the agency or within the department of which the agency is a subdivision, the authorized officer shall give notice as required by subsection 4.3 of this section to the appropriate personnel;

4.4.b. When an agency intends to accept electronic signatures on electronic records sent to or received from other agencies outside the receiving agency's department, the agency shall give notice to the Secretary of State as required by subsection 4.3 of this section, at least thirty (30) days before first acceptance. The Secretary of State shall maintain a database of the agencies and the specific information provided for each type of record;

4.4.c. When an agency intends to use or accept electronic signatures on electronic records received from a person acting on his or her own behalf, or from a person acting on behalf of an entity not subject to the Administrative Procedures Act, or private concerns, the agency shall give notice as required by subsection 4.3 of this section, at least thirty (30) days prior to first acceptance, by publication in the State Register; and

4.4.d. The agency shall make available a summary of procedural information to assist persons desiring to file electronically and utilize electronic signatures.

4.5. An agency not subject to the Administrative Procedures Act, including county and municipal agencies, shall comply with the notice requirements of subsection 4.3 of this section prior to its use or acceptance of electronic signatures on electronic records as follows:

4.5.a. When an agency intends to use or accept electronic signatures on electronic records received from employees within the agency or within the governmental entity of which the agency is a subdivision, the authorized officer shall give notice as required by subsection 4.3 of this section to the appropriate personnel; and

4.5.b. When an agency intends to use or accept electronic signatures on electronic records received from a person acting on his or her own behalf, or from a person acting on behalf of an entity other than the governmental entity of which the agency is a subdivision, or private concerns, the agency shall give notice as required by subsection 4.3 of this section, at least thirty (30) days prior to first acceptance, by publication as a Class I legal advertisement in a qualified newspaper published in the municipality or county where the principal office of the agency is located.

4.6. An agency may modify, suspend, or terminate the acceptance of the electronic signatures after giving notice according to the requirements of this section; provided, that

4.6.a. Notice shall be given as required at least one hundred twenty (120) days prior to the termination of acceptance of a type of electronic signature; and

4.6.b. In an emergency which prevents the acceptance of the electronic signature, an agency may suspend acceptance of electronic signatures and require filings and signatures be provided on paper. The agency shall provide reasonable notice to potential filers.

4.7. Nothing in this rule shall be construed to require an agency to accept electronic signatures in lieu of written signatures.

4.8. Nothing in this rule shall be construed to allow an agency, without the specific authority of statute, to require a person acting on his or her own behalf, or a person acting on behalf of an entity other than a governmental entity to use an electronic signature in order to complete an essential filing.

4.9. All agencies may enter into agreements with other agencies relating to the use and acceptance of electronic signatures on electronic records communicated between those agencies.

§153-30-5. Requirements for Acceptance of Digital Marks.

5.1. An agency which intends to accept digital marks shall establish, at a minimum, the security measures and procedural requirements as provided in this section.

5.2. The agency shall establish a secure registry of persons authorized to sign filings and records, or shall utilize a secure registry for verification of the identity of the signer.

5.2.a. A person who desires to become authorized to file with the agency using a digital mark shall file with the secure registry a signed statement verifying that he or she:

5.2.a.1. Will not share with any other person the password, code or other security key required for use of the mark;

5.2.a.2. Agrees that the use of the mark represents confirmation of a record;

5.2.a.3. Agrees to notify the agency immediately once he or she becomes aware that the security key is compromised; and

5.2.a.4. Understands that the provisions of W. Va. Code §61-3C-10 prescribes the penalties for the unauthorized disclosure of a password, identifying code, personal identification number or other confidential security information.

5.2.b. The agency or secure registry shall issue an authorized person an identifying number and shall enter that number, name and date of authorization into the registry

5.2.c. The appropriate administrator shall revoke the access privileges of the authorized person upon termination of authority.

5.3. Each authorized person shall ~~utilize a~~ use a unique number, password or other personal authorization, which shall be encrypted, and which shall indicate the approval of that person.

5.4. The size, frequency of required changes and other elements of the security code shall meet state or agency security policies, if any are in effect. If no policy has been adopted, the elements of the security code shall meet generally acceptable standards for password security.

§153-30-6. Security Requirements for Acceptance of Digital Signature.

~~5.5.~~ 6.1. The agency shall establish the necessary computer hardware and software security, consistent with current generally acceptable standards for secure transactions, to prevent alteration of the electronic filing and to assure protection of the security key, and shall document that those features and measures are in place.

~~5.5.a.~~ 6.1.a. Information resources shall be protected by use of access control systems. Access control systems can be either internal (passwords, encryption, access control lists, constrained user interfaces) or external (port protection devices, firewalls, host-based authentication).

~~5.5.b~~ 6.1.b. Rules for access to resources (including internal and external telecommunications and networks) shall be established by the information/application owner or manager who is responsible for the resources.

~~5.5.c.~~ 6.1.c. When confidential or sensitive information from one agency is received by another agency in connection with the transaction of official business, the receiving agency shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency.

~~5.5.d.~~ 6.1.d. Pursuant to state security policy, information security and audit controls shall be incorporated into new systems.

~~5.5.e.~~ 6.1.e. Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited, and that violators are subject to criminal prosecution.

~~5.6~~. 6.2. For filings involving financial transmissions or financial liability, an agency may establish dollar limitations on the amount of a transaction for which a digital signature and digital mark will be accepted.

§153-30-7 Requirements for Acceptance of Digital Signatures

7.1. The Secretary of State, pursuant to legislative rule as required by W. Va. Code ~~§39-5-4~~§39A-3-3, shall establish a certification authority for the registration and issuance of certificates to subscribers for the use of digital signatures, as provided in ~~Secretary of State Rule, Use of Digital Signatures, State Certification Authority and State Repository, 153CSR31.~~ in this rule.

7.2. An agency, which agrees to accept a digital signature in connection with an electronic filing, shall obtain, install and test the essential hardware and software prior to giving notice of the intent to accept digital signatures.

7.3. Any authorized officer or other authorized person who becomes a subscriber to the certification authority maintained by the Secretary of State and who maintains an authorized key pair shall be permitted to use a digital signature on any electronic document which the agency agrees to accept.

§153-30-8. Requirements for Acceptance of Other Forms of Electronic Signatures

8.1. When an agency desires to accept a newly developed form of electronic signature not specifically listed in the definition of electronic signature contained in this rule, the agency shall apply to the Secretary of State for authority to accept the electronic signature.

8.2. To be acceptable as an electronic signature, the technology shall:

8.2.a Allow the receiving agency to verify the identity of the sender; and

8.2.b Allow the receiving agency to determine whether the message received has been altered en route.

8.3. The agency is responsible for assuring the security of the record following its acceptance.

§153-30-9. Selection of State Authority; Eligibility Requirements for Registration and Certificate Management and Authority.

9.1. The Secretary of State shall initiate a procurement process to obtain the services of one or more private vendors, at the discretion of the state, to provide services and systems to enable the Secretary of State to manage and authorize the issuance of digital signature/mark certificates.

9.2. The Secretary of State shall initiate a procurement process to obtain the software and systems to serves as the state repository or to obtain the services of one or more private vendors, at the discretion of the state, to serve as a state repository.

9.3. The Secretary of State may contract with a vendor for services of ~~either/or both~~ state certification authority and state repository.

9.4. The state certification authority may issue a certificate that binds a public key to any authorized person for the purpose of verifying a digital signature created by that person on an electronic record in his or her capacity as an agent of the state or any agency in West Virginia, as defined by subsection 2.1. of this rule.

9.5. The state certificate management authority may issue a certificate to any person for the purpose of verifying a digital signature created by that person on an electronic record filed with any agency, as defined by subsection 2.1. of this rule.

9.6. For the duration of the contract, the state certification authority and/or state repository shall comply with the provisions of this rule.

9.7. To be qualified for selection as a state certification authority and/or state repository, a vendor shall:

9.7.a. Maintain a system of internal security controls to restrict access to systems and data only to authorized personnel, and conduct appropriate clearances of those personnel to ensure that they have demonstrated knowledge and proficiency in following the requirements of this chapter, and have never been convicted of a felony or of any other crime involving fraud or misrepresentation;

9.7.b. File with the secretary of state a corporate surety bond or letter of credit for a term of at least five years, in the amount of fifty thousand dollars ($50,000);

9.7.c. Use a trustworthy system, including a secure means for limiting access to its private key;

9.7.d. Be licensed to do business in the state and registered as a vendor for the state;

9.7.e. Provide the Secretary of State with a copy of an unqualified performance audit performed in accordance with standards set in the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards No. 70 (S.A.S. 70) "Reports on the Processing of Service Transactions by Service Organizations" (1992) to ensure that the certification authority's practices and policies are consistent with the certification authority's stated control objectives. The audit shall include a SAS 70 Type Two audit -- A Report of Policies and Procedures Placed in Operation and Test of Operating Effectiveness-- receiving an unqualified opinion; and

9.7.f. Meet any other requirements specified in the request for proposal and contract.

§153-30-10. Requirements for State Certificate Management Authority Practice.

10.1. The state certification authority shall provide the Secretary of State at least annually, or upon any significant change in procedures, a certification practice statement detailing the security and procedural steps utilized in the issuance, management, suspension, and revocation of certificates and authentication of the identity of persons named in certificates.

10.2. The Secretary of State shall publish electronically the certification practice statement within thirty (30) days after it is filed.

10.3. The state certification authority shall use only a trustworthy system to:

10.3.a. Issue, suspend, or revoke a certificate;

10.3.b. Publish or give notice of the issuance, suspension, or revocation of a certificate; or

10.3.c. Create and protect private keys.

10.4. Upon a written, signed and reasonably specific inquiry from an identified person, the state certification authority shall disclose any fact material to the reliability of a certificate that it has issued. The certification authority may require payment of reasonable compensation before making this disclosure.

§153-30-11. Requirements for State Repository Practice.

11.1. The state repository shall provide the Secretary of State at least annually, or upon any significant change in procedures, a practice statement detailing the operation of the repository, the conduct of its repository services, the processes for publishing certificates and notices of revocation into the repository, the processes for obtaining copies of certificates and checking certificate status, and all security and procedural steps related ~~thereto~~. to the certificates?

11.2. The Secretary of State shall publish electronically the practice statement within thirty (30) days after it is filed.

11.3. The state repository shall provide all repository services by means of a trustworthy system.

11.4. Upon a written, signed and reasonably specific inquiry from an identified person, the state repository shall disclose any fact material to the reliability of a specific verification transaction. The state repository may require payment of reasonable compensation before making this disclosure.

11.5. The state repository shall provide an online database containing at least:

11.5.a. All valid certificates published into the database by state certification authorities; and

11.5.b. All notices of revocation of the certificates published into the directory by state certification authorities.

11.6. The state repository shall enable state certification authorities to add information, including certificates and notices of certificate revocation, to the database in a prompt, reasonable, and secure manner.

11.7. The state repository shall store certificates issued by state certification authorities that are no longer valid and provide copies of them on request. The state repository shall also store other information regarding certificates, notices of revocation, certification practice statements, and other matters relating to the services provided by state certification authorities, and shall make copies of the information available on request.

11.8. The state repository shall provide any additional information and services specified in its contract with the state.

11.9. The state repository shall make the required Repository Services available via the protocols and methods specified by the state or mutually agreed to by the state and the state repository.

11.10. The state repository shall be available for use online at least 95 percent of the time during business hours. When down time is planned, the state repository shall give reasonable notice before the down time.

11.11. On receipt of a message from a state certification authority requesting publication of a certificate or notice of revocation of a certificate, the state repository shall promptly place the certificate or notice of revocation online in the repository within 24 hours from the time of receipt of the request, if the message is demonstrably authentic, in the required form, and otherwise complies with the applicable specifications for publication into the repository.

11.12. The repository that the state repository provides for the state shall be operationally distinct and separate from any other repository and directory system that the state repository operates.

§153-30-12. Requirements for Issuance of Certificates.

12.1. The state certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

12.1.a. The certification authority has received a request for issuance signed by the prospective subscriber, and if the subscriber is acting in an official capacity, signed by the appropriate officer; and

12.1.b. The certification authority has received sufficient evidence to reasonably determine that:

12.1.b.1. The prospective subscriber is the person to be listed in the certificate to be issued;

12.1.b.2. The information in the certificate to be issued is accurate;

12.1.b.3. The prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate; and

12.1.c. The certification authority has confirmed that:

12.1.c.1. 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; and

12.1.c.2. The certificate provides information sufficient to locate or identify the repository in which notification of the revocation or suspension of the certificate will be listed if the certificate is suspended or revoked.

12.2. The state certification authority may issue a separate certificate to a subscriber as the agent for another officer or authorized person.

12.2.a. The certificate may be issued only upon evidence that:

12.2.a.1. The officer or other authorized person has the authority to designate the prospective subscriber as an agent to act on his or her behalf;

12.2.a.2. The officer or other authorized person files with the state certification authority a statement appointing the prospective subscriber as agent, designating any limitations on his or her authority to act in the official capacity of the officer or appointing person, and requesting issuance of the certificate listing the corresponding public key; and

12.2.a.3. The subscriber agrees in writing to use the certificate only when acting as agent for the officer or other authorized person.

12.2.b. The state certification authority shall clearly identify the subscriber as the holder of the private key corresponding to the public key to be listed in the certificate for the specific purpose of acting on behalf of the officer or authorized person.

12.3. The requirements of subsection 11.1. of this rule may not be waived or disclaimed by either the certification authority, the subscriber, or both.

12.4. In obtaining information of the subscriber material to 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 perjury.

12.5. If the subscriber accepts the issued certificate, the state certification authority shall publish a signed copy of the certificate in the state repository.

12.6. If the subscriber does not accept the certificate, the state certification authority may not publish it, or shall cancel its publication if the certificate has already been published.

§153-30-13. Subscribers; Duties Upon Acceptance of Certificate.

13.1. By accepting a certificate issued by the state certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate during its operational period that:

13.1.a. The subscriber legally holds the private key corresponding to the public key listed in the certificate; and

13.1.b. All representations made by the subscriber to the state certification authority and included in the information listed in the certificate are true.

13.2. By accepting a certificate, a subscriber recognizes that the provisions of W. Va. Code §61-3C-10 prescribe the penalties for the unauthorized disclosure of confidential security information, including the private key.

13.3. A subscriber to whom a certificate is issued in his or her capacity to act on behalf of an agency shall request the revocation of the certificate immediately upon separation from the agency.

13.4. An agency employing a person to whom a certificate is issued to act on behalf of that agency may request the revocation of the certificate upon separation of the employee or disqualification of the employee to act.

§153-30-14. Suspension of Certificate.

14.1. The state certification authority issuing a certificate shall suspend the certificate for a period not to exceed ninety-six hours:

14.1.a. Upon request by a person whom the certification authority reasonably believes to be:

14.1.a.1. The subscriber named in the certificate, or the officer or other authorized person who originally appointed the subscriber to act as agent;

14.1.a.2. a person duly authorized to act for that subscriber;

14.1.a.3. a person acting on behalf of the unavailable subscriber; or

14.1.b. By order of the Secretary of State.

14.2. The certification authority shall require the name, address, and telephone number, of the person requesting suspension, and other evidence of his or her identity.

14.3. Immediately upon suspension of a certificate by the state certification authority, the authority shall give notice of the suspension to the state repository.

14.4. The state certification authority may remove the suspension upon reasonable determination that the suspension was not warranted.

§153-30-15. Revocation of Certificate.

15.1. The state certification authority shall revoke a certificate it has issued within twenty-four hours after receiving:

15.1.a. Confirmation that it was not issued as required by this rule;

15.1.b. A written request for revocation by the subscriber of that certificate or the officer or authorized person originally appointing the subscriber as agent, subject to confirmation of the identity and authority of the person making the request; or

15.1.c. A certified copy of the subscriber's death certificate, or upon confirming the subscriber's death by other evidence.

15.2. The certification authority shall revoke a certificate it has issued upon presentation of documents effecting a dissolution, termination or revocation of the subscriber, or upon other reliable evidence that the subscriber has ceased to exist.

15.3. The certification authority may revoke a certificate that it issued upon evidence that the certificate has become unreliable, regardless of whether the subscriber consents to the revocation.

15.4. Immediately upon revocation of a certificate by the certification authority, the authority shall give notice of the revocation and shall publish the notice in the state repository.

§153-30-16. Expiration of Certificate.

16.1. The term of the certificate is subject to the contract with the state certification authority.

16.2. The certificate is valid for the duration of the term, unless sooner revoked, beginning on the date of issuance.

16.3. A certificate shall indicate the date on which it was issued and on which it expires.

16.4. Upon expiration of a certificate, the certification authority is discharged of its duties with respect to that certificate, except those duties related to the retention of records relating to the certificate.

§153-30-17. Form of Certificates.

17.1. Certificates issued by the state certification authority shall follow the Basic Certificate Field Standards specified in standard ITV-TX.509, Ver. 3, in accordance with certificate profiles issued by the state.

17.2. If certificate extension fields are used, their use shall conform to the required guidelines referenced in X.509 Section 12, and may be displayed on the certificate.

§153-30-18. Record keeping and Retention.

18.1. The state certification authority shall maintain a data file containing the record of each subscriber, including at least:

18.1.a. The name, address, and social security number or other national identification number of the subscriber, and the name of the agency, if the subscriber holds the digital signature certificate as an agency representative;

18.1.b. The name, address, and title of the officer or authorized person on whose behalf the subscriber will act, if the certificate is issued to the subscriber as an agent; and

18.1.c. The date of the issuance and the expiration of the certificate, and certificate number.

18.2. The state repository shall maintain a data file containing every time-stamp issued by the certification authority, with sufficient information to identify the subscriber and the document.

18.3. The state certification authority shall maintain the records necessary to assure compliance with the provisions of W. Va Code §39A-3-3 and this rule, as they pertain to digital signatures and the certificate authority.

18.4. Except for the names and address of subscribers, and the dates of issuance and expiration of their respective certificates, the records of the state certification authority pertaining to subscribers are not subject to public inspection. All records shall be indexed, stored, preserved and reproduced so as to be accurate, complete and accessible to an auditor.

§153-30-19. Compliance Audit.

19.1. The state certification authority may be subject to an annual compliance audit conducted by a reliable certified public accountant in conjunction with a reliable authority on computer security. The audit shall include a SAS 70 Type Two audit as specified in subdivision 3.7.5 of this rule.

19.2. Following an audit, the Secretary of State may require reports as needed to assure problems identified in the audit are corrected.

§153-30-20. Procedure on Discontinuance of Business of State Certification Authority or State Repository.

20.1. If a state certification authority or state repository goes out of business or otherwise discontinues providing the services specified in the contract prior to expiration of the contract, the certification authority or repository shall:

20.1.a. Notify the Secretary of State at least one hundred twenty days before discontinuing services;

20.1.b. Notify all subscribers listed in valid certificates issued by the certification authority at least thirty days before discontinuing services;

20.1.c. Minimize disruption to the subscribers of valid certificates and relying parties;

20.1.d. Refund, on a pro rata basis, fees paid in advance by subscribers for any certificate period in excess of one month from the date of discontinuation; and

20.1.e. Make reasonable arrangements for the preservation of the state certification authority's records.

20.2. The party issuing the corporate surety bond or letter of credit filed with the application shall continue the bond or letter of credit in effect until the expiration of the term specified in the bond or letter of credit.

20.3. The Secretary of State may specify a process by which he or she may, in any combination, receive, administer, or disburse the records of a state certification authority or state repository that discontinues providing services, for the purpose of maintaining access to the records and revoking any previously issued valid certificates in a manner that minimizes disruption to subscribers and relying parties.

20.4. The state may recover the costs of the state incurred in conjunction with the early termination of the contract and the process of obtaining alternative services.

§153-30-21. Fees for Issuance of Certificates.

21.1. The state certification authority may charge the fee for issuance of a certificate which is set by the terms of the state contract in effect at the time of the application by the subscriber.

21.2. The fee for a certificate shall be paid by the subscriber, or in the case of an agency employee, by the agency on whose behalf the subscriber will use the digital signature certificate