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

Form #2

Do Not Mark In This Box

FILED

2001 JUN 25 P 5:07

OFFICE WEST VIRGINIA
SECRETARY OF STATE

NOTICE OF A COMMENT PERIOD ON A PROPOSED RULE

AGENCY: Secretary of State TITLE NUMBER: 153

RULE TYPE: Legislative CITE AUTHORITY: §39A-3-3

AMENDMENT TO AN EXISTING RULE: YES X NO ___

IF YES, SERIES NUMBER OF RULE BEING AMENDED: 31

TITLE OF RULE BEING AMENDED: Use of Digital Signatures, State Certification Authority & State Repository (Repealing entire rule -- see 153CSR30)

IF NO, SERIES NUMBER OF RULE BEING PROPOSED: ___

TITLE OF RULE BEING PROPOSED: ___

IN LIEU OF A PUBLIC HEARING, A COMMENT PERIOD HAS BEEN ESTABLISHED DURING WHICH ANY INTERESTED PERSON MAY SEND COMMENTS CONCERNING THESE PROPOSED RULES. THIS COMMENT PERIOD WILL END ON July 26, 2001 AT 9:30 a.m. ONLY WRITTEN COMMENTS WILL BE ACCEPTED AND ARE TO BE MAILED TO THE FOLLOWING ADDRESS:

Judy Cooper, Administrative Law Div
Secretary of State's Office
Building 1 Suite 157K
1900 Kanawha Blvd E
Charleston WV 25305-0770

THE ISSUES TO BE HEARD SHALL BE LIMITED TO THIS PROPOSED RULE.

Authorized Signature

ATTACH A **BRIEF** SUMMARY OF YOUR PROPOSAL

APPENDIX B

FISCAL NOTE FOR PROPOSED RULES

Rule Title: Use of Digital Signatures, State Certification Authority & State Repository (153-31)

Type of Rule: X Legislative ____ Interpretive ____ Procedural

Agency: Secretary of State

Address: Administrative Law Division

Judy Cooper, 558-6000, jcooper@secretary.state.wv.us
Building 1, Suite 157K

1900 Kanawha Boulevard E
Charleston WV 25305-0770

1. Effect of Proposed rule:

	ANNUAL		FISCAL YEAR		
	INCREASE	DECREASE	CURRENT	NEXT	THEREAFTER
ESTIMATED TOTAL COST	0	0	0	0	0
PERSONAL SERVICES					
CURRENT EXPENSE					
REPAIRS & ALTERATIONS					
EQUIPMENT					
OTHER					

2. Explanation of Above Estimates:
This repeals 153CSR31. It is being amended into 153CSR30

3. Objectives of These Rules:
This repeals 153CSR31. It is being amended into 153CSR30

4. Explanation of Overall Economic Impact of Proposed Rule:

   A. Economic Impact on State Government:
   None

   B. Economic Impact on Political Subdivisions; Specific Industries; Specific Groups of Citizens:
   None

   C. Economic Impact on Citizens/Public at Large.
   None

Date: July 26, 2001

Signature of Agency Head or Authorized Representative:

Joan Casto

Statement of Purpose

This repeals 153CSR31. This rule is being amended into 153CSR30.

Facts and Circumstances

§39-5-4 has been repealed. This rule is being amended into 153CSR30.

~~TITLE 153~~
~~LEGISLATIVE RULE~~
~~SECRETARY OF STATE~~

~~SERIES 31~~
~~USE OF DIGITAL SIGNATURES, STATE CERTIFICATION AUTHORITY AND STATE REPOSITORY~~

~~§153-31-1. General.~~

~~1.1. Scope. -- This legislative rule establishes the requirements for use of digital signatures in lieu of manual signatures and establishes requirements for a state certification authority.~~

~~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.~~

~~§153-31-2. Definitions.~~

~~2.1. "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. "Authorized officer" means the elected or appointed official, or a designee, who has authority to act on behalf of the agency.~~

~~2.3. "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.~~

~~2.4. "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.~~

~~2.5. "Certificate" or "digital signature certificate" means a computer-based record that:~~

~~2.5.1. Identifies the certification authority issuing it;~~

~~2.5.2. Names or identifies its subscriber;~~

~~2.5.3. Contains the subscriber's public key; and~~

~~2.5.4. Is digitally signed by the certification authority issuing it.~~

2.6. "State certification authority" means an entity with which the State of West Virginia contracts to issue certificates on behalf of the State.

2.7. "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:

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

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

2.7.3. The corresponding keys have the properties that:

2.7.3.a. The private key can encrypt a message which only the public key can decrypt; and

2.7.3.b. Even if the public key is known, it is computationally infeasible to discover the private key.

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

2.9. "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.

2.10. "Repository" means a system for storing and retrieving certificates and other information relevant to certificates, including information relating to the status of a certificate.

2.11. "Subscriber" means a person who:

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

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

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

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

2.13. "Electronic record" means a record generated, communicated, received, or stored by electronic means.

2.14. "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.

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

2.15.1. Are reasonably secure from intrusion and misuse;

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

2.15.3. Are reasonably suited to performing their intended functions; and

2.15.4. Adhere to generally accepted security principles.

2.16. "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.

§153-31-3. Selection of State Certification Authority; Eligibility Requirements for Certification Authority.

3.1. 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 serve as a state certification authority.

3.2. 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 serve as a state repository.

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

3.4. 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.

3.5. The state certification 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.

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

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

3.7.1. 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;

3.7.2. 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);

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

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

3.7.5. 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

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

§153-31-4. Requirements for State Certification Authority Practice.

4.1. 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.

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

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

4.3.1. Issue, suspend, or revoke a certificate;

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

4.3.3. Create and protect private keys.

4.4. 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.

§153-31-5. Requirements for State Repository Practice.

5.1. 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.

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

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

5.4. 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.

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

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

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

5.6. 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.

5.7. 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.

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

5.9. 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.

5.10. 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.

5.11. 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.

5.12. 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.

§153-31-6. Requirements for Issuance of Certificates.

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

6.1.1. 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

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

6.1.2.a. The prospective subscriber is the person to be listed in the certificate to be issued;

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

6.1.2.c. The prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate; and

6.1.3. The certification authority has confirmed that:

6.1.3.a. 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

6.1.3.b. 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.

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

6.2.1. The certificate may be issued only upon evidence that:

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

6.2.1.b. 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

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

6.2.2. 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.

6.3. The requirements of subsection 6.1. of this rule may not be waived or disclaimed by either the certification authority, the subscriber, or both.

6.4. 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.

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

6.6. 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.

§153-31-7. Subscribers; Duties Upon Acceptance of Certificate.

7.1. 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:

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

~~7.1.2. All representations made by the subscriber to the state certification authority and included in the information listed in the certificate are true.~~

~~7.2. 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.~~

~~7.3. 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.~~

~~7.4. 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.~~

~~§153-31-8. Suspension of Certificate.~~

~~8.1. The state certification authority issuing a certificate shall suspend the certificate for a period not to exceed ninety-six hours:~~

~~8.1.1. Upon request by a person whom the certification authority reasonably believes to be:~~

~~8.1.1.a. The subscriber named in the certificate, or the officer or other authorized person who originally appointed the subscriber to act as agent;~~

~~8.1.1.b. a person duly authorized to act for that subscriber;~~

~~8.1.1.c. a person acting on behalf of the unavailable subscriber; or~~

~~8.1.2. By order of the Secretary of State.~~

~~8.2. The certification authority shall require the name, address, and telephone number, of the person requesting suspension, and other evidence of his or her identity.~~

~~8.3. Immediately upon suspension of a certificate by the state certification authority, the authority shall give notice of the suspension to the state repository.~~

~~8.4. The state certification authority may remove the suspension upon reasonable determination that the suspension was not warranted.~~

§153-31-9. Revocation of Certificate.

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

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

9.1.2. 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

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

9.2. 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.

9.3. 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.

9.4. 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.

§153-31-10. Expiration of Certificate.

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

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

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

10.4. 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.

§153-31-11. Form of Certificates.

11.1. 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.

11.2. 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.

§153-31-12. Record keeping and Retention.

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

~~12.1.1. 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;~~

~~12.1.2. 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~~

~~12.1.3. The date of the issuance and the expiration of the certificate, and certificate number.~~

~~12.2. 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.~~

~~12.3. The state certification authority shall maintain the records necessary to assure compliance with the provisions of W. Va Code §39-5-1 et seq. and this rule, as they pertain to digital signatures and the certificate authority.~~

~~12.4. 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.~~

~~§153-31-13. Compliance Audit.~~

~~13.1. 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.~~

~~13.2. Following an audit, the Secretary of State may require reports as needed to assure problems identified in the audit are corrected.~~

~~§153-31-14. Procedure on Discontinuance of Business of State Certification Authority or State Repository.~~

~~14.1. 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:~~

~~14.1.1. Notify the Secretary of State at least one hundred twenty days before discontinuing services;~~

~~14.1.2. Notify all subscribers listed in valid certificates issued by the certification authority at least thirty days before discontinuing services;~~

~~14.1.3. Minimize disruption to the subscribers of valid certificates and relying parties;~~

~~14.1.4. 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~~

~~14.1.5. Make reasonable arrangements for the preservation of the state certification authority's records.~~

~~14.2. 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.~~

~~14.3. 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.~~

~~14.4. 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.~~

~~§153-31-15. Fees for Issuance of Certificates.~~

~~15.1. 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.~~

~~15.2. 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.~~