WEST VIRGINIA
SECRETARY OF STATE
BETTY IRELAND
ADMINISTRATIVE LAW DIVISION

Form #2

Do Not Mark In This Box

2007 JUN 27 P 1:

OFFICE OF
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: 30

TITLE OF RULE BEING AMENDED: Use of Digital Signatures, State Certificate Authority and State Repository

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 27, 2007 AT 9:00 a.m. ONLY WRITTEN COMMENTS WILL BE ACCEPTED AND ARE TO BE MAILED TO THE FOLLOWING ADDRESS:

Ben Beakes, Chief of Staff

West Virginia Secretary of State
1900 Kanawha Boulevard, East

Charleston, WV 25305

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

Betty Ireland
Authorized Signature

ATTACH A **BRIEF** SUMMARY OF YOUR PROPOSAL

APPENDIX B

FISCAL NOTE FOR PROPOSED RULES

Rule Title: Use of Digital Signatures, State Certificate Authority and State Repository

Type of Rule: [X] Legislative [ ] Interpretive [ ] Procedural

Agency: Secretary of State

Address: Building 1, Suite 157-K
1900 Kanawha Blvd., East
Charleston, WV 25305

Phone Number: 304-558-6000 Email: bbeakes@wvsos.com

Fiscal Note Summary

Summarize in a clear and concise manner what impact this measure will have on costs and revenues of state government.

None.

Fiscal Note Detail

Show over-all effect in Item 1 and 2 and, in Item 3, give an explanation of Breakdown by fiscal year, including long-range effect.

FISCAL YEAR			
Effect of Proposal	Current Increase/Decrease (use "-")	Next Increase/Decrease (use "-")	Fiscal Year (Upon Full Implementation)
1. Estimated Total Cost	0.00	0.00	0.00
Personal Services	0.00	0.00	0.00
Current Expenses	0.00	0.00	0.00
Repairs & Alterations	0.00	0.00	0.00
Assets	0.00	0.00	0.00
Other	0.00	0.00	0.00
2. Estimated Total Revenues	0.00	0.00	0.00

Rule Title: _____

Rule Title: Use of Digital Signatures, State Certificate Authority and State Repository

3. Explanation of above estimates (including long-range effect):
Please include any increase or decrease in fees in your estimated total revenues.

The amendments to this already existing rule do not introduce any new elements to the use of digital signatures. The proposed changes addressed simply transfer some of the technical duties of implementing digital signatures from the Secretary of State's Office to the Office of Technology.

Currently the Secretary of State's Office is charged with the responsibility to implement and authorize the use of digital signatures. Given the fact that the Secretary of State's Office is not equipped with the personnel or infrastructure to effectively implement digital signatures and the Office of Technology is, some technical duties will be transferred to the Office of Technology to better serve the state and all of its subdivisions.

For this reason, the net cost is estimated to be $0.00.

MEMORANDUM

Please identify any areas of vagueness, technical defects, reasons the proposed rule **would not** have a fiscal impact, and/or any special issues **not** captured elsewhere on this form.

As described above, no new elements to digital signatures are being proposed in this rule. The proposed amendments to this already existing rule will help the state implement digital signatures more efficiently.

Date: 06/27/07

Signature of Agency Head or Authorized Representative

Bryce R Beach

This proposed rule transfers technical duties associated with implementing digital signatures from the Secretary of State's Office to the Office of Technology. The Office of Technology is better equipped with personnel and infrastructure to efficiently implement and manage digital signatures for any interested state agency more so than the Secretary of State's Office. This rule further sets forth procedures for the Secretary of State's Office, as the official authorizing agency, and the Office of Technology, as the technical manager, to communicate with one another regarding the implementation and management of digital signatures.

TITLE 153
LEGISLATIVE RULE
SECRETARY OF STATE

SERIES 30
USE OF DIGITAL SIGNATURES, STATE CERTIFICATE 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 §39A-3-3.

1.3. Filing Date. -- April 7, 2006.

1.4. Effective Date. -- April 7, 2006.

§153-30-2. Definitions

2.1. The definitions of terms established in W. Va. Code §§39A-1-2 and 39A-3-1 shall apply when those terms are used in this rule.

2.2. "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.

2.3. "Assurance level" means the degree of certainty that the user of an electronic signature has presented an identifier or credential that refers to his or her identity. For the purpose of this rule, assurance levels defined by the United States Office of Management and Budget in the Memorandum M-04-04, E-Authentication Guidance for Federal Agencies dated December 16, 2003 shall be adopted, as follows:

2.3.1. 'Level 1' means little or no confidence in the asserted identity's validity;

2.3.2. 'Level 2' means some confidence in the asserted identity's validity;

2.3.3. 'Level 3' means high confidence in the asserted identity's validity; and

2.3.4. 'Level 4' means very high confidence in the asserted identity's validity

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

2.5. "Certificate practice statement" or "certificate policy" means a declaration of the practices that a certificate authority employs in issuing, managing, suspending, and revoking certificates and providing access to them.

2.6. "Electronic postmark" means an electronic service provided by the United States Postal Service that provides evidentiary proof that an electronic document existed in a certain form at a certain time and the electronic document was opened or the contents of the electronic document were displayed at a time and date documented by the United States Post Office.

2.7. "Federal certificate authority and repository program" means an official program established by an agency of the United States government for the issuance and authentication of digital signature certificates or other secure electronic authorizations to individuals for use in transactions.

2.8. "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.

2.9. "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.

2.10. "State certificate authority and repository" means an entity authorized by a program designated and approved by the Secretary of State under the provisions of section seven of this rule or established under section nine of this rule to issue certificates on behalf of the State and provide repository services.

2.11. "Subscriber" means a person who:

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

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

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

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

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

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

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

2.12.d. Adhere to generally accepted security principles.

2.13. "Type of electronic signature" means the specific technology used to create, apply and validate the electronic signature and the level of assurance of identity provided by the process of issuance.

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

3.1. Each agency shall determine 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~~ shall, giving due consideration to security, specify:

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

3.2.b. The type of electronic signature or electronic postmark that is required or acceptable, the assurance level required for the transaction, the manner and format in which the signature must be affixed to the electronic record, and the criteria that must be met by any third party used by the sender of the electronic record to facilitate the process;

3.2.c. Processes and procedures 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. The specifications outlined in subsection 3.2 shall be submitted to and approved by the Office of Technology, through its chief technology officer or his or her designee, before the agency can begin implementing electronic signature certificates for its usage and acceptance.

~~3.3.~~3.4. 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.~~3.5. Subject to prior notice by the receiving agency, submission of an electronic record containing an electronic signature or electronic postmark 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 type of electronic signature meets the security requirements of the specific transaction.

4.2. For each type of electronic record on which an agency is willing to accept an electronic signature in satisfaction of a legal signature requirement or an electronic postmark in satisfaction of a filing or receipt requirement, the agency shall give notice in conjunction with the electronic filing system which shall specify:

4.2.a. The type or types of electronic signature or postmark that will be accepted on the record;

4.2.b. A description of any restrictions on who may electronically sign the record;

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

4.2.d. 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.

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

4.3.a. Notice shall be given as required at least thirty (30) days prior to the termination of acceptance of a type of electronic signature or electronic postmark; and

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

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

4.5. 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.

4.6. 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 not associated with a certificate shall establish the agency deems necessary to meet the requirements of law.

5.2. The agency may establish a secure registry of persons authorized to sign filings and records, may utilize a secure registry for verification of the identity of the signer, or may accept the mark of an individual possessing the authorization code issued to the entity making the filing.

5.3. A person who makes a filing with the agency using a digital mark agrees that the use of the mark represents his or her affirmation of the

filing and the contents of the filing.

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

5.5. 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. Requirements for Acceptance of Digital Signatures.

6.1. The Secretary of State, pursuant W. Va. Code §39A-3-3, shall authorize a state certificate authority for the registration and issuance of certificates to subscribers for the use of digital signatures, as provided in this rule.

6.2. 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 as prescribed by the Office of Technology, through its chief technology officer or his or her designee.

6.3. Any authorized officer or other authorized person who becomes a subscriber to the certificate authority authorized 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 an agency agrees to accept.

§153-30-7. Selection of Existing Federal Certificate Authority Program as State Authority and Repository; Purchase of Certificates; Fees; Revocation of Authorization.

7.1. The Secretary of State may designate and authorize as the official state certificate authority and repository an existing federal certificate authority and repository program, providing:

7.1.a. The program permits the acquisition and use of electronic signature certificates by state and local government agencies for their employees and by individuals for transactions with those agencies at or below the rate established for the federal program;

7.1.b The program has published a certificate policy or certificate practice statement that establishes comprehensive requirements for the security of all aspects of the system, including the physical and technical security of the software and hardware and the security requirements for authorized personnel.

7.1.c. The program uses a comprehensive requirements evaluation process for selection of qualifying certificate authorities.

7.1.d. The program authorizes one or more entities or vendors to provide the services of certificate authority, repository and registration authority;

7.1.e. Each authorized certificate authority manages the application, issuance and revocation of a certificate that complies with the certificate policy of the program.

7.1.f. Each authorized certificate authority offers subscriptions for certificates through the federal program that meet, at a minimum, the requirements of Level 2 assurance.

7.1.g. The program requires ~~the bonding and~~ an audit of each authorized certificate authority.

7.1.h. The Office of Technology, through its chief technology officer or his or her designee, shall validate that the program meets the standards outlined in subsections 7.1.a through 7.1.g and reports such to the Secretary of State via a form prescribed by the Secretary of State.

7.2. Designation and authorization of the federal certificate authority and repository program as the state certificate authority shall substitute the requirements of the federal certificate authority and repository program for the requirements of the state certificate authority, repository and other requirements stated in sections nine through twenty-one of this rule. The

certificate policy or certificate practice statement of the federal program shall control the form, application, issuance, expiration, suspension, and revocation of certificates and shall control the record keeping, record retention and audit requirements of the certificate authority and repository.

7.3. The ~~Secretary of State~~ Office of Technolgy, through its chief technology officer or his or her designee, may initiate a procurement process to establish a statewide contract for a term no less than one year with any or all of the certificate authorities authorized under the federal certificate authority and repository program, and only those authorized entities may be qualified to bid.

7.3.a. The contract may establish the purchase price of one or more types of electronic signature certificates for a subscription of a specified term, and that price shall be inclusive of the services performed as the registration authority, certificate authority and repository for the term of the subscription.

7.3.b. The contract may include pricing for individual certificates and for business certificates if offered by the authorized certificate authorities.

7.3.c. The contract may include pricing for single certificates and bundles of certificates at preferred rates.

7.3.d. The contract shall allow an agency to purchase certificates for use by agency employees and agency customers at an established contract rate; and an agency may require payment or reiumbursement for certificates issued to customers.

7.4. The Office of Technology, through its chief technology officer or his or her designee, shall submit to the Secretary of State on January 1, 2008, and annually thereafter, a report that outlines the following:

7.4.a. Affirmation that the requirements of the state's official certificate authority and repository are still valid or any changes thereto;

7.4.b. A listing of state agencies and its' subdivisions currently utilizing electronic signature certificates; and

7.4.c. Any future uses, changes or updates relating to the development of electronic signature certificates the state should take into consideration for its benefit.

~~7.4~~ 7.5. The Secretary of State may revoke the authorization of a program designated under this section if the program fails to continue operation or fails to meet the requirements of the state.

7.5.a. The Office of Technology, through its chief technology officer or his or her designee, shall make known to the Secretary of State any information that could contribute to the authorized program being revoked.

~~7.4.a~~ 7.5.b. The Secretary of State shall publish a notice in the State Register of the intent to revoke the authority of the program to act as state certificate authority and repository at least ninety days before the revocation takes effect and shall additionally send notice to each state agency or state agency subdivision currently utilizing electronic signature certificates.

~~7.4.b~~ 7.5.c. Upon revocation of the designation of a state certificate authority and repository, an agency that accepts electronic signatures issued by that entity may determine whether to continue to accept those electronic signatures or establish a date after which those signatures will no longer be accepted, and shall give notice in conjunction with the electronic filing information of the agency's intent.

§153-30-8. Authorization of Electronic Postmark

8.1. An agency may accept an electronic postmark, as defined in subsection 2.6 of this rule, as evidence of compliance with a requirement for United States registered mail or certified mail, return receipt requested.

8.2. This section shall not be construed to require a person or state agency to use or permit

the use of an electronic postmark.

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

9.1. The Secretary of State may 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 electronic signature certificates.

9.2. The Secretary of State may initiate a procurement process to obtain the software and systems to serve 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 certificate authority and a state repository.

9.4. The state certificate 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.

9.5. The state certificate 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.

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

9.7. To be qualified for selection as a state certificate 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 Authority Practice.

10.1. The state certificate authority shall provide the Secretary of State at least annually, or upon any significant change in procedures, a certificate 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 certificate practice statement within thirty (30) days after it is filed.

10.3. The state certificate 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 certificate 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 ninety-five percent (95%) 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 certificate 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 twenty-four (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 certificate 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 certificate 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 certificate 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 certificate 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 certificate 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 certificate 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 certificate 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 certificate 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 certificate 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 certificate authority, the authority shall give notice of the suspension to the state repository.

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

§153-30-15. Revocation of Certificate.

15.1. The state certificate 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 certificate 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 certificate 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 certificate 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 certificate 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 certificate 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 certificate 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 Certificate Authority or State Repository.

20.1. If a state certificate 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 (120) 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 certificate 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 certificate 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. A state certificate authority selected under section nine of this rule 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. A certificate authority authorized under section seven of this rule may charge the fee for issuance of a certificate which is 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.