

WEST VIRGINIA
SECRETARY OF STATE
KEN HECHLER
ADMINISTRATIVE LAW DIVISION

Form #3

Do Not Mark In this Box

RECEIVED
98 AUG -3 PM 4:12
OFFICE OF THE SECRETARY OF STATE

**NOTICE OF AGENCY APPROVAL OF A PROPOSED RULE
AND
FILING WITH THE LEGISLATIVE RULE-MAKING REVIEW COMMITTEE**

AGENCY: SECRETARY OF STATE TITLE NUMBER: 153

CITE AUTHORITY W.VA. CODE §39-5-4

AMENDMENT TO AN EXISTING RULE: YES ☐ NO ☒

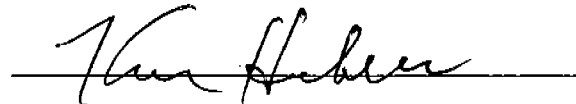
IF YES, SERIES NUMBER OF RULE BEING AMENDED: _____

TITLE OF RULE BEING AMENDED: _____

IF NO, SERIES NUMBER OF NEW RULE BEING PROPOSED: 31

TITLE OF RULE BEING PROPOSED: USE OF DIGITAL SIGNATURES, STATE
CERTIFICATION AUTHORITY AND STATE REPOSITORY

THE ABOVE PROPOSED LEGISLATIVE RULE HAVING GONE TO A PUBLIC HEARING OR A PUBLIC COMMENT PERIOD IS HEREBY APPROVED BY THE PROMULGATING AGENCY FOR FILING WITH THE SECRETARY OF STATE AND THE LEGISLATIVE RULE MAKING REVIEW COMMITTEE FOR THEIR REVIEW.



\$8.20

QUESTIONNAIRE

(Please include a copy of this form with each filing of your rule: Notice of Public Hearing or Comment Period; Proposed Rule, and if needed, Emergency and Modified Rule.)

DATE: JULY 31, 1998

TO: LEGISLATIVE RULE-MAKING REVIEW COMMITTEE

FROM: (Agency Name, Address & Phone No.) SECRETARY OF STATE

BLDG. 1, SUITE 157-K

CHARLESTON, WV 25305

LEGISLATIVE RULE TITLE: USE OF DIGITAL SIGNATURES, STATE CERTIFICATION

AUTHORITY AND STATE REPOSITORY

1. Authorizing statute(s) citation W.VA. CODE §39-5-4

2. a. Date filed in State Register with Notice of Hearing or Public Comment Period:

JULY 1, 1998

b. What other notice, including advertising, did you give of the hearing?

MEMBERS OF INTERGOVERNMENTAL TECHNOLOGY COUNCIL, CONSISTING OF

REPRESENTATIVES OF EACH STATE OFFICE OR AGENCY.

c. Date of Public Hearing(s) *or* Public Comment Period ended:

JULY 31, 1998

d. Attach list of persons who appeared at hearing, comments received, amendments, reasons for amendments.

Attached X

No comments received _____

- e. Date you filed in State Register the agency approved proposed Legislative Rule following public hearing: (be exact)

JULY 31, 1998

- f. Name, title, address and phone/fax/e-mail numbers of agency person(s) to receive all *written correspondence* regarding this rule: (Please type)

MARY RATLIFF

PHONE: 558-6000

SECRETARY OF STATE

FAX: 558-0900

BLDG. 1, SUITE 157-K

E-MAIL: MRATLIFF@SECRETARY.STATE.WV.US

CHARLESTON, WV 25305

- g. **IF DIFFERENT FROM ITEM 'f'**, please give Name, title, address and phone number(s) of agency person(s) who wrote and/or has responsibility for the contents of this rule: (Please type)

SAME

3. If the statute under which you promulgated the submitted rules requires certain findings and determinations to be made as a condition precedent to their promulgation:

- a. Give the date upon which you filed in the State Register a notice of the time and place of a hearing for the taking of evidence and a general description of the issues to be decided.

N/A

b. Date of hearing or comment period:

N/A

c. On what date did you file in the State Register the findings and determinations required together with the reasons therefor?

N/A

d. Attach findings and determinations and reasons:

Attached N/A

Statement of Purpose

The purpose of this rule is to establish procedures and requirements for a state certification authority and state repository for maintaining digital signatures for subscribers, to establish requirements for subscribers to digital signature certificates.

Statement of Circumstances

The Legislature has authorized the acceptance of electronic signatures by state agencies. The type of electronic signature with the highest level of security is the digital signature, which is verified electronically upon each use by a certification authority, much as a credit card is verified by the issuing company. The Legislature provided that the Secretary of State shall serve as the certification authority, and authorized the Secretary to contract with a private vendor for those services.

APPENDIX B

FISCAL NOTE FOR PROPOSED RULES

Rule Title: Use of digital signatures, state certification authority and state repository

Type of Rule: X Legislative Interpretive Procedural

Agency Secretary of State

Address Bldg. 1, Room 157-K

Charleston, WV 25305

1. Effect of Proposed Rule

	ANNUAL FISCAL YEAR				
	INCREASE	DECREASE	CURRENT	NEXT	THEREAFTER
<u>ESTIMATED TOTAL COST</u>	\$ 30,000	\$	\$ 10,000	\$ 30,000	\$ 30,000
PERSONAL SERVICES					
CURRENT EXPENSE	30,000		10,000	30,000	30,000
REPAIRS & ALTERATIONS					
EQUIPMENT					
OTHER					

2. Explanation of above estimates:

Cost of digital signature certificates and related software for subscribers in all state agencies will involve ongoing costs, but those costs should be offset by other savings.

3. Objectives of these rules:

To promote electronic exchange of documents between state agencies and between the general public and state agencies.

Rule Title: Use of digital signatures, state certification authority and state repository

4. Explanation of Overall Economic Impact of Proposed Rule.

A. Economic Impact on State Government.

Longterm savings by replacing expensive manual transactions with electronic transactions.

B. Economic Impact on Political Subdivisions; Specific Industries; Specific groups of Citizens.

Costs to local government will be voluntary, depending on desire to use; use should promote economic development.

C. Economic Impact on Citizens/Public at Large.

Same as B.

Date: July 1, 1998

Signature of Agency Head or Authorized Representative



State of West Virginia

Office of the State Auditor
Building 1, Room W-100
Charleston, West Virginia 25305

Glen B. Gainer III
State Auditor

Telephone: (304) 558-2251
FAX: (304) 558-5200
Internet: <http://www.wvauditor.com>

August 3, 1998

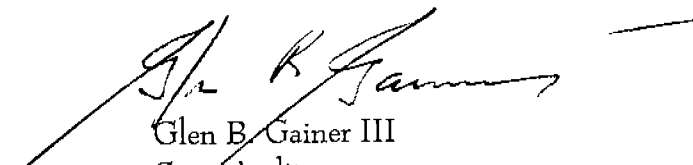
The Honorable Ken Hechler
Secretary of State
Building 1, Room 157K
Charleston, WV 25305

Dear Mr. Hechler:

This letter is to memorialize my approval of the filing of Rules 153-30 and 153-31. I give my approval, however, with reservation to approach the Legislative Rule Making Review Committee should any matters relating to this rule come to my attention after my approval has been given. I take this step because these rules cover matters of national importance and are of great consequence to our state. We must endeavor to incorporate the views of citizens, experts, vendors and others affected thereby.

Thank you for your assistance and direction in this matter. If you have any questions regarding this or any other matters, please do not hesitate to contact me at the above-referenced address.

Sincerely,



Glen B. Gainer III
State Auditor

GBGIII/lq

**TITLE 153
LEGISLATIVE RULES
SECRETARY OF STATE**

RECEIVED
98 AUG -8 PM 4:12

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.

1.3. Filing Date. --

1.4. Effective Date. --

§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 such 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 is authorized to contract with a vendor for services as both state certification authority and state repository.

3.4. The state certification authority shall be authorized to 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 shall be authorized to 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 these rules.

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

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; and

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 certifications authority's stated control objectives. Such 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.

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 must 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 must 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 such 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 such additional information and services as may be specified in its contract with the state.

5.9. The state repository shall make the required Repository Services available via such protocols and methods as the state may specify or as the state and the state repository shall mutually agree.

5.10. The state repository will 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; and

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 must 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;

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 West Virginia 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; or

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, 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 shall be subject to the contract with the state certification authority.

10.2. The certificate shall be 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 X.509, Ver. 3, in accordance with

certificate profiles issued by the state.

11.2. If certificate extension fields are used, usage must conform to the required guidelines referenced in X.509 section 4.1.2.1., section 4.2, 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;

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 such records as are necessary to assure compliance with the provisions of Chapter 39, Article 5 of the West Virginia Code 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 and 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. Such audit shall include a SAS 70 Type Two audit as specified in Section 3.7.5

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 corporate surety bond or letter of credit filed with the application may not be released 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.

TITLE 153
LEGISLATIVE RULES
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 signatures¹ and establishes requirements for a state certification authority.

1.2. Authority. -- W. Va. Code §§ 39-5-4.

1.3. Filing Date. --

1.4. Effective Date. --

§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.

¹ It is important to recognize that the requirements for the use of digital signatures will vary depending upon the application. Critical issues, such as quality control of the certification authority issuing the certificate, and the policies and procedures by which a certificate is issued, will vary depending upon the application. For some applications, a low level certificate (or even another form of electronic signature) might suffice. For other applications, only a high level certificate and a very secure digital signature process will be appropriate. Thus, it may not be appropriate to adopt a "one size fits all" set of rules.

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 electronically ~~approved~~ 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 (A) whether the message was created using the corresponding private key, and (B) 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 [to employees or agents of the State] on behalf of the State.²

2.7. "Key pair" means, a set of corresponding public and private digital keys in an asymmetric cryptosystem, in which two mathematically related keys, referred to as a private key and a public key, having the properties that (1) one key (the private key) can encrypt a message which only the other key (the public key) can decrypt, and (2) even knowing one key (the public key), it is computationally infeasible to discover the other key (the private key).

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

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

2.8. "Corresponding," with reference to keys, means to belong to the same key pair, in which both keys are required for identification and verification of a digital signature.

2.9. "Certification practice statement" means a declaration of the practices that a

² In whose name are these certificates issued? That is, is the State simply contracting with a private CA, such as Verisign, to issue Verisign certificates, or alternatively, is the State contracting with a private CA to issue certificates in the name of the State?

certification authority employs in issuing, managing, suspending, and revoking certificates and providing access to them, certificates generally, or employs in issuing a material certificate.

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

2.11. "Subscriber" means a person who:

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

2.11.2. Accepts the certificate; and

2.11.3. Holds a Controls the private key that corresponds to a the pubic key listed in that certificate; and

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

2.12. "Electronic" means electrical, digital, magnetic, optical, electromagnetic, or any other technology that is similar to these technologies.³

2.13. "Electronic record" means a record generated, communicated, received, or stored by electronic means.⁴

2.14. "Record" means information that is inscribed on a tangible medium or that is

³ This definition is taken from the statute at Section 39-5-2(c).

⁴ This definition is taken from the statute at Section 39-5-2(d).

stored in an electronic or other medium and is retrievable in perceivable form.⁵

2.15 "Trustworthy system" means computer hardware, software, and procedures that (1) are reasonably secure from intrusion and misuse; (2) provide a reasonably reliable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (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 ~~a contract~~ the services of ~~with~~ one or more private vendors,⁶ at the discretion of the state, to serve as a state certification authority.⁷

⁵ This definition is taken from the statute at Section 39-5-2(f).

⁶ As written, this section appears to contemplate multiple State Certification Authorities. Is that the intent?

⁷ As noted in the footnote corresponding to Section 2.6, it is important to determine whether the State Certification Authority will be the State of West Virginia, with the Certification Authority services performed by a private entity, or alternatively, whether the State Certification Authority will be a private entity, such as Verisign. Section 39-5-4(b) of the statute designates the Secretary of State as "the Certification Authority and Repository for all governmental

3.2. The Secretary of State shall initiate a procurement process to obtain ~~a contract with the services of~~ one or more private vendors,⁸ at the ~~deseeration~~ discretion of the state, to serve as a state repository.

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

3.4. The state certification authority shall be authorized to issue a certificate that binds a public key to any authorized person for the purpose of verifying using a digital signature created by such 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 shall be authorized to issue a certificate to any person⁹ for the purpose of verifying using a

agencies". However, the same section also authorizes the Secretary of State to "contract with a private entity to serve as Certification Authority for the State". This would appear to leave either option open. Thus, the issue may come down to a question of who is identified as the Certification Authority in certificates issued by the State Certification Authority - e.g., the State of West Virginia, Verisign, Digital Signature Trust, etc.?

⁸ As written, this section also contemplates multiple vendors operating as a State Repository. Is this the intention? I am currently working on two products involving multiple Certification Authorities, one which will also include multiple repositories and the other which requires a single consolidated repository. Presumably either scenario will work, although both present a variety of practical issues that need to be resolved. Accordingly, this issue may require further attention.

⁹ Does the State want to be in the business (either directly or through a certification authority with which it contracts) of issuing certificates to private citizens for use on electronic records filed with a state agency? The

digital signature created by such 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 these rules.

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

3.7.1. Maintain a system of internal electronic security controls to restrict access to systems and data only to authorized personnel, and conduct appropriate clearances in which of such personnel with access authority to secure data are persons who 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;

alternative is, perhaps, to approve, authorize, or certify private certification authorities as certification authorities whose certificates are acceptable for use in filing specified types of state-related documents. This approach may also require a somewhat extensive set of regulations. However, it is an option that may be worth considering, especially since different levels of certificates will presumably be acceptable for different types of filings with the State.

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

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 certifications authority's stated control objectives. Such 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.

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, operation of the system verification of documents containing digital signatures.

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

4.2.1. ~~To~~ issue, suspend, or revoke a certificate;

4.2.2. ~~To~~ publish or give notice of the issuance, suspension, or revocation of a certificate; or

4.2.3. ~~To~~ create and protect a private keys.

4.3. Upon a written, signed and reasonably specific inquiry from an identified person, the state certification authority must disclose ~~any material~~ its certification practice statement, and any fact material to either the reliability of a certificate that it has issued or its ability to perform its services. The certification authority may require payment of reasonable compensation before making this disclosure.¹⁰

4.4 The State Certification Authority shall at all times comply with the requirements of the applicable certificate policy issued by the State of West Virginia and all certificates that it issues pursuant to its contract with the State shall reference the State Certificate Policy in the manner required in the Policy.¹¹

¹⁰ Given the role of a Certification Practice Statement in this context, it may be more appropriate to simply require that the State Certification Authority publish its Certification Practice Statement so that it is available free of charge to anyone with an interest in reviewing it. Requiring a written and signed inquiry and the payment of reasonable compensation in order to obtain a copy of the Certification Practice Statement of the State Certification Authority does not seem to be appropriate. This issue should perhaps receive further consideration.

¹¹ If the State is going to be in the business of contracting with one or more Certification Authorities, it may be appropriate to issue a certificate policy clearly setting forth the rules for all Certification Authorities. Alternatively, this could also be done by contract. Thus, I include this section primarily as a placeholder to raise the issue for further consideration.

4.5 The State Certification Authority shall provide such services as may be specified in the State Certificate Policy and its contract with the State.

§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 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, utilized in the system of verification of documents containing digital signatures.

5.2. The state repository shall provide all repository services by means of a Trustworthy Ssystem, use only a trustworthy system to store the key combination and process the verification transactions required for each subscriber.

5.3. Upon a written, signed and reasonably specific inquiry from an identified person, the state repository must disclose any material ~~certification~~ practice statement, and any fact material to either the reliability of a specific verification transaction or its ability to perform its services. The state repository may require payment of reasonable compensation before making this disclosure.¹²

¹² See previous footnote corresponding to Section 4.3.

5.4 The state repository shall provide an online database containing at least (a) all valid certificates published into the database by state certification authorities, and (b) all notices of revocation of such certificates published into the directory by state certification authorities.

5.5 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.

5.6 The state repository [may/shall] store certificates issued by state certification authorities that are no longer valid and provide copies of them on request. The state repository [may/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 [may/shall] make copies of the information available on request.

5.7 The state repository shall provide such additional information and services as may be specified in its contract with the state.

5.8 The state repository shall make the required Repository Services available via such protocols and methods as [the state may specify / the state and the state repository shall mutually agree.]

5.9 The state repository will be available for use online _____ % of the time. When down time is planned, The state repository shall give reasonable notice before the down time.

5.10 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

hour(s) 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.

5.11. 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 signed¹³ 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 confirmed that:

6.1.2.1. The prospective subscriber is the person to be listed in the certificate to be issued;¹⁴

¹³ Does the requirement of a "signed" request for a certificate imply a handwritten signature on paper? Is the intent to preclude online applications for certificates? If so, this may make the procedural aspect of obtaining a certificate rather difficult and costly.

¹⁴ This language appears to require the Certification Authority to guarantee the identity of the subscriber (as opposed to conducting a specified process to verify identity). Is that the intention? If so, it may be more difficult to find a Certification Authority who is willing to agree to this obligation.

6.1.2.2. The information in the certificate to be issued is accurate;¹⁵

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

6.1.2.4. 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

6.1.2.5. 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.¹⁶

¹⁵ See previous footnote. This requirement presumably includes an obligation to ensure that the identity of the subscriber listed in the certificate "is accurate". Depending upon the other information included in the certificate, this may also present additional problems for Certification Authorities.

¹⁶ This section raises an interesting issue that deserves further review and analysis. It appears to contemplate some sort of "agency" certificate - i.e., a certificate that not only identifies the subscriber, but also specifies the subscriber's level of authority - i.e., his or her authority to act as an agent for another person. How this is to be accomplished is not clear. I have not attempted to revise this section, but at this point simply raised the question as to whether the certificate should purport to evidence authority or agency (especially since these are dynamic attributes that will change over time). Alternatively, it may make sense to simply limit the certificate to identifying the named subscriber and leave issues of authority or agency to be confirmed separately. That is, for example, when an employee of the State signs a document as agent for the Secretary of State, or when an attorney signs a document as agent

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

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

6.2.1.2. 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

6.2.1.3. 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 5.1. of this rule may not be waived or disclaimed by either the certification authority, the subscriber, or both.¹⁷

for a corporation, the fact of the agency is stated on the document, but must be separately confirmed. In either case, the signature itself is the signature of the agent, but on its face gives no indication of its agency authority.

¹⁷ This section appears to contain a reference to the wrong section. Please verify the intent.

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 must 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 certificate¹⁸ issued by the state certification authority, the subscriber listed in the certificate certifies¹⁹ 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;²⁰

¹⁸ How does a subscriber "accept" a certificate? Also, if the subscriber is an unsophisticated individual, can such person realistically be expected to review and understand the contents of a certificate in order to knowingly accept it?

¹⁹ Why does the subscriber make warranties but the certification authority does not?

²⁰ While this may be an important warranty to be made by the subscriber, there is a question as to whether it is a realistic one. For example, when someone obtains a certificate from Verisign through its Web site, how does that person have any way of knowing whether the mixed up series of numbers and letters that purport to

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

~~7.1.3. All material representations made by the subscriber to a certification authority or made in the certificate and not confirmed by the certification authority in issuing the certificate are true.~~

7.2. By accepting a certificate ~~and using a digital signature~~, a subscriber recognizes that the provisions of West Virginia Code §61-3C-10 prescribe the penalties for the unauthorized disclosure of confidential security information, including the private key.²¹

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.²²

be the public key included in the certificate is in fact the public key that corresponds to the private key stored on the subscriber's computer (which the subscriber has never seen and presumably does not understand).

²¹ This obligation should only apply during the operational period of a certificate. Moreover, it seems strange that the obligation of the West Virginia Code Section 61-3C-10 applies only to the subscriber and only upon acceptance of a certificate. Presumably it should apply to all persons, whether or not they hold a certificate (i.e., if an individual obtains an unauthorized copy of a certificate holder's private key, and discloses that information, he should also be liable).

²² While it is probably appropriate to impose this obligation on the subscriber, it should be recognized that in all likelihood the subscriber will not take the time to revoke his or her certificate upon separation from the agency. Accordingly, these rules should also clearly require the agency to revoke the certificate of any employee or agent upon their separation from the

§153-31-8. Suspension of Certificate²³

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:

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

8.1.1.2. a person duly authorized to act for that subscriber; or

8.1.1.3. 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, telephone number, of the person requesting suspension, and other evidence of his or her identity.

agency or upon any other termination of their ability to act on behalf of the agency. Also, this section refers to certificates issued to a person in their "capacity to act on behalf of an agency". This raises the agency issue discussed in the footnote attached to Section 6.2.

²³ The section on suspension of a certificate and the following section on revocation of a certificate contain provisions taken from other legislation or regulations, but it is not entirely clear that they are appropriate in this circumstance. They appear to mix the issue of whether the subscriber is an employee or agent of the State or whether the subscriber is a private party. This type of detail may also be more appropriate for a certificate policy than a regulation.

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 one or more certificates that it issued if the certificates become unreliable,²⁴

²⁴ What does this mean?

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.

§153-31-9. Expiration of Certificate

9.1. The term of the certificate shall be subject to the contract with the state certification authority ~~as provided in section three of this rule.~~

9.2. The certificate shall be valid for the duration of the term, unless ~~previously~~ sooner revoked, beginning on the date of issuance.

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

9.4. 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~~ions~~.

§153-31-10. Form of Certificates

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

10.2. If certificate extension fields are used, usage must conform to the required guidelines referenced in X.509 section

4.1.2.1., section 4.2, and may be displayed on the certificate.²⁵

§153-31-11. Record keeping and Retention

11.1. The state certification authority shall maintain a data file containing the record of each subscriber,²⁶ including at least:

11.1.1. 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,²⁷

11.1.2. 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;

11.1.3. The date of the issuance and the expiration of the certificate, and certificate number.

11.2. The state repository shall maintain a data file containing every time-stamp issued by the certification authority, with sufficient

²⁵ I'm not sure that this sentence makes sense. Perhaps a reference to a state issued certificate profile would be more appropriate?

²⁶ What about privacy of the data? If a private entity is maintaining personal data on behalf of the state, the estate should control what that private entity can do with that data.

²⁷ This raises questions regarding the nature of the certificates -- i.e., do they certify agency or authority as well as identity?

information to identify the subscriber and the document.

11.3. The state certification authority shall maintain such records as are necessary to assure compliance with the provisions of Chapter 39, Article 5 of the West Virginia Code and this rule, as they pertain to digital signatures and the certificate authority.

11.4. 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 and 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.

§153-31-12. Compliance Audit

12.1. The state certification authority may²⁸ be subject to an annual compliance audit conducted by a reliable certified public accountant in conjunction with a reliable authority on computer security. Such audit shall include a SAS 70 Type Two audit as specified in Section 3.7.5

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

§153-31-13. Procedure on Discontinuance of Business of State Certification Authority or State Repository

13.1. 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:

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

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

13.1.3. Minimize disruption to the subscribers of valid certificates and relying parties;²⁹

13.1.4. 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

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

13.2. The corporate surety bond or letter of credit filed with the application may not be released until the expiration of the term specified in the bond or letter of credit.

13.3. 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 ~~licensed state~~ state certification authority or ~~recognized state~~ 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.

13.4. The state may recover the costs of the state incurred in conjunction with the

²⁸ Is this optional?

²⁹ How?

early termination of the contract and the process of obtaining alternative services.

§153-31-14. Fees for Issuance of Certificates

14.1. 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.

14.2. 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.