960991761

HOUSE BILL NO. 822

Offered January 22, 1996

A BILL to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 39, consisting of sections numbered 59.1-467 through 59.1-493, relating to trade and commerce; digital signatures; penalty.

Patrons—Almand, Plum and Scott

Referred to Committee on Corporations, Insurance and Banking

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 39, consisting of sections numbered 59.1-467 through 59.1-493, as follows:

CHAPTER 39.

THE VIRGINIA DIGITAL SIGNATURE ACT.

Article 1.

General Provisions.

§ 59.1-467. Short title.

This chapter is known as the Virginia Digital Signature Act.

§ 59.1-468. Purposes and construction.

This chapter shall be construed liberally to effectuate the following purposes:

1. To minimize the incidence of forged digital signatures and enable the reliable authentication of computer-based information;

2. To enable and foster the verification of digital signatures on computer-based documents;

3. To facilitate commerce by means of computerized communications; and

4. To give legal effect to the general import of the following and other similar standards;

a. Standard X.509 of the International Telecommunication Union (formerly CCITT or International Telegraph and Telephone Consultative Committee);

b. Standard X.9.30 of the American National Standards Institute (ANSI); and

c. RFC 1421 through 1424 of the Internet Activities Board (IAB).

§ 59.1-469. Definitions.

As used in this chapter unless the context clearly indicates otherwise:

"Accept a certificate" means to either (i) take physical delivery of a certificate or (ii) apply for a certificate without canceling or revoking the application by delivering notice of the cancellation or revocation to the certification authority, and to obtain a signed, written receipt from the certification authority.

"Asymmetric cryptosystem" means a computer algorithm or series of algorithms which utilize two different keys with the following characteristics: (i) one key encrypts a given message; (ii) one key decrypts a given message; and (iii) the keys have the property that, knowing one key, it is computationally infeasible to discover the other key.

"Bit" means a binary digit, or a number, often encoded in a computer-readable form, which has a value of either 0 or 1.

"Certificate" means (i) a computer-based record identifying a subscriber and containing the subscriber's public key or (ii) if the certificate is issued by a licensed certification authority, a computer-based record identifying a subscriber containing the subscriber's public key, and additional data about the subscriber as specified in § 59.1-470.

"Certification authority" means a person who issues one or more certificates.

"Certification authority disclosure record" means an on-line, publicly accessible computer record concerning a licensed certification authority maintained by the Commission in accordance with § 59.1-473.

"Certify" means to declare with reference to a certificate, that all material facts in the certificate are true.

"Confirm" means to ascertain through inquiry and investigation carried out with all the effort and resources commercially reasonable under the circumstances.

"Correspond" means, when referring to keys, that one key belongs to the same key pair as the other.

"Digital signature" is a sequence of bits which a person intending to sign creates in relation to a clearly delimited message by running the message through a one-way function, then encrypting the resulting message digest using an asymmetrical cryptosystem and the person's private key.

"Commission" means the Virginia State Corporation Commission.

"Distinguished name" means a sequence of alphanumeric characters uniquely identifying the person bearing the name.

"Forge a digital signature" means to create an apparent digital signature without the authorization of the rightful holder of the private key.

"Issue a certificate" means to create and digitally sign a certificate and to deliver a copy of the certificate to the subscriber named in the certificate.

"Key pair" means a private key and its corresponding public key which are the keys in an asymmetric cryptosystem having the property that one of the pair will decrypt what the other encrypts.

"Licensed certification authority" means a certification authority to whom a license has been issued by the Commission.

"Material means germane to and having substantial consequences for an actual transaction involving a digital signature.

"Message" means a writing or recording recorded by means of any medium and intended to be signed. As used in this definition, "writings" and "recordings" consist of letters, words, numbers, or their equivalent, set down by handwriting, typewriting, printing, photostatting, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.

"One-way function" means an algorithm mapping or translating one set of bits into another set in such a way that: (i) a message yields the same result every time it is passed through the one-way function; (ii) it is computationally infeasible that a message passed through the one-way function can be derived or reconstituted from the results of the function; and (iii) there is at most only a negligible probability that two messages passing through the same one-way function will produce the same result.

"Operative personnel" means one or more persons (i) acting as a certification authority or its agent, (ii) having managerial or policymaking responsibilities for the certification authority, or (iii) having duties directly involving the issuance of certificates, creation of keys, or administration of computing facilities.

"Person" means a natural person, corporation, partnership, governmental body, or any other entity capable of signing a document.

"Private key" means a sequence of bits in an asymmetric cryptosystem used to affix a digital signature to a message. A private key is intended to be known only by the rightful holder of the key.

"Public key" means a sequence of bits in an asymmetric cryptosystem used to verify a digital signature. A public key may be known and used by anyone in order to verify a signature.

"Publish" means to record or place on file in a repository accessible by multiple persons in the ordinary course of business.

"Recognized repository" means a repository recognized by the Commission pursuant to § 59.1-491.

"Recommended reliance limit" means the limit of an issuing certification authority's liability and financial responsibility specified in a certificate.

"Record address" means (i) the address on file with the Commission for a Virginia corporation or foreign corporation authorized to do business in Virginia; (ii) the principal, official, or record address on file with any other government entity if no address is on file with the Commission; or (iii) if no address is reasonably ascertainable with a government entity, the last-known address of the subscriber ascertained, whenever possible, independently of any representations made in applying for a certificate.

"Record leaders" are (i) the officers and directors or trustees listed for a corporation on the most recent report to the Commission or its counterpart in another state; (ii) the general partners listed for a limited partnership in the records of the Commission or its counterpart in another state; and (iii) the natural persons having authority to manage or direct the affairs of the subscriber, ascertained whenever possible from information sources other than representations made in applying for a certificate.

"Repository" means a database of certificates accessible on-line.

"Repository operator" means the person operating and responsible for the repository.

"Revoke a certificate" means to make a certificate ineffective from a specified time and forward perpetually. Such revocation is effected by notation or inclusion in a set of revoked certificates, and does not imply that a revoked certificate is destroyed or made illegible.

"Rightfully hold a private key" means to know or be able to readily ascertain a private key (i) for which a corresponding public key has not been published in a certificate on file in the repository provided by the Commission or in a recognized repository, (ii) which the holder or the holder's agent has not revealed to any person in violation of subsection A of § 59.1-480; and (iii) which the holder has not obtained through theft, deceit, eavesdropping, or other unlawful means.

"Subscriber" means a person holding a private key which corresponds to a public key listed in a certificate identifying the subscriber.

"Suitable guaranty" means either a surety bond executed by a surety firm authorized by the Virginia State Corporation Commission to do business in this Commonwealth, or an irrevocable letter of credit issued by a financial institution authorized to do business in this Commonwealth by the Virginia State Corporation Commission which satisfies all of the following requirements:

1. It is issued for the benefit of claimants under this chapter and is conditioned upon the certification authority conducting business as required by this chapter;

2. It is in an amount equal to or exceeding the greater or either:

a. 100 percent of the largest recommended reliance limit of a certificate to be issued or published by the filing certification authority during the term of the certification authority's license; or

b. At least thirty-five percent of the recommended reliance limits of all certificates published by the filing certification authority which have not expired or been revoked;

3. It states that it is issued for filing pursuant to this chapter;

4. It specifies a term of effectiveness extending at least as long as the term of the license to be issued to the certification authority; and

5. It is in a form approved by Commission rule.

A suitable guaranty may provide that the total annual liability on the guaranty to all persons making claims based on it may not exceed the face amount of the guaranty.

"Suspend" means to make the certificate ineffective or void temporarily from a specified time forward. However, the term does not imply that the certificate is destroyed or made illegible.

"Time-stamp" means either (i) to append to a message a digitally signed notation indicating the date, time, and identity of the person appending the notation or (ii) the notation so appended according to subdivision 1.

"Verify a digital signature" means:

1. To decrypt a digital signature using the public key listed in a valid certificate;

2. To pass the message through the one-way function used in affixing the digital signature; and

3. To then correctly determine that the results of passing the message through the one-way function and the decrypted digital signature are identical.

§ 59.1-470. Contents and effective date of a certificate.

A. A certificate issued by a licensed certification authority shall contain:

1. The name by which the subscriber is generally known;

2. The distinguished name of the subscriber;

3. A public key corresponding to a private key held by the subscriber;

4. A brief description of any algorithms with which the subscriber's public key was intended to be used in a form prescribed by the Commission;

5. The serial number of the certificate which must be unique among the certificates issued by the issuing certification authority;

6. The date and time on which the certificate was issued and accepted which is the date on which the certificate takes effect;

7. The date and time on which the certificate expires;

8. The distinguished name of the certification authority issuing the certificate;

9. A brief description of the algorithm used to sign the certificate, in a form prescribed by the Commission;

10. The recommended reliance limit for transactions relying on the certificate; and

11. Other items the Commission requires by rule.

b. A certificate issued by a licensed certification authority may, at the option of the subscriber and certification authority, contain any of the following:

1. A secondary public key and its identifier or usage indicate;

2. Information material to the certificate's reliability and to any claims based on it;

3. References incorporating specified and available documents material to the certificate, the issuing certification authority, or the accepting subscriber, and

4. Other items permitted by Commission rule.

C.1. The Commission may by rule require additional information in a certificate, so long as the certificate conforms to generally accepted standards for digital signature certificates and nothing in the certificate disclaims or limits the representations of the subscriber and the certification authority implied in Article 3 (§ 59.1-477, et seq.) of this chapter.

2. The certificate shall be in a database form specified by Commission rule.

D.1. The Commission may, at the joint request of a subscriber and licensed certification authority, create a secret field in its database. The Commission may disclose the contents of the secret field in its database only to:

a. The licensed certification authority publishing the certificate;

b. Authorized personnel of the Commission; and

c. A court clerk or county clerk who has received a request for suspension of the pertinent certificate.

2. The contents of the secret field should be a password or fact likely to be known only by the subscriber, and may, in the discretion of the entity processing a request for suspension, be used to

determine the identity of the requester.

Article 2.

Licensing and Regulation of Certification Authorities.

§ 59.1-471. Licensure and qualifications of certificate authorities.

A. To obtain or retain a license as a certification authority by the Commission, a certification authority must be:

1. An attorney admitted to practice before the courts of this Commonwealth, an attorney's partnership which engages principally in the practice of law if the attorney is a partner, or a professional corporation in which the attorney named in the license is a shareholder;

2. A financial institution, a corporation authorized to conduct a trust business, or an insurance company, if authorized to do business in this Commonwealth;

3. Any title insurance or abstract company authorized to do business in this Commonwealth; or

4. The Governor, an agency of this Commonwealth other than the Commission, the Attorney General, a state court, a city, a county, or the General Assembly provided that:

a. Each of the governmental entities acts through designated officials authorized by ordinance, rule, or statute to perform certification authority functions;

b. The Commonwealth or one of the governmental entities is the subscriber of all certificates issued by the certification authority;

c. Be the subscriber of a certificate published in the repository provided by the Commission or in a recognized repository;

d. Qualify and hold an appointment as a notary public or employ at least one notary public;

e. Employ as operative personnel only persons who have not been convicted of a felony or a crime involving fraud, false statement, or deception;

f. Employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter;

g. File with the Commission a suitable guaranty, unless the certification authority is a governmental entity listed in this subsection;

h. Have access to hardware and software suitable for fulfilling the requirements of this chapter according to Commission rules;

i. Maintain an office in Virginia or have established a registered agency for service of process in Virginia; and

j. Comply with all licensing requirements established by Commission rule.

B. The Commission shall issue a license to a certification authority which:

1. Is qualified under subsection A;

2. Applies in writing to the Commission for a license; and

3. Pays the required filing fee.

C.1. A license may specify that its scope is limited to:

a. A specified number of certificates; or

b. A specified cumulative maximum of recommended reliance limits in certificates issued by the certification authority.

2. If the scope of a license is limited, a certification authority acts as an unlicensed certification authority when issuing a certificate exceeding the limits of the license.

D.1. The Commission may revoke or suspend a certification authority's license for failure to comply with this chapter, or for failure to remain qualified pursuant to subsection A.

2. The Commission's actions under this subsection are subject to the provisions of the Administrative Process Act (§ 9-6.14:1 et seq.).

E. Unless the parties provide otherwise by contract between themselves, the licensing requirements in this section do not affect the validity of any certificate or digital signature issued by an unlicensed certification authority, except that:

1. The presumptions created in Article 4 (§ 59.1-487 et seq.) of this chapter do not apply to a certificate issued by an unlicensed certification authority; and

2. The limitation of liability created in § 59.1-485 does not apply to a certificate issued by an unlicensed certification authority.

§ 59.1-472. Performance audits and investigations.

A. A certified public accountant approved by Commission rule shall audit the operations of each licensed certification authority at least once each year to evaluate compliance with this chapter.

B.1. Based on information gathered in the audit, the auditor shall categorize the licensed certification authority's compliance as one of the following:

a. Full compliance; the certification authority appears to conform to all applicable statutory and regulatory requirements;

b. Substantial compliance; the certification authority generally appears to comply with all applicable statutory and regulatory requirements; however, some instances of noncompliance or inability to

demonstrate compliance were found in the audited sample which were likely to be inconsequential;

c. Partial compliance; the certification authority appears to comply with some statutory and regulatory requirements, but was found not to have complied or not able to demonstrate compliance with one or more statutory or regulatory requirements;

d. Noncompliance; the certification authority complies with few or none of the statutory and regulatory requirements, or fails to keep adequate records to demonstrate compliance with more than a few requirements, or refused to submit to an audit.

2. The Commission shall publish in the certification authority disclosure record the date of the audit and the resulting categorization of the certification authority.

C.1. A licensed certification authority is exempt from the requirement of subsection A if:

a. The certification authority requests exemption in writing;

b. The most recent performance audit, if any, of the certification authority resulted in a finding of full or substantial compliance; and

c. The certification authority states under oath or affirmation that one or more of the following is true with respect to the certification authority:

(1) The certification authority has issued fewer than six certificates during the past year and the recommended reliance limits of all such certificates do not exceed $10,000;

(2) The aggregate lifetime of all certificates issued by the certification authority during the past year is less than thirty days and the recommended reliance limits of all such certificates do not exceed $10,000; or

(3) The recommended reliance limits of all certificates outstanding and issued by the certification authority total less than $1,000.

2. If a licensed certification authority is exempt under this subsection, the Commission shall publish in the certification authority disclosure record that the certification authority is exempt from the performance audit requirement.

§ 59.1-473. Contents of a certification authority disclosure record.

A. A certification authority disclosure record shall contain:

1. The name, addresses, and telephone number of the certification authority;

2. The distinguished name of the certification authority;

3. The current public key of the certification authority;

4. The categorization of the certification authority based on the most recent performance audit of the certification authority's activities, and the date of the most recent performance audit;

5. If the certification authority's certificate has been revoked since licensure, the public key contained in the revoked certificate, date of revocation, and grounds for revocation;

6. The amount of the certification authority's suitable guaranty;

7. If the certification authority's license has been revoked or is currently suspended, the date of revocation or suspension and the grounds for revocation or suspension;

8. The limits, if any, placed on the certification authority's license;

9. Any event or activity which substantially affects the certification authority's ability to conduct its business, or the validity of more than ten of the certificates listed in the repository provided by the Commission or in a recognized repository;

10. If the certificate containing the public key required to verify one or more certificates issued by the certification authority has been revoked or is currently suspended, the date of its revocation or suspension;

11. A statement dated within one year of the current date, containing additional rules or policies, and not exceeding two kilobytes in length, if the certification authority submits such a statement in a form prescribed by Commission rule; and

12. Other information required by Commission rule.

B. The Commission shall maintain an electronic database in its repository containing the disclosure record described in this section for each licensed certification authority.

§ 59.1-474. Enforcement of requirements for licensed certification authorities.

A. Commission actions under this section must be made in accordance with the provisions of the Administrative Process Act (§ 9-6.14:1 et seq.).

B. The Commission may:

1. Investigate the activities of a licensed certification authority material to the requirements of this chapter; and

2. Issue orders to a certification authority to secure compliance with this chapter.

C. Nothing in this section restricts local law-enforcement authorities from investigating and prosecuting violations of criminal laws.

D. The Commission may suspend or revoke the license of a certification authority for serious noncompliance with an order of the Commission.

E. A person may obtain punitive damages against a certification authority in a civil action against the certification authority if:

1. The Commission has issued an order in accordance with subsection B expressly permitting punitive damages to be assessed against the certification authority;

2. The certification authority has not complied with the order;

3. The person has suffered a loss caused by noncompliance with the order; and

4. The Commission has granted permission for punitive damages.

F. The Commission may order a certification authority which it has found to have violated a requirement of this chapter to pay the costs incurred by the Commission in prosecuting and adjudicating proceedings related to the enforcement of the order.

G.1. A licensed certification authority may obtain judicial review of the Commission's actions.

2. The Commission may seek an injunction to compel compliance with any of its order.

§ 59.1-475. Record-keeping by certification authorities.

A. A licensed certification authority shall maintain detailed records documenting compliance with this chapter and all actions taken with respect to each certificate issued by the certification authority. The records shall include evidence supporting the identification of the person named in a certificate with the distinguished name and public key set forth in the certificate. Except for requests for suspension of a certificate, the licensed certification may require a subscriber or agent of a subscriber to submit reasonable documentation sufficient to enable the certification authority to comply with this chapter.

B.1. A licensed certification authority shall retain its records of the issuance, and any suspension or revocation of a certificate, for a period of not less than forty years after the certificate is issued.

2. The licensed certification authority may:

a. Contract with another licensed certification authority for the record retention required by this section; or

b. Place the records required by this section into the custody of the Commission upon ceasing to act as a certification authority.

3. A licensed certification authority shall secure its records in a manner that is commercially reasonable in light of the recommended reliance limits of the certificates.

§ 59.1-476. Cessation of certification authority activities.

A. Before ceasing to act as a certification authority, a licensed certification authority shall:

1. Give to the subscriber of each unrevoked or unexpired certificate ninety days' written notice of the certification authority's intention to discontinue acting as a certification authority;

2. Ninety days after the notice required in subdivision A 1, revoke all certificates which then remain unrevoked or unexpired, regardless of whether the subscriber has requested revocation;

3. Give written notice of revocation to the subscriber of each certificate revoked pursuant to subdivision A 1; and

4. Unless the contract between the certification authority and the subscriber provides otherwise, pay reasonable restitution to the subscriber for revoking the certificate before its expiration date.

B.1. To provide uninterrupted certification authority services, the discontinuing certification authority may arrange with another certification authority, including the Commission, for reissuance of the remaining certificates under the succeeding certification authority's digital signature for the unexpired term of the remaining certificates or one year, whichever is less.

2. In reissuing a certificate pursuant to this subsection, the succeeding certification authority becomes subrogated to the rights and defense of the discontinuing certification authority.

C. The requirements of this section may be varied by contract, except that the contract may not permit the licensed certification authority to discontinue its certification authority activities without first:

1. Giving each subscriber of an unexpired or unrevoked certificate at least ten days' written notice; and

2. Revoking all outstanding certificates upon cessation of certification activities.

D.1. A licensed certification authority shall notify the Commission of its intention to terminate acting as a certification authority.

2. The notice shall be in a form specified by Commission rule and shall be submitted to the Commission at least two months, but not more than six months, before the date of termination.

3. The Commission may by rule or by order in a specific case require additional statements to be filed in order to track compliance with this section.

E.1. If a certification authority dies while licensed, the estate of the certification authority shall comply with the procedures of this section for termination of the deceased certification authority's activities.

2. If a certification authority becomes legally incapacitated within the meaning of § 37.1-128.04, a court may either appoint a guardian as provided in Chapter 4 (§ 37.1-128.01 et seq.) of Title 37.1 or, on the petition of an interested party, appoint a receiver to terminate the incapacitated certification authority's business as provided in this section.

3. The Commission may promulgate rules to facilitate termination of certification authority activities or to protect subscribers and others in cases where the certification authority dies or becomes incapacitated.

§ 59.1-477. Hazardous activities by any certification authority prohibited.

A. A certification authority, whether licensed or not, may not conduct its business in a manner that creates a commercially unreasonable risk of loss to:

1. Subscribers of the certification authority;

2. Persons relying on certificates issued by certification authority; or

3. Any repository recognized pursuant to § 59.1-491.

B.1. The Commission may publish in the repository it provides or elsewhere statements advising subscribers, persons relying on digital signatures, or public repositories about activities of a certification authority, whether licensed or not, that create a risk prohibited by subsection A.

2. The certification authority named in a statement as creating or causing a risk may protest the publication of the statement.

3. Upon receipt of a protest, the Commission shall:

a. Include with its statement a comment that a protest has been received; and

b. Promptly give the protesting certification authority notice and an opportunity to be heard.

4. Following the hearing, the Commission shall:

a. Rescind the advisory statement if its publication was unwarranted;

b. Cancel it if its publication is no longer warranted;

c. Continue or amend it if it remains warranted; or

d. Take further legal action to eliminate or reduce a risk prohibited by subsection A.

5. The Commission shall publish its decision in the repository it provides.

C. In the manner prescribed in the Administrative Process Act (§ 9-6.14:1 et seq.), the Commission may issue orders and obtain injunctions or other civil relief to prevent or restrain a certification authority from violating this section, regardless of whether the certification authority is licensed. This section does not create a right of action in any person other than the Commission.

Article 3.

Duties of Certification Authority and Subscriber.

§ 59.1-478. Issuing a certificate.

A.1. A licensed certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

a. The certification authority has received a signed request for issuance of a certificate by the prospective subscriber.

b. The certification authority confirms that:

(1) The prospective subscriber is the person identified in the request and the person to be identified in the certificate to be issued;

(2) If the prospective subscriber is acting through an agent, the subscriber duly authorized the agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(3) The prospective subscriber bears a distinguished name; and

(4) The prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate.

c. The certification authority confirms that the prospective subscriber holds a key pair capable of:

(1) Affixing a digital signature by the private key corresponding to the public key to be listed in the certificate; and

(2) Verifying that a digital signature has been affixed by the corresponding private key through the use of the public key.

2. The requirements of this subsection may not be waived or disclaimed by the licensed certification authority or the subscriber.

B.1. If a certificate is requested by an agent or an apparent agent of the subscriber, the certification authority may not issue the certificate until after the certification authority has given ten days' written notice to the prospective subscriber through all of its record leaders at is record address.

2. The notice shall express the certification authority's intent to issue a certificate for the prospective subscriber to the requesting agent and the date on which the certificate is to be issued.

3. The requirement of notice in this subsection may be waived or disclaimed only by:

a. A writing signed by all of the record leaders of the prospective subscriber; and

b. Confirmation of the authenticity of the waiver by the certification authority.

C.1. If the subscriber accepts the certificate, the certification authority shall publish a signed copy of the certificate in the repository provided by the Commission or in one or more recognized repositories agreed upon by the certification authority and the subscriber named in the certificate.

2. The contract between the certification authority and the subscriber may provide that the certificate may not be published.

3. If the subscriber does not accept the certificate, a licensed certification authority may not publish the certificate in the repository provided by the Commission.

D. Nothing in this section precludes a licensed certification authority from conforming to standards, security policies, or contractual requirements more rigorous than, but consistent with, this section.

E.1. If a licensed certification authority confirms that a certificate was not issued as required by this section, the certification authority:

a. Shall immediately revoke the certificate; or

b. May suspend the certificate while investigating to confirm grounds for revocation.

2. The certification authority shall give notice as soon as practicable to the subscriber of a certificate revoked or suspended pursuant to this subsection.

F. The Commission may order the licensed certification authority to suspend or revoke a certificate which the certification authority issued if, after notice and an opportunity for the certification authority and subscriber to be heard in accordance with the provisions of the Administrative Process Act (§ 9-6.14:1 et seq.) the Commission determines that:

1. A certificate was issued without substantial compliance to this section; and

2. The noncompliance poses a significant hazard to parties relying on the certificate.

§ 59.1-479. Representations by the subscriber accepting a certificate.

A. By accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate certifies to all who justifiably rely on the information contained in the certificate that:

1. Each digital signature affixed by means of the private key corresponding to the public key listed in the certificate is a legally valid signature of the subscriber, unless the certificate:

a. Is suspended;

b. Is revoked by the certification authority; or

c. Has expired;

2. No unauthorized person has access to the private key corresponding to the public key listed in the certificate;

3. All representations made by the subscriber to the certification authority which are material to information contained in the certificate are true; and

4. The information contained in the certificate is true.

B. By requesting on behalf of a principal the issuance of a certificate naming the principal as subscriber, a person certifies to all who justifiably rely on the information contained in the certificate that:

1. The person holds all authority legally required for issuance of a certificate naming the principal as subscriber; and

2. The person has authority to sign digitally on behalf of the principal, and, if that authority is limited in any way, safeguards exist to prevent a digital signature exceeding the bounds of the person's authority.

C. A person may not disclaim or rebut the representations implied in this section or obtain indemnity for them, if the effect of the disclaimer or indemnity is to limit liability for wrongful issuance of a certification as against persons justifiably relying the certificate.

D.1. If a subscriber makes a false, material and written representation of fact, or fails to disclose a material fact, with either the intent to deceive the certification authority or a person relying on the certificate, or with negligence, the subscriber, by accepting a certificate, becomes obligated to indemnify the issuing certification authority for any loss or damage caused by the misrepresentation or negligence.

2. If the certification authority issued the certificate at the request of agents of the subscriber, both the agents and the subscriber shall indemnify the certification authority in accordance with this subsection.

3. The indemnity provided in this subsection may not be disclaimed or superseded by contract between the certification authority and the subscriber.

E. To obtain information required for issuance of a certificate, the certification authority may require a subscriber to testify under oath or an affirmation of truthfulness.

§ 59.1-480. Control of the private key.

A. By accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care in retaining control of the private key and keeping it confidential.

B. A private key is the property of the subscriber who rightfully holds it.

C.1. If a certification authority holds the private key corresponding to a public key listed in a certificate which it issued, it holds the private key as a fiduciary of the subscriber named in the certificate, regardless of any provision to the contrary in a contract between the subscriber and the certification authority.

2. A certification authority holding the subscriber's private key may use it only upon the prior written consent of the subscriber.

§ 59.1-481. Duties of a licensed certification authority in issuing a certificate.

A.1. By issuing a certificate, a licensed certification authority warrants to the subscriber named in the certificate that:

a. The certificate contains no information known to the certification authority to be false;

b. He certificate satisfies the requirements of this chapter and does not exceed any limitations of the certification authority's license; and

c. The certification authority has not exceeded any limitation of its license in issuing the certificate.

2. The warranties described in this subsection may not be limited or disclaimed by contract.

B. Unless the parties otherwise agree, a certification authority, by issuing a certificate, certifies to the subscriber that it will:

1. Notify the subscriber within a reasonable time of any facts known to the certification authority which affect the validity or reliability of the certificate once it is issued; and

2. Act promptly to suspend or revoke a certificate in accordance with § 59.1-482.

C. By issuing a certificate, a licensed certification authority certifies to all who justifiably rely on the information contained in the certificate that the certification authority has complied with all applicable requirements for issuance of the certificate.

D. By publishing a certificate, a licensed certification authority certifies to the repository and to all who justifiably rely on the information contained in the certificate that the certification authority has issued the certificate to the subscriber.

§ 59.1-482. Suspension of a certificate.

A.1. Unless the certification authority and the subscriber otherwise agree, the licensed certification authority which issued a certificate shall suspend the certificate for a period of forty-eight hours:

a. Upon request by a person identifying himself as:

(1) The subscriber named in the certificate;

(2) An agent of the subscriber;

(3) A business associate of the subscriber;

(4) An employee of the subscriber; or

(5) A member of the immediate family of the subscriber; or

b. Upon order of the Commission pursuant to subsection F of § 59.1-478.

2. The certification authority need not confirm the identity or Commission of the person requesting suspension.

B.1. Unless the certificate or other records in the repository indicate otherwise, the Commission or a clerk of a circuit court may suspend a certificate issued by a licensed certification authority for a period of forty-eight hours, if:

a. A person identifying himself as the subscriber named in the certificate, or as an agent, business associate, employee, or member of the immediate family of the subscriber requests suspension; and

b. The requester represents that the certification authority which issued the certificate is unavailable.

2. The Commission or circuit court clerk may:

a. Require the requester to provide evidence of his identity, authorization, and the unavailability of the issuing certification authority;

b. Inquire of the contents of the certificate and the secret field described in subsection D of § 59.1-470; and

c. Decline to suspend the certificate with or without cause.

3. The Commission or law-enforcement agencies may investigate multiple suspensions by the Commission or circuit court clerk for possible wrongdoing.

C.1. Immediately upon suspension of a certificate, the suspending certification authority, court clerk, or county clerk shall publish signed notice of the suspension in all repositories in which the certificate was published.

2, If the repositories described in subsection C 1 no longer exists, or if the person suspending the certificate does not know all the repositories in which the certificate was published, the certification authority shall publish the notice of suspension in the repository provided by the Commission.

D.1. A certification authority shall terminate the suspension of a certificate that was suspended by request if:

a. The subscriber named in the suspended certificate requests that the suspension be terminated and the certification authority confirms the identity of the person making the request, and, when the requester is acting as agent, the agent's authorization by the subscriber; or

b. The certification authority discovers and confirms that the request for the suspension was made without authorization by the subscriber.

2. This subsection does not obligate the certification authority to confirm a request for suspension.

E. The contract between a subscriber and a licensed certification authority may:

1. Limit or eliminate suspension by the certification authority upon request; or

2. Provide for termination of a suspension or disclosure of information about a suspension that varies from the requirements of this subsection and subsections A, B, and D, except that if the contract varies from the requirements of this section, the certificate must indicate the differences for the contractual variation to be valid.

F.1. No person may knowingly or intentionally misrepresent to a certification authority his identity, name, distinguished name, or authorization when requesting suspension of a certificate.

2. Violation of this subsection is a Class 3 misdemeanor.

G. The subscriber is released from the duty to keep the private key secure pursuant to § 59.1-480 during the period the certificate is suspended.

§ 59.1-483. Revocation of a certificate.

A.1. A licensed certification authority shall revoke a certificate which it issued after receiving and confirming a request for revocation by the subscriber named in the certificate in accordance with subdivision 2.

2. A licensed certification authority shall confirm a request for revocation and revoke a certificate within one business day after:

a. Receiving a subscriber's written request accompanied by evidence reasonably sufficient to confirm the request; and

b. Receiving any required fee.

B. A licensed certification authority shall revoke a certificate which it issued upon receiving a certified copy of the subscriber's death certificate or upon confirming by other evidence that the subscriber is dead.

C.1. A licensed certification authority may revoke one or more certificates which it issued if the certificates are or become unreliable regardless of whether the subscriber consents to the revocation.

2. Unless the contract between the certification authority and the subscriber provides otherwise, the certification authority shall pay reasonable restitution to the subscriber and compensate the subscriber for any interruption to the subscriber's business due to the revocation of the certificate under the circumstances described in subdivision D 1.

D.1. Immediately upon revocation of a certificate, the revoking certification authority shall publish signed notice of the revocation in all repositories in which the certification authority published the certificate.

2. If the repositories described in subdivision D 1 no longer exist, or if all are unrecognized repositories, the certification authority shall publish the notice in the repository provided by the Commission.

E. A subscriber ceases to certify as provided in § 59.1-479, and has no further duty to keep the private key secure as required by § 59.1-480 when either:

1. Notice of the revocation is published as required in subsection D; or

2. The certification authority is required to revoke under subsection A.

F. Upon publication as required by subsection C of § 59.1-482, a licensed certification authority is:

1. Discharged of its warranties based on issuance of the revoked certificate; and

2. Ceases to certify as provided in subsections B and C of § 59.1-481 in relation to the revoked certificate.

§ 59.1-484. Expiration of a certificate.

A.1. A certificate shall indicate the date on which it expires.

2. A certificate's expiration date may be no later than three years after its issuance.

B. When a certificate expires:

1. The subscriber and certification authority cease as provided in §§ 59.1-479 and 59.1-481; and

2. The certification authority is discharged of its duties based on issuance, in relation to the expired certificate.

§ 59.1-485. Liability of a licensed certification authority.

A. By specifying a recommended reliance limit in a certificate, the issuing certification authority and accepting subscriber recommend that persons rely on the certificate only in transactions in which the total amount at risk does not exceed the recommended reliance limit.

B. Except as designed in subsection E of § 59.1-471:

1. A licensed certification authority is not liable for any loss caused by a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with the requirements of this chapter;

2. A licensed certification authority is not liable for a misrepresentation in the certificate, or for error in issuing the certificate in excess of the amount specified in the certificate as the recommended reliance limit; and

3. A licensed certification authority is not liable for punitive or exemplary damages, except as

provided in § 59.1-474.

§ 59.1-486. Collection based on suitable guaranty.

A.1. Notwithstanding any provision in the suitable guaranty to the contrary;

a. If the suitable guaranty is a surety bond, a person may recover from the bond surety the full amount of a claim against the bond principal or, if there is more than one such claim during the term of the bond, a ratable share, up to a maximum total liability of the surety equal to the fact amount of the bond; or

b. If the suitable guaranty is a letter of credit, a person may recover from the issuing financial institution a claim against the customer named in the credit, or, if there is more than one claim during the term of the letter of credit, a ratable share, up to a maximum total liability of the issuer equal to the face amount of the credit.

2. Claimants may recover successively on the same suitable guaranty, provided that the total liability on the guaranty to all persons making claims during its term may not exceed the fact amount of the guaranty.

B. In addition to the actual damages suffered by the claimant, the claimant may recover from the proceeds of a suitable guaranty, until depleted, reasonable attorney fees, and court costs incurred by the claimant in collecting the claim.

C.1. A claim against a surety or issuer of a suitable guaranty must be filed in writing with the Commission and the surety or issuer, within one year after the claim arose.

2. A claim must include a statement of the amount claimed and the basis for the claim.

3. An action or suite against the surety or issuer of the suitable guaranty must be filed with the court within one year after the claim is filed with the Commission.

D. Except as prohibited by Commission rule, a suitable guaranty may, by contract, alter the obligations under this subsection.

Article 4.

Effect of a Digitized Signature.

§ 59.1-487. Presumptions established by a digital signature.

A. The presumptions established in this section, § 59.1-488, and § 59.1-489 do not apply to a certificate issued by an unlicensed certification authority.

B. A certificate is presumed to be an acknowledgment of any digital signature verified using the public key listed in the certificate, regardless of whether words of an express acknowledgment appear with the digital signature in any documents, or in relation to the message if:

1. The certificate is in the repository provided by the Commission or in a recognized repository; and

2. The certificate was not revoked, suspended, or expired at the time of signature.

C. A digital signature verified using a public key is presumed to have been affixed with the intention of the subscriber to authenticate the message and to be bound by the contents of the message if;

1. The public key is listed in a certificate that is in the repository provided by the Commission, or a recognized repository; and

2. The certificate was not revoked, suspended, or expired at the time of signature.

D.1. If a signature is time-stamped by the Commission or a recognized repository, and unless the message otherwise provides, the time-stamp is prima facie evidence that the time-stamped signature took effect as of the date and time indicated in the time-stamp.

2. This subsection does not preclude a finder of fact from concluding, based on other evidence, that the date and time of signature are other than as shown in a time-stamp of the Commission or a recognized repository.

E. The presumptions established in this section may be rebutted:

1. By evidence indicating that a digital signature cannot be verified by reference to a certificate issued by a licensed certification authority;

2. By evidence that the rightful holder of the private key by which the digital signature was affixed had lost exclusive control of the private key, without violating any duty imposed by this chapter, at the time when the digital signature was affixed;

3. By evidence showing a lack of a signature at common law; or

4. By a showing that reliance on the presumption was not commercially reasonable under the circumstances.

§ 59.1-488. Digitally signed document is written.

A. A digitally signed document is as valid as if it had been written on paper.

B. This section does not limit the authority of the State Tax Commission to prescribe the form of tax returns or other documents filed with the State Tax Commission.

§ 59.1-489. Digital signatures making instruments payable to bearer.

Notwithstanding any other provisions of this chapter, a digital signature which would make a negotiable instrument payable to bearer is void, unless the digital signature effectuates either a funds

transfer within the meaning of the Uniform Commercial Code or a transaction between banks or other financial institutions.

Article 5.

Division Services and Recognized Repositories.

§ 59.1-490. Commission duties; rulemaking; fees.

A.1. The Commission shall be a certification authority, and may issue, suspend, and revoke certificates in the manner prescribed for licensed certification authorities.

2. The provisions of Article 4 (§ 59.1-487 et seq.) apply to the Commission with respect to the certificates it issues.

B. The Commission shall provide for an on-line, publicly accessible database as a repository containing:

1. Certificates published in the repository by licensed certification authorities;

2. All orders and advisory statements designated for publication by the Commission;

3. Certification authority disclosure records for all currently or formerly licensed certification authorities;

4. Notices of suspended or revoked certificates published by licensed certification authorities;

5. References to recognized repositories;

6. Information required to be kept by a recognized repository; and

7. Other information as determined by Commission rule.

C. In conjunction with the repository it provides, the Commission shall make available a system for reliably time-stamping digital signatures.

D. The Commission may promulgate rules consistent with this chapter in order to:

1. Govern licensed certification authorities and their licensure;

2. Approve asymmetric cryptosystems for use in signing certificates issued by licensed certification authorities; and

3. Maintain the database required by § 59.1-473.

E. The Commission's rules shall address at least the following:

1. Design and implementation requirements limiting the equipment and software to fulfill the requirements of this chapter;

2. Validation that the hardware and software to be used are limited to those determined to meet the design and implementation requirements;

3. Suitability of algorithms for use in fulfilling the requirements of this chapter;

4. The form of suitable guarantees in accordance with § 59.1-469;

5. Items included in certificates issued by licensed certification authorities in accordance with subsection B of § 59.1-470;

6. Approval of persons authorized to audit licensed certification authorities under § 59.1-472;

7. The contents of a certification authority disclosure record required in § 59.1-473;

8. The termination of certification authority activities under § 59.1-476, including the form of notice and required statements; and

9. Prohibitions against altering obligations under subsection C of § 59.1-486.

F. The Commission may establish fees for the use of the repository provided for in subsection B, for licensing certification authorities, for publishing certificates and other records, and for its other activities required by this chapter.

§ 59.1-491. Recognition of repositories.

A. The Commission shall recognize a repository kept by a licensed certification authority, if the Commission concludes that:

1. The repository includes a database of certificates substantially similar in content and operation to the repository kept by the Commission;

2. The information in the repository appears to be true, accurate, and reasonably reliable;

3. The repository, its operator, and the certification authorities issuing the certificates in the repository conform to legally binding rules which the Commission finds to be substantially similar to, or more stringent toward the certificate authorities than those of Virginia;

4. The repository provides a time-stamping service which the Commission finds to be reasonably trustworthy;

5. The repository keeps an archive of suspended, revoked, or expired certificates; and

6. The repository has expressed in writing its intention to continue acting as a repository for the foreseeable future and is able to do so as indicated from its managerial and financial capabilities.

B. A repository may apply to the Commission for recognition by filing a written request and providing evidence to the Commission that the conditions for recognition are satisfied.

C. The Commission may withdraw or discontinue recognition of a repository in accordance with the provisions of the Administrative Process Act (§ 9-6.14:1 et seq.) if it concludes that the repository no longer satisfies the conditions for recognition listed in this section.

D. The Commission shall publish in its repository the names, addresses, and public keys of all recognized repositories.

§ 59.1-492. Liability of repositories limited.

A recognized repository, the Commission in providing for a repository, or the Commission's repository operator is not liable for any loss arising from:

1. Misrepresentation in a certificate published by a licensed certification authority;

2. Accurately recording or reporting information which a licensed certification authority, a county or court clerk, or the Commission has published as required by this chapter, including information about suspension or revocation of a certificate;

3. Reporting information about a certification authority, a certificate, or a subscriber, if the information is published as required by this chapter or by Commission rule, or is published by order of the Commission in the performance of its licensing and regulatory duties under this chapter; and

4. Failure to record publication of a certificate, suspension, or revocation, unless the repository has received notice of publication and a commercially reasonable time of not more than one business day has elapsed for processing of the publication.

§ 59.1-493. Exemptions.

The following official records of any public body are exempt from the provisions of the Virginia Freedom of Information Act (§ 2.1-340 et seq.):

1. Records containing information that would disclose, or might lead to the disclosure of private keys, asymmetric cryptosystems, or algorithms; or

2. Records, the disclosure of which might jeopardize the security of an issued certificate or a certificate to be issued.