FINAL BILL REPORT

ESB 5962

C 287 L 99

Synopsis as Enacted

Brief Description: Promoting electronic commerce through digital signatures.

Sponsors: Senators Brown, Horn and Finkbeiner; by request of Secretary of State and Governor Locke.

Senate Committee on Energy, Technology & Telecommunications
House Committee on Technology, Telecommunications & Energy

Background: On January 1, 1998, the Washington Electronic Authentication Act became effective. This law allows the use of digital signature technology in electronic transactions and creates a process for licensing certification authorities. The Office of the Secretary of State has responsibility for implementing and administering the Electronic Authentication Act.

Digital signature encryption systems are used to both protect the confidentiality of an electronic document and authenticate its source. These systems operate on the basis of two digital keys or codes created by the person desiring to send encrypted messages. One key is the private key, which is known only to the signer of the electronic message, and the other is the signer's public key, which is given to individuals with whom the sender wishes to exchange the confidential or authenticated message. The public key is used to verify both that the message was signed by the person holding the private key and that the message itself was not altered during its transmission.

The Governor and the Secretary of State are requesting this legislation, drafted by the Secretary of State and Department of Information Services (DIS), to clarify and simplify the Electronic Authentication Act, give greater flexibility to the secretary in administering the act, and allow DIS to become a licensed certification authority (CA) for the purpose of validating digital signatures between state agencies and citizens for official business.

Summary: Presumptions of validity and liability limitations do not apply unless all provisions of the Electronic Authentication Act are met.

The Secretary of State's authority to establish rules is broadened and clarified. The secretary may adopt rules to license CAs, recognize repositories, certify operative personnel, govern the practices of each, determine the form and amount suitable for guaranty, specify reasonable requirements for contents and form of certificates and certification practice statements, specify the procedure and manner by which laws of other jurisdictions may be recognized, and establish audit requirements and auditor qualifications. Provisions for recognizing repositories are modified to require record keeping, recognition and discontinuance of recognition in accordance with rules adopted by the secretary.

Provisions relating to obtaining or retaining a license are modified, including requiring a CA to provide proof of identity, allowing only certified operative personnel to be employed in appropriate positions and authorizing the secretary to create license classifications by rule and impose license restrictions specific to the practices of an individual CA.

The secretary may order penalties, but only a finding of noncompliance and order requiring compliance must be authorized against an agency acting as a CA. Penalties are enforceable in court.

Provisions authorizing the secretary to publish brief statements about activities of a CA that create risk are modified. A licensed CA must use only a trustworthy system and recognized repository for issuance, suspension, or revocation of a certificate. A CA may establish policies regarding the publication and suspension of certificates. If a CA does not establish a policy, it must satisfy certain conditions. A CA may suspend a certificate for a period not exceeding five business days as needed for an investigation.

A licensed CA may issue a certificate to a subscriber only after certain conditions are met. In confirming the identification of a prospective subscriber, a licensed CA must make a reasonable inquiry into the subscriber's identity and must be presumed to have confirmed the identity where the subscriber has appeared and presented a specified form of identification and a certified operative personnel or a notary has reviewed and accepted the identification.

If a signature of a unit of government is required by statute or rule, that unit of government must become a subscriber to a certificate issued by a licensed CA for purposes of conducting official public business with electronic records. No unit of state government, other than the Secretary of State and the Department of Information Services (DIS), must act as CA.

DIS is authorized to become a licensed CA. Before DIS may issue a certificate to a non-governmental entity, it must issue a request for proposals from licensed CAs and make a written determination that such services are not sufficient to meet the department's published requirements.

If DIS issues a certificate to a nongovernmental entity, the Office of Financial Management must convene a task force, which must include both governmental and nongovernmental representatives, to review the practice of the state issuing certificates to nongovernmental entities or individuals for the purpose of conducting official public business. The task force must prepare and submit its findings to the Legislature by December 31, 2001. The task force provision expires June 30, 2001.

Intent language and definitions are modified. Other clarifying and technical changes are made.

Votes on Final Passage:

Senate	38 8	
House	94 0	(House amended)
Senate	42 3	(Senate concurred)

Effective: May 13, 1999