FINAL BILL REPORT

ESB 6423

C 250 L 96
Synopsis as Enacted

Brief Description: Creating the Washington electronic authentication act.

Sponsors: Senators Sutherland, Finkbeiner and Sheldon; by request of Secretary of State.

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

Background: Digital encryption allows a person to protect a message so that only the intended recipients can read it, and to digitally sign it so that people can verify that it came from the sender. Many digital encryption systems exist or are in development.

Dual key encryption uses two digital codes, or "keys": a secret key and a public key. The user keeps the secret key confidential, and shares the public key to friends, business associates, and others to whom confidential messages are sent. Each key can read a message that has been encrypted by the other. If a person wants to digitally sign a message, he or she may use the secret key to create a signature. The recipient then uses the sender's public key to verify the source of the message.

Private companies provide or plan to provide encryption services either as part of their existing services or as a commercial enterprise. In addition, government agencies such as courts or tax offices will have increased need to protect security of electronic documents.

Unless the integrity of digital transmissions can be assured, on-line services cannot be used for such tasks as court filings, financial transactions, or sensitive personal or business correspondence. Digital signatures also raise several legal questions, such as their validity under the statute of frauds and the liability for damages for forgeries.

Summary: The Secretary of State is given authority to license and regulate certification authorities for digital signatures. The Secretary is directed to maintain a data base containing disclosure records for each licensed authority and to adopt rules to determine an amount appropriate for a suitable guaranty, set requirements for recordkeeping, and specify the form and contents of certificates, disclosure records and practice statements. The Secretary becomes a certification authority if none are licensed within six months of the effective date of the act. The Secretary is authorized to set fees for all services rendered in these efforts, and the fees are deposited in the state general fund.

Qualifications of certification authorities are listed. These entities must employ qualified personnel; file with the Secretary a suitable guaranty, with exceptions for public entities; have the right to a trustworthy computer system; present proof of working capital; and maintain an in-state office or have an in-state registered agent. Each licensed authority is required to be audited by a certified public accountant at least once per year with its level

of compliance published by the Secretary. Exemptions are allowed for small or less active authorities.

A certification authority may issue a certificate only if: it has received a request; the prospective subscriber is confirmed; the information in the certificate to be issued is accurate; the prospective subscriber rightfully holds the private key corresponding to the public key in the certificate and the private key is capable of creating a digital signature; and the public key can be used to verify the digital signature. If the certificate is accepted, it must be published in a recognized repository. A certification authority must immediately revoke certificates if not issued correctly and may suspend a certificate pending investigation. The Secretary may order a certification authority to suspend or revoke a certificate.

A certification authority warrants that an issued certificate is accurate and satisfactory, and promises to act promptly to suspend or revoke a certificate and give reasonable notice to the subscriber if reliability is in question.

A subscriber of a certificate certifies that the subscriber holds the private key and all representations are true. The subscriber indemnifies the certification authority for loss or damage if a published certificate relies on false representation or failure to disclose required information.

By accepting the certificate, the subscriber assumes the duty to retain control of the private key. The private key is the personal property of the subscriber; if held by a certification authority, it is held as a fiduciary of the subscriber and it may only be used with approval.

A certification authority must suspend a certificate up to 48 hours if requested by the subscriber, a person likely to know of a compromise of the subscriber's security, or the Secretary. The Secretary or a county clerk may suspend under similar conditions. Immediate notice of the suspension is required. Conditions of terminating a suspension are described.

A certification authority must revoke a certificate after receiving a request and confirming the validity of a subscriber, with confirmation and revocation required within one business day, or after confirming the death or dissolution of subscriber. Certificates may be revoked if they are unreliable. After meeting conditions, the subscriber and the certification authority are relieved of duties and warranties. A certificate must indicate an expiration date.

A reliance limit in a certificate is a recommended limit to persons other than the certificate authority and subscriber. A certification authority is not liable for losses due to fraud of the subscriber or in excess of the amount of the recommended reliance limit.

Details are specified for recovery of the amount of a qualified right to payment if the guaranty is a surety bond or letter of credit, including attorneys' fees and court costs. Filing written notice of claim is required, and must be done within three years of the occurrence of the violation.

When a lawful signature is required, a digital signature satisfies if the digital signature is verified by reference to the public key in a valid certificate, it is affixed by the signer with

intent to sign, and the recipient has no knowledge that the signer either breached a duty or does not rightfully hold the private key.

A recipient of a digital signature assumes the risk of forgery if reliance on the digital signature is not reasonable under the circumstances. If not relied upon, the recipient must notify the signer and the grounds for the determination that it is not reliable. The legislation does not obligate a person to accept a digital signature or to respond to an electronic message containing a digital signature.

A message is as valid as if on paper if it bears in its entirety a digital signature, and the digital signature is verified by the public key listed in a certificate. The certificate must be issued by a licensed certification authority and be valid at the time the digital signature is created.

In adjudicating disputes involving digital signatures, a court presumes a certificate signed by a certification authority is issued by the certification authority and accepted by the subscriber; the information listed is accurate; and if verified by the public key, the signature is the subscriber's and is affixed with the intent of signing the message; that the recipient assumed it is valid; and that the signature is created before it is time-stamped.

The Secretary must recognize one or more repositories after finding that it is operated under the direction of a licensed certification authority; includes a proper data base; operates by means of a trustworthy system; does not contain a significant amount of incorrect information; contains conforming certificates; keeps an archive of suspended or revoked certificates; and complies with other rules of the Secretary. A repository may apply for recognition by the Secretary and may file written notice of discontinuing.

A repository is liable for loss from a suspended or revoked certificate if the loss is incurred more than one business day after receipt of the request to publish notice of suspension or revocation and the repository failed to publish the notice. The repository is not liable for an amount in excess of the recommended reliance limit in the certificate.

The Secretary is given authority to adopt rules to implement the legislation beginning July 1, 1996.

Votes on Final Passage:

Senate	48	1	
House	94	0	(House amended)
Senate	43	1	(Senate concurred)

Effective: January 1, 1998