SENATE BILL REPORT

SB 5959

As of March 10, 1995

Title: An act relating to ensuring security of document transmissions using common carrier, broadcast, and computer technologies.

Brief Description: Attempting to minimize the incidence of forged digital signatures and foster the verification of digital signatures.

Sponsors: Senator Sutherland.

Brief History:

Committee Activity: Energy, Telecommunications & Utilities: 2/28/95.

SENATE COMMITTEE ON ENERGY, TELECOMMUNICATIONS & UTILITIES

Staff: David Danner (786-7784)

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 of Bill: Rules are established governing the creation of a key pair. The Department of Licensing (DOL) is directed to license "certification authorities," which are private companies, government agencies, and individuals who certify the integrity of a digitally signed document in a manner that can be readily verified. This provides a threshold level of assurance that a digital signature is legally valid.

Certification authorities must post surety bonds or letters of credit.

A certificate issued by a certification authority contains the following information: (1) the name of the subscriber; (2) the public key corresponding to a private key held by the subscriber; (3) a brief description of the algorithms with which the public key is intended to be used; (4) the serial number of the certificate; (5) the date and time on which the certificate is issued and accepted, and the date it expires; (6) the name of the certification authority; (7) the recommended reliance limit for transactions relying on the certificate; and (8) other information which DOL may require.

Certification authorities must be audited annually, and must disclose certain information for inclusion in a DOL database. DOL may investigate the activities of a certification authority for noncompliance, and revoke or suspend its license.

A certification authority may issue a certificate only after ascertaining critical facts about the subscriber's identity and the dual key numbers. When a certificate is requested by an agent or apparent agent of a subscriber, the certification authority may issue a certificate only after giving the subscriber 10 days' written notice.

A subscriber, by accepting a certificate, warrants that the information contained thereon is true, that the digital signature is valid, and that no unauthorized person has access to the private key.

It is the subscriber's duty to exercise reasonable care to keep the private key confidential. The private key is the property of the subscriber, and when the certification authority holds the private key, it acts as a fiduciary to the subscriber.

A licensed certification authority is not liable for any loss caused by a false or forged digital signature if it complies with all material requirements of the act. In addition, a certification authority is not liable for failure to comply for more than the amount specified in the certificate as the recommended reliance limit.

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

A digital signature is void if it makes a negotiable instrument payable to bearer, except when the signature effectuates a transfer between banks or financial institutions and other non-consumers.

The Department of Licensing must act as a certification authority, and may issue, suspend, or revoke certificates in the manner prescribed for licensed certification authorities. In addition, DOL must maintain an on-line database as a repository for: (1) certificates published in the repository by licensed certification authorities; (2) a list of all licensed certification authorities and their public keys; (3) a list of all certification authorities whose licenses are revoked or suspended, and the grounds for such actions; (4) certification authority disclosure records; (5) notices of suspended or revoked certificates; (6) references to recognized repositories; (7) information required to be kept by a recognized repository; and (8) other data as determined by DOL.

There is a rebuttable legal presumption that a certificate in a recognized repository is: (1) a valid acknowledgment of a digital signature verified using the public key set forth in the certificate, regardless of whether any words of express acknowledgment appear alongside the digital signature in any document, and (2) affixed with the subscriber’s intent to authenticate the message and to be bound by the contents of the message.

An exemption to the state Open Records Act is created for all records that disclose encryption codes or records jeopardizing the security of an issued certificate.

Appropriation: None.

Fiscal Note: Not requested.

Effective Date: Ninety days after adjournment of session in which bill is passed.