HOUSE BILL ANALYSIS

ENGROSSED SENATE BILL 5962

Title: An act relating to the promotion of electronic commerce through digital signatures.

Brief Description: Promoting electronic commerce through digital signatures.

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

HOUSE COMMITTEE ON
TECHNOLOGY, TELECOMMUNICATIONS & ENERGY

***Meeting Date*:** March 23, 1999.

***Bill Analysis Prepared by*:** Julia Harmatz, (786-7135)

***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 to authenticate its source or the signor of an authenticated document, such as a contract or payment system.

How Digital Signatures Work
Digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly intelligible forms and back again. Digital signatures use what is known as public key cryptography. This employs an algorithm using two different but mathematically related keys, one for creating a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively termed an asymmetric cryptosystem.

The complimentary keys of an asymmetric cryptosystem for digital signatures are arbitrarily termed the private key, known only to the signor and used to create the digital signature, and the ordinarily more widely known public key. The public key is used by a relying party to verify a digital signature. If many people need to verify the

signer's digital signatures, the public key must be available or distributed to all of them, perhaps by publication in an online repository or directory where it is easily accessible. Although the public and private keys are mathematically related if the asymmetric cryptosystem has been designed and implemented securely it is computationally infeasible (a relative concept based on the value of data protected, the computing overhead required to protect it, the length of time needed for protection, and the cost and time required to protect the data, with such factors assessed both currently and in the light of future technological advance) derive the private key from the knowledge of the public key. Thus, although many people may know the public key of a given signor and use it to verify that signor's signature, they cannot discover that signor's private key and use it to forge digital signatures. This is sometimes referred to the principle of irreversibility.

By Request of The Governor and the Secretary of State

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*:** This bill clarifies existing law to facilitate commerce and to ensure electronic signatures are not deprived from legal recognition solely because they are in electronic form. It further establishes procedures governing the use of digital signatures for official public business to provide reasonable assurances of the integrity, authenticity, and non repudiation of an electronic communication.

Digital Signatures are Original Signatures

A digitally signed message is deemed to be an original. As such, a verified digital signature by reference to the public key satisfies the contractual requirements for acknowledgment under law as well as acknowledgment for deeds and other real property conveyances.

Secretary of State

The Secretary of State may act as a certification authority. This bill broadens and clarifies the rules that the secretary may make with regard to implementation of the act. The secretary may adopt rules to license certification authorities (Authority–) as well as govern the practices of signature repositories and operative personnel. The secretary may also determine the amount suitable for a guaranty, specify reasonable requirements for the contents of certificates and certification practice statements, specify the procedure of recognition of other jurisdictions to ensure uniformity, and establish audit requirements.

This bill requires only certified operative personnel will be employed by the authority. Licensed authorities are subject to compliance audits.

This bill further modifies provisions that permits the secretary to publish brief statements about whether an unreasonable risk of loss exists for people who rely on the authority.

Penalties
The secretary may order penalties for non compliance up to $10,000 per incident, per day. If the authority is a state authority that is in noncompliance, the penalties will consist of an order to comply from the secretary.

***Appropriation*:** None.

***Fiscal Note*:** Requested on the engrossed bill.

***Effective Date of Bill*:** Contains an emergency clause and takes effect immediately.