HOUSE BILL REPORT
SB 5962

As Passed House:
April 15, 1999

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 and Finkbeiner; by request of Secretary of State and Governor Locke.

Brief History:
Committee Activity:
Technology, Telecommunications & Energy: 3/23/99, 3/31/99 [DPA].
Floor Activity:
Passed House: 4/15/99, 94-0.

Brief Summary of Engrossed Bill
(As Amended by House Committee)

- Ensures electronic signatures are not deprived from legal recognition solely because they are in electronic form.
- The Department of Information Services (DIS) is required to make a request for proposals prior to the issuance of certificates to nongovernmental persons or entities.

HOUSE COMMITTEE ON TECHNOLOGY, TELECOMMUNICATIONS & ENERGY

Majority Report: Do pass as amended. Signed by 14 members: Representatives Crouse, Republican Co-Chair; Poulsen, Democratic Co-Chair; DeBolt, Republican Vice Chair; Ruderman, Democratic Vice Chair; Bush; Cooper; Delvin; Kastama; McDonald; Mielke; Morris; Reardon; Thomas and Wolfe.

Staff: 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 Washington 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: (1) for creating a digital signature and (2) for 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 signer 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 signer and use it to verify that signer's signature, they cannot discover that signer'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 Washington 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 for purposes of official public business.

Summary of Amended Bill: 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 between and among state and local governmental, and private entities 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.

Department of Information Services (DIS)

The DIS must make a request for proposals prior to the issuance of certificates to nongovernmental persons or entities.

Penalties
If the state authority is in noncompliance, the penalties will consist of an order to comply from the secretary.

The DIS is now required to make a request for proposals prior to the issuance of certificates to nongovernmental persons or entities for the purpose of official public issuance. IF the DIS does issue certification to these nongovernmental entities, the

Office of Financial Management will convene a task force to review the practice to ensure the state is not unfairly competing against the private sector.

Appropriation: None.

Fiscal Note: Available.

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

Testimony For: This bill is really about economic development. Washington, Utah and Minnesota are the lead states with regard to Digital Signature laws. This bill enables electronic commerce and state business to be done via electronic transactions. The two concerns critics pose are: (1) The technological aspects of digital signatures; and (2) The state competing against the private industry. That is why a task force has been formed to study these issues and ensure the state is not competing. This enables the streamlining of government and making it work more efficiently. We want this government to stand side by side with Amazon.Com and Microsoft. The state eventually wants to out source the capacity to authenticate certificates, and this bill gives latitude to accomplish this. Authentication of digital signatures is very similar to the duties of a notary.

Testimony Against: Because the standards for a certification authority are lower than a notary, the bill should not move forward. The original version of the act is more appropriate because it places a larger burden on the authority to determine the authenticity of the subscriber than this bill. It is not appropriate for DIS to compete with the private sector. DIS may act as a certification authority for business between the state and other state entities, otherwise it would place a serious chill on this technology. This bill leaves a great deal to the rulemaking process, and it should articulate more of the specifics. If DIS does not comply with the requirements, they do not have the same risks as the private sector.

Testified: (In Support) Ralph Munro, Secretary of State; Chris Hedrick, Office of the Governor; and Steve Kolodney, Department of Information Services.

(Opposed) Thomas G. Melling, Washington State Bar Association; Donald Bundy, ID Certify, Inc.; and Janeane Dubuar, Computer Professionals for Social Responsibility.