HOUSE BILL REPORT
HB 1326

As Reported By House Committee On:
Commerce & Labor

Title: An act relating to electronic signatures.

Brief Description: Regulating electronic signatures.

Sponsors: Representatives McMorris, Conway, Boldt, Hatfield, Clements, Wood, Lisk, Cole, Wensman, Costa and Dunn; by request of Secretary of State.

Brief History:
Committee Activity:
Commerce & Labor: 2/6/97, 2/27/97 [DPS].

HOUSE COMMITTEE ON COMMERCE & LABOR

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives McMorris, Chairman; Honeyford, Vice Chairman; Conway, Ranking Minority Member; Wood, Assistant Ranking Minority Member; Boldt; Clements; Cole; Hatfield and Lisk.

Staff: Michael Spiro (786-5793).

Background: 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. A message encrypted by the private key is digitally signed– by the sender and the message then can be read only by the person using the corresponding public key. 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.

To ensure public keys really do belong to the people to whom they appear to belong, each public key is provided with a computer-based certificate of authenticity. These certificates are created by certification authorities,– which guarantee that the public keys they certify belong to the people possessing the corresponding private keys.

Further, a chain of certification authorities can be created to provide even greater assurance as to the identity of the holder of the private key. Protections were needed, however, to ensure the reliability of both the certificates and the certificating authorities. Thus, the Washington Electronic Authentication Act was enacted in 1996 to provide rules with respect to the authentication and reliability of digital signature encryption systems, the issuance, suspension, and revocation of certificates, and the licensing of certification authorities. This law will take effect on January 1, 1998.

Duties of the secretary of state: If no certification authority is licensed in the state, then the secretary of state may issue, suspend, and revoke certificates as a licensed certification authority. Once another certification authority becomes licensed in the state, the secretary of state may no longer act as a certification authority.

The Department of Information Services: The Washington Electronic Authorization Act does not authorize the Department of Information Services to become a licensed certification authority.

State and local government units as subscribers and certification authorities: The Washington Electronic Authentication Act does not specifically authorize state or local government units to become subscribers or licensed certification authorities.

Licensing of certification authorities: There is no limitation on the duration of a license issued to a certification authority.

Audit Requirements: The Secretary of state may exempt a licensed certification authority from audit requirements.

Discontinuance of licensed certification authorities: There are no specific actions that licensed certification authorities are required to take when they discontinue providing certification authority services.

Recommended reliance limits and penalties: By specifying a recommended reliance limit in a certificate, both the issuing certification authority and accepting subscriber recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.

A licensed certification authority is not liable for any loss in excess of the certificate's recommended reliance limit that results from (1) the certification authority's failure to comply with the rules for issuing certificates; or (2) a misrepresentation in the certificate of a fact that the certification authority is required to confirm. Further, a licensed certification authority is liable only for direct compensatory damages in an action to recover a loss due to reliance on the certificate.

A repository is liable only for direct compensatory damages in an action to recover a loss due to reliance on a certificate.

The secretary of state may impose a maximum civil monetary penalty of five thousand dollars or ninety percent of the recommended reliance limit of a certificate, whichever is less, for a violation of the Washington Electronic Authentication Act.

Revocation and suspension of certificates: A certificate issued by a licensed certification authority need not contain any information with respect to the location or identity of a repository in which notification of the certificate's revocation or suspension will be listed if the certificate is suspended or revoked.

The secretary of state may revoke or suspend a certification authority's license for failure to comply with the Washington Electronic Authentication Act.

In an emergency resulting from a licensed certification authority's noncompliance with the rules for issuing certificates, the secretary of state may suspend a certificate for a period not to exceed forty-eight hours. The secretary of state also may suspend a certificate for a period of forty-eight hours upon request.

A licensed certification authority upon request or by order of the secretary of state must suspend a certificate for a period not to exceed forty-eight hours.

The county clerk may suspend certificates by a licensed certification authority.

A person who knowingly or intentionally misrepresents to a certification authority his or her identity or authorization in requesting a suspension of a certificate is guilty of a misdemeanor.

Control of private keys: By accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to a person not authorized to create the subscriber's digital signature. However, there is no statutory provision concerning the duty of the subscriber if the certificate expires or is revoked. Further, the subscriber has no duty to keep the private key secure while a certificate is suspended.

The Washington Electronic Authentication Act does not exempt a private key in the possession of a state or local agency from public inspection and copying under Washington's public record disclosure laws.

Satisfaction of signature requirements: Where a signature is required by law, that rule is satisfied by a digital signature if, among other requirements, no party affected by a digital signature objects to the use of digital signatures in lieu of a signature.

No person is obligated to accept a digital signature or to respond to an electronic message containing a digital signature, nor is any person required to honor, accept, or act upon a court order, writ, or warrant if it is electronic in form and signed with a digital signature, including digital signatures that are certified by a licensed certification authority or otherwise issued under court rule.

Factors used in evaluating reasonable reliance upon a certificate: No specific factors must be considered in evaluating the reasonableness of a recipient's reliance upon a certificate and its digital signatures.

Summary of Substitute Bill: A variety of changes are made to the Washington Electronic Authentication Act.

Duties of the secretary of state: The secretary of state is not authorized to act as a certification authority.

The Department of Information Services: The Department of Information Services may become a licensed certification authority for the purpose of providing services to state and local government. The department may only issue certificates when the subscriber is (1) the state of Washington or a department, office, or agency of the state; (2) a city, county, district, or other municipal corporation, or a department, office, or agency of the city, county, district, or municipal corporation; (3) an agent or employee of an entity described in (1) or (2) for purposes of official public business; or (4) an applicant for a license as a certification authority.

State and local government units as subscribers and certification authorities: A state and local government unit, including its appropriate officers or employees, may become a subscriber for the purposes of conducting official business. The only state government units that may act as certification authorities are the secretary of state and the Department of Information Services. A city or county, however, may become a licensed certification authority for the purpose of providing services to local government, but only if authorized by local ordinance.

Licensing of certificated authorities: Licenses expire one year after they are issued, except that the secretary of state may provide by rule for a longer duration.

Audit requirements: The secretary of state no longer may exempt a licensed certification authority from audit requirements.

Discontinuance of licensed certification authorities: A licensed certification authority that no longer provides certification authority services must (1) notify all subscribers listed in valid certificates issued by the licensed certification authority; (2) minimize disruption, to the extent commercially reasonable, to subscribers of the valid

certificates and parties relying on those certificates; and (3) make reasonable arrangements for the preservation of the licensed certification authority's records.

Recommended reliance limits and penalties: By specifying a recommended reliance limit in a certificate, only the issuing certification authority only, and not the subscriber, recommends that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.

A licensed certification authority is no longer liable only for direct compensatory damages in an action to recover a loss due to reliance on a certificate it has issued; the licensed certification authority is also liable for damages for lost profits or opportunity. In addition, a licensed certification authority is liable for breach of any of the warranties it gives or for lack of good faith. A licensed certification authority, however, by agreement may liquidate, limit, alter, or exclude consequential or incidental damages, unless the limitation, alteration, or exclusion is unconscionable.

A repository is no longer liable only for direct compensatory damages in an action to recover a loss due to reliance on a certificate. In addition, a repository is liable for damages for lost profits or opportunity, and by agreement may liquidate, limit, alter, or exclude consequential or incidental damages, unless the limitation, alteration, or exclusion is unconscionable.

The secretary of state may impose a maximum civil monetary penalty of $10,000 or 90 percent of the recommended reliance limit of a certificate, whichever is less, for a violation of the Washington Electronic Authentication Act.

Revocation and suspension of certificates. A certificate issued by a licensed certification authority must provide information sufficient to locate or identify one or more repositories in which notification of the certificate's revocation or suspension will be listed if the certificate is suspended or revoked.

In addition to having the authority to suspend or revoke a certificate for noncompliance, the secretary of state may suspend a license pending revocation proceedings or other actions. The secretary of state must find that the certification authority has used its license to violate a state or federal criminal statute or Washington's consumer protection act or has engaged in conduct giving rise to a serious risk of loss to public or private parties if the license is not immediately suspended.

The maximum length of time for which a certificate may be suspended by the secretary of state in an emergency or upon request is 96 hours.

The maximum period of time for which a certificate may be suspended by a licensed certification authority is 96 hours.

The county clerk may no longer suspend certificates by a licensed certification authority.

A person who knowingly or intentionally misrepresents to a certification authority his or her identity or authorization in requesting suspension of a certificate is guilty of a gross misdemeanor.

Control of private keys. The subscriber identified in a certificate issued by a licensed certification authority has no duty to exercise reasonable care to retain control of the private key and prevent its disclosure to a person not authorized to create the subscriber's digital signature if the certificate expires or is revoked.

A private key in the possession of a state or local agency is exempt from the public inspection and copying requirements in Washington's public record disclosure laws.

Satisfaction of signature requirements. Where a signature is required by law, the absence of any objection to the use of digital signatures in lieu of a signature is no longer required.

No person is obligated to accept a digital signature or to respond to an electronic message containing a digital signature, except that a person may not refuse to honor, accept, or act upon a court order, writ, or warrant upon the basis that it is electronic in form and signed with a digital signature, if the digital signature was certified by a licensed certification authority or otherwise issued under court rule. In addition, the recipient of a digital signature or an electronic message containing a digital signature may establish the conditions under which the recipient will accept a digital signature.

Factors used in evaluating reasonable reliance upon a certificate. The following factors are significant in evaluating the reasonableness of a recipient's reliance upon a certificate and the digital signatures it lists (1) facts which the relying party knows or of which the relying party has notice; (2) the value or importance of the digitally signed message, if known; (3) the course of dealing between the person and subscriber; and (4) usage of trade, particulary trade conducted by trustworthy systems or other computer-based means.

Substitute Bill Compared to Original Bill: The secretary of state's authority to act as a certification authority is removed, and the authority to issue certificates in which the subscriber is an applicant for a license as a certification authority is transferred from the secretary of state to the Department of Information Services. In addition, the maximum penalty that the secretary of state may impose for a violation of the Washington Electronic Authentication Act is changed to $10,000, or 90 percent of the recommended reliance limit of a certificate, whichever is less. The original bill required the secretary of state to choose the greater of the two.

The substitute bill makes a number of clarifications to the original bill. The liability of a licensed certification authority or a repository for damages in an action to recover a loss due to reliance on a certificate is clarified and made to conform with existing law. A private key holder's duty to exercise reasonable care to retain control of the private key is also reaffirmed. The substitute bill further clarifies that a recipient of a digital signature or an electronic message containing a digital signature is obligated to rely on, or respond to that digital signature or electronic message only with respect to court orders, writs, or warrants.

Appropriation: None.

Fiscal Note: Not requested.

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

Testimony For: Washington's digital signature law is the most comprehensive and far-reaching in the United States. Care has been taken to insure the language in this bill prohibits inappropriate uses of digital signatures, and overall it is an excellent construction from which to go forward. Ultimately, however, there needs to be uniform rules concerning this area of law. In addition, there are some remaining areas of concern, including: the liability of certification authorities, the differences between licensed and unlicensed certification authorities, voluntary reliance on digital signatures, and whether reliance on unlicensed certification authorities by parties in commercial transactions will ever be appropriate.

Testimony Against: None.

Testified: Linda McIntosh, Office of the secretary of state; Glenn Anderson, Commercial Information Systems; Mike Rodin, Washington Bar Association; and Jerry Whitting, Azeala Software.