HOUSE BILL REPORT
ESB 6423

As Reported By House Committee On:
Energy & Utilities

Title: An act relating to electronic signatures.

Brief Description: Creating the Washington electronic authentication act.

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

Brief History:
Committee Activity:
Energy & Utilities: 2/20/96, 2/21/96 [DPA].

HOUSE COMMITTEE ON ENERGY & UTILITIES

Majority Report: Do pass as amended. Signed by 9 members: Representatives Casada, Chairman; Crouse, Vice Chairman; Hankins, Vice Chairman; Patterson, Ranking Minority Member; Poulsen, Assistant Ranking Minority Member; Chandler; Kessler; Mastin and Mitchell.

Staff: Karen Tyler (786-5793).

Background: An increasing amount of commerce, particularly international commerce, is transacted electronically. For example, it is possible to use on-line services to conduct financial transactions and to transmit other personal or business correspondence. To make the maximum possible use of the electronic medium in business transactions, however, participants require a means by which to transmit documents confidentially, and, perhaps more importantly, to transmit authenticated documents bearing legally binding original signatures. The ability to transmit electronic messages carrying legally binding signatures would allow businesses to conduct transactions and to enter into binding contracts entirely by electronic means.

A digital encryption system allows a person to 1) protect an electronic message so that only its intended recipients can read it, and 2) authenticate or "sign" the message so that recipients can verify its source. There are several types of digital encryption systems, of which the dual key encryption system is one.

Each person using a dual key encryption system has two digital codes or "keys," a secret key and a public key. The user keeps the secret key confidential, and shares the public key with persons with whom he or she wishes to exchange confidential and/or authenticated electronic messages. Each key can read a message encoded by the other and is the only means by which to read a message encoded by the other.

System users can send confidential electronic messages. Anyone can use a public key to encode a message to that key's owner; the key owner can then use his or her corresponding secret key to read that message. No one but the owner of the public key, the intended recipient of the message, can decode the message, because no one else has access to the secret key.

Users can also authenticate, or "sign," electronic messages. The sender can use his or her secret key to encode, and thereby digitally "sign," a message, and the recipient can verify the electronic signature by using the sender's public key to decode it. Decoding the message with the sender's public key proves that the sender was the true originator of the message, and that no one else has altered it, because the sender alone possesses the secret key that made the signature.

Public keys are kept and made available to the public in computer files called "key certificates" that generally include the key owner's identity, a timestamp indicating when the key pair was generated, and the public key code. "Certification authorities" may be employed to create these certificates and guarantee that they are authentic. Certification authorities can play an important part in a dual key system in guaranteeing that the public keys they make available really belong to the persons to whom they appear to belong. If there is no mechanism by which to ensure that a public key actually belongs to its purported owner, dishonest persons may create "imposter" key pairs, making possible both forgery and interception of confidential communications.

A number of private companies provide or plan to provide encryption services.

Summary of Amended Bill:

Authorities of the Secretary of State

The Secretary of State (secretary) is authorized to license certification authorities, and, if no certification authority is licensed within 6 months of enactment, to serve as a certification authority until another authority is licensed. The secretary is directed to adopt rules a) to govern the practice of licensed certification authorities; b) to determine the value of the surety bond or irrevocable letter of credit which a licensed authority must file with the secretary guaranteeing payment of any damages awarded against it for violation of the statute; c) to review software used in creating digital signatures; d) to specify requirements for the form of certificates issued by licensed

certification authorities; e) to specify requirements for record-keeping by licensed certification authorities; f) to specify requirements for the content and form of certification authority disclosure records; and g) to specify the form of certification practice statements. In addition, the secretary must maintain a publicly accessible data base containing disclosure records for each licensed certification authority setting forth information as the secretary may require by rule.

The secretary is authorized to set fees for all services rendered under the statute, and fee revenues are deposited in the state general fund. The secretary is authorized to adopt rules to implement the act beginning July 1, 1996.

Licensing of Certification Authorities

To qualify for a license, a certification authority must employ qualified persons who have not been convicted within the past 15 years of felonies or crimes involving fraud, false statement, or deception; have the right to use a computer system that is reasonably secure from intrusion and misuse, reasonably reliable, and suited to its intended functions; present proof of sufficient working capital; maintain an office in the state or a registered in-state agent for service of process; file surety bonds or irrevocable letters of credit with the secretary, in an amount the secretary is directed to determine by rule, for payment of damages awarded against the certification authority for violation of the statute (public entities are excepted from this requirement under some circumstances); and comply with all further licensing requirements the secretary may establish. The secretary may issue restricted licenses.

The secretary may recognize the authority of other government entities to license or authorize certification authorities, provided that they impose requirements similar to those of the state.

Issuance of a Certificate

"Certificates" are computer-based records digitally signed by the issuing authority, and containing three pieces of information: 1) the identity of the issuing certification authority; 2) the identity of the subscriber (key holder); and 3) the subscriber's public key. The "subscriber" holds the private key corresponding to the public key listed in the certificate.

A licensed certification authority may issue a certificate to a subscriber only if it has received a signed request for a certificate and has confirmed the identity of the prospective subscriber, the accuracy of information to be listed in the certificate, that the prospective subscriber holds a private key capable of creating a digital signature, and that the prospective key holder has not obtained the private key corresponding to the public key to be listed in the certificate by illegal means, or disclosed it to persons who are not authorized to create the prospective key holder's digital signature. The

authority must publish a signed copy of each certificate it issues in a "recognized repository" unless the parties provide otherwise by contract. A "repository" is a system for storing and retrieving certificates and other information relevant to digital signatures. The secretary must "recognize" repositories that meet specified standards (see below).

In issuing a certificate, a licensed authority warrants to the key holder (the subscriber) that the certificate contains no information known to be false and satisfies the requirements of the law, and promises to act promptly to suspend or revoke the certificate and give the subscriber reasonable notice if its reliability comes into question. The licensed authority certifies to all persons who reasonably rely on the information contained in a certificate that it is accurate and states all information foreseeably material to its reliability, that the subscriber has accepted it, and that the authority has complied with all applicable laws of the state.

Upon request, a licensed certification authority must disclose information material to the reliability of any certificate or to its ability to perform its services.

Duties of Subscriber

In accepting a certificate from a licensed authority, the subscriber certifies that 1) he or she holds the private key corresponding to the public key listed in the certificate and has not obtained it through unlawful means or disclosed it to persons who are not authorized to create his or her digital signature; and 2) that all representations he or she has made to the authority material to information listed in the certificate are true. In accepting a certificate, the subscriber indemnifies the issuing authority for loss or damage caused by issuance or publication of a certificate in reliance on the subscriber's false representations or failure to disclose important facts with the intent to deceive or with negligence.

The subscriber assumes a duty to retain control of the private key. The private key is the personal property of the subscriber; if the certification authority holds the private key, it holds it as a fiduciary to the subscriber and may use it only with the subscriber's approval.

Suspension or Revocation of a Certificate

A licensed certification authority must immediately revoke a certificate upon discovery that it was not issued as required by the statute. The secretary may order a licensed authority to suspend or revoke a certificate if it determines that the certificate was issued without substantial compliance with the statute and noncompliance poses significant risk to persons relying on the certificate.

Unless the certification authority and subscriber agree otherwise, a licensed certification authority must suspend a certificate for up to 48 hours upon request of the secretary, the subscriber, or a person likely to know that the security of the subscriber's private key is compromised. Under specified circumstances, the secretary or a county clerk may suspend a certificate issued by a licensed authority. Licensed authorities must publish notice of a certificate's suspension as specified in the certificate.

A licensed certification authority must revoke a certificate upon request of the subscriber, once the subscriber no longer exists, and if the certificate becomes unreliable. Immediately upon revocation of a certificate, the licensed authority must publish notice in a recognized repository (see below). Once a certificate is revoked, and once they have met specified conditions, the subscriber and certification authority are relieved of duties and warranties.

Each certificate must state its expiration date.

Liability for Damages Due to Reliance on a Certificate

A licensed certification authority must file surety bonds or irrevocable letters of credit with the secretary, in an amount the secretary is directed to specify by rule, to guarantee payment of damages assessed against the authority for violation of the statute. This guarantee may restrict the authority's total annual liability to the face amount of the guarantee.

Requirements are established for recovery on a surety bond or letter of credit. Claimants must file written notice within three years of a violation.

The certification authority and the subscriber may set a "reliance limit" on a certificate, suggesting that third parties rely on the certificate only to the extent that total risk does not exceed the recommended limit. A licensed certification authority is not liable for loss caused by reliance on false or forged digital signatures of a subscriber if the authority has complied with all requirements of the law, and is not liable in excess of the amount specified in the certificate as its recommended reliance limit either for loss caused by reliance on a misrepresentation of fact in the certificate that the authority was required to confirm or for failure to comply with statutory requirements in issuing the certificate. A licensed certification authority is liable only for direct compensatory damages in an action to recover loss due to reliance on a certificate, and is not liable for punitive or exemplary damages, damages for lost profits or opportunities, or for damages due to pain and suffering.

A recipient of a digital signature assumes the risk of forgery if reliance on the digital signature is not reasonable under the circumstances.

Effect of a Digital Signature

When a lawful signature is required, a digital signature will suffice if the digital signature is verified by reference to the public key in a valid certificate issued by a licensed certification authority and was affixed by the signer with the intent to sign, and the recipient has no knowledge that the signer has improperly disclosed the private key used to affix the signature or obtained it illegally.

An electronic message is as valid, enforceable and effective as if it had been written on paper 1) if it bears a digital signature; and 2) if that signature is verified by the public key listed in a certificate that was issued by a licensed certification authority and valid at the time the signature was created. A digital message is not a negotiable instrument under the Uniform Commercial Code unless this is agreeable to all parties to a transaction.

Courts are required to make certain presumptions in adjudicating disputes involving digital signatures. A court must presume that a certificate signed by a licensed certification authority was issued by that authority, accepted by the subscriber, and contains accurate information. If a digital signature is verified by a public key listed in a valid certificate issued by a licensed certification authority, a court must presume that the signature is that of the certificate subscriber and affixed with the intention of signing the message, that the message recipient assumed it was valid, and that the signature was created before it was timestamped.

Repositories

A repository is a system for storing and retrieving certificates and other information relevant to digital signatures. Licensed certification authorities must publish copies of certificates they issue in "recognized repositories," unless the parties provide otherwise by contract.

The secretary is required to recognize one or more repositories that 1) are operated under the direction of a licensed certification authority; 2) include a proper data base; 3) operate by means of a trustworthy system; 4) do not contain a significant amount of false information; 5) contain certificates published by certification authorities that conform to legally binding requirements that the secretary finds similar or more stringent than those of the state; 6) keep an archive of certificates that are suspended or revoked, or that have expired; and 7) comply with other requirements the secretary may adopt. A repository may apply for recognition by the secretary.

A repository is liable for loss incurred due to reliance on a digital signature verified by the public key listed in a suspended or revoked certificate, if the loss was incurred more than one business day after the repository received a request to publish notice of suspension or revocation of the certificate and failed to do so. A recognized

repository is liable only for direct compensatory damages not to include punitive or exemplary damages, damages for lost profits or opportunity, or damages for pain and suffering, and is not liable for misrepresentation in a certificate published by a licensed certification authority, for reporting or recording information as required or permitted under the statute, or for an amount in excess of the recommended reliance limit set for the certificate at issue.

Oversight and Discipline of Certification Authorities

The secretary may investigate activities of a licensed certification authority material to its compliance with the statute, may suspend or revoke licenses, and may impose fines for violations not to exceed $5,000 per incident. The secretary may publish in the repository it maintains or elsewhere brief statements advising subscribers, persons relying on digital signatures, or other repositories about activities of licensed or unlicensed certification authorities that create an unreasonable risk of loss. A process is defined by which a named authority may contest these reports.

A certified public accountant with expertise in computer security or an accredited computer security professional must audit the operations of each licensed certification authority at least once per year to assess compliance with the statute. The secretary must publish the results of these audits in the certification authority disclosure records it maintains for all licensed authorities. The secretary may exempt small or less active certification authorities from audit requirements under certain circumstances.

Amended Bill Compared to Engrossed Bill: Technical amendments make the act more consistent with current banking law; clarify that the act applies only to those certification authorities that choose to become licensed by the state, and that use of digital signatures is voluntary; and make other clarifications. Digital signatures will not serve as negotiable instruments under the Uniform Commercial Code unless this is agreeable to all parties to a transaction. The secretary is authorized to adopt rules to implement the act beginning July 1, 1996.

Appropriation: None.

Fiscal Note: Available.

Effective Date of Amended Bill: The bill takes effect on January 1, 1998.

Testimony For: Various digital encryption technologies exist, but a legal framework within which to use these tools is needed. Electronic commerce will gain widespread acceptance and use only once businesses feel confident that electronic communications are secure, valid, and protected from fraud. State government leadership is imperative in setting forth guidelines for a system that will impart this confidence. Enactment of the bill will enhance Washington's position in international commerce.

Bill sponsors are pleased with the support they have received from the private sector. Washington can learn from mistakes other states have made in developing and implementing similar legislation.

The bill should be amended to update the definition of a financial institution; make certain provisions consistent with current banking law; and clarify that use of digital signatures is voluntary, that parties certifying signatures through unlicensed private systems aren't subject to requirements of the bill, and that digital messages aren't negotiable instruments under the UCC unless this is agreeable to all parties to the transaction.

In considering this bill, the Legislature should proceed with caution, should not attempt to "legislate progress," should remain responsive to private sector concerns, and should not impose requirements that interfere with banking procedures. Statutes in this area should allow room for evolution of the technology. The system should include security measures sufficient to ensure public trust, but not so excessive as to increase costs beyond what customers will pay.

Testimony Against: None.

Testified: Senator Sutherland, prime sponsor; Representative Barney Beeksma (with concerns); Ralph Munro, Secretary of State; Meara Nisbet, Washington Bankers' Association; Deborah Brunton, Microsoft; Linda MacIntosh, Office of Secretary of State; and Jerry Whiting, Azalea Software, Inc.