FINAL BILL REPORT
SHB 1632

C 39 L 01
Synopsis as Enacted

Brief Description: Prescribing criminal penalties for fraudulently obtaining or using digital signatures and digital certificates.

Sponsors: By House Committee on Technology, Telecommunications & Energy (originally sponsored by Representatives Ruderman, Anderson, Schual-Berke and Casada; by request of Department of Information Services).

House Committee on Technology, Telecommunications & Energy
Senate Committee on Economic Development & Telecommunications

Background:

Digital signature encryption systems are used to both protect the confidentiality of an electronic document and to authenticate its source or signer.

These systems operate on the basis of two digital keys,– or codes, created by the person desiring to send an encrypted message or document. One key is the private– key, which is known only to the signer of the electronic message or document, and the other is the signer's public– key, which is provided to the individuals with whom the sender wishes to exchange the confidential or authenticated message. A message or document encrypted by the private key is digitally signed by the sender and the message can be read only by those 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 authenticity in the use of digital signatures, each public key is registered with a certification authority and is part of a digital signature certificate issued by the authority. The certificate is a computer-based record that identifies the certification authority that issues it, names or identifies the subscriber (holder of the private key), and contains the public key. This certificate is used to verify that the public key belongs to the person possessing the corresponding private key. In this way, the identity of the signer of a document is verified. Digital certificates can be used much like a driver's license or a passport as electronic identification.

A person forges a digital signature when he or she creates a digital signature without authorization of the holder of the private key or uses a digital signature where the subscriber in the digital certificate is a person that does not exist or that does not hold the private key that corresponds to the public key in the certificate.

Summary:

A criminal violation is established for fraudulent actions in applying for digital certificates and using digital signatures.

It is unlawful for a person to knowingly misrepresent his or her identity or authorization when obtaining a digital certificate. It is also unlawful to knowingly forge a digital signature or use the signature of another person. A violation of these provisions is a class C felony that carries a penalty of up to five years in prison or a fine of up to $10,000, or both.

Votes on Final Passage:

House 94 1
Senate 48 0

Effective: July 22, 2001