SENATE BILL REPORT
SHB 1632

As Reported By Senate Committee On:
Economic Development & Telecommunications, March 26, 2001

Title: An act relating to fraudulently obtaining or using digital signatures and digital certificates.

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).

Brief History:
Committee Activity: Economic Development & Telecommunications: 3/20/01, 3/26/01 [DP].

SENATE COMMITTEE ON ECONOMIC DEVELOPMENT & TELECOMMUNICATIONS

Majority Report: Do pass.
Signed by Senators T. Sheldon, Chair; B. Sheldon, Vice Chair; Fairley, Finkbeiner, Haugen, McCaslin, Rossi and Stevens.

Staff: William Bridges (786-7424)

Background: In 1996, the Legislature passed the Washington Electronic Authentication Act to provide a secure and convenient way for people to send a "signed" document electronically without having to follow up with a hand-signed paper copy. These electronic signatures are called "digital signatures."

"Digital signatures" use two digital codes or "keys," a private key and a public key. The user keeps the private key confidential, and shares the public key to business associates and others to whom confidential messages are sent. A message or document encrypted by the private key is digitally signed by the sender and the message then 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. A digital signature certificate is like a driver's license--a unique piece of identification containing state registration numbers--that certifies the identity of the person who creates and sends an electronic document, payment or other data.

Summary of Bill: Three crimes are created for fraudulently obtaining or using digital signatures or certificates:

- It is unlawful for a person to knowingly apply for a digital signature certificate in someone else's name.

- It is unlawful for a person to knowingly forge a digital signature.

- It is unlawful for a person to knowingly use another person's digital signature certificate as identification to gain access to or engage in a transaction for which the person is not authorized.

A violation of these provisions is a class C felony that carries a penalty of up to five years in prison or a fine up to $10,000, or both.

Appropriation: None.

Fiscal Note: Available. New fiscal note requested on March 23, 2001.

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

Testimony For: The bill updates the law on paper forgery to include electronic forgery. The bill is supported by the Governor's Internet Council.

Testimony Against: None.

Testified: Representative Laura Ruderman, prime sponsor (pro); Carrie Tellefson, DIS (pro); Steve Kolodney, DIS (pro).