
THE WASHINGTON DIGITAL SIGNATURES ACT (1998) Update Bulletin

On January 1, 1998, the Washington Electronic Authentication Act aka The Washington Digital Signature Act, RCW 19.34 (the "Act") became effective. The Act was designed to help make transactions safer over the internet by providing a uniform system for use of digital signatures. The use of digital signatures can help to electronically ensure that a message is authentic (that is, not forged), that it has not been altered, and that the sender cannot repudiate the message after it is sent.

1. Digital Signatures.

A digital signature is not a regular handwritten signature or even a scanned or digitized signature. A digital signature consists of a message digest that is generated unique for the message using a mathematical algorithm. The "message digest" is then encrypted with the sender's "private key" and attached to the message. The message digest may then only be decoded using a "public key" that is mathematically related to the sender's private key. If the public key decrypts the message, then the recipient knows the sender (or at least the sender's private key) "signed" the contract and that the message was not modified since it was signed. The sender keeps the private key confidential but distributes the public key, as needed. The private key and public key paired together constitute a "signature."

2. The Act.

The Act treats a digital signature as the equivalent of a manual signature and of a "writing." It also creates a presumption of authenticity that, unless rebutted, precludes the owner of the private key from repudiating the message or claiming that it was altered.

3. Certification Authority.

The private-public key system only works properly if a third party also verifies the identity of the sender and certifies that the public key used corresponds to the private key of the subscriber. This third party, called a certification authority, issues a certificate verifying the transaction. These certificates may only be issued by State of Washington licensed certification authorities. This works well, so long as the sender does not permit others to use the private key or the private key is stolen. Under this process, the sender must register its public key with a certification authority.

4. Conclusion.

The effect of the Act is unclear, as it relates to other laws involving forgery, banking regulations, etc. However, it is clear that some form of electronic signature must become standard to enable the ever-increasing electronic commerce. We will now have to see if other states pass similar legislation and if companies embrace this system.