HOUSE BILL 66

45TH LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2001

INTRODUCED BY

Joe Mohorovic

AN ACT

RELATING TO ELECTRONIC RECORDS; PROVIDING FOR TECHNOLOGICAL NEUTRALITY IN THE ELECTRONIC AUTHENTICATION OF DOCUMENTS.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

Section 1. Section 14-15-2 NMSA 1978 (being Laws 1996, Chapter 11, Section 2, as amended) is amended to read:

"14-15-2. PURPOSE.--The purpose of the Electronic Authentication of Documents Act is to:

A. provide a centralized, public sector, electronic registry for authenticating electronic documents by means of a public and private key system;

B. promote electronic commerce by eliminating barriers resulting from uncertainties over signature requirements and promoting the development of the legal and business infrastructure necessary to implement secure electronic commerce;

C. facilitate electronic filing of documents with government agencies and promote efficient delivery of government services by means of reliable, secure electronic records and document transactions; [~~and~~]

D. establish a coherent approach to rules and standards regarding the authentication and integrity of electronic records that can serve as a model to be adopted by other states and help to promote uniformity among the various states; and

E. promote technological neutrality in electronic authentication."

Section 2. Section 14-15-3 NMSA 1978 (being Laws 1996, Chapter 11, Section 3, as amended) is amended to read:

"14-15-3. DEFINITIONS.--As used in the Electronic Authentication of Documents Act:

A. "archival listing" means entries in the register that show public keys that are no longer current;

B. "authenticate" means to ascertain the identity of the originator, verify the integrity of the electronic data and establish a link between the data and the originator;

C. "certificate" means a record that at a minimum:

(1) identifies the certification authority issuing it;

(2) names or otherwise identifies its

subscriber or the device or electronic agent under the control of the subscriber;

(3) contains a public key under the control of the subscriber;

(4) specifies the public key's operational period; and

(5) is signed with a digital signature by the certification authority issuing it;

D. "digital signature" means a type of electronic signature created by transforming an electronic record using a message digest function and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key so that any person having the initial untransformed electronic record, the encrypted transformation and the signer's corresponding public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial electronic record has been altered since the transformation was made;

E. "document" means [~~any~~] an identifiable collection of words, letters or graphical knowledge representations, regardless of the mode of representation. "Document" includes correspondence, agreements, invoices, reports, certifications, maps, drawings and images in both electronic and hard copy formats;

F. "electronic authentication" means the electronic signing of a document that establishes a verifiable link between the originator of a document and the document by means of optical, electrical, digital, magnetic, electromagnetic, wireless, biological or other technology providing similar capabilities, including by means of a public key and private key system;

G. "key pair" means, in a public and private key system, a private key and its corresponding public key that can verify an electronic authentication created by the private key;

H. "message digest function" means an algorithm that maps or translates the sequence of bits comprising an electronic record into another generally smaller set of bits, referred to as the message digest, without requiring the use of any secret information, such as a key, and with the result that an electronic record yields that same message digest every time the algorithm is executed using the electronic record as input and it is computationally unfeasible for two electronic records to be found or deliberately generated to produce the same message digest using the algorithm unless the two records are precisely identical;

I. "office" means the office of electronic documentation;

J. "originator" means the person who signs a document electronically;

K. "person" means [~~any~~] an individual or entity, including:

(1) an estate, trust, receiver, cooperative association, club, corporation, company, firm, partnership, joint venture or syndicate; and

(2) any federal, state or local governmental unit or subdivision or any agency, department or instrumentality thereof;

L. "private key" means the code or alphanumeric sequence used to encode an electronic authentication that is known only to its owner and that is the part of a key pair used to create a digital signature;

M. "public key" means the code or alphanumeric sequence used to decode an electronic authentication and that is the part of a key pair used to verify a digital signature;

N. "public and private key system" means the hardware, software and firmware provided by a vendor for the following purposes:

(1) to generate public and private key pairs;

(2) to produce a record abstraction by means of a message digest function;

(3) to encode a signature block and a record abstraction or an entire document;

(4) to decode a signature block and a record abstraction or an entire document; and

(5) to verify the integrity of a document;

O. "register" means a system for storing and retrieving certificates or information relevant to certificates, including information relating to the status of a certificate;

P. "revocation" means the act of notifying the secretary that a public key has ceased or will cease to be effective after a specified time and date;

Q. "secretary" means the secretary of state; [~~and~~]

R. "signed" or "signature" means [~~any~~] a symbol executed or adopted or [~~any~~] a security procedure employed or adopted using electronic means or otherwise, by or on behalf of a person with the intent to authenticate a record; and

S. "technological neutrality" means the methods selected to carry out electronic authentication that do not require or accord greater legal status or effect to the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating or authenticating electronic records or electronic signatures."

Section 3. Section 14-15-5 NMSA 1978 (being Laws 1996, Chapter 11, Section 5) is amended to read:

underscored material = new
[~~bracketed material~~] = delete

"14-15-5. [~~REGULATIONS~~] RULES.--

A. The secretary shall adopt [~~regulations~~] rules to accomplish the purposes of the Electronic Authentication of Documents Act.

B. The [~~regulations~~] rules shall address the following matters:

(1) registration of public keys;

(2) revocation of public keys; and

(3) reasonable public access to the public keys maintained by the office.

C. The [~~regulations~~] rules may address the following matters:

(1) circumstances under which the office may reject an application for registration of a public key;

(2) circumstances under which the office may cancel the listing of a public key; [~~and~~]

(3) circumstances under which the office may reject an attempt to revoke registration of a public key; and

(4) circumstances under which the office may approve electronic authentication other than by means of public or private key systems."