SENATE BILL 146

44TH LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 1999

INTRODUCED BY

Pauline B. Eisenstadt

AN ACT

RELATING TO RECORDS; AMENDING THE ELECTRONIC AUTHENTICATION OF DOCUMENTS ACT TO CLARIFY THE PURPOSE AND CHANGE CERTAIN TECHNICAL DEFINITIONS.

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) is amended to read:

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

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

B. promote electronic commerce [~~and~~] by eliminating barriers resulting from uncertainties over signature requirements and promoting the development of the

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

legal and business infrastructure necessary to implement secure electronic commerce;

C. facilitate electronic [~~information~~] 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."

Section 2. Section 14-15-3 NMSA 1978 (being Laws 1996, Chapter 11, Section 3) 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A. "archival listing" means entries in the register that show public keys that are no longer current;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

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

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. [~~"sign" or "signing"~~] "digital signature" means [~~the execution or adoption of any symbol by a person with the intention to establish the authenticity of a document as his own~~] any symbol executed or adopted or any security procedure employed or adopted using electronic means or otherwise, by or on behalf of a person with the intent to authenticate a record;

[~~C.~~] E. "document" means any 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;

[~~D.~~] 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 a public key and private key system;

[~~E.~~] G. "key pair" means, in a public and private

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

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;

[~~F.~~] I. "office" means the office of electronic documentation;

[~~G.~~] J. "originator" means the person who signs a document electronically;

[~~H.~~] K. "person" means any 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

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

instrumentality thereof;

[~~I.~~] 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 [~~an electronic authentication~~] a digital signature;

[~~J.~~] 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 [~~an electronic authentication~~] a digital signature;

[~~K.~~] 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 [~~secure hash code~~] 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;

[~~L. "record abstraction" means a condensed representation of a document that is prepared by using a secure hash code;~~

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

~~M.~~] O. "register" means [~~a database or other electronic structure that binds a person's name or other identity to a public key~~] a system for storing and retrieving certificates or information relevant to certificates, including information relating to the status of a certificate;

[~~N.~~] 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; and

[~~O.~~] Q. "secretary" means the secretary of state.

[~~P. "secure hash code" means a mathematical algorithm that, when applied to an electronic version of a document, creates a condensed version of the document that makes it computationally impossible to identify or recreate the document without essential knowledge of that document; and~~]"

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

FORTY-FOURTH LEGISLATURE

FIRST SESSION, 1999 SB 146/a

February 3, 1999

Mr. President:

Your JUDICIARY COMMITTEE, to whom has been referred

SENATE BILL 146

has had it under consideration and reports same with recommendation that it DO PASS, amended as follows:

1. On page 1, line 20, after "public", insert "sector".

2. On page 3, strike lines 8 through 14 and insert in lieu thereof:

"D. "digital signature" means a type of electronic signature created by transforming an electronic record using a

.124596.1

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

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;".

3. On page 6, line 8, strike the second occurrence of "and", and on line 9, strike the period after "state" and insert in lieu thereof "; and".

4. On page 6, line 15, strike the closing quotation mark.

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

5. On page 6, between lines 15 and 16, insert the following new subsection:

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

Respectfully submitted,

_____

Michael S. Sanchez, Chairman

Adopted_____ Not

Adopted_____

(Chief Clerk) (Chief Clerk)

Date _____

The roll call vote was 6 For 0 Against

Yes: 6

No: None

Excused: Davis, Stockard

Absent: None

underscored material = new
[bracketed material] = delete