HOUSE BILL 608

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

INTRODUCED BY

Joe Mohorovic

AN ACT

RELATING TO ELECTRONIC RECORDS; PROVIDING FOR TECHNOLOGICAL
NEUTRALITY; CHANGING DEFINITIONS; PROVIDING BROAD RULE-MAKING
AUTHORITY; CHANGING RESPONSIBILITY FOR ELECTRONIC
AUTHENTICATION OF DOCUMENTS FROM THE SECRETARY OF STATE TO THE
INFORMATION TECHNOLOGY MANAGEMENT OFFICE; AMENDING AND
REPEALING SECTIONS OF THE NMSA 1978.

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] technical approach to authenticating electronic
documents [by means of a public and private key system];

.136005.1

1   B.   promote electronic commerce by eliminating

2   barriers resulting from uncertainties over signature

3   requirements and promoting the development of the legal and

4   business infrastructure necessary to implement secure

5   electronic commerce;

6   C.   facilitate electronic filing of documents with

7   government agencies and promote efficient delivery of

8   government services by means of reliable, secure electronic

9   records and document transactions; [and]

10   D.   establish a coherent approach to rules and

11   standards regarding the authentication [and integrity] of

12   electronic records [that can serve as a model to be adopted by

13   other states and help to promote uniformity among the various

14   states]; and

15   E.   promote technological neutrality in electronic

16   authentication."

17   Section 2.   Section 14-15-3 NMSA 1978 (being Laws 1996,

18   Chapter 11, Section 3, as amended) is amended to read:

19   "14-15-3.   DEFINITIONS.--As used in the Electronic

20   Authentication of Documents Act:

21   [A.   "archival listing" means entries in the

22   register that show public keys that are no longer current;

23   B.] A.   "authenticate" means to ascertain the

24   identity of the originator, verify the integrity of the

25   electronic data and establish a link between the data and the

.136005.1

- 2 -

1   originator;

2   [C.   "certificate" means a record that at a

3   minimum:

4   (1)   identifies the certification authority

5   issuing it;

6   (2)   names or otherwise identifies its

7   subscriber or the device or electronic agent under the control

8   of the subscriber;

9   (3)   contains a public key under the control

10   of the subscriber;

11   (4)   specifies the public key's operational

12   period; and

13   (5)   is signed with a digital signature by the

14   certification authority issuing it;

15   D.   "digital signature" means a type of electronic

16   signature created by transforming an electronic record using a

17   message digest function and encrypting the resulting

18   transformation with an asymmetric cryptosystem using the

19   signer's private key so that any person having the initial

20   untransformed electronic record, the encrypted transformation

21   and the signer's corresponding public key can accurately

22   determine whether the transformation was created using the

23   private key that corresponds to the signer's public key and

24   whether the initial electronic record has been altered since

25   the transformation was made;

.136005.1

1   E.-] B.   "document" means [any] an identifiable

2   collection of words, letters or graphical knowledge

3   representations, regardless of the mode of representation.

4   "Document" includes correspondence, agreements, invoices,

5   reports, certifications, maps, drawings and images in both

6   electronic and hard copy formats;

7   [F.] C.   "electronic authentication" means the

8   electronic signing of a document that establishes a verifiable

9   link between the originator of a document and the document by

10   means of optical, electrical, digital, magnetic,

11   electromagnetic, wireless, biological, a public key and

12   private key system or other technology providing similar

13   capabilities;

14   [G.   "key pair" means, in a public and private key

15   system, a private key and its corresponding public key that

16   can verify an electronic authentication created by the private

17   key;

18   H.   "message digest function" means an algorithm

19   that maps or translates the sequence of bits comprising an

20   electronic record into another generally smaller set of bits,

21   referred to as the message digest, without requiring the use

22   of any secret information, such as a key, and with the result

23   that an electronic record yields that same message digest

24   every time the algorithm is executed using the electronic

25   record as input and it is computationally unfeasible for two

.136005.1

1 electronic records to be found or deliberately generated to

2 produce the same message digest using the algorithm unless the

3 two records are precisely identical;

4 I.] D. "office" means the [office of electronic

5 documentation] information technology management office;

6 [J.] E. "originator" means the person who signs a

7 document electronically;

8 [K.] F. "person" means [any] an individual or

9 entity, including:

10 (1) an estate, trust, receiver, cooperative

11 association, club, corporation, company, firm, partnership,

12 joint venture or syndicate; and

13 (2) any federal, state or local governmental

14 unit or subdivision or any agency, department or

15 instrumentality thereof;

16 [L. "private key" means the code or alphanumeric

17 sequence used to encode an electronic authentication that is

18 known only to its owner and that is the part of a key pair

19 used to create a digital signature;

20 M. "public key" means the code or alphanumeric

21 sequence used to decode an electronic authentication and that

22 is the part of a key pair used to verify a digital signature;

23 N. "public and private key system" means the

24 hardware, software and firmware provided by a vendor for the

25 following purposes:

.136005.1

1   (1) to generate public and private key

2   pairs;

3   (2) to produce a record abstraction by means

4   of a message digest function;

5   (3) to encode a signature block and a record

6   abstraction or an entire document;

7   (4) to decode a signature block and a record

8   abstraction or an entire document; and

9   (5) to verify the integrity of a document;

10   O. "register" means a system for storing and

11   retrieving certificates or information relevant to

12   certificates, including information relating to the status of

13   a certificate;

14   P. "revocation" means the act of notifying the

15   secretary that a public key has ceased or will cease to be

16   effective after a specified time and date;

17   Q. "secretary" means the secretary of state;

18   R.] G. "signed" or "signature" means [any] a

19   symbol executed or adopted or [any] a security procedure

20   employed or adopted using electronic means or otherwise, by

21   or on behalf of a person with the intent to authenticate a

22   record; and

23   H. "technological neutrality" means the methods

24   selected to carry out electronic authentication that do not

25   require or accord greater legal status or effect to the

. 136005. 1

1 implementation or application of a specific technology or

2 technical specification for performing the functions of

3 creating, storing, generating, receiving, communicating or

4 authenticating electronic records or electronic signatures."

5 Section 3. Section 14-15-5 NMSA 1978 (being Laws 1996,

6 Chapter 11, Section 5) is amended to read:

7 "14-15-5. [REGULATIONS] RULES.--

8 A. The [secretary] information technology

9 commission shall adopt [regulations] rules and standards to

10 accomplish the purposes of the Electronic Authentication of

11 Documents Act.

12 B. The [regulations] rules shall address [the

13 following matters:

14 (1) registration of public keys;

15 (2) revocation of public keys; and

16 (3) reasonable public access to the public

17 keys maintained by the office.

18 C. The regulations may address the following

19 matters:

20 (1) circumstances under which the office

21 may reject an application for registration of a public key;

22 (2) circumstances under which the office

23 may cancel the listing of a public key; and

24 (3) circumstances under which the office

25 may reject an attempt to revoke registration of a public

.136005.1

1 key] circumstances under which standards other than adopted

2 standards may be used."

3   Section 4. Section 14-15-6 NMSA 1978 (being Laws 1996,

4 Chapter 11, Section 6) is amended to read:

5   "14-15-6. CONTRACTING SERVICES.--The [secretary]

6 office may contract with a private, public or quasi-public

7 organization for the provision of services under the

8 Electronic Authentication of Documents Act. A contract for

9 services shall comply with [regulations] rules adopted

10 pursuant to the Electronic Authentication of Documents Act

11 and the provisions of the Public Records Act and the

12 Procurement Code."

13   Section 5. REPEAL.--Section 14-15-4 NMSA 1978 (being

14 Laws 1996, Chapter 11, Section 4) is repealed.

15   Section 6. EFFECTIVE DATE.--The effective date of the

16 provisions of this act is July 1, 2001.

17   - 8 -

18

19

20

21

22

23

24

25

.136005.1