This rule was filed as 1 NMAC 3.2.70.2.

TITLE 1 GENERAL GOVERNMENT
CHAPTER 12 INFORMATION TECHNOLOGY
PART 7 ELECTRONIC AUTHENTICATION

1.12.7.2.1 ISSUING AGENCY: Commission of Public Records
[6-1-96; Rn, 1 NMAC 3.51, 5-15-97; Recompiled 11/30/01]

1.12.7.2.2 SCOPE: All state agencies, public officials, persons who wish to transact business with the state, and others where registration will promote the purpose of NMSA 1978 14-3-15.2.
[6-1-96; Rn, 1 NMAC 3.51, 5-15-97, 4-18-98; Recompiled 11/30/01]

1.12.7.2.3 STATUTORY AUTHORITY: NMSA 1978 14-3-15.2
[6-1-96; Rn, 1 NMAC 3.51, 5-15-97; Recompiled 11/30/01]

1.12.7.2.4 DURATION: Permanent
[6-1-96; Rn, 1 NMAC 3.51, 5-15-97; Recompiled 11/30/01]

1.12.7.2.5 EFFECTIVE DATE: July 1, 1996 unless a later date is cited at the end of a section or paragraph.
[6-1-96; Rn, 1 NMAC 3.51, 5-15-97; A, 5-15-97; Recompiled 11/30/01]

1.12.7.2.6 OBJECTIVE: To establish standards and procedures to allow for the use of electronic authentication in substitution for a signature.
[6-1-96; Rn, 1 NMAC 3.51, 5-15-97, 4-18-98; Recompiled 11/30/01]

1.12.7.2.7 DEFINITIONS:

A. **"Archival listing"** means entries in the register showing public keys that are no longer current.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 the link between the data and the originator.

C. **"Cancel and cancellation"** refer to the act of the office in terminating the current listing of a public key. It does not affect an archival listing.

D. **"Document"** means any identifiable collection of words and letters or graphical knowledge representations, regardless of the mode of representation. It includes, but is not limited to, correspondence, agreements, invoices, reports, certifications, maps, drawings, and images in both electronic and hard copy formats.

E. **"Electronic authentication"** means the electronic signing of a document consisting of establishing a verifiable link between the originator and the document by means of a public/private key system.

F. **"FIPS PUB"** means *Federal Information Processing Standards Publication* produced by the U.S. department of commerce, technology administration, national institute of standards and technology. FIPS PUBS are available from the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. FIPS PUB 140-1 is available electronically at http://csrc.ncsl.nist.gov.

G. **"Key pair in a public/private key system",** means a private key and its corresponding public key, having the property that the public key can verify an electronic authentication that the private key creates.

H. **"Office"** means the office of electronic documentation.

I. **"Originator"** means the person who signs a document electronically.

J. **"Person"** means any individual or entity including but not limited to an estate, trust, receiver, cooperative association, club, corporation, company, firm, partnership, joint-venture, syndicate, or other association; "person" also means any federal, state, or other governmental unit or subdivision, or any agency, department or instrumentality thereof.

K. **"Private key"** means the code or alphanumeric sequence used to encode an electronic authentication and which is known only to its owner. The private key is the part of a key pair used to create an electronic authentication.

L. **"Public key"** means the code or alphanumeric sequence used to decode an electronic authentication. The public key is the part of a key pair used to verify an electronic authentication.

M. **"Public/private key system"** means the hardware, software, and firmware that are provided by a vendor for

(1) the generation of public/private key pairs,
(2) the record abstraction by means of a secure hash code,
(3) the encoding of the signature block and the record abstraction or the entire record,
(4) the decoding of the signature block and the record abstraction or the entire record, and
(5) the verification of the integrity of the received record.

N. **"Record abstraction"** means a condensed representation of a document, which condensation is prepared by use of a secure hash code; it is also known as a message digest.

O. **"Register"** means a data base or other electronic structure that binds a person's name or other identity with its public key.

P. **"Repudiate"** and "non-repudiation" refer to the acts of denying or proving the origin of a document from its sender, and to the acts of denying or proving the receipt of a document by its recipient.

Q. **"Revoke"** and "revocation" refer to the act of notifying the secretary that the person's public key has or will cease to be effective after a specified time and date.

R. **"Secretary"** means the secretary of state.

S. **"Secure hash code"** is a mathematical algorithm that, when applied to an electronic version of a document, creates a condensed version of the document from which it is computationally infeasible to identify or recreate the document which corresponds to the condensed version of the document without extrinsic knowledge of that correspondence.

T. **"Sign"** and **"signing"** includes the execution or adoption of any symbol by a person with the present intention to establish the authenticity of the document as theirs.

U. **"Signature block"** means the portion of a document, encoded by the private key, which contains the identity of the originator and the date and time of the records creation, submittal or approval.

V. **"Trusted entity"** means an independent, unbiased third party that contributes to , or provides, important security assurances that enhance the admissibility, enforceability and reliability of information in electronic form. In a public/private key system, a trusted entity registers a digitally signed data structure that binds an entity's name (or identity) with its public key.

[6-1-96; Rn, 1 NMAC 3.51, 5-15-97, 4-18-98; Recompiled 11/30/01]

1.12.7.2.8 PUBLIC/PRIVATE KEY SYSTEM OPERATION: The most effective authentication of electronic documents is by a public/private key system. In a public/private key system, each user generates a key "pair" that has two inverse components -- a private key and a public key. Each key of a pair bears a complex, mathematical relationship to the other (e.g., an algorithm). The system is designed such that one component can be made public (the public key, along with other identifying information) without compromising the other component (the private key). The private component, known only to the user, is used to encode the signature on outgoing documents. The public key is registered with a trusted entity and distributed to other users with whom the sender plans to exchange documents, and is used to verify authenticity of the sender's document (decode the signature). The office of electronic documentation, under the secretary of state, is the trusted entity for the registration of the public keys of public officials, persons who wish to transact business with the state, and others where such registration will promote the purpose of NMSA 1978 section 14-3-15.2. As the trusted entity, the office maintains an electronic register of public keys which includes both current listings and archival listings. The list of registered signatures contains the key holder's name, the date of application, the public key number, and other identifying information. The register also contains a history of all public keys issued to that person. Additionally, the register identifies the vendor of the software, the product name, and the version number used to produce the public/private key, Thus, users can communicate securely without having previously exchanged keys. The trusted entity also insures that the user of the private key will not repudiate their authentication of a record because the user must notify the trusted entity in the event their private key has been lost, stolen, or otherwise compromised (see 1 NMAC 3.2.70.2.10.5).

[6-1-96; Rn, 1 NMAC 3.51, 5-15-97; A, 5-15-97; Recompiled 11/30/01]

1.12.7.2.9 CERTIFICATION OF PUBLIC/PRIVATE KEY SYSTEMS:

A. A vendor's public/private key system must be approved by the Commission of Public Records prior to its use.

B. The following vendors public/private key systems are approved by this rule:

(1) RSA Data Security (RSA): Address all correspondence to RSA's electronic mail address <rsaref-administrator@rsa.com>, or to: RSA Laboratories. ATTN: RSAREF Administrator; 100 Marine Parkway, Suite 500, Redwood City, CA 94065.

(2) Pretty Good Privacy (PGP) versions 2.6 and above: PGPcommercial version address all correspondence to ViaCrypt's electronic mail address <70275.1360@compuserve.com>, or non-profit education version information <http://web.mit.edu/network/pgp.html>, distribution authorization <http://bs.mit.edu:8001/pgp-form.html>.

C. Additional public/private key systems may be approved by a vendor following these steps:

(1) Make a written application for approval to the commission of public records.

(2) Provide proof, from a national institute of standards and technology (NIST) accredited national laboratory, that the system is in compliance with the derived test requirements for FIPS PUB 140-1, *Security Requirements for Cryptographic Modules* and meets, at a minimum, the requirements for security level 1 of FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*.

[6-1-96; Rn, 1 NMAC 3.51, 5-15-97; 5-15-97, 4-18-98; Recompiled 11/30/01]

1.12.7.2.10 PUBLIC/PRIVATE KEY SYSTEMS REQUIREMENTS:

A. To be accepted as a public record, or by the state in respect to transactions, the public key of a user must be registered with the secretary of state.

B. The signature block of an electronic authentication must contain the identity of the originator and the date and time of the record's creation, submittal or approval.

C. A state agency may require by regulation that certain types of transactions have an additional signature block for a trusted entity containing a date and time stamp. [

D. A state agency may require by regulation that certain types of transactions have a higher level of security than the requirements for security level 1 of FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*.

E. It is the responsibility of the registered user of a private key to maintain the key's security. Repudiation may only occur by the determination of a court of competent jurisdiction that the private key of the registered user was compromised through no fault of the registered user and without knowledge on the part of the registered user. It is the legal prerequisite for a claim of repudiation that the repudiator have filed a notice of revocation with the secretary prior to making the claim of repudiation.

F. A state agency is only bound to accept as a trusted entity the Secretary of State or a person listed as a trusted entity by the secretary of state.

G. A state agency must comply with the security requirements in the *Performance Guidelines for the Legal Acceptance of Public Records Produced by Information Technology Systems*, 1 NMAC 3.2.70.1 [now 1.13.70 NMAC].

H. A state agency must comply, at a minimum, with the requirements for security level 1 of FIPS PUB 140-1, *Security Requirements for Cryptographic Modules* with respect to distribution and maintenance of public and private keys. A state agency must use a seed number for generation of public/private keys equal to or greater than the seed number specified in FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*.

[6-1-96; Rn, 1 NMAC 3.51, 5-15-97; Recompiled 11/30/01]

HISTORY OF 1.12.7 NMAC [RESERVED.]