TITLE 1 GENERAL GOVERNMENT
CHAPTER 12 INFORMATION TECHNOLOGY
PART 7 DIGITAL / ELECTRONIC SIGNATURE

1.12.7.1 ISSUING AGENCY: State Commission of Public Records and State Records Administrator
[1.12.7.1 NMAC - Rp, 1 NMAC 3.2.70.2.1, 7/1/2015]

1.12.7.2 SCOPE: To implement the electronic signature authority pursuant to the Public Records Act, Section 14-3-15.2 NMSA 1978 and the New Mexico Uniform Electronic Transactions Act, Section 14-16-1 et seq NMSA 1978.
[1.12.7.2 NMAC - Rp, 1 NMAC 3.2.70.2.2, 7/1/2015]

1.12.7.3 STATUTORY AUTHORITY: Public Records Act, Section 14-3-15.2 NMSA 1978; Uniform Electronic Transactions Act, Section 14-16-1 et seq NMSA 1978.
[1.12.7.3 NMAC - Rp, 1 NMAC 3.2.70.2.33, 7/1/2015]

1.12.7.4 DURATION: Permanent
[1.12.7.4 NMAC - Rp, 1 NMAC 3.2.70.2.4, 7/1/2015]

1.12.7.5 EFFECTIVE DATE: July 1, 2015, unless a later date is cited at the end of a section.
[1.12.7.5 NMAC - Rp, 1 NMAC 3.2.70.2.5, 7/1/2015]

1.12.7.6 OBJECTIVE: To establish standards for state agencies regarding the use of electronic signatures for legal signing purposes as authorized under the provisions of the Uniform Electronic Transactions Act. These rules are an adaption of the Use of Electronic Signatures in Federal Organization Transactions, Version 1.0 issued January 25, 2013.
[1.12.7.6 NMAC - Rp, 1 NMAC 3.2.70.2.6, 7/1/2015]

1.12.7.7 DEFINITIONS: For purposes of this part, all terms defined in the Uniform Electronic Transactions Act, Section 14-16-1 et seq NMSA 1978 have the meanings set forth in statute. Additionally, the following terms shall have the following meanings:

A. Terms beginning with the letter "A":

(1) "Agreement" refer to Uniform Electronic Transactions Act, Section 14-16-2(1) NMSA 1978.

(2) "Attribution" means the process of establishing or confirming that someone is the previously identified person they claim to be.

(3) "Authenticate" refer to Electronic Authentication of Documents Act, Section 14-15-3(A) NMSA 1978.

(4) "Automated transaction" refer to Uniform Electronic Transactions Act, Section 14-16-2(2) NMSA 1978.

B. Terms beginning with the letter "B":

(1) "Biometrics" means the unique physical characteristics of individuals that can be converted into digital form and then interpreted by a computer. Among these are voice patterns, fingerprints, and the blood vessel patterns present on the retina of one or both eyes.

C. Terms beginning with the letter "C":

(1) "Click wrap" means a click wrap agreement, also known as click through agreement or click wrap license, that require an end user to manifest his or her assent by clicking a button or pop-up window that says "OK" or "agree" or some similar form. A user indicates rejection by clicking "cancel" or some similar form or by closing browsing window.

(2) "Computer program" refer to Uniform Electronic Transactions Act, Section 14-16-2(3) NMSA 1978.

(3) "Contract" refer to Uniform Electronic Transactions Act, Section 14-16-2(4) NMSA 1978.

(4) "Credential" means a digital document that binds a person' identity to a token possessed and controlled by a person; data that is used to establish the claimed attributes or identity of a person or an entity.

Common paper credentials include passports, birth certificates, driver's licenses and employee identification cards. Common digital credentials include user IDs and digital certificates. Credentials are a tool for authentication.

(5) **"Cryptographic key"** means a value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.

D. **Terms beginning with the letter "D":**

(1) **"Digital signature"** means any electronic signature that can be used to authenticate the identity of the sender of or signer of a document, and may also ensure that the content of the sent document is unaltered.

(2) **"Digitized signature"** means a graphical image of a handwritten signature.

(3) **"Document"** refer to Electronic Authentication of Documents Act, Section 14-15-3(B) NMSA 1978.

E. **Terms beginning with the letter "E":**

(1) **"Electronic"** refer to Uniform Electronic Transactions Act, Section 14-16-2(5) NMSA 1978.

(2) **"Electronic agent"** refer to Uniform Electronic Transactions Act, Section 14-16-2(6) NMSA 1978.

(3) **"Electronic authentication"** refers to Electronic Authentication of Documents Act, Section 14-15-3(C) NMSA 1978.

(4) **"Electronic record"** refer to Uniform Electronic Transactions Act, Section 14-16-2(7) NMSA 1978.

(5) **"Electronic signature"** refer to Uniform Electronic Transactions Act, Section 14-16-2(8) NMSA 1978.

F. **Terms beginning with the letter "F": [RESERVED]**

G. **Terms beginning with the letter "G":**

(1) **"Governmental agency"** refer to Uniform Electronic Transactions Act, Section 14-16-2(9) NMSA 1978.

H. **Terms beginning with the letter "H":**

(1) **"Hash" or Hash function"** means a mathematical function that takes a variable length input string and converts it to a smaller fixed-length output string, that is for all relevant purposes unique to the data used as input to the message digest function. The message digest is, in essence, a digital fingerprint of the data to which it relates.

(2) **"Hyperlink"** means any electronic link providing direct access from one distinctively marked place in a hypertext or hypermedia document to another in the same or a different document.

I. **Terms beginning with the letter "I":**

(1) **"Identification"** means the process of verifying and associating attributes with a particular person designated by an identifier.

(2) **"Identity"** means the unique name of an individual person, and any associated attributes; the set of the properties of a person that allows the person to be distinguished from other persons.

(3) **"Information"** refer to Uniform Electronic Transactions Act, Section 14-16-2(10) NMSA 1978.

(4) **"Information processing system"** refer to Uniform Electronic Transactions Act, Section 14-16-2(11) NMSA 1978.

(5) **"Integrity"** means a state in which information has remained unaltered from the point it was produced by a source, during transmission, storage and eventual receipt by the destination.

(6) **"Intent to sign"** means the intent of a person that a sound, symbol or process is applied to a record in order to have a legally binding effect.

(7) **"Level of assurance"** means the level of authentication assurance that describes the degree of certainty that a user has presented an identifier that refers to her identity.

J. **Terms beginning with the letter "J": [RESERVED]**

K. **Terms beginning with the letter "K": [RESERVED]**

L. **Terms beginning with the letter "L": [RESERVED]**

M. **Terms beginning with the letter "M":**

(1) **"Method"** means a particular way of doing something, a means, process or manner of procedure, especially a regular and systematic way of accomplishing something and an orderly arrangement of steps to accomplish an end.

N. **Terms beginning with the letter "N":**

(1) **NIST Special Publication 800-63"** refers to the National Institute of Standards and Technology, Special Publication 800-63, Electronic Authentication Guidance.

O. **Terms beginning with the letter "O":**

(1) **"Originator"** refers to Electronic Authentication of Documents Act, Section 14-15-3(E) NMSA 1978.

P. **Terms beginning with the letter "P":**

(1) **"Password"** means a secret word or string of characters that is used for authentication, to prove identity or to gain access to a record or resource. Passwords are typically character strings.

(2) **"PDF"** or Portable Document Format refers to a file format used to present documents in a manner independent of application software, hardware, and operating systems. A PDF file encapsulates a complete description of a fixed-layout flat document, including the text, fonts, graphics, and other information needed to display it.

(3) **"Person"** refer to Uniform Electronic Transactions Act, Section 14-16-2(12) NMSA 1978.

(4) **"Personal identification number (PIN)** means a shared secret a person accessing a government organization's electronic application is requested to enter, such as a password or PIN. The system checks that password or PIN against data in a database to ensure its correctness and thereby "authenticates" the user.

(5) **"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.

(6) **"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.

(7) **"Public/private key system"** means the hardware, software, and firmware that are provided by a vendor for: (a) the generation of public/private key pairs, (b) the record abstraction by means of a secure hash code, (c) the encoding of the signature block and the record abstraction or the entire record, (d) the decoding of the signature block and the record abstraction or the entire record, and (e) the verification of the integrity of the received record.

Q. **Terms beginning with the letter "Q": [RESERVED]**

R. **Terms beginning with the letter "R":**

(1) **"Reason for signing"** means the purpose statement of a person with regard to a document or electronic record that is affirmed by signing the document or record. The reason for signing should be distinguished from the intent to sign.

(2) **"Record"** refer to Uniform Electronic Transactions Act, Section 14-16-2(13) NMSA 1978.

(3) **"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.

(4) **"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.

(5) **"Risk"** is a function of the likelihood that a given threat will exploit a potential vulnerability and have an adverse impact on an organization.

S. **Terms beginning with the letter "S":**

(1) **"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.

(2) **"Security procedure"** refer to Uniform Electronic Transactions Act, Section 14-16-2(14) NMSA 1978.

(3) **"Signed"** and **"signature"** refer to Electronic Authentication of Documents Act, Section 14-15-3(G) NMSA 1978..

(4) **"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.

(5) **"Signing requirements"** means the requirements that must be satisfied to create a valid and enforceable electronic signature.

(6) **"State"** refer to Uniform Electronic Transactions Act, Section 14-16-2(15) NMSA 1978.

T. **Terms beginning with the letter "T":**

(1) **"TIF"** or "TIFF" or Tagged Image Format refers to an image file format for high-quality graphics.

(2) **"Threat"** means a potential circumstance, entity or event capable of exploiting vulnerability and causing harm. Threats can come from natural causes, human actions, or environmental conditions. A threat does not present a risk when there is no vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited.

(3) **"Token"** refers to something that a person possesses and controls (typically a cryptographic key or password) that is used to authenticate the person's identity.

(4) **"Transaction"** refer to Uniform Electronic Transactions Act, Section 14-16-2(16) NMSA 1978.

(5) **"Transferable record"** means an electronic record that would: (a) be a note under Chapter 55, Article 3 NMSA 1978 or a document under Chapter 55, Article 7 NMSA 1978 if the electronic record were in writing; and (b) the issuer of the electronic record expressly has agreed is a transferable record.

(6) **"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.

U. **Terms beginning with the letter "U": [RESERVED]**

V. **Terms beginning with the letter "V":**

(1) **"Voice signature"** means an audio recording created by an individual who intends to sign a particular transaction (or document) and used as the electronic form of signature.

W. **Terms beginning with the letter "W": [RESERVED]**

X. **Terms beginning with the letter "X": [RESERVED]**

Y. **Terms beginning with the letter "Y": [RESERVED]**

Z. **Terms beginning with the letter "Z": [RESERVED]**

[1.12.7.7 NMAC - Rp, 1 NMAC 3.2.70.2.7, 7/1/2015]

1.12.7.8 GENERAL OVERVIEW:

A. A signature, whether electronic or on paper, is the means by which a person indicates an intent to associate oneself with a document in a manner that has legal significance (e.g., to adopt or approve a specific statement regarding, or reason for signing, a document). It constitutes legally-binding evidence of the signer's intention with regard to a document. The reasons for signing a document will vary with the transaction, and in most cases can be determined only by examining the context in which the signature was made. Generally, a person's reason for signing a document falls into one of the following categories:

(1) approving, assenting to, or agreeing to the information in the document or record signed (e.g., agreeing to the terms of a contract or inter-agency memorandum or indicating approval for legal sufficiency);

(2) certifying or affirming the accuracy of the information stated in the document or record signed (e.g., certifying that the statements in one's tax return are true and correct);

(3) acknowledging access to or receipt of information set forth in the document or record signed (e.g., acknowledging receipt of a disclosure document);

(4) witnessing the signature or other act of another (e.g., notarization); or

(5) certifying the source of the information in the document or record signed (e.g., certifying data in a clinical trial record, certifying an inventory count, etc.).

B. The Uniform Electronic Transaction Act sets forth the requirements that must be satisfied by an electronic signature to establish functional equivalence to the paper-based requirement for a signature.

[1.12.7.8 NMAC - N, 7/1/2015]

1.12.7.9 ELECTRONIC SIGNATURES COMPARED TO DIGITAL SIGNATURES:

A. "Electronic signature" is the term used for the electronic equivalent of a handwritten signature. It is a generic, technology- neutral term that refers to the universe of all of the various methods by which one can "sign" an electronic record. Although all electronic signatures may be represented digitally (i.e., as a series of ones and zeroes), they can take many forms and can be created by many different technologies.

B. "Digital signature" is the term used to describe the small segment of encrypted data produced when a specific mathematical process (involving a hash algorithm and public key cryptography) is applied to an electronic record.

[1.12.7.9 NMAC - N, 7/1/2015]

1.12.7.10 ELECTRONIC SIGNATURE, SECURITY PROCEDURE AND SIGNING PROCESS:

A. An electronic signature is used to indicate a person's intent to associate themselves in some way to information or to a reason for signing (e.g., agreeing to the terms of a contract, acknowledging receipt of information, etc.) with legal effect. Any sound, symbol, or process that is made or adopted by a person with intent to sign a document can be used as the form of signature for purposes of creating an electronic signature. This includes, for example, a typed name, clicking on an "I Agree" button, or a cryptographically created digital signature. But the mere use of any such sound, symbol, or process does not necessarily create a legally binding electronic signature.

B. A security procedure is employed for the purpose of verifying that an electronic record, signature, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record (integrity). A digital signature can be used as both a security procedure and as a legally binding form of signature. It is important that the context make clear whether the digital signature is intended merely for purposes of attribution, integrity, or whether it is also intended to be a legally binding electronic signature.

C. A signing process is the overall set of actions, steps, and elements that is used to create a valid and enforceable electronic signature, and includes both the application to an electronic record of a form of signature (i.e., the sound, symbol, or process) to be used as the electronic signature, and one or more processes or security procedures to address the other signature requirements listed.

[1.12.7.10 NMAC - N, 7/1/2015]

1.12.7.11 LEGAL REQUIREMENT FOR A SIGNATURE: A transaction is governed by a law or regulation that requires the presence of a signature before it will be considered legally effective. A state agency must review the law applicable to each proposed transaction to determine if it requires that the transaction be "signed." If the applicable law or regulation requires a signature, then to conduct the transaction in electronic form requires an electronic signature.

[1.12.7.11 NMAC - N, 7/1/2015]

1.12.7.12 TRANSACTION-BASED NEED FOR A SIGNATURE: If there is no legal requirement for a signature on a particular type of transaction a state agency may undertake a further analysis to evaluate the desirability of incorporating a signature requirement into the transaction. An electronic signature may be desirable, even when not legally required, where there is a:

A. Need for emphasizing the seriousness of the transaction. A signature may serve to reinforce the significance of the undertaking to the party involved. It gives the transaction a more formal tone, and helps to drive home to the signing party the seriousness of what is being undertaken.

B. Need for binding a party to the transaction. If the transaction involves an intent element (e.g., agreement, approval, acknowledgment, receipt, witnessing, etc.), a signature may be useful to help formally bind a person to that reason for signing and make it more likely to be enforced (e.g., to mitigate concerns regarding repudiation).

[1.12.7.12 NMAC - N, 7/1/2015]

1.12.7.13 REQUIREMENTS FOR LEGALLY BINDING ELECTRONIC SIGNATURE: Where an electronic signature is required by law or otherwise deemed desirable, it is critical that the electronic signature and the associated signing process satisfy all of the applicable legal requirements. Generally, creating a valid and enforceable electronic signature requires satisfying the following signing requirements.

A. A person (i.e., the signer) must use an acceptable electronic form of signature. Electronic signatures can take many forms, and can be created by many different technologies. No specific technology or form of signature is required. Generally, any electronic "sound, symbol, or process" can be used as the form of signature. Examples of commonly used electronic forms of signature include, but are not limited to:

(1) Symbols such as a typed name (e.g., typed at the end of an e-mail message by the sender, or typed into a signature block on a website form by a party); digitized image of a handwritten signature that is attached to an electronic record; a shared secret (e.g., a secret code, password, or PIN) used by a person to sign the electronic record; a unique biometrics-based identifier, such as a fingerprint, voice print, or a retinal scan; or a digital signature.

(2) Sounds such as sound recording of a person's voice expressing consent.

(3) Processes such as using a mouse to click a button or hyperlink (such as clicking an "I Agree" button); using a private key and applicable software to apply a "digital signature;" or scanning and applying a fingerprint.

B. The electronic form of signature must be executed or adopted by a person with the intent to sign the electronic record, (e.g., to indicate a person's approval of the information contained in the electronic record). A person's intent to sign is often inferred from his or her approval of the reason for signing as stated in the text of either: (i) the electronic record being signed or (ii) the surrounding signing process. For example, words appearing immediately above a blank signature line on a contract document might state "By signing below I agree to the foregoing contract terms." That statement indicates both the reason for signing (agreement to the contract) as well as the means by which a person can indicate an intent to sign (i.e., by applying the form of signature where indicated). Thus, a person indicates his or her intention to sign, for the reason stated, by signing on the applicable blank line. Likewise, text on a website might state that "By checking this box I agree to the terms of use." A person indicates his or her intention to sign, for the reason stated, by checking the box on the website.

C. The electronic form of signature must be attached to or associated with the electronic record being signed. Specifically, it must be attached to, or logically associated with, the record being signed. Satisfying this requirement requires storing the data constituting the electronic form of signature, and doing so in a way that permanently associates it with the electronic record that was signed. Where the electronic form of signature consists of a symbol or a sound (such as a typed name, a digitized image of a handwritten name, a PIN, a digital signature, a voice recording, etc.), the data representing the symbol or sound must be saved. Where the electronic form of signature consists of a process (such as clicking on an "I Agree" button), the system must be programmed so that completion of the process generates some specific data element to indicate completion of the signing process, or some other procedure (such as generation of a log record or audit trail) to record the act of signing. It is also recommended that the following additional data elements be appended to or associated with the signature data provided privacy considerations have been taken into account:

(1) Identity of the signer or a link to the source of identifying information, such as a validated UserID, a digital certificate, a biometric database, etc.;

(2) Date and time of the signature;

(3) Method used to sign the record; and

(4) An indication of the reason for signing.

D. There must be a means to identify and authenticate a particular person as the signer. Meeting this burden of proof requires establishing a link between an identified person and the signature. An electronic form of signature may or may not provide proof of identity. Many forms of signature do not contain or directly link to the identity of the person making them (such as clicking an "I Agree" button), or if they do provide evidence of identity, such identity may not be reliable (e.g., a typed name). Other security procedures may be used to accomplish this objective. The signer's identity may be authenticated as part of an overall process of obtaining access to a website or electronic resource that includes the record to be signed. If the act of signing is performed during the session authorized by the authentication process, the signature itself is attributed to the signer because the person accessing the record for signing has been duly authenticated.

E. There must be a means to preserve the integrity of the signed record. The usability, admissibility, and provability of a signed electronic record requires procedures be undertaken to ensure the continuing integrity of both the electronic record and its electronic signature following completion of the signing process. Data integrity is concerned with the accuracy and completeness of electronic information communicated over the internet or stored in an electronic system, and with ensuring that no unauthorized alterations are made to such information either intentionally or accidentally. Ensuring "integrity" requires "guarding against improper information modification or destruction, for the full retention period of the record. Electronic records are easily altered in a manner that is not detectable. In an electronic transaction of any significance, the parties to the transaction must be confident of the integrity of the information before they rely or act on the record.
[1.12.7.13 NMAC - N, 7/1/2015]

1.12.7.14 BUSINESS ANALYSIS AND RISK ASSESSMENT:

A. The selection of an electronic signature process is a business decision involving more than technical consideration. State agencies are strongly encouraged to complete and document a business analysis and risk assessment. The extent, level of detail, and format of the business analysis and risk assessment is up to the state agency. The goal is to implement a signing process that is reliable as is appropriate for the purpose in question.

B. A state agency may evaluate each factor differently and accord them different weights based on the nature and specifics of the underlying transaction. A state agency may also devise its own process for conducting and documenting a business analysis and risk assessment in the selection of an electronic signature process.

C. Business analysis. The focus of the business analysis is the business transaction that the electronic signature will support and the larger related business process. The business analysis may include the following components: overview of the business process, analysis of legal and regulatory requirement specifically related to the transaction, identification of industry standards or generally accepted practices related to the transaction, analysis of those who will use electronically signed records and related requirements, and determination of interoperability requirements including those of business partners, determination of the cost of alternative approaches.

D. Risk Assessment. The selection of an appropriate electronic signature process includes identifying the potential risks involved in a signed electronic transaction and how various electronic signature approaches can address those risks. This paragraph draws upon the national institute of standards (NIST) approach to risk assessment but is more narrowly focused on the risks inherent in a signed electronic transaction. To assess risks, a state agency should identify and analyze: sources of threats, vulnerabilities (such as repudiation, intrusion, loss of access to records for business and legal purposes), potential impacts (such as financial, reputation and credibility, productivity), and likelihood that a threat will actually materialize.

E. Risk Matrix. A state agency may wish to develop a matrix in which risk level for each threat is determined by the relationship between the threat's likelihood and the degree of impact against the background of existing risk reduction measures. The greatest risks are those that have extreme consequences and almost certain to occur. Conversely, a rare event with negligible consequences may be considered trivial.

F. Both the analysis of the likelihood of a successful challenge to the enforceability of a signature and the analysis of the cost or impact of an unenforceable signature should result in a "Low," "Moderate" or "High" determination.

G. The Department of Information Technology has statutory responsibility for all state-wide, executive agency information and computer systems. Given the specific and particular expertise of the Department, any state agency may defer to any determination made by the Secretary of the Department of Information and Technology as to 'business analysis', 'risk assessment', or constructing a 'risk matrix'.
[1.12.7.14 NMAC - N, 7/1/2015]

1.12.7.15 ELECTRONIC FORM OF SIGNATURE:

A. Low risk transactions.

(1) For low risk transactions, any form of signature is acceptable. This includes clicking an on-screen button, checking an on-screen box, typing ones name, using a PIN number, or any other reasonable method, so long as it is clear to the signer that such act constitutes a signature, and is not being done for any other purpose.

(2) Evidence of intent to sign may be included either in the record being signed or in the on-screen signing process. Shorter or more cursory indicators of intent may be used as necessary to facilitate the signing experience, so long as it is reasonably clear to the signer that they are signing the record, not doing something else.

(3) Any method may be used to associate the signature to the records being signed. This can include establishing a process that could not be completed unless a person has signed; using a process that appends the signature date to the record signed; or establishing a database-type link between the signature date and the records signed.

(4) Any approach to identification and authentication of the signer is acceptable. This includes self-assertion of identity by the signer. Successful authentication at this level requires that the signer prove through a secure authentication protocol that they possess and control the token. However, this level does not require cryptographic methods that block offline attacks. Refer to NIST Special Publication 800-63-2 for additional information related to electronic authentication guidelines.

(5) The system or application must be reasonably trusted to invalidate signature upon modification of the record and provide a secure method to transfer and store the signed record.

B. Moderate risk transactions.

(1) For moderate risk transactions, any electronic form of signature is acceptable. This includes clicking an on-screen box, typing ones name, using a PIN number, or any other reasonable method, so long as it is clear to the signer that such act constitutes a signature, and is not being done for any other purpose.

(2) Evidence of intent to sign may be included either in the records being signed or in the on-screen signing process. Clear evidence of intent to sign must be unmistakably provided. Shorter or more cursory indicators of intent should be avoided in favor of clear evidence of intent to facilitate the signing experience, so that it is very clear to the signer that they are signing the record.

(3) Any reasonable method may be used to associate the signature data to the records signed, or establishing a database-type link between the signature data and the records signed. The signing data can then be either attached or appended to the records signed, or a database-type link can be established between the signature data and the record signed.

(4) A single factor remote network authentication is acceptable for medium level risk transactions. There are a wide range of available authentication technologies that can be employed. For example, memorized secret tokens, pre-registered knowledge tokens, look-up secret tokens, out of band tokens and single factor one-time password devises are acceptable. This level requires cryptographic techniques and successful authentication requires that the signer prove through a secure authentication protocol that they control the token. Refer to NIST Special Publication 800-63-2 for additional information related to electronic authentication guidelines.

(5) The system or application must be reasonably trusted to invalidate signature upon modification of the record and provide a secure method to transfer and store the signed record.

C. High risk transactions.

(1) For high risk transactions, the only acceptable electronic form of signature is a cryptographically based digital signature created with a private cryptographic key that corresponds to the public key specified in a digital credential list.

(2) Evidence of intent to sign must be included both in the record being signed and in the on-screen signing process. Such evidence of intent to sign must be clearly provided in both places and make it unmistakable to the signer that they are signing the record and the reason that they are signing.

(3) A cryptographic signing process whereby a hash of the content of the record being signed is incorporated into the signature data must be used so there is an intrinsic relationship between the signature data and the record signed. The signing data can then be either attached or appended to the record signed, or a database-type link can be established between the signature data and the record signed.

(4) The signer must be identified and authenticated by reference to a digital certificate that provides at least two authentication factors or is based on proof of possession of a key through a cryptographic protocol.

(5) The system or application must be digitally signed using the identification and authentication specified in 1.12.7.15(4) NMAC that will invalidate signature upon modification of the record and provide a secure method to transfer and store the signed record.

[1.12.7.15 NMAC - N, 7/1/2015]

HISTORY OF 1.12.7 NMAC:

History of Repealed Material:
1 NMAC 3.2.70.2, Records - Information Technology Systems - Electronic Authentication, filed 4/1/97 - Repealed 7/1/15.