State of New Jersey
Circular Letter 01-01-ST:
UETA Guidance

Cover Letter

12 October 2001

CIRCULAR: 01-01-ST

ATTENTION: Heads of State and Local Government Agencies

SUBJECT: UETA Guidance

EXPIRATION DATE: Indefinite

INFORMATION: Albin Wagner, 609.530.3204

1. What is the purpose of this bulletin?

This bulletin transmits *Records Management Guidance for Agencies Implementing Electronic Signature Technologies* (Circular Letter 01-01-ST), which was developed by the Department of State, Division of Archives and Records Management (DARM) as mandated by Section 19 of the New Jersey *Uniform Electronic Transactions Act* (commonly known as UETA).

2. What is the background to this guidance?

UETA (P. L. 2001, c. 116), authorizes state and local government agencies in New Jersey, as of 26 June 2001, to use electronic forms, electronic filing, and electronic signatures to conduct official business with the public. In doing this, agencies will create records with business, legal, and in some cases, historical value. This guidance focuses on records management issues involving records that have been created using electronic signature technology.

Circular Letter 01-01-ST supplements other Division of Archives and Records Management (DARM) records management guidance, including, but not limited to:

- Guidance for agencies implementing image processing systems, as mandated by P. L. 1994, c. 140, promulgated by the Secretary of State in the Administrative Code as NJAC 15:3-4, *Image Processing of Public Records*, and NJAC 15:3-5, *Certification of Image Processing Systems*;
- N.J.A.C. 15:3-1 to 3, *Records Retention*;
- N.J.A.C. 15:3-6, *Storage of Public Records*;
- *New Jersey State Records Manual* (Trenton: Department of State, Division of Archives and Records Management, 1994); and
- *New Jersey Local Records Manual* (Trenton: Department of State, Division of Archives and Records Management, 1986).

3. How is DARM disseminating this guidance to state and local government agencies?

In addition to this Circular Letter, DARM will distribute copies of the guidance to agency records officers and chief information officers. Records management and information technology staff will need to work together to ensure that records requirements are addressed when implementing electronic signature technologies.

DARM staff members will summarize the guidance at several Records and Information Management Forums. The schedule for these meetings will be published on the DARM web site http://www.state.nj.us/state/darm. These meetings will afford an opportunity for interested agency personnel to ask questions and discuss the records management implications of UETA with DARM officials. To facilitate the discussion, participants may submit questions in advance via email to albin.wagner@sos.state.nj.us. Based on this discussion, DARM may develop additional guidance and training. Both records officers and information technology managers are invited to these meetings.

The guidance will also be available on the DARM web site at http://www.state.nj.us/state/darm

4. Is Further Information Available?

For further records management information and assistance, State and local agencies may contact the Bureau of Records Management, Division of Archives and Records Management by mail at P.O. Box 307, Trenton, NJ 08625-0307, e-mail at albin.wagner@sos.state.nj.us, telephone at 609.530.3200, or fax at 609.530.6121.

DEFOREST B. SOARIES, JR.
Secretary of State

KARL J. NIEDERER
Director, Division of Archives and Records Management

Attachment:
Circular 01-01-ST

Posted on Division of Archives and Records Management home page
URL: http://www.state.nj.us/state/darm

CIRCULAR: 01-01-ST

ATTENTION: Heads of State and Local Government Agencies

SUBJECT: UETA Guidance

EXPIRATION DATE: Indefinite

INFORMATION: Albin Wagner, 609.530.3204

Records Management Guidance for Agencies Implementing Electronic Signature Technologies

1.0 SUMMARY

The New Jersey *Uniform Electronic Transactions Act* (UETA), P. L.2001, c. 116, authorizes, with certain exceptions, state and local government agencies to use electronic forms, electronic filing, and electronic signatures to conduct official business with the public after 26 June 2001. An agency's decisions concerning how to adequately document program functions, its records management practices, and its risk assessment methodologies are essential and interrelated aspects of any electronic signature initiative. The following key points are discussed more fully in this guidance:

Agencies must consider records management requirements when implementing the *Uniform Electronic Transactions Act* (UETA), P. L. 2001, c. 116, as mandated by Sections 17 of the law (C. 12A:12-17). (See: Section 2.0)

Section 19 of UETA (C.12A:12-19) mandates the adoption of standards for electronic forms, electronic filing, and electronic signatures for governmental agencies by the Secretary of State.

If the electronically signed record needs to be preserved, whether for a finite period of time or permanently, then the agency needs to ensure its trustworthiness over time. (See: Section 4.0)

There are various approaches to ensure the trustworthiness of electronically-signed records. (See: Section 4.3)

Information systems that agencies use to implement the electronic signature requirements of UETA will produce new records or augment existing records. (See: Section 5.1.)

Agencies determine which electronic signature records to retain based on their operational needs and perceptions of risk. (See: Section 5.2)

Agencies are not authorized to dispose of records without an approved records disposition authorization from the State Records Committee. (See: Section 2.0)

Agencies should develop records schedules with proposed retention periods for new electronic records or records including electronic signatures with the assistance of DARM. The State Records Committee must review and approve retention and disposition schedules for any new records. Records retention and disposition schedules for existing records may need to be modified if electronic signatures are utilized. (See: Sections 5.1 and 5.4)

Electronically-signed records documenting legal rights and electronically-signed records that must be retained permanently have special considerations. (See: Sections 5.5 and 5.6)

When agencies use third party contractors they must include specific contract language to help ensure that records management requirements are met. (See: Section 5.3)

This guidance does not deal with issues associated with development and implementation of technologies used to generate electronic signatures. Development and implementation of such technologies are under the purview of the Office of Information Technology (OIT).

2.0 INTRODUCTION

2.1 UETA modifies federal E-Sign legislation.

The federal *Electronic Signatures in Global and National Commerce Act*, Pub. L. 106-229, 114 Stat. 464 (2000), popularly known as the " E-Sign Act," adopted by the U.S. Congress, encourages states to enact the *Uniform Electronic Transactions Act* (UETA) proposed for adoption by the National Conference of Commissioners on Uniform State Laws. The adoption of the UETA invokes the provisions of Section 102 of Pub. L. 106-229, which states that federal law will not preempt the laws of an enacting state relating to electronic transactions and electronic signatures. Section 102 of Pub. L. 106-229 provides that a state, in enacting UETA, may "modify, limit or supersede" the provisions of the federal law. The New Jersey Legislature declared in their adoption of UETA, per Section 22 (C.12A:12-22), that it was their intention that the legislation would modify, limit and supersede the provisions of Pub. L. 106-229 to the fullest possible extent permitted under the federal law.

2.2 Applicability of guidance to electronic records, signatures; exceptions

This guidance does not deal with issues associated with development and implementation of technologies used to generate electronic signatures. Development and implementation of such technologies are under the purview of the Office of Information Technology (OIT).

Circular Letter 01-01-ST supplements other Division of Archives and Records Management (DARM) guidance on records management, including, but not limited to:

a. Guidance for agencies implementing image processing systems, as mandated by P. L. 1994, c. 140, promulgated by the Secretary of State in the Administrative Code as NJAC 15:3-4, *Image Processing of Public Records*, and NJAC 15:3-5, *Certification of Image Processing Systems*;

b. N.J.A.C. 15:3-1 to 3, *Records Retention*;

c. N.J.A.C. 15:3-6, *Storage of Public Records*;

d. *New Jersey State Records Manual* (Trenton: Department of State, Division of Archives and Records Management, 1994); and

e. *New Jersey Local Records Manual* (Trenton: Department of State, Division of Archives and Records Management, 1986).

This guidance applies to any electronic record or electronic signature to the extent it is governed by a law other than those specified in Section 6 of UETA (C.12A:12-6).

Per Section 6 of UETA (C.12A:12-6), this guidance does not apply to a transaction to the extent it is governed by:

a. a law governing the creation and execution of wills, codicils or testamentary trusts;

b. the Uniform Commercial Code other than sections 1-107 and 1-206, Article 2 and Article 2A;

c. a statute, regulation or other rule of law governing adoption, divorce or other matters of family law.

Per Section 7 of UETA (C.12A:12-7), Legal effect and enforceability,

a. if a law requires a record to be in writing, an electronic record satisfies the law; and

b. if a law requires a signature, an electronic signature satisfies the law.

If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath,

a. Per Section 11 of UETA (C.12A:12-11), the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.

b. Section 18 and 19 of UETA (C.12A:12-18 and 19) requires the application of an equivalent electronic signature technology, such as PKI (public-private key) technology.

Per Section 5 of UETA (C.12A:12-5), Electronic record, signature not required

a. UETA does not require a record or signature to be created, generated, stored, sent, communicated, received, stored or otherwise processed or used by electronic means or in electronic form.

b. UETA applies only to transactions between parties, each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

Per Section 6 of UETA (C.12A:12-6), this guidance does not apply to:

a. court orders or notices or official court documents (including briefs, pleadings and other writings)
required to be executed in connection with court proceedings;

b. any notice of:

   1. the cancellation or termination of utility services (including water, heat and power);

   2. the default, acceleration, repossession, foreclosure or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;

   3. the cancellation or termination of health insurance benefits or life insurance benefits (excluding annuities); or

   4. the recall of a product, or material failure of a product, that risks endangering health or safety; or

c. any document required to accompany any transportation or handling of hazardous materials,
pesticides or other toxic or dangerous materials.

This guidance discusses the records management principles that apply to electronic signature technology generally. Per Section 18 of UETA (C.12A:12-18), electronic signatures should be accomplished by the most appropriate technology. The different available technologies include, but are not limited to, Personal Identification Number (PIN), digital signatures, smart cards and biometrics. Per Section 19 of UETA (C.12A:12-18), if additional records management guidance is necessary, DARM will provide assistance to agencies in selection of the appropriate electronic signature technology when developing a recordkeeping system.

2.3 Guidance on implementation of UETA

The *Uniform Electronic Transactions Act* (UETA), P. L.2001, c. 116, authorizes state and local government agencies in New Jersey to use electronic forms, electronic filing, and electronic signatures to conduct official business with the public after 26 June 2001. In doing so, agencies will create records with administrative, legal and, in some cases, historical value. This guidance focuses on records management issues involving records that have been created using electronic signature technology.

A sound records management program is an integral part of an agency's standard business operations. Agencies must consider records management requirements when implementing the provisions of UETA, or whenever they design or augment an electronic information system. State and local government agencies are required to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. This requirement applies to electronic records as well. Section 19 of UETA (C.12A:12-19) mandates the adoption of standards for electronic forms, electronic filing, and electronic signatures for governmental agencies by the

Secretary of State. Agencies that do not consistently adhere to standard records management practices run the risk of not having records that can be depended upon in the course of subsequent business transactions or activities.

This guidance is directed both toward agency records management personnel and information technology specialists who establish electronic signature systems and who may not be familiar with the records management implications. Good information technology practices complement or parallel good records management practices. In systems implemented as a result of the UETA, records management requirements will form the core of the IT system requirements. In implementing electronic signature technologies, IT professionals need to be aware that signatures are an integral part of a record. If the record needs to be preserved, whether for a finite period of time or permanently, then the agency needs to ensure the trustworthiness of the electronically-signed record over time.

The State Records Committee, established pursuant to P. L. 1953, c.410 (N.J.S.A. 47:3-16), must approve the disposition of state and local government records by means of a DARM-approved *Request and Authorization for Records Disposal*, as authorized by an approved records retention schedule before agencies can destroy them. New information systems or records series that have not been scheduled (i.e. do not have a records disposition authority) need to be appraised by DARM. Agency records management staff should contact DARM to begin the scheduling process. DARM will assist agencies with the review and approval of new or revised retention schedules by the State Records Committee. Further information on scheduling records and DARM records management guidance is available on the DARM web site http://www.state.nj.us/state/darm and in DARM publications. See Appendix B for further information about DARM's records management programs and services.

3.0 BACKGROUND

3.1 Records Life Cycle vs. System Development Life Cycle

The terms "records life cycle" and "system development life cycle" are important concepts that are sometimes confused in information technology and records management discussions.

Records life cycle: The records life cycle is the life span of a record from its creation or receipt to its final disposition. It is usually described in three stages: creation, maintenance and use, and final disposition. Much of this guidance deals with the creation stage because the electronic signature record is created during the first stage of the records life cycle. The second stage, maintenance and use, is the portion of the records life cycle in which the record is either maintained at the agency while in active use, or is maintained off-line when use is less frequent. The final stage of the records life cycle is disposition, which describes the ultimate fate of the record. State and local government records are categorized as having either a "temporary" or "permanent" disposition status. Temporary records are held by agencies for specified time periods before they are destroyed or deleted. Permanent records are first held by agencies and

then legally transferred to the State Archives. Electronically-signed records may be either temporary or permanent. The eventual disposition of electronically-signed records is subject to negotiation between the agency and DARM, but agencies are not authorized to dispose of records without approval from DARM per N.J.A.C. 15:3-2.6-2.8 and N.J.A.C. 15:3-3.1-3.7, as mandated by N.J.S.A. 47:3-1 to 6.

System development life cycle: The "system development life cycle" describes the phases of development of an electronic information system. These phases typically include initiation, definition, design, development, deployment, operation, maintenance, enhancement, and retirement. A significant step in several of the stages is the definition, development, and refinement of the data model that includes treatment of the records being created or managed. Information systems developed according to system development methodologies, including those that agencies use to implement the electronic signature requirements of UETA, will produce new records or augment existing records.

The records life cycle often exceeds the system development life cycle. When it does, the agency needs to retain the record for a period of time longer than the life of the electronic information system that generated the electronic signature. This presents special challenges, such as maintaining the trustworthiness of the record when migrating from one system to another.

4.0 TRUSTWORTHY RECORDS

4.1 Characteristics of Trustworthy Records

Reliability, authenticity, integrity, and usability are the characteristics used to describe trustworthy records from a records management perspective. An agency needs to consider these characteristics when planning to implement an electronic signature technology so that it can meet its internal business and legal needs, and external regulations or requirements. The degree of effort an agency expends on ensuring that these characteristics are attained is dependent on the agency's business needs or perception of risk. (See: Section 5.2 for a discussion of risk assessment.) Transactions that are critical to the agency business needs may need a greater assurance level that they are reliable, authentic, maintain integrity and are usable than transactions of less critical importance. For guidance on whether records are trustworthy for legal purposes, consult your attorney or legal counsel.

> **Reliability:** A reliable record is one whose content can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests and can be depended upon in the course of subsequent transactions or activities.
>
> **Authenticity:** An authentic record is one that is proven to be what it purports to be and to have been created or sent by the person who purports to have created and sent it.

A record should be created at the point in time of the transaction or incident to which it relates, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

To demonstrate the authenticity of records, agencies should implement and document policies and procedures which control the creation, transmission, receipt, and maintenance of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, and alteration.

Integrity: The integrity of a record refers to it being complete and unaltered.

It is necessary that a record be protected against alteration without appropriate permission. Records management policies and procedures should specify what, if any, additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation or addition to a record made after it is complete should be explicitly indicated as annotations or additions.

Another aspect of integrity is the structural integrity of a record. The structure of a record, that is, its physical and logical format and the relationships between the data elements comprising the record, should remain physically or logically intact. Failure to maintain the record's structural integrity may impair its reliability and authenticity.

Usability: A usable record is one which can be located, retrieved, presented, and interpreted. In any subsequent retrieval and use, the record should be capable of being directly connected to the business activity or transaction which produced it. It should be possible to identify a record within the context of broader business activities and functions. The links between records which document a sequence of activities should be maintained. These contextual linkages of records should carry the information needed for an understanding of the transaction that created and used them.

4.2 Preserving Trustworthy Records

For a record to remain reliable, authentic, with its integrity maintained, and useable for as long as the record is needed, it is necessary to preserve its content, context, and sometimes its structure. A trustworthy record preserves the actual content of the record itself and information about the record that relates to the context in which it was created and used. Specific contextual information will vary depending upon the business, legal, and regulatory requirements of the business activity (e.g., issuing land use permits). It also may be necessary to preserve the structure or arrangement of its parts. Failure to preserve the structure of the record will impair its structural integrity. That, in turn, may undermine the record's reliability and authenticity.

There are special considerations when dealing with the preservation of the content, context, and structure of records that are augmented by electronic signatures:

Content: The electronic signature or signatures in a record are part of the content. They indicate who signed a record and whether that person approved the content of the record. Multiple signatures can indicate initial approval and subsequent concurrence. Signatures are often accompanied by dates and other identifiers such as organization or title. All of this is part of the content of the record and needs to be preserved. Lack of this information seriously affects a document's reliability and authenticity.

Context: Some electronic signature technologies rely on individual identifiers that are not embedded in the content of the record, trust paths, and other means to create and verify the validity of an electronic signature (See: Section 5.1). This information is outside of the content of the record, but is nevertheless important to the context of the record as it provides additional evidence to support the reliability and authenticity of the record. Lack of these contextual records seriously affects one's ability to verify the validity of the signed content.

Structure: Preserving the structure of a record means its physical and logical format and the relationships between the data elements comprising the record remain physically and logically intact. An agency may determine that it is necessary to maintain the structure of the electronic signature. In that case it is necessary to retain the hardware and software that created the signature (e.g., chips or encryption algorithms) so that the complete record could be revalidated at a later time as needed.

4.3 What approaches are available to agencies to ensure the trustworthiness of electronically-signed records over time?

There are various approaches agencies can use to ensure the trustworthiness of electronically-signed records over time. Agencies may choose an approach that is practical for them and will fit their business needs and risk assessment per Section 18 of UETA (C.12A:12-18). Per Section 19 of UETA (C.12A:12-18), DARM will provide agencies assistance in this process. Below is a discussion of two different approaches that agencies have used.

One approach: An agency may choose to maintain adequate documentation of the records' validity, such as trust verification records, gathered at or near the time of record signing. This approach requires agencies to retain contextual information to adequately document the processes in place at the time the record was electronically-signed, along with the electronically-signed record itself. The additional contextual information must be retained for as long as the electronically-signed record is retained. Thus the agency preserves the signature's validity and meets the adequacy of documentation requirements by retaining the contextual information that documented the validity of the electronic signature at the time the record was signed.

Maintaining adequate documentation of validity gathered at or near the time of record signing may be preferable for records that have permanent or long-term retention since it is less dependent on technology and much more easily maintained as technology

evolves over time. However, using this approach, the signature name may not remain readable over time because of bit-wise deterioration in the record or as a result of technological obsolescence. Agencies must ensure that for permanent records the printed name of the signer and the date when the signature was executed be included as part of any human readable form (such as electronic display or printout) of the electronic record.

Another approach: An agency may choose to maintain the ability to re-validate digital signatures. The re-validation approach requires agencies to retain the capability to revalidate the digital signature, along with the electronically-signed record itself. The information necessary for revalidation (i.e., the public key used to validate the signature, the certificate related to that key, and the certificate revocation list from the certificate authority that corresponds to the time of signing) must be retained for as long as the digitally-signed record is retained. Both contextual and structural information of the record must be retained, as described in Section 4.2.

This approach is potentially more burdensome, particularly for digitally-signed records with long retention needs, due to issues of hardware and software obsolescence. If an agency chooses this approach for permanent records, it must contact DARM to discuss what they will need to do to transfer the records to DARM. As in the first approach, the agency must ensure that the printed name of the electronic signer and the date when the signature was executed be included as part of any human readable form (such as electronic display or printout) of the electronic record.

Special considerations for records documenting legal rights and records that must be retained permanently are discussed in Sections 5.5 and 5.6, respectively.

Non-repudiation: Irrespective of the approach an agency takes, some form of technical non-repudiation services must be implemented to protect the reliability, authenticity, integrity, and usability, as well as the confidentiality, and legitimate use of electronically-signed information. Non-repudiation is one of the essential security services in computing environments, being mainly applied in message handling systems and electronic commerce. The non-repudiation services that are being used in e-commerce can also be used in ascertaining the reliability of electronically-signed records. Non-repudiation services provide irrefutable evidence that an action took place. The services protect one party to a transaction (e.g., electronically signing a record) against the denial of the other party that a particular event or action took place. The services also provide safeguards that protect all parties from a false claim that a record was tampered with or not sent or received.

There are multiple frameworks for non-repudiation and agencies will choose the framework that matches their needs. One possible framework is the ISO (International Organization for Standardization) non-repudiation model (Non-repudiation - Part 1: General Model, ISO/IEC JTC1/SC27 N1503, November 1996; Non-repudiation - Part 2: Using symmetric techniques,

ISO/IEC JTC1/SC27 N1505, November 1996). The essential elements of the ISO model are listed below:

a. **Evidence of the Origin of the Message & Verification:** This shows that the originator created the message (electronically-signed record). The sender (person signing the record electronically) has to create a proof-of-origin certificate using the non-repudiation service. The electronically-signed record can be sent to another party (receiver of the electronically-signed record or another application for further processing) using the non-repudiation delivery authority service. The receiver has to store this evidence using the non-repudiation storage service. In case of dispute, the sender can later retrieve this evidence.

b. **Evidence of Message Receipt:** This proves that the message (electronically-signed record) was delivered. The recipient must create and send a proof of receipt certificate using non-repudiation delivery authority service. The sender receives this evidence and stores it using the non-repudiation storage service; it can later be retrieved if there is a dispute.

c. **Transaction Timestamp:** This timestamp is generated by the non-repudiation service as part of the evidence that an event or action took place.

d. **Long-term Storage Facility:** This is used to store the certificates of origin and receipt. If there is a dispute, the adjudicator uses this storage facility to retrieve the evidence. Depending on the length of storage, it might be necessary to address software and hardware migration concerns as part of the design of this facility.

e. **The Adjudicator:** The adjudicator is used to settle disputes based on stored evidence if either the sender or the receiver of electronically-signed records makes false claims.

Modified from: Orfali, Robert, Harkey, Dan, & Jeri Edwards. Client-Server Survival Guide. John Wiley & Sons: New York, 1999, p. 144.

4.4 What steps should agencies follow to ensure that electronically-signed records are trustworthy?

To create trustworthy records with electronic signatures an agency should:

a. create and maintain documentation of the systems used to create the records that contain electronic signatures;

b. ensure that the records that include electronic signatures are created and maintained in a secure environment that protects the records from unauthorized alteration or destruction;

c. implement standard operating procedures for the creation, use, and management of records that contain electronic signatures and maintain adequate written documentation of those procedures;

d. create and maintain records according to these documented standard operating procedures.

e. train agency staff in the standard operating procedures.

f. obtain official disposition authorization from DARM for both the records that contain electronic signatures and for the associated records that are necessary for trustworthy records (See: Section 4.0). Per N.J.S.A. 47:3-3, having official disposition authorization will assist the agency when faced with demands to produce records that have been destroyed according to these authorities.

5.0 OTHER RECORDS MANAGEMENT ISSUES

5.1 What new records may be created by electronic signature technology?

Agency decisions to accept or create electronically-signed records will generate new types of associated records. Agencies must identify the content, context, and structure of records with electronic signatures and determine what they will need to preserve to have trustworthy records for the agency's purposes. The following list includes many of the records that might be associated with an electronic signature initiative. These records need to be scheduled (have records retention and disposition schedules approved by the State Records Committee) in coordination with the electronically-signed records to which they relate.

a. **Documentation of individual identities:** Information the agency uses to identify and authenticate a particular person as the source of an electronically-signed record. Examples of this would be a pin number or digital certificate assigned to an individual. This information may be passed to individuals via written correspondence, and do not necessarily appear in the electronically-signed record. Depending on method of implementation, this is either content or context.

b. **Electronic signatures:** A method of signing an electronic document that identifies and authenticates a particular person as the source of the message and indicates such person's approval of the information contained in the electronic message. The electronic signature may be embedded in the content of the record, or it may be stored separately. If an electronic signature technology separates the signature from the rest of the record, it must be associated in some way and captured in the recordkeeping system to preserve the complete content of the record.

c. **Trust verification records:** Records that the agency deems necessary to document when and how the authenticity of the signature was verified. An example of this would be

an Online Certificate Status Protocol (OCSP) or other response from a Certificate Authority server. This is context information.

d. **Certificates:** The electronic document that binds a verified identity to the public key that is used to verify the digital signature in public key infrastructure implementations. This is context information.

e. **Certificate Revocation List:** In public key infrastructure implementations, a list of certificates that a Certificate Authority has revoked at a particular time. When a Certificate Authority places a certificate on a revocation list, an agency application may reject the digital signature. This is context information.

f. **Trust paths:** In public key infrastructure implementations, a chain of certificates of trusted third parties between parties to a transaction which ends with the issuance of a certificate that the relying party trusts. The trust path is one of the data necessary for validation of a received digital signature. This is context information.

g. **Certificate policy:** In public key infrastructure implementations, a set of rules that defines the applicability of a certificate to a particular community and/or class of application with common security requirements. This is context information.

h. **Certificate practice statements:** In public key infrastructure implementations, a certification authority's statement of practice for issuing certificates. This is context information.

i. **Hashing/encryption/signing algorithms:** Software for generating computational calculations used to create or validate digital signatures. This is structure information.

5.2 How do agencies determine which of these electronic signature records to retain?

Agencies establish records management practices based on their operational needs and perceptions of risks. Operational needs are determined on the basis of the approach taken to ensuring the trustworthiness of electronically-signed records over time (See: Section 4.3). Risk assessment and risk mitigation, along with other methodologies, are used to establish documentation requirements for agency activities.

A risk assessment should consider the possible consequences of lost or unrecoverable records, including the legal risk and financial costs of potential losses, the likelihood that a damaging event will occur, and the costs of taking mitigating actions. Risk is defined here, from a records management perspective, as:

a. a risk of challenge to the records (e.g., legal challenge) that can be expected over the life of the
record, and

b. the degree to which the agency or citizens would suffer loss if the trustworthiness of

the electronically-signed records could not be adequately documented.

Risk assessment also can be applied to records of electronic signature programs to determine the level of documentation required for signature validation. The concepts of reliability, authenticity, integrity, and usability as discussed in Section 4.1, may help agencies establish criteria for the types of electronic signature-related records they need to retain to document their programs.

5.3 Transferring electronic signature record material from contractors to agencies

As state and local governments begins to interact with citizens electronically, agencies may employ third party contractors to integrate electronic signature technology into their business processes. Use of a third party contractor does not relieve an agency of its obligation to provide adequate and proper documentation of electronic signature record material. When agencies use third party contractors they must use specific contract language to help ensure that records management requirements are met. It may be necessary for agencies to make special provisions for obtaining electronic signature record material from third parties or to ensure that the third parties adhere to the records schedule retention requirements.

5.4 When must an agency modify its records schedule to cover electronic signature records?

Records schedules are the business rules that describe the types of records an agency produces and the retention periods for those records. Records schedules need to be modified when:

a. new records, such as those listed in Section 5.1, are created;

b. the agency determines that incorporation of an electronic signature into a record will result in changes to the retention period for that record; or

c. incorporation of the electronic signature and/or resulting parallel changes in the work process significantly changes the character of the record.

DARM will provide agency records officers with specific guidance on scheduling. If an agency is applying electronic signature technology to records scheduled for permanent retention, please contact DARM. (See: Appendix B)

5.5 Special considerations relating to long-term, electronically-signed records that preserve legal rights.

When implementing electronic signature technology, agencies should give special consideration to the use of electronic signatures in electronic records that preserve legal rights. Because long-term temporary and permanent electronically signed records have greater longevity than typical

software obsolescence cycles, it is virtually certain that agencies will have to migrate those records to newer versions of software to maintain access. The software migration (as opposed to media migration) process may invalidate the digital signature embedded in the record. This may adversely affect an agency's ability to recognize or enforce the legal rights documented in those records.

5.6 DARM requirements for permanent, electronically-signed records

For permanent records, agencies must ensure that the printed name of the electronic signer, as well as the date when the signature was executed, be included as part of any human readable form (such as electronic display or printout) of the electronic record. This is requirement so that the name of the signer will be preserved as part of the record.

Note: Circular Letter 0101-ST was modeled upon NARA Bulletin 2001-02, *Records Management Guidance for Agencies Implementing Electronic Signature Technologies,* which was developed by the National Archives and Records Administration (NARA) in response to the federal *Government Paperwork Reduction Act* (Pub. L. 105-277).

DEFOREST B. SOARIES, JR.
Secretary of State
Management

KARL J. NIEDERER
Director, Division of Archives and Records

APPENDIX A: Key Terms and Definitions

Note: Many of these definitions are taken from the *Uniform Electronic Transactions Act* (UETA), P. L. 2001, c. 116, and Lewis J. Bellardo and Lynn Lady Bellardo, comps., *A Glossary for Archivists, Manuscript Curators, and Records Managers*, Archival Fundamentals Series (Chicago: The Society of American Archivists, 1992).

Agreement: The bargain of the parties in fact, as found in their language or inferred from other circumstances, and from rules, regulations and procedures given the effect of agreement under laws otherwise applicable to a particular transaction. (UETA)

Appraisal: The process of determining the value and thus the disposition of records (i.e., designating them temporary or permanent) based upon their current administrative, legal, and fiscal use; their evidential and informational value; their arrangement and condition; their intrinsic value; and their relationship to other records. (SAA Glossary)

Authenticity: An authentic record is one that is proven to be what it purports to be and to have been created or sent by the person who purports to have created and sent it.

Automated transaction: A transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract or fulfilling an obligation required by the transaction. (UETA)

Certificate Authority [CA]: As part of a public key infrastructure, an authority in a network that issues and manages security credentials and public keys for message encryption and decryption.

Content: The information that a document is meant to convey (SAA Glossary). Words, phrases, numbers, or symbols comprising the actual text of the record that were produced by the record creator.

Context: The organizational, functional, and operational circumstances in which documents are created and/or received and used (SAA Glossary). The placement of records within a larger records classification system providing cross-references to other related records.

Documentation: 1. In archival usage, the creation or acquisition of documents to provide evidence of the creator, an event, or an activity. 2. In electronic records, an organized series of descriptive documents explaining the operating system and software necessary to use and maintain a file and the arrangement, content, and coding of the data which it contains. (SAA Glossary)

Electronic record: A record created, generated, sent, communicated, received or stored by electronic means. (UETA) See also: definition of "Record."

Electronic signature: A technologically neutral term indicating various methods of signing an electronic message that (a) identify and authenticate a particular person as source of the electronic message; and (b) indicate such person's approval of the information contained in the electronic message (UETA). Examples of electronic signature technologies include PINs, user identifications and passwords, digital signatures, digitized signatures, and hardware and biometric tokens.

General records schedule: A records schedule governing specified series of records common to several or all agencies or administrative units of a corporate body (SAA Glossary). The DARM General Records Schedules (GRS) provide disposition authority by the State Records Committee for administrative records common to several or all agencies of the state and local government.

Governmental agency: An executive, legislative or judicial agency, department, board, commission, authority, institution or instrumentality of the state government or of a county, municipality, or other political subdivision of the state. (UETA)

Integrity: The integrity of a record refers to its being complete and unaltered.

Non-repudiation: Steps taken by an agency to provide assurance, via the use of an audit trail, that a sender cannot deny being the source of a message, and that a recipient cannot deny receipt of a message.

Online Certificate Status Protocol [OCSP]: A draft Internet communications protocol of the IETF X.509 PKI Working Group that is useful in determining the current status of a digital certificate without requiring certificate revocation lists.

Public Key Infrastructure [PKI]: An IT infrastructure that enables users of a basically unsecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Record: Any paper, written or printed book, document or drawing, map or plan, photograph, microfilm, data processed or image processed document, sound-recording or similar device, or any copy thereof which has been made or is required by law to be received for filing, indexing, or reproducing by any officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received by any such officer, commission, agency or authority of the State or of any political subdivision hereof, including subordinate boards thereof, in connection with the transaction of public business and has been retained by such recipient or its successor as evidence of its activities or because of he information contained therein. (N.J.S.A. 47:3-16)

Recordkeeping System: A manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

Records Schedule: A document describing records of an agency, organization, or administrative unit, establishing a timetable for their life cycle, and providing authorization for their disposition (SAA Glossary), i.e., off-site storage followed by destruction or transfer to the State Archives.

Record Series: File units or documents arranged in accordance with a filing system or maintained as a unit because they result from the same accumulation or filing process, the same function, or the same activity; have a particular form; or because of some other relationship arising out of their creation, receipt, or use. (SAA Glossary)

Reliability: A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities, or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

Re-validation: Re-confirming the validation process for a previously validated electronic signature.

Structure: The physical and logical format of a record and the relationships between the data elements.

Transaction: An action or set of actions occurring between two or more persons relating to the conduct of business, commercial or governmental affairs. (UETA)

Usability: A useable record is one which can be located, retrieved, presented and interpreted.

Validation: The process by which a message/record is confirmed to have originated from an authenticated network user, that is, one who has appropriately established his/her identity on the network.

APPENDIX B: FOR FURTHER INFORMATION AND ASSISTANCE

In addition to the policy guidance available from the agency's records officer and legal counsel, records management assistance is available to state and local government agencies through several DARM offices and programs. Agencies will find the most current list of DARM records management contacts and programs posted on the DARM Records Management web page at: http://www.state.nj.us/state/darm Records management policy and guidance and links to State and local government regulations, records management publications, Circular Letters, and other valuable resources are also available through the DARM web site.

The Bureau of Records Management receives and reviews all records disposition requests submitted to DARM by state and local government agencies and provides records management training open to all state and local government employees. The bureau is organized into six workgroups, each of which is assigned responsibilities for specific state and local government Agencies. This liaison structure ensures that agencies will be able to discuss their records issues with someone who is familiar with their agency and their records. The list of workgroups and agency assignments is available by contacting DARM or consulting the DARM web site at: http://www.state.nj.us/state/darm/recman.html. The schedule of records management training classes is also available from the Bureau.

Agencies may write or call for further information about DARM's records services at:

Bureau of Records Management
Division of Archives and Records Management
P.O. Box 307
Trenton, NJ 08625-0307

E-mail: albin.wagner@sos.state.nj.us
Telephone: 609.530.3200
Fax: 609.530.6121