The National Electronic Commerce
Coordinating Council

Management of Electronic Transactions and Signed Records

Presented at the NECCC Annual Conference, December 4-6, 2002, New York, NY

NATIONAL ELECTRONIC COMMERCE COORDINATING COUNCIL

In 1997, as the use of the Internet was increasing at a stunning rate, a group of public and private professionals—government executives and information technology practitioners—met in San Antonio, Texas to discuss their common issues, problems and ideas. This first meeting was productive. Participants learned from each other. They felt that continuing to meet as a group would help them meet the challenges and opportunities posed by the rush of engulfing information technologies. This founding group formed the National Electronic Commerce Coordinating Council (NECCC), which has continued to meet regularly.

Today, NECCC serves as an alliance of government organizations dedicated to promoting electronic government through the exploration of emerging issues and best practices. Alliance partners are the National Association of State Auditors, Comptrollers and Treasurers; the National Association of Secretaries of State NASS; and the National Institute of Governmental Purchasing.

NECCC also works in partnership with these affiliate organizations: the Information Technology Association of America; National Automated Clearing House Association; National Association of Government Archives and Records Administrators; and National Association of State Treasurers

ACKNOWLEDGEMENTS

Charles Arp
Martha Combs – Chair
Bruce Garner
Jerry Johnson
Alan Kowlowitz
Mark LaVigne
Roselyn Marcus
Renee Mauzy
John Messing
Dino Tsbouris
Amelia Winstead

CONTACT INFORMATION

The National Electronic Commerce Coordinating Council
2401 Regency Road, Suite 302
Lexington, KY 40503
P: (859) 276-1147
F: (859) 278-0507
www.ec3.org

2002 NECCC EXECUTIVE BOARD

Signatory Members

Chair, *J. Kenneth Blackwell*, NASS, Secretary of State, Ohio
Vice Chair, *Ralph Campbell, Jr.*, NASACT, State Auditor, North Carolina
Secretary/Treasurer, *Mary Kiffmeyer*, NASS, Secretary of State, Minnesota

Steve Adams, NASACT, State Treasurer, Tennessee
David Dise, NIGP, Procurement Manager, Fairfax County Water Authority, Virginia
Rick Grimm, NIGP, NIGP Chief Executive Officer, Virginia
Stephen Gordon, NIGP, Purchasing Agent, Metropolitan Govt. of Nashville/Davidson County, Tennessee
Elaine Marshall, NASS, Secretary of State, North Carolina
Robert Childree, NASACT, State Comptroller, Alabama

Affiliate Members

P.K. Agarwal, ITAA, CIO and Executive Vice President, National Information Consortium
William Kilmartin, NACHA, Vice President, Accenture
Jack Markell, NAST, State Treasurer, Delaware
Amelia Winstead, NAGARA, State and Local Government Services Manager, Office of the Secretary of State, Georgia

Ex-Officio Members

Carolyn Purcell, CIO, Department of Information Resources, Texas
Basil Nikas, CEO, iNetPurchasing
J.D. Williams, Director, State and Local Government, PeopleSoft, USA, Inc.

At-Large Members

Avi Duvdevani, CIO/Deputy General Manager, New York
Daniel Greenwood, Director, MIT E-Commerce Architecture Program, Massachusetts Institute of Technology
David Lewis, Retired Director and CIO, Massachusetts
Jay Maxwell, Senior Vice President, AAMVA
Eric Reeves, State Senator, North Carolina
David Temoshok, PKI Program Manager, Government Services Administration
Costis Toregas, CEO, Public Technology, Inc.
Susan Hogg, Chief, Statewide e-Government Initiatives Office

This page left blank intentionally.

Table of Contents

This page left blank intentionally.

EXECUTIVE SUMMARY

The need to preserve transactions and electronically-signed records over time, whether for a defined period or permanently, presents special challenges to state agencies. This document is intended to provide guidance for state agencies concerning the risks involved in the creation and maintenance of transactions and signed electronic records, and issues to consider when determining how such records should be retained over time.

This document is organized as follows:

INTRODUCTION

A sound records management program must be considered an integral part of a state agency's standard business and information resource management activities. Agencies must consider records management requirements whenever they design or augment an electronic information system.

It is crucial for state agencies to perform an assessment of the risks that are associated with various categories of records that may exist in electronic form. Such an assessment requires an understanding of the nature of the records involved and of the principles and means of retaining records.

NOTE: This guidance does not deal with records management issues associated with the electronic systems used to generate electronic records or electronic signatures.

PART 1: ELECTRONIC TRANSACTIONS AND SIGNED RECORDS

1.1 Electronic Records

UETA provides definitions for several key terms that pertain to this guideline document. Some of those definitions are set out below.

Electronic means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

Electronic record means a record created, generated, sent, communicated, received, or stored by electronic means.

Record means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

Transaction means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

1.2 Electronic Signatures

Electronic signature, as defined in UETA, means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

Digital signature is one type of electronic signature. Digital signature is generally accepted as an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature.

Digital certificate is the result of authentication by a certificate authority. This is properly part of a PKI implementation.

Electronic signatures may be accomplished by several different technologies, such as Personal Identification Number (PIN), digital signatures, smart cards and biometrics. And within different technologies, there may be differentiations that impact the maintenance and preservation of the digital signature and record. For example, digital signature is one technology with significant subcategory considerations. Digital signatures may be enveloping, enveloped or detached. When enveloping, they encompass the signed data. When enveloped, they reside within the signed data. When detached, they are separate from the data and may reside in a database or XML document separate from the signed data. All possible requirements of the document and signature need to be considered before a specific technology can be chosen.

Electronic signatures often involve the creation of new records in addition to the electronic record that has been signed. These new records must also be retained as a part of a state agency's records retention program.

1.3 Trustworthy Records

Trustworthy records are **reliable, authentic,** have maintained their **integrity,** and are **usable.** Each of these terms is discussed below. The degree of effort an agency expends on creating or maintaining trustworthy records depends on the agency's business needs or perception of risk. 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. Notwithstanding, this discussion does not apply to the issue of whether an electronic record is usable in a legal proceeding. Consequently, for guidance on whether signed electronic records are useable for a particular legal purpose or in a legal proceeding, consult your agency's legal counsel. Where a second paragraph appears there are identified considerations of procedural policy or standards that apply to each subcategory of trustworthy records.

Reliable records are records whose content 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.

Authentic records are records that are proven to be what they purport to be, and to have been created or sent by the person who purports to have created and sent them.

To demonstrate the authenticity of records, agencies should implement and document policies and procedures that control the creation, transmission, receipt, and maintenance of records. These policies and procedures should ensure that records creators have been authorized and identified.

Records that have integrity are records that are complete and have not been altered. Records must 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. The structural integrity of records must also be maintained. The physical and logical format of the record and the relationships between the data elements comprising the record should remain intact. The policies and procedures should ensure that records have been protected against unauthorized addition, deletion and alteration; therefore they must include an audit trail of any changes to records. Failure to maintain the record's structural integrity may impair its reliability and authenticity.

Usable records are records that 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.

Steps to follow to ensure that electronically signed records are trustworthy.

To create trustworthy records with electronic signatures an agency should:

- Create and maintain documentation of the systems used to create the records that contain electronic signatures.
- 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.
- Implement standard operating procedures for the creation, use, and management of records that contain electronic signatures and maintain adequate written documentation of those procedures.
- Create and maintain records according to these documented standard operating procedures.
- Train agency staff in the standard operating procedures.
- Use audit trails to indicate changes.
- Keep an electronically "locked" version of the original document. Records may be locked by various methods, such as assigning "read-only" attributes to a document, digitally signing the data, or encrypting it.
- When systems change, either maintain the original hardware, software and documentation or translate the document into a form readable by the new system. Alternatively, XML syntax to describe the records and the reliability of the methods for signing is being studied by one or more standards bodies and new methods may emerge shortly to enable preserving the information without having to maintain the original tools used to create and read the records or their signatures.

PART 2: RISKS PERTAINING TO ELECTRONIC TRANSACTIONS AND SIGNED RECORDS

2.1 Common Types of Risks

Common risks pertaining to electronic records and signatures may include:

(1) The risk of legal or other challenge to the records that can be expected over the life of the record.

(2) The degree to which the agency or citizens would suffer loss if the trustworthiness of the electronically signed records could not be adequately documented.

Some Risk factors to Consider

In determining whether electronic records or electronic signatures may be sufficiently reliable for a particular purpose, state agencies should consider the ***relationships between the parties***, the ***value of the transaction***, the ***risk of intrusion***, and the likely ***need for accessible, persuasive information*** regarding the transaction at some later date. In addition, state agencies should consider any other risks relevant to the particular process or transaction. Once these factors are considered separately, an agency should also consider them collectively to evaluate the overall sensitivity to risk of a particular process.

Relationships Between Parties

Agency transactions may be grouped into several general categories, each of which may be vulnerable to differing security risks:

- Intra-agency transactions (i.e., those which remain within the same state agency).
- Inter-agency transactions (i.e., those between state agencies).
- Transactions between a state agency and local governments.
- Transactions between a state agency and a private organization, such as contractors, businesses, universities, non-profit organizations, or other entities.
- Transactions between a state agency and a member of the general public.
- Transactions between a state agency and the federal government.

Ongoing relationships. Risks tend to be relatively low in cases where there is an ongoing relationship between the parties. Generally speaking, there will be little risk of a partner later repudiating inter- or intra-governmental transactions of a relatively routine nature.

Other types of transactions involving an ongoing relationship between an agency and non-governmental entities can have varying degrees of risk, depending on the nature of the relationship between the parties. The same may be true in circumstances where state

programs involve an ongoing relationship between entities that are acting on behalf of an agency and such non-governmental entities.

One-time transactions. On the other hand, the highest risk of fraud or repudiation is for a one-time transaction between a person and an agency that has legal or financial implications. In all cases, the relative value of the transaction needs to be considered as well.

Value of the Transaction

Agency transactions may be grouped into categories, each of which may be vulnerable to different security risks. Categories may include:

- Transactions involving the transfer of funds.
- Transactions where the parties commit to actions or contracts that may give rise to financial or legal liability.
- Transactions involving information protected under state or federal privacy law.
- Transactions where the party is fulfilling a legal responsibility, which, if not performed, creates a legal liability (criminal or civil).
- Transactions where no funds are transferred, no financial or legal liability is involved and no privacy or confidentiality issues are implicated.

Agency risk analyses should attempt to identify the type of transaction being automated, the value of the transaction to each of the participants and the legal requirements involved in supporting the transaction to determine what type of electronic signature or authentication is required. Where authentication is necessary, the method of electronic signature should be appropriate to the level of risk.

Risk of Intrusion

The probability of a security intrusion on the transaction can depend on the benefit to the potential attackers and their knowledge that the transaction will take place. Agency transactions may include:

Regular or periodic transactions between parties. These may pose a higher risk than intermittent transactions because of their predictability, causing higher likelihood that an outside party would know of the scheduled transaction and be prepared to intrude on it.

High-value transactions. The value of the information to outside parties could also determine their motivation to compromise the information. Information relatively unimportant to an agency may have high value to an outside party.

Nature of the state agency's mission. Certain agencies, because of their perceived image or mission, may be more likely to be attacked independent of the information or transaction. The act of disruption can be an end in itself.

Need for Information at a Later Point

Agency transactions may include:

- Transactions where the information generated will be used for a short time and discarded;
- Transactions where the information generated may later be subject to audit or compliance;
- Transactions where the information will be used for research, program evaluation, or other statistical analyses;
- Transactions where the information generated may later be subject to dispute by one of the parties (or alleged parties) to the transaction;
- Transactions where the information generated may later be subject to dispute by a non-party to the transaction;
- Transactions where the information generated may later be needed as proof in court;
- Transactions where the information generated will be archived later as permanently valuable records.

When analyzing the benefits of converting from paper systems to electronic systems, agencies should reflect on what information would be lost in the conversion, e.g., an envelope containing a postmark and the sender's fingerprints and handwriting. Agencies should determine whether collecting the potentially lost information is truly important and whether an electronic system could cost-effectively collect and store similarly useful information.

In some paper transactions requiring a party's signature, the signature both identifies the party and establishes that party's intent to submit a truthful answer. Sometimes a notary or other third party signs as witness to the signature. When converting these transactions to electronic systems, agencies should carefully evaluate whether the selected technology and its implementation are able to provide analogous functions.

The greatest paradigm shift is considering if and why a signature is necessary at all.

2.2 Assessment of Risk

State agencies must conduct appropriate risk analyses for conducting transactions involving electronic records or electronic signatures. 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 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 (addressed above in the section on Trustworthy Records) may help agencies establish criteria for the types of electronic signature-related records they need to retain to document their programs.

Conducting Risk Assessments

A decision to embrace or reject the option of electronic filing or record keeping should demonstrate whether the methods under consideration are cost-effective and sufficiently minimize the risk of significant harm.

Accordingly, agencies should develop and implement plans supported by an assessment of whether to use and accept documents in electronic form and to engage in electronic transactions. The assessment should weigh costs and benefits and involve an appropriate risk analysis, recognizing that low-risk information processes may need only minimal consideration, while high-risk processes may need extensive analysis. Performing the assessment to evaluate electronic signature alternatives should not be viewed as an isolated activity or an end in itself.

An assessment should include strategies to mitigate risks and maximize benefits in the context of available technologies, and should address the relative total costs and effects of implementing those technologies on the program being analyzed.

In addition to serving as a guide for selecting the most appropriate technologies, the assessment of costs and benefits should be designed to establish a business case to support agency decisions in light of statutory mandates and budgetary priorities. In doing so, agencies should consider the effects on the public, its needs, and its readiness to move to an electronic environment.

Where risk management measures are appropriate, agency risk assessments should indicate when and how a combination of information security practices, authentication technologies, management controls, or other business processes for each application will be practicable. In addition, if a particular application is not practicable for conversion to electronic interaction as part of the plan, agencies should explain the reasons and discuss any strategy to make such conversion practicable.

Assessing Risks, Costs and Benefits

A risk assessment should identify the particular technologies and management controls best suited to agency objectives in light of the risks, costs and benefits to the parties involved. Often parts of the assessment can be quantified, but some factors - particularly the risk analysis - usually can only be estimated qualitatively.

Quantitative Analysis. A quantitative approach to risk analysis generally attempts to estimate the monetary cost of risk compared to the cost of risk reduction techniques based on:

- The likelihood that a damaging event will occur.
- The cost of potential losses.
- The cost of mitigating actions that could be taken.

Qualitative Analysis. Where reliable data on likelihood and costs is not available, a qualitative approach can be taken by defining risk in more subjective and general terms such as high, medium, and low. Qualitative analyses depend more on the expertise, experience, and good judgment of the agency managers conducting them than on quantified factors.

The same can be true with other costs and benefits. Some factors, such as the value of deterring fraud, are difficult to quantify. If a new automated system is less secure than an old, paper-based system, attempts to commit fraud or to repudiate transactions may increase. It usually is not possible to quantify in monetary terms attitudes such as increased customer satisfaction and willingness to cooperate with an agency, which may result from electronic processes designed to be user-friendly.

However, many costs (design, development, and implementation) and benefits (reduced transaction costs, saved time etc.) can be quantified, as is the case for other IT projects. Clearly, then, the assessment should use a combination of quantitative and qualitative methods to judge the practicability of any electronic transaction method and should include a comprehensive risk analysis when warranted by the sensitivity of the data and/or the transaction.

Alternatives that minimize risk should be assessed in terms of net benefit to the agency and the customer in order to determine the electronic signature most appropriate for the transaction. If the net benefits are negative, the agency may determine that using an electronic process is not practicable at this time. In any event, all risk analyses are exercises in managerial judgment.

2.3 Cost-Benefit Analysis

Determine if electronic transaction is practical. The primary goal of a cost-benefit analysis should be to find a cost-effective package of security mechanisms and management controls that can support automated systems using electronic communications. In estimating the cost of any system, agencies should include costs associated with hardware, software, administration, and support of the system, both short-term and long-term.

Agencies should consider the following issues when framing the cost-benefit analysis:

- Offering more than one way to communicate electronically may enable more people to conduct electronic transactions. If different partners have different skills and differing security concerns, providing a combination of mechanisms will

meet the needs of a greater number of possible partners. While admittedly adding cost, offering multiple alternatives can add greater benefit, as well.

- Electronic transactions can impose costs on the transaction partners. Many electronic signature techniques require specialized computer hardware and technical knowledge. The higher these threshold costs are, the higher the participation costs are for users. Higher costs will tend to narrow the range of potential users, which in turn limits the benefits of electronic communications.
- Agencies should assess the costs of developing and maintaining electronic transactions. Information technology costs continue to fall and electronic signature techniques continue to evolve. As a result, the agency should periodically redo its risk and cost-benefit analyses, including a reassessment of those programs where electronic transactions were initially deemed impracticable to determine whether costs and/or technologies have changed enough so that electronic transactions have become practicable.
- If the cost-benefit analysis of a proposed solution indicates that the electronic solution is not cost effective, the agency should seek to identify opportunities to reengineer the underlying process being automated. Occasionally, practices and rules under the control of an agency are based on factors or circumstances that may no longer apply. In these cases new practices and rules should be proposed if the changes do not undermine the objective or impair security, and if the changes lead to a more efficient process.

Document agency decisions. Agencies should select an appropriate combination of technologies, practices, and management controls to minimize risk cost-effectively while maximizing benefits to all parties to the transaction. Agency managers should document these decisions, however qualitative, for later review and adjustment.

Costs of risk mitigation. Neither handwritten signatures nor electronic signatures are totally reliable and secure. Every method of signature, whether electronic or on paper, can be compromised with enough skill and resources, or due to poor security procedures, practices, or implementation. Setting up a very secure, but expensive, automated system may in fact buy only a marginal benefit of deterrence or risk reduction over other alternatives and may not be worth the extra cost. For example, past experience with fraud risks, and a careful analysis of those risks, shows that exposure is often low. If this is the case a less expensive system that substantially deters fraud may be warranted, and not an absolutely secure system.

2.4 Risk Mitigation and Security

As defined in UETA, a "security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

The goal of information security procedures is to protect the integrity and confidentiality of electronic records and transactions that enable business operations. Different security approaches offer varying levels of assurance in an electronic environment and are appropriate depending on a balance between the benefits from electronic information transfer and the risk of harm if the information is compromised.

Transferring Electronic Signature Record Material From Contractors to Agencies

As the government 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 may 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 should 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.

Approaches utilized in maintaining the security of electronic records and signatures include the following (in an ascending level of assurance):

- "Shared secrets" methods (e.g., personal identification numbers or passwords).
- Digitized (as opposed to *digital*) signatures or biometric means of identification, such as fingerprints, retinal patterns, and voice recognition.
- Cryptographic digital signatures.

Combinations of approaches (e.g., digital signatures with biometrics) are also possible and may provide even higher levels of assurance than single approaches by themselves.

Deciding which to use in an application depends first upon finding a balance between the risks associated with the loss, misuse, or compromise of the information, and the benefits, costs, and effort associated with deploying and managing the increasingly secure methods to mitigate those risks. Agencies must strike a balance, recognizing that achieving absolute security is likely to be highly improbable in most cases and prohibitively expensive if possible.

Nonrepudiation

Irrespective of the approach an agency takes, some form of technical nonrepudiation services must be implemented to protect the reliability, authenticity, integrity, and usability, as well as the confidentiality, and legitimate use of electronically-signed information. Nonrepudiation is one of the security services in computing environments, being mainly applied in message handling systems and electronic commerce. The nonrepudiation services that are being used in e-commerce can also be used in ascertaining the reliability of electronically signed records. Nonrepudiation 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 nonrepudiation, and agencies will choose the framework that matches their needs. One possible framework is the ISO (International Organization for Standardization) nonrepudiation model (Nonrepudiation - Part 1: General Model, ISO/IEC JTC1/SC27 N1503, November 1996; Nonrepudiation - Part 2: Using symmetric techniques, ISO/IEC JTC1/SC27 N1505, November 1996 - for additional information see Appendix 4). The essential elements of the ISO model are listed below:

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 nonrepudiation 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 nonrepudiation delivery authority service. The receiver has to store this evidence using the nonrepudiation storage service. In case of dispute, the sender can later retrieve this evidence.

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 nonrepudiation delivery authority service. The sender receives this evidence and stores it using the nonrepudiation storage service; it can later be retrieved if there is a dispute.

Transaction Timestamp: This timestamp is generated by the nonrepudiation service as part of the evidence that an event or action took place.

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 or, as it emerges, the proper standards and applications to define the records and signatures during and beyond their useful life as part of the design of this process and facility.

PART 3: RECORDS MANAGEMENT ISSUES

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 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. The process for the legal disposition of state records is subject to the same documentation requirements as any other format or medium. This usually requires agency permission and some type of disposition log to adequately document disposition and destruction of electronic records.

System Development Life Cycle: 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.

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.

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 activity to which the record relates. 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.

3.2 Preserving Electronically Signed Records

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 concurrences. Dates and other identifiers such as organization or title often accompany signatures. 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. 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 may also be necessary to retain the hardware and software that created the signature (e.g., chips or encryption algorithms) so that the complete record can be revalidated at a later time as needed

Ensuring 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. Below is a discussion of two different approaches. Agencies should choose an approach that is appropriate in light of the results of their risk assessment, is practical for them, and will fit their needs.

Maintaining the Ability to Re-Validate Electronic Signatures. 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. For this approach the cost of technology migrations and technology limitations need to be considered

Another approach may be a third party verification at a point in time when all is functioning correctly that the signature was valid at that moment, and to save the verification as part of the signature documentation.

These issues are currently evolving with changes in technology, real world user experience and focused legal considerations.

3.3 Records Managers and Auditors

For an organization to effectively implement a process for accepting electronically signed documents, all levels of management must be supportive and ultimately executive management needs to have ownership over the initiative. Records managers and auditors will play a critical role in the system design for the acceptance of electronic records. The auditor often has tools or techniques for assessing risks and can offer guidance in that area or can review the risk assessment and point out areas for improvement. The records manager will be able to address ensuring the preservation of records. High-risk systems should include an independent verification and document the reliability of the systems and the electronic records.

In December 2001, the National Electronic Commerce Coordinating Council published it's exposure draft *Electronic Records Management Guidelines for State Government: Ensuring the Security, Authenticity, Integrity, and Accessibility of Electronic Records* that included the following:

"**Maintain audit trails of system activity by system or application processes and by user activity:** In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. It can be used to document the trustworthiness and reliability of a system as well as the integrity of the e-records stored in the system. If possible, audit trails should be generated automatically by the system receiving, processing, and maintaining the records. All audit records should be retained in compliance with established State or local government records retention and disposition schedules."

A copy of the NECCC publication is available in pdf and by simple conversion to html, the official version and other papers on e-government issues are available at http://www.ec3.org

3.4 Other Records Management Issues

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 in coordination with the electronically signed records to which they relate.

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*.

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 record keeping system to preserve the complete content of the record.

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.

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.

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.

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.

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.

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

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

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

Agencies establish records management practices based on statutory requirements, their operational needs and perceptions of risks. The central document in establishing and maintaining control over records is the records retention schedule. The schedule is prepared by or under the authority of the records management officer, lists all records created or received by an agency, and specifies how long they are to be retained. Operational needs are determined on the basis of the approach taken to ensuring the trustworthiness of electronically signed records over time. Risk assessment and risk mitigation, along with other methodologies, are used to establish documentation requirements for agency activities.

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.

Human readable 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 page left blank intentionally.

Appendix 1 - Current Electronic Signature Technologies

Two categories: cryptographic and non-cryptographic

Non-crypto most common today.

Cryptographic Control

Creating electronic signatures may involve the use of cryptography in two ways: symmetric (or shared private key) cryptography, or asymmetric (public key/private key) cryptography. The latter is used in producing digital signatures, discussed further below.

(1) **Shared Symmetric Key Cryptography**

In shared symmetric key approaches, the user signs a document and verifies the signature using a single key (consisting of a long string of zeros and ones) that is not publicly known, or is secret. Since the same key does these two functions, it must be transferred from the signer to the recipient of the message. This situation can undermine confidence in the authentication of the user's identity because the symmetric key is shared between sender and recipient and therefore is no longer unique to one person. Since the symmetric key is shared between the sender and possibly many recipients, it is not private to the sender and hence has lesser value as an authentication mechanism. This approach offers no additional cryptographic strength over digital signatures (see below). Further, digital signatures avoid the need for the shared secret.

(2) **Public/Private Key (Asymmetric) Cryptography - Digital Signatures**

(a) To produce a digital signature, a user has his or her computer generate two mathematically linked keys -- a private signing key that is kept private, and a public validation key that is available to the public. The private key cannot be deduced from the public key. In practice, the public key is made part of a "digital certificate," which is a specialized electronic file digitally signed by the issuer of the certificate, binding the identity of the individual to his or her private key in an unalterable fashion. The whole system that implements digital signatures and allows them to be used with specific programs to offer secure communications is called a Public Key Infrastructure, or PKI.

(b) A "digital signature" is created when the owner of a private signing key uses that key to create a unique mark (the signature) on an electronic document or file. The recipient employs the owner's public key to validate that the signature was generated with the associated private key. This process also verifies that the document was not altered. Since the public and private keys are mathematically linked, the pair is unique: only the public key can validate signatures made using the corresponding private key. If the private key has been properly protected from compromise or loss, the signature is unique to the individual who owns it, that is, the owner cannot repudiate the signature. In relatively high-risk transactions, there is always a concern that the user will claim some else made the transaction. With public key technology, this concern can be mitigated. To claim he

did not make the transaction, the user would have to feign loss of the private key. By creating and holding the private key on a smart card or an equivalent device, and by using a biometric mechanism (rather than a PIN or password) as the shared secret between the user and the smart card for unlocking the private key to create a signature this concern can be mitigated. In other words, combining two or three distinct electronic signature technology approaches in a single implementation can enhance the security of the interaction and lower the potential for fraud to almost zero. Furthermore, by establishing clear procedures for a particular implementation of digital signature technology, so that all parties know what the obligations, risks, and consequences are, agencies can also strengthen the effectiveness of a digital signature solution.

The reliability of the digital signature is directly proportional to the degree of confidence one has in the link between the owner's identity and the digital certificate, how well the owner has protected the private key from compromise or loss, and the cryptographic strength of the methodology used to generate the public-private key pair. The cryptographic strength is affected by key length and by the characteristics of the algorithm used to encrypt the information.

Non-Cryptographic Methods of Authenticating Identity

(1) **Personal Identification Number (PIN) or password:** A user accessing an agency's electronic application is requested to enter a "shared secret" (called "shared" because it is known both to the user and to the system), such as a password or PIN. When the user of a system enters her name, she also enters 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. If the authentication process is performed over an open network such as the Internet, it is usually essential that at least the shared secret be encrypted. This task can be accomplished by using a technology called Secure Sockets Layer (SSL), which uses a combination of public key technology and symmetric cryptography to automatically encrypt information as the user sends it over the Internet and decrypt it before the intended recipient reads it. SSL currently is built into almost all popular Web browsers, in such a fashion that its use is transparent to the end user. Assuming the password is protected during transmission, as described above, impersonating the user requires obtaining the user's password. This may be relatively easy if users do not follow appropriate guidelines for password creation and use. Agencies should establish adequate guidelines for password creation and protection.

(2) **Smart Card:** A smart card is a plastic card the size of a credit card containing an embedded integrated circuit or a chip that can generate, store, and/or process data. It can be used to facilitate various authentication technologies also embedded on the same card. By having different authentication choices the user can pick the authentication technique that meets but does not exceed the information requirement for the transaction. A user inserts the smart card into a card reader device attached to a computer or network input device. Information from the card's chip is provided to the computer only when the user also enters a PIN, password, or biometric identifier recognized by the card. Thus, the user authenticates to the card, making available electronic credentials, which can then be used

by the computer or network to strongly authenticate the user for transactions. This method offers far greater security than the typical use of a PIN or password, because the shared secret is between the user and the card, not with a remote server or network device. Moreover, to impersonate the user requires possession of the card as well as knowledge of the shared secret that activates the electronic credentials on the card. Thus, proper security requires that the card and the PIN or password used to activate it be kept separate. This is not a concern if a biometric is used for the latter purpose.

(3) **Digitized Signature:** A digitized signature is a graphical image of a handwritten signature. Some applications require an individual to create his or her hand-written signature using a special computer input device, such as a digital pen and pad. The digitized representation of the entered signature may then be compared to a previously-stored copy of a digitized image of the handwritten signature. If special software judges both images comparable, the signature is considered valid. This application of technology shares the same security issues as those using the PIN or password approach, because the digitized signature is another form of shared secret known both to the user and to the system. The digitized signature can be more reliable for authentication than a password or PIN because there is a biometric component to the creation of the image of the handwritten signature. Forging a digitized signature can be more difficult than forging a paper signature since the technology digitally compares the submitted signature image with the known signature image, and is better than the human eye at making such comparisons. The biometric elements of a digitized signature, which help make it unique, are in measuring how each stroke is made duration, pen pressure, etc. As with all shared secret techniques, compromise of a digitized signature image or characteristics file could pose a security (impersonation) risk to users.

(4) **Biometrics:** Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer. Among these are voice patterns (where an individual's spoken words are converted into a special electronic representation), fingerprints, and the blood vessel patterns present on the retina (or rear) of one or both eyes. In this technology, the physical characteristic is measured (by a microphone, optical reader, or some other device), converted into digital form, and then compared with a copy of that characteristic stored in the computer and authenticated beforehand as belonging to a particular person. If the test pattern and the previously stored patterns are sufficiently close (to a degree which is usually selectable by the authenticating application), the software will accept the authentication, and the transaction allowed to proceed. Biometric applications can provide very high levels of authentication especially when the identifier is obtained in the presence of a third party to verify its authenticity, but as with any shared secret, if the digital form is compromised, impersonation becomes a serious risk. Thus, just like PINs, such information should not be sent over open networks unless it is encrypted. Moreover, measurement and recording of a physical characteristic could raise privacy concerns where the biometric identification data is shared by two or more entities. Further, if compromised, substituting a different, new biometric identifier may have limitations (e.g., you may need to employ the fingerprint of a different finger). Biometric authentication is best suited for access to

devices, e.g. to access a computer hard drive or smart card, and less suited for authentication to software systems over open networks.

Appendix 2 – Checklist for Evaluating Electronic Signatures

To summarize the process and restate the principles that agencies should employ to evaluate authentication mechanisms (electronic signatures) for electronic transactions and documents, the following steps apply:

- Examine the current business process that is being considered for conversion to employ electronic documents, forms or transactions, identifying customer needs and demands as well as the existing risks associated with fraud, error or misuse.
- Identify the benefits that may accrue from the use of electronic transactions or documents.
- Consider what risks may arise from the use of electronic transactions or documents. This evaluation should take into account the relationships of the parties, the value of the transactions or documents, and the later need for the documents.
- Consult with counsel about any agency specific legal implications about the use of electronic transactions or documents in the particular application.
- Evaluate how each electronic signature alternative may minimize risk compared to the costs incurred in adopting an alternative.
- Determine whether any electronic signature alternative, in conjunction with appropriate process controls, represents a practicable trade-off between benefits on the one hand and cost and risk on the other. If so, determine, to the extent possible at the time, which signature alternative is the best one. Document this determination to allow later reevaluation.
- Develop plans for retaining and disposing of information, ensuring that it can be made continuously available to those who will need it, for managerial control of sensitive data and accommodating changes in staffing, and for ensuring adherence to these plans.
- Develop management strategies to provide appropriate security for physical access to electronic records.
- Determine if regulations or policies are adequate to support electronic transactions and record keeping, or if "terms and conditions" agreements are needed for the particular application. If new regulations or policies are necessary, disseminate them as appropriate.
- Seek continuing input of technology experts for updates on the changing state of technology and the continuing advice of legal counsel for updates on the changing state of the law in these areas.
- Integrate these plans into the agency's strategic IT planning and regular reporting to the Legislative Budget Board.
- Perform periodic review and re-evaluation, as appropriate.

This page left blank intentionally.

Appendix 3 - Technical Considerations of Various Electronic Signature Alternatives

(1) To be effective, each of these methods requires agencies to develop a series of policy documents that provide the important underlying framework of trust for electronic transactions and which facilitate the evaluation of risk. The framework identifies how well the user's identity is bound to his authenticator (e.g., his password, fingerprint, or private key). By considering the strength of this binding, the strength of the mechanism itself, and the sensitivity of the transaction, an agency can determine if the level of risk is acceptable. If an agency has experience with the technology, existing policies and documents may be available for use as guidance. Where the technology is new to an agency, this may require additional effort.

(2) While digital signatures (i.e. public key/private key) are generally the most certain method for assuring identity electronically, the policy documents must be established carefully to achieve the desired strength of binding. The framework must identify how well the signer's identity is bound to his or her public key in a digital certificate (identity proofing). The strength of this binding depends on the assumption that only the owner has sole possession of the unique private key used to make signatures that are validated with the public key. The strength of this binding also reflects whether the private key is placed on a highly secure hardware token, such as a smart card, or is encapsulated in software only; and how difficult it is for a malefactor to deduce the private key using cryptographic methods (which depends upon the key length and the cryptographic strength of the key-generating algorithm).

A Public Key Infrastructure (PKI) is one mechanism to support the binding of public keys with the user's identity. A PKI can provide the entire policy and technical framework for the systematic and diligent issuance, management and revocation of digital certificates, so that users who wish to rely on someone's certificate have a firm basis to check that the certificate has not been maliciously altered, and to confirm that it remains active (i.e., has not been revoked because of loss or compromise of the corresponding private key). This same infrastructure provides the basis for interoperability among different agencies or entities, so that a person's digital certificate can be accepted for transactions by organizations external to the one that issued it.

(3) By themselves, digitized (not digital) signatures, PINs, biometric identifiers, and other shared secrets do not directly bind identity to the contents of a document as do digital signatures which actually use the document information to make the signature. For shared secrets to bind the user's identity to the document, they must be used in conjunction with some other mechanism. Biometric identifiers such as retinal patterns used in conjunction with digital signatures can offer far greater proof of identify than pen and ink signatures.

(4) While not as robust as biometric identifiers and digital signatures, PINs have the decided advantage of proven customer and citizen acceptance, as evidenced by the universal use of Pins for automated teller machine transactions. Pins combined with encrypted Internet sessions, particularly through the use of Secure Sockets Layer

technology on the World Wide Web, are very popular for retail consumer transactions requiring credit card or other personal authenticating information. This may well be suited for a variety of government applications. Also, secure Web browsers are increasingly being designed to accommodate web authentication, making this approach a possible interim step towards implementing the more robust authentication provided by digital signatures.

(5) It is important to remember that technical factors are but one aspect to be considered when an agency plans to implement electronic signature-based applications.

Appendix 4 - Comments on the ISO (International Organization for Standardization) Nonrepudiation Model

"Nonrepudiation," as used in ISO standards, is a technical, not a legal, concept. Technical nonrepudiation refers to circumstances and systems employed in the creation, transmission, receipt and response to a message that reliably establish the fact of receipt, acknowledgment, or response. The mere fact that a message-handling system provides a security service that establishes technical nonrepudiation does not establish "nonrepudiation" in a legal sense. In fact, nonrepudiation is not a generally accepted legal term or legal concept (see, for example, the discussion of these terms in the ABA Digital Signature Guidelines issued in 1996). In legal terms, technical nonrepudiation may give rise to the establishment of a "rebut table presumption." This means that the burden of proving that a message was not signed shifts from the recipient back to the sender. A rebut table presumption is not as black-and-white as "nonrepudiation;" unfortunately, this distinction has been lost on many people involved in the creation of policies or procedures pertaining to electronic signatures, including some lawyers. For additional information see the Internet X.509 Public Key Infrastructure: Roadmap .