Guidelines for the Management of Electronic Transactions and Signed Records

Prepared by the UETA Task Force of the Department of Information Resources and the Texas State Library and Archives Commission

August 2004

Executive Summary

Texas Uniform Electronic Transactions Act (UETA)

The 77th Legislature passed UETA in 2001 to help establish a legal framework for the growing use of Internet transactions between state and local government and citizens. As is true with the complex nature of the Internet, the new laws can seem imposing and complicated. This Executive Summary will brief you on the uses and risks associated with UETA. You can search the Guidelines for the Management of Electronic Transactions and Signed Records (the Guide) to learn more detail.

Introduction and Applicability

Information can be contained in a tangible medium such as paper, or in an intangible form, such as electronic documents stored on a computer disk or diskette. This Guide applies to transactions that are created, sent, received, maintained or stored electronically. The Guide must be followed by state agencies, as defined in Texas Government Code, Section 2054.003(12), if it applies as a rule of the Department of Information Resources. The Guide must be followed by state agencies, and in some instances, by local governments, if it applies as a rule of the Texas State Library and Archives Commission. Local governments may use this Guide even if they are not required to do so by law or by a rule of the Texas State Library and Archives Commission. Use the Guide to evaluate transaction risks and the effectiveness of a given signature method, to match the signature method to the degree of risk, and to formulate plans and procedures for the management of electronic records and electronic signatures.

Uses for UETA

With the tremendous growth of the Internet in the past few years, there has been an explosion of business contracts transacted using the Internet. Accordingly, in 2000, Congress created a law commonly called "e-Sign" to have one national standard for signatures. As a corollary of "e-Sign," Texas adopted UETA to facilitate the creation of contracts and related record-keeping via the Internet.

Risks without UETA

The legislative history makes clear that until UETA was enacted, the government and business had risk that what they thought were legally binding agreements were indeed unenforceable. The UETA Task Force was created by the Department of Information Resources and the Texas State Library and Archives Commission to study the impact and utility of UETA for the State. The Task Force concluded that each Internet user should assess their risk of the loss of valuable resources or money in determining whether they should use the features of certification of signatures and public keys, both of which add to the cost of using the Internet. Those risks are explained in detail in the Guide.

Must agencies' e-records be electronically signed?

Electronically signed e-records pose management problems. Electronic signatures can be created in a number of ways, with varying degrees of reliability and a wide range of cost. The question that agencies must first ask is whether their e-records must be signed at all. If a record must be signed electronically, this Guide is instructive on how to maintain e-signatures so that they can be relied upon if a dispute arises later regarding the authenticity of the signature.

How should a state agency choose which form of electronic signature it should use?

Agencies should:

- Evaluate the risks of the transaction. Is the transaction high-risk? It may be risky in any number of ways: dollar value, consequences of failure, damage to credibility, political risk, and so on.
- Evaluate the effectiveness of the electronic signature method. How secure is the signature method? An ID and password may not provide a high level of assurance that the signature is authentic. A signature method that involves encryption or biometrics (e.g., fingerprints or voice prints) may provide a much higher level of assurance.
- Evaluate the cost of the available alternatives. How much does it cost to implement and maintain a particular signature method? Using ID and password is inexpensive and relatively easy to implement. A biometric or encryption-based signature method is likely to be far more expensive.
- Decide which method to use by balancing risk factors, effectiveness and cost. Agencies need not employ costly signature methods for low-risk transactions, nor should they use inexpensive but less effective means for higher-risk transactions.

Guidelines for the Management of Electronic Transactions and Signed Records

The need to preserve transactions and electronically-signed records over time, whether for a defined period or permanently, presents special challenges to government entities. This Guide for the Management of Electronic Transactions and Signed Records (the "Guide") provides guidance for state agencies, and, in some instances, for local governments, 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 managed and retained over time. The Guide was created pursuant to Texas Business & Commerce Code, Section 43.017(b) which authorizes the Department of Information Resources and the Texas State Library and Archives Commission to promulgate rules relating to electronic records and electronic signatures accepted by state agencies. The Guide is being issued in a specifications format rather than a rule format because the technology available to protect the authenticity, security and retention of electronic records is in flux.

The Guide was created by the UETA Task Force, chaired by the Honorable Reagan Greer, Bexar County District Clerk and a member of the TexasOnline Authority. Other members of the UETA Task Force were Teresa Aguirre, Texas Association of Counties; Douglas Allen, FileNet Corporation; John Dahill, Conference of Urban Counties; Derrek Davis, Comptroller of Public Accounts; James Gosdin, Sr., Stewart Title Guaranty Company; Dr. Michael Heskett, Texas State Library and Archives Commission; Everett Jobe, Department of Banking; Jerry Johnson, Department of Information Resources; Karl Miller, the University of Texas at Austin; Tim Nolan, Texas State Library and Archives Commission; John Petrie, the University of Texas Health Science Center, San Antonio; Martha Richardson, Department of Information Resources; Andy Robinson, Texas Department of Insurance; Hyattye Simmons, Dallas Area Rapid Transit; Peter Vogel, Gardere Wynne Sewell, L.L.P.; and Reid Witliff, Office of the Texas Attorney General.

If being followed as a rule of the Department of Information Resources, the Guide is applicable to state agencies as defined in Texas Government Code, Section 2054.003(12). If being followed as a rule of the Texas State Library and Archives Commission, the Guide is applicable to state agencies as that term is defined in Texas Government Code, Chapter 441.180(9), and to some local governments. Local governments may use the Guide even if they are not required to do so by law or by a rule of the Texas State Library and Archives Commission. Any electronic record created shall meet the minimum requirements for the management of electronic records in 13 Texas Administrative Code, Sections 6.91-6.96.

This Guide is organized as follows:

Part 1: Electronic Transactions and Signed Records
§ 1.1 Electronic Records
§ 1.2 Electronic Signatures
§ 1.3 Trustworthy Records

Part 2: Risks Pertaining to Electronic Transactions and Signed Records
§ 2.1 Common Types of Risks
§ 2.2 Assessment of Risk
§ 2.3 Cost-Benefit Analysis
§ 2.4 Risk Mitigation and Security

Part 3: Records Management Issues
§ 3.1 Records Life Cycles and System Development Life Cycles
§ 3.2 Preserving Trustworthy Records
§ 3.3 Records Managers and Auditors
§ 3.4 Other Records Management Issues

Appendix 1: Current Electronic Signature Technologies
Appendix 2: Checklist for Evaluating Electronic Signatures
Appendix 3: Technical Considerations of Various Electronic Signature Alternatives
Appendix 4: Appendix 4: Comments on the ISO (International Organization for Standardization) nonrepudiation model

INTRODUCTION

A sound records management program must be considered an integral part of a state agency's standard business and information resource management activities. State 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.

PART 1: Electronic Transactions and Signed records

1.1 Electronic records

The Uniform Electronic Transactions Act (UETA) was enacted into law in Texas by the 77th Legislature (Senate Bill 393) in May 2001, and became effective on January 1, 2002. UETA provides definitions for several key terms that pertain to this Guide. 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. (Note: As used in this Guide, however, the term "transaction" is intended to refer to the sending or acceptance of electronic records and electronic signatures by state agencies, to and from other persons.

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.*

Texas law also provides a definition for the term digital signature, which is sometimes used interchangeably with electronic signature. Section 2054.060, Government Code, includes the following:

"Digital signature" means an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature.

It should be noted that the term digital signatures is now generally accepted as referring to a particular type of electronic signature that is created by cryptographic means involving the use of two mathematically related keys (i.e., a public and private key pair, often referred to as Public Key Infrastructure or PKI). Both the definition of "electronic signature" in UETA and the definition of "digital signature" in Section 2054.060, Government Code, incorporate the concept of intent; i.e., the intent of a person to sign an electronic record. The Department of Information Resources has published "Digital Signatures & Public Key Infrastructure (PKI) Guidelines," and adopted a rule addressing Digital Signatures.

Electronic signatures may be accomplished by several different technologies, such as Personal Identification Number (PIN), digital signatures, smart cards and biometrics. If additional technology-specific records management guidance is necessary, the Department of Information Resources will work with state agencies to develop it.

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 a state agency expends on creating or maintaining trustworthy records depends on the state agency's business needs or perception of risk. Transactions that are critical to the state agency business needs may require a greater assurance level that they are reliable, authentic, maintain integrity and are usable than less critical transactions. Notwithstanding, this discussion does not apply to the issue of whether an electronic record is usable in a legal proceeding. Under Texas Business and Commerce Code, Section 43.013, evidence of a record or signature may not be excluded in a legal proceeding solely because it is in electronic form. Consequently, for guidance on whether signed electronic records are useable or trustworthy for a particular legal purpose or in a legal proceeding, consult your legal counsel.

are have maintained their and are   Each of these terms is discussed below. The degree of effort a state agency expends on creating or maintaining trustworthy records depends on the state agency's business needs or perception of risk. Transactions that are critical to the state agency business needs may require a greater assurance level that they are reliable, authentic, maintain integrity and are usable than less critical transactions. Notwithstanding, this discussion does not apply to the issue of whether an electronic record is usable in a legal proceeding. Under Texas Business and Commerce Code, Section 43.013, evidence of a record or signature may not be excluded in a legal proceeding

solely because it is in electronic form. Consequently, for guidance on whether signed electronic records are useable or trustworthy for a particular legal purpose or in a legal proceeding, consult your legal counsel.

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, and that records have been protected against unauthorized addition, deletion, and alteration.

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 an annotation or addition. 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. 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:

- 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, management, and "preservation" 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 staff in the standard operating procedures.

PART 2: Risks Pertaining to Electronic Transactions and Signed Records

2.1 Common Types of Risks

Common risks pertaining to electronic records and signatures include:

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

(2) the degree to which the state 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 state and federal laws that apply to the transactions, the relationships between the parties, the value of the transaction, the risk of intrusion, the likely need for accessible, persuasive information regarding the transaction at some later date, and the cost of management and preservation of electronic records over time. In addition, state agencies should consider any other risks relevant to the particular process or transaction. Once these factors are considered separately, a state 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-state agency transactions (i.e., those which remain within the state agency).
- Inter-state agency transactions (i.e., those between state agencies).
- Transactions between a state agency and local government.
- Transactions between a state agency and a private organization, such as a contractor, business, private university, non-profit organization, or other entity.
- 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, and little risk of a governmental trading partner committing fraud. Similarly, transactions between a regulatory state agency and a publicly traded corporation or other known entity regulated by that state agency often bear a relatively low risk of repudiation or fraud, particularly where the regulatory state agency has an ongoing relationship with, and enforcement authority over, the entity. Risks tend to be relatively low within rulemaking contexts, as all parties can view the submissions of others so the risk of imposture is minimized.

Other types of transactions involving an ongoing relationship between a state 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 a state 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 a state agency that has legal or financial implications. In all cases, the relative value of the transaction needs to be considered.

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.

Risk analyses should attempt to identify the relative value of the type of transaction being automated and factor that against the costs associated with implementing technological and management controls to mitigate risk. Note that the value of the transaction depends on the perspective of the state agency and the transaction partner. In general, electronic records and signatures are least necessary in very low value transactions, and need not be used unless specifically required by law or regulation. 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. State 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 a state agency may have high value to an outside party.

Nature of the 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 for the intruder.

Need for information at a later point.

State 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, state 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, or the specific questions that were asked on a questionnaire. State 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.

For transaction records that have medium-term (five to nine years) or long-term retention periods (ten or more years), state agencies should consider cost and methods to maintain authentic, reliable, complete, unaltered, and usable records through multiple hardware and software technological changes for the entire retention period.

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, state agencies should ensure that the selected technology and its implementation are able to provide similar functions as were provided by the paper transaction.

2.2 Assessment of Risk

State agencies must conduct appropriate risk analyses for 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 state 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, state 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. The risk assessment should recognize 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 state agency decisions in light of statutory mandates and budgetary priorities. In doing so, state agencies should consider the effects on the public, state agency needs, and the state agency's readiness to move to an electronic environment.

Where risk management measures are appropriate, state 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, state 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 state agency objectives, minimizing risk and cost while maximizing the benefits to the parties involved. Parts of the assessment can be quantified, but some factors - particularly the risk analysis - usually can only be estimated qualitatively.

Guidelines and Tools for Assessing Risks.
The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standard (FIPS) 199 Standards for Security Categorization of Federal Information and

Information Systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

The NIST published Special Publication (SP) 800-63, "Electronic Authentication Guideline" to provide technical guidance on implementing authentication, based on the security category. The Software Engineering Institute (SEI) at Carnegie Mellon University developed a risk-based approach to authentication requirements, called the e-Authentication Risk and Requirements Analysis, or e-RA.

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, and
- the cost of mitigating actions that could be taken.

Qualitative Analysis. Where reliable data on 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 state 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 a state agency, which may result from electronic processes designed to be user-friendly.

However, many costs (design, development, and implementation) and benefits (reduced transaction costs and saved time) can be quantified. 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 state agency and the customer in order to determine the electronic signature most appropriate for the transaction. If the net benefits are negative, the state 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, state agencies should include both short-term and long-term costs associated with hardware, software, administration, and support of the system.

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, state agencies should include both short-term and long-term costs associated with hardware, software, administration, and support of the system.

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 adding cost, offering multiple alternatives also can add greater benefit.

- 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.

- State 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 state agency should periodically redo its risk and cost-benefit analyses on those programs where electronic transactions were initially deemed impracticable to determine whether costs and/or technologies have changed enough 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 state agency should identify opportunities to reengineer the underlying process being automated. Occasionally, practices and rules under the control of a state agency are based on factors or circumstances that 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 Decisions. State 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. State 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, rather than absolutely, deters fraud may be warranted.

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 state agencies.

As government begins to interact with citizens electronically, state agencies may employ third party contractors to integrate electronic signature technology into business processes. Use of a third party contractor does not relieve a state agency of its obligation to provide adequate and proper documentation of electronic signature record material. When state 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 state 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 applicable to the state agencies.

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, and
- 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.

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.

Nonrepudiation.

Irrespective of the approach a state 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 essential 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 state agencies should 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 as part of the design of this 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 record 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 state agency while in active use, or is maintained off-site when use is less frequent. The final stage of the record 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 state agency permission and some type of disposition log to adequately document disposition and destruction of electronic records. The Texas State Library and Archives Commission's rule concerning standards and procedures for electronic records and Government Code Section 441.187 describes the requirements for the disposition and destruction of electronic state 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 state agency needs to retain the record for a period of time longer than the life of the electronic information system that generated the electronic record or electronic signature. This presents special challenges, such as maintaining the trustworthiness of the record when migrating from one system to another. The minimum requirements for the retention of electronic state records are described in 13 T.A.C. Section 6.94 of the Texas State Library and Archives Commission's Electronic Records Standards and Procedures.

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 that relates to the context in which the record 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. 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. 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. A state 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 can be revalidated at a later time as needed.

Ensuring the trustworthiness of electronically-signed records over time. There are various approaches state agencies can use to ensure the trustworthiness of electronically-signed records over time. Below is a discussion of two different approaches. State 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 Documentation of the Electronic Signature. A state agency may choose to maintain adequate documentation of the record's 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.

Maintaining adequate documentation of validity may be preferable for records that have permanent or long-term retention periods since such documentation may be retained more easily over time than the technology can be maintained. However, using this approach, the signature name may not remain readable over time as a result of technological obsolescence. Therefore, state agencies should ensure that, for permanent records, a human readable form (such as electronic display or printout) of the electronic record the printed name of the signer and the date when the signature was executed be included as part of any permanent record.

Maintaining the Ability to Re-Validate Electronic Signatures. A state agency may choose to maintain the ability to re-validate digital signatures. The re-validation approach requires retention of 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.

This approach is potentially burdensome, particularly for digitally-signed records with long retention requirements, due to issues of hardware and software obsolescence. As in the first approach, the state agency must ensure that the printed name of the electronic signer and the date when the signature was executed are included as part of any human readable form (such as electronic display or printout) of the electronic record.

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. 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 management and 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 assist in designing the system to enable the identification of records for preservation and disposition. The records manager will also assist the agency head in establishing the appropriate retention for electronically signed records, as well as establishing procedures that ensure that adequate training and up-to-date documentation are provided. 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 (NEC3) published an 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."

3.4 Other Records Management Issues

What new records may be created by electronic signature technology?

Decisions to accept or create electronically-signed records will generate new types of associated records. State 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. The following list includes many of the records that might be associated with an electronic signature initiative. These records need to be archived and stored in coordination with the electronically-signed records to which they relate.

Documentation of individual identities: Information the state 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 does 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 recordkeeping system to preserve the complete content of the record.

Trust verification records: records that the state 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, a state 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 state agencies determine which of these electronic signature records to retain?

State 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 state 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 state agency activities.

When must a state agency amend its records retention schedule to cover electronic signature records?

Thirteen T.A.C.Texas Administrative Code Section 6.4 states that during a certification period the records management officer must keep the state agency's retention schedule current by submitting amendments to the schedule to:
(1) add or drop a records series;
(2) propose an amended period of time a records series will be retained;
(3) propose an amended period of time a records series will be retained in storage by the commission; and
(4) indicate changes to information concerning a records series required under subsection (a)(2) of Section 6.5 (relating to Certification of records Retention Schedules and Amendments).

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

When implementing electronic signature technology, state 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 a state 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, state 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.

New Technology and Records

New Instant messaging (IM) services provide real-time textual communications between individuals. Unlike e-mail, no artifact that documents the content of the communications exchange is retained on the state agency's network, therefore no record is created. Agencies need to address the use of IM within their organization. Unless the state agency establishes an enterprise-wide instant messaging system that provides for managing and archiving IM messages as records, the state agency should publish a policy that IM will not be used for any official communication. For additional information, see the Texas State Library and Archives Commission Model Policy for Records Management Requirements for Electronic Mail.

Appendix 1 - Current Electronic Signature Technologies.

Two categories: cryptographic and non-cryptographic

Non-cryptographic 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. 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 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, and the owner cannot repudiate the signature. In relatively high-risk transactions, there is a concern that the user will claim someone else made the transaction. With public key technology, this concern can be mitigated. To claim he or she did not make the transaction, the user has 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. Combining two or three distinct electronic signature technology approaches in a single implementation enhances the security of the interaction and lowers the potential for fraud to almost zero. 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 strengthen the effectiveness of a digital signature solution.

The reliability of the digital signature is 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 state 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 his or her name, he or 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, at least the shared secret must 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 it is sent over the Internet by the user and decrypt it before it is read by the recipient. 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. State 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 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 handwritten 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 authentication will be accepted by the software, 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 state 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 state 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 the alternative.
- Determine whether any electronic signature alternative, in conjunction with appropriate process controls, represents a practicable trade-off between benefits and costs and risks. If so, determine, to the extent possible at the time, which signature alternative is the best one. Document this determination to allow later re-evaluation.
- 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 changes in relevent laws.
- Integrate these plans into the state agency's strategic information technology planning and reporting to the Legislative Budget Board.
- Perform periodic review and re-evaluation, as appropriate.

Appendix 3 - Technical Considerations of Various Electronic Signature Alternatives

(1) To be effective, each of these methods requires state 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, a state agency can determine if the level of risk is acceptable. If a state agency has experience with the technology, existing policies and documents may be available for use as guidance. Where the technology is new to the state agency policies and documents should be developed and published.

(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 owner having 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).

Public Key Infrastructure (PKI) is one mechanism to support the binding of public keys with the user's identity. 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 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 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 digital signatures, 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 state 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 "rebuttable presumption." This means that the burden of proving that a message was not signed shifts from the recipient back to the sender. A rebuttable 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

Endnotes:

The UETA Guideline was first published in September 2002. In August 2004 the UETA Guideline was updated. Several new documents published by the National Institute of Standards and Technology (NIST) were added to section 2.2 as additional resources that state agencies may use in conducting risk assessments. The new resources are as follows:

Federal Information Processing Standard (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems.

NIST Special Publication (SP) 800-63, “Electronic Authentication Guideline.”
Also added was information about a sofware tool developed by the Software Engineering Institute (SEI) at Carnegie Mellon University. SEI developed a risk-based approach to authentication requirements, called the e-Authentication Risk and Requirements Analysis, or e-RA.