The State of New Hampshire

Electronic Signatures
Analysis and Implementation Guide

October 1, 2012

Proposed by the UETA Task Force

Electronic Signatures
Analysis and Implementation Guide

Contents

1) Determinations of RSA 294-E

New Hampshire's "Uniform Electronic Transactions Act" (UETA), RSA 294-E, provides in part that the Department of Administrative Services (DAS), in cooperation with the Secretary of State (SOS), shall determine whether and the extent to which a governmental agency will "send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures." DAS and SOS have determined that State agencies **may** send and accept electronic records and electronic signatures, as defined by UETA, if consistent with those laws, policies, procedures, information technology practices, and statewide directives applicable to the agency and/or transaction; and if (and to the extent that) the agency itself concludes that to do so will assist it in meeting its particular business and legal needs in light of the level of risk inherent in the particular transactions it handles. State agencies **shall** create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures in compliance with those laws, policies procedures, information technology practices or statewide directives that are applicable to the agency and/or transaction.

2) Introduction to RSA 294-E and Electronic Transactions

RSA 294-E was in part designed to establish a framework for electronic transactions between the State and other parties. It recognizes that electronic transactions are a reality of modern business and that such transactions may create legally binding agreements. It is therefore important that agencies understand what electronic transactions are. It is also important that agencies assess how and when such transactions should be conducted.

Laws and requirements relating to digital technology and electronic transactions can at times seem complex, but the concepts are largely similar to those involved in the use of hard-copy documents. As a general matter, a person who places his or her signature on a hard-copy document is indicating that he or she accepts the statements made in the document. The same is true when a person takes some form of electronic action to show his or her acceptance of a set of statements. Assuming that prescribed electronic steps are followed, the action is treated just as if the person placed his or her signature on a hard copy of the same document. That being the case, a primary question under UETA is just what electronic steps an agency wishes to prescribe in order to give effect to an electronic transaction.

This Analysis and Implementation Guide (Guide) will help you to determine what electronic steps are appropriate for use in your agency, by assisting you in analyzing the risks associated with various forms of electronic transactions. Your agency can then make an informed decision about when, how and whether to make use of available electronic technologies.

Should you have questions about what electronic technologies are potentially available for use by your agency, or how such technologies can best be implemented, you are encouraged to consult with your Agency Technology Manager within the Department of Information Technology (DoIT). Should you have questions regarding the specific legal import of accepting particular electronic transactions, your attorneys in the New Hampshire Department of Justice are available to provide assistance.

3) Electronic Signature Analysis and Implementation Guide

a) Overview

This Guide was created by a task group that included personnel of the New Hampshire Secretary of State, the Department of Information Technology, the Department of Administrative Services and the Department of Justice. It is intended to assist agencies that wish to implement electronic solutions to address their business needs. It expands upon the basic foundation provided by UETA (RSA 294-E), a statute that agencies are encouraged to review. The purpose of the Guide is to:

i) Assist you in understanding the definition of an electronic signature ("e-signature") under UETA (Section 3b);

ii) Explain the business and legal functions that may be served by an e-signature (Sections 3c and 3d);

iii) Assist your agency in determining whether an e-signature solution is necessary or desirable in light of the agency's particular business needs (Section 3e);

iv) Provide general direction regarding Records Management issues and the authenticity, integrity, security, and accessibility of e-records, including those that are electronically signed (Section 3f); and

v) Assist you in selecting electronic transaction and signature solutions that meet business and legal needs given the level of risk inherent in the transaction to which the signature will be applied (Sections 3g, 3h and 3i).

b) E-Signatures Generally

Ever since the invention of written documents, people have used various methods of indicating acceptance or adoption of the contents of a document. Over the years, the act of signing one's name to a document has become the most common – but not the only – method of indicating such acceptance. If you keep in mind that "signature" is the term we use to describe the manifestation of a person's adoption or acceptance of a document, some of the definitions appearing in UETA become more understandable.

> UETA defines an "electronic signature" as follows:
>
> "Electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record. [RSA 294-E:2, VIII].

The definition of "electronic signature" has two easily understandable parts. First, an electronic signature is some form of action "attached to or logically associated with an electronic record." An "electronic record" is broadly defined by UETA as "a record created, generated, sent, communicated, received, or stored by electronic means." [RSA 294-E:2, VII]. That portion of the definition recognizes that it is important to be clear about just what the person taking the action is accepting.

c) Purpose and Effectiveness of an E-Signature

In the context of an electronic transaction, the **purpose** of an electronic signature is to attest to:

i) the identity of one or more parties to the transaction,

ii) the truth and accuracy of information provided, often under penalty of law,

iii) the terms of an agreement (e.g., a contract) being established by the transaction, and/or

iv) approval to proceed with the transaction (e.g. to file a tax return or charge a credit card).

v) bind the parties to the contract.

An electronic signature does not exist in a vacuum; there must be an electronic record which is signed by the electronic signature. This record may exist prior to the transaction. For example, an electronic tax return transmitted to the Department of Revenue by the IRS. Or, the records may be created by the transaction itself; for example, a tax return created by a State's electronic filing application. Or, the record may simply be the log or audit record of the transaction itself. In any case, the effectiveness of the signature is dependent on several factors normally associated with security concerns:

- **Authentication:** the ability to prove that the actual signer is the intended signer.
- **Non-Repudiation:** the inability of the signer to deny the signature.
- **Integrity:** the assurance that neither the record nor the signature has been altered since the moment of signing.

d) Standards of an E-Signature

Generally accepted standards advise that the validity of an electronic signature is dependent upon four factors:

i) **Use of signature unique to the signer:** The electronic signature must uniquely identify the signer, and must be under reasonable control of the signer. That is, it must be unlikely that any other unauthorized entity provided the signature.

ii) **Agreement by the parties:** A party signs a document in order to convey a mutually understood message to another party, such as authorship, receipt, or approval of the document. In the case of an electronic signature, both the signer and the intended recipient of the signed document must agree that the electronic sound, symbol, or action will be accepted as serving as a signature for the electronic document or record.

iii) **Intent to sign:** The application of the electronic signature to the electronic record must be a deliberate act. It cannot be implied or inferred.

iv) **Association of the signature with the signed record:** The electronic signature must be physically or logically associated with the electronic record that is signed, and that association must persist for as long as the signature is in effect, which may be the life of the record.

Appendix A expands on each of these four factors and explores some of the implementation considerations in each of the four areas.

e) Is an E-Signature Solution Needed or Desirable?

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. Understanding the definition and purpose of an electronic signature, an agency must first determine if an electronic record must be signed at all. In doing so, business and legal requirements and risks need to be reviewed carefully. The creation and maintenance of electronically signed e-records may require more resources and effort than unsigned e-records.

Agencies should consider three primary determinants in assessing the need for electronic signatures:

i) **Is there a legal requirement for a signature?** If the current paper version of the process in question does not require a signature, then the electronic version probably does not require an electronic signature. Validate if the laws (federal, state and local government statutes and regulations) require a signature for various contracts and transactions.

ii) **Will there be a business need to verify the authentication, non-repudiation, or integrity of an electronic record created by the transaction, independently of the transaction itself, over the life of the electronic record?** If not, the agency may need security and authentication processes at the time of the transaction, but may not need the creation of electronic signatures.

iii) **Does the frequency, volume, or complexity of the paper process justify the work to build an electronic process at all, with or without electronic signatures?** Carefully analyze the trade-off between benefits, costs, and risks.

Pursuant to RSA 294-E:5, an agency is not required to utilize electronic records or electronic signatures. To the extent that state government entities do need or choose to utilize electronic records or signatures, they are subject to the standards set forth herein. Before embarking on new initiatives, agencies should study their requirements and options carefully to ensure that there is a clear business need and that any proposed solution utilizing electronic signatures is appropriate, feasible, and represents a practical trade-off between benefits, costs, and risks. Once a decision has been made to move forward, agencies will find this guide useful and instructive in choosing and implementing the appropriate technology to meet their needs.

f) Records Management Issues

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

i) Trustworthy Records

A key issue with electronic signatures is proving the signature is from the person the signature represents and the document has not been altered. According to the National Archives and Records Administration (NARA), the characteristics listed below are used to describe trustworthy records from a records management legal

perspective.

(1) **Reliability -** Record content can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests and can be depended upon in the course of subsequent transactions or activities.

(2) **Authenticity -** A record proven to be what it claims to be and to have been created or sent by the person who claims to have created and sent it; assurance of identity.

(3) **Integrity -** Proof that a record is complete and has not been altered.

(4) **Usability -** A record can be located, retrieved, presented, and interpreted in connection with the business transaction that created it.

(5) **Signature Intent -** The process used to obtain the electronic signature must demonstrate that the user intended to sign the record. Establishing intent includes:

   (a) Identifying the purpose for signing the electronic record (could be apparent within the context of the transaction);

   (b) Being certain the signer knows which electronic record is being signed; and

   (c) Providing notice to the signer that their electronic signature is about to be applied to, or associated with, the electronic record (such as an online notice advising the signer that continuing the process will result in an electronic signature).

(6) **Trustworthiness of the process -** The process used to conduct electronic transactions must be documented, such as in a formal procedure, and followed consistently.

(7) **Trustworthiness of the system** - As characterized by the following:

   (a) **Consistent -** The system processes information in a manner that assures the records they create are credible.

   (b) **Complete -** Contains the content, structure, and context generated by the transaction they document.

   (c) **Accurate -** Quality controlled at input to ensure the information in the system correctly reflects what was communicated in the transaction.

   (d) **Preserved -** Continue to reflect content, structure, and context within any system by which the records are retained over time.

(8) **Non-repudiation -** A property that protects against an individual or entity from denying having performed a particular action related to the data. Non-repudiation services protect the reliability, authenticity, integrity, usability, confidentiality, and legitimate use of electronically-signed information. Essential elements of a non-repudiation model include:

   (a) Evidence of the origin of the message

   (b) Evidence of being sent

(c) Evidence of receipt

(d) Timestamp, as needed, by the agency of origin

(e) Long-term storage of evidence

(f) Designated adjudicator of prospective disputes

State agencies shall maintain adequate documentation of the system design, implementation, use, and migration. The documentation shall include a narrative description of the system, physical and technical characteristics, and any other technical information required to access or process the records.

ii) Preserving Trustworthy Records

For a record with an electronic signature to remain trustworthy over the record life cycle, it is necessary to preserve its content, context, and sometimes its structure.

(1) **Content -** Includes the electronic signature and any associated date or other identifiers, such as organization or title. It provides evidence of a document's reliability and authenticity.

(2) **Context -** Includes individual identifiers that are not embedded in the content of the record but are used to create and verify the validity of an electronic signature. It provides additional evidence to support the reliability and authenticity of the record.

(3) **Structure** - Includes the physical and logical format of the record and the relationships between data elements comprising the record. If an agency determines it is necessary to maintain the structure of the electronic signature, it must be able to recreate the signature or demonstrate the process used to create the signature.

iii) Steps to Ensure Electronically-signed Records are Trustworthy

(1) Create and maintain documentation of the systems used to create the records that contain electronic signatures.

(2) Ensure records that include electronic signatures are created and maintained in a secure environment that protects the records from unauthorized alteration or destruction.

(3) Implement standard operating procedures for the creation, use, and management of records that contain electronic signatures and maintain written documentation of those procedures.

(4) Create and maintain records according to the documented standard operating procedures.

(5) Train agency staff in the standard operating procedures.

(6) Dispose of records that contain the electronic signatures and the associated records according to the established retention schedule for the agency.

iv) Records Retention Issues

Records created as a result of electronic transactions must be retained according to the agency's retention schedule and in accordance with the Division of Archives & Records Management policy. General electronic records management guidelines dictate that electronically signed records must contain all the information necessary to reproduce the entire electronic record and associated signatures in a form that permits the person viewing or printing the entire electronic record to verify:

- The contents of the electronic record
- The method used to sign the electronic record, if applicable
- The person(s) signing the electronic record
- The date when the signature was executed

In summary, when implementing electronic signatures, agencies need to be aware that signatures are an integral part of a record. The trustworthiness of the electronically-signed record needs to be maintained for the full records life cycle. The records life cycle is the life span of the record from its creation or receipt to its final disposition and it is usually described in three stages: creation, maintenance and use, and final disposition. Final disposition can mean permanent deletion or destruction, or transfer to the State Archives if the record has historical value. Therefore, the electronic signature must remain accessible for the full retention period of the record to which it is associated.

Appendix B - Records Management Issues, and **Appendix C - Summary Guidelines for Ensuring the Security, Authenticity, Integrity, and Accessibility of Electronic Records,** have been included to provide agencies with additional detail and summary-format information on the management of electronic records. Specific guidance for the retention and preservation of electronically signed records, including maintaining the attachment or logical association between the signed record and signature, should be sought from the Division of Archives & Records Management.

g) E-Signature Approaches

Electronic signature is a basic term for a variety of methods used as an alternative to a traditional ink signature on paper. Three basic classifications of electronic signatures exist, each with an increased level of cost, integrity, authenticity, security, and non-repudiation based on the level of technology and sophistication employed.

i) **Common Electronic Signatures** - Common electronic signatures are any signature methods that do not employ a specific technology to increase the security, authenticity, or evidentiary value of a signature. They are commonly used for low risk, low value transactions. Common electronic signatures include a digitized image of a handwritten signature, a password or PIN (Personal Identification Number), "click wrap" signature method where the user clicks a button onscreen to accept what is being stated, or a mark or symbol indicating intent to sign.

ii) **Secure Electronic Signatures** - Secure electronic signatures typically use technology to link the electronic signature to an individual or device. Secure electronic signatures may use biometric, biorhythmic, holographic, and cryptographic technology.

- Biometric signature - The automatic identification of a person based on their physical characteristics, such as a thumbprint or retina scan.
- Biorhythmic signature - The comparison of physical signature characteristics, typically speed and pressure of the stroke, to a previously provided and stored sample.
- Holographic signature - A physical likeness of an individual signature, applied electronically and bound to the content via cryptographic technology.
- Cryptography - The science of mapping readable text, called plaintext, into an unreadable format through encryption and back to readable text through decryption. This process affects the appearance of the data, without altering the content.

iii) **Digital Signatures (Public/Private Key) -** The digital signature process, in conjunction with a digital certificate, uses a private key to sign and encrypt the document and a public key to de-crypt and authenticate the signature. Digital certificates are typically issued by a trusted third party that verifies facts about your identity and issues a certificate that attests to those facts.

Digital signatures offer the highest level of authenticity, security, and integrity and are the most difficult and costly to implement.

Most methods of creating an e-signature involve a number of technologies, credentials or digital objects, and processes. Therefore, it is more accurate to think of a range of approaches to electronic signing rather than an array of stand-alone e-signature technologies. These approaches provide varying levels of security, authentication, record integrity and protection against repudiation. As such, state agencies must make informed decisions regarding the appropriate use of electronic signatures at each level by determining the risks and benefits of the available technologies for their specific applications.

Please refer to **Appendix D** for a more comprehensive discussion of E-signature approaches. For examples of E-signature usage and how they satisfy the validity standards, refer to **Appendix E.**

h) Independent Features of an Electronic Signature

An electronic signature is valid if it meets the four characteristics presented in section 3d. Beyond these characteristics, however, a specific implementation of electronic signatures may need or wish to provide one or more of the following capabilities. Both business application requirements and risk assessment should be utilized to determine the utility of these features.

- **Continuity of signature capability:** The ability to ensure that public verification or revelation of a signature, encryption method or element of an electronic signature

does not compromise the ability of the signer to apply additional secure signatures at a later date.

- **Countersignatures:** The capability to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where a party signs a document that has already been signed by another party. In an electronic signature, the issue of record originality must be considered, especially if a copy of the record(s) is made during the process of applying a countersignature.
- **Independent verifiability:** The capability to verify a party's signature (electronic record or digitized signature) without the cooperation of the signer.
- **Interoperability of Electronic Signature Technology:** The assurance that applications, systems or other electronic components used during phases of communication between trading partners and/or between internal components of an entity, are able to read and correctly interpret the transaction information communicated from one to the other.
- **Multiple signatures:** The capability of multiple parties to sign an electronic record, document or transaction. Conceptually, multiple signatures are simply appended to the document or record. Depending upon the implementation, the issue of originality may arise. As with any e-signature application, governmental entities need to ask themselves whether or not additional signatures are legally required and/or necessary for business purposes.
- **Data Transportability:** The ability of a signed document to be transported over an insecure network to another system, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes.

i) Selecting an E-Signature Approach

The selection of an e-signature solution is foremost a business decision involving more than technical considerations. Some or all of the implementation decisions for an agency utilizing electronic signatures may be dictated by legislation, regulation, or the parameters of a national program such as HIPAA. To the extent that the agency is free to design the implementation, key decisions include:

- The technology utilized to create the electronic signature
- The method of authenticating the signer and/or the user of the electronic transaction
- The security measures surrounding the execution of the transaction, including the transmission of data, and
- The security measures surrounding the subsequent storage of the signed electronic record.

The recommended approach to making these implementation decisions is to conduct a **Business Analysis and Risk Assessment** of the entire program and its participants. From a high-level Business Analysis and Risk Assessment standpoint, an agency should

evaluate the risk of the transaction against the effectiveness of the e-signature method and its related cost in selecting the optimal e-signature approach.

- 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.

After the possible risks have been identified, a **Risk Management Plan** should be created. This plan will examine each dimension of the proposed electronic signature in light of the identified risks. Action may be taken to resolve the risk, mitigate the risk, have a contingency for the risk, or the risk may simply be accepted. Critical risks should be resolved fully prior to proceeding with the implementation. The risk management process should be fully documented.

An agency is free to devise its own process for conducting and documenting a business analysis and risk assessment in the selection of an e-signature solution. The extent, level of detail, and format of the business analysis and risk assessment is up to the agency. **Appendix F** has been included to provide agencies with a more detailed discussion of the Business Analysis and Risk Assessment Process. Refer to **Appendix G** for a summary guideline presentation of the business analysis and risk assessment process. Finally, refer to **Appendix I** for a checklist to complete when evaluating e-signatures.

Agencies are encouraged to consult with their Agency Technology Manager within the DoIT and the Attorney General before selecting or implementing an e-signature solution.

4) Additional Assistance

This Guide provides a starting point for those agencies contemplating an e-signature solution. If there are additional questions concerning these guidelines, the implementation of specific technologies, or conducting a business analysis and risk assessment, please contact your Agency Technology Manager within the DoIT.

5) Appendices

Appendix A - Expanded Discussion of the Four Factors of the E-Signature Standards

Appendix B – Records Management Issues

Appendix C - Summary Guidelines for Ensuring the Security, Authenticity, Integrity, and Accessibility of Electronic Records

Appendix D - E-Signature Approaches

Appendix E - Examples of Electronic Signature Usage

Appendix F - Business Analysis and Risk Assessment

Appendix G – Business Analysis and Risk Assessment Summary Guidelines

Appendix H - Technical Considerations of Various Electronic Signature Alternatives

Appendix I – Checklist for Evaluating Electronic Signatures

Appendix A - Expanded Discussion of the Four Factors of the E-Signature Standards

Appendix A discusses in greater detail each of the four factors of the electronic signature Standards from section 3d. It discusses some of the risks associated with each of the factors, and some of the implementation considerations that may be used to mitigate the associated risk.

(1) Use of Signature Unique to the Signer

The most fundamental determination regarding this factor of the electronic signature is the nature of the signer. If the signer is a specific person, then the electronic signature must be reasonably unique to that person. The most unique electronic signatures involve the physical characteristics of the individual. Such "biometric" signatures depend on the digitization of a physical characteristic, such as a finger or thumbprint or retinal scan. The resulting electronic pattern is compared to known patterns to authenticate the signer. A digitized paper signature, although less precise, is still based on physical characteristics of an individual signer.

Alternatively, the signer may in fact be a computer system or server. In the case of a business to government transaction, or agency to agency, the concern may be that the transaction was originated by the proper business or agency, rather than a specific individual. In this case, the appropriate form of signature may utilize a digital certificate issued to the business or agency by a valid certificate authority and installed on a server under control of the business or agency. An application system may generate the proper signature without human intervention.

Other forms of electronic signature may be appropriate to either an individual or to a business or government entity. A user-id and password, for example, may be thought up by an individual, or they may be randomly generated by a password server application. In either case, in order to be verifiable as an electronic signature, the user-id and password must be registered with, or made known to, the party intended to receive the electronic signature.

Risk assessment concerning this factor of the electronic signature in any program implementation focuses on two areas:

- Failure of authentication – what is the risk to the participants or the program if the signer was not the party that the signer represented himself to be, and
- Repudiation – what is the risk to the participants or the program if the signer denies that he signed the electronic record?

There are two general types of electronic transactions involving electronic signatures. The first is the transmission of a previously created electronic document or record containing an electronic signature. Examples include the retrieval of medical records, or the receipt by the Department of Revenue of a taxpayer return from the IRS. Formats of the electronic signature itself can include the digitized image of a paper signature, the inclusion in the record of a code or PIN assigned to the signer, or a digital signature created from the electronic record by means of a private encryption key, and can represent either an individual or a business or agency. Considerations for this type of

electronic transaction include:

- Whether associated risk dictates that every electronic signature must be verified at the time of the transaction, or whether the signature is only verified if the electronic record is contested or repudiated. For example, a digitized paper signature would be impractical if large volumes of electronic transactions required that the signature be verified at the time of the transaction.
- Whether the transmitter of the signed electronic record is a trusted party that has itself verified the electronic signature. For example, the IRS may only transmit valid tax returns to the State.

The second type of electronic transaction is one where the signer is in fact the user of an electronic service such as an online transaction system. In this case, generally some form of authentication of the user takes place when the user logs onto the electronic service or transaction system. The electronic signature is created by some action of the user during the electronic transaction. Considerations for this type of electronic transaction include:

- What is the probability that an unauthorized user can "spoof" the authorized user by logging onto the electronic service or transaction system in place of the authorized user?
- What assurance is there that the creator of the electronic signature is the same party who logged onto the electronic service or transaction system? For example, what can happen if the authorized individual human user steps away from the workstation during the transaction. Requiring the user to re-submit the same credentials used to log onto the electronic service or transaction system as the act of signing can reduce the risk that an unauthorized party has taken over the user's access.

Considerations common to both types of electronic transaction involving electronic signatures include:

- What is the level of technology available to the population of signers? For example, if the application is internal to a state agency or group of agencies, it is feasible to issue some form of electronic token to this limited set of signers, or to require the use of digital certificates installed on servers within the agency infrastructure. If this is an application intended for use by the general public, however, then either the issuance of electronic tokens or the requirement for digital certificates is probably neither cost justifiable nor manageable.
- What are reasonable steps that can be taken to increase the probability that the signature is unique to the signer? For example, if cost and availability considerations dictate the use of Personal Identification Numbers (PINs) or passwords, what complexity can be required such as the use of special characters and combinations of alpha and numeric?
- What is the risk that the electronic signature or the electronic record could be accessed during the transaction, providing an unauthorized party with the means to create future invalid electronic signatures? Measures for mitigating this risk

include security measures for telecommunications, such as the encryption of the transmitted record or online transaction.

(2) Agreement by the Parties

The second requirement for use of electronic signatures is an agreement by all parties to transact business electronically. For example, a citizen may not be able to e-mail to a state agency information normally contained in a notarized paper document and assume that the agency will accept the e-mail contents as a signed document.

In the commercial world, businesses enter into peer-to-peer Trading Partner Agreements to spell out the legal, technical, and logistical requirements for the business to conduct electronic commerce. Governmental agencies may execute a similar Memorandum of Understanding to establish agreement. The situation changes, however, in a program offered by a governmental agency to the general public. Clearly it is not feasible to execute separate agreements with a large populace.

In this case, the agreement between the parties may be implicit rather than explicit. The governmental agency offers the electronic program, thereby indicating its willingness to conduct the transaction by electronic means. If the program is voluntary, the citizen indicates his agreement to conduct the transaction electronically by his participation in the program itself. The program may in fact be mandated by law or regulation. In this case the issue of agreement becomes moot.

The **risk**, in terms of impact on the use of electronic signatures, is that one or both parties will repudiate the transaction. Either the supposed signer will claim that the supposed signing party never agreed that the transaction would represent a signed document or record - for example, that the party never understood that the results of the transaction would be taken as acceptance of contractual conditions - or the recipient will claim that the receiving party never agreed to accept the electronic transaction as a signed document or record. Mitigation of this risk is generally procedural, and may include clear and unequivocal statement in the presentation of an electronic transaction that the completion of the transaction will be considered to be a signed document or record.

(3) Intent to Sign

Agreement between the parties refers to a program in general, or a capability to conduct business by electronic means. Intent to sign refers to a specific transaction. There must be clear evidence that the signer intended to complete this particular transaction.

Several forms of electronic signature inherently indicate intent to sign. A paper and ink signature takes a deliberate act to create, so a digitization of that paper signature inherits that intent. A digital signature takes programmatic action to create the encrypted mathematical reduction of the electronic document or record being signed. Electronic transactions that transmit or retrieve documents or records previously signed in either of these manners obtain an intentionally created signature which may be verified if necessary or desired.

Intent to sign becomes more open to question with online transactions. If the user of an online service is properly authenticated at logon to the service, and provides the

necessary data for an electronic transaction, it is easy to infer that the user intended to complete the transaction, and to utilize the user's logon credentials as a signature to the transaction. But what if the user enters all of the data, but then shuts down the browser? Did the user intend to complete the transaction, or to cancel it? To assume intent to sign without clear indication of that intent may incur risk that the user may later repudiate the transaction.

To mitigate this **risk**, it is recommended that any online transaction conclude by requiring some affirmative action by the user to indicate clear intent to complete the transaction. This may take the form of a simple "click through," where the user clicks on a button that states "I agree," "I hereby sign," or other appropriate affirmation. However, as noted previously in this document, there may still be a slight risk that the party who executed the click is not the same party who was authenticated at logon. If this risk is still unacceptable, then stronger risk mitigation is provided by requiring the user to present authentication credentials a second time to serve as an explicit electronic signature.

As with Agreement Between the Parties, risk mitigation strategy for Intent to Sign is generally procedural.

(4) Association of the Signature with the Signed Record

An electronic signature has no meaning apart from the electronic document or record which it signs. The record may be in the form of business data, such as a tax return or an application for a license; it may be a digitally signed logon request, a request for a medical record, or the retrieved medical record itself. Even though an individual or organization's credentials, such as a user-id and password, a fingerprint, or a physical token, are used for authentication of that individual or organization, unless those credentials are physically or logically associated with a record, with intent to sign the record, no electronic signature has been created. For example, an e-mail that is created and sent is generally accepted as being signed; however, the act of opening and reading an e-mail is generally not considered to have created a signature.

Some electronic signatures, such as the signature on a digitized paper document, cannot be physically separated from the document itself. In most cases, however, the signature is itself a piece of electronic data which can be logically, rather than physically, associated with the record. If a user's authentication credentials are used as an electronic signature on repeated transactions, for example, it would not be sound security practice to store an increasing number of copies of those credentials, increasing the risk of unauthorized use. In this case, some more public form of identification of the party, such as an account number, is used to link the electronic record to the party, with the properly secured credentials available only on an as-needed basis.

Risks associated with this factor of electronic signature implementation include:

- Risk that the signature may be disassociated from the document or record, increasing the possibility of repudiation
- Risk that a signature could be fraudulently associated with an unauthorized document or record

- Risk that a document or record could be modified without authorization after it has been electronically signed.

The form of electronic signature that best addresses these risks is the digital signature. Because a digital signature can only be created using the signer's private encryption key, it is a secure from fraud as the measures that the signer takes to protect that private key. Because the digital signature is created from a mathematical reduction of the electronic record or document, it can be used to detect whether the document has been altered since the digital signature was created. Moreover, as noted previously, a digital certificate, used to create the digital signature, generally identifies a system or server, rather than an individual. If the identification of an individual person is critical to the validity of an electronic program, then an additional form of authentication and/or electronic signature may be needed to authorize the creation of the digital signature. (See Example 5 - Use of Biometrics).

Whether or not digital signatures are used, reasonable security measures should be taken by all parties to an electronically signed transaction, in order to protect both the electronic signature and the signed electronic record or document, both during the transaction (in flight) and during their subsequent storage (at rest). It must be noted that many electronically signed documents in governmental programs are in fact public records which must be managed in accordance with legally-established record retention schedules and which must be made available on demand, often for extended periods of time. The challenges then becomes ensuring that these records are not altered, forged, or counterfeited and that they are adequately preserved and remain accessible for the full amount of time they must be retained.

Appendix B – Records Management Issues

The need to preserve transactions and electronically-signed records over time, whether for a defined period or permanently, presents special challenges to government entities. 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, must be carefully considered, especially considering the technology available to protect the authenticity, security and retention of electronic records is in flux. For example, 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 record or electronic signature. This presents special challenges, such as maintaining the trustworthiness of the record when migrating from one system to another.

a) 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. 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.

b) 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.

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.

c) Ensuring the trustworthiness of electronically-signed records over time.

There are various approaches state agencies may 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.

d) 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:

(a) **"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."

e) Other Records Management Issues

Electronic signature technology gives rise to unique records management issues that must be considered when implementing an e-signature approach:

(1) 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: An agency may withdraw a certificate by placing it in a revocation list and therefore reject a digital signature.
- 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.

(2) 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 New Hampshire State Archivist, lists all records created or received by a 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.

(3) Determine when to amend agency records retention schedule to cover electronic signature records.

State agencies must review their retentions schedules when their workflow models change, and request assistance in revising the schedule from the New Hampshire State Archivist. There is no rule for regular reevaluation of retention schedules, which may be done at any time.

(4) 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.

(5) 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.

In summary, when implementing electronic signatures, agencies need to be aware that signatures are an integral part of a record. The trustworthiness of the electronically-signed record needs to be maintained for the full records life cycle. The records life cycle is the life span of the record from its creation or receipt to its final disposition. It is usually described in three stages: creation, maintenance and use, and final disposition. Final disposition can mean permanent deletion or destruction, or transfer to the State Archives if the record has historical value. Therefore, the electronic signature must remain accessible for the full retention period of the record to which it is associated.

Specific guidance for the retention and preservation of electronically signed records, including maintaining the attachment or logical association between the signed record and signature, should be sought from the Division of Archives & Records Management.

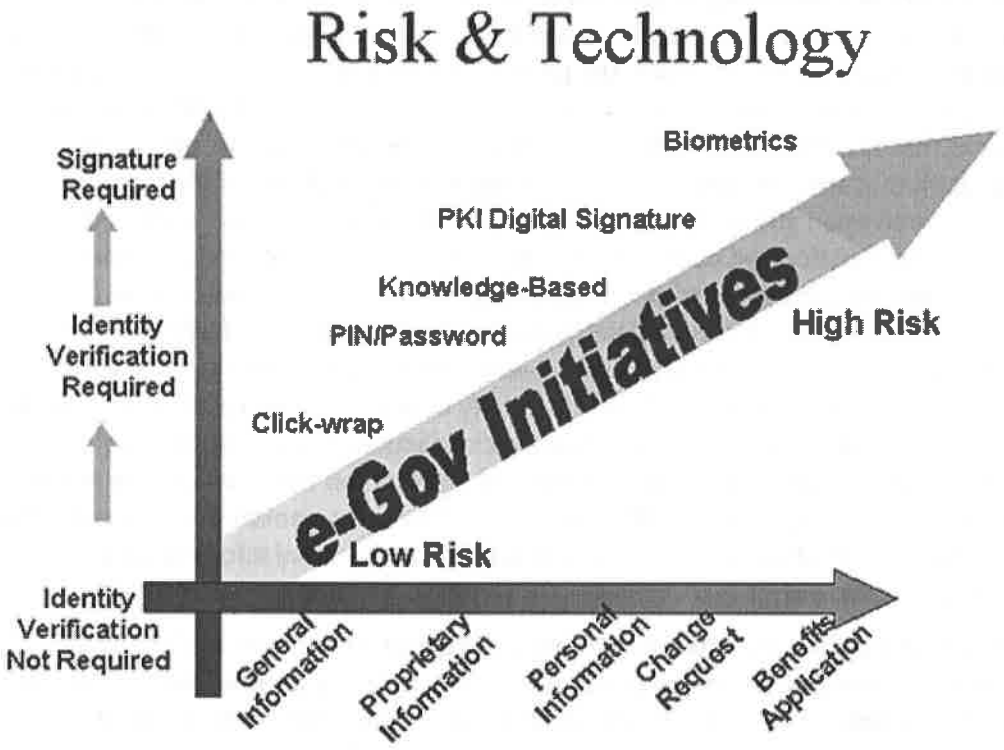
Appendix C- Summary Guidelines for Ensuring the Security, Authenticity, Integrity, and Accessibility of Electronic Records

General Guidelines ***Identify and assess specific legal, business, and other requirements that apply to e-records*** ***Base e-records management measures on the value of the records*** ***Focus on the systems and business processes that produce e-records*** ***Training is critical***	
Receiving, Capturing and Creating E-Records	
Outcomes	**Implementations**
Create or capture a record for each business transaction that complies with all legal or other requirements regarding the record's structure, content, and time of creation or capture	Develop and document clear procedures and processes for the receipt, creation, processing, and filing of e-records Designate a receiving device
Authenticate (prove the identity of) the sender of the record and make sure the e-record has not been altered	Establish policies and procedures to authenticate senders and determine the integrity of each type of e-record Establish measures to secure transmission of e-records including the integrity of records during transmission and processing Maintain measures to authenticate the identity of the sender based on potential risk and legal requirements Maintain measures to document the date and time of receipt
Uniquely identify each record	Establish a method to uniquely identify each record
Maintaining Accessible, Authentic, and Complete E-Records	
Outcomes	**Implementations**
Maintain integrity of e-records as captured or created so that they can be accessed, displayed, and managed as a unit	Maintain e-records management policy documenting the organization's policy on information management and storage Develop controlled storage or filing systems that maintain the integrity and accessibility of e-records
Retain e-records in an accessible form for their legal minimum retention periods as established in state or local retention schedules	Adopt and use records retention and disposition schedules in compliance with state and local law Adopt and use state preferred technical standards Maintain e-records in encrypted form only as long as security concerns warrant Develop retention solutions that best address an e-record's retention requirements
Search and retrieve e-records in the normal course of business for all business uses throughout their entire legal minimum retention period	Maintain adequate search and retrieval capabilities to ensure that e-records can be retrieved for all legitimate business purposes for their full retention period

Produce authentic copies of e-records and supply them in useable formats, including hard copy, for business purposes and all public access requirements	Develop or revise access and personal privacy protection policies to cover e-records Develop methods to provide public access to e-records and to protect personal privacy and confidentiality Provide access to e-records in the form the user prefers
Maintaining Secure, Reliable and Trustworthy E-Records Systems	
Outcomes	**Implementations**
Make sure the system performs in an accurate, reliable, and consistent manner in the normal course of business	Define and document system management policies and procedures Assign system management roles and responsibilities, and implement the principle of separation of duties implemented pursuant to written policies Develop and maintain problem resolution procedures, including incident reporting and response procedures Test system performance including the reliability of hardware and software Maintain audit trails of system activity by system or application processes and by user activity Provide training and user support are adequate to ensure users will implement system procedures
Protect e-records to enable their accurate and ready retrieval throughout their retention period	Develop a contingency plan that includes data backup, disaster recovery, and emergency operations Establish controls for the accuracy and timeliness of input and output Implement media controls Perform routine backups
Limit system access to authorized individuals and for authorized purposes	Maintain physical and environmental security controls Provide for identification and authentication Maintain logical access control Maintain external access control mechanisms

Appendix D - E-Signature Approaches

Most methods of creating an e-signature involve a number of technologies, credentials or digital objects, and processes. Therefore, it is more accurate to think of a range of approaches to electronic signing rather than an array of stand-alone e-signature technologies. These approaches provide varying levels of security, authentication, record integrity and protection against repudiation. The chart below indicates that as the risk associated with a specific transaction increases, so does the type (and cost) of the technology.



The descriptions below provide information on the major approaches to electronic signing in use today. They are roughly organized from the lowest to the highest level of security, authentication, record integrity and non-repudiation. However, each approach can be implemented in various ways and can be combined with techniques from other approaches to increase the strength of the above-mentioned attributes. The ultimate selection of an e-signature approach or combination of approaches for use in a governmental transaction will involve the weighing of various factors, including public policy and legal concerns that might relate to the use of certain technologies or processes. The consideration of these and other factors are addressed in greater detail below.

Some more secure approaches also require the entry of some personal information (e.g., name, date of birth or sex) along with the PIN and password. Occasionally e-signature solutions based on other approaches will include a digitized signature to give the look and feel of a handwritten signature. In such cases the digitized signature is captured in advance and stored electronically.

Click Through or Click Wrap: In this approach, a signer is asked to affirm his or her intent or agreement by clicking a button. Some click wrap approaches require signers to type "I agree" before clicking a button to protect against later claims of errors. The identification information collected and authentication process (if any) before the signature is applied can vary greatly, as can the security procedures surrounding the signing process. The Click Through or Click Wrap approach is commonly used for low risk, low value consumer transactions. It is also sometimes combined with approaches that use Personal Identification Numbers (PINs) and/or passwords to authenticate signers.

Personal Identification Number (PIN) or password: When using a PIN or password for an e-signature, a person accessing an application is requested to enter identifying information, which may include an identification number, the person's name and a "shared secret" (called "shared" because it is known to both the user and the system), such as a PIN and/or password. The system checks that the PIN and/or password is indeed associated with the person accessing the system and "authenticates" the person. Authentication is the first part of the signature process that often involves an affirmation of intent to sign when the signature is applied. If the authentication process is performed over an open network such as the Internet, the shared secret is usually encrypted using an encryption technology called Secure Sockets Layer (SSL). SSL is currently built into almost all popular Web browsers and encrypts in a fashion that is transparent to the end user. The identification and verification process used to issue a PIN and/or password varies depending on the level of security deemed necessary and the assumed risk or value of a transaction. For low risk or low value transactions the person may define a PIN and/or password after supplying minimal identifying information that may or may not be verified. For higher risk transactions, the PIN may be issued by the organization sponsoring the application after the identification process requiring substantial personal information and rigorous verification procedures.

Digitized Signature: A digitized signature is a graphical image of a handwritten signature. Some applications require a person to create a handwritten signature using a special computer input device, such as a digital pen and pad. The digitized representation of the entered signature is compared with a stored copy of the graphical image of the signature. If special software judges the two images comparable, the signature is deemed valid. This approach shares the same security issues as those using the PIN or password, because the digitized signature is another form of shared secret known both to the person and to the system. Forging a digitized signature can be more difficult than forging a paper signature because the technology that compares the submitted signature image with the known signature image is more accurate than the human eye. (See Appendix B, Example 3).

Signature Dynamics: This is a variation on a digitized signature in which each pen stroke is measured (e.g., duration, pen pressure, size of loops, etc.), creating a metric. This metric can also be compared to a reference value created earlier, thus authenticating the person who applied the signature. The signature dynamics measurements can be combined with techniques used to create a digital signature (see below) to ensure document integrity and a more reliable authentication of the signer.

Shared Private Key (Symmetric) Cryptography: In shared private key approaches, the person electronically signs a document and verifies the signature using a single cryptographic key that is not publicly known. Since the same key is used to sign a document and verify the identity of

the signer, it must be transferred from the signer to the recipient of the document. The private key is shared between the sender and possibly many recipients; therefore, it is really not "private" to the sender and hence has less value as an authentication mechanism. A private key can be made more secure by incorporating other security techniques involving the use of smart cards or other hardware tokens in which the private key is stored (see Smart Cards).

Digital Signatures - Public/Private Key or Asymmetric Cryptography: To produce a digital signature, two mathematically linked keys are generated -- a private signing key that is kept private, and a public validation key that is publicly available. The two keys are mathematically linked, but the private key cannot be deduced from the public key. The public key is often made part of a "digital certificate," which is a digitally signed electronic document binding the individual's identity to a private key in an unalterable fashion. A "digital signature" is created when the signer uses the private signing key to create a unique mark (called a "signed hash") on an electronic document. The recipient of the document employs the signer's public key to validate the authenticity of the attached private key and to verify that the document was not altered subsequent to signing. Digital signatures are often used within the context of a Public Key Infrastructure (PKI) in which a trusted third party known as a Certification Authority (CA) binds individuals to private keys and issues and manages certificates. A PKI is governed by a certificate policy that governs all aspects of a digital certificate's generation, management, use, and storage as well as the roles and responsibilities of all entities involved in the PKI. Digital signatures can be implemented without the use of a CA (see Alternate Approaches below).

Physical Token: A potentially more secure means of entering data to be used both for authentication and as an electronic signature is the use of a physical token, such as a smart card or one-time password device. The signer must be in physical possession of the device, so that it cannot be used by an unauthorized party unless it is lost or shared by the authorized signer.

One-Time Password Device: A one-time password (OTP) device contains an integrated circuit or chip with both a date/time clock and password generation software. The device, which is synchronized with similar software in possession of the intended recipient, continuously generates new passwords at regular time intervals, such as a minute or even a second. When the OTP device is connected to a computer, the generated password may be used either for authentication or to serve as an electronic signature. Because the password is continuously changing, an unauthorized party cannot reuse a previously used password that the party may be able to acquire.

Smart Cards: A smart card is a plastic card the size of a credit card that contains an embedded chip that can generate, store, and/or process data. Although not a separate e-signature approach in itself, it can be used to facilitate various authentication technologies and e-signature approaches. A person inserts the smart card into a card reader attached to a computer or network input device. Information from the card's chip is read by security software only when the person enters a PIN, password or biometric identifier. This method provides greater security than use of a PIN alone, because a person must have both physical possession of the smart card and knowledge of the PIN. Note that the PIN, password or biometric identifier in this case is a secret shared between the person and the smart card, not between the user and a computer. Therefore, smart cards can be used to further augment the security of a shared secret approach to e-signatures. Smart cards can also be used in combination with digital signatures.

Biometrics: Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer. Among these are voice patterns, fingerprints, and the blood vessel patterns present on the retina (or rear) of one or both eyes. In this approach, the physical characteristic is measured (by a microphone, optical reader, or some other device) and converted into a digital form or profile. These measurements are compared to a profile of the given biometric stored in the computer and authenticated beforehand as belonging to a particular person. If the measurements and the previously stored profile match, the software will accept the authentication, and the transaction is allowed to proceed. A biometric application can provide a high level of authentication especially when the identifying physical characteristic is obtained in the presence of a third party (making spoofing difficult). (See Appendix B, Example 5).

Hybrid Approaches: Hybrid e-signature solutions are available by combining techniques from various approaches to provide increased security, authentication, record integrity and non-repudiation for less secure signing techniques. One well-publicized solution involves improved signature-capture techniques combined with click wrap and PINs and password approaches. This solution enhances such signatures by recording the entire transaction process, which is then bound to the signed document using hashing and SSL encryption techniques to achieve document integrity and non-reputability. Another solution provides a click wrap process that results in an encrypted signature object being created within a document, which is treated as a read-only file. A number of products provide a signing ceremony designed to capture the signer's intent.

Electronic signing approaches are also available that use PKI-related or digital signature technologies but avoid some of the complexities and costs of developing a full infrastructure. Some solutions use centralized private key management by the issuing organization and identification and authentication methods that avoid the need for a third party CA. These approaches reduce the risks of requiring individuals to protect their private keys and the necessity for special software on the computer of each participant to a transaction.

As with many technologies, new approaches could be developed and deployed very rapidly in response to changes in the market or the legal and fiscal environment. Agencies are encouraged to continue to check back with their Agency Technology Manager within the DoIT for new technological developments.

Appendix E - Examples of Electronic Signature Used in Other States

Example 1 – Employee Online Benefits Administration (PIN/ Password)

Description of Program

An internet-based Electronic Benefits System (EBS) that allows eligible employees to access their benefit information and to submit changes electronically, online, in a total secure environment. Upon initial use of the EBS, employees will register online by providing personal information along with their Benefits Identification Number (BIN). This information will be verified against employee data within a master database. Once the employee has successfully registered online, he can view his account or perform direct data entry in the system such as annual/open enrollment or updates such as beneficiary changes or change of address.

Unique Identification of the Party

The employee logs into the system by providing a BIN and a password. The BIN has been assigned by the state agency. At the time of registration, employees are required to select a password that must meet certain guidelines that have been established by the Agency and are best practices for security. Such requirements include mixing letters, numbers, and special characters, as well as, a minimum string length.

Agreement by the Parties

The Agency provides the online EBS for employees to update their insurance benefit options, indicating EIP's agreement to conduct business in this manner. Employees indicate their agreement to make changes to their insurance benefits electronically by registering within and usage of the online EBS. This voluntary act of registering and making online changes constitutes the agreement of parties.

Intent to Sign

Once a state employee has completed changes to the benefits system online, there is a series of explicit actions to accept the changes representing the employee's "intent to sign." There are certain benefit changes that require documents that have a traditional handwritten signature. Such documents are imaged, securely stored and indexed in a relational database.

Association with the Record

The employee's BIN is kept by the Agency along with any associated imaged documents and the subscriber's insurance benefits record.

Security Considerations

In order to insure that a human is making the request within EBS, the subscriber (employee) will be required to repeat a string of characters (i.e., CAPTCHA) displayed within the first screen of the registration routine. Upon successfully entering the string, the subscriber will then be required to enter his/her full name and BIN. Since the nature of this transaction involves protected health information, the system uses a PKI (Public Key Infrastructure) framework in which all transactions are performed over an SSL (Secure Sockets Layer) connection.

Example 2 – Online Filing of Individual Income Tax (PIN/ Password)

Description of Program

A state taxpayer wishes to file and, if necessary, pay Individual Income Tax online. The taxpayer logs onto the system using primary and possibly secondary Social Security Numbers, and a Personal Identification Number (PIN) that was mailed to the taxpayer by the agency. The taxpayer then is guided through the submission of tax return data, including W-2 data from employers, and the system computes either the refund due to the taxpayer or else the balance due that the taxpayer must pay the state. If there is a balance due, the taxpayer selects either credit card or direct bank account debit as a payment method. When the taxpayer has entered all data, the taxpayer is shown a page with a "jurat" – a statement that the data that was entered is true and accurate – and is asked to re-enter the PIN to serve as signature.

Unique Identification of the Party

The taxpayer logs onto the system utilizing a PIN that was randomly assigned by the Agency, and was mailed to the taxpayer's address of record. While the PIN could conceivably be stolen from the mail, the thief would have to know the taxpayer's Social Security Number. There is reasonable assumption that the combination of SSN and PIN would uniquely identify the taxpayer and be known only to the taxpayer.

Agreement by the Parties

The state agency provides the online application for filing and paying Individual Income Tax, indicating its agreement to conduct business in this manner. The taxpayer indicates agreement to conduct his personal business of income tax filing electronically by participating in the program. The voluntary act of filing, and if necessary paying, online is all the agreement that is required.

Intent to Sign

The online program explicitly instructs the taxpayer to re-enter the PIN to sign the tax return. By re-entering the correct PIN, the taxpayer is again authenticated and performs a deliberate act of signing.

Association with the Record

The electronic Individual Income Tax return is indexed by the state agency using the taxpayer's primary Social Security Number. This SSN is stored as part of the taxpayer's account record with the state agency, and all tax returns are associated with the account. The PINs are associated with the SSN via a separate and highly secured file. This file serves to link the PIN to the tax return as needed.

Security Considerations

The taxpayer is authenticated using a PIN that has been previously established. The PIN is transmitted to the taxpayer by US mail in a sealed mailer, and is not provided online or over the telephone, even if requested by the taxpayer. Although fraud is possible, the risk of an unauthorized party filing the return is considered to be only moderate. SSL is used to encrypt all data exchange between the taxpayer and the Department of Revenue. The resulting electronic Individual Income Tax return is stored in a database with controlled, limited access.

NOTE: By contrast, the Department of Revenue e-sales application for online filing and payment of Sales Tax does not present a jurat or request that any data be entered for the purpose of signing the return. The application is otherwise similar to SCnetFile. While the e-sales application creates a legally filed tax return, it is not considered by the Department of Revenue to have been signed. There is no legal requirement for a Sales Tax return to be signed.

Example 3 – Business One Stop (Digitized Signature)

Description of Program

State law requires that a state agency receive a signed copy of certain documents. One example is the Articles of Incorporation for a corporation registering to do business in the state. The Business One Stop (BOS) program is an online application to allow businesses to register electronically with a number of state agencies. Although registration data is provided in electronic format, BOS also supports the ability for the business to upload a scanned PDF copy of the business's Articles of Incorporation.

Unique Identification of the Party

The Articles of Incorporation is a paper document signed in ink by an officer of the corporation and an attorney. These signatures, even when digitized, are provably unique to the signer as described above.

Agreement by the Parties

By providing the capability to upload a digitized copy of the Articles of Incorporation through the BOS program, the agency indicates its agreement to accept this as a signed document. By completing the action of uploading the digitized Articles, the business indicates its agreement to provide this electronic signature and to conduct this electronic transaction.

Intent to Sign

The business is asked to demonstrate intent to sign twice – first, by applying an ink signature in the appropriate place on the paper Articles of Incorporation, and secondly by uploading the signed document in PDF format. The BOS program asks the user to provide this signature, which is an intentional act.

Association with the Record

Because the ink signature is an integral part of the paper Articles of Incorporation, the digitized signature is an integral part of the digitized Articles of Incorporation in PDF format. As long as the PDF file is preserved intact, the signature will remain a part of the record.

Security Considerations

The signature on the PDF Articles of Incorporation is assumed to be valid with low risk, the same as if the paper version were brought to the Secretary of State. Self-selected user-id and password are used to register and authenticate the business user on BOS. Secure Socket Layer (SSL) encryption is used to secure BOS data exchange and to protect sensitive information such as Social Security Numbers during the transaction.

Example 4 – Tax returns between State Agency and the IRS (Digital Signature)

Description of Program

An individual files an electronic Individual Income Tax return using a preparer such as H&R Block, or a third party software such as TurboTax™. The individual is asked to enter a self-selected PIN to serve as signature. Both federal and state returns are transmitted to the IRS. IRS splits out and batches the state returns and makes them available to the state for download. The state digitally signs its logon request to the IRS using a previously registered digital certificate.

Unique Identification of the Party

The taxpayer's PIN is self-selected, so it can be assumed to be under the unique control of the taxpayer. However, duplication across millions of taxpayers is possible, so the PIN is used in combination with the filer's SSN for taxpayer identification. The state must obtain a unique digital certificate from a commercial certificate authority. The private key used to encrypt the state's logon uniquely identifies the trusted computer system used to communicate with the IRS.

Agreement by the Parties

The IRS sanctions electronic filing of Individual Income Tax by use of approved third parties. Its acceptance of electronically filed returns from these parties indicates IRS agreement to transact business in this manner. Electronic filing is voluntary, so the taxpayer's use of an electronic filing program, either through a paid preparer or through third party software, indicates the taxpayer's agreement to transact business electronically.

Intent to Sign

All electronic filing software approved by the IRS explicitly asks the taxpayer to enter the self-selected PIN to sign the return. The use of the PIN is therefore a deliberate act of signing. The state's communications gateway with IRS creates a digital signature from the electronic record created as its logon request. Although this is an automated function, the fact that this program was created and implemented by the state makes this an intentional act of signing.

Association with the Record

The taxpayer PIN is retained by IRS in association with the taxpayer's return. The digital signature of the state's logon request to IRS is created from the logon request record itself, and is logically associated in that the logon record cannot be altered without invalidating the electronic signature.

Security Considerations

Although there is known to be some amount of fraud associated with electronic tax filing, it generally does not involve misrepresentation of the identity of the filer. For that reason, the self-selected PIN is accepted by IRS as electronic signature. The state assumes that IRS has validated this signature, and does not re-authenticate the signature. The transmission of batches of tax returns from the IRS to the state, however, contains highly sensitive information. For that reason, the IRS requires the digitally signed logon to ensure that the state's tax returns are transmitted only to the state. The data is encrypted during

transmission. The state then stores these electronic returns using controlled limited access storage.

Example 5 –Department of Corrections Offender Supervision (Biometrics)

Description of Program

Agents process real-time offender data capture and information storage through the agent's issued tablet PCs. Agents effect data collection, signature, and immediate information storage on the tablet for subsequent synchronization with the agency's main database.

Unique Identification of the Party

Agents register with login user ID's and passwords and record their fingerprints for biometric identification. This information is recorded as a credential in both the agency's main information system as well as on agent PCs. Additionally, supervised offenders are also required to register a fingerprint through use of a biometric identification device.

Agreement by the Parties

As a matter of agency business practice and processes inherent with offender supervision, agents agree to the use of biometrics to register their digital signatures.

Intent to Sign

When an agent is required to certify who created a business transaction, the ultimate goal is to use the registered fingerprint, plus an issued PIN, as the certification mechanism.

Association with the Record

This two-part authentication activates a standard digital certificate and is used to apply the digital signature from the agent's machine to the offender case supervision business processes and is retained with the record(s).

Security Considerations

The agent is authenticated by both the fingerprint and their login user ID and password. The password requires a mix of numbers, letters, and special characters to make it more difficult to guess. The use of the finger print is more secure for authentication due to the high risk of this application. The use of the digital signature securely identifies the source of the transaction and allows the recipient to determine if the document has been altered.

Appendix F - Business Analysis and Risk Assessment

The business analysis and risk assessment should be viewed as two parts of an integrated process. Discussed below are the components and considerations recommended for each part.

(1) **Business Analysis**

The focus of the business analysis is the business transaction that the e-signature will support and the larger related business process. The information collected through the business analysis will also be a key input to the risk assessment. The business analysis may include the following components:

(a) Overview of the business process, including but not limited to, identifying and understanding:

- The transaction's purpose and origins.
- Its place within the larger business process.
- What services will be delivered and their value to the governmental entity.
- The various parties to the transaction, including stakeholders who are not directly involved in the transaction, and their business relationships to each other.
- The transaction's workflow.

(b) Analysis of legal and regulatory requirements specifically related to the transaction, such as the following:

- How the transaction must be conducted, including timeframes.
- Signature requirements (e.g., are they specifically required, what records need to be signed, who must or can sign, do they need to be notarized, etc.).
- Records related requirements including:
  - What records must be produced.
  - How long do they need to be retained.
  - Who must or can have access to the records.
  - Specific formats prescribed for the creation, filing or retention of the records.
  - Confidentiality requirements.
- Degree of importance that the identity of parties to the transaction has to conducting the transaction.
- Legal filings and court documents.

(c) Identification of industry standards or generally accepted practices related to the transaction: Industry and professional standards and practices can impact how a transaction is generally conducted and how records evidencing a transaction are created, filed and retained in various media. In addition, certain industries or professions may have established or preferred standards or practices on how electronic transactions are to be conducted and electronically signed. Such considerations may be controlling factors for governmental entities selecting e-signature solutions.

(d) Analysis of those who will use electronically signed records and related requirements: Consideration of the parties to an electronically signed transaction and other individuals or entities who must or can have access to the transaction, and their business relationships to each other are key factors in selecting an e-signature approach. These individuals can be identified in terms of their:

- Numbers
- Location
- Demographic characteristics
- Access to technology
- Accessibility requirements
- Prior business relationships

This information can be used to analyze the degree to which potential participants would accept or could easily use various e-signature approaches, determine the cost of deploying various e-signature solutions, and as a critical input to a risk assessment.

(e) Determination of interoperability requirements including those of business partners: E-signature solutions are not implemented in a vacuum. Governmental entities already have an installed base of technology. E-signature solutions need to be compatible and interoperable with an entity's existing technology environment in order to be functional and convenient. In addition, some entities may have important regulatory or business relationships with federal, state or local government agencies, as well as private sector partners that have already implemented e-signature solutions. Entities may determine that interoperability or consistency with the e-signature approaches implemented by these other government agencies or private partners is an overriding factor in their selection of an e- signature solution. Alternatively, they may decide that leveraging an existing and proven e- signature solution may be the most cost-effective approach or has the highest potential for user acceptance.

(f) Determination of the cost of alternative approaches: Consideration of costs of various e-signature alternatives is both an independent factor in selecting an e-signature solution and part of a cost-benefit analysis that a governmental entity may elect to employ (discussed below). As an independent factor, governmental entities will likely need to identify e-signature approaches that will meet their business needs **and** that they can afford to implement and maintain. The cost of various e-signature solutions may include, but are not limited to, the following:

- Hardware and software purchases.
- Implementing additional policies and procedures.
- Hiring additional personnel to implement proposed policies, procedures, or services.
- Training costs.
- Maintenance costs including help desk and user support.

(2) Risk Assessment

E-signatures may serve a security function as well as a legal one. E-signature processes usually include authentication of the signer, and some approaches can provide other security features such as message authentication and repudiation protection. Therefore, the selection of an appropriate e-signature solution includes identifying the potential risks involved in a signed electronic transaction and how various e-signature approaches can address those risks. This section draws upon the National Institute of Standards (NIST) approach to risk assessment but is more narrowly focused on the risks inherent in a signed electronic transaction.

Risk is a function of the likelihood that a given threat will exploit a potential vulnerability and have an adverse impact on an organization. A threat is a potential circumstance, entity or event capable of exploiting vulnerability and causing harm. Threats can come from natural causes, human actions, or environmental conditions. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat does not present a risk when there is no vulnerability. Impact refers to the magnitude of harm that could be caused by a threat.

To assess risks an entity should identify and analyze:

- Sources of threats
- Vulnerabilities
- Potential Impacts
- Likelihood that a threat will actually materialize

(a) Identify and analyze sources of threat: Threats to electronic transactions can come from parties to the transaction, governmental entity staff, or malicious third parties such as hackers or crackers. A threat can be an intentional act, such as a deliberate attack by a malicious person or disgruntled employee, or an unintentional act, such as negligence and error. In assessing the sources of threats, it is important to consider all potential entities that could cause harm or disrupt a transaction.

(b) Identify and analyze vulnerabilities: Some potential vulnerabilities and methods to analyze them include but are not limited to the following:

Repudiation is the possibility that a party to a transaction denies that the transaction ever took place. Repudiation could be a result of a purposeful act of fraud, a misunderstanding or a difference in interpretation. **Fraud** is a knowing misrepresentation of the truth or concealment of facts to induce another to act to his or her detriment. Governmental entities can analyze the nature of the transaction to determine the potential for fraud or repudiation. Government transactions fall into five general categories.

- Intra-agency that remain within the same government agency.
- Inter-agency between agencies in the same government.
- Inter-governmental between different government levels or other governments.

- Between a governmental entity and a private entity - contractor, university, not-for-profit, or other entity.
- Between a governmental entity and a member of the general public.

Each type of transaction may represent a different potential for fraud or repudiation. For example, inter- or intra-governmental transactions of a relatively routine nature may entail little risk, while a one-time transaction between a person and a governmental entity, which has legal or financial implications, may have a high risk of repudiation or fraud. Governmental entities should assess the potential threats of repudiation or fraud inherent in the type of transaction based on knowledge of the specific parties involved in the transaction, the nature of their business relationships to each other, and data on past incidences of repudiation and fraud.

Intrusion is the possibility that a third party intercepts or interferes with a transaction. The probability of an intrusion can depend on the benefit to the potential attackers and their knowledge that the transaction will take place. Regular or periodic transactions are more vulnerable than intermittent ones because they are predictable and it is more likely that an outside party would know they are scheduled and be prepared to intrude on them. The information's value to outside parties could also provide a motive to compromise the information. Information relatively unimportant to an agency may have high value to an outside party. Certain entities, because of their perceived image or mission, may be more likely to be attacked regardless of the value of the information or transaction.

Loss of access to records for business and legal purposes. For analyzing this vulnerability, entity transactions can be viewed as falling into the following general categories based on the nature of the records generated. The records may be:

- Used for a short time and destroyed.
- Subject to audit or compliance.
- Used for research, program evaluation, or other statistical analyses.
- Subject to dispute by either party to the transaction or by a non-party to the transaction, and needed as proof in court or an administrative tribunal.
- Archived later as permanently valuable records.

(c) Identify potential impacts: Assessing risk also involves determining the adverse impacts resulting from later repudiation, fraud, intrusion, or other threats. Potential impacts and factors include but are not limited to the following:

Financial - Potential financial loss can be determined using a variety of factors, including but not limited to:

- Average dollar value of transactions.
- Direct loss to the governmental entity.
- Loss to a citizen.

- Direct or indirect loss to a business, other government entity or other trading partner.
- Liability for the transaction (e.g., personal, corporate, insured, or shared).

Reputation and credibility - A governmental entity's loss of reputation or credibility in the event of a breach or an improperly completed transaction can be more damaging than a monetary loss. Such impacts can be determined by:

- Relationship with the other involved party (e.g., trading partner).
- Public visibility and public perception of programs.
- History or patterns of problems or abuses.
- Consequences of a breach or improper transaction either in accepting the record or as a consequence of accepting it.

Productivity - Loss of productivity associated with a breach or improper transaction can be determined using elements such as:

- Time criticality of transactions affected by the signature.
- Scope of system and number of transactions effected by the signature.
- Number of system users or dependents.
- Backup and recovery procedures.
- Claims and dispute resolution procedures.

(d) Likelihood: The final part of assessing risk is to determine the likelihood that a threat will actually occur. The following factors can be explored to determine the probability that a threat will actually happen:

- Motivation and capability of the source of the threat.
- Nature of the vulnerability.
- Existence and effectiveness of current controls.

A threat is highly likely where its source is highly motivated and capable and controls are ineffective. It is not likely where the source lacks motivation or capability and effective controls can prevent or significantly impede the threat. Entities may use other methods to determine the likelihood of a threat such as past history and legal constraints on the source of the threat. For example, it is not likely that a person would attempt to repudiate a tax filing or drivers license renewal because this could be an admission against the person's interest (i.e., failure to file a tax return or driving without a valid license).

Agencies may wish to develop a risk matrix in which the risk level for each threat is determined by the relationship between the threat's likelihood and the degree of impact against the background of existing risk reduction measures. The greatest risks are those that have extreme consequences and are almost certain to occur. Conversely, a rare event with negligible consequences may be considered trivial. The risk matrix shown below uses a scoring system and is provided for illustrative purposes only.

RISK = LIKELIHOOD x IMPACTS				
LIKELIHOOD	**IMPACTS**			
	High 4	**Medium 3**	**Low 2**	**Negligible 1**
High 4	High 16	High 12	Medium 8	Low 4
Medium 3	High 12	Medium 9	Low 6	Negligible 3
Low 2	Medium 8	Low 6	Low 4	Negligible 2
Unlikely 1	Low 4	Negligible 3	Negligible 2	Negligible 1

High Risk =10-16 Medium Risk =7-9 Low Risk =4-6 Negligible Risk =1-3

Cost-Benefit Analysis: An Agency, after identifying possible alternatives and evaluating their feasibility and effectiveness, may conduct a cost-benefit analysis for each proposed solution or solution component to determine which are appropriate for their circumstances. A cost-benefit analysis can help entities decide how to allocate resources and implement a cost-effective e-signature solution. The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the solution are appropriate to the level of risk. For example, an entity would not want to spend millions of dollars on an e-signature solution that addresses repudiation where such a risk is unlikely and would only have an impact of a few thousand dollars. On the other hand, if the risk could have devastating consequences, selecting a low cost, less secure solution would not be advisable. A cost-benefit analysis for a proposed e-signature solution can encompass the following:

- Determining the impact of implementing the solution.
- Determining the impact of not implementing it.
- Estimating the costs of the implementation.
- Assessing costs and benefits against system and data criticality to determine the importance of implementing the solution, given their costs and relative impact.

Appendix G– Business Analysis and Risk Assessment Summary Guidelines

Business Analysis and Risk Assessment

Defined as:

> Identifying and evaluating various factors relevant to the selection of an electronic signature for use or acceptance in an electronic transaction. Such factors include, but are not limited to, relationships between parties to an electronic transaction, value of the transaction, risk of intrusion, risk of repudiation of an electronic signature, risk of fraud, functionality and convenience, business necessity and the cost of employing a particular electronic signature process.

The factors listed in this definition should be addressed but **do not** represent a checklist of considerations. They should be integrated into a business analysis and risk assessment process. A governmental entity may evaluate each factor differently and accord them different weights, based on the underlying transaction.

The UETA regulation **does not** stipulate the extent, level of detail, or format of the required business analysis and risk assessment. A governmental entity must make this decision based on an evaluation of its business needs, potential legal risk and resulting impact should its e-signature selection be unsuitable for the transaction in question.

Components	Considerations
Business Analysis: Focus is on the business transaction that the e-signature will support and the larger related business process.	Overview of the business process Analysis of legal and regulatory requirements specifically related to the transaction Identification of industry standards or generally accepted practices related to the transaction Analysis of those who will use electronically signed records and related requirements Determination of interoperability requirements including those of business partners Determination of the cost of alternative approaches
Risk Assessment: Identifying potential risks involved in a signed electronic transaction and how various e-signature approaches can address them	Identify and analyze sources of threat Identify and analyze vulnerabilities Identify potential impacts likelihood of threat occurring

Using Business Analysis and Risk Assessment to Select an E-signature

- Up to the governmental entity to identify its overriding concerns.
- Selection will often be the result of balancing business concerns with risk reduction.
- Combining features from various e-signature approaches may achieve such a balance.
- An established or de facto standard or the need or ability to achieve compatibility with an existing e- signature solution employed by others may be an overriding factor.
- Budget constraints will be a key consideration in the selection process and cost may be an overriding consideration where risks are low.

Components	Considerations
Matching E-signature Functionality to Risk Level	**Signer identification or registration:** the method or process used to identify and authorize an individual to use an e-signature application. The more robust or stringent the identification method the more assurance that the signature has been used by the person who he or she purports to be. **Signer Authentication:** the policy, process and procedures used to authenticate the signer and thereby establish a link or association between the signer and the information and method used to sign. The strength of the authentication system can protect against fraud and repudiation. **Signature attestation of the record's integrity:** refers to the ability of an e-signature to protect against unauthorized access or tampering with the signed e-record and therefore reduce the risk of intrusion, inadvertent disclosure, fraud, and repudiation.
Cost-Benefit Analysis: to demonstrate that the costs of implementing the solution are appropriate to the level of risk.	Determine the impact of implementing the solution. Determine the impact of not implementing it. Estimate the costs of the implementation. Assess costs and benefits against the system and data criticality to determine the importance of implementing the solution, given their costs and relative impact.

Appendix H - 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, it 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 a state agency plans to implement electronic signature-based applications.

Appendix I – Checklist for Evaluating Electronic Signatures

Process/Step	Date Completed
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 relevant laws.	
Perform periodic review and re-evaluation, as appropriate	

6) References

UETA

New Hampshire Uniform Electronic Transactions Act (UETA)
http://www.gencourt.state.nh.us/rsa/html/XXVII/294-E/294-E-mrg.htm

A copy of the UETA document with embedded comments
http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

National Conference of Commissioners on Uniform State Laws
UETA Summary
http://uniformlaws.org/ActSummary.aspx?title=Electronic%20Transactions%20Act

Guidelines and Tools for Assessing Risk

National institute of Standards and Technology (NIST) Electronic Authentication Guideline
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

Software Engineering Institute e-Authentication Risk and Requirements Analysis (SEI e-RA)
http://www.sei.cmu.edu/library/abstracts/news-at-sei/feature13q03.cfm

Nonrepudiation

International Organization for Standardization Nonrepudiation Model
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38192

7) Revision History

First Draft	January 31, 2012	UETA Task Force
Revision	February 13, 2012	UETA Task Force
Revision	June 8, 2012	UETA Task Force
Final Draft	October 1, 2012	UETA Task Force

The UETA Task Force is comprised of personnel of the New Hampshire Secretary of State, the Department of Information Technology, the Department of Administrative Services and the Department of Justice.