

<p>New York State Information Technology Policy</p>	<p>No: NYS-G04-001</p>
<p>Best Practice Guideline:</p> <p>Electronic Signatures and Records Act (ESRA) Guidelines</p>	<p>Effective : 05/26/2004</p> <p>Issued By: Melodie Mayberry-Stewart State Chief Information Officer Director Office for Technology</p> <p>Published By: Enterprise Strategy & Acquisitions Office</p>

1.0 Purpose and Benefits of the Guideline

This best practice guideline:

- explains the definition of an e-signature under ESRA;
- assists in the selection of e-signature solutions that meet business and legal needs;
- provides general direction on ensuring the authenticity, integrity, security, and accessibility of e-records including those that are electronically signed.

2.0 Scope of the Guideline

This best practice guideline applies to all governmental entities as defined under ESRA as:

any state department, board, bureau, division, commission, committee, public authority, public benefit corporation, council, office, or other governmental entity or officer of the state having statewide authority, except the state legislature, and any political subdivision of the state.

Private individuals and entities may also find these guidelines useful.

3.0 Guidelines

3.1 Introduction

The purpose of the [Electronic Signatures and Records Act \(ESRA\)](#) is to facilitate e-Commerce and e-Government in New York State by giving electronic signatures ([e-signatures](#)) and electronic records ([e-records](#)) the same force and effect as signatures and records produced by non-electronic means.¹ ESRA does not require private parties or governmental entities to use or accept e-signatures or e-records. In other words, the use and acceptance of e-signatures or e-records is completely voluntary. The regulation implementing ESRA allows a [governmental entity](#) to deploy e-records in a manner that satisfies its business practices and needs. However, unless otherwise provided by law, governmental entities that use e-records must:

- Ensure that citizens can access records as permitted by law and receive copies of them in paper form;
- Accept hard copy documents for submission or filing; and
- Allow for non-electronic means for submission or filing of records.

In addition, all laws applicable to government records are applicable to e-records including retention, accessibility and disposition requirements established under the Arts and Cultural Affairs Law, the Judiciary Law, or local statute. Governmental entities that use and accept e-records must also ensure their authenticity, integrity, and security and, when appropriate, their confidentiality (see [Title 9 NYCRR Part 540.5\(d\)](#)).

Chapter 314 of the Laws of 2002, adopted on August 6, 2002, amended ESRA to provide consistency between state and federal laws that support and promote the use and acceptance of e-signatures and e-records in electronic commerce and electronic government applications. The amended ESRA definition of “electronic signature” (subdivision 3 of Section 302) has been modified to conform to the definition found in the [Federal Electronic Signatures in Global and National Commerce Act](#) (“E-Sign”). ESRA now defines an “electronic signature” as:

¹ However, ESRA (Section 307) does not apply to:

- Any document providing for the disposition of an individual’s person or property upon death or incompetence, or appointing a fiduciary of an individual’s person or property, including, without limitation, wills, trusts, decisions consenting to orders not to resuscitate, powers of attorney and health care proxies, with the exception of contractual beneficiary designations.
- Any negotiable instruments (check or notes) and other instruments of title wherein possession of the instrument is deemed to confer title, unless an electronic version of such record is created, stored or transferred pursuant to this article in a manner that allows for the existence of only one unique, identifiable and unalterable version which cannot be copied except in a form that is readily identifiable as a copy.
- Any conveyance or other instrument recordable under article nine of the real property law.

Under ESRA, OFT, as “electronic facilitator,” can exempt other types of records but it has not done so to date.

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.

This definition affords the parties to an electronic transaction the greatest possible flexibility in selecting an appropriate e-signature solution.

The ESRA regulation (Title 9 NYCRR Part 540) was amended on May 7, 2003, to reflect these amendments to ESRA. The Chief Information Officer/Office for Technology (CIO/OFT), in its role as the “electronic facilitator” under ESRA, has revised and expanded these guidelines to ensure that they are relevant to the amended ESRA and its implementing regulation. While the guidelines are targeted for use by governmental entities, private individuals and entities may also find these guidelines to be useful.

The guidelines are organized into two major sections entitled:

E-signature Guidelines (explaining the definition of an e-signature under ESRA and assisting in the selection of e-signature solutions that meet business and legal needs).

E-records Guidelines (providing general direction on ensuring the authenticity, integrity, security, and accessibility of e-records including those that are electronically signed).

The guidelines conclude with a listing of Additional Web-Available Resources on relevant e-signature and e-record topics.

Interested parties are urged to periodically visit the ESRA page on CIO/OFT’s website (<http://www.cio.ny.gov/esra/esra.htm>), to keep apprised of regulatory changes and other developments in regard to ESRA.

Governmental and private entities are also encouraged to contact CIO/OFT for additional guidance and advice on any aspect of ESRA. For detailed inquiries on specific technologies or solutions, CIO/OFT can arrange for an informal meeting or teleconference. Such meetings are most useful if technical and legal staff knowledgeable about the relevant business function and proposed technology attend.

3.2 E-Signatures Guidelines

3.2.1 Background

This section is designed to assist in understanding the definition of an e-signature under ESRA and selecting e-signature solutions that meet an entity’s business and legal needs. This section provides guidance on:

- ✓ The business and legal function of a signature.
- ✓ Determining if an e-signature solution is necessary or desirable.
- ✓ The ESRA definition of an e-signature.
- ✓ E-signature approaches.
- ✓ Selecting an e-signature approach including conducting the business analysis and risk assessment required by the ESRA regulation, 9 NYCRR §540.4(c).
- ✓ Multiple e-signatures.
- ✓ The security of systems and information used to create e-signatures.
- ✓ Consultation with the CIO/OFT concerning potential e-signature solutions.

3.2.2 How to Use this Section

It is recommended that this section be used to:

- Help determine if an e-signature is necessary or desirable.
- Serve as a starting point in a search for potential e-signature solutions.
- Select an e-signature solution that meets business needs and is appropriate to the level of risk inherent in the transaction to which the signature will be applied.
- Question and work with vendors of e-signature solutions to determine if and how their product produces an e-signature, as defined by ESRA, that meets an entity's business and legal needs.

Governmental entities are encouraged to consult with CIO/OFT in its role as Electronic Facilitator before selecting or implementing an e-signature solution. Under the ESRA regulation, §540.3(b), governmental entities must consult with CIO/OFT before defining additional standards for e-signatures and records to ensure that such standards are consistent with ESRA. It is **extremely important** to bear in mind that governmental entities must conduct and document a [business analysis and risk assessment](#) when electing to use or accept an e-signature solution.

3.2.3 Overview of the Business and Legal Function of a Signature

A signature can serve the following business and legal purposes:

- **Demonstrate intent:** A signature identifies the signer and signifies that the signer understood and intended to carry out whatever was stipulated in the document.
- **Authentication and approval:** A signature authenticates a document by linking the signer with the signed document. A signature may also express the signer's approval or authorization of the document and what it contains, and his or her intent that it has legal effect. The signature provides evidence that the signer really did something and actually saw and approved a particular document at the time of signing.
- **Security:** A signature is often used to protect against fraud, impersonation, or intrusion. For

instance, to a limited degree the signature on a check is a form of security because drafting an unauthorized check often requires forging a signature. A signature on a document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document.

- **Ceremony:** The act of signing warns or puts the signer on notice that he or she may be making a legally binding commitment. The signature will show that a meaningful act occurred when the person approved the document. A signature should force the person to deliberate over the document and become aware of its significance before making it final.

3.2.4 Determining if an E-signature is needed or desirable

Business and legal requirements and risks need to be reviewed carefully before deciding if an e-signature solution is needed or desirable. The creation and maintenance of electronically signed e-records may require more resources and effort than unsigned e-records. Government entities should consider the following questions in contemplating the use or acceptance of an e-signature solution in a transaction.

Is there a legal requirement for a signature? The law (statutes or regulations) can require a signature. The Statute of Frauds requires certain contracts to be in writing and others to be in writing and signed to be enforceable. Additionally, specific federal, state, and local government laws and regulations require signatures for various transactions.

Is there a business need for a signature? Signatures are often used on paper documents for authentication, security, or other purposes even if they are not legally mandated. For instance, it may be necessary or desirable to document through the use of a signature that a party to a transaction attested to the accuracy of the information provided, agreed to certain conditions, and/or read and understood related documents. In electronic transactions where no formal signature requirement is legally mandated, it may be desirable to address authentication and security issues with technologies and procedures that meet business needs without using an e-signature. However, system security, audit, and program management issues may have legal implications that would require an e-signature. Higher risk transactions may also need the level of protection against fraud or repudiation provided by certain types of e-signatures. Legal counsel should be consulted in considering the above issues and before deciding to implement an e-signature solution.

3.2.5 ESRA Definition of an Electronic Signature

ESRA, at §302 (3), defines an “electronic signature” as:

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.

This definition affords the parties to an electronic transaction the greatest possible flexibility in selecting an appropriate e-signature solution. However, it also sets some parameters on what constitutes an e-signature for purposes of ESRA:

“[A]n electronic sound, symbol, or process. . .”

ESRA provides that a very wide range of [digital objects](#) may serve as an e-signature. These objects can be as simple as a set of keyboarded characters or as sophisticated as an encrypted hash of a document’s contents. ESRA also allows a process to serve as an e-signature. A process can create an e-signature when a system used to create a signed e-record associates the recorded events of accessing an application with the content to be signed, thereby creating a virtual record of the signer’s actions and intent. Often such signing processes also utilize a password, PIN, or other digital object for authenticating the signer. Similarly, signing techniques that rely on a digital object may use them within a process that could include a separate authentication and certification process to capture a signer’s identity and intent.

“[A]ttached to or logically associated with . . .”

A penned signature becomes part of the physical paper document and remains with it during transit and after it is filed. Under ESRA and its enabling regulation, an e-signature is considered to be “attached to or logically associated with an electronic record” if the e-signature is linked to the record during transmission and storage. The linking of the e-record to an e-signature can be achieved by various means. For instance, a [digital signature](#) can be a discrete digital object that is part of the document in the same manner as an ink signature or it can be an object associated with the document through an embedded link. The signature object can also be maintained separately but logically associated with the record through a database, index, or other means.

When a process serves as an e-signature, the system used to create a signed e-record logically associates all the signed record’s components. An example is a document created with an official’s sign-on to a procurement system, where the official has only been authorized to access the system to create a signed procurement document. In this example, the official’s authority to sign is embedded in the system. The record is created through a sign-on authentication using a PIN or password and the official’s subsequent actions are captured while he or she is accessing the system. The record exists conceptually as a ‘document’ in the system, although the various pieces of the “record” may be maintained in various databases and system logs. The collection and maintenance of different informational pieces, along with the official’s intent to sign the record, creates an e-signature under ESRA.

Under ESRA the attachment or logical association between the signed record and signature must be created at the point a record is signed, maintained during any transmission of the signed record, and retained for as long as the signed record is needed including any subsequent storage. The creation of the electronic signature, including its attachment or logical association to the signed record, can occur in a system other than that of the government entity to which it is submitted. For example, a private sector entity that regularly submits reports to a government

agency may have an internal system that houses and formats the electronic reports. An authorized signer can electronically sign such reports at one point in time and a government entity could elect to accept those signed reports when they are electronically submitted at a later time.

Guidelines for the retention and preservation of electronically signed records, including maintaining the attachment or logical association between the signed record and signature, are provided in this document.

“[E]xecuted or adopted by a person with intent to sign the record.”

The essence of a signature is to identify the signer and signify that he or she understood and intended to carry out whatever was stipulated in the document. The ceremonial act of signing with pen and ink warns the signer that he or she may be making a legally binding commitment. ESRA requires that an e-signature be accompanied by the same intent as the use of a signature affixed by hand. ESRA does not require any specific level or method of signer identification or authentication. Therefore, governmental entities are free to select an identification and authentication method that meets their needs. The selection of an appropriate approach to identify and authenticate signers is one of the considerations in selecting an e-signature solution.

A signer’s intent can be captured in a number of ways. For example, intent can be automatically captured and documented by the signer’s actions after entering an information system. However, to avoid any confusion as to what signers intended by their actions, it is advisable that governmental entities not rely solely on a signer’s actions as recorded by a system to document intent. A number of simple practices can help avoid confusion regarding a signer’s intent:

- **Prior to applying an e-signature, afford the signer an opportunity to review the entire document or content to be signed.**
- **Make it impossible for an e-signature to be applied to a document without the signer having been informed that a signature is being applied.**
- **Format an electronically signed record to contain the same accepted signature elements contained in a paper record that allows a reader to readily identify the significance of the signature appearing on the bottom line.**
- **Allow the signer’s intent to be expressed as part of the record or in a certification statement submitted with and linked to the signed record.**
- **Require the signer to act affirmatively to indicate assent to the document being signed. For example, require the signer to click an "Accept" button. A button allowing the signer to "Reject" could also be presented to demonstrate that a choice was made. Alternately, the signer could be required to type specific words of acceptance (e.g., "I ACCEPT" or "I AGREE").**
- **Record the date, time, and fact that the signer indicated his or her intent and retain this information for evidentiary purposes. This may be different than the time the signer accessed the application or was authenticated.**

Below is an example of a generic signature attestation/affirmation statement that can be used as the basis for developing such statements for specific e-signature applications.

I agree, and it is my intent, to sign this record/document and affirmation by (describe the e-signature solution used) and by electronically submitting this record/document to (name of recipient individual or entity). I understand that my signing and submitting this record/document in this fashion is the legal equivalent of having placed my handwritten signature on the submitted record/document and this affirmation. I understand and agree that by electronically signing and submitting this record/document in this fashion I am affirming to the truth of the information contained therein.

Some e-signature products on the market specifically address the issue of the intent of an electronic signatory. These products provide a “ceremony” that warns a signer that a legally binding commitment is being made, collect contextual information about the circumstances of the signing, provide formats and visual signatures similar to those found in paper documents, and collect information concerning the signer’s intent.

3.2.6 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 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.

- **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.² 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 an identification process requiring substantial personal information and rigorous verification procedures. The strength or [entropy](#) of the password can provide additional security. The higher the entropy the more difficult the password is to guess or crack using hacker techniques. Medium and high risk transactions often require a hardened password consisting of a combination of letters, numbers, and special symbols at least eight (8) characters in length.
- **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. Digitized signatures are most often used in face-to-face consumer transactions using credit cards. In such cases the signature is rarely validated. However, some applications can compare the digitized representation of the entered signature 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.³

² 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. State agencies seeking to collect such personal information must comply with the obligations and requirements of the New York State Personal Privacy Protection Law (Public Officers Law, Article 6-A).

³ 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.

- **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.
- **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). However, biometric applications are not foolproof and have relatively high error rates. They can result in “false positives” where authentication attempts are mistakenly denied, and “false negatives” where the authentication of unauthorized persons are allowed, resulting in security breaches. Error rates can be as high as 10% for fingerprint readers and even higher for other biometric approaches.⁴ Some biometrics can be more easily spoofed than is commonly believed through the capture of fingerprint impressions using as simple a device as play-dough or modeling clay.⁵
- **Shared Private Key (Symmetric) Cryptography:** In this e-signature method, a person electronically signs using a single [cryptographic key](#) for authentication purposes that is not publicly known. The same key is used to sign a document and verify the signer’s identity, and is shared between the signer and the entity hosting the transaction requiring the signature. Therefore, the key is really not “private” to the signer and hence has lesser value as an authentication mechanism. A symmetric key can be made more secure through the use of standards-based encryption techniques and smart cards or other hardware tokens (see Smart Cards). A common and secure use of symmetric encryption for authentication is a one-time password token (e.g. RSA SecureID). This is a small secured hardware device where the symmetric key generates “one time” passwords every few minutes. The one-time password

⁴ There is extensive literature on biometric error rates. For example see **SABER (Statistical Analysis of Biometric Error Rates)** Project at St. Lawrence University <http://it.stlawu.edu/~msch/biometrics/index.htm>; the Biometric Consortium <http://www.biometrics.org/index.htm> ; Biometric Newportal http://www.biometricnewportal.com/biometrics_issues.asp .

⁵ It should be noted that the National Institute of Science and Technology (NIST) has yet to approve any biometric devices or approaches for dual authentication.

typically is displayed on the device and is inputted from the device to a computer, usually along with a PIN.

- **Public/Private Key or [Asymmetric Cryptography](#) - Digital Signatures:** 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. New York State has issued the [New York State Certificate Policies for Digital Signatures & Encryption](#) for use by State agencies and other governmental entities that choose to implement PKI technology for digital signatures and encryption purposes. Digital signatures can be implemented without the use of a CA (see **Hybrid Approaches** below).

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.

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 methods.⁶ For example, one 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. One state entity developed a hybrid e-signature solution for an application that required a very high degree of security. This approach involved strong authentication using a one-time password token and hashing techniques to achieve a high degree of non-repudiation.

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.⁷ These approaches reduce the risks of requiring individuals to protect their private keys and negate 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.

3.2.7 Selecting an E-signature Approach

The selection of an e-signature solution is foremost a business decision involving more than technical considerations. In amending ESRA in 2002, the Governor and Legislature endorsed the idea that governmental entities should utilize a process in selecting the type of e-signature solution to employ in a given transaction as a way of protecting the public's interest in the use of sound and appropriate practices in their electronic transactions with government. The ESRA regulation, § 540.4 (c), requires governmental entities to complete and document a business analysis and risk assessment of the underlying transaction when selecting an e-signature solution for use in that transaction. This business analysis and risk assessment should be viewed as a tool for governmental entities to use in the early stages of designing electronically signed transactions. The regulation defines a *business analysis and risk assessment* as:

⁶ Kristen Noakes-Fry, *E-Signatures—Digital and Electronic: Technology Overview* (Gartner Technology Overview, June 17, 2003).

⁷ V. Wheatman, *Public Key Infrastructure IH02 Magic Quadrant* (Gartner Research Note, February 14, 2002). See also *Standard for Web-based digital signatures completed*, Government Computer News (June 11, 2007) http://www.gcn.com/online/vol1_no1/44444-1.html.

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 the above definition **do not** represent a checklist of considerations in selecting an e-signature solution. They are rather factors that 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 nature and specifics of the underlying transaction. A governmental entity may determine that a particular factor has no weight for a particular transaction. For example, in completing a risk assessment the “relationships between parties to an electronic transaction” will be but one factor in determining the “risk of fraud” inherent in a given transaction. This same factor is also relevant to one’s understanding of the underlying business process to which the e-signature will be applied. In completing a business analysis, “the cost of employing a particular electronic signature process” is a business consideration that may also be used as part of a cost benefit analysis in support of the selection of an e-signature solution.

The ESRA 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 its evaluation of its business needs and the potential legal risk and resulting impact should its e-signature selection be unsuitable for the transaction in question. This section provides guidance on:

- Conducting a business analysis and risk assessment.
- Using it to select an e-signature solution.
- Documenting the process that is utilized.

This guidance is not intended to be exhaustive, and governmental entities are free to devise their own process for conducting and documenting a business analysis and risk assessment in the selection of an e-signature solution.

3.2.7.1 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.

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:

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.

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.
 - What level of assurance is needed that the signer is who he or she claims to be. One way this can be viewed is in terms of [Trust Level](#) as defined in the New York State CIO's **Best Practice Guidelines G07-001 Identity and Access Management: Trust Model** (referred to hereafter as **NYS Trust Model**).

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.

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 participants 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.

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. Alternately, 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.

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.

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 legal, security and technological 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.⁸

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

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.

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.

⁸ The National Institute of Standards (NIST) has published guidelines for risk management for information systems. See Gary Stoneburner, Alice Goguen, and Alexis Feringa, **Risk Management for Information Technology Systems: Recommendations of the National Institute of Standards and Technology** (NIST Special Publication 800-30, January 2002) available at <http://csrc.nist.gov/publications/nistpubs/index.html>.

- 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.

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.

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).

Governmental entities 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

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

In selecting an e-signature solution the business analysis and risk assessment should be viewed as integrated, mutually supporting processes. It is up to the governmental entity to identify its overriding concerns in the selection of an e-signature solution. In many cases the selection of an e-signature approach will be the result of balancing business concerns, such as user acceptance and ease of deployment, with the reduction of risks. Often combining features from various e-

signature approaches will achieve such a balance. In some cases, the existence of established or de facto standards in a field, or the need or ability to achieve compatibility with an existing e-signature solution employed by others, will be overriding factors. Budget constraints will also be a key consideration in the selection process and cost may be an overriding consideration where risks are low.

Matching E-signature Functionality to Risk Level: In integrating the risk considerations into the e-signature selection process, governmental entities should consider that **within** and **between** each general approach to e-signing the level of certainty of identifying the signer, attributing a signature, and securing the integrity of both the record and the signature can vary tremendously. Therefore, governmental entities may want to investigate how various components of an e-signature solution can reduce risks. Some components discussed below can be incorporated into any e-signature solution regardless of the general approach adopted, thereby reducing risks.⁹

Signer identification or registration is the method or process used to identify and authorize an individual to use a particular e-signature application. Signer identification is independent of the signature or record creation technology employed. However, it is a critical component of any e-signature solution because 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. This can help protect against fraud and repudiation. Prior to implementing an e-signature solution, governmental entities should consider whether or not existing processes for registering the identity or existence of participants in a transaction need to be refined or will suffice. It is recommended that State government entities use the **NYS Trust Model** to select the Trust Level that provides the identity registration and verification processes that best address the risk inherent in the transaction under consideration. Local government entities should consider using the **NYS Trust Model** or something equivalent for the same purposes. Entities may wish to use the opportunity afforded by moving to an online environment to implement a more rigorous approach to identifying participants that is consistent with a higher Trust Level. The following chart provides some identification options linked to Trust Levels found in the **NYS Trust Model** and the risk levels where their implementation may be appropriate.

Identification Methods	Level of Risk
Trust Level 1 – little or no confidence in the asserted identity’s validity. No registration, only self-identification as	Negligible or very low

⁹ An exception is PKI supported solutions, where components and options are specified in the operative Certification Policy.

part of the signing process	
<p>Trust Level 2 – confidence exists that the asserted identity is accurate.</p> <p>Visual inspection of a photo-identification issued by state/federal officials in the presence of the individual.</p> <p>Individual supplies identification information that is independently verified by a trusted data source to be valid and consistent.</p> <p>Acceptance of a previously conducted and trusted identification and registration process that meets one of the above criteria.</p>	Low
<p>Trust Level 3 – high confidence in the asserted identity’s validity.</p> <p>Individuals provide, in-person, two pieces of valid and unexpired government-issued identification (certified copies or originals) that are consistent and independently verified as valid by a trusted data source.</p> <p>Acceptance of a previously conducted and trusted identification and registration process that meets one of the above criteria.</p>	Medium/High
<p>Trust level 4 – very high confidence in the asserted identity’s validity.</p> <p>A separate identification process to authorize the use of an e-signature where individuals provide in-person two pieces of valid and unexpired government-issued identification (certified copies or originals) that are independently verified by a trusted data source to be valid and consistent.</p>	High

There are many variations on the approaches presented above, including requiring specific identification documents. For instance, the **NYS Trust Model**, Trust Level 3, requires two pieces of identification (certified copies or originals), at least one of which is a government identification containing a photograph (e.g., driver’s license, non-driver identification, passport) for medium or high-risk transactions.¹⁰ Identification may also include a follow-up verification process sometimes conducted by a third party.

Signer Authentication refers to 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 for additional information on authentication). The strength of the authentication system, including the level of trust that the credential or information used to authenticate has remained in the signer’s sole possession, can protect against fraud and repudiation. State government entities should use the **NYS Trust Model** to select the Trust Level that provides the authentication methods that best address the risk inherent in the transition under consideration. Local government entities should consider using the **NYS Trust Model** or something equivalent for the same purposes. The following chart provides some authentication options and the risk levels where they may be appropriately used.

Authentication Methods	Level of Risk
No method of authentication beyond user identification as part of the signing process	Negligible
Trust Level 1 User selected PIN or password	Negligible to Low
Trust Level 2 A hardened password of sufficient length and complexity to make it statistically difficult to crack.	Low to Medium
Trust Level 3 If over a private trusted network, a hardened password assigned of sufficient length and complexity to make it statistically difficult to crack. Dual factor authentication, using a	Medium to High

¹⁰ State agencies seeking to collect personal information must do so in compliance with the mandates and requirements of New York State’s Personal Privacy Protection Law (Public Officers Law, Article 6-A)

password and a cryptographic-based hard or soft token.	
Trust Level 4 Dual factor authentication, using a password and a cryptographic-based hard token or smart card.	High

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. Various e-signature approaches provide different levels of protection for an e-records integrity. This protection can be achieved by the system that collectively manages the e-record and the associated e-signature. In such a case, the key factor is the system's trustworthiness and its controls to ensure that a record or signature has not been tampered with or modified, as well as the system's ability to detect if that has occurred. Governmental entities may also need to implement controls to ensure that the integrity of the electronically signed record is not compromised during transmission. Added security is provided by technologies (e.g., digital signatures) where the validation of the signature itself ensures that the record and signature have not been tampered with or modified. The following chart provides some e-signed record integrity options and the risk levels where they may be appropriate.

Record Integrity Security Options	Level of Risk
System reasonably ensures the integrity of the record and the signature and record link	Negligible to low
The above plus use of a secure network or secure cryptographic method (e.g., secure socket layer (SSL) or VPN) to transfer the electronically signed record	Low to medium
All of the above plus use of a cryptographic method with hashing techniques to ensure record integrity and the link between the record and the signature (e.g., PKI)	Medium to high

Cost-Benefit Analysis: Governmental entities, 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.

3.2.7.3 Documenting a Business Analysis and risk Assessment

Business Analysis and Risk Assessment

The ESRA regulation requires that the business analysis and risk assessment used in the selection process for an e-signature solution be documented. However, the regulation does not specify how, or in what detail, the analysis and assessment must be documented. This decision is left to the governmental entity. The following principles should be considered when documenting a business analysis and risk assessment:

- Documentation should:
 - Describe the process used to conduct the business analysis and risk assessment.
 - Include the results of the business analysis and risk assessment addressing the factors specifically mentioned in the ESRA regulation, [§ 540.2\(a\)](#)
 - Conclude with the decision reached on an e-signature approach and include support or justification for this decision.
- The resulting documentation should be:
 - Accurate and readily available.
 - Clear and understandable to an outside audience as well as current and future staff who may be asked to explain the decision making process.
 - Retained as long as the e-signature solution is used.

A governmental entity may elect to develop a more formal business case document that would evidence the business analysis and risk assessment employed in the selection of its e-signature

solution. For instance, the development of a more formal record may be justified where an entity anticipates its selection to be disputed by third parties.

3.2.8 Special Issue: Multiple Signatures

Records that require multiple signatures raise the same issues involved with single e-signatures as well as a number of unique concerns. As with any signature application, governmental entities need to ask themselves whether or not additional signatures are legally required and/or necessary for business purposes. Multiple signatures will typically be required if multiple approvals are needed to complete a transaction, information is collected from multiple individuals and each must attest to its accuracy, multiple individuals need to be held accountable for actions, there is a risk of repudiation or fraud from a number of individuals to a transaction, or contractual documents are required to be signed by all parties to a transaction. To conform to the ESRA definition of an e-signature, each e-signature must be attached to or associated with the e-record being signed during transmission and storage, each must be executed or adopted by an identified individual who intends to sign the record, and the signing process must capture each signer's intent.

If multiple signatures are required or desirable, the various risks, benefits, and costs should be considered as part of a governmental entity's business analysis and risk assessment in selecting an e-signature solution. Some issues unique to multiple e-signatures include:

- What cost impact will multiple signatures have on the implementation of an e-signature solution?
- What impact will the collection of multiple signatures have on proving the authenticity of an e-record over time?
- What impact will the collection of multiple signatures have on the ability to retain an e-record with a retention period of over 10 years?
- Is the chronological sequence of signing important? How will the system ensure that signatures are applied in the appropriate sequence and will the sequence of signatures be documented?
- Will signers be signing the entire document or only specific sections? How will signatures be associated with the appropriate sections of the document?
- Will the intent or purpose of each signer be the same or different? How will the different intents of the various signers be documented?

3.2.9 Special Issue: Security of Systems and Information Used to Create E-signatures

State governmental entities should have system security policies and programs that are compliant with the NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) [PO 03-](#)

002 Information Security Policy. A security policy and program for systems and information used to create and/or authenticate e-signatures may require some additional elements including:

Role of Signer: The important information used to create and authenticate e-signatures requires a high-level of security as well as some special considerations. Regardless of signature approach the role of the signer is critical to securing e-signature information. Information used to create an e-signature should be under the sole control of the signer. Therefore, a key component of the security of e-signatures is dependent on the signer's behavior. The behavioral standards followed by signers should include the following:

- Not disclosing information used to create a signature to a person not authorized to sign on his or her behalf.
- Preventing unauthorized use.
- Taking precautions not to lose the medium, if used, on which the information is recorded.
- Preventing eavesdropping during use of such information in insecure circumstances. Ensuring that access controls prevent unauthorized access to computer equipment on which such information resides. Eavesdropping could take the form of key logging software (or "spyware") that can be installed over a network, or by direct access to a target computer, and can be used to discover entered passwords or security keys.
- Taking appropriate measures to ensure that the information cannot be used to sign if it is lost or compromised.

Special Requirements for the Protection of Cryptographic Keys: Cryptographic methods impose specific requirements on both individual signers and governmental entities to protect the cryptographic keys used to sign. It should be noted that NIST has developed comprehensive guidelines for the management of cryptographic keys.¹¹ The following principles should be pursued in managing cryptographic keys used for signing purposes.

Cryptographic keys used to create e-signatures should not be used for other purposes: These other purposes include encryption and challenge/response authentication. This principle is particularly important with technologies using asymmetric cryptography, such as public key infrastructure (PKI), where the information or key used to validate the signature is different than the information or key used to create the signature. Such systems can support multiple security services along with e-signatures. The principle of ***separation of keys*** is designed to prevent misuse or compromise of keys including inappropriate disclosure of [private keys](#) used for signing and weakening of encryption.

Cryptographic keys used to sign should be generated so that they are only revealed to or can be used by the intended electronic signatory: The key can be generated by the actual user and installed for use within his or her hardware or software by a variety of techniques

¹¹ [SP 800-57 Recommendation on Key Management](#) (August 2005 rev. June 2006).

including one or more of the following: manual entry, transfer of a disk, read-only-memory device, smart card or other hardware token. The initial information used to establish an e-signature (often referred to as *keying material* in [asymmetric crypto-systems](#)) may serve to establish a secure online session through which a cryptographic key is generated and installed.

Distribute keys used to sign so they are revealed only to the intended signer: Keys can be distributed by manual methods, automated methods, or a combination of automated and manual methods. Manually distributed keys may be entered or outputted through purely manual methods such as a keyboard or by electronic methods such as hardware tokens (e.g., smart cards). When a key is entered the following precautions should be taken:

- The key should not be displayed in a decipherable or [plaintext](#) form.
- A means should be provided to ensure that the key is associated with the intended signer.
- The key should be entered into or outputted from a system component in encrypted form or using split knowledge procedures where it is entered as two or more plaintext components. When a key is entered or output under split knowledge procedures, the system should provide the capability to separately authenticate the person entering each component.

An electronically distributed key should be entered or outputted directly from the creating system (e.g., via a trusted path or directly attached cable), without traveling through any enclosing or intervening systems where the information could be stored, combined, or otherwise processed.

A key used to create an e-signature must be stored so that only the intended signer can use it solely for signing purposes: The key should not be accessible from outside of the signing application. It can be stored as part of software, hardware, or as an offline hardware token such as a smart card.

- **Storage on personal computers:** The storage of a cryptographic key within software applications such as browsers affords the lowest level of security. If stored on a personal computer, the key should reside in a software or hardware component that is password-protected or protected in some other way. Storing the key in an encrypted form will afford a higher-level of security. Storing it as an encrypted software token separate or independent of other applications is more secure. It is **not** recommended that a signing key be stored in an Internet browser even if it is in encrypted form. The key must be decrypted to be used. Sophisticated attackers could gain access to a key by writing a program that manages to get itself run on a user's computer, waits for the signing information to be decrypted, and then sends it out over the network. User profiles and personal information including signing information in browsers can be protected through

high security settings. However, security for popular browsers is usually set at medium by default, which makes such attacks possible.

- Storage on hardware tokens:** The storage of a signing key on hardware tokens such as smart cards affords a higher-level of security if signers appropriately protect them. Hardware tokens should not allow export or import into the storage area used for signing information. They should also require a PIN, passwords, or other security parameters for access and use. Preventing signers from obtaining direct access to their own signing information may prevent its intentional or unintentional disclosure.

3.2.10 Governmental Entity Consultation with CIO/OFT

The ESRA regulation, at 9 NYCRR §540.3 (b), requires governmental entities to consult with CIO/OFT before defining additional standards for e-signatures and e-records to ensure that such standards are consistent with ESRA. Additionally, as the “electronic facilitator” under ESRA, CIO/OFT provides informal advice and guidance to governmental entities seeking to select an appropriate e-signature solution for use in an electronic transaction. Governmental entities contemplating the use or acceptance of an e-signature solution should confer with CIO/OFT early in the planning process. For detailed inquiries on specific technologies or e-signature solutions, or on how to complete and document the requisite business analysis and risk assessment process, CIO/OFT can arrange for an informal meeting or teleconference. Such meetings are most useful if technical and legal staff knowledgeable about the relevant government function and proposed technology attend.

Summary E-records Guidelines

<p>General Concepts and Guidelines</p> <p><i>Identify and assess specific legal, business, and other requirements that apply to e-records</i></p> <p><i>Base e-records management measures on the records’ value</i></p> <p><i>Focus on the systems and business processes that produce e-records</i></p> <p><i>Training is critical</i></p>

Producing E-records	
Outcomes	Implementations
Produce a record for each business transaction that complies with all legal or other requirements regarding	Develop and document clear procedures and processes for the receipt, creation, and storage of e-

the record's structure, content, and time of creation or receipt	<p>records</p> <p>Designate a receiving device</p> <p>Establish controls for the accuracy and timeliness of input and output</p>
Authenticate (prove the identity of) the sender of the record (if necessary) and make sure the e-record has not been altered	<p>Establish policies and procedures to authenticate senders and determine the integrity of each type of e-record</p> <p>Establish measures to secure transmission of e-records including the integrity of records during transmission and processing</p> <p>Provide and maintain measures to authenticate the identity of the sender based on potential risk and legal requirements</p> <p>Maintain measures to document the date and time of receipt</p> <p>Confirm receipt (when necessary)</p>
Uniquely identify each record	Establish a method to uniquely identify each record
Capture an e-record for each transaction conducted through a multi-entity web portal	<p>Determine who owns the data and records captured in the portal</p> <p>Define the participants' roles and responsibilities in managing data and records</p> <p>Maintain e-records of transactions conducted in the portal in secure e-records system</p>

Maintaining Authentic, and Complete E-records that are Accessible Over Time

Outcomes	Implementations
Maintain integrity of e- records as captured or created so that they can be accessed, displayed, and managed as a unit	<p>Maintain e-records management policy documenting the organization's policy on information management and storage</p> <p>Develop controlled storage or filing systems that maintain the integrity and accessibility of e-records</p>

<p>Retain e-records in an accessible form for their legal minimum retention periods</p>	<p>Adopt and use records retention and disposition schedules in compliance with the Arts and Cultural Affairs Law or local law</p> <p>Develop a contingency plan that includes data backup, disaster recovery, and emergency operations</p> <p>Implement media controls</p> <p>Perform routine backups</p> <p>Maintain e-records in encrypted form only as long as security concerns warrant</p> <p>Develop retention solutions that best address an e-record's retention requirements</p> <p>Address long-term retention requirements and records preservation</p> <p>Ensure that records are destroyed once retention periods are met and records are no longer needed for business or legal purposes</p>
<p>Search and retrieve e-records in the normal course of business for all business uses throughout their entire legal minimum retention period</p>	<p>Maintain adequate search and retrieval capabilities to ensure that e-records can be retrieved for all legitimate business purposes for their full retention period</p>
<p>Produce authentic copies of e-records and supply them in useable formats, including hard copy, for business purposes and all public access purposes</p>	<p>Develop or revise access and personal privacy protection policies to include e-records</p> <p>Develop methods to provide public access to e-records and to protect personal privacy and confidentiality</p> <p>Provide access to e-records in the form the user prefers</p>
<p>Develop an approach to maintain the authenticity and integrity of electronically signed e-records</p>	<p>Determine what information needs to be retained to maintain a valid, authentic, and reliable signed e-record</p> <p>Preserve the link or association between the various components of a signed record over time</p>

Maintaining Secure, Reliable and Trustworthy E-records Systems

Outcomes	Implementations
<p>Make sure the system performs in an accurate, reliable, and consistent manner in the normal course of business</p>	<p>Define and document system management and operation</p> <p>Define and document system management policies and procedures</p> <p>Assign system management roles and responsibilities, and implement the principle of separation of duties pursuant to written policies</p> <p>Develop and maintain problem resolution procedures including incident reporting and response procedures</p> <p>Develop notification procedures that conform to the NY State Information Security Breach and Notification Act</p> <p>Test system performance including the reliability of hardware and software</p> <p>Maintain audit trails of system activity by system or application processes and by user activity</p> <p>Provide training and user support to ensure users will implement system procedures</p>
<p>Limit system access to authorized individuals and for authorized purposes and maintain physical and environmental security controls</p>	<p>Establish a system security policy and program compliant with NYS Technology Policy related to information security</p>

Additional Web-Available Resources

1. New York State Standards, Guidelines and Resources

OCIO and [CIO/OFT Policies, Standards and Guidelines Related to E-signatures and E-records](#) including:

[NYS Trust Model Best Practice Guideline](#)

[New York State Certificate Policies for Digital Signatures & Encryption](#)

[ESRA Regulations \(Part 540\)](#)

[ESRA Law](#)

[November 2002 ESRA Report to the Governor and Legislature](#)

[November 2004 ESRA Report to the Governor and Legislature](#)

[New York State Archives' Guidelines Most Relevant to E-signatures and E-records](#) including:

Imaging Production Guidelines (2006)

Conducting Needs Assessments for New Recordkeeping Systems (Technical Information Series #64)

Preparing for the Worst: Managing Records Disasters (Technical Information Series # 82)

Managing Voice Mail Records (online service)

Managing E-Mail Effectively (Technical Information Series #62)

Services for Managing Records Communicated via Electronic Mail (online service)

Records Management Software Guidelines (online service)

Guidelines for Choosing Records Management Software (Technical Information Series #63)

Indexing Minutes Web Service (online service)

Managing Geographic Information Systems (GIS) Records (online service)

General Retention and Disposition Schedule for New York State Government Records, Effective April 1997 through March 2002

Local Government Records Retention Schedules

Records Retention and Disposition Schedule CO-2: for used by Counties.

Records Retention and Disposition Schedule MU-1: for use by Municipalities -- Cities, Towns, Villages and Fire Districts.

Records Retention and Disposition Schedule ED-1: for use by School Districts, BOCES and Teacher Centers.

Records Retention and Disposition Schedule MI-1: for use by Miscellaneous Local Governments.

Retention and Disposition of Library and Library System Records

Retention and Disposition Schedule: Election Records: For Use by New York County Boards of Elections

2. Other New York State Resources

Committee on Open Government, Department of State, e-mail, opengov@dos.state.ny.us; web, <http://www.dos.state.ny.us/coog/coogwww.html> provides the complete text of the NYS Freedom of Information law as well as FAQs and advisory opinions that specifically address e-records issues.

Electronic Records Guidelines (Unified Court System website)

3. Other Resources

[Center for Technology in Government, University at Albany](#)

Building State Government Digital Preservation Partnerships: A Capability Assessment and Planning Toolkit, Version 1.0

Opening Gateways: A Practical Guide for Designing Electronic Records Access Programs

Practical Tools for Electronic Records Management and Preservation

The Records Requirements Analysis and Implementation Tool

Preserving State Government Digital Information: A Baseline Report

State Government Digital Preservation Profiles

Exemplary Practices in Electronic Records and Information Access Programs

Models for Action: Practical Approaches to Electronic Records Management & Preservation

Functional Requirements to Ensure the Creation, Maintenance, and Preservation of Electronic Records

A Survey of Key Concepts and Issues for Electronic Recordkeeping

A Framework for Evaluating Public Sector Geographic Information Systems

Cornell University, [Digital Preservation Management: Implementing Short-Term Strategies for Long Term Problems](#) (online tutorial)

Council on Library and Information Resources (CLIR), [The State of Digital Preservation: An International Perspective](#). Provides a good overview of research and development activities and technical approaches to digital. CLIR, [Authenticity in a Digital Environment](#).

Commission on Preservation and Access, [Magnetic Tape Storage and Handling](#)

Joint Interoperability Test Command, DISA, DoD, [Records Management Application \(RMA\) Certification Testing](#)

National Institute of Standards and Technology, [NIST Computer Security Special Publications](#) provides many standards and guidelines publications related to digital signature, PKI, system security, risk management, and other relevant topics.

[National Archives of Australia](#) provides a number of very useful guidelines and publications on the management and preservation of e-records.

National Archives and Records Administration (NARA) [Records Management Guidance for Agencies Implementing Electronic Signature Technologies](#)

National Archives and Records Administration (NARA), [Electronic Records Management Initiative](#) contains information on a number of NARA activities to address e-records management activities.

[National Electronic Commerce Coordinating Council \(NECCC\)](#) has produced a number of white papers on e-records management and e-signature topics.

Office of Management and Budget (OMB), [Appendix II to OMB Circular No. A-130 Implementation of the Government Paperwork Elimination Act](#)

Office of Management and Budget (OMB), [Guidance on Implementing the Electronic Signatures in Global and National Commerce Act](#)

4. Resources on the Security of E-signatures Created by Cryptographic Technologies

Some e-signature technologies are based on cryptographic techniques, including public key infrastructure (PKI) and pretty good privacy (PGP). The federal government has developed a set of technical standards and guidelines on the security of cryptographic systems and system components that are relevant to the security of e-signatures created by such systems.

Governmental entities that use cryptographic systems for creating e-signatures are referred to the following federal resources.

[FIPS 140-2, Security Requirements for Cryptographic Modules](#) defines security requirements covering 11 areas related to the design and implementation of a crypto-module including the cryptographic keys used to create and authenticate e-signatures. Within most areas, a crypto-module receives a security level rating (from 1 to 4, 1 being the lowest rating). Cryptographic keys used for signing should meet at least a 3 security level rating.

Other helpful federal documents include [Special Publication 800-21: Guideline for Implementing Cryptography in the Federal Government](#), which provides guidance to federal agencies on how to select cryptographic controls for protecting Sensitive Unclassified information and [Special Publication 800-12 An Introduction to Computer Security: The NIST Handbook](#).

4.0 Definitions of Key Terms

A complete listing of defined terms for NYS Information Technology Policies, Standards, and Best Practice Guidelines is available in the "NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary" (<http://www.cio.ny.gov/policy/glossary.htm>). The following defined terms are used in this Best Practice Guideline.

Alphanumeric - Describes the combined set of all letters in the alphabet and the numbers 0 through 9. It is useful to group letters and numbers together because many [programs](#) treat them identically and differently from [punctuation characters](#). For example, most [operating systems](#) allow you to use any letters or numbers in [filenames](#) but prohibit many punctuation characters. Your [computer](#) manual would express this rule by stating: "Filenames may be composed of alphanumeric characters."

Asymmetric or public key cryptography or crypto-system - A system of cryptography that employs two computationally related alphanumerics usually known as a key pair. A private key, known only to the holder, is used to create an e-signature or decrypt, and the other or public key known to others is used to verify the e-signature or encrypt. Public key cryptography is often employed within the context of a [public key infrastructure \(PKI\)](#).

Biometrics - In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints or speech.

Business analysis and risk assessment – is defined by the ESRA regulation 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.”

Checksum - A simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set [bits](#) in the message. The receiving station then applies the same formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been garbled.

Cryptographic - Related to cryptography which is (i) The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key (ii) A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized uses.

Cryptographic keys – Data used to encrypt or decrypt a message or information.

Digital object - Any discrete set of digital data that can be individually selected and manipulated. This can include shapes, pictures, string of numbers, or characters that appear on a display screen as well as less tangible software entities.

Digital Signatures - are produced by two mathematically linked [cryptographic keys](#), a private key used to sign, and a public key used to validate the signature. A digital signature is created when

a person uses his or her private key to create a unique mark (called a "signed hash") on an electronic document. The recipient of the document employs the person's public key to validate the authenticity of the digital signature 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.

Electronic record (E-record) – Shall have the same meaning as defined in State Technology Law §302. This shall mean “information, evidencing any act, transaction, occurrence, event, or other activity, produced or stored by electronic means and capable of being accurately reproduced in forms perceptible by human sensory capabilities.” This definition is consistent with the definition of “records” in the laws that govern the admissibility of records in legal proceedings (including Civil Practice Law and Rules sec. 4518), the retention and disposition of government records (Arts and Cultural Affairs Law Art. sections 57.05 and 57.17), and the Freedom of Information Law (Public Officers Law Art. 6, sec. 86).

Electronic Signature (E-signature) – Shall have the same meaning as defined in State Technology Law §302. This shall mean “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.” This definition conforms to the definition found in the Federal E-Sign Law.

Entropy - A measure of the amount of uncertainty that an attacker faces to determine the value of a secret such as a password. Entropy is usually stated in bits. See NIST 800-63 Recommendation for Electronic Authentication.

Governmental Entity – Shall have the same meaning as defined in State Technology Law §302. This shall mean “any state department, board, bureau, division, commission, committee, public authority, public benefit corporation, council, office, or other governmental entity or officer of the state having statewide authority, except the state legislature, and any political subdivision of the state.”

Hashing - Producing *hash values* for accessing [data](#) or for [security](#). A hash value (or simply *hash*) is a number generated from a [string](#) of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hashes play a role in security systems where they are used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, [encrypts](#) it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they are the same, there is a very high probability that the message was transmitted intact.

Independently verified - Information provided by a user is verified to a source that is independent of the user (most often a trusted database) which finds that the claimed identity exists and is consistent with the identity and address information provided.

Pretty Good Privacy (PGP) - A technique for [encrypting](#) messages developed by Philip Zimmerman. PGP is one of the most common ways to protect messages on the [Internet](#) because it is effective, easy to use, and free. PGP is based on the [public-key method](#), which uses two keys -- one is a public key that you disseminate to anyone from whom you want to receive a message. The other is a private key that you use to [decrypt](#) messages that you receive. To encrypt a message using PGP, you need the PGP encryption package, which is available for free from a number of sources. The official repository is at the Massachusetts Institute of Technology.

Plaintext - In cryptography, plaintext refers to any message that is not encrypted and therefore easily read and understood.

Private key - A cryptographic key kept secret or known only by the holder. Private keys can be used to create e-signatures or decrypt messages or files. The same private key used to sign should not be used to decrypt.

Public Key Infrastructure (PKI) - The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based asymmetric or public key cryptographic system. The PKI consists of systems that collaborate to provide and implement e-signatures, encryption, and authentication services.

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

Secure Sockets Layer (SSL)- This is a [protocol](#) developed by [Netscape](#) for transmitting private documents via the [Internet](#). SSL works by using a private [key](#) to [encrypt](#) data transferred over the SSL connection. Both [Netscape Navigator](#) and [Internet Explorer](#) support SSL, and many [Web sites](#) use the protocol to obtain confidential user information, such as credit card numbers. By convention, [Web pages](#) that require an SSL connection start with *https:* instead of *http:*. SSL has been approved by the [Internet Engineering Task Force \(IETF\)](#) as a [standard](#).

Smart card - A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and possesses some inherent resistance to tampering.

S/MIME - Short for *Secure/MIME*, a new version of the [MIME protocol](#) that supports [encryption](#) of messages. S/MIME is based on [RSA's public-key encryption](#) technology. It is expected that S/MIME will be widely implemented, which will make it possible for people to send secure e-mail messages to one another, even if they are using different e-mail clients.

Token - A small hardware device used for security purposes to store confidential user identification or authentication information such as a **private key**.

Trust Level - Trust is defined as:

- the degree of confidence in the vetting process used to establish the identity of the individual to whom the *credential* was issued
- the degree of confidence that the individual who uses the *credential* is the individual to whom the *credential* was issued.

An appropriate *trust* level for *user credential* and *authentication* must be assigned and implemented to protect the integrity and confidentiality of the *information* and validity of *transactions*. The four trust levels supported by the NYS Trust Model are:

<i>Level</i>	<i>Description</i>
1	Little or no confidence in the asserted identity's validity.
2	Confidence exists that the asserted identity is accurate.
3	High confidence in the asserted identity's validity.
4	Very high confidence in the asserted identity's validity.

Trustworthy system - Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

Virtual Private Network (VPN) - A *network* that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use [encryption](#) and other [security](#) mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

5.0 CIO/OFT Contact Information

This Guideline provides a starting point for those 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:

NYS Chief Information Officer/Office for Technology
 Counsel and Legal Services
 State Capitol Empire State Plaza
 PO Box 2062

Albany, NY 12220-0062

518-473-5115 voice

nyecom@cio.ny.gov

<http://www.cio.ny.gov/ecommerce/index.htm>

The State of New York Enterprise IT Policies may be found at the following website:

<http://www.cio.ny.gov/policy/technologypolicyindex.htm>

6.0 Revision Schedule and History

Date	Description of Change
5/26/2004	Original Guidelines issued.
9/28/2007	Revised and republished.
10/23/2007	Reformatted and updated to reflect current CIO, agency name, logo and style.