NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Guideline	**No:** NYS-G04-001
IT Guideline:	**Updated:** 9/6/2017
Electronic Signatures and Records Act	**Issued By:** NYS Office of Information Technology Services **Owner:** Division of Legal Affairs

1.0 Purpose and Benefits

This best practice guideline:

- explains the definition of an e-signature under the Electronic Signatures and Records Act (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.[1]

2.0 Authority

State Technology Law, and Section 2 of Executive Order No. 117, provide the State Chief Information Officer and the Office of Information Technology Services (ITS) the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in *NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.*

[1] Terms defined in this Guideline's Glossary are, in their original use in this ESRA Guideline, colored in blue.

3.0 Scope

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 ESRA Guidelines useful.

4.0 Information Statement

4.1 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.[2] ESRA does not require private parties or governmental entities to use or accept e-signatures or e-records, unless some other law provides otherwise. In other words, the use and acceptance of e-signatures or e-records is completely voluntary in most cases. 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;

---

[2] 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 and the registration of making an anatomical gift in accordance with the Public Health Law and related regulations.
- 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.

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

- Accept hard copy documents for submission or filing, unless otherwise required by law; and
- Not require someone to submit or file records electronically, unless otherwise provided by law.

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) was modified to conform to the definition found in the Federal Electronic Signatures in Global and National Commerce Act ("E-Sign"). So, since 2002, ESRA 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.

When originally enacted in 2000, ESRA excluded real property conveyances and recordable instruments from its provisions. ESRA and the Real Property Law were amended by Chapter 549 of the Laws of 2011, and as of September 23, 2012 local recording officers can elect to participate in the electronic recording of instruments affecting real property, which is referred to generally as e-Recording.

The ESRA regulations (Title 9 NYCRR Part 540) were subsequently revised to reflect these amendments to ESRA, and are subject to periodic additional updating in accordance with the NY State Administrative Procedure Act, with the most recent revisions expected by 2018.

The NYS Office for Information Technology Services (ITS), in its role as the "electronic facilitator" under ESRA, has revised and expanded these ESRA Guidelines to ensure that they remain relevant to the amended ESRA, its current implementing regulations, and changes in laws and technologies. While the ESRA Guidelines are targeted for use by governmental entities, private individuals and entities may also find these ESRA 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 ESRA Guidelines conclude with a listing of additional online resources on relevant e-signature and e-record topics.

Interested parties are encouraged to periodically visit the ESRA page on ITS' website (https://its.ny.gov/electronic-signatures-and-records-act-esra) to keep apprised of regulatory changes and other developments in regard to ESRA. Governmental and private entities are also encouraged to contact ITS for additional guidance and advice on any aspect of ESRA.

4.2 E-Signatures Guidelines

4.2.1 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 of governmental entities 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 ITS concerning potential e-signature solutions.

4.2.2 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 ITS 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 ITS 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.

4.2.3 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 that is signed.
- **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 signed 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.

4.2.4 Determining if an E-signature is Needed or Desirable

Business and legal requirements and transactional 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 and other documents 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.

4.2.5 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 later 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 signed 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 captured in a paper record allowing 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 modified for use with specific e-signature applications.

> I agree, and it is my intent, to sign this record/document 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 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.

4.2.6 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 in section 4.2.7.

- **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.[3] 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 ***Transport Layer Security (TLS)***. TLS 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, **alphanumeric** numbers, and special symbols at least eight (8) characters in length. The user might be forced to authenticate using a security **token** or digital certificate and a second password different than the one that they log on to for accessing enterprise low risk systems, application and information.

- **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.[4]

---

[3] 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).

[4] 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.

- **S-signatures:** Some federal agencies expressly allow or require the use of S-signatures in various scenarios, as opposed to graphical, digitized images of handwritten signatures. For example, federal regulation 37 CFR 1.4 concerning correspondence with the United States Patent and Trademark Office prescribes rules for signing formal correspondence exchanged with the Office using S-signatures, and at section (d)(2) defines such a signature as follows: "An S-signature is a signature inserted between forward slash marks . . . includ[ing] any signature made by electronic or mechanical means, and any other mode of making or applying a signature other than a handwritten signature." The U.S. Bankruptcy Court for the Southern District of California expressly allows S-signatures on certain forms, see: www.casb.uscourts.gov/html/cmecf/Tutorial/Rules_forms/04b_1547.html. And the federal Department of Health and Human Services has a specific "Standard and Usability Guideline" for signatures posted on DHHS websites indicating that because of the risk of identity theft and misuse, "Images of an original official signature should not be displayed, especially on a publicly accessible Web site." Instead, DHHS recommends that the "proper way to indicate an official signature for a document on a Web site (when there is a requirement that a signature be displayed) is the S-signature." https://webstandards.hhs.gov/standards/41. So long as an S-signature meets the other indicia of an electronic signature under ESRA, it has the same validity as any other e-signature.

- **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, face recognition, DNA, palm print, gait analysis, hand geometry, and retinal and iris recognition. 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). Biometric accuracy continues to improve as technology advances. However, biometric applications are not foolproof. 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. Although biometrics at one time were more easily spoofed, technology has advanced to a point where spoofing is far less possible. For instance, technologies such as liveness detection are used to ensure that only characteristics from a living human being can be enrolled, stored and recognized in a biometric system.[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 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

[5] The National Institute of Science and Technology (NIST) created the "NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards" which can be found at http://www.biometrics.gov/standards/. This policy was drafted by the NSTC Subcommittee on Biometrics and Identity Management and was approved by the NSTC Committee on Technology in September 2007. The goal of the Policy is to establish a framework to reach interagency consensus on biometric standards adoption for the Federal government.

involved in the PKI. Digital signatures can be implemented without the use of a CA (see Hybrid Approaches below).

- **Microchip Devices:** Microchip Devices can be any device that may contain a microchip and can be used for identification purposes. This may be a smart card that is a plastic card the size of a credit card, a USB drive, a watch or phone 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 may insert the microchip device into a microchip reader attached to a computer or network input device or the device may be read through contactless technology such as a radio frequency reader.[6] Information from the device'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 microchip device, not between the user and a computer. Therefore, microchip devices can be used to further augment the security of a shared secret approach to e-signatures. Microchip devices 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. For example, a solution may involve improved signature-capture techniques combined with click wrap and PINs and password approaches. This solution would enhance 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 hybrid solution could provide 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. Some governmental entities have developed hybrid e-signature solutions for applications requiring a very high degree of security, involving 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

[6] http://www.smartcardalliance.org/smart-cards-faq

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. For commercial solutions, the e-signature market has matured and there are several possible solutions available that may be compatible with ESRA.

4.2.7 Selecting an E-signature Approach

The selection of an e-signature solution is foremost a business decision involving more than technical considerations. Amendments to ESRA in 2002 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. To this end, the ESRA regulation, 9 NYCRR § 540.4 (c), requires governmental entities to complete and document a business analysis and risk assessment of the underlying electronic transaction when selecting an e-signature solution for use in that transaction. Governmental entities are not required to submit such analyses and assessments to ITS for approval, but instead should maintain documentation of this exercise for future use should the selection of an electronic signature technology or process be called into question. As the "electronic facilitator," ITS is available to consult with governmental entities on the completion and documentation of these business analyses and risk assessments.

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:

> 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

---

[7] See, e.g., *Standard for Web-based digital signatures completed*, Government Computer News (June 11, 2007) at: https://gcn.com/articles/2007/06/11/standard-for-webbased-digital-signatures-completed.aspx, referencing https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss.

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.

A recent amendment to § 540.4 (c) of the regulation allows governmental entities to conduct joint business analyses and risk assessments when selecting an appropriate electronic signature solution for use or acceptance in electronic transactions common to such entities. The amendment allows all governmental entities to collaborate in the completion and documentation of those business analyses and risk assessments involving electronic transactions common to such entities. It allows a governmental entity to adopt as its own a business analysis and risk assessment that has been completed and documented by another governmental entity that involves that same electronic transaction. By combining and leveraging efforts to select appropriate electronic signature solutions for use in government electronic transactions, governmental entities, including local governments, will be able to eliminate redundant, time-consuming and costly activities.

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.

4.2.7.1 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 records 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 NYS IT Policy NYS-P10-006 ("Identity Assurance", at https://its.ny.gov/sites/default/files/documents/nys-p10-006_identity_assurance_3.pdf, 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, including governmental entities, that 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

As addressed later in these ESRA Guidelines, e-signatures may serve a security function as well as a legal purpose. 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.

---

[8] The National Institute of Standards (NIST) has published guidelines for risk management for information systems. See ***Guide for Conducting Risk Assessments: Recommendations of the National Institute of Standards and Technology*** (NIST Special Publication 800-30, Revision 1, September 2012) available at: http://csrc.nist.gov/publications/PubsSPs.html#800-30.

***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. In this regard, Government transactions fall into five general categories.
    - Intra-agency that remain within the same government agency.
    - Inter-agency between agencies in the same government.
    - Inter-governmental between different government levels or other governments.
    - Between a governmental entity and a private entity - contractor, university, not-for-profit, or other entity.
    - Between a governmental entity and a member of the general public.

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

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

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

- Used for a short time and destroyed.

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

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.

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 consider other factors 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).

4.2.7.2 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 conducting the analysis and assessment to identify those business, legal, security and technological factors most important to it 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 industry, or the need or ability to achieve compatibility with an existing e-signature solution employed by others, will be overriding factors. To this end, and as mentioned above, governmental entities now may collaborate in the completion and documentation of those business analyses and risk assessments involving electronic transactions common to such entities. A governmental entity may even adopt as its own a business analysis and risk assessment that has been completed and documented by another governmental entity that involves that same electronic transaction, thus selecting an e-signature solution that has already been tried and tested. Budget constraints also will 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]

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

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. State government entities as defined in NYS Executive Order 117 are subject to the *NYS Trust Model* in selecting 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.

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. 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 as defined in NYS Executive Order 117 must 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.

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.

***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.

4.2.7.3 Documenting a 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, 9 NYCRR § 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 at a minimum for 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.

4.2.8 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 electronic transactions involving the use or acceptance of 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 for the required retention period or beyond?
- 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?

4.2.9 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 Information Technology Services *PO-03-002 Information Security Policy*.[10] A security policy and program for systems and information used to create and/or authenticate e-signatures may require some additional elements including:

[10] See: https://its.ny.gov/document/information-security-policy

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.

4.2.10 Governmental Entity Consultation with ITS

The ESRA regulation, at 9 NYCRR §540.3 (b), requires governmental entities to consult with ITS 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, ITS 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 ITS 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, ITS 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.

4.3 E-Records Guidelines

4.3.1 Background

ITS developed this section of the ESRA Guidelines to provide general direction on how governmental entities can protect the authenticity, integrity, security, and accessibility of e-records and e-record systems. These ESRA Guidelines are not primarily designed to explain how statutory or regulatory requirements applicable to

e-records can be met, nor intended to exclude the use of other methods of achieving these objectives. However, where specific ESRA or other legal requirements are mentioned, the ESRA Guidelines provide an explanation of the requirement and/or a link or reference to other relevant information.

This section provides guidance on:

- General concepts and guidelines for creating and managing e-records.
- Producing e-records.
- Maintaining authentic and reliable e-records that are accessible over time.

The headings under each main topic reflect what governmental entities can do to create and maintain secure and authentic e-records that are accessible over time. This guidance is technology neutral and focused on achieving certain outcomes or performance standards, including guidance on the policies and processes as well as the technological and physical measures that can help achieve the desired outcomes.

4.3.2 General Concepts and Guidelines

4.3.2.1 Identify and Assess Specific Legal, Business, and Other Requirements that Apply to E-records

An "electronic record" is defined in ESRA as "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, that govern the retention and disposition of government records (Arts and Cultural Affairs Law Art. 57, sections 57.05 and 57.17), and the Freedom of Information Law (Public Officers Law Art. 6, sec. 86).

The creation, format, and management of records, both electronic and non-electronic, are often based on specific legal mandates, business needs, and past practices. When contemplating the use of e-records, governmental entities should assess their existing recordkeeping practices to determine which practices are based on:

- Legal mandates that must be met.
- Business needs which may or may not continue once an e-records system is developed.
- Past practices in managing paper records that can be eliminated when an e-record system is developed.

When developing e-records systems, legal counsel and other appropriate staff should be consulted as soon as possible to help identify applicable mandates, needs

and practices. Another resource that State agencies and local governments (excluding the City of New York) can use in the development of e-record systems is the New York State Archives. State Archives provides advisory services in identifying records retention, disposition and archival requirements that are equally applicable to e-records as to paper documents. State Archives also publishes materials and provides advisory services focused on record management best practices. New York City agencies should consult with the NYC Department of Records and Information Services (DORIS) for similar information and guidance.

4.3.2.2 Base E-records Management Measures on the Records' Value

Just as with paper records, the e-records a governmental entity produces or receives are not all of equal importance or value. Although all government records should be maintained properly, the effort and resources a governmental entity expends to manage and maintain records, including e-records, should be related to the records' value to the agency and the citizens it serves. The concept of risk management may be useful in this regard. Risk management requires: an analysis of risks relative to potential benefits, consideration of alternative measures to address risks and implementation of the measures that best address risk based on this analysis. In applying risk management to e-records, the following questions should be asked.

- What would be the impact on entity operations if the records were lost or otherwise unavailable?
- Would the entity or others suffer a financial loss if the records were unavailable?
- What is the likelihood that the records would be subject to or needed for a legal action? Would the inability to produce the records in a form admissible in court have a critical impact on the outcome of a case?
- Are the records required for an extended period of time?
- Do the records have significant cultural or historical value?

4.3.2.3 Focus on the Systems and Business Processes that Produce E-records

The reliability and accuracy of the systems, processes and procedures used to produce and maintain e-records are critical to demonstrating their authenticity and integrity. These factors are much more important than the format or medium of e-records or the specific technology used to produce and maintain them. Governmental entities need to identify, specify and document these processes and procedures if they expect their e-records to be accepted in legal and other proceedings.

4.3.2.4 Training is Critical

Training, which ensures that staff adequately maintains systems used to create and retain e-records, is critically important in preserving the authenticity, integrity and

legal admissibility of e-records. In addition, it is important to ensure awareness of the unique management issues associated with e-records, such as the fragile media on which e-records are stored, the technology platform needed to access and use e-records, and the responsibilities to manage e-records diligently to ensure their admissibility in legal proceedings and their accessibility throughout their legal retention periods.

4.3.3 Producing E-records

E-records can be produced through various means. They can be created internally or through an online application, or they can be received electronically. The systems supporting an entity function must be able to produce records in the required form, which includes required informational content and contextual elements (e.g., authorizations, date stamps, e-signatures), and unique identifiers. In transmitting and receiving e-records, precautions must be taken to prevent unauthorized persons from tampering with and corrupting them. Failure to do so would compromise or cast doubt on the e-records' authenticity and integrity. Regardless of how they are produced, e-records must be stored in a secure recordkeeping system.

4.3.3.1 Produce a Record for Each Business Transaction that Complies with all Legal or Other Requirements Regarding the Record's Structure, Content, and Time of Creation or Receipt

Develop and document clear procedures and processes for the receipt, creation, and storage of e-records: These documented policies and procedures should describe acceptable record formats, indicate the point at which a transaction is completed, and specify how the record is securely stored so that it cannot be modified without detection.

Designate a receiving device: ESRA's implementing regulation, at 9 NYCRR Part 540.5(e) requires governmental entities that accept e-records to designate the receiving device where they will be accepted. A "device" could mean a specific server but it also could be a specific e-mail address or website. A governmental entity should inform the public of what devices it has designated to receive e-records.

Establish controls for the accuracy and timeliness of input and output: The accuracy and timeliness of the input and output of systems is critical to demonstrating the integrity and authenticity of the e-records produced by a system.

4.3.3.2 Authenticate (Prove the Identity of) the Sender of the Record (if necessary) and Make Sure the E-record has not been Altered

Establish policies and procedures to authenticate senders and determine the integrity of each type of e-record: These policies should be driven by the potential risk and costs if the records were tampered with, inappropriately disclosed, or otherwise proven deficient.

Establish measures to secure transmission of e-records including the integrity of records during transmission and processing: These measures will vary with the level of risk, the business requirements, and the technology used. For example:

- *Public Key Cryptography*, which provides a very strong encryption for higher risk transactions, can support electronic signatures as well as the following secure transmission measures.
    - Transport Layer Security (TSL) is often used for web-based applications
    - E-mail applications often use Secure Multipurpose Internet Mail Extensions (S/MIME).
- *Pretty Good Privacy* (PGP) is a technique for sending secure messages over a public network using a freeware encryption package available from the Massachusetts Institute of Technology.
- *Virtual Private Networks* (VPN) are used to encapsulate data transfers between devices that are not on the same private network, and ensure a certain amount of privacy for ongoing business relationships via public networks.

Specific techniques may be used independently (**independently verified**) or combined to determine if e-records have been altered. These can include measures as simple as providing the sender with a receipt and copy of the received document or established data processing techniques such as edit checks and *checksum*, and *hashing* techniques, such as those used in digital signature technologies, that can easily detect changes to a record.

Provide and maintain measures to authenticate the identity of the sender based on potential risk and legal requirements: Authentication is the means of establishing the validity of a person's identity. The need for these measures may vary based on the nature of the transaction and specific business requirements. In fact, some transactions do not require authentication of the sender. There are three means to authenticate a sender's identity and these can be used alone or in combination:

- Something that only the individual knows: A secret (e.g., a password, Personal Identification Number (PIN), or cryptographic key).
- Something the individual possesses: A token (e.g., an ATM card or a smart card).
- Something the individual is: A biometric (e.g., characteristics such as a voice pattern or a fingerprint).

Typically for applications with low to moderate risk, authentication is accomplished through the use of unique passwords and/or PINs. Using unique personal information such as mother's maiden name could enhance authentication. However, higher risk applications often rely on "two-factor" authentication that includes a PIN

and something the user "possesses" (a token, smart card, or cryptographic key) or "is" (a biometric -- e.g., voice pattern, handwriting dynamics, iris recognition or a fingerprint).

Maintain measures to document the date and time of receipt: It may be important to document this information for certain government transactions. Date and time of receipt information is usually captured in an automated fashion by the receiving system. Receipt information should be attached or linked to the record received, as a time stamp would be on a paper record. For high-risk applications, secure or trusted time stamping can be used where a neutral or trusted third party applies the electronic date and time stamp. A trusted time authority can apply such electronic time stamps and binds it to a record through the use of public key cryptography.

Confirm receipt: Some business processes or statutory mandates require that the receipt of documents be confirmed. Confirmation may take different forms depending on the type of application. For example, web-based applications may return a screen confirming a transaction along with a unique transaction number for tracking or auditing purposes. For high security environments, a separate confirmation via an alternative route is recommended. For example, a person's postal address could be confirmed via an external database and the person could be sent a confirmation via mail or courier (e.g., FedEx, UPS, etc.).

4.3.4 Maintaining Authentic and Reliable E-records that are Accessible Over Time

Entities must maintain reliable and authentic e-records that at a minimum remain accessible and useable for their legal retention periods. E-records with long term or permanent retention requirements must be preserved in an accessible and useable form by the entity or, in the case of State agencies, transferred to the State Archives. Other e-records maintained by governmental entities should be legally destroyed only under a records disposition authorization issued by the State Archives or, in the case of New York City, the City Department of Records and Information Services.

4.3.4.1 Maintain the Integrity and Accessibility of E-records as Captured or Created so that They Can be Accessed, Displayed and Managed as a Unit

Maintain an e-records management policy documenting the organization's policies and practices on electronic information management and storage: Policies should cover the following areas:

- **Specify what e-records are covered:** E-records should be grouped into "types" or "series" that can be managed in a consistent manner. For example, information types may be specified either by reference to the business activity that created them (such as "vehicle registration," "public assistance case files," "fishing license file"), or to generic group (such as "accounting data,"

"customer documents," "manufacturing documents"). Some records will be more critical for entity operations, or more likely to be needed for legal purposes, than others. These records should be afforded more management attention and a higher level of protection. State Archives retention and disposition schedules provide guidance in determining record series for governmental e-records.

- **Establish standards for file formats**: Policy should designate approved data file formats for each record "type." All information stored on a computer system requires software for retrieval and display. This software is subject to change, either by the implementation of new releases, or by changes to operating systems or hardware. A policy of approved media formats for records storage will facilitate data migration to ensure long-term retrieval of e-records.

- **Define responsibilities for information management functions:** An effective information policy needs to define responsibilities for implementing its various components. In the case of e-records, responsibilities will often be shared between entity e-mail users; program and technical staff as well as staff specifically assigned to records management functions.

- **Define procedures for the storage and management of e-records to ensure access for the full length of their retention period.** (See also section 3.3.4.2 of these ESRA Guidelines, above)

Develop controlled storage or filing systems that maintain the integrity and accessibility of e-records: Once e-records are created or captured they need to be retained in a controlled environment that can maintain their integrity and authenticity. This demands that e-records be stored in a secure, reliable and trustworthy e-records system. In addition, e-records must be stored so that any unauthorized change or modification can be prevented or at least detected. Document management or knowledge management products are available that can provide such solutions. The U.S. Department of Defense also tests and certifies document management products that include e-records management capabilities.

4.3.4.2 Retain E-records in an Accessible Form for their Legal Minimum Retention Periods

Adopt and use records retention and disposition schedules in compliance with the Arts and Cultural Affairs Law or local law: General records retention and disposition schedules exist which cover the general functions of State agencies and all functions of local governments outside of New York City. State agencies can develop schedules for their unique records following State Archives' procedures. The State Archives provides assistance for developing schedules and interpreting general schedules. The State Archives' website contains copies of general schedules and information on developing agency-specific schedules for State

agencies. New York City agencies should contact the City Department of Records and Information Services (DORIS).

Develop a contingency plan that includes data backup, disaster recovery, and emergency operations: Contingency plans can help governmental entities quickly put systems back into operation after a disaster. The plans should include data backup and recovery to prevent the loss of e-records

Implement media controls: Physical and environmental threats can have an impact on e-records, especially those stored on fragile data storage devices. Various measures, such as standard labeling and maintaining tracking logs, provide physical and intellectual control over the many forms of physical data storage. Secondary or tertiary data storage devices should also be stored in environmentally and physically controlled locations. The extent of media control depends upon many factors, including the type of data, the quantity of media, and the nature of the user environment. Media used to store critical or high-risk e-records will normally demand higher levels of control than other data.[11]

Perform routine backups: It is critical to back up software and data especially if that data constitutes e-records. Frequency of backups will depend upon how often data changes and the importance of those changes. Program managers should be consulted to determine what backup schedule is appropriate. Backup copies should be tested to determine if they are useable and stored securely at a location away from the system in the event of a disaster.

Ensure that records are destroyed once their retention periods are met: E-records that have met their legal retention requirement and which serve no other business needs should be destroyed. Destruction involves controlling all copies on all computers, detachable equipment, and media; documenting destruction; and using appropriate media sanitization and destruction methods depending on the e-records' confidentiality. NIST Special Publication 800-88 Guidelines for Media Sanitization[12] provides detailed recommendation on the sanitization and destruction of most types of digital media.

Maintain adequate search and retrieval capabilities to ensure that e-records can be retrieved for all legitimate business purposes for their full retention period: This should include retrieval during the period that records are stored on near line or physical data storage devices. This will demand adequate indexing as well as search tools.

4.3.4.3 Produce Authentic Copies of E-records and Supply Them in Useable Formats, including Hard Copy, for Business and Public Access Purposes

---

[11] Academic institutions including Cornell and M.I.T. have produced and maintained tutorials concerning "Digital Preservation Management" which are available from their libraries.

[12] See: http://csrc.nist.gov/publications/PubsSPs.html

Develop or revise access and personal privacy protection policies to include e-records: Such policies should be consistent with the requirements of the Freedom of Information Law (FOIL), Personal Privacy Protection Law (PPPL), agency specific laws, and ESRA. State agencies that maintain websites must also comply with the Internet Security and Privacy Act (State Technology Law, Article II). This Act requires such agencies to adopt and post on an agency website an Internet privacy policy describing the practices and procedures related to the management, retention, and disclosure of personal information collected about users through the website. ITS has developed a model Internet Security and Privacy Policy for use by State agencies, which highlights a number of considerations that should be taken into account in drafting an Internet privacy policy and provides an outline for the contents of an Internet security and privacy policy.

Develop methods to provide public access to e-records and to protect personal privacy and confidentiality: When e-record systems are designed, a governmental entity must consider developing methods of access that take into account public access and confidentiality requirements. The need for public access to e-records must constantly be weighed against a governmental entity's duty to protect personal privacy and confidentiality. One solution is for governmental entities to develop automated means to redact or mask confidential information from e-records before releasing them to the public.

Provide access to e-records in the form the user prefers: Some people do not have access to the technology needed to use e-records or prefer records in paper form. ESRA, and the ESRA regulation (see 9 NYCRR Part 540.5(b)(1)) require governmental entities to provide access to e-records as permitted by statute and in paper form if requested. This does not mean that governmental entities must maintain paper copies of e-records, only that they have the technical capability to generate copies of e-records that are accessible under the law in both paper and electronic form. This will likely require appropriate output devices, such as a high-quality printer capable of producing legible or useable copies of records.

4.3.4.4 Develop an Approach to Maintain the Authenticity and Integrity of Electronically Signed E-records

These ***E-records Guidelines*** apply equally to signed and unsigned e-records. Electronically signed e-records raise special concerns. The ability to preserve the context and links between components of e-records is critical where such records are electronically signed. Such contextual information provides additional evidence to support the reliability and authenticity of the signed e-record and/or may actually constitute the e-signature process itself. Therefore, the key challenges faced by governmental entities in maintaining electronically signed e-records are to:

- Determine what information needs to be retained to maintain a valid, authentic, and reliable signed e-record.

- Preserve the link or association between the various components of a signed record over time.

Determining what information needs to be retained: Determining what minimal information will be needed to demonstrate the authenticity and reliability of an electronically signed record in a legal proceeding requires a legal analysis.[13] While preparing their business analysis and risk assessments for selecting an e-signature approach, to determine what information needs to be retained as part of the signed e-record, governmental entities should research current caselaw to identify any reported court decisions wherein the authenticity or validity of an e-signature has been challenged or assessing the reliability of an electronically signed record on the basis of its e-signature. In fact, the e-signature method selected will partially determine the approaches available and necessary to ensure the trustworthiness of the electronically signed e-record over time.

Described below are two such approaches that the US National Archives and Records Administration (NARA) has identified as being the current practices used by Federal agencies.[14]

- ***Maintain adequate documentation of the e-signature's validity*** gathered at or near the time the record was signed. Depending on the signing method, this contextual information may actually constitute part of the signed e-record or may be captured in supporting records.

- ***Maintain the ability to revalidate e-signatures.*** This approach requires agencies to retain the capability to revalidate the e-signature, along with retaining the signed e-record.

In considering these approaches, governmental entities should take into account the following:

- As with any e-record, the acceptance of signed e-records for legal, audit, and other purposes is contingent on demonstrating the trustworthiness of the system used to produce them regardless of which option is used.

- The maintenance of the ability to revalidate e-signatures is only available where the e-signature method relies primarily on a **digital object** that can be revalidated (e.g., encrypted hash, digitized signature, biometric). Entities

[13] Some court decisions that have addressed the proper evidentiary foundation that should be established when electronic documents are submitted for admission into evidence, while not controlling, are informative on this topic; See, In re: Vee Vinhnee, 336 B.R. 437, (9th Cir. BAP (Cal.) Dec 16, 2005); Miriam Osborn Memorial Home Association v. Assessor of the City of Rye, 9 Misc. 3d 1019 (Sup. Ct. West. Co., 2005).

[14] NARA, ***Records Management Guidance for Agencies Implementing Electronic Signature Technologies*** (October 18, 2000, last rev. Feb. 14, 2006), pp. 7-8. Copies of this publication are available at: https://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html

would need to retain all records of the system's functionality specific to a particular e-signature technology or approach for the revalidation process to be successful. For digital signatures produced using a PKI, a government entity should ensure its PKI is governed by a certificate policy that addresses 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.

Regardless of the approach used, entities should minimally retain documentation of the:

- Signer's identity and the process used to identify and authenticate him or her.
- Date and time an individual was authenticated.
- Signer's intent.
- Date and time that the signing process was completed.

Preserve the link or association between the various components of signed records over time:

Most creating systems should be designed to manage all of the components of a signed e-record and even revalidate an e-signature where that is possible. Unless the signed record has a relatively short retention period, it will likely need to be migrated to a new system and may ultimately be stored offline. Unsigned e-records face these same issues. The need to retain contextual information is even more critical for signed e-records. Therefore, when planning an e-signature solution it is important to consider the retention requirements of the signed e-records, and how those with longer retention periods (over 6 years) will be migrated to new systems and/or stored on data storage devices while preserving the link between or association of their various components.

If the creating system's functionality is no longer available, preserving the relationship of the various components of the signed e-record may involve reformatting it. In such cases, the reformatting process should be planned, well documented, conducted in the normal course of business, and performed in such a manner so that the records' authenticity, integrity, and reliability can be demonstrated.

Governmental entities need to seriously consider if the ability to revalidate an e-signature throughout a signed e-records retention period is really critical. Retaining the ability to revalidate an e-signature may be a difficult and costly task especially for records with longer retention periods. An organization will also need to assign responsibility for long-term signature validation services. For example, where a PKI-supported digital signature is used, the certification authority (CA) that issued the digital certificate for signing purposes could be assigned this responsibility. However, records retention requirements may extend beyond the life of any agreement with a CA that issued the certificate or beyond the existence of the CA.

Therefore, long-term signature validation services must be viewed as a separate function that cannot be left solely to an independent CA.

Maintaining adequate documentation of an e-signature's validity and the ability to re-validate an e-signature at a later date are not necessarily mutually exclusive options. Both strategies can be used simultaneously or during different stages in the e-record's life cycle. The use of these options should be based on business requirements and an assessment of risks, in which an entity determines how long it needs to validate an e-signature and the acceptability of something other than original signature validation. For example, the ability to revalidate a signature and documentation of its validity could be maintained during the period of highest risk of repudiation and/or during the record's active life. During the record's inactive storage, when repudiation risk is low, an entity may determine it can rely solely on documentation of the signed e-record's validity.[15]

On this topic, governmental entities should consider reviewing guidance issued by NARA, the National Archives of Canada, and the Australian National Archives generally questioning the practicality of maintaining the ability to revalidate signed e-records that will be maintained for long periods of time or permanently, and averring that maintaining adequate documentation of validity gathered at or near the time of record signing may be preferable for such records. Such an approach is less dependent on technology and much more easily maintained as technology evolves over time.

5.0 Compliance

This guideline shall take effect upon publication. Compliance with enterprise guidelines is optional, but strongly suggested. ITS may amend its guidelines at any time; compliance with amended guidelines is optional, but strongly suggested.

6.0 Definitions of Key Terms

Except for terms defined in these ESRA Guidelines, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

Term	***Definition***
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

[15] NARA provides record management and retention "Transfer Guidance" for digital signature authentication. See: https://www.archives.gov/records-mgmt/policy/transfer-guidance.html

	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."
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
Electronic transaction	Shall mean an action or set of actions occurring through the use of electronic technology by or with a governmental entity.
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.
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
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.
Token	A small hardware device used for security purposes to store confidential user identification or authentication information such as a private key.
Transport Layer Security (TLS)	This is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security and the TLS Handshake Protocol allows the server and client to authenticate each other. TLS is the successor to the Secure Sockets Layer (SSL).
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:

Level	Description
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.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Division of Legal Affairs
Reference: NYS-G04-001
NYS Office of Information Technology Services
State Capitol, PO Box 2062
Albany, NY 12220-0062
Telephone: (518) 473-5115
Email: its.sm.dla@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This guideline shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
5/26/2004	Original ESRA Guidelines issued.	CIO/OFT
9/28/2007	Revised and republished.	CIO/OFT
10/23/2007	Reformatted and updated to reflect current CIO, agency name, logo and style.	CIO/OFT
11/02/2011	Revised and republished.	CIO/OFT

Date	Description of Change	Reviewer
12/20/2013	Revised and republished.	ITS
9/6/2017	Revised and republished.	ITS

9.0 Related Documents

1. New York State Standards, Guidelines and Resources

https://its.ny.gov/electronic-signatures-and-records-act-esra

NYS IT Policy NYS-P10-006 - "Identity Assurance" (NYS Identity Trust Model. See: https://its.ny.gov/sites/default/files/documents/nys-p10-006_identity_assurance_3.pdf

ESRA Regulations (9 NYCRR Part 540)

ESRA Law (Article III of the NYS Technology Law)

The NYS Archives' Guidelines Most Relevant to E-signatures and E-records (See: www.archives.nysed.gov/publications?category=ServicesGovRecs), including:

- Digital Imaging Guidelines (2014)
- 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: (www.archives.nysed.gov/records/mr_erecords_vmail.shtml)
- Developing a Policy for Managing eMail (Technical Information Series #85)
- Managing eMail Records: www.archives.nysed.gov/records/mr_erecords_email.shtml
- Guidelines for Choosing Records Management Software (Technical Information Series #63)
- Indexing Records: www.archives.nysed.gov/records/mr_id_index.shtml
- Managing Geographic Information Systems (GIS) Records: www.archives.nysed.gov/records/mr_erecords_gis.shtml

2. Other New York State Resources

The NYS Department of State's Committee on Open Government provides the complete text of the NYS Freedom of Information law as well as FAQs and advisory opinions that specifically address e-records issues:

Internet address: https://www.dos.ny.gov/coog/
Contact: https://www.dos.ny.gov/about/contact.asp

The NYS Unified Court System's Electronic Records Guidelines. See: http://www.courts.state.ny.us/admin/recordsmanagement/policies/Policy9.pdf

3. Other Resources

The Center for Technology in Government, University at Albany's publications (https://www.ctg.albany.edu/):

- *"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"*

The online Cornell University/MIT tutorial, "Digital Preservation Management: Implementing Short-Term Strategies for Long Term Problems." http://web.mit.edu

The Council on Library and Information Resources (CLIR) publications, "*The State of Digital Preservation: An International Perspective"* and "*Authenticity in a Digital Environment*," which provide a good overview of research and development activities and technical approaches to digital preservation. See:

http://www.clir.org/pubs/abstract/pub107abst.html and http://www.clir.org/pubs/abstract/pub92abst.html

The Commission on Preservation and Access publication, "*Magnetic Tape Storage and Handling."* See: http://www.clir.org/pubs/reports/pub54/index.html

The Joint Interoperability Test Command, DISA, DoD, publication, *"Records Management Application (RMA) Certification Testing."* See: http://jitc.fhu.disa.mil/projects/rma/standards.aspx

The Computer Security Special Publications of the National Institute of Standards and Technology provide many standards and guidelines publications related to digital signature, PKI, system security, risk management, and other relevant topics. See: http://csrc.nist.gov/publications/PubsSPs.html

The National Archives of Australia provides a number of useful guidelines and publications on the management and preservation of e-records. See: http://www.naa.gov.au/records-management/index.aspx

The U.S. National Archives and Records Administration (NARA) publication, *"Records Management Guidance for Agencies Implementing Electronic Signature Technologies."* See: https://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html

The Office of Management and Budget (OMB), Appendix II to OMB Circular No. A-130 Implementation of the Government Paperwork Elimination Act. See: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

The Office of Management and Budget (OMB), Guidance on Implementing the Electronic Signatures in Global and National Commerce Act. See: https://www.whitehouse.gov/omb/memoranda_m00-15

The Property Records Industry Association (PRIA) website has background documents and standards that have been incorporated by reference into the ESRA regulation relating to electronic recording of real property instruments. See: http://www.pria.us/

There are two non-technical documents to explain e-recording:

- *"How To Get Ready for eRecording – Recorders."*
  See: http://www.pria.us/i4a/doclibrary/getfile.cfm?doc_id=45

- *"How To Get Ready for eRecording – Submitters."*
  See:, http://www.pria.us/i4a/doclibrary/getfile.cfm?doc_id=46

The technical documents and standards that ITS has expressly incorporated by reference into the regulation are collectively known as the "PRIA Guidelines" which are available via the PRIA website and consist of the following:

- *"PRIA Request Version 2.4.2, August 2007";*
- *"PRIA Response Version 2.4.2, August 2007"*
- *"Document Version 2.4.1, October 2007";*
- *"Notary Version 2.4.1, October 2007"; and*
- *"eRecording XML Implementation Guide for Version 2.4.1, Revision 2, March 2007"*.

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

Some e-signature technologies are based on cryptographic techniques like public key infrastructure (PKI). 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.

The Federal Information Processing Standards Publication FIPS Pub 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. See: https://doi.org/10.6028/NIST.FIPS.140-2

Another helpful federal document published by the National Institute of Standards and Technology (NIST) is, *"An Introduction to Computer Security: The NIST Handbook*." See: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf