

**NYS BEST PRACTICE GUIDELINE # G04-001
ELECTRONIC SIGNATURES AND RECORDS (ESRA) GUIDELINES**



**JAMES T. DILLON
CHIEF INFORMATION OFFICER FOR THE STATE OF NEW YORK**

BEST PRACTICE GUIDELINE

Reference:	G04-001
Technology Category:	Electronic Signatures and Records
Title:	Electronic Signatures and Records (ESRA) Guidelines
Replaces & Supersedes:	Electronic Signatures and Records Act (ESRA) Guidelines (Issued Jan. 2001, revised Sept. 2002)
Authority:	NYS State Technology Law §103
Issue Date:	May 26, 2004
Publication Date:	May 26, 2004
Policy Effective Date:	May 26, 2004
Review Date:	May 26, 2007

Purpose

This ***best practice guideline***:

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

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 guidelines useful.

Best Practice Guideline

- 1. Introduction..... 5**
- 2. E-signature Guidelines 7**
 - 2.1 Background..... 7
 - 2.2 How to Use This Section..... 7
 - 2.3 Overview of the Business and Legal Function of a Signature 7
 - 2.4 Determining if an E-signature Solution is Needed or Desirable 8
 - 2.5 ESRA Definition of an Electronic Signature..... 8
 - 2.6 E-signature Approaches..... 11
 - 2.7 Selecting an E-signature Approach..... 14
 - 2.7.1 Business Analysis and Risk Assessment..... 15
 - 2.7.2 Using Business Analysis and Risk Assessment to Select an E-signature..... 20
 - 2.7.3 Documenting a Business Analysis and Risk Assessment 23
 - 2.8 Special Issue: Multiple Signatures..... 23
 - 2.9 Special Issue: Security of Systems and Information Used to Create E-signatures 24
 - 2.10 Governmental Entity Consultation with OFT 26
 - 2.11 Additional Assistance 26
 - Summary Guidelines for Selecting an E-signature Solution..... 27
- 3. E-records Guidelines..... 30**
 - 3.1 Background..... 30
 - 3.2 General Concepts and Guidelines 30
 - 3.2.1 Identify and Assess Specific Legal, Business, and Other Requirements that Apply to E-records 30
 - 3.2.2 Base E-records Management Measures on the Records' Value..... 31
 - 3.2.3 Focus on the Systems and Business Processes that Produce E-records 31
 - 3.2.4 Training is Critical 31
 - 3.3 Producing E-records..... 32
 - 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 32
 - 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 32
 - 3.3.3 Uniquely Identify Each Record 34
 - 3.3.4 Capture an E-record for Each Transaction Conducted through a Multi-entity Web Portal 34
 - 3.4 Maintaining Authentic and Complete E-records that are Accessible Over Time 35
 - 3.4.1 Maintain Integrity of E-records as Captured or Created so that They Can be Accessed, Displayed, and Managed as a Unit..... 35
 - 3.4.2 Retain E-records in an Accessible form for Their Legal Minimum Retention Periods as Established in State Archives or Local Retention Schedules 36

3.4.3	Search and Retrieve E-records in the Normal Course of Business for all Business Uses throughout Their Entire Legal Minimum Retention Period.....	38
3.4.4	Produce Authentic Copies of E-records and Supply Them in Useable Formats, including Hard Copy, for Business and Public Access Purposes.....	38
3.4.5	Develop an Approach to Maintain the Authenticity and Integrity of Electronically Signed E-records.....	39
3.5	Maintaining Secure, Reliable and Trustworthy E-records Systems.....	41
3.5.1	Make Sure the System Performs in an Accurate, Reliable, and Consistent Manner in the Normal Course of Business.....	41
3.5.2	Protect E-records to enable their Availability throughout Their Retention Period.....	43
3.5.3	Limit System Access to Authorized Individuals and for Authorized Purposes and Maintain Physical and Environmental security controls.....	43
3.6	Additional Assistance.....	43
	Summary E-records Guidelines.....	44
Additional Web-Available Resources.....		47

1. Introduction

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

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

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 102) has been modified to conform to the definition found in the [Federal Electronic Signatures in Global and National Commerce Act](#) (“E-Sign”). ESRA now defines an “electronic signature” as:

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.

¹ However, ESRA (section 107) does not apply to:

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

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

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

The ESRA regulation (Title 9 NYCRR Part 540) was amended on May 7, 2003, to reflect these recent amendments to ESRA. The Office for Technology (OFT) has revised and expanded these guidelines to ensure that they are relevant to the amended ESRA. While the guidelines are targeted for use by governmental entities, private individuals and entities may also find these guidelines to be useful.

The guidelines are organized into two major sections entitled:

- ***E-signature Guidelines*** (explaining the definition of an e-signature under ESRA and assisting in the selection of e-signature solutions that meet business and legal needs).
- ***E-records Guidelines*** (providing general direction on ensuring the authenticity, integrity, security, and accessibility of e-records including those that are electronically signed).

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

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

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

2. E-signature Guidelines

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 their business and legal needs. This section provides guidance on:

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

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 needs.

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

2.3 Overview of the Business and Legal Function of a Signature

A signature can serve the following business and legal purposes:

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

document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document.

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

2.4 Determining if an E-signature Solution is Needed or Desirable

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

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

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

2.5 ESRA Definition of an Electronic Signature

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. 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 possible transmission, and retained for as long as a valid signature is required including any subsequent storage, which may be the record’s full legal minimum retention period. The creation of the electronic signature, including its attachment or logical association to the signed record, can occur in a system other than that of the government entity to which it is submitted. For example, a private sector entity that regularly submits reports to a government agency may have an internal system that houses and formats the electronic reports. An authorized signer can electronically sign such reports at one point in time and a government entity could elect to accept those signed reports when they are electronically submitted at a later time.

Guidelines for the retention and preservation of electronically signed records, including maintaining the attachment or logical association between the signed record and signature, are provided in [section 3.4.5](#) of this document.




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

The essence of a signature is to identify the signer and signify that he or she understood and intended to carry out whatever was stipulated in the document. The ceremonial act of signing with pen and ink warns the signer that he or she may be making a legally binding commitment. ESRA requires that an e-signature be accompanied by the same intent as the use of a signature affixed by hand. ESRA does not require any specific level or method of signer identification or authentication. Therefore, governmental entities are free to select an identification and authentication method that meets their needs. The selection of an appropriate approach to identify and authenticate signers is one of the considerations in selecting an e-signature solution (see [section 2.7](#)).

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

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

Below is an example of a signature certification statement from the Department of Taxation and Finance International Fuel Tax Agreement (IFTA) report’s filing application.

9 Credits to be applied 	<input type="text"/>
10 Balance due/(credit) 	<input type="text" value="50.00"/>
11 Refund amount requested 	<input type="text"/>

I understand and agree that by entering my password and clicking the Submit button below, I am electronically signing and filing my business' IFTA report for the current period. I hereby state that this business is duly licensed and that this report, including any schedules, is to the best of my knowledge and belief true, correct and complete. I also state that I am acting in the capacity of owner (if an individual business), corporate officer, partner (except a limited partner), or member or manager of a limited liability company, and that I have the authority to sign and file my business' IFTA report.

Please enter your Password:

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

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 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.² Authentication is the first part of the signature process that often involves an affirmation of intent to sign when the signature is applied. If the authentication process is performed over an open network such as the Internet, the shared secret is usually encrypted using an encryption technology called *Secure Sockets Layer (SSL)*. SSL is currently built into almost all popular Web browsers and encrypts in a fashion that is transparent to the end user. The identification and verification process used to issue a PIN and/or password varies depending on the level of security deemed necessary and

² Some more secure approaches also require the entry of some personal information (e.g., name, date of birth or sex) along with the PIN and password. State agencies seeking to collect such personal information must comply with the obligations and requirements of the New York State Personal Privacy Protection Law (Public Officers Law, Article 6-A).

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.

- **Digitized Signature:** A digitized signature is a graphical image of a handwritten signature. Some applications require a person to create a handwritten signature using a special computer input device, such as a digital pen and pad. The digitized representation of the entered signature is compared with a stored copy of the graphical image of the signature. If special software judges the two images comparable, the signature is deemed valid. This approach shares the same security issues as those using the PIN or password, because the digitized signature is another form of shared secret known both to the person and to the system. Forging a digitized signature can be more difficult than forging a paper signature because the technology that compares the submitted signature image with the known signature image is more accurate than the human eye.³
- **Signature Dynamics:** This is a variation on a digitized signature in which each pen stroke is measured (e.g., duration, pen pressure, size of loops, etc), creating a metric. This metric can also be compared to a reference value created earlier, thus authenticating the person who applied the signature. The signature dynamics measurements can be combined with techniques used to create a digital signature (see below) to ensure document integrity and a more reliable authentication of the signer.
- **Shared Private Key (Symmetric) Cryptography:** In shared private key approaches, the person electronically signs a document and verifies the signature using a single *cryptographic key* that is not publicly known. Since the same key is used to sign a document and verify the identity of the signer, it must be transferred from the signer to the recipient of the document. The private key is shared between the sender and possibly many recipients; therefore, it is really not "private" to the sender and hence has lesser value as an authentication mechanism. A private key can be made more secure by incorporating other security techniques involving the use of smart cards or other hardware tokens in which the private key is stored (see **Smart Cards**).
- **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

³ Occasionally e-signature solutions based on other approaches will include a digitized signature to give the look and feel of a handwritten signature. In such cases the digitized signature is captured in advance and stored electronically.

entities involved in the PKI. New York State has issued the [New York State Certificate Policies for Digital Signatures & Encryption](#) for use by State agencies and other governmental entities that choose to implement PKI technology for digital signatures and encryption purposes. Digital signatures can be implemented without the use of a CA (see **Alternate Approaches** below).

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

Smart Cards

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

Hybrid Approaches

Hybrid e-signature solutions are available by combining techniques from various approaches to provide increased security, authentication, record integrity and non-repudiation for less secure signing techniques. One well-publicized solution involves improved signature-capture techniques combined with click wrap and PINs and password approaches.⁴ This solution enhances such signatures by recording the entire transaction process, which is then bound to the signed document using *hashing* and SSL encryption techniques to achieve document integrity and non-reputability. Another solution provides a click wrap process that results in an encrypted signature object being created within a document, which is treated as a read-only file. A number of products provide a signing ceremony designed to capture the signer's intent.

Electronic signing approaches are also available that use PKI-related or digital signature technologies but avoid some of the complexities and costs of developing a full infrastructure. Some solutions use centralized private key management by the issuing

⁴ D. McKibban, *Silanis Technology: Signature Technology for E-Business* (Gartner Research Note, August 14, 2001); Jan Sundren, *Achieving the Functions of Signatures Online* (Giga Ideabyte, March 4, 2002).

organization and identification and authentication methods that avoid the need for a third party CA.⁵ These approaches reduce the risks of requiring individuals to protect their private keys and the necessity for special software on the computer of each participant to a transaction.

As with many technologies, new approaches could be developed and deployed very rapidly in response to changes in the market or the legal and fiscal environment.

2.7 Selecting an E-signature Approach

The selection of an e-signature solution is foremost a business decision involving more than technical considerations. In amending ESRA in 2002, the Governor and Legislature endorsed the idea that governmental entities should utilize a process in selecting the type of e-signature solution to employ in a given transaction as a way of protecting the public's interest in the use of sound and appropriate practices in their electronic transactions with government. The ESRA regulation, § 540.4 (c), requires governmental entities to complete and document a business analysis and risk assessment when selecting an e-signature solution. 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 should be integrated into a business analysis and risk assessment process. A governmental entity may evaluate each factor differently and accord them different weights based on the nature and specifics of the underlying transaction. A governmental entity may determine that a particular factor has no weight for a particular transaction. For example, in completing a risk assessment the "relationships between parties to an electronic transaction" will be but one factor in determining the "risk of fraud" inherent in a given transaction. This same factor is also relevant to one's understanding of the underlying business process to which the e-signature will be applied. In completing a business analysis, "the cost of employing a particular electronic signature process" is a business consideration that may also be used as part of a cost benefit analysis in support of the selection of an e-signature solution.

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

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

⁵ V. Wheatman, *Public Key Infrastructure IH02 Magic Quadrant* (Gartner Research Note, February 14, 2002).

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.

2.7.1 Business Analysis and Risk Assessment

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

Business Analysis

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

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

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

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

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

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

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

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

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

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

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

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

Risk Assessment

E-signatures may serve a security function as well as a legal one. E-signature processes usually include authentication of the signer, and some approaches can provide other security features such as message authentication and repudiation protection. Therefore, the selection of an appropriate e-signature solution includes identifying the potential 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.⁶

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

To assess risks an entity should identify and analyze:

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

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

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

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

- Intra-agency that remain within the same government agency.
- Inter-agency between agencies in the same government.
- 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

⁶ The National Institute of Standards (NIST) has published guidelines for risk management for information systems. See Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management for Information Technology Systems: Recommendations of the National Institute of Standards and Technology* (NIST Special Publication 800-30, January 2002) available at <http://csrc.nist.gov/publications/nistpubs/index.html>.

fraud. Governmental entities should assess the potential threats of repudiation or fraud inherent in the type of transaction based on knowledge of the specific parties involved in the transaction, the nature of their business relationships to each other, and data on past incidences of repudiation and fraud.

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

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

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

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

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

- Average dollar value of transactions.
- Direct loss to the governmental entity.
- Loss to a citizen.
- Direct or indirect loss to a business, other government entity or other trading partner.
- Liability for the transaction (e.g., personal, corporate, insured, or shared).

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

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

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

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

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

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

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

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

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

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

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

In selecting an e-signature solution the business analysis and risk assessment should be viewed as integrated, mutually supporting processes. It is up to the governmental entity to identify its overriding concerns in the selection of an e-signature solution. In many cases the selection of an e-signature approach will be the result of balancing business concerns, such as user acceptance and ease of deployment, with the reduction of risks. Often combining features from various e-signature approaches will achieve such a balance. In some cases, the existence of established or de facto standards in a field, or the need or ability to achieve compatibility with an existing e-signature solution employed by others, will be overriding factors. Budget constraints will also be a key consideration in the selection process and cost may be an overriding consideration where risks are low.

Matching E-signature Functionality to Risk Level: In integrating the risk considerations into the e-signature selection process, governmental entities should consider that **within** and **between** each general approach to e-signing (see [section 2.6](#)) 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.⁷

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. Entities may wish to use the opportunity afforded by moving to an online environment to implement a more rigorous approach to identifying participants. The following chart provides some identification options and the risk levels where their implementation may be appropriate.

Identification Methods	Level of Risk
No registration, only self-identification as part of the signing process	Negligible or very low
Comparison of user supplied information with a trusted data source before authorization	Low
Acceptance of a previously conducted and trusted identification and registration process where the individuals personally presented themselves and proof of their identities	Medium
A separate identification process to authorize the use of an e-signature where the individuals personally present	High

⁷ An exception is PKI supported solutions, where components and options are specified in the operative Certification Policy.

themselves and proof of their identities	
--	--

There are many variations on the approaches presented above, including requiring specific identification documents. For example, a governmental entity may require two pieces of identification (certified copies or originals), at least one of which is a government identification containing a photograph (e.g., driver's license, non-driver identification, passport) for medium or high-risk transactions.⁸ Identification may also include a follow-up verification process sometimes conducted by a third party.

Signer Authentication refers to the policy, process and procedures used to authenticate the signer and thereby establish a link or association between the signer and the information and method used to sign (see [section 3.5.3](#) for additional information on authentication). The strength of the authentication system, including the level of trust that the credential or information used to authenticate has remained in the signer's sole possession, can protect against fraud and repudiation. The following chart provides some authentication options and the risk levels where they may be appropriate.

⁸ State agencies seeking to collect personal information must do so in compliance with the obligations and requirements provided in the New York State Personal Privacy Protection Law (Public Officers Law, Article 6-A)

Authentication Methods	Level of Risk
No method of authentication beyond user identification as part of the signing process	Negligible
User selected PIN or password	Negligible to low
PIN or password assigned by the governmental entity	Low
PIN or password assigned by the governmental entity along with user supplied verifiable personal information	Low to medium
Cryptographic key or biometric (often includes two factor authentication through the use of a password or PIN)	Medium to high
Two factor authentication including the use of hardware device such as a smart card	High

Signature attestation of the record's integrity refers to the ability of an e-signature to protect against unauthorized access or tampering with the signed e-record and therefore reduce the risk of intrusion, inadvertent disclosure, fraud, and repudiation. Various e-signature approaches provide different levels of protection for an e-records integrity. This protection can be achieved by the system that collectively manages the e-record and the associated e-signature. In such a case, the key factor is the system's trustworthiness and its controls to ensure that a record or signature has not been tampered with or modified, as well as the system's ability to detect if that has occurred (see [section 3.5](#)). Governmental entities may also need to implement controls to ensure that the integrity of the electronically signed record is not compromised during transmission (see [section 3.3.2](#)). Added security is provided by technologies (e.g., digital signatures) where the validation of the signature itself ensures that the record and signature have not been tampered with or modified. The following chart provides some e-signed record integrity options and the risk levels where they may be appropriate.

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

Cost-Benefit Analysis: Governmental entities, after identifying possible alternatives and evaluating their feasibility and effectiveness, may conduct a cost-benefit analysis for each proposed solution or solution component to determine which are appropriate for their circumstances. A cost-benefit analysis can help entities decide how to allocate resources

and implement a cost-effective e-signature solution. The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the solution are appropriate to the level of risk. For example, an entity would not want to spend millions of dollars on an e-signature solution that addresses repudiation where such a risk is unlikely and would only have an impact of a few thousand dollars. On the other hand, if the risk could have devastating consequences, selecting a low cost, less secure solution would not be advisable. A cost-benefit analysis for a proposed e-signature solution can encompass the following:

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

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, [§ 540.2\(a\)](#)
 - Conclude with the decision reached on an e-signature approach and include support or justification for this decision.
- The resulting documentation should be:
 - Accurate and readily available.
 - Clear and understandable to an outside audience as well as current and future staff who may be asked to explain the decision making process.
 - Retained as long as the e-signature solution is used.

A governmental entity may elect to develop a more formal business case document that would evidence the business analysis and risk assessment employed in the selection of its e-signature solution. For instance, the development of a more formal record may be justified where an entity anticipates its selection to be disputed by third parties.

2.8 Special Issue: Multiple Signatures

Records that require multiple signatures raise the same issues involved with single e-signatures as well as a number of unique concerns. As with any signature application, governmental entities need to ask themselves whether or not additional signatures are legally required and/or necessary for business purposes. Multiple signatures will typically be required if multiple approvals are needed to complete a transaction, information is collected from multiple individuals and each must attest to its accuracy, multiple individuals need to be held accountable for actions, there is a risk of repudiation or fraud from a number of individuals to a transaction, or contractual documents are required to be signed by all parties to a transaction. To conform to the ESRA definition of an e-signature, each e-

signature must be attached to or associated with the e-record being signed during transmission and storage, each must be executed or adopted by an identified individual who intends to sign the record, and the signing process must capture each signer's intent.

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

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

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

Governmental entities should have system security policies and programs that are compliant with the [New York State Technology Policies](#). A security policy and program for systems and information used to create and/or authenticate e-signatures may require some additional elements including:

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

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

Special Requirements for the Protection of Cryptographic Keys: Cryptographic methods impose the following specific requirements on both individual signers and governmental entities to protect the cryptographic keys used to sign:

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

Cryptographic keys used to sign should be generated so that they are only revealed to or can be used by the intended electronic signatory: The key can be generated by the actual user and installed for use within his or her hardware or software by a variety of techniques including one or more of the following: manual entry, transfer of a disk, read-only-memory device, smart card or other hardware token. The initial information used to establish an e-signature (often referred to as *keying material* in *asymmetric crypto-systems*) may serve to establish a secure online session through which a cryptographic key is generated and installed.

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

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

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

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

- **Storage on personal computers:** The storage of a cryptographic key within software applications such as browsers affords the lowest level of security. If stored on a personal computer, the key should reside in a software or hardware component that is password-protected or protected in some other

way. Storing the key in an encrypted form will afford a higher-level of security. Storing it as an encrypted software token separate or independent of other applications is more secure. It is **not** recommended that a signing key be stored in an Internet browser even if it is in encrypted form. The key must be decrypted to be used. Sophisticated attackers could gain access to a key by writing a program that manages to get itself run on a user's computer, waits for the signing information to be decrypted, and then sends it out over the network. User profiles and personal information including signing information in browsers can be protected through high security settings. However, security for popular browsers is usually set at medium by default, which makes such attacks possible.

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

2.10 Governmental Entity Consultation with OFT

The ESRA regulation requires governmental entities to consult with OFT before defining additional standards for e-signatures and e-records to ensure that such standards are consistent with ESRA. Governmental entities contemplating the use or acceptance of an e-signature solution should confer with OFT early in the planning process. For detailed inquiries on specific technologies or e-signature solutions, OFT will 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.

2.11 Additional Assistance

This section provided a starting point for those contemplating an e-signature solution. If there are additional questions concerning these guidelines, the implementation of specific technologies, or conducting a business analysis and risk assessment, please contact:

NYS Office for Technology
Office of Counsel
State Capitol Empire State Plaza
PO Box 2062
Albany, NY 12220-0062
518-473-5115 voice
nyecom@oft.state.ny.us
<http://www.oft.state.ny.us/ecommerce/index.htm>

**Summary Guidelines for Selecting an E-signature Solution
Business Analysis and Risk Assessment**

Defined in ESRA regulation, § 540.4 (c), as:

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

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

The 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 an evaluation of its business needs, potential legal risk and resulting impact should its e-signature selection be unsuitable for the transaction in question.

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

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

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

Components	Considerations
<p>Matching E-signature Functionality to Risk Level</p>	<p>Signer identification or registration: the method or process used to identify and authorize an individual to use an e-signature application. The more robust or stringent the identification method the more assurance that the signature has been used by the person who he or she purports to be.</p> <p>Signer Authentication: the policy, process and procedures used to authenticate the signer and thereby establish a link or association between the signer and the information and method used to sign. The strength of the authentication system can protect against fraud and repudiation.</p> <p>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.</p>
<p>Cost-Benefit Analysis: to demonstrate that the costs of implementing the solution are appropriate to the level of risk.</p>	<p>Determine the impact of implementing the solution.</p> <p>Determine the impact of <i>not</i> implementing it.</p> <p>Estimate the costs of the implementation.</p> <p>Assess costs and benefits against the system and data criticality to determine the importance of implementing the solution, given their costs and relative impact.</p>

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 [§ 540.2\(a\)](#) of the ESRA regulation.
- Conclude with the decision reached on an e-signature approach and include support or justification for this decision.

The resulting documentation should be:

- Accurate and readily available.
- Clear and understandable to an outside audience as well as current and future staff who may be asked to explain the decision-making process.
- Retained as long as the e-signature solution is used.

3. E-records Guidelines

3.1 Background

Governmental entities are required to retain e-records to meet legal minimal records retention requirements imposed by business or administrative needs and legal mandates. OFT developed this section to provide general direction on how governmental entities can ensure the authenticity, integrity, security, and accessibility of e-records. This section is not primarily designed to explain how statutory or regulatory requirements can be met, nor intended to exclude the use of other methods of achieving these objectives. However, where specific ESRA or other requirements are mentioned, the section provides 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 managing e-records.
- Producing e-records.
- Maintaining authentic and complete e-records that are accessible over time.
- Maintaining secure, reliable and trustworthy e-records systems.

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 material 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.

3.2 General Concepts and Guidelines

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 (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).

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 that should be addressed but can be modified or replaced when an e-records system is developed.
- Past practices in managing paper records that can be eliminated when an e-record system is developed.

Legal counsel and other knowledgeable staff should be consulted to identify requirements relevant to e-records as soon as possible in developing e-records systems. The New York State Archives also provides advisory services in identifying records requirements for state agencies and local governments outside of New York City. New York City agencies should consult with the NYC Department of Records and Information Services (DORIS).

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 discussed in section [2.7.1](#) may be useful. As discussed, 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?

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. Additional guidance on the legal admissibility of e-records can be found in the State Archives' [Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment, 1994 \(State Government Records Management Information Series\)](#).

3.2.4 Training is Critical

Training is particularly important in ensuring that staff adequately maintains systems used to create and retain 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.

3.3 Producing E-records

A governmental entity must produce records necessary to carry out its functions and to meet the specific recordkeeping requirements tied to those functions. 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.

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 ([Title 9 NYCRR Part 540.5 Electronic Records](#)) 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. Specific controls are discussed in the State Archives' [Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment 1994 State Government Records Management Information Series](#).

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.

- Secure Sockets Layer (SSL) is often used for web-based applications. However, older browsers are not necessarily enabled to use this technology.
- 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 Network* (VPN), which generally requires the same vendor's equipment at both endpoints, is used for ongoing business relationships via public networks.

Specific techniques may be used independently 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, retinal scan or a fingerprint). Governmental entities could use the business analysis and risk assessment required for selection of an e-signature solution (see [section 2.7](#)) to help determine what authentication measures, if any, would be appropriate to address potential risk in a given transaction.

Maintain measures to document the date and time of receipt: It is important to document this information for many 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-date stamping can be used where a neutral or trusted third party applies the electronic date and time stamp. A trusted time authority applies 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.).

3.3.3 Uniquely Identify Each Record

Establish a method to uniquely identify each record: Minimal unique identification data may include:

- Identification number or name
- Identity of record creator, information source or the owner (business unit)
- Date and time of receipt or creation
- Indexing information such as subject terms

3.3.4 Capture an E-record for Each Transaction Conducted through a Multi-entity Web Portal

Many Federal agencies and state governments are developing web portals that allow citizens, businesses, and local governments to seamlessly access services and information provided by multiple governmental entities. Some portals are designed to allow users to complete or begin a number of related transactions provided by different entities. Often one lead entity hosts and manages such a portal. For example, a prospective business owner could use a small business portal operated by an economic development agency to apply for a tax incentive offered by that agency as well as apply for business permits required by other agencies. The portal user might begin by providing baseline data required for all of the transactions and then complete each transaction directly with the appropriate agencies. To the user, however, these multiple transactions appear seamless. Portals that allow multiple transactions with multiple governmental entities raise e-records' issues that participant entities will need to address.

Determine who owns the data and records captured in the portal: The custody of information and records is a policy and legal issue, not a technical one. Regardless of its physical custody, the entity responsible for the government function to which the e-record relates is most likely its legal custodian. However, entities should consult with their legal counsel to clarify record custody issues. Using the above example, the economic development agency may collect baseline data from a user, which is used by all participating agencies. However, each participant also collects unique data needed to complete its transaction and retains legal custody of the record of that transaction. Any common data that may reside with the agency managing the portal could be viewed as an interim record of that agency.

Define the participants' roles and responsibilities in managing data and records: Although a portal will likely be hosted and managed by one agency, each of the participants will have some role in managing the records and information captured in the portal. These roles will vary based on the technology used, the transactions conducted, the legal custody of the records captured, and the relationship between the participating entities. However, records and information management roles need to be determined when the portal is being

developed. It is advised that a governance policy be developed to serve as the constitution for entities participating in a portal project. The policy should explain how the portal will operate and how participating agencies will work together including the role each will play in managing information and records.

Maintain e-records of transactions conducted in the portal in secure e-records system: Regardless of how an e-record is originally captured, it should ultimately be maintained in a secure e-records system under the control of the entity that has legal custody of the record and will rely on it. It is not likely or advisable that the database that supports the portal or even the participating entities' website is an appropriate repository for such records.

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

Entities must maintain reliable and authentic e-records that 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 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](#).

3.4.1 Maintain Integrity 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 policy on 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.
- **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 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 [3.4.2](#))

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 as described in [section 3.5](#). 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. OFT's [Electronic Document Management Systems: A Cookbook for Success](#) provides an introduction to these solutions. The [U.S. Department of Defense](#) also tests and certifies document management products that include e-records management capabilities.

3.4.2 Retain E-records in an Accessible Form for their Legal Minimum Retention Periods as Established in State Archives or Local Retention Schedules

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 functions 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).

Maintain e-records in encrypted form only as long as security concerns warrant: E-records are sometimes encrypted for security purpose during transmission over networks and during the course of a transaction. Highly sensitive records may be stored in encrypted form for extended periods of time. However, the loss or destruction of a decryption key could result in the loss of access to encrypted records. Therefore, governmental entities should avoid storing e-records in encrypted form beyond the point that security concerns warrant such a measure. The system security measures described in [section 3.5](#) should be sufficient to protect most e-records maintained by governmental entities.

Develop retention solutions that best address an e-record's retention requirements: Any e-records retention solution should address the required length of time records must be retained. For instance, records retained for only a short period of time (three to six years) could be maintained in the system that created or captured them for their entire retention period. However, any e-records retention solution developed should accomplish the following:

- **Maintain the e-record's original functionality to the degree necessary:** Many e-records lose their meaning and usefulness if they cannot be used or function as they did when they were in their original environment (e.g., ability to be processed or searched). Determine if it is necessary to retain an e-record's functionality. If so, the record should be retained in a format that can be processed or used by available technology.

- **Preserve the context and links between components of e-records:** In order to interpret the meaning of some e-records, all necessary file structures and relationships between record components need to be retained for the record's retention period. For example, a video file and the file that is part of a multimedia document might need to be retained for the record's retention period. Preservation of the context and links between components of an e-record becomes a critical issue for electronically signed e-records (see [section 3.4.5](#)).
- **Develop solutions that can be applied with the least human intervention:** A solution that is more automated is likely to be less labor-intensive and more efficient, therefore increasing the likelihood that it will be implemented.
- **Develop solutions that are independent of media format:** Long-term preservation solutions should be independent of media because media formats and standards will generally change during the retention period. Solutions need to focus on managing the records so that they are accessible and useable throughout their retention periods.

Address long-term retention requirements and records preservation: Some e-records have very long or permanent retention requirements and the retention solution developed must preserve long-term access to them. Unfortunately, there is no easy technical solution to the long-term retention of e-records. However, there are a number of approaches to the problem. The costs and benefits of any approach must be weighed along with continuing internal and external access needs. The various approaches to maintaining long-term access to e-records are described below.

- **Migration:** System migration is the most commonly cited solution to preserving e-records. It requires the manager of an automated record keeping system to move e-records from an existing system to a more modern system before the original system becomes obsolete and inoperable. Migration should be implemented incrementally along with periodic system and software upgrades. It is a strategy often used in conjunction with maintaining e-records in a standard format.
- **Storing e-records in standard formats:** The use of standard formats (relational databases, ASCII, Portable Document Format, SGML, etc.) can help reduce the rate of technological obsolescence and the need for migration. However, this is not a permanent solution because standards change or are replaced over time. The National Institute of Standards and Technology has been exploring the use of standard e-records storage formats since 2000.
- **Encapsulation:** Encapsulation refers to a method of capturing the look and feel of the original record along with any required metadata as a single digital object in a portable format. In some ways, encapsulation combines system migration with use of standard formats. Encapsulation strategies are just beginning to be investigated.
- **Conversion to other media:** It is relatively simple to output e-records to durable media such as paper or microfilm. E-records can be output directly to microfilm through computer-output microfilm (COM) and the microfilm can be maintained as the preservation copy. This solution is only viable for e-records in relatively simple formats, when all required metadata can be captured on the output media, and where there will be no critical need to access or use the record in electronic form.
- **Emulating obsolete technology:** Emulation consists of using hardware and software to allow one computer technology to act as if it were another technology. This solution

allows e-records to remain in their original file formats while the hardware and software change. Emulation is complicated and expensive to achieve for any sophisticated system. Research on emulation solutions is ongoing.

3.4.3 Search and Retrieve E-records in the Normal Course of Business for all Business Uses throughout Their Entire Legal Minimum Retention Period

Maintain adequate search and retrieval capabilities to ensure that e-records can be retrieved for all legitimate business purposes for their full retention period: This should include retrieval during the period that records are stored on nearline or offline media. This will demand adequate indexing (see [section 3.3.](#)) as well as search tools. The document management solutions mentioned in section **3.1.2** also include robust search capabilities.

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

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. OFT has developed a model [Internet 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 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 should 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 [Part 540.5\(b\)\(1\)](#)) require governmental entities to provide access to e-records 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 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.

3.4.5 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 importance of preserving the context and links between components of e-records is critical if they 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 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: To date, there have not been any reported court decisions wherein the authenticity of an e-signature has been challenged. Nor has any court decision questioned the reliability of an electronically signed record on the basis of its e-signature. Therefore, it is difficult to determine what minimal information will be needed to demonstrate the authenticity and reliability of an electronically signed record in a legal proceeding. Absent a clear position from the courts, governmental entities can use the business analysis and risk assessment conducted in selecting an e-signature approach to determine what information needs to be retained as part of the signed e-record for these purposes (see [section 2.7](#)). In fact, the e-signature method selected will partially determine the approaches available 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.⁹

- [*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 noted, until the courts have addressed the issue, it will be difficult to define clearly what constitutes adequate documentation of an e-signature.

⁹ NARA, *Records Management Guidance for Agencies Implementing Electronic Signature Technologies* (October 18, 2000), pp. 7-8. Copies of this publication are available at: http://www.archives.gov/records_management/policy_and_guidance/electronic_signature_technology.html

- 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 (see [section 3.5](#)) 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 would need to retain all the records and the system functionality specific to a particular e-signature technology or approach needed for the revalidation process. For digital signatures produced using a PKI, [New York State Digital Certificate Policy](#) specifies the records that need to be retained to validate a digital signature as well as governing the issuance and use of digital certificates issued under the policy.¹⁰

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 (see [section 3.4.1](#)). 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 offline media 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 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.

¹⁰ See *New York State Digital Certificate Policy* section 4.6 Records archival at: <http://www.oft.state.ny.us/policy/PolicyByPubDate.htm>

Maintaining adequate documentation of an e-signature's validity and the ability to revalidate 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 records inactive storage, when repudiation risk is low, an entity may determine it can rely solely on documentation of the signed e-record's validity.¹¹

NARA, the National Archives of Canada, and the Australian National Archives have generally questioned the practicality of maintaining the ability to revalidate signed e-records that will be maintained for long periods of time or permanently.¹² They believe 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. For the foreseeable future, the long-term retention of both signed and unsigned e-records will remain one of the more difficult challenges faced by all entities.

3.5 Maintaining Secure, Reliable and Trustworthy E-records Systems

The acceptance of e-records for legal, audit, and other purposes is contingent on establishing their authenticity and reliability by demonstrating the trustworthiness of the system used to produce them. Systems that produce records must be shown to do so in the normal course of business and in an accurate and timely manner. The following suggestions should assist record keepers in their efforts to maintain authentic and reliable e-records that can be successfully used for these purposes.

3.5.1 Make Sure the System Performs in an Accurate, Reliable, and Consistent Manner in the Normal Course of Business

Define and document system management policies and procedures: Written policies and procedures for each system should:

¹¹ Another option available where PKI-based or other digital signatures are used is to appoint a records custodian or "digital archivist" who would periodically over-sign the original record (and original signature), using a signature with stronger cryptography. The digital archivist's signature would include a certification that the records had been validly signed at the time of the digital archivist oversigning. Both the Canadian and US federal governments' PKI are considering this function. See for example Federal PKI Technical Work Group, Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations (4 September 1998), Chap. 13 Records and Archives, pp. 42-44 available at <http://csrc.nist.gov/pki/twg/>

¹² NARA, Records Management Guidance for Agencies Implementing Electronic Signature Technologies (October 18, 2000), pp. 7-8; National Archives of Canada, Guidelines For Records Created Under a Public Key Infrastructure Using Encryption And Digital Signatures (Date Modified: 2001-09-04) http://www.archives.ca/06/0618_e.html; e-mail correspondence with Anne Robertson, Assistant Director, Recordkeeping Standards and Policy, National Archives of Australia, Jan. 29, 2003.

- Describe the methods used to create, modify, duplicate, and destroy records.
- Define the roles and responsibilities of the individuals involved in records creation, maintenance, and destruction.
- Provide for consistent quality control, problem resolution, and other activities that might be subject to inconsistent action or misinterpretation.
- Demonstrate the purpose and uses of the system.
- Be kept up-to-date and readily available.

Assign system management roles and responsibilities, and implement the principle of separation of duties pursuant to written policies: *Separation of duties* refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes the payment.

Develop and maintain problem resolution procedures including incident reporting and response procedures: These can help ensure that a system's problems are quickly identified, attended to and resolved. They, along with operation logs and a help desk can help document that problems have not jeopardized the integrity of the system and its e-records.

Test system performance including the reliability of hardware and software: The reliability of hardware and software affects the authenticity and integrity of e-records. Equipment malfunctions can alter the content of e-records. If data processing equipment and software used to store and produce e-records are not reliable, the integrity of the records may be challenged. The integrity of e-records can be enhanced by:

- Routinely testing hardware and software as well as performing maintenance in accordance with the manufacturer's advice.
- Retaining documentation related to hardware and software procurement, installation, and maintenance.
- Maintaining operation logs and running schedules to document the reliability of system operation and performance.

Governmental entities should consider an external technical evaluation (or audit) of their high-risk systems. An independent verification of such systems could document the reliability of the systems and the e-records they produce as well as increase public confidence in them. Retention requirements for records that document the reliability of hardware and software are contained in the "Electronic Data Processing" sections of the various records retention and disposition schedules issued by the State Archives.

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

Provide training and user support to ensure users will implement system

procedures: Formal training and support programs help ensure that staff understand and implement policies and procedures. Providing staff with instructions for data input, processing and retrieval will support staff training and document the entity's efforts to train staff. Documentation showing that the entity provided sufficient supervision to oversee staff in the system's proper use and maintenance will also strengthen the case that proper procedures were implemented during such use and maintenance. It is also advisable to keep records of both attendance at training sessions and the issuance of certifications for training received.

3.5.2 Protect E-records to Enable their Availability throughout their Retention Period

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 offline media. Various measures, such as standard labeling and maintaining tracking logs, provide physical and intellectual control over tapes, diskettes, and other media. Offline media 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. Detailed information on magnetic tape media is available in the National Commission on Preservation's guide to [Magnetic Tape Storage and Handling](#).

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.

3.5.3 Limit System Access to Authorized Individuals and for Authorized Purposes and Maintain Physical and Environmental Security Controls

Establish a system security policy and program compliant with NYS Technology Policy related to information security that limits system access to authorized individuals and for authorized purposes and maintains physical and environmental security controls.

3.6 Additional Assistance

If there are additional questions concerning ESRA-related e-records issues, please contact:

Office of Counsel
NYS Office for Technology
State Capitol, ESP PO Box 2062, Albany, NY 12220-0062
Call 518-473-5115; email nyecom@oft.state.ny.us;
Visit www.oft.state.ny.us/ecommerce/index.htm

Summary E-records Guidelines

General Concepts and Guidelines

Identify and assess specific legal, business, and other requirements that apply to e-records

Base e-records management measures on the records' value

Focus on the systems and business processes that produce e-records

Training is critical

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

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

Outcomes	Implementations
Maintain integrity of e- records as captured or created so that they can be accessed, displayed, and managed as a unit	Maintain e-records management policy documenting the organization's policy on information management and storage

	Develop controlled storage or filing systems that maintain the integrity and accessibility of e-records
Retain e-records in an accessible form for their legal minimum retention periods as established in State Archives or local retention schedules	<p>Adopt and use records retention and disposition schedules in compliance with the Arts and Cultural Affairs Law or local law</p> <p>Maintain e-records in encrypted form only as long as security concerns warrant</p> <p>Develop retention solutions that best address an e-record's retention requirements</p> <p>Address long-term retention requirements and records preservation</p>
Search and retrieve e-records in the normal course of business for all business uses throughout their entire legal minimum retention period	Maintain adequate search and retrieval capabilities to ensure that e-records can be retrieved for all legitimate business purposes for their full retention period
Produce authentic copies of e-records and supply them in useable formats, including hard copy, for business purposes and all public access purposes	<p>Develop or revise access and personal privacy protection policies to include e-records</p> <p>Develop methods to provide public access to e-records and to protect personal privacy and confidentiality</p> <p>Provide access to e-records in the form the user prefers</p>
Develop an approach to maintain the authenticity and integrity of electronically signed e-records	<p>Determine what information needs to be retained to maintain a valid, authentic, and reliable signed e-record</p> <p>Preserve the link or association between the various components of a signed record over time</p>

Maintaining Secure, Reliable and Trustworthy E-records Systems	
Outcomes	Implementations
Make sure the system performs in an accurate, reliable, and consistent manner in the normal course of business	<p>Define and document system management policies and procedures</p> <p>Assign system management roles and responsibilities, and implement the principle of separation of duties pursuant to written policies</p> <p>Develop and maintain problem resolution procedures including incident reporting and response procedures</p> <p>Test system performance including the reliability of hardware and software</p> <p>Maintain audit trails of system activity by system or</p>

	<p>application processes and by user activity</p> <p>Provide training and user support to ensure users will implement system procedures</p>
<p>Protect e-records to enable their accurate and ready retrieval throughout their retention period</p>	<p>Develop a contingency plan that includes data backup, disaster recovery, and emergency operations</p> <p>Implement media controls</p> <p>Perform routine backups</p>
<p>Limit system access to authorized individuals and for authorized purposes and maintain physical and environmental security controls</p>	<p>Establish a system security policy and program compliant with NYS Technology Policy related to information security</p>

Additional Web-Available Resources

1. New York State Standards, Guidelines and Resources

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

Best Practice Guideline G02-001: Guidelines for Internet Privacy Policies

New York State Certificate Policies for Digital Signatures & Encryption

Other OFT Resources: [Electronic Document Management Systems: A Cookbook for Success](#)

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

EGovernment Archives Technical Information

Guidelines for Ensuring the Long-Term Accessibility and Usability of Records Stored as Digital Images

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

Local Government Records Retention Schedules

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

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

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

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

Retention and Disposition of Library and Library System Records

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

Managing Records In Automated Office Systems

Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment

Managing E-Mail Effectively

Guidelines for Determining if a Stand-alone Imaging System is the Best Choice for You

Laws and Regulations Relating to Local Government Records: Local Government Records

Optical Storage Systems for Records and Information Management: Overview, Recommendations and Guidelines for Local Governments

Retention and Disposition of Records: How Long to Keep Records and How to Destroy Them

2. Other New York State Resources

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

3. Other Resources

Center for Technology in Government, *University at Albany*, [Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation](#)

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

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

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

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

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

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

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

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

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

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

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

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

[FIPS 140-1, 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. FIPS 140-1 is in the process of being replaced by [FIPS 140-2](#).

Cryptographic module validation testing is performed using the [Derived Test Requirements for FIPS PUB 140-1](#). It lists all of the vendor and tester requirements for validating a cryptographic module, and it is the basis of testing done by the CMT accredited laboratories.

The National Institute of Standards and Technology (NIST) maintains the [FIPS 140-1 Cryptographic Modules Validation List](#) of all validated FIPS 140-1 implementations. An alphabetical [list of FIPS 140-1 vendors](#) (vendors with validated crypto-modules) is now available.

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

Defined Terms

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

Terms defined in this policy:

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

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

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

Business analysis and risk assessment – is defined by the ESRA regulation as "identifying and evaluating various factors relevant to the selection of an electronic signature for use or acceptance in an electronic transaction. Such factors include, but are not limited to, relationships between parties to an electronic transaction, value of the transaction, risk of intrusion, risk of repudiation of an electronic signature, risk of fraud, functionality and convenience, business necessity and the cost of employing a particular electronic signature process."

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

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

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

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

Digital Signatures - are produced by two mathematically linked [cryptographic keys](#), a private key used to sign, and a public key used to validate the signature. A digital signature is created when a person uses his or her private key to create a unique mark (called a "signed hash") on an electronic document. The recipient of the document employs the person's public key to validate the authenticity of the digital signature and to verify that the document was not altered subsequent to signing. Digital signatures are often used within the context of a Public Key Infrastructure (PKI) in which a trusted third party known as a Certification Authority (CA) binds individuals to private keys.

Electronic record (E-record) – Shall have the same meaning as defined in State Technology Law §102. 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 (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 §102. 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.

Governmental Entity – Shall have the same meaning as defined in State Technology Law §102. 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.

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

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

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

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

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

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

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

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

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

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

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

Required Submissions & Notices

Not applicable.

Compliance

Not applicable.

Contact Information

Questions concerning this best practice guideline may be directed to the New York State Office for Technology, Office of Counsel, (518) 473-5115 or NYECOM@oft.state.ny.us.