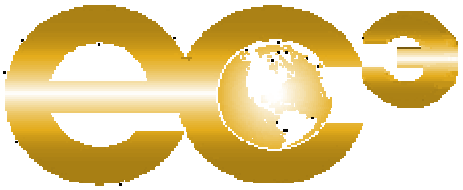
Impact of Electronic Signatures on Security Practices for Electronic Documents



Exposure Draft

A National Electronic Commerce Coordinating Council White Paper

December 2001

National Electronic Commerce Coordinating Council

The National Electronic Commerce Coordinating Council (**NECCC**) is an alliance of national state government associations dedicated to the advancement of electronic government within the states. The Council is comprised of the National Association of State Auditors, Comptrollers and Treasurers (**NASACT**), the National Association of State Chief Information Officers (**NASCIO**), the National Association of State Purchasing Officials (**NASPO**), and the National Association of Secretaries of State (**NASS**). In addition to these voting members, other governmental and private organizations participate in an advisory capacity. These associations include the Information Technology Association of America (**ITAA**), the National Automated Clearing House Association (**NACHA**), the National Association of Government Archives and Records Administrators (**NAGARA**), the National Association of State Chief Administrators (**NASCA**), the National Association of State Treasurers (**NAST**), and the National Governors Association (**NGA**). ITAA and NACHA represent private information technology companies and the financial services and technology industries.

NECCC Board

Chair: **Carolyn Purcell**, NASCIO, Texas CIO

Vice Chair: **Hon. J. Kenneth Blackwell**, NASS, Ohio Secretary of State

Secretary/Treasurer: **Richard B. Thompson**, NASPO, Maine Director of State Purchasing

Immediate Past Chair: **Hon. J.D. Williams**, NASACT, Idaho State Controller

NASACT	**Hon. Ralph Campbell, Jr.**, North Carolina State Auditor **Hon. Jack Markell**, Delaware State Treasurer
NASCIO	**David Lewis**, Chief Information Officer, Commonwealth of Massachusetts **Aldona Valicenti**, Chief Information Officer, Commonwealth of Kentucky
NASPO	**Dave Ancell**, Director, Office of Purchasing, Michigan Dept. of Management & Budget **Denise Lea**, Director, Louisiana Office of State Purchasing
NASS	**Hon. Mary Kiffmeyer**, Minnesota Secretary of State **Hon. Elaine Marshall**, North Carolina Secretary of State
ITAA	**Basil Nikas**, CEO, iNetPurchasing.com
NACHA	**William Kilmartin**, Accenture
NAGARA	**Terry Ellis**, Salt Lake County Records Management and Archives
NASCA	**Pam Ahrens**, Director, Idaho Department of Administration
NAST	**Hon. Jack Markell**, Delaware State Treasurer
NGA	**Thom Rubel**, National Governors Association

Acknowledgements

This white paper was prepared by the 2001 NECCC E-Sign Security group. Contributors include: **Dave Dovenbarger**, **Heidi T. Glunz**, **Peter Goolsby**, **Jerry Johnson**, **Roselyn Marcus**, **Valerie McNevin**, **John Messing**, **Nancy Rainosek**, **Russ Savage**, **Doug Seidman**, and **Michael Totherow**.

Table of Contents

Government preserves public trust through public record maintenance under its direct control or by regulation. Record integrity smoothes the course of commerce and helps to maintain a stable society. Electronic signatures introduced by E-Sign[1] and UETA[2], create new security challenges for maintaining public records integrity. This paper discusses those challenges. It introduces a document classification scheme, a best practice state governments can adopt to help them face the security challenges of E-Sign and UETA.

E-sign states electronic documents containing electronic signatures cannot be denied force of law just because they are electronic. When can they be denied force of law? One answer is when the electronic document cannot be proven valid, or when document integrity has been compromised due to inadequate security. With the introduction of E-sign/UETA, governments have a new type of reliance upon electronic records. Governments need to take a new look at their information security practices.

Two principal system methods give evidence of authenticity:

System secure -- secure the system and provide evidence demonstrating a secure system.

Document secure --secure the record and provide evidence demonstrating a secure record.

These methods represent the ends of a continuum for securing electronic records. Security system design may incorporate features and benefits of either method in building effective security practices.

Behold the consequence of the electronic signature – the electronic document

Government's record retention, whether paper or electronic, is intended to give evidence of some action. E-sign establishes that record retention requirements of electronic records created by electronic signatures are not different than retention requirements for paper records. A record may not be denied solely because it is electronic, but the requirement for proving a record's authenticity still remains. As does the requirement for the record to remain accessible to all parties entitled to access.

Money is one of the most well known 'records' maintained by government. Paper money is a representation of resources valuable in society--it is a record of value. Similarly we consider signed records of societal value. The value may be relative, such as ownership, obligation or statement of fact, but it is a value nonetheless. Where we have relied upon a physical presence (i.e. paper) for proof of that value in the past, E-Sign and UETA enable proofs of value to exist in an electronic format. The value represented by a record must be considered when securing electronically signed records intended for reliable, authentic recorded evidence.

---

[1] E-Sign, Electronic Signatures in Global and National Commerce Act, Public Law 106-229 adopted June 30, 2000.

[2] Uniform Electronic Transactions Act, as promulgated to the states to adopt by the National Conference of Commissioners on Uniform State Laws. See http://www.nccusl.org for more information.

Money also has its electronic counterpart. While the establishment of the credit card was originally based upon the presence of the wet signature to capture the commitment to payment, the growth of electronic commerce has brought about payment without the presence of a credit card. While there is strong regulation and security burden to maintain these electronic transactions, the industry is also based on acceptable losses and averages to outweigh denying payments. Government transactions, where the value is the authenticity of the record, generally does not have the luxury of factoring in acceptable losses. The electronic document, created by an electronic signature, does not have a direct correlation to electronic commerce regulation.

Securing the electronic document

Security relative to electronic documents is not new. For years, network administrators and chief security officers have built systems to protect electronic documents. With the introduction of E-sign, governments face the challenge of ensuring the electronically signed document is not changed during the retention period and therefore retains authenticity of its origination. Thus the security of electronic documents signed electronically takes on the new dimension of time to prove authenticity and remain accessible to the parties interested.

In creating the signed paper document, the signer verifies the contents to match their intent at signing. Upon acceptance of the contents, they formalize their intent by attaching their signature to the document. The formalized document then becomes the record of intent. When the intent is questioned after the document is signed, the document is inspected for alterations and the signature is often compared to the signer's verifiable signature to assure the authenticity of the formalized document. Both the electronic document and the electronic signature need to be secured for similar tests of authenticity. The document that retains its original integrity and is conclusively linked to the original signer retains "authenticity."

Introducing electronic signatures has not changed the reliance upon security, but the objective has changed. The past requirements focused on securing the perimeter of the system to control access. The objective was to maintain authoritative information by controlling who may access the system. The information, in the current record, represented the authoritative record and an index to the supporting paper documents that actually formalized the actions. Thus the questioning of either the authenticity or integrity of the information is about who may access or update the record backed by paper records authorizing the changes. With electronic documents, the supporting action is also based electronically and will need to be as verifiable as the paper records.

So the twist with electronically signed documents is that as information (documents) enters the system, each information object (document) must retain its own authenticity and integrity within the greater system. This requires systems to not only maintain the authoritative record, but also be able to prove the integrity of the supporting document when questioned. The objective now includes proving the authenticity of the documents

that represent the incremental information updates to the system over the record life cycle.

It can be argued that a properly secured system maintains its own integrity. Because that system retains integrity, the documents can be assumed to retain integrity from the point they enter the system. Thus, integrity of the document relies upon the security of the system. This is a valid argument and should be considered when designing security systems. Given the geometric growth of networking, proving the total enterprise integrity for the validity of a single document may be a daunting and uneconomical task.

Defining the System Secure Electronic Record

Creating system secure electronic records is achieved by associating events of access to a system in order to create a document signifying intent.

An example of a system secure electronic record is a document created with a user's sign-on to a multi-jurisdiction procurement system. The user's authority to sign for procurement is embedded in the system; the record is created through a sign-on and event based authentication captures intent. The record exists conceptually as a 'document' in the system. The collection of different informational pieces along with the user's intent creates a 'document' secured from that user's modification (repudiation) as well as from other users (forgery by impostor). When the 'document' is inspected after the signing, system security and integrity are confirmed (usually a validation process against internal checks and balances hidden from user control) to validate the document. Authority granted to the user and the appropriateness of access control at the document creation time also affects validation. As time passes, the enduring security processes will need not only provide current security procedures, but also maintain secure audit and auxiliary proofs of security throughout time.

Defining the Document Secure Electronic Record

Creating document secure electronic records are achieved by attaching or associating an electronic signature to create a document signifying intent.

Document secure electronic records are typified by documents created with digital signatures (an application of key encrypted messaging, or public key technology). The document is processed into a hash. The hash is encrypted with the signer's private key using a standard algorithm; the resulting encrypted hash, the digital signature, is attached to the document. When the document is inspected after the signing, the encrypted hash is decrypted with the public key and compared to a re-hash of the document. If the two results are the same, then the document has remained unchanged. The document has maintained authenticity.

Any particular signing encryption strength weakens with time as newer tools increase the risk of the document's integrity and authenticity being compromised. An on-going security process is needed to apply and maintain a *current encryption standard* upon the aging document. When the current encryption standard becomes weak, the document is again checked for authenticity. Upon validating the hash comparisons, the

document is digitally signed with the system's private key and the encrypted hash is attached to the document. To validate authenticity over time, the last digital signature (with current encryption standards) is checked. This effectively envelops the contents without affecting its contents.

The two methods of signing are different means to the same end. Both require continuous security precautions; security processes and potential for compromise are distinctively different. Governments need to consider these characteristics when designing security systems for electronically signed records.

Security to Risk

Electronic Signature Classification

Security must be approached with the objective of minimizing potential risks with either record evidencing approach. To properly secure an electronically signed document as evidence, signing process risks and risks associated with the significance of the information must be considered. One example of risk consideration is found in The NECCC's Framework for Electronic Signature Reciprocity (ESR) paper. The Framework establishes levels of trust for cross-jurisdictional reliance upon electronic signatures. That is, the framework establishes the levels of trust at which a state government or other entity can assume electronically signed electronic record (e-record) received from another state has authenticity, integrity, and reliability. The evaluations of authenticity, integrity, and reliability are statements of 'how' the transaction is evidenced, not the content which is evidenced. In most situations, the classification of content is expected to match the classification of trust but this is not guaranteed. Consider an internal employee time sheet process versus the information often contained on those time sheets (SSN) – the time sheet process may be much more relaxed than is generally appropriate for something as sensitive as a person's SSN.

ESR Framework considers three electronic signature process aspects when establishing trust levels:

- Signer is identified.
- Signer is linked to the signature.
- Signature is linked to the integrity of the record.

Analysis of these three aspects of the electronic signature process is the basis for Trust Level: Basic, Medium and High. The ESR also comments on a fourth category: *Rudimentary* which provides a low degree of assurance concerning identity of the individual and is largely only relevant to non-signing transactions with little risk of malicious activity and where the individual's identity is not critical.

The Trust Level gives us a sense of how much we can trust the authenticity of the document. Here's a summary:

	Trust Level	Type of Acknowledgement	Example
1.	Rudimentary	Unauthenticated self-identification	Unauthenticated messages
2.	Basic	Self Acknowledgement or proclamation to systems provides 'application acceptable' or 'potential' repudiation	Self imposed e-signature, like IRS example
3.	Medium	Regulated Closed Acknowledgement provides strong non-repudiation, but defensible	PKI Certificate from known source
4.	High	Control of Confirmation of Acknowledgement and environment allows no repudiation	PKI Certificate within secure system

Content/Data Classification

Classification systems are one generally accepted method of assigning risk levels to documents. To determine the classification of the contents of a document, first break the document into the pieces of information (data elements). Next, determine the classification of each data element in order to identify the highest level of Classification in the document. A document is assigned a classification equal to the classification of its most highly classified data element. Classification allows degree of risk to be expressed in an ordinal way; the degree of risk helps identify how to manage the transaction electronically.

This table is a recommended government document classification structure.

	Classification	**Who can get to**	**Example**
1.	Unclassified	Public Anonymous Access	Free publication
2.	Unclassified but Sensitive	Public Acknowledged Access	Detailed Campaign Finance Reports
3.	Confidential	Restricted "Owner" Access	Detailed Health Care Information
4.	Restricted	Top Secret – Background checks required	Public Safety related Information

Some data element combinations have a higher degree of classification than when the same data elements are presented individually. This phenomenon is evaluated in the context of the document. While the data elements themselves may be of little value individually, the unique combination forming the context can create value greater than the individual data elements alone. Degree of risk may be rated higher, but never lower than the data element / individual level of classification warranted.

Reliance: Data classification and Electronic Signature Classification

Information security practitioners can use the ESR Framework and data classification to determine an appropriate level of security needed for specific electronically signed documents. Using the chart below, plot Reliance (Trust of the electronic signature) against Risk (data compromise / exposure to harm associated with its contents). The resulting matrix of reliance versus risk provides quadrants of security levels to consider. These factors, along with funding, help determine the security provisions to implement for electronic signatures.

		A	B	C	D
		Rudimentary	Basic	Medium	High
1	Public	X (unsigned)	X		
2	Sensitive		X	X	
3	Confidential			X	X
4	Restricted				X

The greater the importance of the data classification, the more important to use an electronic signing process of equal or greater trust. The darker shaded cells to the lower left are inappropriate signing processes for the level of trust the data classification requires. The lighter shaded cells to the upper right are certainly usable but may be more than is needed as a signing process trust level for the data classification being signed.

Building Reliability into Electronic Documents

Regardless of the methodology to retain a document, addressing security requires many considerations. Considerations include everything from network environment to application design. When addressing security, you need to consider all of the pieces that come together from receiving the document up to document destruction. System design to secure electronically signed documents should consider the entire life of the document.

Some systems security professionals contend that to truly document security requires process security from the inception of the document. This means controlling the access and the creation process up to the point the user decides to formalize the document by signing it. The argument is that failure to control the entire process makes the document susceptible to Trojans, viruses, scripting or other programs or techniques intended to alter the document prior to signing.

Proving document authenticity depends upon showing document security during all the phases of the record life cycle. From modification to even simple access, systems must secure documents up to the point of document destruction. Logging document accesses may be more important than originally thought. Because these are authoritative public records, access logging may be a way to prove the document was evidence at an earlier time; or access logging may be the foundation for proving the record has been “reliable” over the life cycle.

Realizing the evolution of security

The nature of security has changed, especially for informational security. Traditional security has matured but has its roots in the *physical world.* The purpose of traditional security was to preserve an authoritative record: an original. This design for security descended from the physical world.

Gold and other things of value are secured by keeping them locked up. A perimeter is drawn around the gold and crossing the security perimeter entails controls on who can enter and what can leave. So much effort is put into securing this perimeter, yet very little is done to ensure the authenticity of the gold. Audits and inventories are performed, weight is measured, but is the gold's chemical structure verified to make sure it's still authentic?

As we design security around documents, we are continually attempting to secure the perimeter—to control the access to the information. This continues to become more difficult as networking expands with the advent of rapid technological change. We should begin to think of information security as more than controlling access. Information security now needs to ensure the integrity of the information as well as access– ensuring authenticity.

With an electronic document it is difficult to assure authenticity, integrity and reliability, because it is just a jumble of ones and zeroes. It can be disassembled, rearranged and reassembled without anyone knowing the difference. The beauty in the electronic realm is that a copy is indiscernible from the original. The information can be duplicated without degrading the value of the information or its authenticity. Whether by backups, mirroring or duplication, copies of an electronic document are just as reliable as the original (at the moment of copying). Gold, on the other hand, only has value in the original composition. This is the difference between traditional security and informational security relative to electronically signed records. Securing the perimeter requires the additional ability to validate the authenticity, reliability and integrity of the information while it was within the system's custodial care.

Redrawing the security lines

The objective is not to completely ignore the security of the perimeter; it merely means we move our last line of defense inwards. Since most records filed with the government are public records, access is expected. What cannot be expected is the alteration of those documents, and that is what we guard against. This is a suggestion to build the last line of defense at the *ability* to duplicate the value. We all backup and we all rely on those backups for disasters, but how many systems know when the disaster hits. Integrating the backup to conduct a comparison of the trusted record as valid against the record requested *at the time of request* is rare. This is comparable to conducting an audited check at the time the record passes through the perimeter. If the audit check finds discrepancy in the record, then the record is questionable. Separating these portions of the network are typically more reasonable to secure than the perimeter itself because of the pervasive networking principles in practice today. System design should

entail description of how the document's life cycle was secure during its life in the system.

Realizing the threats to electronic documents

Security threats to electronically signed documents exist at all phases of the record life cycle.

The nature of electronic signatures in an environment of threat leads to the definitions agreed to for secure electronic signatures: unique to the individual; capable of reliable verification; and linked to the record in a manner such that if the record is changed, the signature is invalidated.

These are also the questions that should be asked.

- How will the electronic signature be unique to the individual?
- How will the electronic signature be reliably verified?
- How will the electronic document retain integrity over its life cycle to detect alteration from the original intent of the signer?

These questions are based on how wet signatures are proven to capture intent in paper documents. Similarly, the secure electronic signature must also retain the authenticity, integrity and reliability throughout the document life cycle.

Security threats remove uniqueness

Keeping the electronic signature unique to the individual using it as primarily a design consideration in the physical process, i.e. where the technology meets the human factor. Proper training and sense of responsibility need to be impressed upon the digital electronic signature user, just as safe credit card practices have become part of user consciousness – perhaps more so.

However, with either a system secure or a document secure system, since electronic signatures are based on security technology and eventually authenticate electronically, the uniqueness can only be maintained if the trust in the authentication module is maintained. This is a lesson learned long ago in network security. Even password-based systems are designed to keep passwords encrypted so they are not ”viewable” to humans, including the super users. Electronic signature password file compromise has more effect than just the vulnerability of newly created electronic documents. Time is simply bytes to a computer; fraud from adding pre-dated documents to the system must also be foiled by security measures.

Security threats stop verification

Although we may be more concerned about keeping verification modules running 99.999% of the time so that electronically signed document creation or validation is not inhibited, we must also worry about protecting against spoofed verification. Just as verifying identity in the real world is subject to impersonation, process design must consider verification impersonation. Situations in which electronic signature validation is intercepted, or spoofed are possible, and detectable in most situations. Secured

transmissions, routing log tables or secondary validation at later dates can assure dependable verification.

Security threats that break signatures

Encryption technology is the heart of electronic signatures, for system secure or document secure documents. Unfortunately for every security algorithm created there will be an algorithm guaranteed to break the technology. Just as we plan to retire hardware at the end of their life cycles, security technology must also be retired, or succeeded, at the end of its useful life cycle. We expect it; systems need to anticipate that encryption technology will be broken. A life cycle may have a retirement date in mind; successor processes need to be ready when a life cycle is cut short.

Building evidence into electronic documents

To provide electronically signed documents as evidence, proving the document's authenticity and integrity since creation is heavily dependent upon the system method used to assure integrity. The concept of electronic documents is still evolving. It might be stated that electronic documents are those pieces of information in an arrangement and format as presented to the signer at the time of signing. It's not just the data that has been signed; it is the format plus the data and the signature that make an electronically signed document. Maintaining evidence is an ongoing question and answer dialog "Has due diligence been committed to maintaining the electronic document?" Doubts arise for systems that collect the answers and not the questions in that dialog. If a system only stores the answers presented in the process of creating the electronic document, how can it be proven later what questions the user was presented with? When the document is questioned, can you re-create the electronic document as signed?

Proving authenticity requires the ability to evidence the history of the document's existence. Proper history should be able to detect the *actions* around the life cycle of a document. This includes:

- Creation of the document
- Storage of the document
- Retrieval of the document
- Access of the document
- Modification of the document
- Retention of the document
- Destruction of the document

Below is a suggested list of record meta information to be kept when building authoritative record systems. The meta information helps meet the elements of evidence:

- Unique Identifier
- Indicator of Authority Version
- Author/Organization information

- Creation Date
- Document Description
- Identification of originating system
- Protection Method
- Media type/format
- Data classification

When the existence of the document is rooted in a system, integrity is based on the entire system integrity. A history of creation through destruction is in the securing electronic document system audit logs and/or transaction logs. Since the electronic document resides there, all of the *actions* affecting the document must be collected from the system.

But a self-evidencing document has more in common with traditional document management techniques. The self-evidencing document contains the authenticity of creation within the document, and more importantly, the evidence of modification from its originally signed creation. From there forward, the document enters a document management system to track its storage, retrieval, access, retention and destruction. Document integrity is preserved through subsequent life cycle events by the validation of the authenticity of creation (re-inspecting electronic signature on the document to still be valid).

With either method, “system secure” or “document secure”, effective evidence can only be obtained through proper planning and identifying the security aspects surrounding the electronic document *before* creation. Jurisdictions should begin to look at the environments in which electronically signed documents will reside, and begin to build properly secure, and audited, storage systems.

Documenting the entire system is not only good practice--it also serves as a map of evidence for the electronic document.

System documentation includes:

- description of entire system
    - function description
    - process flow description
    - hardware
    - software
        - Network Operating System
        - Operating System
        - dependencies
        - auxiliary
- description of maintenance procedures
        - backups
        - security test procedure
        - audit procedure

        - external cross reference audit procedure
- description of document format
        - standard
        - version control
        - control check
        - medium control
        - fail-safes

Procedure documentation accompanies system documentation. The documentation should be detailed to the point of outlining who would have access to systems and at what times:

- User
    - Identification and authorization control
    - Access control
- System
    - Documentation control
    - Use Access control
    - Medium Access Control
    - Hardware / Software acquisition and disposal
- External
    - Identification of external processes affecting system
    - Verification of integrity for those processes
    - Contact information

For system secure records, documentation volume necessary to show integrity and authenticity is undoubtedly larger. Access to and use of user names and passwords must be maintained in addition to the record. For example, systems using username and passwords for access to, and subsequently for signing, must show integrity not only in the record that is to be evidence, but also within the whole system. “Someone else used my password” or trend analysis of system abuse might highlight weaknesses in the integrity of the user having unique control over the electronic signature.

Such information should include:

- Audit logs
    - System Environment
    - User access
    - User management
    - User authorization modification (including password changes)
    - Document / Transaction as evidence
        - Creation
        - Modification
        - Deletion
        - other actions?
- Independent Audit
    - Procedural Check-up
    - Reliance of Administrator’s to system

- Check's and balances against superior permissions from altering lower permission transactions

The untested frontier of electronic documents: Time

Fast paced technology advances demand the discipline of technology refreshment be incorporated into today's system design. Both the system secure and the document secure approaches have drawbacks that are evidenced over time. With a little ingenuity, the drawbacks can be overcome. Both methods have the potential to maintain integrity and authenticity over the document life cycle, There are ways to mitigate the risks of time.

As time increases, the potential for security compromise increases. The longer a system is present in the universe, the more time is available for the system, procedures or encryption, to be compromised. If compromised, then assurance of electronic record integrity or authenticity is lost.

For system secure electronic records, maintaining the system perimeter is an ongoing challenge. The environment is ever changing; the risks are ever changing. From port buffer overflows to straight access control list compromise, the systems administrator understands the risks associated with securing the network. The question is, "How does this affect the electronically signed record?"

The risk is that any compromise can be devastating to ALL documents contained in the system. If a password file is compromised, then all active electronically signed records could be invalidated. This raises the stakes of network security. Systems designed for system secure electronic records should have procedures and processes in place to address compromise. Upon compromise detection, the electronically signed documents should be locked down immediately; policy should describe procedures for re-validating the existing record integrity.

Beyond security threats, there is an abundance of information necessary to maintain system secure electronically signed documents over the life cycle. Mixed medium environment design should be considered to minimize risks associated with time. Such environments create "write once only" media that store the electronically signed records for authenticity purposes. The write once mediums are handled in similar fashion to document management storage; this is similar to current day practice. This way the system secure electronic record may reside within the system. However when authenticity is challenged, the record can be compared to the hard medium copy.

Beyond the scope of this paper, but a rising issue over the past 25 years, is the consideration of long term storage and retrieval from write-once mediums (or any system/medium for that matter), and how that might affect validating records many years past creation.

For document secure records, the nature of technology and the limitations of encryption over the life cycle pose a problem of time. Compared to the average terms of document retention for government, document management systems also need to account for the decaying strength of encryption used on the document or system to access the document. For instance, a document secure document created four years ago with 24-bit keys can easily be broken. If the encryption can be compromised, then modification to the original content *could* take place and the document might be re-signed fraudulently. The document management system, or the document storage, must consider the potential for authenticity instability over time. A system not only should show the *actions*, but also re-apply technology to maintain the encryption level comparable to the risk of the document associated.

This reapplication of encryption technology is referred to as “enveloping the document”. The self-evidencing document then becomes envelope upon envelope containing the original document, where the application of the latest envelope needs to be a secure process ensuring the integrity of the previous envelope had not been altered.

Conclusion

E-sign and UETA present new challenges and risks to governments’ safekeeping of records. It is the obligation of the agency in which the information originates to ensure the integrity of the information contained and to maintain the link to the electronic signature used to create the document for later reliance. A document classification system and employee training on security risks will help ensure records kept are not compromised. Routine internal and external audit of security practices are essential for agency management to ensure systems are sound and documents are safeguarded. Agencies need to review their system designs to build evidence into the electronic record’s life cycle for reliance and ultimately reciprocity with other jurisdictions.

Other Resources:

The Financial Management Service of the US Department of the Treasury has issued (12/22/00) a final version of its Electronic Authentication Policy, for Federal payment, collection, and collateral transactions conducted over open networks such as the Internet. The policy is published in the Federal Register of January 3, 2001 (pages 394-397), and is also available at http://www.fms.treas.gov/eauth/index.html.

While this model applies basically financial transactions, there is some correlation between a financial transaction and an electronically signed record.