Framework for Electronic Signature Reciprocity

A White Paper Exposure Draft

NECCC
E-SIGN INTEROPERABILITY WORK GROUP
December, 2001

National Electronic Commerce Coordinating Council

The National Electronic Commerce Coordinating Council (**NECCC)** was established in 1997 to promote electronic government based on emerging issues and best practices through an alliance of national associations. The Alliance is comprised of the National Association of State Auditors, Comptrollers and Treasurers (**NASACT**), The National Association of Chief Information Officers (**NASCIO**), the National Association of State Procurement Officials (**NASPO**), the National Association of Secretaries of State (**NASS**). In addition, there are six non-voting affiliated members: the Information Technology Association of American (**ITAA**), the National Automated Clearing House Association (**NACHA**), the National Association of State Chief Administrators (**NASCA**), the National Governors Association (**NGA**). The National Association of Government Archive and Records Administrators (**NAGARA**), and the National Association of State Treasurers (**NAST**) became Council members in October 2001. The ITAA and NACHA specifically represent private information technology companies and the financial services and technology industries.

NECCC 2001 EXECUTIVE BOARD

Chair: **Carolyn Purcell**, NASCIO, CIO, State of Texas
Vice Chair: **Hon. J. Kenneth Blackwell**, NASS, Secretary of State, Ohio
Secretary/Treasurer: **Richard Thompson**, NASPO, Director, Maine Division of Purchases
Immediate Past Chair: **Hon. J. D. Williams,** NASACT, Idaho State Controller

NECCC 2001 BOARD

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

NECCC STAFF

Eveanna Barry • ebarry@nasact.org
Scott Etter • setter@nasact.org
web: www.ec3.org

For Interoperability Work Group members and contact information see: *An Introduction to the NECCC E-Sign Interoperability Work Group, Issues Relating to Interoperability and State Electronic Records and Signatures Reciprocity.*

Table of Contents

Introduction

There are many different signing processes[1] possible to form electronically signed electronic documents. The different signing processes provide varying levels of certainty and flexibility when identifying and attributing a signature to an individual and assuring the integrity of both the document and the signature. These variations suggest a need for defined levels of trust to establish the extent to which a state government or other entity can assume that an electronically signed electronic record (e-record) received from another state has authenticity, integrity, and reliability. Authenticity refers to the purported source or origin of an e-record.

A record has integrity if its contents have not been changed, deleted or otherwise altered. In addition, integrity addresses the accuracy and timeliness of the contents of a record. Reliability refers to the extent to which the signature is that of the person to whom it purports to be and the e-record represents his or her intent.

A state or other entity must understand trust in an objective way for effective electronic signature and e-record decision making and processing. This framework provides objective criteria for determining levels of trust in electronic signatures and e-records.

[1] The term "signing process" used in this document refers to a process where definable types of document or documents are routinely signed by a consistent, definable method. A signed electronic record is also known as a signed electronic document. The term "transaction" is used in the widest sense of an exchange or transfer event between two or more parties.

Defining Levels of Risk

Signatures are largely thought of as providing legal assurance of a signer's identity, of the significance or meaning of the signing and of whether or not a record has been altered. The three general factors used to determine the overall risk and the level of care applicable to the signing process are: risk of monetary loss, reputation risk, and productivity risk. The level of trust necessary for a state entity to accept an electronically signed e-record from another state is tied to the potential risk involved in the acceptance of the signed record.

The risk of monetary loss is determined using a variety of elements, including but not limited to:

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

The reputation risk to a government entity in the event of a breach or an improper transaction is determined by:

- Relationship with the other state and any 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 risk associated with a breach or improper transaction is determined using elements such as:

- Time criticality of transactions effected 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.

Assessing Risk

Assessing the combined risk factors (monetary loss, reputation risk, and productivity risk) determines the risk category of a type of record. The risk category indicates the level of trust necessary for a state government entity to accept a signed record from another state.

This framework defines four levels of trust in evaluating authenticity, reliability, and integrity of signed e-records. Each of these trust levels should be tied to the potential risk involved in and levels of security for a type of transaction. The trust levels defined are as follows:

- **Rudimentary** - This level provides the lowest degree of assurance concerning identity of the individual and reflects a situation where there is negligible risk. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to transactions in which the risk of malicious activity is considered to be low and which authentication of an individual's identity is not critical. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality.

- **Basic** - This level provides a basic level of assurance relevant to transactions where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.

- **Medium** - This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

- **High** - This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

The rudimentary trust level is not considered appropriate for interstate transactions largely because the identity of the signer or maker of the record cannot be strongly authenticated. This policy will identify appropriate implementations for basic, medium, and high trust levels as far as how the:

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

Signer Identification

Signer identification refers to the method by which an individual is identified and authorized to use a particular electronic signature method. Signer identification is independent of the signature or records creation technology being employed. However, it is critical to the level of trust that can be attributed to a signed record because the more robust or stringent the method of identification and authorization the more assurance that the signature has been authorized for use by the person who he or she purports to be. The identification and authentication methods for each level of trust are displayed in the table below.

Basic	• A government entity, its agent or an appropriate individual licensed by a government entity (e.g., notary) as being authorized to confirm identities has for the purposes of issuing or authorizing an electronic signature compared the identity of the individual with two pieces of identification (copies or originals). At least one of these must be a government issued identification containing a photograph (e.g., driver's license, non-driver identification, passport); or • A sponsoring government entity or its agent has compared trusted information in a data base with user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person); or • By attestation of a supervisor, or administrative or information security officer, or an individual certified or licensed by a government entity as being authorized to confirm identities (e.g., notary) who uses a stamp, seal or other mechanism to authenticate their identity confirmation

Medium	• A government entity, its agent or an appropriate individual certified or licensed by a government entity (e.g., notary) as being authorized to confirm identities has for the purposes of issuing or authorizing compared the identity of the individual with two pieces of identification (certified copies or originals). At least one of these must be government issued identification containing a photograph (e.g., driver's license, non-driver identification, passport); or • A sponsoring government entity or its agent has previously established the identity of an individual using a process that satisfies the above requirements and there have been no changes in the information presented.
High	• A government entity, its agent, or an appropriate individual certified or licensed by a government entity (e.g., notary) as being authorized to confirm identities, in the presence of the individual for the purposes of authorizing or issuing a signature, compares the identity of the individual with two pieces of identification (certified copies or originals). At least one of these must be government identification containing a photograph (e.g., driver's license, non-driver identification, passport).

Along with the above identification requirements, the originating government entity or its agent must keep a record of the type and details of identification used and on request make it available to the state entity receiving the signed record for that signed record to be accepted at the purported trust level.

Signer Linkage to Signature

Signer linkage to signature refers to the policy, process and procedures establishing a link between the signer and the information and method used to sign. This linkage has two dimensions.

- The first dimension is the way by which the unique signature characteristics are linked to the signer. This linkage can be achieved through one thing or by a combination of things only the individual:

- ***Knows*** (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key);

- ***Possesses*** (a token -- e.g., an ATM card or a smart card); or

- ***Is*** (a biometric -- e.g., characteristics such as a voice pattern, handwriting dynamics, retinal scan or a fingerprint).

- The second dimension is trust level. Trust level is closely related to the specific signing method (e.g., shared secrets, biometric, cryptographic keys).

The level of trust of an electronically signed record is in part a function of how convinced the receiving government is that the information used to sign has remained in the sole possession of the individual authorized to use it. In developing the levels of trust for this component of the policy it is assumed that there will be multiple ways to meet the requirements of each level and that multiple methods could theoretically meet the requirements of the same level.

The methods for linking signers to signing information or electronic signatures for each level of trust are displayed in the table below.

Basic	• Two shared secrets (e.g., pin, password) where a governmental body has assigned at least one secret and the signer has been provided with and has conformed to appropriate security standards as far as protecting the shared secrets. • A shared secret and a private cryptographic key or biometric information in which the cryptographic key cannot be accessed without the shared secret. “Private” in this sense means in the sole possession of the signer.

Medium	• Three shared secrets in which one has been assigned by a governmental body and one consists of private information that only the signer would know (e.g., income tax information), and the third could be selected by the signer. • A shared secret and a private cryptographic key or biometric stored in a secure software token on a secure computer.
High	• A shared secret and a cryptographic key or biometric stored on a hardware token where the key or biometric cannot be accessed without the shared secret and the shared secret is only known by the signed and the hardware token. • A biometric where the signer needs to be present to sign.

Along with the above identification requirements, the originating government entity or its agent must keep a record of the methods and approaches used to link a signer to signature information.

Signature Linkage to the Integrity of the Record

This element of trust has two components.

- An electronic signature must be linked to the record to which it is affixed or associated. E-signatures can be linked to an e-record in many different ways. The e-signature can become part of the record's data structure or imbedded as a data object within the document. The e-signature can also be stored in a different location but logically linked to the e-record. However, a government agency must manage the e-record and electronic signature as a unit and ensure that the link between them is maintained for the record's legal minimum retention period.
- There must be some method to ensure that the signature is linked to the record content that the signer intended to sign in such a manner that any change to the record since the record was signed is detectable and invalidates the signature.

This signature linkage to the integrity of the record can be achieved by the system that collectively manages the e-record and the associated signature. In such a case, trust is a function of the system's trustworthiness and its controls to ensure that a record or signature has not been tampered with or modified and the system's ability to detect that such has occurred. However, transferring agencies also need to use a transmission method to ensure that the integrity of the electronically signed record is not compromised. Linkage can also be created using technologies in which the signature and record exist as a unified object in which validation of the signature itself provides assurances that the record and signature have not been tampered with or modified. Technologies that use cryptography and hashing techniques can achieve this outcome.

The methods for linking an electronic signature to the integrity of the record for each level of trust are displayed in the table below.

Basic	• Self-certification that the system used to capture and manage the electronically signed record reasonably ensures, through complying with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link.[2] Transferring agencies

[2] NIST SP 800-14***Generally Accepted Principles and Practices for Securing Information Technology Systems*** will serve as a general guideline for generally accepted system security practices.

	have mutually agreed to a secure method for: transferring the electronically signed record, ascertaining the integrity of the record, and ascertaining the integrity of the signature and record link.
Medium	• An outside entity or auditor has certified that the system used to capture and manage the electronically signed record reasonably ensures, through compliance with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually agreed to: a secure method for transferring the electronically signed record, ascertaining the integrity of the record, and ascertaining the integrity of the signature and record link. • Self-certification that system used to capture and manage the electronically signed record reasonably ensures, through complying with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link Transferring agencies have mutually agreed to secure methods for ascertaining the integrity of the record and the integrity of the signature and record link. Transferring agencies use a secure network or secure cryptographic method (e.g., secure socket layer (SSL) or VPN to transfer the electronic signed record.
High	• An outside entity or auditor has certified that the system used to capture and manage electronically signed record reasonably ensures, through

	compliance with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually agreed to: a secure method for transferring the electronically signed record and secure methods for ascertaining the integrity of the record and the integrity of the signature and record link. Transferring agencies use a secure network or secure cryptographic methods (e.g., secure socket layer (SSL) or VPN to transfer the electronic signed record. • Self-certification that the system used to capture and manage the electronically signed record reasonably ensures, through complying with generally accepted principles and practices for securing information technology systems, the integrity of the record, and the integrity of the signature and record link. Transferring agencies have mutually agreed to a secure method for transferring the electronically signed record and to the use of a cryptographic method with hashing techniques to ensure record integrity and the link between the record and the signature (e.g., PKI)