Recommendations for Electronic Signature Infrastructure, Policy Management, and Governance in States

A White Paper

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, Delaware State Treasurer
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

Table of Contents

Introduction

Overview of a State's Electronic Signature Infrastructure

- Roles and Responsibilities within the ESI
- ESI Deployment Options
- Electronic Signature Policy Management Authority (ESPMA)
- ESPMA Membership

The Functions of Electronic Signature Policies

Conclusion

Introduction

While there must be collaboration and distribution of authority among participating parties in a State's Electronic Signature Infrastructure (ESI), a single enterprise-level (state-level) authority for the collection, distribution, and enforcement of all related electronic signature policies will increase the likelihood of efficient, and effective authentication, encryption, and awareness of the signing act's legal significance and transferability over time. As a first step, we recommend that a State acknowledge the party or parties responsible for the electronic signature infrastructure and establish an Electronic Signature Policy Management Authority (ESPMA) appropriately delegating management authority to the responsible party or parties.

Several technologies are available to electronically sign, strongly authenticate individuals, and protect the information confidentiality through encryption. Protections and other advantages afforded by these technologies are essential elements for state electronic government initiatives. States have many options for developing, implementing, and operating an electronic government infrastructure. However, states must maintain a degree of control and authority if the tools employed are to serve the needs of the state, its constituent agencies, local jurisdictions, business partners, and its citizens. The nature of this control and authority is defined by each state's ESPMA as it develops Electronic Signature Policies (ESPs); those policies, in turn, define the operation, rights, and obligations of all entities involved in state related electronic signature processes.

Using the "Framework for Electronic Signature Reciprocity," the ESPMA creates ESP's that give guidelines to ESI participants. ESP guidelines are used to appraise and assign value to transaction content. The requisite level of trust is identified in consideration of transaction value and further risk analysis. The ESI solution(s) selected protects transaction value, affords the acceptable / requisite level of trust and attenuates other risk analysis concerns. The ESPMA functions as the state's quality control agent for the electronic signature infrastructure.

This white paper provides an overview of the role of a state's ESPMA and how it can govern electronic signature initiatives. It provides guidance to states on how to configure the ESPMA and how this authority can insure states' electronic signature processes function in the interest of the state regardless of which technologies are implemented.

Overview of a State's Electronic Signature Infrastructure

A state's Electronic Signature Infrastructure (ESI) is an integrated system of policy, procedures, people and technology for the purposes of: (1) binding the identity of an individual to a signing process that indicates legal intent and (2) specifying a signing method that assures a signing party's signature uniqueness. And, in keeping with the ***Framework for Electronic Signature Reciprocity,*** an electronic signature, in addition to a method for binding an individual or custodial identity to a unique signature, requires: 1) assuring the binding integrity and verifiability and, 2) assuring the signed record integrity and accessibility.

Roles and Responsibilities within the ESI

One of the first policy decisions a state must make when developing an ESI (Electronic Signature Infrastructure) is to define the following various roles and responsibilities within the infrastructure and who will perform these roles:

Electronic Signature Policy Management Authority (ESPMA)[i] - The ESPMA is a body[ii] established to oversee the creation and update of Electronic Signature Policies, review contractual obligations of the parties involved in the ESI, review the results of any audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the ESI. For purposes of this document, it is assumed that the ESPMA for governance in states is the state-level authority responsible for the policies and standards for the Electronic Signature Infrastructure. Specific state statutes define where the authority for either decentralized or centralized management of its electronic signing processes lies. In some states the authority may function as part of an overall Information Technology Infrastructure, it may be associated with a state's Enterprise Security Office, or it may be housed within a particular agency, or with policy management in one agency and technology standards delegated to another agency. Regardless of a state's position on distributed deployment decisions, a state cannot relinquish control of the ESPMA to an outside party without threatening the integrity of the signing process.

ELECTRONIC SIGNATURE POLICY (ESP) – ESP's are set of rules that define the interrelated rights and obligations of parties in the ESI. The ESP indicates whether or not a particular unique signing method is suitable for a particular application or purpose. The ESP is the cornerstone of trust in the unique signing method and defines what degree of assurance can be placed in the unique signing method.

REGISTRATION AUTHORITY – A Registration Authority (RA) is the entity responsible for identification and authentication of prospective signers (subscribers).

SUBSCRIBER - A subscriber is an individual or business entity that has contracted / agreed to receive a unique signing method which, when used, is recognized as the subscriber's electronic signature.

SIGNING METHOD MANUFACTURER - A Signing Method Manufacturer (SMM) issues the unique signing method to a subscriber once they are appropriately identified and authenticated to be a qualified subscriber. An SMM for a particular ESI must conform with the ESI's ESP.

REPOSITORY – Any signing process requires a method to verify the validity of the unique signing method used by a subscriber over the legal life of the signed record, this verification is managed by the Repository. Repository is an entity / object where evidence establishing the link between signer and unique signing method is stored and is made accessible to Signer, Relying Party or others to confirm authenticity, integrity, non-repudiability, or to assure confidentiality.

RELYING PARTY - The Relying Party (RP) is a person or entity receiving information that includes the result of the unique signing method of a subscriber (their signature) which is verifiable using the method managed by the Repository.

ESI Deployment Options

States have a number of ESI deployment options. They can develop the ESI completely in-house and assume all RA, SMM, Repository and other roles; they can outsource all core functions (except for the role of Electronic Signature Policy Management Authority); they can combine both in-house and outsource options. It is beyond the scope of this white paper to provide direction in this regard.

States, regardless of the deployment option, must exercise control and direction over ESI operation. The type of deployment is less critical than: 1) control over policies that set rules for unique signing method issuance, and; 2) a clear delegation of authority to the state's ESPMA to establish and manage those policies. As previously stated, regardless of deployment, a state cannot relinquish control of the ESPMA.

An ESI may include a Public Key Infrastructure (PKI), though deployment of a PKI is not required for establishing a state's ESI. States implementing a PKI may establish a PKI Policy Management Authority (PKI PMA) to define the single point of view for PKI policy management which may include policies for electronic signatures (to be covered in more detail in "The Model PKI CP"). If a PKI PMA is in place or under development, parties involved in a PKI PMA may serve as a foundation for a state-level ESPMA or may negotiate with the ESPMA to demonstrate how two bodies with overlapping yet distinct responsibilities can effectively support each other.

Electronic Signature Policy Management Authority (ESPMA)

The ESPMA is the entity with final authority and responsibility for how an ESI operates.

The ESPMA drafts Electronic Signature Policies to fit the basic organizational business needs the ESI will serve. The various Electronic Signature Policies differ depending upon application design, participants involved, transactions engaged in, and the appropriate transaction signing processes for those organizational business needs.

The ESPMA must promulgate, monitor, and enforce compliance with policies affecting private entities, state agencies, and possibly local governments, public health organizations, and public education. ESI participants are particular to each state's electronic government mission. An ESPMA does not need separate statutory existence if its authority can be derived from its parent or host agency. An ESPMA parent or host agency must have statewide authority, conferred by statute or proximity to gubernatorial authority. Parent / host agencies must be willing and able to act as the ESPMA. It may be sensible to place the ESPMA in an agency with statewide policy development function, particularly if this policy function is related to electronic government, electronic signatures, or information technology.

ESPMA Membership

The structure of government may affect ESPA membership. Membership can be partially defined by the authority's statutory and regulatory environment. The ESPMA may be formed as a committee of various agencies or as a responsibility of one agency that consults with the other agencies when forming electronic signature policies. It is very important that the ESPMA collaborate with all stakeholders in the state government ESI. This can include agencies developing ESI-enabled applications, SMM approving / licensing agencies, RAs and Repositories, and agencies funding the ESI or overseeing ESI expenditures and project development.

The ideal is a membership structure that assures effective performance and addresses the range of issues critical to all participants in the ESI. In general, the state needs to recognize that its ESI deployment overlaps responsibilities for:

1. Information technology deployment and management,
2. business process re-engineering for (and management of) electronic government,
3. general management of electronic records over their legal and historic life, and
4. general management of electronic signatures over the legal and historic life of the signed record.

These responsibilities may reside in one agency or in several. It is important for the state to establish who is responsible for each of these areas and how they affect the state's ESI deployment.

The Functions of Electronic Signature Policies

Electronic Signature Policies set the roles and obligations of all ESI entities and oversee the technical standards and operations of all ESI functions. These rights and obligations for entities involved in the ESI are stated in the form of both contract obligations and technical requirements. As the controlling documents for the ESI, ESPs need to be developed by the ESPMA and should not be left to vendors who might be governed by the policy.

The ESPs should govern the approval of RAs, SMMs and Repositories to operate within the state's electronic signature infrastructure. ESPs must be monitored to ensure that they are serving the needs of the community and will need to be occasionally revised.

In addition, compliance with ESPs must also be monitored. The development and adoption of new policies, as well as monitoring for compliance, are the responsibility of the ESPMA.

As the governing body of the ESI, the ESPMA will have a relationship with each entity within the ESI. This relationship is either explicitly stated in the ESI's ESPs or implicit in the ESPMA governing roles.

As previously stated, the ESPMA's governing roles include overseeing and directing the electronic signature infrastructure's SMMs, RAs, and Repository(ies). The Authority establishes and approves responsibilities and the operational standards and procedures that determine when and how new SMMs, RAs and Repositories can become members of the ESI; the Authority serves as liaison with external organizations for any purpose related to the promotion and better operation of the ESI. The Authority establishes dispute resolution procedures, including clarification of dispute resolution jurisdictions, in the event of disputes between SMMs, RAs, Respositories and other parties within the ESI. The Authority ensures government-wide interoperability of the ESI and has a role in ESI services procurement by developing standards to select technologies which support appropriate levels of trust as defined by each participant's business rules including those for content management. It keeps the government informed of developments in electronic signature technologies, standards, and industry practices and promotes awareness of the roles of the various technologies in enabling secure service delivery, interoperability, public administration and communications. The ESPMA also ensures that appropriate records management and retention policies are in place to insure that long-term standards for archival needs are met so that signed and encrypted records are accessible for as long as they are needed.

An agency's role may be defined by an explicit, unique contract with the ESPMA or by statute or regulation. The agency needs defined contractual arrangements with other ESI participants.

Where ESI services are outsourced, an ESPMA function may be slightly different. In outsourced solutions, the ESPMA must retain responsibility to ensure ESP requirements are written into any contracts for ESI services (including the rights and authority of the ESPMA). The ESPs should insist that out-sourced service providers require Subscriber and Relying Party contracts include roles and obligations of ESI entities, consistent with the ESP. The ESPMA should reserve the right to review and approve all such contracts before they are used.

Conclusion

A state Electronic Signature Infrastructure includes several responsibilities that can be met by coordination and integration under a managing entity aegis. Integration and coordination of electronic signature policy can be accomplished effectively when a single entity is responsible. An Electronic Signature Policy Management Authority, with authority to implement state Electronic Signature Policies, can be an effective means for electronic signature program management.

[i] The Electronic Signature Policy Management Authority's evolving organizational model builds on these key steps:

? ? ? ? 1. Derive functions *from the operational requirements for ESI use. Certain actions must be done by devices and the people or business entities that run those devices for the technology to work. A list of* functions *or things that must be done for the technology to effectively work comprises the starting point for a business-legal framework for an ESI business application.*

? ? ? ? 2. Allocate functions to roles*. The functions that must be performed for an ESI application to work are assigned in an ESI Policy document to the classes of participants involved (parties). These classes or* roles *are named and their functions and qualifications described. This labeling and describing leads to defining role-terms such as "Signer" or "Registration Authority."*

? ? ? ? 3. Commit parties to the roles through binding obligations. *Each party interested in participating in an ESI application become actual participants by committing to contracts or otherwise becoming subject to the legally binding requirements that involve enforceable duties associated with one or more roles. These legally binding commitments are* obligations *that can be enforced judicially in case of a failure to perform according to the commitment.* Parties *are the persons who are thus committed.*

? ? ? ? 4. Resolve disputes if an obligation is breached*. There is a* liability *if a judicial or agreed alternative administrative tribunal has determined an unsatisfied obligation exists. Each signing process has an Electronic Signature Policy that defines the minimum obligations and judicial recourse. Each party will be responsible for assuring that any additional commitment needed is set down in contracts or otherwise becomes subject to legally binding requirements external to the Certificate Policy.*

There are sets of functions that can be logically and conveniently grouped and delegated. Most of these functions can be divided into several sets of functions with each set representing a *role.* Roles can be named according to the nature of the functions in each set. It is important to be clear that a particular *party* may perform one or more *roles* in the ESI. And evolving business models may change the way in which functions are logically grouped, which may make it necessary for the PMA and the parties to further evolve the naming of roles in the future.

[ii] An Electronic Signature Policy is generally not legally binding unless it is imposed by a party that has certain sovereign power such as through statutory enactment or regulatory adoption. While the parties can bind themselves to obligations by agreeing contractually to be subject to the Electronic Signature Policy, without some sovereign imposition there is little likelihood the variety of parties will agree on a common Electronic Signature Policy or ones "close enough" for cross-certification among them - each use of an ESP then becomes an island with little hope of bridging to other uses.