

Procedures

POLICY AUTHORITY PROCEDURES
For the Arizona Electronic Signature Infrastructure (AESI)

Draft Version 3.2
April 25, 2002

State of Arizona
Policy Authority
Office of the Secretary of State

TABLE OF CONTENTS

| | | |
|-----------|--|-----------|
| 1 | Purpose of the Policy Authority | 1 |
| 2 | The Policy Authority's Responsibilities | 1 |
| 2.1 | Form of the Policy Authority | 1 |
| 2.2 | Policy Authority Catalog of Electronic Signing Processes | 1 |
| 2.3 | Approving Certification Authorities..... | 3 |
| 2.4 | Defining Electronic Signing Policies | 3 |
| 3 | Elements Required in a Electronic Signing Policy..... | 4 |
| 3.1.1 | <i>Issuer Functions and Obligations</i> | <i>4</i> |
| 3.1.1.1 | Issuer-Subscriber Functions and Obligations | 4 |
| 3.1.1.2 | Issuer-Relying Party Functions and Obligations | 4 |
| 3.1.1.3 | Other Issuer-Related Roles | 4 |
| 3.1.1.3.1 | Registrar | 5 |
| 3.1.1.3.2 | Certificate Manufacturer | 5 |
| 3.1.1.3.3 | Other Roles Assisting Issuers..... | 5 |
| 3.1.2 | <i>Subscriber Functions and Obligations.....</i> | <i>5</i> |
| 3.1.3 | <i>Relying Party Functions and Obligations.....</i> | <i>5</i> |
| 3.1.4 | <i>Repository Functions and Obligations.....</i> | <i>6</i> |
| 3.1.4.1 | Repository-Subscriber Functions and Obligations | 6 |
| 3.1.4.1.1 | Privacy and Other Information Rights | 6 |
| 3.1.4.1.2 | Other Functions and Obligations | 6 |
| 3.1.4.2 | Repository-Relying Party Functions and Obligations | 6 |
| 3.1.4.3 | Repository-Issuer Functions and Obligations..... | 6 |
| 3.1.4.3.1 | Publication Functions and Obligations | 6 |
| 3.1.4.3.2 | Other Functions and Obligations | 6 |
| 4 | Drafting a Electronic Signing Policy..... | 7 |
| 4.1 | Overview..... | 7 |
| 4.2 | Identification | 7 |
| 4.3 | Community and Applicability | 7 |
| 4.4 | Contact Details..... | 7 |
| 4.5 | General Provisions | 8 |
| 4.5.1 | <i>Obligations.....</i> | <i>8</i> |
| 4.5.2 | <i>Liability.....</i> | <i>8</i> |
| 4.5.3 | <i>Financial responsibility</i> | <i>8</i> |
| 4.5.4 | <i>Interpretation and Enforcement.....</i> | <i>8</i> |
| 4.5.4.1 | Governing law | 8 |
| 4.5.4.2 | Severability, survival, merger, notice | 8 |
| 4.5.5 | <i>Dispute resolution procedures</i> | <i>9</i> |
| 4.5.6 | <i>Fees.....</i> | <i>9</i> |
| 4.5.7 | <i>Publication and Repository.....</i> | <i>10</i> |
| 4.5.8 | <i>Compliance audit.....</i> | <i>10</i> |
| 4.5.9 | <i>Confidentiality.....</i> | <i>10</i> |
| 4.5.10 | <i>Intellectual Property Rights</i> | <i>10</i> |
| 4.6 | Identification And Authentication..... | 10 |
| 4.6.1 | <i>Initial Registration</i> | <i>10</i> |
| 4.6.2 | <i>Types of names</i> | <i>11</i> |
| 4.6.3 | <i>Need for names to be meaningful.....</i> | <i>11</i> |
| 4.6.4 | <i>Method of proving possession of unique and private identifier</i> | <i>11</i> |
| 4.6.4.1 | Method to prove possession of PKI private key | 11 |
| 4.6.4.2 | Method to prove possession of non-PKI identifier..... | 11 |
| 4.6.5 | <i>Authentication of organization identity.....</i> | <i>12</i> |
| 4.6.6 | <i>Authentication of individual identity.....</i> | <i>12</i> |
| 4.6.7 | <i>Routine Rekey [Renewal].....</i> | <i>12</i> |

| | | |
|-----------|--|-----------|
| 4.6.8 | <i>Rekey after Revocation [Renewal after Revocation]</i> | 12 |
| 4.6.9 | <i>Revocation Request</i> | 12 |
| 4.7 | Operational Requirements | 12 |
| 4.7.1 | <i>Subscriber Application or Other Recognition of Legal Obligations of using Signing Process</i> | 12 |
| 4.7.1.1 | Certificate Application | 12 |
| 4.7.1.2 | Non-PKI Application | 12 |
| 4.7.1.3 | Non-PKI Recognition of Legal Obligations of using Signing Process..... | 13 |
| 4.7.2 | <i>Application approval</i> | 13 |
| 4.7.2.1 | PKI Certificate Issuance | 13 |
| 4.7.2.2 | Non-PKI approval and issuance | 13 |
| 4.7.3 | <i>Issuance Acceptance</i> | 13 |
| 4.7.3.1 | PKI Certificate Acceptance | 13 |
| 4.7.3.2 | Non-PKI Acceptance..... | 13 |
| 4.7.4 | <i>Subscriber Signing Approval Revocation</i> | 14 |
| 4.7.4.1 | PKI Certificate Revocation..... | 14 |
| 4.7.4.1.1 | Circumstances for revocation | 14 |
| 4.7.4.1.2 | Circumstances for suspension | 14 |
| 4.7.4.1.3 | CRL issuance frequency (if applicable) | 14 |
| 4.7.4.1.4 | CRL (or other revocation list) checking requirement..... | 14 |
| 4.7.4.1.5 | On-line revocation/status checking availability | 14 |
| 4.7.4.1.6 | On-line revocation checking requirements..... | 14 |
| 4.7.4.2 | Non-PKI signing approval Revocation | 15 |
| 4.7.4.2.1 | Circumstances for revocation..... | 15 |
| 4.7.4.2.2 | Circumstances for suspension | 15 |
| 4.7.4.2.3 | CRL issuance frequency (if applicable) | 15 |
| 4.7.4.2.4 | CRL checking requirement | 15 |
| 4.7.4.2.5 | On-line revocation/status checking availability (if applicable) | 16 |
| 4.7.4.2.6 | On-line revocation checking requirements (if applicable) | 16 |
| 4.7.5 | <i>Security Audit Procedures</i> | 16 |
| 5 | Records Archival | 16 |
| 5.1 | Signing Tools changeover..... | 16 |
| 5.1.1 | <i>PKI Key changeover</i> | 16 |
| 5.1.2 | <i>Non-PKI tools changeover</i> | 16 |
| 5.2 | Compromise and Disaster Recovery | 16 |
| 5.3 | CA Termination | 16 |
| 5.4 | PKI key pairs..... | 17 |
| 6 | Electronic Signing Policy Administration | 17 |
| 7 | Plans for PKI Cross-Certification | 17 |

1 Purpose of the Policy Authority

A.R.S. 41-132 defines an electronic signature used by or with state agencies, boards and commissions as having specific qualities:

1. shall be unique to the person using it,
2. shall be capable of reliable verification and
3. shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated.

A.R.S. 41-121 states that the Secretary of State shall “Accept, and approve for use, electronic and digital signatures that comply with section 41-132, for documents filed with and by all state agencies, boards and commissions. In consultation with the government information technology agency, the department of administration and the state treasurer, the secretary of state shall adopt rules pursuant to chapter 6 of this title establishing policies and procedures for the use of electronic and digital signatures by all state agencies, boards and commissions for documents filed with and by all state agencies, boards and commissions.”

The Administrative Rules for A.R.S. 41-132 define the role of the Policy Authority: “The office of the Secretary of State shall serve as the Policy Authority as defined within the CARAT Guidelines. These guidelines provide a prudent operational model that may be applied to new technologies as they are approved.”

2 The Policy Authority's Responsibilities

The procedures defined in this document shall govern the full range of electronic signature solutions that evolve within Arizona's Electronic Signature Infrastructure (AESI)¹.

2.1 Form of the Policy Authority

The Office of the Secretary of State serves as the Policy Authority (PA). The Secretary of State shall designate the person or persons with delegated responsibility to act for and as the Policy Authority.

2.2 Policy Authority Catalog of Electronic Signing Processes

It is recognized that there are many processes to form signatures and documents. There are also varying levels of certainty desired for identifying a person, attributing a signature to them and assuring the integrity of the signed document. The Policy Authority shall accept, and approve for use, policies and procedures for the use of electronic signatures by all state agencies, boards and commissions for documents filed with and by all state agencies, boards and commissions. The policies and procedures for a particular use of electronic

¹ taking liberties with IETF's conception of PKI (Public Key Infrastructure), AESI is Arizona's collections (note plural) of electronic signing mechanisms and the entities and tools that support and provide the means to validly use these mechanisms as signatures. The concept of “Certificate Policy” is also extended from describing a PKI policy document to being any policy document governing a specific electronic signing technology. Each technical signing process will have one or more “Certificate Policies” defining the framework for the use of that technology for electronic signatures by and with Arizona state agencies.

signatures will be defined within the following technology specific Electronic Signing Policies:

- 1) A PKI Certificate Policy² (alternatively known as a PKI Electronic Signing Policy) that defines the policies and procedures for use of a PKI based signing process where there is a Certification Authority responsible for authenticating a prospective signing party and issuing to them the digital certificate that uniquely and verifiably links the signer to the signing,
- 2) A PGP Certificate Policy (alternatively known as a PGP Electronic Signing Policy) that defines the policies and procedures for use of a signing process where there is a PKC³ signing process without a formal Certification Authority. There may be a party responsible for authenticating a prospective signing party and for issuing to the signing party that which uniquely and verifiably links the signer to the signing but without requiring a X509 Certificate (i.e. a PKI certificate) or similar method of a third party vouching for the signer's credentials in the manner used for PKI, or
- 3) A Signature Dynamics Electronic Signing Policy⁴ that defines the policies and procedures for use of a Signature Dynamic signing process. This signing process does not have a Certification Authority role within its framework but there may be a party responsible for authenticating a prospective signing party and there may be a party responsible for issuing or providing access to a Signature Dynamic Toolset to the signing party. The Signature Dynamic Toolset will provide a biometric-based electronic signatures use that will uniquely and verifiably link the signer to the signing, or
- 4) Other Electronic Signing Policies that define the policies, procedures and appropriate technologies for use within other specific signing processes. These signing processes will need:
 - a) some method of identifying the Signer,
 - b) some method of verifying the link between the Signer and the signature, and
 - c) some method to verify that what was signed has not been altered since the signing.These requirements lead to consideration of particular roles some party in the process will need to fulfill. For example:
 - a) While these signing processes will not have a PKI style Certification Authority, there is often an independent third party responsible for authenticating a prospective signing party and often an independent third party responsible for issuing to the signing party the materials and methods that will uniquely and

² The term Electronic Signing Policy is related to the term Certificate Policy which comes from the framework for public key cryptography known as PKI (Public Key Infrastructure). The term Electronic Signing Policy is used in a wider sense by the Policy Authority to mean the document establishing the formal framework for a particular signing process regardless of the underlying technology.

³ PKC – “public key cryptography” is the basis for various signing technologies with PKI and PGP being the two more commonly known technologies.

⁴ The concept of Electronic Signing Policy is extended from describing a PKI Certificate Policy to being any policy document governing an electronic signing technology. Each technical signing process will have one or more Electronic Signing Policies defining the framework for the use of that technology for electronic signatures by and with Arizona state agencies.

verifiably link the signer to the signing⁵ or at least provide access to the materials and methods.

- b) While these signing processes will not have a PKI style X509 Certificate there will usually be some publicly available record that links the Signer (Subscriber) of a signing tool to that particular signing tool. For simplicity, this may be described as a Certificate⁶.
- c) While these signing processes will not have a PKI style Repository (CRL/OCSP services), there will be some mechanism for verifying the “signature” made by the “signing tool” was done with a valid signing tool of the appropriate Subscriber².

Note that the term “signing process” used in this document refers to a process where a definable type of document or documents are routinely signed by a consistent, definable method. The Policy Authority may, at any time, determine that a particular definable signing method requires an Electronic Signing Policy to govern its use. The Policy Authority may, at any time, determine that a particular signing process does not satisfy A.R.S. 41-132 and any further use is at risk of being deemed unlawful. Further, that the Policy Authority has received a report justifying the use of a particular signing process does not, in itself, provide assurance as to the legality of any signature or document signed by that signing process, that assurance is established, in part, by the contractual framework established by the applicable Electronic Signing Policy (if any) and Agency contracts.

2.3 Approving Certification Authorities

The Policy Authority shall maintain a list of accepted Certification Authorities⁷ (CA) as prescribed in Arizona's Administrative Rules where a PKI Certification Authority is required for the signing process.

The PA shall also maintain lists of CAs that are approved to issue Certificates for each Electronic Signing Policy issued by the Policy Authority where a PKI style Certification Authority is required for the signing process.

2.4 Defining Electronic Signing Policies

A Electronic Signing Policy creates a specific Electronic Signature Infrastructure (ESI) within the global AESI setting.

The list of accepted CAs for an Electronic Signing Policy, if applicable, and the list of accepted BPU⁸s for the same Electronic Signing Policy and any parties the CAs or BPU

⁵ Note that for a given signing process there might not be an independent third party responsible for vouching for the signer's identity or authentication credentials but there will always need to be some mechanism for associating the “signature” to the “signing tool” and the “signing tool” to the Subscriber of that “signing tool.”

⁶ Certificate is a term originating in PKI but used here to mean the published information that links a Subscriber to their signing tool. X509 Certificate or PKI Certificate will be used whenever a PKC context is specifically intended.

⁷ The term Certification Authority comes from the framework for public key cryptography known as PKI (Public Key Infrastructure) (see the Policy Authority's Glossary for further information).

contractually bind to the Electronic Signing Policy or project comprise the ESI for the Electronic Signing Policy. Any other use is not approved by the PA and falls outside the terms of the Electronic Signing Policy and its assignment of responsibility and liability.

The Policy Authority shall endeavor to develop Electronic Signing Policies that meet a wide range of business needs, but each organization will need to ascertain which Electronic Signing Policy meets a particular set of business needs (a BPU). And the BPU parties will usually need to draft a contract to incorporate additional rights and obligations specific to that business process.

Several aspects of AESI are controlled by statute, administrative rule and Statewide IT standards. A Electronic Signing Policy is bound by those requirements and shall not circumvent them.

3 Elements Required in a Electronic Signing Policy

3.1.1 Issuer Functions and Obligations

The Issuer⁹ of

- a PKI certificate (generally known as a Certification Authority or CA) , or
- a PGP key pair, or
- issuer of other methods to uniquely identify the signer and link the signer to the signature

has certain functions and obligations relating to Subscribers and Relying Parties.

3.1.1.1 Issuer-Subscriber Functions and Obligations

The Electronic Signing Policy shall establish explicit functions, obligations and remedies between Issuer and Subscriber¹⁰.

3.1.1.2 Issuer-Relying Party Functions and Obligations

The Electronic Signing Policy shall establish explicit functions, obligations and remedies between Issuer and Relying Party¹¹.

3.1.1.3 Other Issuer-Related Roles

An Issuer's basic set of obligations can be divided up and reallocated by a Electronic Signing Policy or delegated by subcontract in many ways.

For PKI, by definition, an Issuer is the person listed in the certificate in the *issuer* field.

⁸ A signing process may be unique to a particular set of business needs for a particular Agency or sub-unit of an agency or political subdivision, but often a signing process will be appropriate for similar business needs in several Agencies and political subdivisions – the range of business processes that the signing process is appropriate for is called a Business Process Unit (a BPU).

⁹ The Issuer is the party that conveys (issues) the “signing tool” to the person who will use it to sign. The “signing tool” will vary depending on the signing process and technologies employed.

¹⁰ Subscriber is the one using the “signing tool” that will uniquely link them to the signature.

¹¹ Relying Party is the one wishing to 1) verify that the signature is that of the signer (Subscriber) and 2) that what has been signed hasn't been altered since being signed.

The Electronic Signing Policy shall establish what delegation is allowed between an Issuer and subcontractors (e.g. *Registrar* or *Certificate Manufacturer*) and what explicit functions, obligations and remedies exist between the Issuer and a Party performing those functions.

3.1.1.3.1 Registrar

It may be useful and prudent to have a Local Registration Authority (LRA) rather than having the Issuer develop its own extensive local presence. For example, an agency obtaining PKI certificates for its employees is usually in a good position to address the certification needs of its employees as prospective Subscribers and provide high-quality certificate information.

The Electronic Signing Policy shall establish whether a Local Registration Authority is allowed and the extent of any delegated functions, obligations and remedies between Issuer and LRA.

3.1.1.3.2 Certificate Manufacturer

A Certificate Manufacturer¹² (CMA) provides operational services for an Issuer. The exact obligations and functions of a Certificate Manufacturer depend on the contractual arrangements between Issuer and manufacturer.

The Electronic Signing Policy shall establish whether a Certificate Manufacturer is allowed and the extent of any delegated of functions, obligations and remedies between Issuer and the Certificate Manufacturer.

3.1.1.3.3 Other Roles Assisting Issuers

The Electronic Signing Policy shall establish whether the Issuer may subcontract other roles and the extent of any delegated of functions, obligations and remedies between Issuer and the other roles.

3.1.2 Subscriber Functions and Obligations

The Subscriber owes duties mainly to the Issuer and to Relying Parties. The Electronic Signing Policy shall establish the Subscriber's functions, obligations toward other parties and any remedies available against Subscriber.

3.1.3 Relying Party Functions and Obligations

Relying Parties owe duties mainly to the Issuer and to Subscribers. The Electronic Signing Policy shall establish the Relying Party's functions, obligations toward other parties and any remedies available against Relying Party.

¹² A Certificate Manufacturer (another PKI based term) is the one that actually creates the "signing tool" that is delivered to the Subscriber or the Subscriber is provided access to for signing purposes.

3.1.4 Repository Functions and Obligations

3.1.4.1 Repository-Subscriber Functions and Obligations

3.1.4.1.1 Privacy and Other Information Rights

Any user of any signing process will need to keep in mind that they are signing electronic government documents which will need to be accessible and verifiable over the legal life of the signed document.

Subscribers are the persons about whom information is published in a Repository¹³ that will allow Relying Parties to verify the integrity of the signed document and that the Subscriber is linked to the “signing tool” (for PKI, this is generally available as an online information resource). If implementing contracts, the Electronic Signing Policy, or any applicable statutes or regulations provide for the Subscriber having rights of 1) privacy, 2) confidentiality, and/or 3) information accuracy, then the Certification Authority and the Repository will have an obligation to safeguard those rights.

The Electronic Signing Policy shall recognize the right to any lawful access to Subscriber information.

3.1.4.1.2 Other Functions and Obligations

The Electronic Signing Policy shall establish explicit functions, obligations and remedies between Repository and Subscriber.

3.1.4.2 Repository-Relying Party Functions and Obligations

The Electronic Signing Policy shall establish explicit functions, obligations and remedies between Repository and Relying Party.

3.1.4.3 Repository-Issuer Functions and Obligations

3.1.4.3.1 Publication Functions and Obligations

The Electronic Signing Policy shall establish minimum publication functions, obligations and remedies between Repository and Issuer.

The Repository and the Issuer will agree on the terms and conditions governing publication by the Issuer of information (such as certificates and notices of revocation) into the Repository. As a minimum, this agreement shall meet the requirements established in the Electronic Signing Policy. A Repository is obligated to perform according to that agreement.

3.1.4.3.2 Other Functions and Obligations

The Electronic Signing Policy may establish other explicit functions, obligations and remedies between Repository and Issuer.

¹³ A Repository is the location of current and historic evidence associating the Subscriber to the “signing tool.”

4 Drafting a Electronic Signing Policy

4.1 Overview

An Electronic Signing Policy creates a particular Electronic Signature Infrastructure (ESI). An Electronic Signing Policy shall contain an Overview with the “requirements” specified for the utilization of that ESI for the particular type(s) of transactions in which End Entities will participate. It is helpful for the Overview to provide a summary level description of the type of transactional relationship that the Electronic Signing Policy supports and the identity of the parties that will participate in the transaction. Such an overview can help facilitate the establishment of the contractual arrangements between AESI Service Providers, the Policy Authority and End Entities.

4.2 Identification

An Electronic Signing Policy shall be referenced by an object identifier ("OID") assigned to the policy in the United States by the American National Standards Institute ("ANSI").

The general format is:

This Policy is registered with the Arizona Secretary of State and has been assigned an object identifier ("OID") of _____.

4.3 Community and Applicability

The community and applicability section should state the roles to be played by parties in the ESI system; the legal names of the parties operating under the Electronic Signing Policy, or a means by which legal names can be ascertained; and the specific transactions governed by the Electronic Signing Policy.

For a PKI community, the Policy Authority will maintain a list for each Certificate Policy (Electronic Signing Policy) of the Certification Authorities approved to issue Certificates meeting that Certificate Policy.

The Policy Authority may maintain a list for each Electronic Signing Policy of the Business Processes (pilots and other agency projects and applications) that have been accepted to use “signing tools” approved for that Electronic Signing Policy.

4.4 Contact Details

The Contact Detail section should identify the Policy Authority, its scope of authority, and the contact person for the Policy Authority for purposes of communications related to the Policy.

4.5 General Provisions

4.5.1 Obligations

A Electronic Signing Policy shall describe the obligations of each ESI Service Provider and End Entity¹⁴ to each of the other parties that are subject to the Electronic Signing Policy.

4.5.2 Liability

An Electronic Signing Policy shall describe any limits or requirements governing liability of parties based upon breach of contractual obligations by one or more parties to other parties.

4.5.3 Financial responsibility

An Electronic Signing Policy shall describe what a ESI Service Provider is required to produce as evidence of financial responsibility or indications of creditworthiness that help to assure that a ESI Service Provider is able to satisfy its liabilities within the Electronic Signing Policy.

4.5.4 Interpretation and Enforcement

An Electronic Signing Policy should describe all legal documents contemplated in addition to the Electronic Signing Policy and should indicate the order of precedence of those documents.

4.5.4.1 Governing law

An Electronic Signing Policy shall state the governing law under which the Electronic Signing Policy will be interpreted. An Electronic Signing Policy should also indicate whether implementing contracts and other relevant agreements may state governing law other than that stated for the Electronic Signing Policy itself.

Since the Internet has no international borders, it may be pertinent to include provisions of law for international disputes, and/or disclaimers disavowing any intent to provide services to parties outside the US.

4.5.4.2 Severability, survival, merger, notice

An Electronic Signing Policy may contain contract provisions such as severability, survival, merger, and notice.

If an Electronic Signing Policy contains contract provisions, the Electronic Signing Policy should state the order of precedence of the Electronic Signing Policy contract provisions and provisions of other contracts, such as implementing contracts. (It may not be possible in all situations to override the provisions of preexisting contracts with the provisions of the Electronic Signing Policy.)

¹⁴ An End Entity may be a Subscriber, a Relying Party or both.

Survival: Refers to the continuation of rights, duties and obligations specific to the successors and assigns of parties associated with the Certificate or other signing tools issued.

Notice: Many legal obligations arise or are discharged as a result of notice or lack of notice of an event. A means of giving notification to all parties should be stipulated in the Electronic Signing Policy. Each Electronic Signing Policy will consider the following issues regarding notice and define notice requirements appropriate for the given business model:

- a) *Physical Notice* involves written notice that is delivered by hand or by certified or registered mail.
- b) *Non-secure Virtual Notice* involves electronic methods of delivery such as fax and unsigned e-mail. If they are used then the Electronic Signing Policy will need to describe appropriate uses of each type of delivery to provide notice.
- c) *Secure Virtual Notice* involves secure electronic methods, such as digitally signed messages. This should be the primary means of providing notification to all parties. An Electronic Signing Policy may require parties to register an e-mail address which would be considered a secure and reliable place to send and receive notification from all related parties.
- d) *Notice Obligations* occur when parties are responsible for providing notification of (1) changes to the party's registered e-mail and postal address; (2) security compromises affecting the secrecy of the Subscriber's PKI Private Key or other issued signing tool. Other types of notice events may be specified within a Electronic Signing Policy.
- e) *Acknowledgment* completes the communication of notification. A notice only gains the assurance of receipt when the sending party receives a secured electronic acknowledgment.

Merger and integration. Such an Electronic Signing Policy section should state that implementing contracts must include provisions that incorporate the Electronic Signing Policy and any other relevant documents and that specify the order of precedence of the documents.

The Electronic Signing Policy may provide that contracts shall include provisions requiring the contract to be governed by the Electronic Signing Policy.

4.5.5 *Dispute resolution procedures*

Dispute resolution procedures shall be addressed in the Electronic Signing Policy and shall include mechanisms for resolving disputes short of litigation.

4.5.6 *Fees*

An Electronic Signing Policy shall specify whether ESI Service Providers are authorized to charge fees and any limitations or caps on fees.

4.5.7 *Publication and Repository*

An Electronic Signing Policy should state what information must be published by ESI Service Providers.

4.5.8 *Compliance audit*

The Electronic Signing Policy shall include adequate and enforceable methods to assure compliance by each party required to submit to an audit. These methods shall meet and extend the provisions of Statute, Administrative Rules, and any general provisions defined by the Policy Authority.

For PKI Certificate Policies, the SAS70 audit process has been replaced with the CA WebTrust audit process and will be required within a PKI Certificate Policy.

The Common Criteria audit process (known as CS2) is recognized as being at least the equivalent of the SAS70 audit process and may be required within an Electronic Signing Policy where the business practices are consistent with the measures used in a CS2 audit.

4.5.9 *Confidentiality*

A Electronic Signing Policy shall provide that the information in PKI and PGP certificates is not confidential.

An Electronic Signing Policy shall provide that other personally identifiable information not in a certificate should be considered confidential, unless otherwise provided in the Electronic Signing Policy. Notices of any kind, including certificate or signing tool revocation, should not be considered confidential with respect to parties to whom such notice is due under the Electronic Signing Policy.

4.5.10 *Intellectual Property Rights*

An Electronic Signing Policy shall specify intellectual property requirements as well as limits on the use of intellectual property related to the Electronic Signing Policy and materials governed by the Electronic Signing Policy.

A statement of no stipulation is allowed, after due consideration of:

- The Electronic Signing Policy should limit the assertion of intellectual property rights on information that must be available in accordance with other sections of the Electronic Signing Policy.
- In addition, any requirements related to intellectual property that must be included in implementing contracts or other agreements may be specified.

4.6 *Identification And Authentication*

4.6.1 *Initial Registration*

An Electronic Signing Policy will generally require Subscriber applicants to sign a Subscriber Agreement during the application process and before a certificate or

equivalent is issued. An Electronic Signing Policy should specify the means by which communications between Subscribers and Issuers/Registrars or other Service Providers are conducted.

1. Subscriber Agreement: Since these Procedures and the AESI generally are intended for use with closed ESI systems, participation should be limited to defined Subscribers who have signed a Subscriber agreement.
2. Application Process: The Electronic Signing Policy shall define whether an applicant is to complete an application and sign a Subscriber agreement before the application is submitted for approval or if the applicant can first complete an application and then, if approved, sign a Subscriber Agreement. Where the Applicant is to be a Relying Party, the Subscriber may sign a Relying Party agreement simultaneously with the Subscriber agreement.
3. Communication: The Electronic Signing Policy shall state how an application is communicated from the Subscriber applicant to the Issuer/Registrar or other ESI Service Provider. Possible methods include electronically via e-mail or a web site, (provided that all communication is secure such as by using a suitable cryptographic protocol for electronic communications), by first class U.S. mail, or in-person.

4.6.2 Types of names

A PKI Certificate Policy (PKI Electronic Signing Policy) shall require that Issuers/Registrars express all names specified in a certificate as X.509 Distinguished Names. Any other information that may be required will be based upon the needs of the particular application.

4.6.3 Need for names to be meaningful

The general policy of the Policy Authority is that names must be meaningful and unique. Therefore, an Electronic Signing Policy shall require names to be meaningful and unique.

4.6.4 Method of proving possession of unique and private identifier

4.6.4.1 Method to prove possession of PKI private key

A PKI Certificate Policy (PKI Electronic Signing Policy) shall provide that an Issuer/Registrar must confirm that the Subscriber applicant is in possession of the private key corresponding to the public key specified in the application; that such private key is capable of creating a digital signature verifiable by the public key and an algorithm listed in the certificate; that the private key has not knowingly been compromised since its creation; that the public key is not shown in another certificate listed within a defined domain; and that there are no reasonable grounds to suspect that the Applicant/Subscriber's private key was obtained through theft, deceit, eavesdropping, or other unlawful means.

4.6.4.2 Method to prove possession of non-PKI identifier

Such criteria proving possession will be defined by the Policy Authority at such time as a non-PKI technology is approved for electronic signature use. An

Electronic Signing Policy for such an application shall require proof consistent with the criteria defined by the Policy Authority for that technology.

4.6.5 *Authentication of organization identity*

These policies are intended for personal identity uses only. Any organization or device identity certificates must be legally binding on a natural person.

4.6.6 *Authentication of individual identity*

An Electronic Signing Policy for any signing process that requires periodic renewal (e.g. PKI) shall define how the identity and any other assertions of a New or Renewing Subscriber are to be confirmed, including whether in-person or through the use of other techniques and the reliability required of those techniques.

4.6.7 *Routine Rekey [Renewal]*

An Electronic Signing Policy for any signing process that requires periodic renewal (e.g. PKI) shall specify the requirements that a Subscriber must meet in order to obtain renewal of his or her certificate, provided that the original certificate has not been revoked.

4.6.8 *Rekey after Revocation [Renewal after Revocation]*

An Electronic Signing Policy for any signing process that requires periodic renewal (e.g. PKI) shall not permit renewal of a certificate that has been revoked or that has expired.

4.6.9 *Revocation Request*

An Electronic Signing Policy for any signing process that can be revoked (e.g. PKI, PGP, and passphrase) shall identify the means of requesting a revocation and the criteria for accepting and acting on the request.

4.7 *Operational Requirements*

4.7.1 *Subscriber Application or Other Recognition of Legal Obligations of using Signing Process*

4.7.1.1 *Certificate Application*

A PKI Certificate Policy shall define the minimum content to be used for a certificate application. The PKI Certificate Policy should also specify that all applications are subject to review, approval, and acceptance by the Policy Authority in addition to the Issuer.

4.7.1.2 *Non-PKI Application*

An Electronic Signing Policy shall define the minimum information to be used for a Subscriber application. The Electronic Signing Policy should also specify that all applications are subject to review, approval, and acceptance by the Policy Authority in addition to the Issuer.

4.7.1.3 Non-PKI Recognition of Legal Obligations of using Signing Process

Some signing processes do not require that the Signer be issued the signing tools, they might merely need access to an approved signing tool (e.g. Signature Dynamics). Such signing processes will still require some method of the Signer acknowledging that their use of the signing tool has the same force and effect as a signature by pen on paper. The Policy Authority will define an appropriate procedure for the specific signing process – this may require a range of options in the Electronic Signing Policy with very clear guidance on the options may be deployed.

4.7.2 Application approval

4.7.2.1 PKI Certificate Issuance

A PKI Certificate Policy shall allow the issuance of a requested certificate only after the Subscriber identification and confirmation process is completed. The PKI Certificate Policy shall also require that the Subscriber be notified of the issuance of the certificate and specify the process by which the certificate is delivered or otherwise made available to the Subscriber.

4.7.2.2 Non-PKI approval and issuance

An Electronic Signing Policy for a signing process that requires the Signer be issued signing tools shall allow the issuance of requested signing tools only after the Subscriber identification and confirmation process is completed. The Electronic Signing Policy shall also require that the Subscriber be notified of the issuance of the signing tools and specify the process by which the tools are to be delivered or otherwise made available to the Subscriber.

4.7.3 Issuance Acceptance

4.7.3.1 PKI Certificate Acceptance

A PKI Certificate Policy should require an Issuer to specify how the Subscriber accepts or rejects the certificate. The PKI Certificate Policy may place limitations on the Issuer's choices. The PKI Certificate Policy shall require the Subscriber to acknowledge that by accepting the certificate the Subscriber agrees to the terms and conditions contained in the PKI Certificate Policy relating to that certificate.

4.7.3.2 Non-PKI Acceptance

An Electronic Signing Policy for a signing process that requires the Signer be issued signing tools should require an Issuer to specify how the Subscriber accepts or rejects the signing tools. The Electronic Signing Policy may place limitations on the Issuer's choices. The Electronic Signing Policy shall require the Subscriber to acknowledge that by accepting the signing tools the Subscriber agrees to the terms and conditions contained in the Electronic Signing Policy relating to the use of those tools.

4.7.4 *Subscriber Signing Approval Revocation*

4.7.4.1 *PKI Certificate Revocation*

4.7.4.1.1 *Circumstances for revocation*

A PKI Certificate Policy shall specify the circumstances under which a certificate should be revoked. A PKI Certificate Policy shall provide for

- permissive revocation upon request of the Subscriber and
- required revocation when it is reasonably determined that a certificate is unreliable.

4.7.4.1.2 *Circumstances for suspension*

PKI Certificate suspension is not allowed. In general suspension is not allowed but the Policy Authority may find the need for exceptions to this as signing processes evolve.

4.7.4.1.3 *CRL issuance frequency (if applicable)*

A PKI Certificate Policy shall require the Issuer to provide, promptly following revocation, notice to potential Relying Parties and any other parties specified in the PKI Certificate Policy of the fact of revocation. A PKI Certificate Policy shall require prompt updating of the certificate revocation list, if one is used, or of the certificate status database, as applicable, and should require all revocation requests received by the Issuer and the resulting actions taken by the Issuer to be archived. A PKI Certificate Policy shall specify the manner and the period in which the certificate revocation list or certificate status database should be updated following revocation.

4.7.4.1.4 *CRL (or other revocation list) checking requirement*

If a certificate revocation list is used, a PKI Certificate Policy shall specify when a Relying Party should check a certificate revocation list in order to establish that the Relying Party's reliance upon a certificate was reasonable.

4.7.4.1.5 *On-line revocation/status checking availability*

A PKI Certificate Policy shall require the Issuer to provide, promptly following revocation, notice to potential Relying Parties and any other parties specified in the PKI Certificate Policy of the fact of revocation. A PKI Certificate Policy shall require prompt updating of the certificate status database, if one is used, and should require all revocation requests received by the Issuer and the resulting actions taken by the Issuer to be archived. A PKI Certificate Policy shall specify the manner and the period in which the certificate status database should be updated following revocation.

4.7.4.1.6 *On-line revocation checking requirements*

If an on-line certificate status database is used, a PKI Certificate Policy shall specify that the frequency with which a Relying Party must check the database in

order to establish that the Relying Party's reliance upon a certificate was reasonable.

4.7.4.2 Non-PKI signing approval Revocation

4.7.4.2.1 Circumstances for revocation

An Electronic Signing Policy for a signing process that requires the Signer be issued signing tools (e.g. password) shall specify the circumstances under which signing approval should be revoked and how that is enforced. An Electronic Signing Policy shall provide for

- permissive revocation upon request of the Subscriber and
- required revocation when it is reasonably determined that a signing tool is unreliable.

Revocation is typically thought to be unique to PKI but any signing process that relies on a "secret" or the sole possession of something is open to compromise if the "secret" or the possession is not limited to the Subscriber. For example, any signing process that relies on a password in the process is subject to compromise if the password is compromised. Any revocation process will need to incorporate information about the revocation in a form and manner appropriate to the signing process so Relying Parties have a reasonable opportunity to judge the validity of a particular signature.

4.7.4.2.2 Circumstances for suspension

In general suspension is not allowed but the Policy Authority may find the need for exceptions to this as signing processes evolve.

4.7.4.2.3 CRL issuance frequency (if applicable)

A Electronic Signing Policy for a signing process that requires the Signer be issued signing tools (e.g. password) shall require the Issuer to provide, promptly following revocation, notice to potential Relying Parties and any other parties specified in the Electronic Signing Policy of the fact of revocation. An Electronic Signing Policy shall require prompt updating of any applicable revocation list or of any applicable approved signer status database and should require all revocation requests received by the Issuer and the resulting actions taken by the Issuer to be archived. An Electronic Signing Policy shall specify the manner and the period in which the revocation list or status database should be updated following revocation.

4.7.4.2.4 CRL checking requirement

If a revocation list is used, an Electronic Signing Policy shall specify whether and when a Relying Party should check a revocation list in order to establish that the Relying Party's reliance upon a certificate was reasonable.

4.7.4.2.5 On-line revocation/status checking availability (if applicable)

An Electronic Signing Policy shall require the Issuer to provide, promptly following revocation, notice to potential Relying Parties and any other parties specified in the Electronic Signing Policy of the fact of revocation. An Electronic Signing Policy shall require prompt updating of the status database, if one is used, and should require all revocation requests received by the Issuer and the resulting actions taken by the Issuer to be archived. An Electronic Signing Policy shall specify the manner and the period in which the status database should be updated following revocation.

4.7.4.2.6 On-line revocation checking requirements (if applicable)

If an on-line status database is used, an Electronic Signing Policy shall specify that the frequency with which a Relying Party must check the database in order to establish that the Relying Party's reliance upon a certificate was reasonable.

4.7.5 Security Audit Procedures

An Electronic Signing Policy shall assure that each party undertaking important obligations shall agree to maintain adequate electronic records that pertain to such obligations. Policies shall assure that sufficient records are kept to allow parties to access relevant and necessary information and to assist in carrying out the dispute resolution policies specified or permitted under the policy and as agreed upon by the parties. Record-keeping requirements should be tailored to meet no more than the actual needs for recordation based on the circumstances surrounding the business environment that the policy exists to facilitate.

5 Records Archival

5.1 Signing Tools changeover

5.1.1 PKI Key changeover

A PKI Certificate Policy shall define the minimum procedures, including process for secure new key distribution, associated with the change of a key pair used by Issuers to sign certificates.

5.1.2 Non-PKI tools changeover

An Electronic Signing Policy for a signing process that requires the Signer be issued signing tools (e.g. password) shall define the minimum procedures, including process for secure new tools distribution, associated with the change of a signing tool used by Issuers.

5.2 Compromise and Disaster Recovery

An Electronic Signing Policy shall require that ESI Service Providers have an appropriate disaster recovery/business resumption plan in place.

5.3 CA Termination

An ESI Service Provider should promptly notify all parties operating under the Electronic Signing Policy should it cease operation. An Electronic Signing Policy shall specify an

ESI Service Provider's obligations as operations are ceasing. An Electronic Signing Policy shall require that all PKI certificates and/or signing tools issued by the Issuer that reference the Electronic Signing Policy are revoked at the time of the termination (if not before).

5.4 PKI key pairs

PKI is used for several purposes but primarily these uses fall into 3 categories:

1. To identify and authenticate someone
2. To encrypt a message
3. To sign a document

Best practices for the PKI process of encrypting a message requires a “back door” way of unencrypting in case the private key is lost. Best practices for signing require that the private key not be recoverable or circumvented in anyway since the signer could otherwise repudiate the signing by claiming someone else used the alternative method to sign. Therefore any use of PKI for signing will not be done with any PKI tool designed to allow for encryption.

6 Electronic Signing Policy Administration

An Electronic Signing Policy shall define the process by which its policy is promulgated, amended and terminated. It should also address and provide for any additional relevant functions of the Policy Authority with respect to specification of the Electronic Signing Policy.

7 Plans for PKI Cross-Certification

While the Policy Authority expects PKI cross-certification to become a reality, the current state of the art prohibits any firm plans beyond assuring a common set of core extensions within all Certificates issued within AESI.

The long term expectation is that something like the method being explored by the U.S. ACES project will become feasible. Certain "hooks" will be implemented in AESI PKI projects to allow later cross-certification should it become possible and desirable.