

**PGP DIGITAL SIGNATURE
CERTIFICATE POLICY
for electronic signature use**

version as of August 24, 2001
the current version may be found at
<http://www.sos.state.az.us/pa/default.htm>

**State of Arizona
Policy Authority
Office of the Secretary of State**

**ARIZONA ELECTRONIC SIGNATURE INFRASTRUCTURE (AESI)
Pretty Good Privacy (PGP)
VERSION 1.00
September 2001**

TABLE OF CONTENTS

1	Introduction.....	1
2	Policy Specification.....	1
2.1	Overview.....	1
2.2	Policy overview	2
2.3	Identification alphanumeric OID.....	4
2.4	Community and applicability	4
2.4.1	Description of PGP infrastructure	5
2.4.2	Registration Authorities and Certificate Manufacturing Authorities	5
2.4.3	Local Registration Authorities (LRAs)	5
2.4.4	Certificate Repositories	6
2.4.5	Signers	6
2.4.6	Relying parties	6
2.4.7	Policy applicability	6
2.4.8	Approved and prohibited applications	6
2.4.8.1	Approved Applications	13
2.4.8.2	Prohibited Applications	13
2.4.9	Contact details	13
2.4.9.1	Policy Authority contact person:	13
2.4.9.2	Contact person determining CPS suitability for this Policy:.....	13
3	General Provisions	14
3.1	Obligations.....	14
3.1.1	Certificate creation and management obligations	14
3.1.1.1	Representations By Certificate Manufacturer	14
3.1.1.2	Time between certificate request and issuance	14
3.1.2	Registration Authorities (RA) and Certificate Manufacturing Authorities (CMA) Obligations	15
3.1.3	LRA obligations (LRA duties)	15
3.1.4	Signer Obligations	15
3.1.5	Relying Party Obligations.....	15
3.1.6	Policy Authority Obligations	15
3.2	Requirements	16
3.3	Disclaimers of warranties and obligations.....	16
3.4	Liability.....	16
3.5	Interpretation & Enforcement	16
3.5.1	Governing Law	16
3.5.2	Severability, survival, merger, notice	16
3.5.3	Dispute Resolution Procedures	17
3.6	Fees.....	17
3.7	Publication & Repositories	17
3.7.1	Publication Of CA Information.....	17
3.7.2	Frequency of Publication.....	17
3.7.3	Access Controls	17
3.8	Compliance Audit.....	17
3.9	Intellectual property rights.....	18
4	Identification And Authentication	18
4.1	Initial Registration	18
4.1.1	Types of Names	18

Draft

4.1.2	Name Meanings	18
4.1.3	Rules For Interpreting Various Name Forms	18
4.1.4	Name Uniqueness	18
4.1.5	Verification of Key Pair.....	19
4.1.6	Authentication of Organization	19
4.1.7	Authentication of Individual -- No Affiliation	19
4.1.7.1	Identification.....	19
4.1.7.2	Investigation And Confirmation.....	19
4.1.7.3	Personal Presence	19
4.1.8	Authentication of Individual – Affiliated Certificate	20
4.1.8.1	Identification.....	20
4.1.8.2	Authentication Confirmation Procedure.....	20
4.1.8.3	Personal Presence	20
4.1.8.4	Duties of Responsible Individuals	20
4.1.9	Authentication of devices or applications	20
4.2	Renewal Applications (Routine Rekey)	21
4.3	Rekey After Revocation	21
4.4	Satisfactory Evidence of Identity.....	21
5	Operational Requirements.....	21
5.1	Certificate Application.....	21
5.1.1	Application for a cross-certificate	21
5.2	Certificate Issuance.....	22
5.3	Certificate Acceptance	22
5.4	Certificate Revocation	22
5.4.1	Circumstances For Revocation.....	22
5.4.1.1	Permissive Revocation	22
5.4.1.2	Required Revocation.....	22
5.4.2	Procedure For Revocation Request	23
5.4.2.1	Repository/CRL Update	23
5.4.3	Revocation Request Grace Period	23
5.4.4	Certificate Suspension	24
5.4.5	CRL Issuance Frequency.....	24
5.4.6	CRL checking requirements	24
5.4.7	On-Line Revocation/Status Checking Availability	24
5.4.8	Special requirements rekey compromise	24
5.5	Computer Security Audit Procedures	24
5.6	Records Archival.....	24
5.6.1	Types Of Records Archived	24
5.6.2	Retention Period For Archive	25
5.6.3	Protection Of Archive	25
5.6.4	Archive Backup Procedures	25
5.6.5	Archive Collection System (Internal Or External)	25
5.6.6	Procedures To Obtain And Verify Archive Information.....	25
5.7	Key Changover	25
5.8	Compromise And Disaster Recovery	25
5.8.1	Disaster Recovery Plan.....	25
5.8.2	CR Key Compromise Plan.....	26
5.9	CR Termination	26
6	Physical, Procedural And Personnel Security.....	26
6.1	Physical Controls	26

Draft

6.1.1	Physical Security -- Access Controls.....	26
6.2	Procedural Controls	26
6.2.1	CM Trusted Roles.....	26
6.2.2	CR Trusted Roles.....	26
6.2.3	Multiple Roles (Number Of Persons Required Per Task)	27
6.3	Personal Security Controls	27
6.3.1	Background And Qualifications	27
6.3.2	CR Background Investigation.....	27
6.3.3	CM Background Investigation.....	27
6.3.4	Training Requirements	27
6.3.5	Documentation Supplied To Personnel	27
7	Technical Security Controls.....	27
7.1	Key Pair Generation And Installation.....	28
7.1.1	Key Pair Generation	28
7.1.2	Private Key Delivery To Entity.....	28
7.1.3	Signer Public Key Delivery To CR.....	28
7.1.4	CR Public Key Delivery To Users.....	28
7.1.5	Key Sizes	28
7.2	CR Private Key Protection.....	28
7.2.1	Standards For Cryptographic Module	28
7.2.2	Private Key (N-M) Multi-Person Control.....	28
7.2.3	Private Key Escrow	29
7.2.4	Private Key Backup	29
7.2.5	Private Key Archival	29
7.2.6	Private Key Entry Into Cryptographic Module	29
7.2.7	Method Of Activating Private Key.....	29
7.2.8	Method Of Deactivating Private Key	29
7.2.9	Method Of Destroying Private Key.....	29
7.3	Other Aspects Of Key Pair Management	29
7.3.1	Public Key Archival	29
7.3.2	Key Replacement	29
7.3.3	Restrictions On CR's Private Key Use.....	29
7.4	Activation Data	29
7.5	Computer Security Controls	29
8	Certificate And CRL Profiles.....	30
8.1	Certificate Profile.....	30
8.1.1	Certificate extensions	30
8.2	CRL Profile.....	30
8.2.1	Version number	30
8.2.2	CRL and CRL entry extensions	30
9	Policy Administration.....	30
9.1	Policy Change Procedures	30
9.1.1	List Of Items	30
9.1.2	Comment Period	31
9.2	Publication & Notification Procedures	31
9.2.1.1	Notification mechanism.....	31
9.2.1.2	Mechanism to handle comments.....	31
9.2.2	Items whose change requires a new policy.....	31

Draft

1 **Introduction**

This Certificate Policy (CP) defines Arizona's PGP Digital Signature Certificate Policy – Basic Assurance Level. This Policy is for use in the PGP portion of the State of Arizona's Electronic Signature Infrastructure (AESI)¹ as defined and managed by Arizona's Policy Authority (PA).

This document uses several technical concepts associated with PGP technology. To become familiar with the terminology used, we strongly recommend that you read the Electronic and Digital Signature Definitions and Acronyms document before reading this one and then refer to it as needed while reading this.

The security mechanisms provided by the AESI are not intended to be used alone for the protection of classified or sensitive information.

2 **Policy Specification**

2.1 **Overview**

This certificate policy is intended for use by agencies and departments of the State of Arizona and anyone having PGP digital signature use with them.

PGP allows individuals to create their own public/private key pair and to share the public key with trading partners. PGP use can be a simple exchange of identity and public keys between parties but it may be used in larger communities using reliable third parties as intermediaries to exchange identity and authenticate signatures. Parties in a PGP user community might agree on reliable third parties to perform one or more of three specific PGP critical roles:

- 1) A Certificate Manufacturing Authority role can be played by a third party if PGP community members do not create and distribute their own key pairs.
- 2) A Registration Authority role provides some reliable means to authenticate the identity of the person claiming association with a public key.
- 3) A Certificate Repository role provides means to reliably store public keys and a means for community members to verify the link between an individual and his public key. This removes a requirement for each community member to share public keys with every other community member with whom they interact.

This Certificate Policy will discuss the various roles involved in creating, maintaining, and validating PGP Certificates. The primary roles are:

- the Signer (holder of the key pair),
- the Relying Party (one relying on the validity of the digital signature created using the private key),
- the Certificate Repository (one keeping the list of validated public keys that the Relying Party can verify against),
- the Registration Authority (one authenticating that the Signer is the party they represent themselves to be) and

¹ taking liberties with IETF's conception of PKI, 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 Certificate Manufacturing Authority (one who creates the key pair, usually the Signer but this might be delegated).

This Certificate Policy discusses the obligations associated with each of these roles and with other possible roles that part of the process might be delegated to. Note that a participant can be the Signer in one case (when signing something) and the Relying Party in another (when relying on someone else's signature).

Communities of interest (ESI's), determining that the certificate levels of trust (basic, medium, and high) within this PGP Certificate Policy do not exactly meet their needs, should accept and use the closest *less* restrictive certificate level of trust and create a binding agreement among themselves adding any additional conditions required. They may not reduce or otherwise undermine the terms and conditions of this CP. Relying Parties rely on this CP being fully enforceable.

The digital signature policies within this CP are for the management and use of Certificates for electronic signature use.

Certificate issuance under any of these Arizona PGP Digital Signature Certificate Policies does not imply that the Signer has any authority to conduct business transactions on behalf of an organization.

The Certificate Repository's compliance with this Certificate Policy will be governed by the laws of the State of Arizona and any applicable Federal and local law concerning the enforceability, construction, interpretation and validity of this Certificate Policy.

The Certificate Manufacturing Authority's compliance with this Certificate Policy will be governed by the laws of the State of Arizona and any applicable Federal and local law concerning the enforceability, construction, interpretation and validity of this Certificate Policy.

The Registration Authority's compliance with this Certificate Policy will be governed by the laws of the State of Arizona and any applicable Federal and local law concerning the enforceability, construction, interpretation and validity of this Certificate Policy.

The State of Arizona will not enter into a cross certification agreement with another PGP community or Certificate Repository without the approval of the Policy Authority.

2.2 Policy overview

The Policy Object Identifier Designation for this Policy is registered under the Policy Authority arc { joint-iso-ccitt (2) country (16) us (840) state (3) AZ (04) EB (01) Secretary of State (002) DO (02) Policy Authority (999) } as OO (00) id-AESIpgp-certpcy-sign-1 (003). This policy has been designed to be used in certain situations and identifies specific roles to implement them. Signers and Relying Parties as well as any parties assuming delegated roles as Certificate Repositories (CR), Registration Authorities (RAs), and Certificate Manufacturing Authority (CMA) all have specific obligations which are outlined in this policy.

Signers and Relying Parties or their designated Certificate Repositories may only cross-certify Certificates with other parties bound to this CP by appropriate agreements and as approved by the Policy Authority.

The Signers and Relying Parties must agree on a method to securely create key pairs and certificates; that method must be managed by a party known as a Certificate Manufacturing Authority. Any of the parties may be the Certificate Manufacturing Authority or a mutually agreed upon third party may do so. The Certificate Manufacturing Authority must contractually agree to comply with this CP and any other agreement between it and the Signers and Relying Parties.

The Signers and Relying Parties must agree on a method to identify the party applying to be a Signer. The identification method is managed by the party known as a Registration Authority. Any of the parties may be the Registration Authority or a mutually agreed third party may do so. The party acting as the Registration Authority must contractually agree to comply with this CP and any other agreement between it and the Signers and Relying Parties.

Signers and Relying Parties must agree on a method for public key certificate verification and maintenance. That method is managed by a party known as a Certificate Repository. Any of the parties may be a Certificate Repository or a mutually agreed third party may do so. The party acting as the Certificate Repository must contractually agree to comply with this CP and any other agreement between it and the Signers and Relying Parties.

The appropriate use of this assurance level's certificates and keys is for signing documents that, if compromised, could cause minimal injury to the interests of the State of Arizona unless there is an explicit agreement by the agency (or agencies) participating in the ESI to alter this limitation.

The State of Arizona disclaims all liability for any use of this type of certificate other than uses permitted within this document. The State of Arizona limits its liability for permitted uses to \$5,000 per instance of use unless there is an explicit agreement by the agency (or agencies) participating in the ESI to extend that limit.

Any disputes concerning key or certificate management under this policy are to be resolved by the Parties concerned using an appropriate dispute settlement mechanism (i.e. through negotiation, mediation or arbitration).

Certificates may be placed in a Certificate database managed by the Certificate Repository following authentication of a Signer's identity as required by this policy.

Identification and authentication will be in the manner set out in this policy.

A Certificate Repository will remove certificates from the repository database of certificates in the circumstances enumerated in this policy.

A Certificate Repository is required to maintain records or information logs in the manner described in this policy.

PGP Electronic Signature CP - Version 1.00

This CP does not allow the ability to recover any private key other than by the owner of that key (Signer). The private key is in the sole possession of the Signer. Applications that require recoverable encrypted messaging will employ a CP defining confidentiality with key recovery *for the encryption only*. Such applications may also use this CP, but only for a separate *signature* and as long as there is no mingling of the two types of Certificates in a repository. Certificates based on this Certificate Policy rely on the Signer's sole possession to assert the signature process and must not be mingled with any Certificates that allow recovery and thereby break the criteria of sole possession.

Certificate Repository activities are subject to inspection by the PA and agents of the PA.

2.3 Identification alphanumeric OID

id-AESIpgp-certpcy-digitalSignature-basicAssurance ::= { id-AESIpki-certpcy-sign-3 }

Certificate Types (levels of signing process trust)

The following certificate types and OIDs will be recognized for use within the ESI established by this Certificate Policy. The certificate types listed below — Basic, Medium and High — vary depending on the method of identifying the Signer, the method for linking the Signer to the Certificate and the processes for assuring the Integrity of the Record. The ESI electronic signature level (Basic, Medium, High) is determined from the matrix of trust levels in section 2.4.8.1. The Certificate assigned should support the highest trust level required among the categories: Signer Identification, Signer Linkage to Signature, and Signature Linkage to the Integrity of the Record. Each level of Certificate subsumes the level(s) below it. All Certificates issued under this Certificate Policy will contain the OID listed below in the Certificate Policies field of the Certificate:

- Basic Trust Signing Certificate OID is: 2.16.840.3.04.01.002.02.999.00.003.01.01
- Medium Trust Signing Certificate OID is:
2.16.840.3.04.01.002.02.999.00.003.01.02
- High Trust Signing Certificate OID is: 2.16.840.3.04.01.002.02.999.00.003.01.03

2.4 Community and applicability

The State of Arizona's Electronic Signature Infrastructure (AESI), and consequently, its PGP infrastructure, is managed by the Office of the Secretary of State serving as the Policy Authority (PA) in accordance with appropriate Statute and Administrative Rules.

This Policy describes a PGP infrastructure within AESI. This PGP infrastructure is used by bounded communities of interest. A bounded PGP community of interest will be described herein as an Electronic Signature Infrastructure (ESI). The ESI is designed to enable the use of electronic signatures as the equivalent of handwritten signatures. This requires a similar range of protections of the authenticity and verification as a handwritten signature on a physical document. It also requires, given its nature, additional protections that the signer cannot repudiate their signing later.

An ESI community is comprised of Signers and Relying Parties who have mutually agreed to participate in this community and any parties that they have agreed to delegate specific roles to.

PGP Electronic Signature CP - Version 1.00

2.4.1 Description of PGP infrastructure

Any PGP use involves the mutual agreement of parties to employ PGP key pairs to sign in an agreed upon fashion. This requires agreement on:

1. How the Signer will be authenticated as the party they represent themselves to be,
2. Who will generate the PGP keys (one or more of the parties or an agreed on third party) and agreement that the method assures the Signer has sole possession of the private key,
3. How the validity of the public key will be ascertained (requires one or more of the parties or an agreed on third party to act as a Certificate Repository),
4. How the integrity of the record will be ascertained and how that integrity is linked to the Signer's public key.
5. Agreement that the reception of a record linked to a valid public key and with proof of record integrity completes a legally binding signing of the record by the holder of the corresponding private key (Signer).

This Policy is binding on each party that issues certificates that identify this Policy, and governs each party's performance with respect to all certificates they issue or use that reference this Policy.

All Signers shall use certificates issued in accordance with this Certificate Policy. Should a state Agency use a contractor to provide Certificate Repository, LRA or CMA services, the Agency will remain responsible and accountable for the operation of its contractors.

2.4.2 Registration Authorities and Certificate Manufacturing Authorities

The Signers and Relying Parties shall agree on who might perform the role and functions of the Registration Authority (RA). They may subcontract Registration Authority functions to a third party who agrees to be bound by this Policy, but the Signers and Relying Parties remain responsible for the performance of those services in accordance with this Policy and the requirements of their AESI Contract.

The ESI's Signers and Relying Parties must agree on who will generate the PGP keys (one or more of the parties or an agreed on third party) and agree that the method assures the Signer has sole possession of the private key. The Signers and Relying Parties shall agree on who might perform the role and functions of the Certificate Manufacturing Authority (CMA). They may subcontract CMA functions to a third party who agrees to be bound by this Policy, but the Signers and Relying Parties remain responsible for the performance of those services in accordance with this Policy and the requirements of their AESI Contract.

2.4.3 Local Registration Authorities (LRAs)

An LRA operating under this certificate policy is responsible for all duties assigned to it by the Signers and Relying Parties or their RA subcontractor(s).

An LRA may perform RA duties providing that in doing so it satisfies all the requirements of this CP.

2.4.4 Certificate Repositories

The Signers and Relying Parties must agree on a method for transferring and maintaining valid public key certificates with that method managed by a party known here as a Certificate Repository. Any of the parties may maintain it or a mutually agreed third party may do so. The party acting as the Certificate Repository must contractually agree to comply with this CP and any other agreement between it and the Signers and Relying Parties. Signers and Relying Parties remain responsible for the performance of those services in accordance with this Policy and the requirements of their AESI Contract.

2.4.5 Signers

The ESI's Signers and Relying Parties must agree on who will generate the PGP keys (one or more of the parties or an agreed on third party) and agree that the method assures the Signer has sole possession of the private key. Certificates that reference this Policy may be issued to the following classes of Signers:

- individuals (unaffiliated)
- individuals associated with a sponsor recognized by the ESI ("affiliated individuals"), provided the sponsor is the Signer of a valid Certificate issued within the ESI in accordance with this Policy.
- organizations that qualify as legal entities provided that responsibility and accountability is attributable to an designated living agent for the organization.
- government agencies provided that responsibility and accountability is attributable to an designated living agent for the agency.

Signers may also be issued Certificates for assignment to devices or applications provided that responsibility and accountability is attributable to the Signer.

2.4.6 Relying parties

This Policy is intended for the benefit of the following persons who may rely on Certificates issued to others that reference this Policy (Qualified Relying Parties):

- State government agencies that specify this Policy by regulation
- Federal and other government agencies that specify this Policy by regulation
- Businesses that agree to accept AESI Certificates and agree to be bound by the terms of this Policy regarding those Certificates.
- Individuals that agree to accept AESI Certificates and agree to be bound by the terms of this Policy regarding those Certificates.

2.4.7 Policy applicability

This Certificate Policy is suitable for the integrity and authentication of business transactions within the originator's approval limits and such that the falsification of the transaction would cause only minor financial loss or require only administrative action for correction.

2.4.8 Approved and prohibited applications

Certificates that reference this Policy are intended to support verification of electronic signatures.

2.4.8.1 Electronic Signature Framework of Trust

Each signing community will need to evaluate the levels of risk associated with their signing processes and associate those risks to a framework that defines three levels of trust in evaluating authenticity, reliability, and integrity of signed electronic records. Each of these trust levels should be tied to the potential risk involved in and levels of security for the highest risk type of transaction. The trust levels defined are as follows:

- **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.

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.

2.4.8.1.1 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	<ul style="list-style-type: none">• 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
-------	---

	<p>(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</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

PGP Electronic Signature CP - Version 1.00

	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.

2.4.8.1.2 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.

1. 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).
2. 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	<ul style="list-style-type: none"> • Two shared secrets (e.g., pin, password) where a governmental body has assigned at least one secret and the
-------	---

	<p>signer has been provided with and has conformed to appropriate security standards as far as protecting the shared secrets.</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

2.4.8.1.3 Signature Linkage to the Integrity of the Record

This element of trust has two components.

1. 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.

2. 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	<ul style="list-style-type: none"> • 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 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	<ul style="list-style-type: none"> • 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

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.

	<p>transferring the electronically signed record, ascertaining the integrity of the record, and ascertaining the integrity of the signature and record link.</p> <ul style="list-style-type: none"> • 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.
<p>High</p>	<ul style="list-style-type: none"> • 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

PGP Electronic Signature CP - Version 1.00

	<p>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)</p>
--	---

2.4.8.2 *Approved Applications*

Certificates that reference this Policy may be used for any purpose authorized by regulations adopted by Qualified Relying Parties, except to the extent specifically prohibited by agreements among the ESI Signers and Relying Parties.

The ESI electronic signature level (Basic, Medium, High) is determined from this matrix of trust levels. The Certificate assigned should support the highest trust level required among the categories: Signer Identification, Signer Linkage to Signature, Signature Linkage to the Integrity of the Record.

2.4.8.3 *Prohibited Applications*

Certificates that reference this Policy may not be used for any application requiring fail-safe performance such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems or any other system whose failure could lead to injury, death or environmental damage.

Certificates that reference this Policy should not be used for transactions where the per use value exceeds \$25,000.00 without the explicit agreement among the parties.

2.4.9 **Contact details**

This Policy is administered by the Policy Authority:

State of Arizona
Office of the Secretary of State
1700 W. Washington #7
Phoenix, Arizona 85007

2.4.9.1 *Policy Authority contact person:*

Russ Savage
Phone number: 602.542.2022
E-mail address: pa@mail.sosaz.com

2.4.9.2 *Contact person determining CPS suitability for this Policy:*

Russ Savage

3 General Provisions

3.1 Obligations

3.1.1 Certificate creation and management obligations

The ESI's Signers and Relying Parties must establish contractual agreement on controls over the application and enrollment process, the identification and authentication process, the actual certificate manufacturing process, publication of the certificate, suspension and revocation of the certificate, renewal of the certificate, and for ensuring that all aspects of the services, methods, operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

These contractual agreements will operate in accordance with this Certificate Policy and the laws of Arizona when fulfilling these obligations. The parties will ensure that any LRAs operating on their behalf will comply with the relevant provisions of this CP concerning the operation of LRAs. The parties will individually take all reasonable measures to ensure that Signers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, Certificates or End-Entity hardware and software used within the ESI.

3.1.1.1 Representations By Certificate Manufacturer

The ESI's Signers and Relying Parties must establish a contractual agreement with the party or parties known as Certificate Manufacturer such that by issuing a certificate that references this Policy, the Certificate Manufacturer certifies to the Signer, and to all Qualified Relying Parties who reasonably and in good faith rely on the information contained in the certificate during its operational period and in accordance with this Policy, that:

- (a) The certificate was issued in accordance with this Policy
- (b) The requirements of this Policy were complied with when authenticating the Signer and issuing the certificate
- (c) There are no misrepresentations of fact in the certificate known to the Certificate Manufacturer.
- (d) Information provided by the Signer in the certificate application for inclusion in the certificate has been accurately transcribed to the certificate.
- (e) The certificate meets all material requirements of this Policy.

3.1.1.2 Time between certificate request and issuance

There is no stipulation for the period between the receipt of an application for a Certificate and the generation of the Entity's key material.

The Certificate Manufacturer must ensure that the period for which the Entity has to complete its initialization process is no longer than five working days.

3.1.2 Registration Authorities (RA) and Certificate Manufacturing Authorities (CMA) Obligations

The parties (Signer and Relying Party) are responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. However, they may delegate performance of some or all of these obligations to an identified Registration Authority (RA) and/or Certificate Manufacturing Authority (CMA) provided that they assume primary responsibility for the performance of those services by such third parties in a manner consistent with the requirements of this Policy.

3.1.3 LRA obligations (LRA duties)

Should the ESI allow the use of LRAs, then the parties must ensure that LRAs comply with all the relevant provisions of this CP. Administrators must be individually accountable for actions performed on behalf of the parties. (There must be evidence that attributes an action to the person performing the action for it to be individually accountable.) Records of all actions carried out in performance of LRA duties must identify the individual who performed the particular duty.

The LRA is not required to notify a Relying Party of the issuance or revocation of a certificate.

3.1.4 Signer Obligations

In all cases, the Signer shall enter into an enforceable contractual commitment for the benefit of Qualified Relying Parties obligating the Signer to:

- (a) activate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key
- (b) acknowledge that by accepting the Certificate the Signer is warranting that all information and representations made by the Signer that are included in the Certificate are true
- (c) use the Certificate exclusively for authorized and legal purposes, consistent with this Policy
- (d) request the Certificate Repository to revoke the Certificate promptly upon any actual or suspected compromise of the Signer's private key

3.1.5 Relying Party Obligations

A Qualified Relying Party has a right to rely on a Certificate that references this Policy only if the Certificate was used and relied upon for lawful purposes and under circumstances where:

- (a) the reliance was reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of reliance
- (b) the purpose for which the Certificate was used was appropriate under this Policy
- (c) the Relying Party checked the status of the Certificate prior to reliance and it was valid. Reliance in the case of an inability to check the status shall be governed by any contract between the parties and by applicable statute.

3.1.6 Policy Authority Obligations

The Policy Authority is responsible for the terms of this Policy and its administration.

3.2 Requirements

An RA will ensure that its practices and actions (including certification) are in accordance this CP.

A CMA will ensure that its practices and actions are in accordance this CP.

An CR will ensure that its practices and actions (including repository services, issuance and revocation of certificates, and issuance of CRLs) are in accordance this CP.

3.3 Disclaimers of warranties and obligations

The State of Arizona assumes no liability whatsoever in relation to the use of AESI Certificates or associated public/private key pairs for any use other than in accordance with this CP and any other explicit agreements.

The State of Arizona, its employees and agents makes no representations, warranties or conditions, express or implied other than as expressly stated in this CP or in any other official document.

3.4 Liability

Except as expressly provided in this Policy and in ESI agreements, every CMA, RS and CR is responsible to Qualified Relying Parties for direct damages suffered by such Relying Parties that are caused by the failure of the CMA, RS or CR to comply with the terms of this Policy, and sustained by such Relying Parties as a result of reliance on a Certificate in accordance with this Policy, but only to the extent that the damages result from the use of Certificates for a suitable applications listed as defined in this CP.

Except as expressly provided in this Policy and in ESI agreements, any CMA, RFA or CR disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.

3.5 Interpretation & Enforcement

3.5.1 Governing Law

The enforceability, construction, interpretation, and validity of this Policy shall be governed by the laws of the State of Arizona and the United States of America.

3.5.2 Severability, survival, merger, notice

Any CR, or agent of a CR, shall ensure that any of its agreements will have appropriate provisions governing severability, survival, merger or notice.

Any CR or agent of a CR shall have PA approval of its provisions governing severability, survival, merger or notice before beginning operation within an ESI and shall gain approval of any amendment to those provisions before such amendment can take effect.

3.5.3 Dispute Resolution Procedures

Each party shall ensure that any agreement they enter into provides appropriate dispute resolution procedures

3.6 Fees

No party may impose any fees on the reading of this Policy.

CR may charge the Signer access fees on Certificates, Certificate status information, or CRLs, subject to agreement between the CR and Signer and in accordance with a publicly available fee schedule.

3.7 Publication & Repositories

3.7.1 Publication Of CA Information

Each CR shall have a mechanism for appropriate Qualified Relying Parties to validate a PGP digital signature. This mechanism will provide the necessary information regarding:

1. issued Certificates that reference this Policy,
2. either:
 - a) a Certificate Revocation List ("CRL") or on-line certificate status database, or
 - b) an valid Certificate list withrevoked or suspended Certificates removed
3. the CR's Certificate for its signing key,
4. a copy of this Policy (if required by the ESI), and
5. other relevant information relating to Certificates that reference this Policy.

3.7.2 Frequency of Publication

All information to be published in the Repository shall be published promptly after such information is available to the CR. Certificates issued by the CM that reference this Policy will be published promptly upon acceptance of such Certificate by the Signer.

3.7.3 Access Controls

The Repository will be available to appropriate Qualified Relying Parties on a basis that is stipulated by the ESI parties' terms of access. The CR shall not impose any access controls on this Policy, the CR's certificate for its signing key. The CR may impose access controls on Certificates, certificate status information, or CRLs at its discretion, subject to agreement between the CR and Signer, in accordance with published.

3.8 Compliance Audit

The Policy Authority may outline specific requirements for a compliance audit. These requirements will conform to any statutory or regulatory requirements of the State of Arizona.

As deemed necessary by the PA, the CMA, RA, and CR, as applicable, shall submit to a compliance audit by an independent nationally recognized security audit firm that is approved by the Policy Authority as being qualified to perform such an audit and that has significant experience in the application of PGP and cryptographic technologies. The

purpose of such audit shall be to verify that the party and its delegated parties have a system in place:

- to assure the quality of the services provided,
- that the party complies with all of the requirements of this Policy, and
- that assures the meets the requirements of this Policy and any related agreement with the PA.

3.9 Intellectual property rights

No stipulation.

4 Identification And Authentication

4.1 Initial Registration

Subject to the requirements noted below, Certificate applications may be communicated from the applicant to the RA and authorizations to issue certificates may be communicated from an RA to the CMA:

- electronically via E-mail or a web site, provided that all communication is secure, such as by using SSL or a similar security protocol,
- by first class U.S. mail, or
- in person.

4.1.1 Types of Names

The subject name used for certificate applicants shall be a unique X.509 Distinguished Name (DN).

4.1.2 Name Meanings

The subject name listed in a Certificate must have a reasonable association with the authenticated name of the Signer. In the case of individuals this should be a combination of first name and/or initials and surname. In the case of an organization the name should reflect the legal name of the organization and/or unit.

A Certificate that refers to a role or position shall also contain the identity of the person who holds that role or position.

Any Certificate issued for a device or application shall, within the DN, include the name of the person or organization responsible for that device or application.

4.1.3 Rules For Interpreting Various Name Forms

No stipulation.

4.1.4 Name Uniqueness

The subject name listed in a Certificate shall be unambiguous and unique for all certificates issued for the ESI by any CMA and conform to X.500 standards for name uniqueness. If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of certificates issued by the CMA.

No wildcard name forms are allowed. Each name shall be unique and for a single unique entity.

4.1.5 Verification of Key Pair

The CMA shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application in accordance with an appropriate secure protocol. Only then may the CMA securely transmit the public key to the CR for placement in the CR's database.

4.1.6 Authentication of Organization

When an RA receives a certificate application from an organization, it shall conduct an independent investigation in order to determine whether:

- The organization exists and conducts business at the address listed in the certificate application.
- The certificate application is signed by a signatory who is a duly authorized representative of the organization named therein.
- The information contained in the certificate application is correct.

In conducting its review and investigation, the RA shall review official government records and/or engage the services of a reputable third party vendor of business information to provide validation information concerning each organization applying for a certificate, including legal company name, type of entity, year of formation, names of directors and officers, address, telephone number, and good standing in the jurisdiction where the applicant is incorporated or otherwise organized.

The RA will keep a record of the type and details used for verifying identity.

4.1.7 Authentication of Individual -- No Affiliation

4.1.7.1 Identification

In authenticating an unaffiliated individual applicant, the RA shall require proof of identity as defined in the following section *Satisfactory Evidence of Identity*.

Copies of the identification used to establish the Signer's identity shall be initialed by the RA upon acceptance and archived.

4.1.7.2 Investigation And Confirmation

No Stipulation

4.1.7.3 Personal Presence

Authentication of an unaffiliated individual requires that the applicant must either (1) personally present himself or herself to the RA to be authenticated prior to certificate issuance, or (2) securely deliver signed and notarized copies of the requisite identification to the RA (in which case, electronic procedures may be used thereafter). Where the applicant delivers notarized copies of identification to the RA, authentication of such identification will be confirmed through the use of a shared secret (such as a PIN

number) that is separately communicated in a trustworthy manner to the applicant and included with the documents delivered as part of the certificate application process.

4.1.8 Authentication of Individual – Affiliated Certificate

4.1.8.1 Identification

The RA may establish a trustworthy procedure whereby a sponsoring organization that has been authenticated by the RA and issued a certificate may designate one or more Responsible Individuals, and authorize them to represent the sponsoring organization in connection with the issuance and revocation of certificates for affiliated individuals. The RA may rely on a designated Responsible Individual appointed by the sponsor to properly authenticate the individual applicant (provided that the RA has previously authenticated the sponsor as an organization and the Responsible Individual as an unaffiliated individual, in accordance with this Policy). The Responsible Party shall require proof of identity as defined in the following section *Satisfactory Evidence of Identity*.

In the absence of the foregoing procedure, affiliated individuals shall be authenticated in the same manner as unaffiliated individuals.

4.1.8.2 Authentication Confirmation Procedure

Authentication of the individual may be confirmed through the use of a shared secret (e.g. a PIN number) that is distributed to the applicant by a trustworthy communication method not used for digital signatures. The shared secret may be distributed directly or through the sponsor as part of the certificate enrollment process.

4.1.8.3 Personal Presence

Applicants that are affiliated with an Approved sponsor can be authenticated through an electronically submitted application, based on an appropriate agreement with the sponsor, the approval of a designated Responsible Individual, and the distribution of PIN numbers or a similar security device.

4.1.8.4 Duties of Responsible Individuals

The Responsible Individual represents the sponsoring organization with respect to the issuance and management of certificates. In that capacity he or she is responsible for properly indicating which Signers are to receive Certificates.

4.1.9 Authentication of devices or applications

An application for a device or application to be an End-Entity may be made by an approved Signer for whom the device's or application's signature is attributable for the purposes of accountability and responsibility.

Identification and authentication of the applicant must follow this Policy's requirements as if the Signer was applying for the Certificate on its own behalf.

The device Certificate will be revoked if the Signer's Certificate is revoked. This type of certificate can only be issued by a CMA that can assure accomplishment of such revocation.

4.2 Renewal Applications (Routine Rekey)

Within three months prior to the scheduled expiration of the operational period of a Certificate issued following authentication under this Policy, a Signer may request issuance of a new Certificate for a new key pair from the CMA that issued the original Certificate, provided the original Certificate has not been suspended or revoked. Such a request may be made electronically via a digitally signed message based on the old key pair in the original Certificate.

Renewal of an affiliated individual shall require verification that the affiliation still exists. Such verification of affiliation shall be the same as what is required for a new application.

4.3 Rekey After Revocation

Revoked or expired Certificates shall not be renewed. Applicants without a valid Certificate from the CMA that references this Policy shall be re-authenticated by the RA on certificate application, just as with a first-time application.

4.4 Satisfactory Evidence of Identity

What is satisfactory evidence of identity is determined by the certificate level of trust desired (See 2.4.8 Electronic Signature Framework of Trust).

5 Operational Requirements

5.1 Certificate Application

An applicant for a Certificate shall complete a certificate application in a form prescribed by the ESI parties and enter into a Signer agreement with the ESI parties. All applications are subject to review, approval and acceptance by an ESI's RA. The certificate application process may be initiated by the following persons:

<u>Potential Signer</u>	<u>Authorized Initiator</u>
Individual (unaffiliated)	Potential Signer only
Individual affiliated with a sponsor	Potential Signer or duly authorized representative of sponsor
Organization	Duly authorized representative of the subscribing organization (who shall be individually responsible for the certificate.)

5.1.1 Application for a cross-certificate

The PA will identify the necessary procedures to apply for a cross-certificate.

At this time the PA does not foresee the applicability of cross-certification for PGP ESI's.

An application for a cross-certificate does not oblige the PA to authorize a cross-certificate. The PA shall review any ESI's request for cross-certification and approve or deny any such request according to established procedures.

5.2 Certificate Issuance

Upon successful completion of the Signer identification and authentication process in accordance with this Policy, and complete and final approval of the certificate application, the RA will securely communicate the necessary information to the CMA who shall issue the requested Certificate, notify the applicant thereof, and make the Certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or available for pickup by, the Signer only. A CMA will not issue a Certificate without the consent of the applicant and, if applicable, the applicant's sponsor.

5.3 Certificate Acceptance

The ESI parties shall contractually require that the Signer expressly indicate acceptance or rejection of the Certificate following its issuance, in accordance with procedures established by the ESI.

There will be a short time period when the Signer must act to accept or, once the time has expired, the Certificate will be revoked and the Signer will have to begin a new application.

5.4 Certificate Revocation

5.4.1 Circumstances For Revocation

5.4.1.1 Permissive Revocation

A Signer may request revocation of their individual Certificate at any time for any reason.

A sponsoring organization may, where applicable, request revocation of an affiliated individual Certificate at any time for any reason.

The ESI parties shall provide a procedure in their contractual framework for the CR to be able to revoke a Certificate upon failure of the Signer (or any sponsoring organization, where applicable) to meet its obligations under this Certificate Policy or any other agreement, regulation, or law applicable to the Certificate that may be in force. This includes revoking a Certificate when a suspected or known compromise of the private key has occurred.

The PA may, at its discretion, revoke a cross-certificate when parties of an ESI fail to comply with obligations set out in this CP, any agreement or any applicable law.

5.4.1.2 Required Revocation

A Signer, or a sponsoring organization (where applicable) shall promptly request revocation of a Certificate:

- whenever any of the information on the Certificate changes or becomes obsolete

- whenever the private key, or the media holding the private key, associated with the certificate is known or suspected of being compromised
- whenever an affiliated individual is no longer affiliated with the sponsor

The CR shall revoke a Certificate:

- upon request of the Signer or sponsoring organization
- upon failure of the Signer (or the sponsoring organization, where applicable) to meet its material obligations under this Certificate Policy or any other agreement, regulation, or law applicable to the certificate that may be in force.
- if knowledge or reasonable suspicion of compromise is obtained
- if the CR determines that the certificate was not properly issued in accordance with this Policy and the agreements between the ESI parties.

5.4.2 Procedure For Revocation Request

A certificate revocation request should be promptly communicated to the CR, either directly or through an RA. A certificate revocation request may be communicated electronically if it is digitally signed with the private key of the Signer, or the sponsoring organization (where applicable). Alternatively the Signer, or sponsoring organization (where applicable), may request revocation by contacting the CR or an authorized RA in person and providing adequate proof of identification in accordance with this Policy.

A revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the old key pair. The identity of a person submitting a revocation request in any other manner shall be authenticated. Revocation requests authenticated on the basis of the old (compromised) key pair shall always be accepted as valid. Other revocation request authentication mechanisms may be used as well. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke Certificates.

Requests for revocation of Certificates will be logged.

5.4.2.1 Repository/CRL Update

The ESI parties will have determined the method of managing the Certificate databases maintained by the Certificate Repository. The simple method is to have a repository only consisting of the currently valid public keys. However more elaborate processes might be used to allow for verification not only of what is currently valid but to also verify that certificates were or were not valid at the time of past signings.

Promptly following revocation of a Certificate, the CRL or certificate status database in the Repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the CR shall be archived.

5.4.3 Revocation Request Grace Period

Requests for revocation shall be processed within a contractually agreed time (e.g. twenty four hours) of receipt by the CR.

5.4.4 Certificate Suspension

Certificate suspension is not allowed.

5.4.5 CRL Issuance Frequency

If CRLs are used, the ESI parties shall contractually define how frequently an up-to-date CRL shall be issued (suggested frequency is at least every three hours).

The updated CRL must be issued immediately when a Certificate is revoked due to key compromise.

The CR will synchronize any CRL issuance with any State directory services that relies on the CR's certificates to determine access to State resources.

5.4.6 CRL checking requirements

The ESI parties shall contractually define whether a Relying Party must check the status of a certificate and whether the Relying Party must also verify the authenticity and integrity of CRLs and ARLs.

5.4.7 On-Line Revocation/Status Checking Availability

Whenever an on-line certificate status database is used as an alternative to a CRL, such database shall be updated and checked according to the same requirements as defined for a CRL.

5.4.8 Special requirements rekey compromise

A CR must immediately notify all parties to whom it has issued cross-certificates and the PA after the compromise or suspected compromise of its signing key.

Any other Entity must notify the issuing CR immediately in the event of the compromise or suspected compromise of its signing key.

A CR must ensure that provisions outlining the means it will use to provide notice of compromise or suspected compromise are in a publicly available document and appropriate agreements.

5.5 Computer Security Audit Procedures

All significant security events on the CR system should be automatically recorded in audit trail files. The audit log shall be processed at least once a week. Such files shall be retained for at least six (6) months onsite, and thereafter shall be securely archived according to the PA's record retention schedule.

5.6 Records Archival

5.6.1 Types Of Records Archived

The following data and files must be archived by or on behalf of the CR:

- All computer security audit data (including access logs)

- All certificate application data (including changes to certificate and registration information)
- All certificates, and all CRLs or certificate status records generated
- Key histories
- All correspondence between the CR and RAs, CMAs, CMs, and/or Signers.

The CR is responsible for the satisfactory archiving of this material.

5.6.2 Retention Period For Archive

Archive of the key and certificate information must be retained *after expiration* for the “legal” life of the most enduring document signed within the ESI. If that “legal” life is unknown, then for at least 30 years. Archives of the audit trail log files must be retained for at least six (6) months.

Any signed document may also have public records retention requirements that must also be met.

5.6.3 Protection Of Archive

The archive media must be protected either by physical security alone, or a combination of physical security and cryptographic protection. This protection must meet or exceed State of Arizona and Agency electronic records retention requirements for such material.

5.6.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.

5.6.5 Archive Collection System (Internal Or External)

No stipulation.

5.6.6 Procedures To Obtain And Verify Archive Information

During the compliance audit required by this Policy, the auditor shall verify the integrity of the archives.

5.7 Key Changover

No stipulation.

5.8 Compromise And Disaster Recovery

5.8.1 Disaster Recovery Plan

The CR must have in place an appropriate disaster recovery and business resumption plan. The plan must set up and render operational a facility located in a geographic diverse area that is capable of providing CR Services in accordance with this Policy within forty eight (48) hours of an unanticipated emergency. Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be referenced

within appropriate documentation and readily available to Qualified Relying Parties for inspection.

5.8.2 CR Key Compromise Plan

The CR must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by the CR to authenticate the status of a certificate in a CR database.

5.9 CR Termination

In the event that the CR ceases operation, all Signers, sponsoring organizations, RAs, CMAs, and Qualified Relying Parties will be promptly notified of the termination. In addition, all parties with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All current and archived CR identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be transferred to the PA (or designate) within 24 hours of CR cessation and in accordance with this Policy. Transferred data shall not include any non-AESI data.

6 Physical, Procedural And Personnel Security

6.1 Physical Controls

6.1.1 Physical Security -- Access Controls

The CR, all RAs and all CMAs, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CR Services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section on Procedural Controls (6.3.1). Access shall be controlled through the use of: electronic access controls, mechanical combination locksets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

6.2 Procedural Controls

6.2.1 CMA Trusted Roles

All employees, contractors, and consultants of CMA (collectively "CMA personnel") that have access to or control over cryptographic operations that may materially affect the CMA's issuance, use, suspension, or revocation of certificates shall, for purposes of this Policy, be considered as serving in a trusted role. Such CMA personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CMA's operations.

6.2.2 CR Trusted Roles

All employees, contractors, and consultants of CR (collectively "CR personnel") that have access to or control over cryptographic operations that may materially affect the

CR's use, suspension, or revocation of certificates, including access to restricted operations of the CR's repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such CR personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CR's operations.

6.2.3 Multiple Roles (Number Of Persons Required Per Task)

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at a CR or CMA server should be shared by multiple roles and individuals. Each account on the CR or CMA server shall have limited capabilities commensurate with the role of the account holder.

6.3 Personal Security Controls

6.3.1 Background And Qualifications

CRs, RAs, and CMAs shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this Policy.

6.3.2 CR Background Investigation

CRs shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and CR's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

6.3.3 CMA Background Investigation

CMAs shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and CMA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

6.3.4 Training Requirements

All CR, RA, and CMA personnel must receive proper training in order to perform their duties, and update briefings thereafter as necessary to remain current.

6.3.5 Documentation Supplied To Personnel

All CR, RA, and CMA personnel must receive and read comprehensive user manuals detailing the procedures for certificate creation, update, renewal, suspension, and revocation, and software functionality.

7 Technical Security Controls

7.1 Key Pair Generation And Installation

7.1.1 Key Pair Generation

Key pairs for CRs, CMAs, RAs, and Signers must be generated in such a way that the private key is not known by other than the authorized user of the key pair. Acceptable ways of accomplishing this include:

- Having all users (CRs, CMAs, RAs, and Signers) generate their own keys on a trustworthy system, and not reveal the private keys to anyone else
- Having keys generated in hardware tokens from which the private key cannot be extracted.

CR, RA, and CMA keys should be generated in hardware tokens. Key pairs for end-entities can be generated in either hardware or software.

7.1.2 Private Key Delivery To Entity

See Section on Physical Security - Access Controls (6.1.1).

7.1.3 Signer Public Key Delivery To CR

The Signer's public key must be transferred to the CR in a way that ensures that:

- it has not been changed during transit;
- the sender possesses the private key that corresponds to the transferred public key; and
- the sender of the public key is the legitimate user claimed in the certificate application.

7.1.4 CR Public Key Delivery To Users

The public key of the CR signing key pair may be delivered to Signers in an on-line transaction by appropriate mechanism.

7.1.5 Key Sizes

Minimum key length for other than elliptic curve based algorithms is 1024 bits.

Minimum key length for elliptic curve group algorithms is 170 bits (M.J.Wiener, "Performance Comparison of Public-Key Cryptosystems", RSA CryptoBytes, Volume 4, Number 1, Summer 1998).

Acceptable algorithms for public key cryptography applications include but not limited to:

RSA (Rivest, Shamir, Adelman)	-- digital signature and information security
ElGamal	-- digital signature and information security
Diffie * Hellman	-- digital signature and information security
DSA /DSS (Digital Signature Algorithm)	-- digital signature applications

7.2 CR, RA and CMA Private Key Protection

The CR, the RA, and the CMA, as appropriate, shall each protect its private key(s) in accordance with the provisions of this Policy.

7.2.1 Standards For Cryptographic Module

No stipulation.

7.2.2 Private Key (N-M) Multi-Person Control

No stipulation.

7.2.3 Private Key Escrow

CR, CMA and RA signing private keys shall not be escrowed.

7.2.4 Private Key Backup

An entity may optionally back up its own private key.

7.2.5 Private Key Archival

An entity may optionally archive its own private key.

7.2.6 Private Key Entry Into Cryptographic Module

No stipulation.

7.2.7 Method Of Activating Private Key

No stipulation.

7.2.8 Method Of Deactivating Private Key

No stipulation.

7.2.9 Method Of Destroying Private Key

Upon expiration or revocation of a certificate, or other termination of use of a private key for creating signatures, all copies of the private key shall be securely destroyed.

7.3 Other Aspects Of Key Pair Management

7.3.1 Public Key Archival

The CR must retain all verification public keys.

7.3.2 Key Replacement

CR key pairs must be replaced at least every two (2) years. RA, CMA and Signer key pairs must be replaced not less than every two (2) years and a new certificate issued

7.3.3 Restrictions On CMA's Private Key Use

The CR's signing key used for signing CRLs that conform to this Policy shall be used only for signing CRLs and not be used for any other purpose without the express permission with a general ESI agreement.

A private key used by an RA or RSP for purposes associated with its RA or RSP function shall not be used for any other purpose without the express permission with a general ESI agreement.

A private key held by a CMA and used for purposes of manufacturing certificates or any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the ESI parties.

7.4 Activation Data

No stipulation.

7.5 Computer Security Controls

All CR servers must include the following functionality either provided by the operating system, or through a combination of operating system, PKI application, PGP application, and physical safeguards:

- *access control to CR services and ESI roles;*
- *enforced separation of duties for ESI roles;*
- *identification and authentication of ESI roles and associated identities;*
- *object re-use or separation for CR random access memory;*

- *use of cryptography for session communication and database security;*
- *archival of CR and End-Entity history and audit data;*
- *audit of security related events;*
- *self-test of security related CR services;*
- *trusted path for identification of PGP roles and associated identities;*
- *recovery mechanisms for keys and the CR system.*

8 Certificate And CRL Profiles

8.1 Certificate Profile

Certificates that reference this Policy shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages -- i.e., public keys used for digital signature verification.

All certificates that reference this Policy will be issued in standard PGP format and will include a reference to the OID for this Policy within the appropriate field.

8.1.1 Certificate extensions

An ESI agreement among the parties shall identify the PGP fields required for End-Entity software used within the ESI.

8.2 CRL Profile

An ESI agreement among the parties shall identify the CRL fields and extensions supported and the level of support for these fields and extensions.

8.2.1 Version number

An ESI agreement among the parties shall identify the PGP version or versions to be used within the ESI.

8.2.2 CRL and CRL entry extensions

All Entity PKI software must correctly process all CRL extensions identified in the Certificate and CRL profile. An ESI agreement among the parties must define the use of any extensions supported by the CR, RAs and End Entities.

9 Policy Administration

9.1 Policy Change Procedures

9.1.1 List Of Items

Notice of all proposed changes to this Policy under consideration by the Policy Authority that may materially impact users of this Policy (other than editorial or typographical corrections, or changes to the contact details) will be provided to the designated contact for the ESI, and will be posted on the World Wide Web site of the Policy Authority. CRs

shall post notice of such proposed changes in their repositories and shall advise their Signers, in writing or by e-mail, of such proposed changes.

9.1.2 Comment Period

Impacted users may file comments with the Policy Authority within 45 days of original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.

9.2 Publication & Notification Procedures

A copy of this Policy is available in electronic form on the Internet at <http://www.sos.state.az.us/pa/cp>, and via e-mail from pa@sos.state.az.us.

CRs shall post copies of this Policy in their repositories.

9.2.1.1 Notification mechanism

The PA will notify, in writing, all CRs that are directly cross-certified with the AESI of any proposed changes to this certificate policy. The notification must contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of change. The PA may request CRs to notify their Signers of the proposed changes.

9.2.1.2 Mechanism to handle comments

Written and signed comments on proposed changes must be directed to the PA. Decisions with respect to the proposed changes are at the sole discretion of the PA.

9.2.2 Items whose change requires a new policy

If a policy change is determined by the PA to warrant the issuance of a new policy, the PA may assign a new Object Identifier (OID) for the modified policy.