Digital Signature Policy Authority

Introduction to Electronic Signatures

Digital Signatures? What are they? What do I need to do? What is Arizona doing? And why is the Secretary of State in the middle of it?

The Short Answer:
Arizona passed legislation enabling the use of digital signatures by and with state agencies (A.R.S. 41-132 (http://www.azleg.state.az.us/ars/41/00132.htm)). That legislation gave the Secretary of State a statutory duty (http://www.azleg.state.az.us/ars/41/00121.htm) to "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." And it defined an electronic signature: "An electronic signature shall be unique to the person using it, shall be capable of reliable verification and shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated."

Which leads to the Long Answer:
It can be confusing to wade into the range of documents that describe Arizona's Digital Signature policy and practices. This introduction is intended to provide a "mental picture" of how the policy of electronic signature use fits with a range of business needs for signatures and how a range of technologies have been organized within that policy framework to flexibly satisfy that range of business needs.

The Secretary of State has a statutory duty to "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." The Policy Authority is how the Secretary of State establishes "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." (A.R.S. 41-121, Duties of the Secretary of State). The Policy Authority is designed to provide a "technology neutral" policy framework for electronic signing processes and then to build within that framework more specific specifications for using particular technologies.

Arizona was one of several states that passed electronic signature statutes in the late 1990's. Arizona was unusual in that we limited the statute to signing documents filed with and by state agencies. This was followed by many states have passing the Uniform Electronic Transactions Act (UETA), most states enacted a version in 2000 and 2001. Arizona passed UETA in 2000. UETA establishes a more common recognition of electronic signature. The U.S. Federal government also passed an electronic signatures act known as E-SIGN. E-SIGN had some implications to how states interpreted and implemented state electronic signature statutes (UETA or otherwise) and several states collaborated to review those implications and other state issues with electronic signatures. Russ Savage of Arizona's Office of Secretary of State chaired a multi-state workgroup in 2001 that developed a general framework for electronic signing processes and the Arizona Policy Authority's framework now includes many elements that came out of that multi-state effort.

The core multi-state documents are a good introduction into the process of establishing what is a good electronic signing practice and how to determine which technology to implement for particular uses. They are in PDF format below and along with an Introduction document that inadvertently was not published. More information on the National Electronic Commerce Coordinating Council can be found on its website (http://www.ctg.albany.edu/publications/reports/proper_systems?chapter=1).

Multi-state Electronic Signature/Record Reciprocity papers:

- Introduction (https://www.azsos.gov/sites/azsos.gov/files/pa_ec3_e-sign_interop_intro.pdf) (PDF)
- Framework for Electronic Signature Reciprocity (https://www.azsos.gov/sites/azsos.gov/files/pa_ec3_signature_reciprocity.pdf) (PDF)
- Recommendations for E-Sign Infrastructure, Policy Management and Governance in the States (https://www.azsos.gov/sites/azsos.gov/files/pa_ec3_policy_governance.pdf) (PDF)
- Electronic Records Management Guidelines for State Government (https://www.azsos.gov/sites/azsos.gov/files/pa_ec3_records_mgmt.pdf) (PDF)
- Record Retention Analysis Under E-Sign (https://www.azsos.gov/sites/azsos.gov/files/pa_ec3_record_retention_ed.pdf) (PDF)
- Impact of Electronic Signatures on Security Practices for Electronic Documents (https://www.azsos.gov/sites/azsos.gov/files/pa_ec3_security_practices_ed.pdf) (PDF)

- PKI Model Certificate Policy (https://www.azsos.gov/sites/azsos.gov/files/pa_ec3_pki_model_ed.pdf) (PDF)

Now, for what Arizona's Electronic Signature framework looks like. As mentioned, there is a specific statute for state agencies that places responsibiltiy on the Secretary of State to establish policy, procedures and approve signing processes used by agencies. The Admistrative Rules for that legislation (http://apps.azsos.gov/public_services/Title_02/2-12.pdf) establish a Policy Authority (PA) within the Secretary of State which handles this responsibility according to defined PA practices.

Many of the documents on this website define the rules for using particular technologies for signing processes, for example:

Public Key Cryptography (PKC) technologies:

PKI Certificate Policy
PGP Certificate Policy (https://www.azsos.gov/sites/azsos.gov/files/pa_pgp-cp.pdf) (PDF)
PKI & PGP technical standards were established by ADOA-ASET (with the Policy Authority collaborating)

Signature Dynamics technologies

Signature Dynamics Electronic Signing Policy
(https://www.azsos.gov/sites/azsos.gov/files/pa_sigdynamicscp.pdf) (PDF)
(conceptually similar to a Certificate Policy - except there is no certificate)

Note that other technologies, such as the use of PIN or password are unique applications and a generalized policy defining the security and audit requirements can not be developed. The state does permit (and have in use) electronic signing processes that do not conform to established technical standards or have an established audit evaluation process. These signing processes require specific review and specific policies for them to be approved by the Secretary of State.

There are also agency, project and vendor related documents, for example:

Application Form for Certification Authority Approval (https://www.azsos.gov/sites/azsos.gov/files/pa_ca-application.pdf) (PDF)
Certificate Authorities Approved to Issue Certificates
Agency Guidelines
Miscellaneous Exhibits
Definitions and Acronyms

There are also links to various statutes, administrative rules and projects related to electronic signing processes

AZ Electronic Transactions Act (http://www.azleg.gov/ArizonaRevisedStatutes.asp?Title=44) (A.R.S. Title 44, , Chapter 26, Articles 1 through 4)
AZ Electronic Notarization (http://www.azleg.gov/ArizonaRevisedStatutes.asp?Title=41) (A.R.S. Title 41, Chapter 2, Article 3)

The federal electronic signature and e-authentication efforts (https://www.whitehouse.gov/omb/e-gov) can be explored online as well.

Hopefully this introduction gives you a good sense of why the Policy Authority exists and how its policies facilitate the state's use of electronic signatures. Electronic signatures allow agencies to move, as appropriate, from paper based records to more efficient and timely electronic records. Some current electronic signing processes are described here.

Policy Authority Procedures & Practices

Forward (https://www.azsos.gov/sites/azsos.gov/files/policy_authority_procedures_forward.pdf) (9/05/99)

Introduction (https://www.azsos.gov/sites/azsos.gov/files/policy_authority_procedures_introduction.pdf) (9/05/99) a fast "lay of the land" look at Arizona's implementation.

Overview (https://www.azsos.gov/sites/azsos.gov/files/policy_authority_procedures_overview.pdf) (9/05/99) a deeper description of why it is structured the way it is.

Policy Authority Practices (https://www.azsos.gov/sites/azsos.gov/files/pa_PAP.pdf) (PAP version 3.2) (4/25/02) Defines the general procedures the Policy Authority employs to manage electronic signature use within the government of Arizona

Certificate Authorities Approved to Issue Certificates

Approved Certification Authorities for Arizona's electronic signature PKI CP (OID: 2.16.840.3.04.01.002.02.999.00.002)

VeriSign Inc

VeriSign Inc. is the approved PKI certificate authority for the State of Arizona.
For information about obtaining a VeriSign certificate for State Government use, please contact:
Jack Monahan at jmonahan@verisign.com (mailto:jmonahan@verisign.com).
More information about VeriSign including their certification practice statement (https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf) (PDF) can be found on the VeriSign website (http://www.verisign.com/).

Approved CA certificates by Certificate Type

Basic Certificate Type (OID: 2.16.840.3.04.01.002.02.999.00.002.01.01)

- VeriSign Standard

Medium Certificate Type (OID: 2.16.840.3.04.01.002.02.999.00.002.01.02)

- VeriSign Medium

High Certificate Type (OID: 2.16.840.3.04.01.002.02.999.00.002.01.03)

- VeriSign High

ChosenSecurity, Inc.

ChosenSecurity, Inc. is an approved PKI certificate authority for the State of Arizona.

For information about obtaining a ChosenSecurity certificate for State Government use, please contact:

ChosenSecurity, Inc.
57 Wells Avenue Suite 1
Newton, MA 02459
1.866.468.2180
email: info@chosensecurity.com (mailto:info@chosensecurity.com)
web: www.chosensecurity.com (http://www.chosensecurity.com/)

More information about ChosenSecurity including their certification practice statement can be found on the ChosenSecurity website.

Approved CA certificates by Certificate Type

- Class 2, Assurance Level Basic OID 1.2.276.0.44.1.1.6.12.1.
- Class 3, Assurance Level Medium OID 1.2.276.0.44.1.1.6.12.2
- Device Certificates OID 1.2.276.0.44.1.1.6.12.3

PKI Certificate Policy

PKI Certificate Policy *(version 2)*

The *PKI Certificate Policy* defines specific electronic signature implementation types.
PKI Certificate Policy *(https://www.azsos.gov/sites/azsos.gov/files/pa_pki-cp_v2.pdf)* (PDF) (PKI-CP) (9/1/2001)

Arizona's PKI Certificate Policy (PKI-CP) includes a range of certificates (Basic, Medium and High).

Notice of change in Approved Certification Authority Audit Requirements:

Performance Audit Standards For Approval Of Certification Authorities

July 28, 2009

The Secretary of State (in the capacity of Policy Authority) has added an audit type to the Certification Authority audit requirements. The ETSI audit type listed below may now now be subsituted for the WebTrust Audit requirement for CA's.

Acceptable Certificate Authority Audit Types:

- WebTrust for Certificate Authorities v1.0 or later, completed by a licensed WebTrust for CAs auditor,
- ETSI TS 102 042 V1.1.1 or later

Please direct any comments or issues to the policy authority (https://www.azsos.gov/contact/Website-feedback).

Application for becoming an Approved PKI Certification Authority

CA application/acceptance form (https://www.azsos.gov/sites/azsos.gov/files/pa_ca-application.pdf) (PDF) (06/06/02)

PGP Certificate Policy

PGP Digital Signature Certificate Policy for Electronic Signature Use
(https://www.azsos.gov/sites/azsos.gov/files/pa_pgp-cp.pdf) (PDF)

Signature Dynamics Electronic Signing Policy

Signature Dynamics Electronic Signing Policy for Electronic Signature Use
(https://www.azsos.gov/sites/azsos.gov/files/pa_sigdynamicscp.pdf) (PDF)

Definitions and Acronyms

Acronyms

5 Nines - Five Nines (5 9's)
AA – Accreditation Authority
AESI – Arizona Electronic Signature Infrastructure
ARL – Authority Revocation List (PKI)
CA – Certification Authority (PKI)
CM – Certificate Manufacturer (PGP)
CP – Certificate Policy
CPS – Certification Practice Statement (PKI)
CR - Certificate Repository (PGP)
CRL – Certificate Revocation List
CSR – Certificate Signing Request
DN – Distinguished Name
ESI – Electronic Signature Infrastructure

IETF – Internet Engineering Task Force
ISO – International Standards Organization
LRA – Local Registration Authority
NIST – National Institute of Standards and Technology
OID – Object Identifier
OCSP – Online Certificate Status Protocol
PA – Policy Authority
PIN – Personal Identification Number
PKI – Public Key Infrastructure
PKIX – Public Key Infrastructure X.509 as extended by IETF.
RA – Registration Authority
RFC – Request For Comments
rootCA – Root CA (PKI)
RSA – Rivest–Shamir–Adleman (*see* RSA in glossary section)
topCA – Top CA (PKI)
URL – Uniform Resource Locator
VA – Validation Authority

Definitions

5 Nines - refers to a goal of 99.999% uptime, that is, the system is accessible 99.999% of the calendar year (also 5 9's, Five Nines).

Accreditation Authority (AA) – An ESI management Entity with the authority to permit a subordinate ESI Entity to operate within a particular domain. The PA is the accreditation authority for all connections to the AESI. A particular department within an Agency may be assigned the role of accreditation authority for the Level One CA within that Agency.

Activation Data – The private data that are required to access cryptographic modules (password, biometric authentication, any items other than the direct cryptographic keys).

Affiliated Certificate – A certificate issued to an affiliated individual. (*see* Affiliated Individual)

Affiliated Individual – a person affiliated with an organization (i) as an officer, director, employee, partner, contractor, intern, or other role within the organization, or (ii) as a person maintaining a contractual relationship with the organization where the organization has business records providing strong assurances of the identity of such person. (*see* Affiliated Certificate)

Authentication – relates to the process where one party has presented an identity and claims to be that identity. Authentication of a Subscriber by a CA or RA enables the Relying Party to be confident that the assertion is legitimate.

Authenticating Entity – the Entity performing authentication and asserting that the Subscriber is the party they are represented to be.

Authority Revocation List (ARL) – A list of revoked CA certificates. An ARL is a CRL for CA cross–certificates.

Archive – to store records and associated journals for a given period of time for security, backup, or auditing purposes.

Arizona Electronic Signature Infrastructure (AESI) –This is the set of organizations, policies, processes and equipment used to administer Arizona's electronic signature tools and the instruments created from their use. [This is an extension of the definition of PKI to include the fact that Arizona's statute recognizes the possibility of non–PKI based electronic signatures.] The AESI is defined and managed by the Policy Authority with support from the Office of the Secretary of State, ADOA-ASET and State Treasurer's Office as defined in the Administrative Rules and Statute.

Audit – a procedure that validates that appropriate controls are in place. An audit would include recording and analyzing activities to detect intrusions or abuses of the information system. Inadequacies are appropriately reported.

Availability – the extent that information or processes are reasonably accessible and usable as needed by authorized Entities allowing timely performance of time–critical operations.

Binding – an affirmation by a CA (or its LRA) of the relationship between a named Entity and its Public Key.

Certification – The process where a CA issues a Certificate for a Subject's Public Key and sends that Certificate to the Subject for acceptance and, on acceptance, posts that certificate in a Repository. [Some non–AESI systems employ a less restrictive process]

Certificate – The public PKI–based key of a Subscriber (or non–PKI technology based equivalent), together with related information, digitally signed with the private PKI–based key of the Certification Authority that issued it(or non–PKI technology based equivalent). The certificate technology is in accordance with standards established by ADOA-ASET.

The Certificate data record, at a minimum: (a) identifies the Issuing CA; (b) identifies its Subscriber; (c) contains a public key that corresponds to a private key under the control of the Subscriber; (d) identifies its operational period; and (e) contains a Certificate serial number and is digitally signed by the Issuing CA. As used by AESI, the term of "Certificate" refers to certificates that expressly reference the OID of a specific Certificate Policy in the "*CertificatePolicies*" field of a PKI Certificate or the non–PKI equivalent..

Certificate Repository – The party maintaining a list of valid PGP certificates. They may or may not have a CRL or a list of certificates showing when they were valid for validation after the fact.

Certificate Revocation List (CRL) – A list maintained by a Certification Authority of the certificates that it has issued that have been revoked before their scheduled expiration date.

A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made available in a Repository. Each revoked certificate is identified in a CRL by its certificate serial number. When a End–Entity uses a Certificate (e.g., for verifying a Subject's electronic signature), the End–Entity not only checks the certificate signature and validity but also acquires a reasonably current CRL and checks that the certificate serial number is not on that CRL. The appropriate CP and CPS will define what is "reasonably current," but it usually means the most recently–issued CRL. A CA issues a new CRL on a regular periodic basis (e.g., hourly, daily, or weekly). CAs may also issue CRLs when an important key is deemed compromised and the CA wishes to expedite notification of that fact.

On– line methods of revocation notification may be applicable as an alternative CRL in some circumstances. PKIX defines a protocol known as OCSP [OCSP] to facilitate on–line checking of the status of certificates. On–line revocation checking may significantly reduce the delay between a revocation report and the information reaching Relying Parties. This requires a trusted Validation Authority rather than the trust indifference in using a CRL, that is, this method is faster but imposes new security requirements since the Relying Party must trust the on–line Validation Authority while the repository does not need to be trusted.

CA Applicant – an Entity submitting a CA application to the PA requesting to become a CA or subordinate CA under the terms of a CP. (*see* Subscriber)

Certificate Applicant – an Entity requesting the issuance of a Public Key Certificate by an CA. (*see* CA Applicant; Subscriber)

Certificate Application – a request from a Certificate Applicant to a CA for the issuance of a Certificate. (*see* Certificate Applicant; Certificate Signing Request)

Certificate Chain – an ordered list of Certificates containing an End–Entity Subscriber Certificate and CA Certificates (*see* Valid Certificate)

Certificate Expiration – the time and date specified in the certificate when the operational period ends, without regard to any earlier suspension or revocation.

Certificate Extension – a PKI certificate may employ extension fields to convey additional information about the Public Key being certified, the Subscriber, the Certificate Issuer, and elements of the certification process (such as identifying the Certificate Policy by OID).

Standard extensions will be used by CAs within AESI. Custom extensions can also be defined within a Certificate Policy issued by the Policy Authority.

Certificate Hierarchy – the ESI domain of CAs, each categorized with respect to its role in a "tree structure" of subordinate CAs. A CA issues and manages Certificates for End–Entity Subscribers and/or for one or more CAs at the next level. The CP defining an ESI establishes certain uniform practices for addressing issues such as naming, maximum number of levels, etc., to assure integrity of the domain and thereby ensure uniform accountability, auditability, and management through the use of trustworthy operational processes. A CA in an ESI is in a trust hierarchy and shall conform to the practices established in the CP..

Certificate Issuance – the actions performed by a CA creating a certificate and notifying the certificate Applicant (anticipated to become a Subscriber) listed in the Certificate’s contents.

Certificate Management – certificate management includes, but is not limited to, storage, dissemination, publication, revocation, and suspension of certificates. An CA undertakes certificate management functions by serving as a Registration Authority for Subscriber Certificates. A CA designates issued and accepted Certificates as valid by publication to a Repository.

Certificate Serial Number – a value that unambiguously identifies a Certificate generated by a CA.

Certificate Signing Request (CSR) – a machine–readable form of a certificate application. (*see* Certificate Application)

Certification Authority (CA) – An authority trusted by one or more users to issue and manage Certificates and CRLs. Each CA within the AESI may issue certificates under a choice of policies based on the assurance level the CA has been accredited to and the requirements and role of the Subscriber. It is important to note that the CA is responsible for the certificates during their whole lifetime, not just for issuing them.

Certificate Manufacturer (CM)– the Entity that manufactures and delivers PGP Certificates. The Subscriber may do this themselves, but this may be delegated to another. The CM is not responsible for identification and authentication of certificate Subjects, the RA is.

Certificate Manufacturing Authority (CMA) – the Entity that manufactures and delivers the Certificates signed by an CA. The CA may do this itself, but it may subcontract this activity. The CMA is not responsible for identification and authentication of certificate Subjects, the CA is.

Certificate Policy (CP) – a named set of rules that indicates the applicability of a certificate to a particular community with a class of applications having common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic procurement transactions within a given price range.

Certification Authority Software – The cryptographic software required to manage the PKI keys (or non–PKI technology based equivalent) of End Entities.

Certification Practice Statement (CPS) – a statement of the practices that a Certification Authority employs in issuing, suspending, revoking, and renewing Certificates and providing access to them. The CPS is a statement of the CA's practices that fulfill and expand on the specific requirements the Policy Authority has published in the Policy Authority Practices document and in the specific Certificate Policy document that the CPS is bound to.

Class [n] Certificate – A certificate of a specified level of trust (denoted as n).

Compromise – an unauthorized disclosure (or loss of control) of sensitive information may have occurred in violation (or suspected violation) of a security policy *(see* Data Integrity). Usually discussed in terms of compromise of a Certificate's Private Key.

Confidentiality – the need to keep sensitive data secret and disclosed only to authorized parties.

Confirmation Of Certificate Chain – the process of validating a certificate chain and subsequently validating a Subscriber certificate. (*see also* Valid Certificate)

The Relying Party, to authenticate the public key (in each certificate), must confirm that each certificate in the chain is valid, that each was issued within the operational period of the corresponding CA certificate, and that all parties (CAs, Subscribers, and Relying Parties) have operated in accordance with the appropriate CP as well as the appropriate CA's CPS for each certificate in the chain.

Cross–Certificate – A Certificate used to establish a trust relationship between two Certification Authorities.

A Cross–Certificate is a Certificate issued by one CA to another CA which contains a public CA key associated with the private CA signature key used for issuing Certificates. Typically, a cross– certificate is used to allow End Entities in one ESI to communicate security with End Entities in another ESI (but may also occur within a single ESI). Use of a cross–certificate issued from CA#1 to CA#2 allows Entity#a (who trusts, has a Certificate issued by, CA#1) to accept a certificate used by Entity#b (who trusts, hase a Certificate issued by CA#2). Cross–certificates between two CA's can be issued in one direction only, or in both directions. The cross–certification often is for a specific Class or for a specific Class and "higher" so cross–certification involves a "mapping" of Certificate Class attributes between the two CAs to assure a correct match between them.

Cryptographic Algorithm – a clearly defined mathematical computation, that is, a complete set of rules to produce a prescribed result.

Cryptography – is both a mathematical method and a discipline using that method.

- The mathematical method assures the confidentiality and authentication of data by replacing it with a transformed version that can be converted back into the original data but only by someone possessing the appropriate cryptographic algorithm and key for converting it back to the original form.

- The discipline employs the method along with related principles, means, and processes for transforming data to 1) hide its content, 2) prevent it being modified without detection, and 3) prevent unauthorized uses of it.

Data Integrity – Assurance that the data are unchanged from creation to reception.

Digital Signature – The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine: (a) whether the transformation was created using the key that corresponds to the signer's key; and (b) whether the message has been altered since the transformation was made. [Note that Digital Signature is commonly associated with PKI–based technology whereas Arizona recognizes a wider range of possible signature technologies – see Electronic Signature.]

Distinguished Name (DN) – a data set that identifies an Entity in the real world (such as a natural person) in the electronic context. *(e.g.,* countryName=US, state=California, organizationName=Electronic Inc., commonName=JohnDoe).

Electronic Signature – [Note that whereas Arizona recognizes a wider range of possible signature technologies, most common current implementations employ PKI–based technology – see Digital Signature.]

Electronic Signature Infrastructure (ESI) –A set of organizations, policies, processes and equipment established within AESI to administer a specific community or class of applications. [This is an extension of the definition of PKI to include the fact that Arizona's statute recognizes the possibility of non–PKI based electronic signatures.]

Encryption – the process of transforming ordinary text data into an unintelligible form (ciphertext) so the original data cannot be either recovered directly (one–way encryption) or through an inverse decryption process (two–way encryption).

Enrollment – the process of an applicant applying for a Certificate.

Extensions – the extension fields in PKIX based certificates.

End–Entity – An entity that uses the keys and certificates created within the ESI for purposes other than the management of the aforementioned keys and certificates. An End–Entity may be a Subscriber, a Relying Party, a device, or an application.

Entity – Any autonomous element within the Electronic Signature Infrastructure. This may be a CA, an LRA, or an End–Entity.

Five Nines - (see 5 Nines)

Government Information Technology Agency (GITA) – Agency directed by Arizona's CIO.

Issuing Authority Certificate – a certificate issued by an superior IA/CA to a subordinate IA/CA. (*see* Issuing Authority, topCA, Level One CA, and Level Two CA)

Identification / Identify – the process of confirming a person's identity. Certificates facilitate identification in public key cryptography (and non–PKI equivalent systems).

Internet Engineering Task Force (IETF) – is a large, open international community of network designers, operators, vendors, and researchers collaborating on the evolution of the Internet architecture to improve the operation of the Internet.

Issuing CA –the CA that signed and issued the particular certificate. (*see* Issuing Authority)

Issuing Authority (IA) – the CA that signed and issued the particular certificate.

Key Generation – the trustworthy process of creating a Private Key and Public Key pair. The Public Key is supplied to a CA during the certificate application process while the Private Key is only supplied to the Subscriber.

Key Pair – two keys mathematically related such that (i) one key can be used to encrypt a message which can then only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key (or the non–PKI equivalent).

Key Pair Recovery – Some CPs will provide for having key exchange or encryption keys "backed up" or recoverable in case the key is lost and access to previously encrypted information is needed. This will seriously damage any claim for Non–Repudiation and is only used in implementations where the importance of information recovery over–rides the need for Non–Repudiation. The issue is generally to read e–mail or other documents encrypted by or for a particular employee when that employee is no longer available to access the document. In such a case, the Subject's Private Key is backed up by a CA or by a separate key backup system. If Subject or the Subject's employer needs to recover these backed up key materials, the ESI must provide a system that permits the recovery without an unacceptable risk of compromise of the Private Key. Key Pair Recovery

Repositories should never include Certificates where Non–Repudiation is paramount. Inclusion in such a Repository opens a challenge to any claim for Non–Repudiation.

Level One CA – The highest level CA within a State agency. Level One CAs are cross–certified with the AESI and may also be cross–certified with subordinate departmental (Level Two) CAs.

Level Two CA – Any CA within a State agency that is subordinate to the Agency's Level One CA.. Level Two CAs are cross–certified with the Agency (Level One) CAs with that cross–certification process subject to approval by the PA.

Local Registration Authority (LRA) – A person or organization that is responsible for the identification and authentication of certificate Subscribers before certificate issuance, but does not actually sign or issue the certificates. A LRA is delegated certain tasks on behalf of a CA. [see Registration Authority]

Notary - a natural person authorized by State of Arizona to perform notarial services which include witnessing or attesting to signatures.

Non–Repudiation – asserts proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. Only a trier of fact (someone with the authority to resolve disputes) can actually make a determination of nonrepudiation. An electronic signature verified in accordance with the relevant CPS can provide proof in support of a determination of nonrepudiation by a trier of fact, but does not by itself constitute nonrepudiation.

Object Identifier (OID) – The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the AESI PKI they are used to uniquely identify each of the eight policies and cryptographic algorithms supported.

Operational Authority – Agency personnel who are responsible for the overall operation of an AESI CA.

Operational Certificate – a certificate within its operational period at the specified date and time.

Operational Period – the period beginning with the date and time the certificate was issued (or on a later date and time if so stated in the certificate) and ending with the earlier date and time of either when it expired or when was revoked.

Organization – A agency, department, corporation, partnership, trust, joint venture, or other association or governmental body.

Out–of–band – parties communicate by a different method from the current method of communication (e.g., one party using U.S. Postal mail to communicate with the other party while current communication is done online).

Policy Authority (PA) – The State of Arizona body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the AESI.

The PA signs and manages the cross–certificates of State of Arizona Agency Level One CAs. The PA also signs and manages cross–certificates with non–State of Arizona CAs. The PA does not manage any Subscriber certificates.

Private Key – The key of a key pair used to create a digital signature. It is the publicly *unknown* half of the Public/Private key pair employed by PKI technology to uniquely link a key pair to the entity possessing the Private key of the pair while the world possesses the Public key of the pair (used here to also define the non–PKI technology based equivalent of these elements).

Public Key – The key of a key pair used to verify a digital signature. It is the publicly *known* half of the Public/Private key pair employed by PKI technology to uniquely link a key pair to the entity possessing the Private key of the pair (used here to also define the non–PKI technology based equivalent of these elements).

Public Key Infrastructure (PKI) – A set of organizations, policies, processes, and equipment used to administer public/private keys and certificates created from their use. [Note that Arizona's statute recognizes the possibility of non–PKI based electronic signatures.]

"A collection of certificates, with their issuing CA's, subjects, relying parties, RA's, and repositories, is referred to as a Public Key Infrastructure, or PKI." from the IETF draft *Internet X.509 Public Key Infrastructure PKIX Roadmap* (draft–ietf–pkix–roadmap–02.txt)

Registration – The process where a Subject: 1) applies for a Certificate with a CA (directly, or through an RA), and 2) the CA issues a Certificate(s) for that Subject. Registration involves: 1) the Subject's providing the personal information required for the Class of Certificate applied for, and other attributes needed to be put in the Certificate, followed by 2) the CA's (possibly with help from the RA) verifying in accordance with its CPS that the name and other attributes are correct.

Registration Authority (RA) – an entity that may be given responsibility for performing some of the administrative tasks necessary in the registration of Subjects, such as: confirming the Subject's identity; validating that the Subject is entitled to have the attributes requested in a Certificate; and verifying that the Subject has possession of the Private Key associated with the Public Key requested for a Certificate. [see Local Registration Authority]

Relying Party – A person who: 1) uses a certificate signed by a AESI CA to authenticate an electronic signature or to encrypt communications to the certificate Subject, and 2) is a Subscriber of a AESI CA or a ESI that is cross–certified with the AESI.

Repository – A location where CRLs, ARLs and Certificates are stored for access by End–Entities. (*see* Repository Services Provider)

Responsible Individual - represents the sponsoring organization with respect to the issuance and management of certificates. The Responsible Individual is responsible for properly indicating which subscribers are to receive Certificates.

Revocation – A Certificate is expected to be in use for its entire validity period when it is issued. But various circumstances can invalidate a certificate prior to its expiration date. Such circumstances include change of Subject name, change of association between Subject and CA, and compromise or suspected compromise of the Certificate's Private Key. The CA will then need to revoke the certificate. Current protocols define one method of certificate revocation which involves each CA periodically issuing a signed data structure called a CRL (*see* Certificate Revocation List).

Root CA (rootCA) – a CA that is directly trusted by an end entity [the process of securely acquiring the value of a root CA public key requires some out–of–band step(s)]. Note that this term is not meant to imply that a root CA is necessarily at the top of any hierarchy, simply that the CA in question is trusted directly. [For top of a hierarchy CA, see topCA]

Repository Services Provider (RSP) - a Certificate Authority or their agent that maintains the CA's Repository. An RSP by provide services to more than one CA. (see Certificate Authority, Repository)

RSA – An public–key encryption technology developed by RSA Data Security, Inc. The acronym RSA stands for the technique's inventors: Rivest, Shamir, and Adelman. They developed the RSA algorithm from the fact that there is no efficient way to factor very large numbers. Therefore deducing an RSA key requires an extraordinary amount of computer processing power and time. RSA has become the de facto standard for industrial–strength encryption, especially for data sent over the Internet.

Sponsor – A Sponsor in the AESI is the Agency, department or public servant who has nominated that a specific individual or organization be issued a certificate. (e.g., for an employee this may be the employee's manager). In the case of a certificate for a citizen or a commercial enterprise the Sponsor could be the manager of the State of Arizona business unit that has a requirement to communicate with that Entity.

The Sponsor might suggest an appropriate DN for the certificate and will be responsible for either supplying or confirming that the certificate attribute details to the LRA. The Sponsor is also responsible for informing the CA or LRA if the Sponsor's relationship with the Subscriber is terminated or has changed such that the certificate should be revoked or updated.

Subject – a subject is the entity (CA or End–Entity) named in a Certificate. Subjects can be natural persons, devices or even software agents.

Subordinate CA – a CA that is not a rootCA for the End Entity in question. A subordinate CA will usually not be a rootCA for any entity but this is not mandatory

Subscriber – An individual or organization whose Public Key is certified in a Certificate. In the AESI this could be a public servant, a citizen, or a government client or supplier. Subscribers may have one or more certificates from a specific CA associated with them; most will have at least two active certificates – one containing their Electronic Signature verification key; the other containing their Confidentiality encryption key.

Time Stamp – a notation indicating the correct date and time of an action and the identity of the End–Entity that sent or received the time stamp.

Token – a hardware security token containing an End Entity's Private Key(s), Public Key Certificate, and, optionally, a cache of other Certificates, including all certificates in the End–Entity's Certification Chain.

Top CA (topCA) – a CA that is at the top of the ESI hierarchy. Note: this is often also called a "root CA" since, in data structures terms and in graph theory, the node at the top of a tree is the "root". However, to minimize confusion, it is here called the "Top CA" or "topCA" with "root CA" reserved for the CA directly trusted by the user. [Readers should be aware that these terms are not used consistently throughout the Electronic/Digital Signature community. Some documents use "root CA" to refer to what other documents call a "top CA", and "most–trusted CA" to refer to what this and other documents call a "root CA".]

Transaction – an electronic transfer of information (typically over the Internet).

Trust – the assumption that an Entity will behave substantially as expected. Trust may be only extended for one specific function. The key role of this term within Authentication is to describe the relationship between an authenticating Entity and a CA. An authenticating Entity must be certain that it can trust the CA to create only valid and reliable Certificates, and that Relying Parties and other users of those Certificates rely upon the authenticating Entity's determination of trust.

Trusted Person – a person who serves in a trusted position and is qualified to serve in it in accordance with the governing CP and CPS. *(see* Trust; Trusted Position; Trusted Third Party)

Trusted Position – the role within a CA that includes access to or control over operations that may materially affect the issuance, use, suspension, or revocation of certificates.

Trusted Root – a trusted root is the Public Key that an Entity will find reaffirmed as bound to a CA. Software and systems implementing authentication based on PKIX and Certificates assume that this key value has been correctly obtained. It is confirmed by always accessing it from a trusted system Repository that can only be modified by identified and trusted administrators.

Type (Of Certificate) – the critical properties of a certificate that limit its intended purpose to a class of applications uniquely associated with that type. (*see* Class [n] Certificate)

Uniform Resource Locator (URL) – the addressing method used for identifying and locating certain records and other resources located on the World Wide Web.

Validation Authority (VA) –

Valid Certificate – a Certificate that 1) was issued by an Approved CA, 2) was accepted by the Subscriber listed in it, 3) has not expired, and 4) has not been revoked. A Certificate is not "valid" until it is both issued by an Approved CA and been accepted by the Subscriber.

Validate A Certificate Chain - see Confirmation of Certificate Chain.

Verify (A Digital Signature) – to determine for a given digital signature and message that

- the digital signature was created while the Certificate was valid and
- the message has not been altered since the digital signature was created.
- some Certificate Policies will also require Confirmation of the Certificate Chain, that is, that each Certificate in the chain was valid at the time the digital signature was created.