

Government
Information
Technology
Agency

Statewide
STANDARD
P800 – S850 V1.0

TITLE: PKI and PGP Encryption
Technologies

Effective Date: January 10,
2002 DRAFT

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

This standard establishes acceptable criteria for Public Key Infrastructure (PKI) and Pretty Good Privacy (PGP) technology used for ensuring the authenticity, integrity, confidentiality, and reliability of digital transactions conducted with/by the State of Arizona.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology PSPs within each Agency.

4. STANDARD

The State of Arizona is continually moving towards electronic government in its methods of providing benefits and services to the public as well as in conducting business with the Federal government, local governments, and the private sector. As a result of transitioning from face-to-face to online interactions, statewide security must change to ensure identities, authenticity, confidentiality, and reliability of digital information. This standard identifies the minimum acceptable technical features of PKI- and PGP-based digital identity for use by State of Arizona agencies as well as requirements for securing e-mail transmissions.

- 4.1. **PKI-based Electronic Signature Functionality:** The recommended PKI-based technical functionality is defined by Standard X.509 and its extension in the evolving definition developed by the Internet Engineering Task Force (IETF) through their PKIX Standards Development Task Group. This standard provides and defines certified identification of digital signatures having integrity, nonrepudiation, and authentication.
- 4.2. **PGP-based Electronic Signature Functionality:** The recommended PGP-based technical functionality is defined by standards initially developed by Phil R Zimmermann in the early 1990's. The current, open standard, known as the Open Specification for Pretty Good Privacy, is an evolving definition developed by the Internet Engineering Task Force (IETF) through their OpenPGP working group.
- 4.3. **X.509/PKIX:** This document provides technical standards as well as the basic operational framework (PKIX 4) forming a basis for relating the various roles in any use of PKI. The tools will change but the roles of the parties involved will not.

These roles are:

- someone (aka subscriber) needing representation that the package sent is from him/her;
 - someone (aka certificate authority) attesting that the subscriber is who he/she represents himself/herself to be;
 - someone (aka repository authority) attesting that the public key in the repository corresponds to the private key controlled by the party needing representation that the communication sent is from him/her;
 - someone (aka relying party) receiving the communication and needing the assurance of whom it's from and that it is being delivered intact.
- 4.4. **Certificate Verification Meta-Directory:** The State may eventually implement a single, statewide, master X.500/LDAP based meta-directory or repository to validate PKI Certificates and to maintain a PKI Certificate Revocation List (CRL). At that time, State agencies will be required to use that master directory. Until the statewide meta-directory exists, state agencies shall implement such a directory for themselves. Once the statewide meta-directory exists, State agencies may implement their own directory subset for management purposes, but any changes must be communicated to the master directory to be mirrored there.
 - 4.5. **OID (Object Identification):** OID is primarily used for uniquely defining distinguished names and object identifiers. This classification schema builds on the joint US arc of the registration tree established according to CCITT Recommendation X.660 and ISO/IEC Standard 9834-1. Under the joint-ISO-CCITT arc in the registration tree, the US-JRA has registered subauthorities, including states. The base code for the state arcs are defined by FIPS PUB 5-2. The registration sub-authority for Arizona is the Secretary of State and the root Arizona arc is 2-16-840-3-04 (see US-JRA v2.0 page 18 for basic structure and

authority, pages 22 through 24 establish the state-permitted use and delegation). The Certificate Policies (CPs) established by the Secretary of State use OIDs to uniquely identify the Certificate Policy governing specific PKI and PGP Certificates and framework for their legal use (see attached document “Object Identification (OID) Classification Procedure for the state of Arizona”).

4.6. E-Mail Security: S/MIME Version 3, or succeeding approved standards, shall be used to accomplish secure e-mail communications. Even when the contents of an e-mail have been secured via encryption, the message itself is not secure from unauthorized modification during transmission. The S/MIME protocol encompasses encryption, sender authentication, and message integrity services.

- Any email message containing an electronic signature intended to be a legal signature must meet the Electronic Signature Policy Authority’s general operational policy and procedures concerning State use of electronic signatures.

4.7. **Security Levels:** Agencies and the Policy Authority will determine the appropriate security levels for specific PKI and PGP uses. Table 1 (below) provides guidance regarding the major industry algorithms used in support of encryption, message integrity, authentication, and PKI-/PGP-based electronic signatures. Any vendor of electronic signature technology will provide independently validated measures of the level of security achieved by their product. They will provide a table of security levels, should more than one be incorporated or possible using their product or products.

4.7.1. **Encryption, Message Integrity and Authentication** - The vendor assurances of security levels will be used by the Agencies in developing policies and procedures for defining the use of each level of encryption, message integrity, and authentication.

Table 1: Cryptographic Algorithms
 (The terms “Obsolescent, Transitional, Strategic, and Emerging”
 are defined in Definitions and Abbreviations.)

Item	Obsolescent	Transitional	Strategic	Emerging
Public Key	Rivest-Chor Merkle-Hellman	Rabin Diffie-Hellman ElGamal LUC (Lucas sequences)	RSA (Rivest-Shamir-Adleman) DSS (Digital Signature Standard) ECC (Elliptic Curve Cryptosystem)	XTR (Efficient Compact Subgroup Trace Representation) NTRU
Secret Key	RC2	OTP (One Time Pad) DES (Digital Encryption Standard) RC4	3DES (Triple Digital Encryption Standard) IDEA (International Data Encryption Algorithm) Blowfish	AES (Advanced Encryption Standard) Twofish MARS RC6 Serpent
Hash Functions	MD2 (Message Digest 2) MD4 (Message Digest 4)	MD5 (Message Digest 5)	SHA-1 (Secure Hash Algorithm)	RIPEMD-160 (Race Integrity Primitives Evaluation Message Digest)

- 4.7.1.1. The use of cryptology technologies for data storage and data communications (transmission of data) must be based on open standards.
- 4.7.1.2. Each agency should establish a policy and accompanying procedures that address appropriate use of different levels of encryption.
- 4.7.1.3. Each agency should establish an Encryption Key Management policy and procedures to address the integrity and recovery of the “keys.”

4.7.2. **Electronic Signatures** – The vendor assurances of security levels will be used by the Policy Authority and the agencies in developing policies and procedures for defining the use of each level of PKI-/PGP-based electronic signature.

4.8. **Public Key Infrastructure (PKI) Uses** - The technology known as Public Key Infrastructure (PKI) is an acceptable technology for use by budget units in Arizona for electronic signatures, message integrity, sender authentication, and encryption. This specifically requires compliance with X.509 Version 3 (or a succeeding version adopted by the IETF) as incorporated into PKIX. All references to PKI encryption herein require adherence to any statewide encryption standard and any agency- specific encryption standard.

4.8.1. **Electronic Signatures.** The use of PKI for electronic signatures

requires the encapsulation of the message in such a way that altering the message invalidates the electronic signature. As previously noted, the particular policy and processes required are defined by the Policy Authority. The signing process also assures the message integrity and sender authentication described in 4.7.2.

- When PKI is deemed necessary for encryption and used in conjunction with electronic signature, it must involve a different key pair from the signing pair.
- A transient PKI encryption process may use the recipient's signing pair to maintain the confidentiality of the message delivery. However, any non-transient PKI encryption must use a key pair as defined in 4.7.3 below and must not use a key pair approved by the Policy Authority for signing only.

4.8.2. **Message Integrity and Sender Authentication.** The use of public key digital signatures provides a high level of confidence that a digital communication is intact and authentic.

- PKI shall not be used for "legal" signing of an electronic document in accordance with A.R.S. § 41-132, except as defined in 4.7.1 above.

4.8.3. **Encryption.** Any PKI-based encryption keys used for non-transient encryption:

- 4.8.3.1. shall be maintained with a method allowing private key recovery.
- 4.8.3.2. shall not be used for electronic signature purposes ("legal" signing of an electronic document in accordance with A.R.S. § 41-132).

4.9. **Pretty Good Privacy (PGP) Uses** - The technology known as Pretty Good Privacy (PGP) is an acceptable technology for use by budget units in Arizona for electronic signatures, message integrity, sender authentication, and encryption. This specifically requires compliance with OpenPGP as specified by the IETF. PGP is only appropriate for very small, closed communities that have agreed to recognize the use of PGP in that community. PGP is generally not usable in other communities without considerable education and re-verification of key holder identities. All references to PGP encryption herein require adherence to any statewide encryption standard and any agency-specific encryption standard.

4.9.1. **Electronic Signatures.** The use of PGP for electronic signatures requires the encapsulation of the message in such a way that altering the message invalidates the electronic signature. As previously noted, the particular policy and processes required are defined by the Policy Authority. The signing process also assures the message integrity and

sender authentication described in 4.8.2.

- When PGP is deemed necessary for encryption and used in conjunction with electronic signature, it must involve a different key pair from the signing pair.
- A transient PGP encryption process may use the recipient's signing pair to maintain the confidentiality of the message delivery. However, any non-transient PGP encryption must use a key pair as defined in 4.8.3 below and must not use a key pair approved by the Policy Authority for signing only.

4.9.2. **Message Integrity and Sender Authentication.** The use of PGP provides a medium level of confidence that a digital communication is intact and authentic.

- PGP shall not be used for "legal" signing of an electronic document in accordance with A.R.S. § 41-132, except as defined in 4.8.1 above.

4.9.3. **Encryption.** Any PGP-based encryption keys used for non-transient encryption:

- 4.9.3.1. shall be maintained with a method allowing private key recovery.
- 4.9.3.2. shall not be used for electronic signature purposes ("legal" signing of an electronic document in accordance with A.R.S. § 41-132).

4.10. **Electronic Signature Policy Authority:** By statute (A.R.S. § 41-132) and administrative rule, the Secretary of State is the electronic signature Policy Authority and will define and manage the relationships between the parties identified in Section 4.3 (PKIX roles) and their attending rights and obligations. This includes general operational policy and procedure concerning State agencies' use of certificate policies in relation to their need for a range of defined trustworthiness for various types of transactions. These roles apply in any electronic signature use, regardless of the technologies employed.

4.10.1. Certificate Authorities approved by the Policy Authority shall meet verification standards as defined in the IETF PKIX Certificate Management Protocol.

4.10.2. The Policy Authority will be responsible for defining how a Certificate Authority may delegate activities such as Certificate Manufacturing Authority (CMA), Registration Authority (RA), Repository Services Provider (RSP), as well as how a Certificate Authority and Repository Authority may or may not be combined into a single entity.

4.10.3. PKIX/X.509 defines the minimum obligations between the above parties. The Policy Authority shall govern the relevant operational and procedural policies and standards for electronic signature use. The Policy Authority is responsible for establishing the policies and processes that assure the operational integrity of the issuance, acceptance, suspension and revocation of Certificates, as well as the use of Certificate Revocation List(s) (CRL), records archival, disaster recovery planning, and termination of CAs and RAs.

4.11. This standard shall be applied by GITA in the processing of agency IT plans and Project and Investment Justifications (PIJs).

4.12. When planning to meet new requirements or significantly expand existing PKI implementations, the agency shall determine whether the proposed use meets or exceeds these standards and document the project in a PIJ. The agency shall submit the PIJ to GITA for review and approval as well as to the Policy Authority and State Library, Archives and Public Records (SLAPR). The agency must obtain written approval from the Policy Authority and SLAPR for the electronic signature-related portion of the PIJ.

5. DEFINITIONS AND ABBREVIATIONS

5.1. **“Asymmetric Cryptography System”** means an electronically processed algorithm or series of algorithms which utilize two different keys with the following characteristics:

- One key encrypts a given message;
- One key decrypts a given message; and,
- The keys have the property that makes it infeasible to discover one key from merely knowing the other key.

5.2. **“Authentication”** means the process of verifying the identity of a user.

5.3. **“Authorization”** means the process of establishing and enforcing a user’s rights and privileges to access specified resources.

5.4. **“Certificate Policy”** means the formal document that describes the various roles involved in creating, maintaining, and validating certificates. It also specifies obligations associated with the roles and which parts of the process may be delegated.

5.5. **“Certification Authority”** means a person or entity that issues, revokes, and manages a PKI certificate.

5.6. **“Critical” (or Mission Critical)** refers to those information resources whose unavailability or improper use has the potential to adversely affect the ability of an agency to accomplish its mission.

- 5.7. **“Emerging”** refers to one of four categories used in the PSP program to guide technology use in the State of Arizona (see also obsolescent, strategic, and transitional). “Emerging” implies that the State’s Enterprise Architecture promotes only evaluative deployments of this technology. This technology may be in development or may require evaluation in government and university settings.
- 5.8. **“Encryption”** means a method of electronically processing a message so that the algorithm used to encode the message is infeasible to decipher without the corresponding decryption algorithm.
- 5.9. **“Key Pair”** means a private key and its corresponding public key in an asymmetric crypto-system. The key pair is unique in that the public key can verify a digital signature that the private key creates.
- 5.10. **“Obsolescent”** refers to one of four categories used in the PSP program to guide technology use in the state of Arizona (see also emerging, strategic, and transitional). “Obsolescent” implies that the State’s Enterprise Architecture actively promotes that agencies employ a different technology. Agencies should not plan new deployments of this technology and instead should develop a plan to replace it. This technology may be waning in use or no longer supported.
- 5.11. **“Open Standard”** means a standard that is not proprietary to a specific manufacturer, vendor, product, or owner, but may be used among various components and products such that it facilitates interoperability; and that has been approved by an appropriate national or international standards body.
- 5.12. **“Owner”** means that group (i.e., Agency or Agency unit) which controls a set of information resources and determines its level of criticality and sensitivity. As such, they determine access, authorization rights, and dissemination regarding those resources.
- 5.13. **“PGP Certificate”** means an electronic record which includes (but is not limited to)¹:
- The PGP version number — this identifies which version of PGP was used to create the key associated with the certificate.
 - The certificate holder's public key — the public portion of the subscriber’s key pair, together with the algorithm of the key: RSA, DH (Diffie-Hellman), or DSA (Digital Signature Algorithm).
 - The certificate holder's information — this consists of "identity" information about the user, such as his or her name, user ID, photograph, and so on.

¹ For more detail, refer to “How PGP Works” by PGP International, <http://www.pgpi.org/doc/pgpintro/>

- The digital signature of the certificate owner, also called a self-signature — this is the signature using the corresponding private key to the public key associated with the certificate.
 - The certificate's validity period — the certificate's start date/time and expiration date/time.
 - The preferred symmetric encryption algorithm for the key — indicates the encryption algorithm to which the certificate owner prefers to have information encrypted. The supported algorithms are CAST, IDEA or Triple-DES.
 - Conformance to IETF OpenPGP standards².
- 5.14. **“PKI Certificate”** (also known as an X.509 Certificate) means an electronic record which:
- Identifies the certification authority issuing it,
 - Names or identifies its subscriber,
 - Contains the subscriber’s public key,
 - Is electronically signed by the certification authority issuing it, and
 - Conforms to X.509/PKIX standards³.
- 5.15. **“Policy”** means any general statement of direction and purpose designed to promote the coordinated planning, practical acquisition, effective development, and efficient use of information technology resources.
- 5.16. **“Policy Authority”** means the Secretary of State acting as the authoritative party designated in Arizona’s Statute (A.R.S. § 41-121 and A.R.S. § 41-132) and Administrative Rules for Electronic Signatures to establish policies and procedures for the use of electronic and digital signatures.
- 5.17. **“Pretty Good Privacy (PGP)”** means a non-PKI implementation of asymmetric cryptography. Note that PGP recognizes two different certificate formats:
- PGP certificates and
 - X.509 (PKI) certificates.
- 5.18. **“Private Key”** means the privately held key of a key pair used to create a digital signature.
- 5.19. **“Public Key”** means the public key of a key pair used to verify a digital signature.
- 5.20. **“Public Key Infrastructure (PKI)”** means “a collection of certificates, with their issuing CA's, subjects, relying parties, RA's, and repositories.”⁴

² See <http://www.ietf.org/html.charters/openpgp-charter.html>

³ See <http://www.ietf.org/html.charters/pkix-charter.html>

- 5.21. **“Repository Authority (RA)”** means the party that validates the electronic signature for a relying party. It is generally an online source of up-to-date information about certificates, their current reliability, and other related information.
- 5.22. **“Relying Party”** means the party receiving the message incorporating the electronic signature and relying on it to authenticate the message’s asserted ownership.
- 5.23. **“Sensitive Information”** means any confidential or critical information for which the loss, misuse, unauthorized access to, modification of or improper disclosure of could adversely affect the State of Arizona’s interest, the conduct of agency programs, or the privacy to which individuals are entitled.
- 5.24. **“S/MIME” is the abbreviation for Secure Multi-Purpose Internet Mail Extensions, an application security protocol used primarily for email communications. It uses the uses the Rivest-Shamir-Adleman (RSA) encryption system to secure MIME-standard transmissions and has itself been proposed as a standard to the Internet Engineering Task Force (IETF).**
- 5.25. **“Standard”** means a directive or specification whose compliance is mandatory, and whose implementation is deemed achievable, measurable, and auditable for compliance.
- 5.26. **“Strategic”** refers to one of four categories used in the PSP program to guide technology use in the State of Arizona (see also emerging, obsolescent, and transitional). “Strategic” implies that the State’s Enterprise Architecture promotes use of this technology by agencies. New deployments of this technology are recommended.
- 5.27. **“Subscriber”** means a person who:
- Is the subject listed in a certificate,
 - Accepts his or her own certificate, and
 - Holds a private key which corresponds to a public key listed in that certificate.
- 5.28. **“Transitional”** – refers to one of four categories used in the PSP program to guide technology use in the State of Arizona (see also emerging, obsolescent, and strategic). “Transitional” implies that the State’s Enterprise Architecture promotes other standard technologies. Agencies may be using this technology as a transitional strategy in movement to a strategic technology. This technology may be waning in use or no longer supported.

⁴ From the IETF draft *Internet X.509 Public Key Infrastructure PKIX Roadmap* (draft-ietf-pkix-roadmap-02.txt)

- 5.29. “User” means an individual or group who has access to an information system or its data.
- 5.30. “X.509/PKIX” means the specific set of technical standards, defined by the Internet Engineering Task Force (IETF) through their PKIX standards development task group, that are based on and extend the X.509 standards adopted by the International Telecommunication Union, formerly known as the International Telegraph and Telephone Consultation Committee. Any reference to X.509 in this standard refers to Version 3 (or a succeeding version adopted by the IETF). Compliance with only Version 1 or 2 shall not be construed as compliance with X.509.

6. REFERENCES

- 6.1 A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions.”
- 6.2 A. R. S. § 41-1335 ((A (6 & 7))), “State Agency Information.”
- 6.3 A. R. S. § 41-1339 (A), “Depository of State Archives.”
- 6.4 A. R. S. § 41-1461, “Definitions.”
- 6.5 A. R. S. § 41-1463, “Discrimination; unlawful practices; definition.”
- 6.6 A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities.”
- 6.7 A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability.”
- 6.8 A. R. S. § 41-3501, “Definitions.”
- 6.9 A. R. S. § 41-3504, “Powers and Duties of the Agency.”
- 6.10 A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”
- 6.11 A. R. S. § 44-7041, “Governmental Electronic Records.”
- 6.12 Arizona Administrative Code, Title 2, Chapter 7.
- 6.13 Arizona Administrative Code, Title 2, Chapter 10.
- 6.14 Arizona Administrative Code, Title 2, Chapter 18.
- 6.15 Statewide Information Technology Policy P100.
- 6.16 Statewide IT Security Policy P800.
- 6.17 State of Arizona Target Security Architecture,
http://gita.state.az.us/enterprise_architecture.
- 6.18 A.R.S. § 41-132 Electronic and Digital Signatures
- 6.19 Arizona Administrative Code Title 2, Administration, Chapter 12, Office of the Secretary of State, Article 5, Electronic Signatures.
- 6.20 Secretary of State Electronic Signature Policies and Procedures
(<http://www.sos.state.az.us/pa>)
- A. Policy Authority Procedures – Introduction
 - B. Policy Authority Procedures for AESI – Overview
 - C. Policy Authority Procedures – Forward
 - D. Policy Authority Procedures; Section 3.6 – Identification and Authentication
 - E. PKI Certificate Policy (in “Certificate Policy”)
 - F. PGP Certificate Policy
 - G. Considerations for Agencies Contemplating Electronic Signature Pilot Projects

- H. Arizona Electronic Signature Infrastructure (AESI) – Definitions and Acronyms
- I. Arizona Electronic Signature Infrastructure (AESI) – Miscellaneous Exhibits

7. **ATTACHMENTS**

Attachment A -- "Object Identification (OID) Classification Procedure for the State of Arizona."

Object Identification (OID) Classification Procedure**ATTACHMENT A****Object Identification (OID) Classification Procedure for the State of Arizona
Initial Implementation
September 2001****OID schema**

OID is primarily used for uniquely defining Distinguished Names and Object Identifiers. This classification schema builds on the joint US arc of the registration tree established according to CCITT X.660 Recommendation and ISO/IEC 9834-1 Standard. Under the joint-ISO-CCITT arc in the registration tree, the US-JRA has registered sub-authorities, including states. The base code for the state arcs are defined by FIPS PUB 5-2. The registration sub-authority for Arizona is the Secretary of State with the root Arizona arc being 2-16-840-3-04 (see US-JRA v2.0 page 18 for basic structure and authority, pages 22-24 establish the state permitted use and delegation)¹.

The registration sub-authority (or delegated party) shall keep a database which contains all registered Organization Names (both numeric and alphanumeric) along with the data elements defined in Appendix C of US Registration Authority Procedures. Note that there are several prospective uses purposed for the alphanumeric name, the key one being as the Distinguished Name in the OSI directory (as such, number of character limitations should be considered when creating such a name).

Arizona's arc will follow a model implied by the ISO/CCITT arc. There will be alternating class type (object association) and class identifier (object) assignments in the arc. The first numeric assignment after 2-16-840-3-04 will identify the type of entity within the state.

- 01 = (EB) exec branch (non-educational – not universities, colleges, etc)
- 02 = (LB) legislative branch
- 03 = (JB) judicial branch
- 04 = (CO) county
- 05 = (CI) city [and similar subdivisions]
- 06 = (OP) other public entities
- 07 = (NP) non-profit entities
- 08 = (PB) private business (corp., LLC, etc)
- 09 = (PC) private citizen
- 10 = (EE) exec branch (educational – universities, colleges, etc)
- 00 = (SO) state object

The following numeric assignment will be for the particular entity.

examples:

2-16-840-3-04-01-001 = Office of the Governor

2-16-840-3-04-01-002 = Secretary of State

etc.

The following numeric assignment will be for subdivision types of this entity

01 = person

02 = division of organization

¹ The Certificate Policies (CPs) established by the Secretary of State use OIDs to uniquely identify the Certificate Policy governing specific PKI and PGP Certificates and the framework for their legal use.

Object Identification (OID) Classification Procedure

00 = object of the entity

The following numeric assignment will be for objects/entities as designated examples:

2-16-840-3-04-01-001-01-001 = the Governor

2-16-840-3-04-01-002-01-001 = the Secretary of State

2-16-840-3-04-01-002-01-002 = the Assistant Secretary of State

2-16-840-3-04-01-002-02-999 = Policy Authority

2-16-840-3-04-01-002-02-002 = Elections Division

2-16-840-3-04-01-002-00-001 = SecState web server 1

2-16-840-3-04-01-002-02-002-01-001 = Elections Division Manger

2-16-840-3-04-01-002-02-002-00-001 = Elections Division web server 1

Note that any sub-tree could be repeated under another tree. For example, while cities are defined at the top state entity level, they could be a subset under counties as well. Private citizens and businesses are also defined at the top state entity level but they could be subsets under counties, and they could also be subsets under cities.

Linking OID assignment to LDAP Distinguished Names (DN)

LDAP relies on DN and RDN (Relative Distinguished Name) to define unique entries in the directory schema. The common elements for mapping between LDAP DN and OID alphanumeric assignments are:

(LDAP element = OID element)

cn=CommonName

sn=Surname

l=LocalityName

st=StateName

o=OrganizationName

ou=OrganizationUnitName

c=CountryName

street=StreetAddress

uid=UserIdentifier

The suggested policy is that the registered OID alphanumeric arc is the LDAP DN.

(The alphanumeric naming will ignore the object association elements of the arc

And the LDAP entry will have an object association type field.)

The DN is basically a concatenation of the unique names in the OID arc:

cn = John Smith

sn = Smith

serialNumber = 123

uid = Smith + 123

ou=ISD

ou=ADOA

o=Arizona

DN: uid = Smith + 123, ou=ISD, ou=ADOA, o=Arizona

Object Identification (OID) Classification Procedure

Note that the common name for persons is not unique and cannot be used to uniquely identify the DN. We will need an agreed common serial number schema for the upper tier persons (DMV?) and companies (SoS/CC?).

Note this requires that a serial number be used one time only at a particular arc point.

Forward thinking issues

Consideration needs to be given to the mapping of this approach to the Common Information Model (CIM). This is a relatively new object modeling method attempting to model all objects within an organization's business process in one unified model. The LDAP DN and object association type field values should be designated according to a CIM schema.

Concluding comments

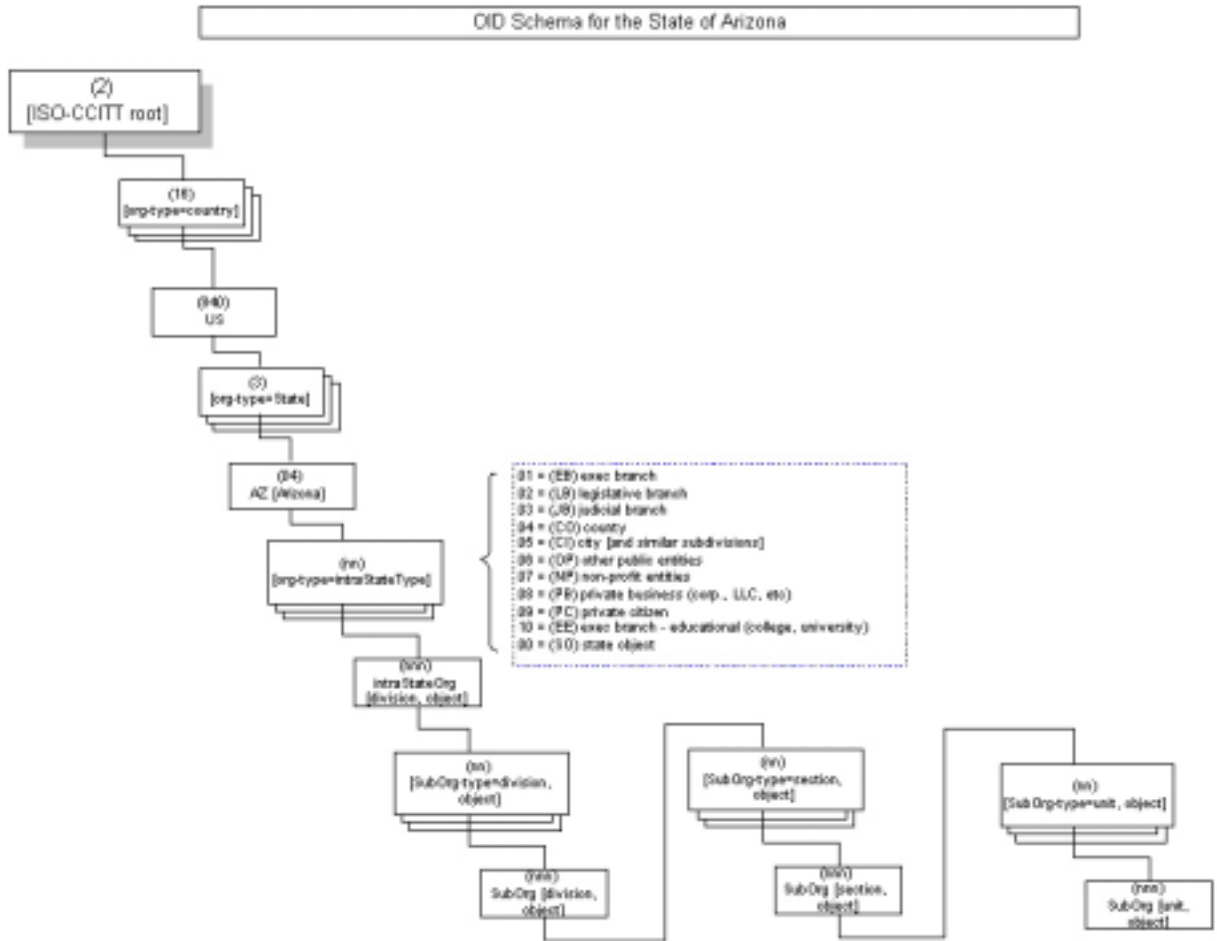
A close review of this schema will show that object associations are not differentiated. This is intentional. OID assignment and naming needs to be permanent. Placing object association names in that assignment limits our ability to remodel our object associations. This schema contemplates a unique ID being associated with an object but with the detailed object class association done within the LDAP description and mapped in CIM. Identifying (and naming) the object class associations that are common across organizations is beyond the scope of this schema definition project. The intent here is two fold: establish a unique identifiers schema (OID) and then uniquely link the names in that schema to real world object mapping (LDAP) and modeling (CIM) schema.

There is a proposal under consideration by IETF for a LDAP-OID Filter/Match standard. This proposal would lead to an open standard for automating the matching between OID and DN that this paper contemplates. This automation would simplify unique naming assignments in both and allow for common policy management through a common CIM model. A common CIM model simplifies, among other things, a common user security implementation across all users and systems (a common authentication and access module). Note that OID, LDAP and CIM are open standards with the related vendor communities actively involved in the formation and support of those standards.

Note that this schema is open to *any* entity wishing to register an OID within the Arizona arc. It is recommended that a multi-jurisdictional task team attempt to identify the object class associations that are common across organizations within this schema.

The following two graphics illustrate the OID schema within the State of Arizona.

Object Identification (OID) Classification Procedure



Object Identification (OID) Classification Procedure

