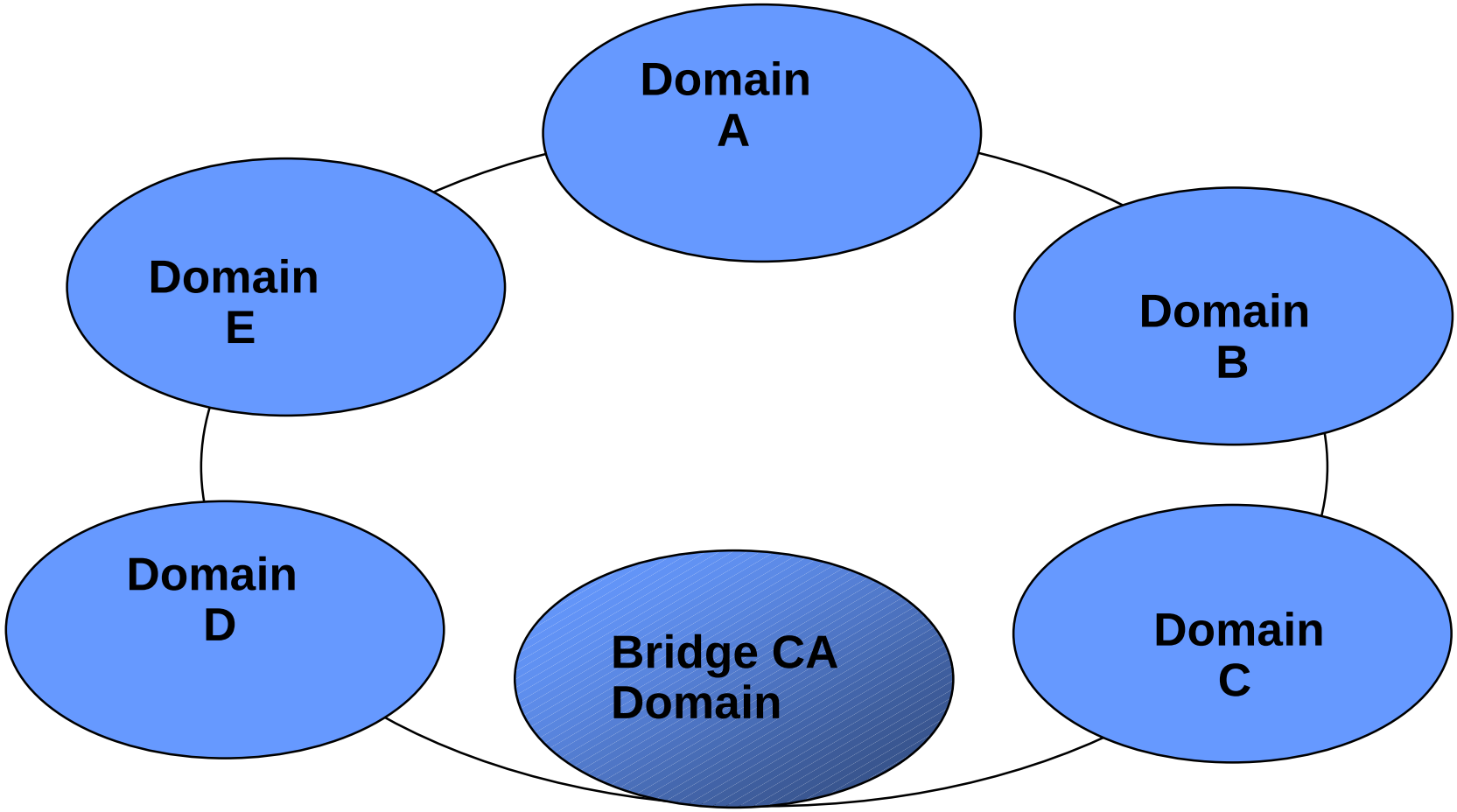
Directory Interoperability: Requirements, Standards and Conformance (or, “PICS”)

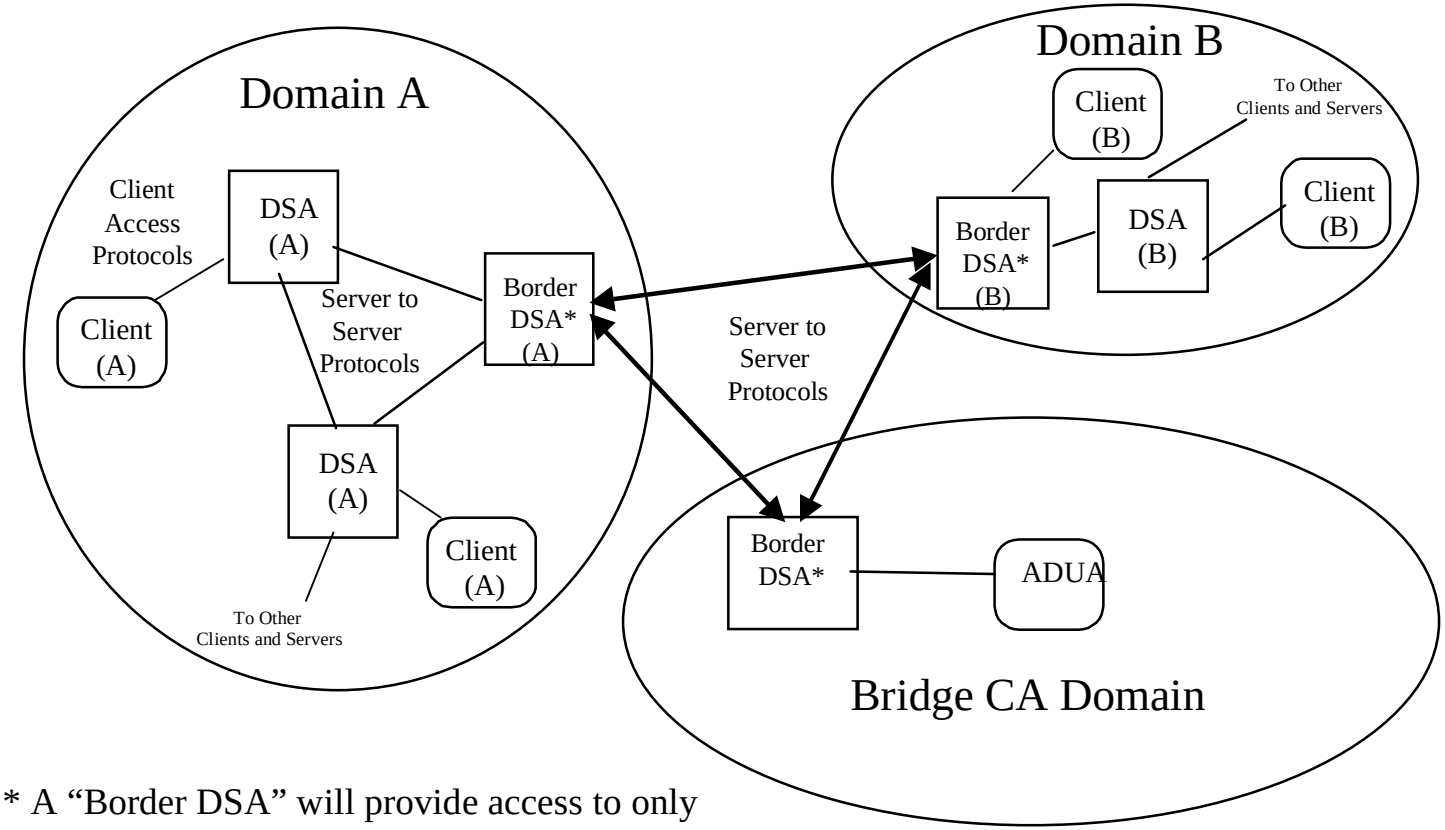
Sandi Miklos, Technical Director
Security Management Infrastructure
National Security Agency
samiklo@missi.ncsc.mil

14 January 1999

Directory Domains

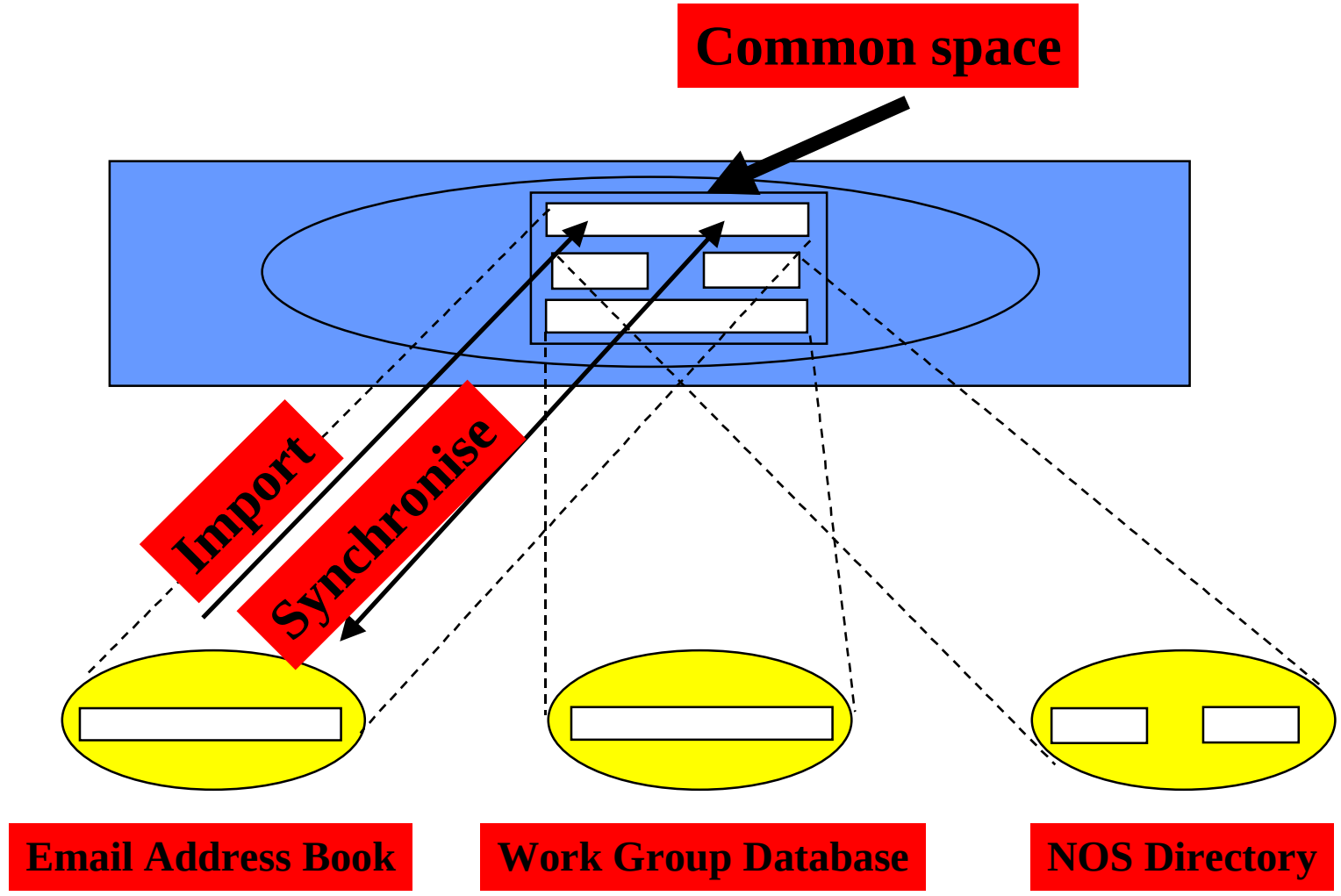


Fundamental Premise: NO Client accesses between domains - DOES THIS INCLUDE THE BRIDGE CA?

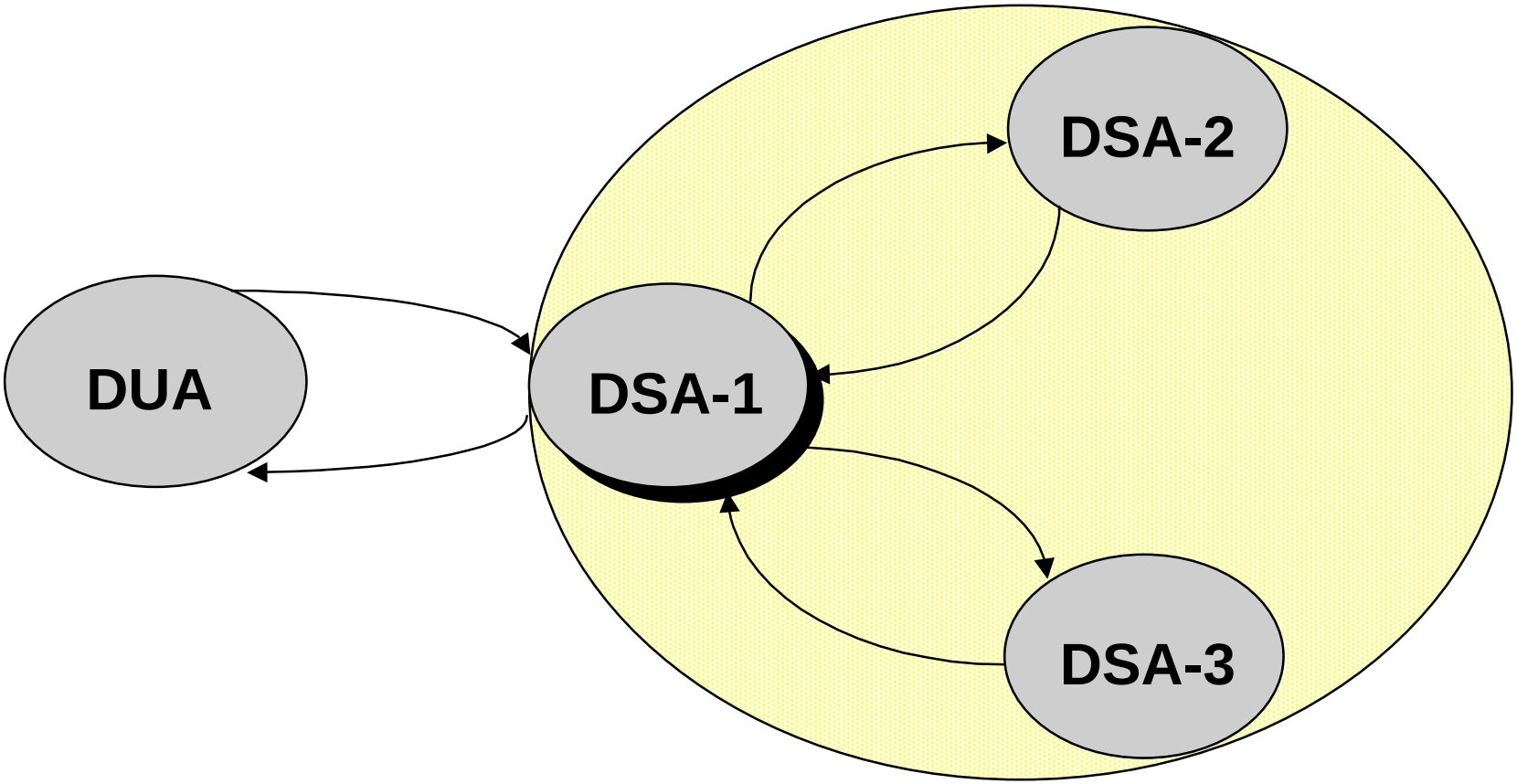


* A "Border DSA" will provide access to only a subset of the DIB held by its domain, and may support multiple security mechanisms.

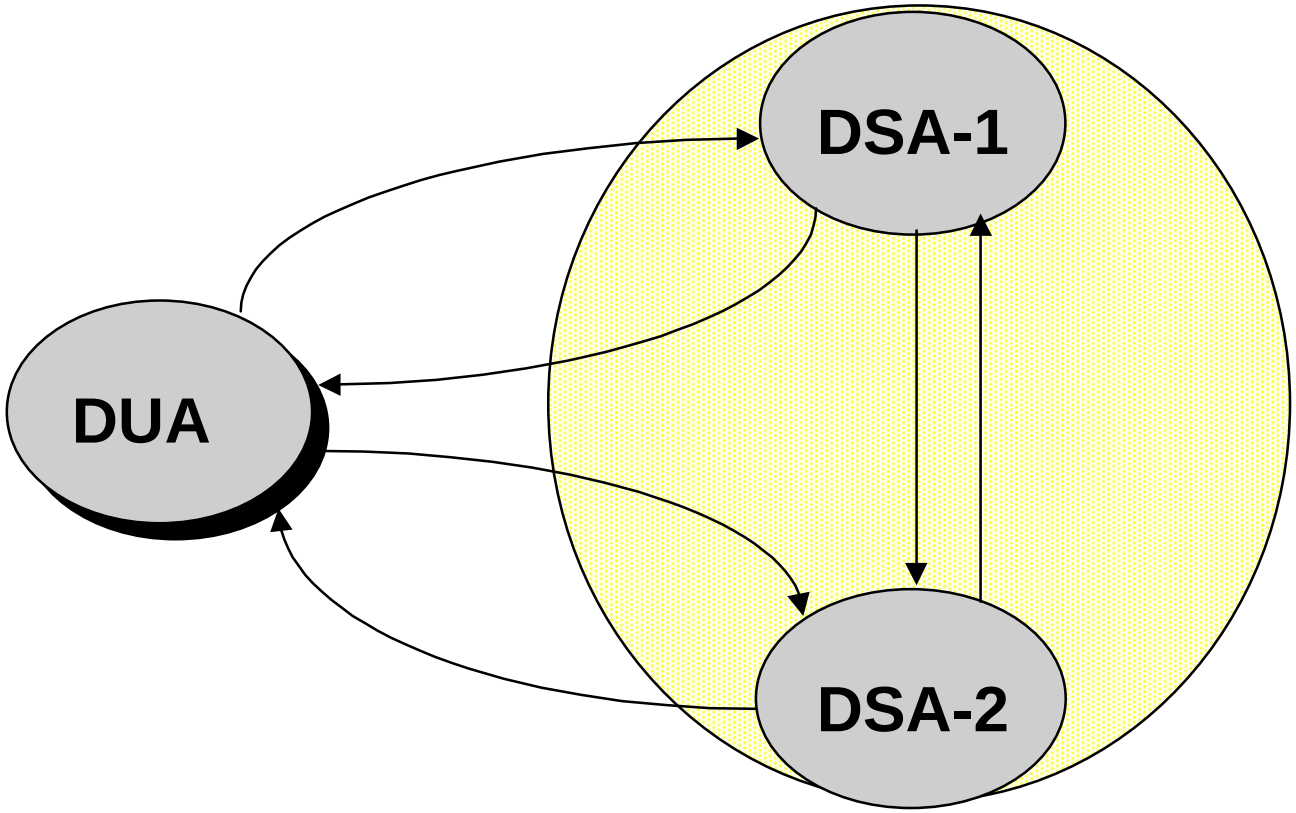
Domain Directory



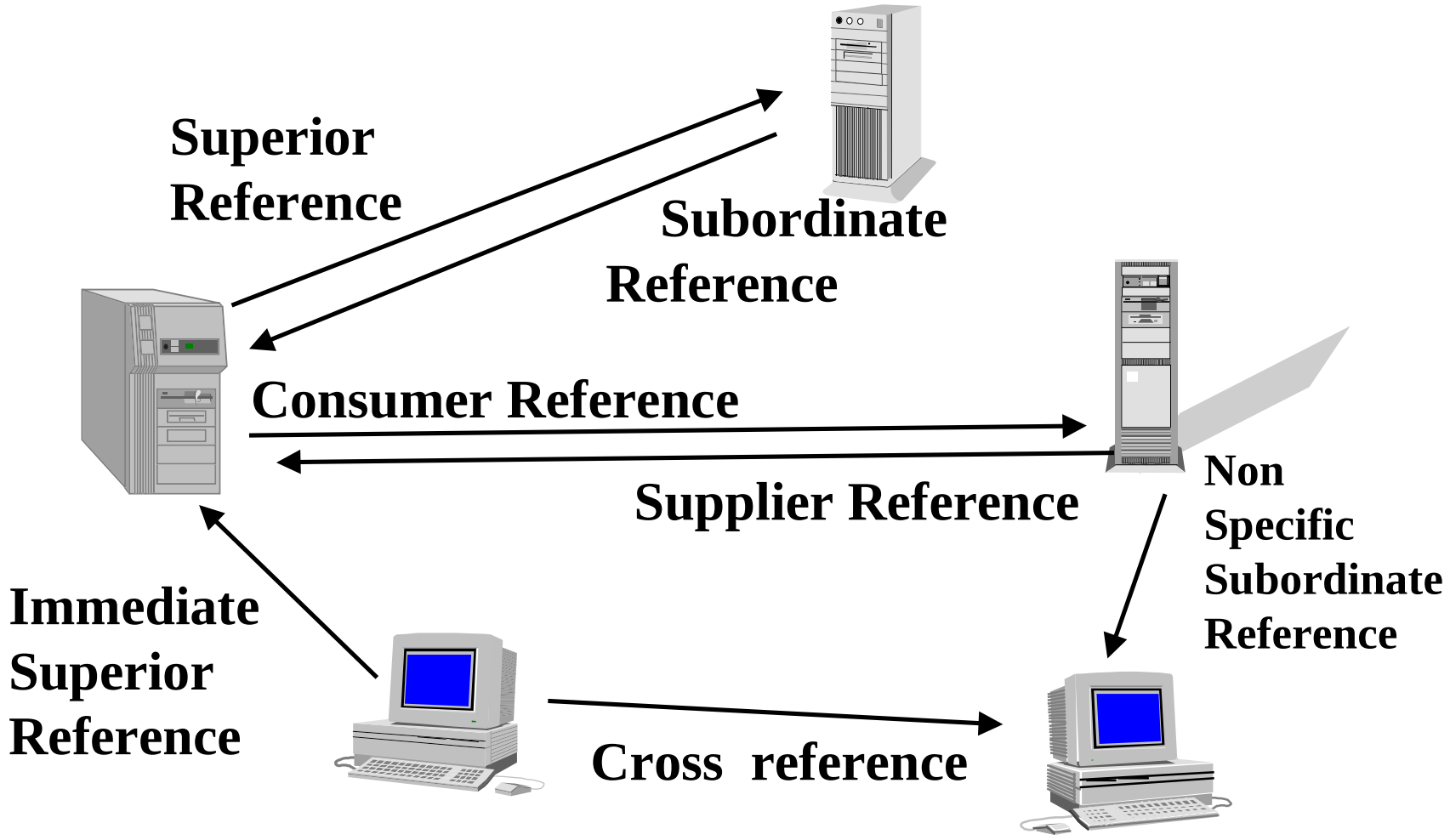
Chaining



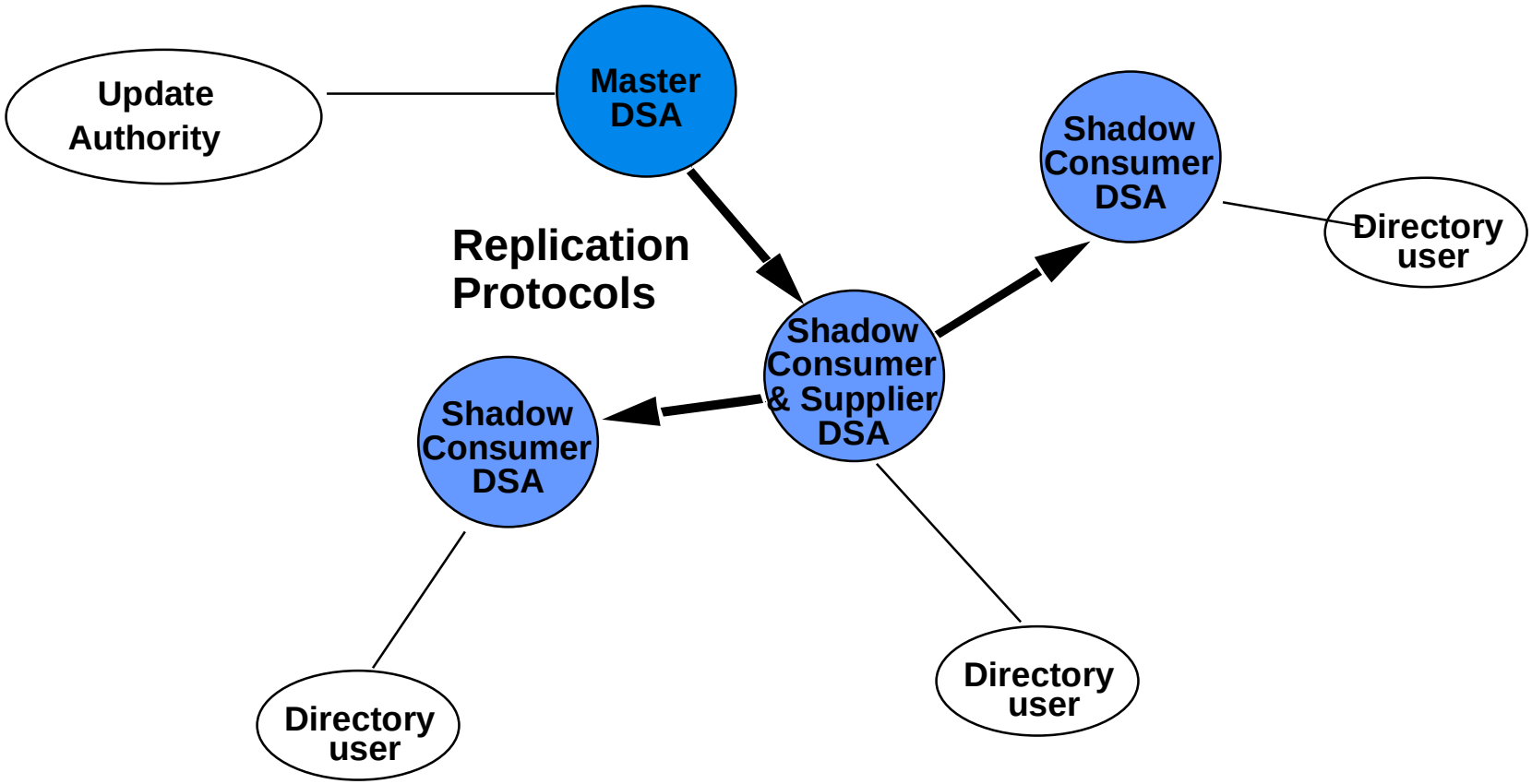
Referrals



KNOWLEDGE REFERENCES



Shadowing


Update Authority
Master DSA
Replication Protocols
Shadow Consumer DSA
Directory user
Shadow Consumer & Supplier DSA
Shadow Consumer DSA
Directory user
Directory user

Service Controls

- preferChaining
- chainingProhibited*
- localScope
- dontUseCopy*
- dontDereferenceAliases
- subentries
- copyShallDo
- priority
- timeLimit*
- sizeLimit*
- scopeOfReferral
- attributeSizeLimit

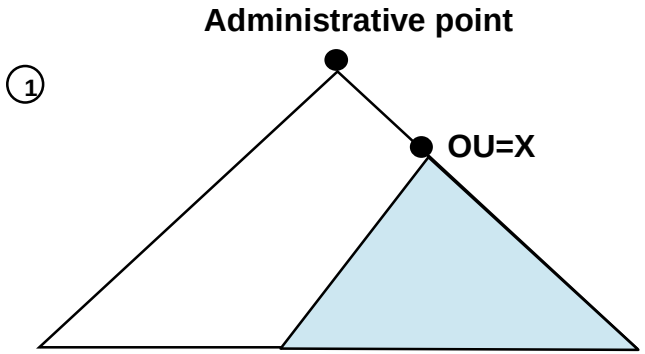
Shadowing agreements

- Made between DSA administrators
- May be activated by a shadowing operational binding or they may be made via a method outside the scope of the standard
- Required before shadowed information may be shared between any pair of DSAs
- Establishes technical parameters of the agreement
  - update frequency
  - replicated area
  - information to be shadowed

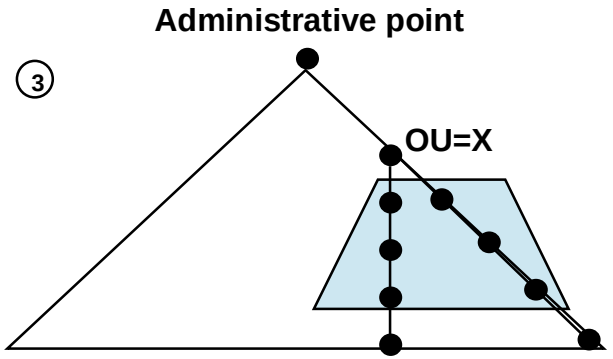
Updating the shadowed information

- Synchronizing the DSAs
  - Coordination of Update operation
  - Requesting Update operation
- Transferring the Shadowed Information
  - What's reliability criteria that transfer as well as database update occurred?
- Types of updates
  - Incremental refresh/delta changes only
  - Total refresh/ all shadowed information sent again

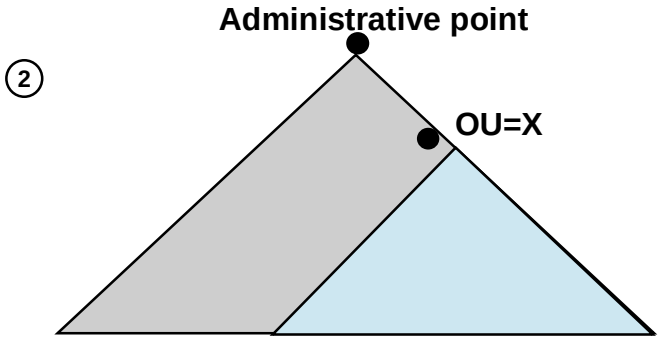
Example: subtree specification



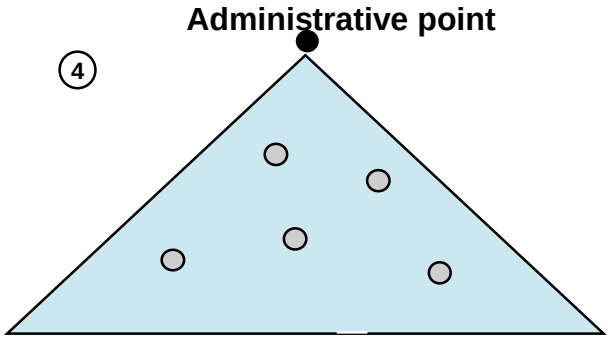
Subtree Specification
base is OU=x



Subtree Specification
base is OU = x
chop minimum is 1
chop maximum is 3

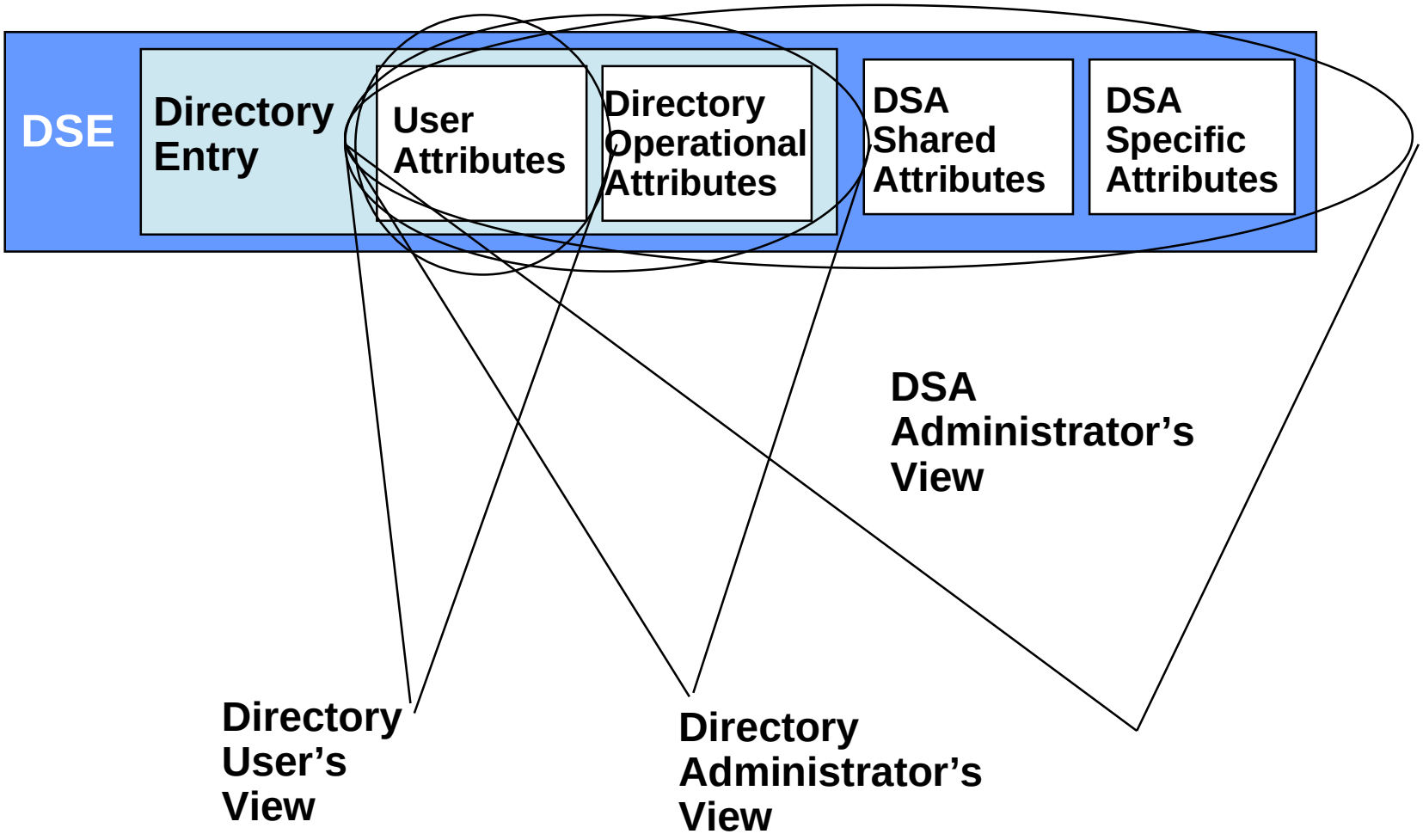


Subtree Specification
chop after OU=x



Subtree Specification
filter on object class = organizationalPerson

Various views of a DSE's attributes



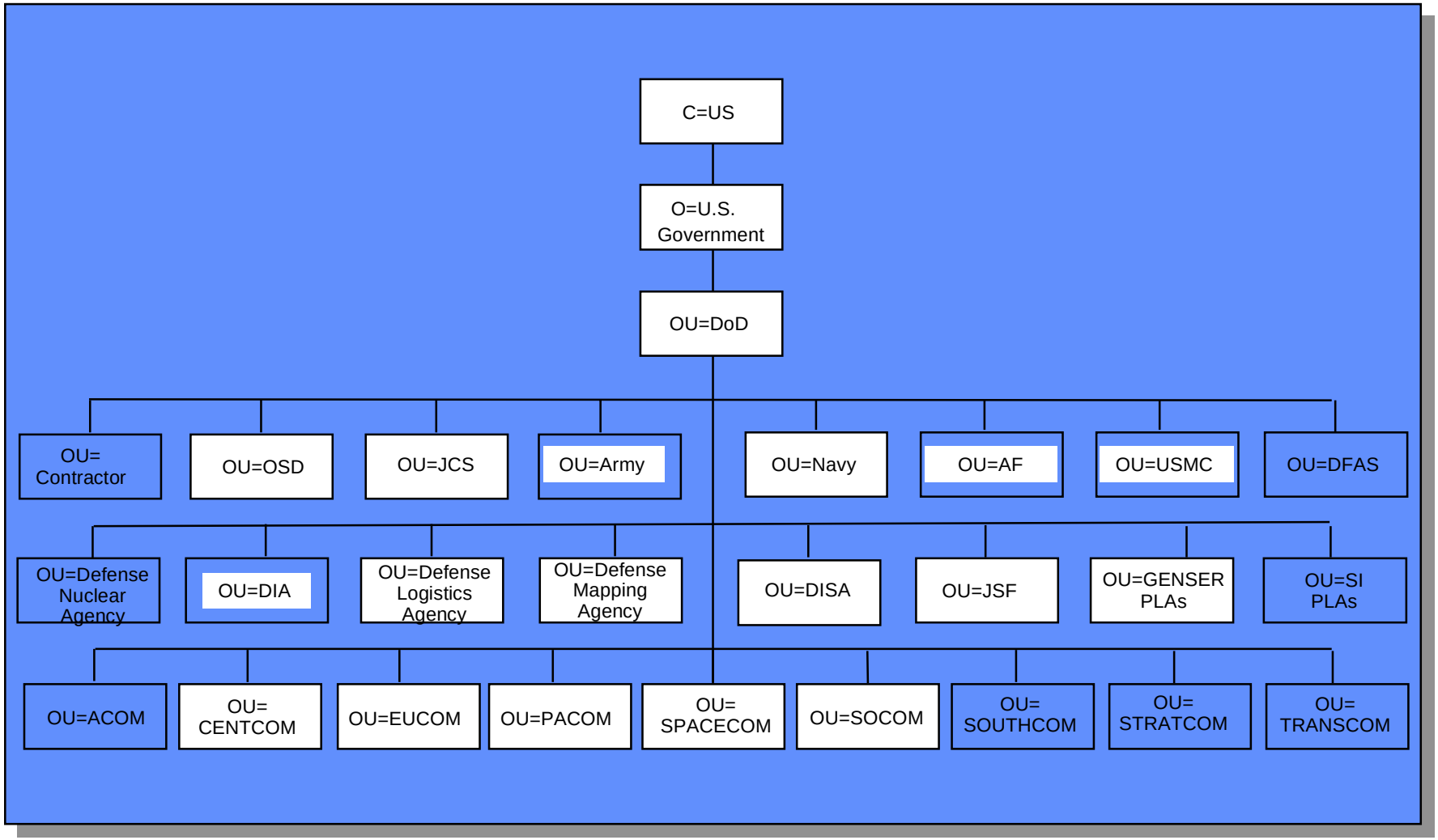
DSE types

- root — root DSA
- glue — knowledge of a name only
- cp — context prefix
- entry — object entry
- alias — alias entry
- subr — subordinate reference
- nssr — non-specific subordinate reference
- supr — superior reference
- xr — cross reference
- admPoint — administrative point
- subentry — subentry
- shadow — shadow copy
- immSupr — immediate superior reference
- rhob — relevant hierarchical operational binding information
- sa — subordinate reference to alias entry

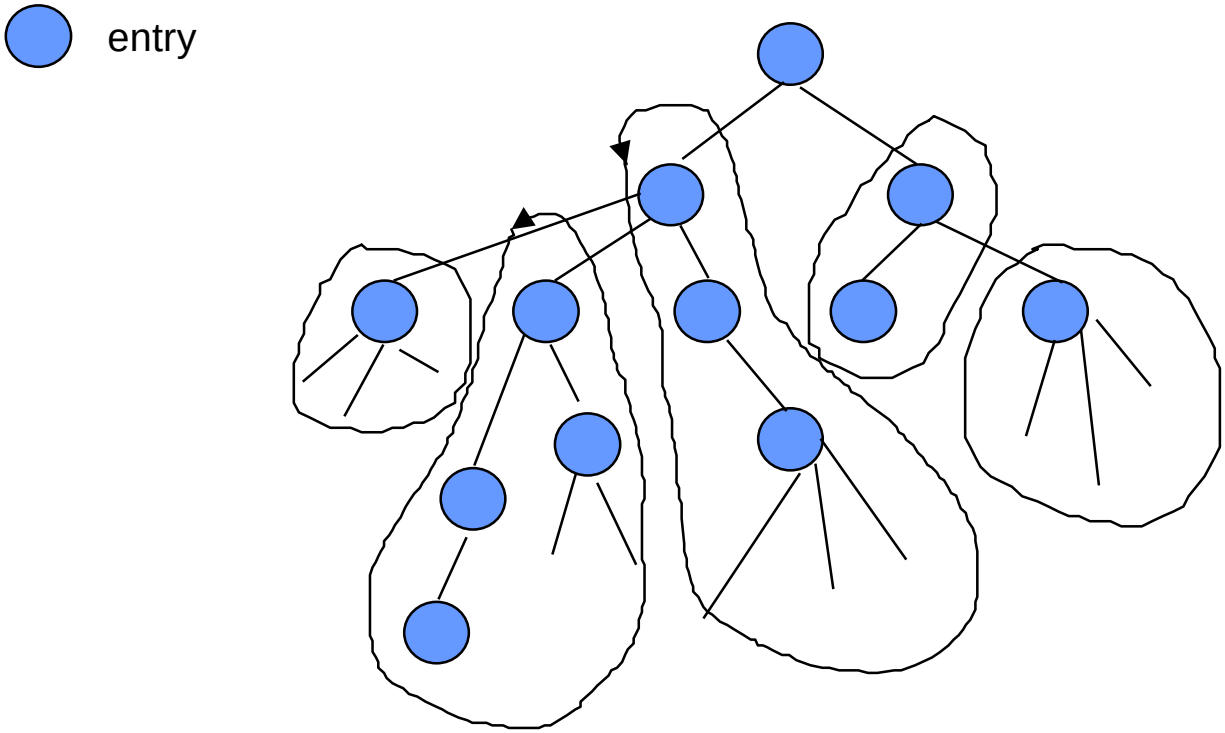
Operational attributes

- Attributes representing operational or administrative information; not normally visible to the user
- Examples:
  - Creation Timestamp
    - records when the entry was first created
  - Modify Timestamp
    - records when the entry was last modified
  - Creator’s Name
    - distinguished name of user that created the entry
  - Modifier’s Name
    - distinguished name of user that last modified the entry
  - EntryACI
    - access control information that applies to this entry only

Directory Information Tree (DIT)

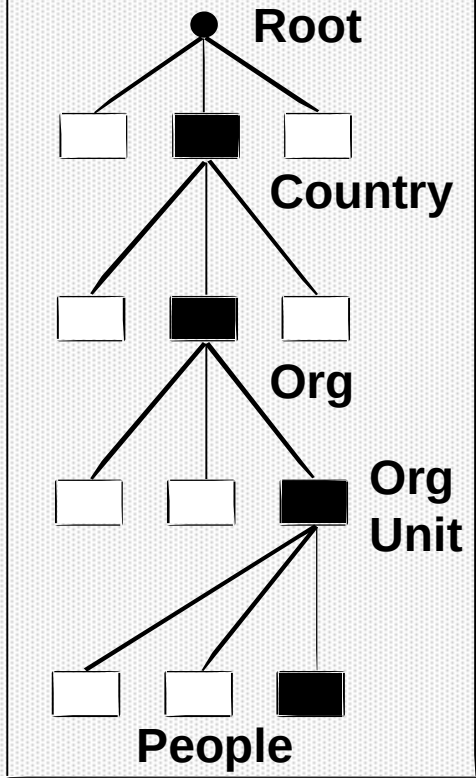


Naming Context



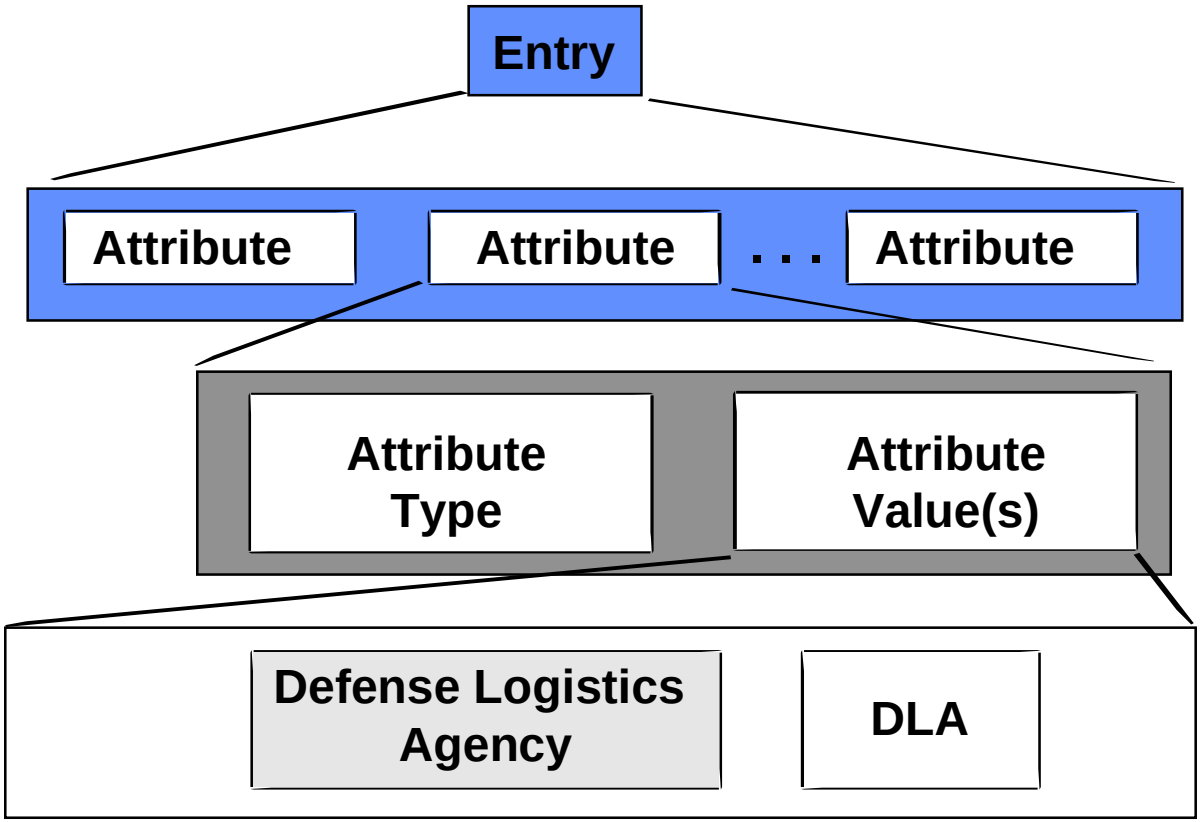
Part of a DIT showing allowed subtrees or naming contexts.

Distinguished Name (DN) and Relative Distinguished Name (RDN)

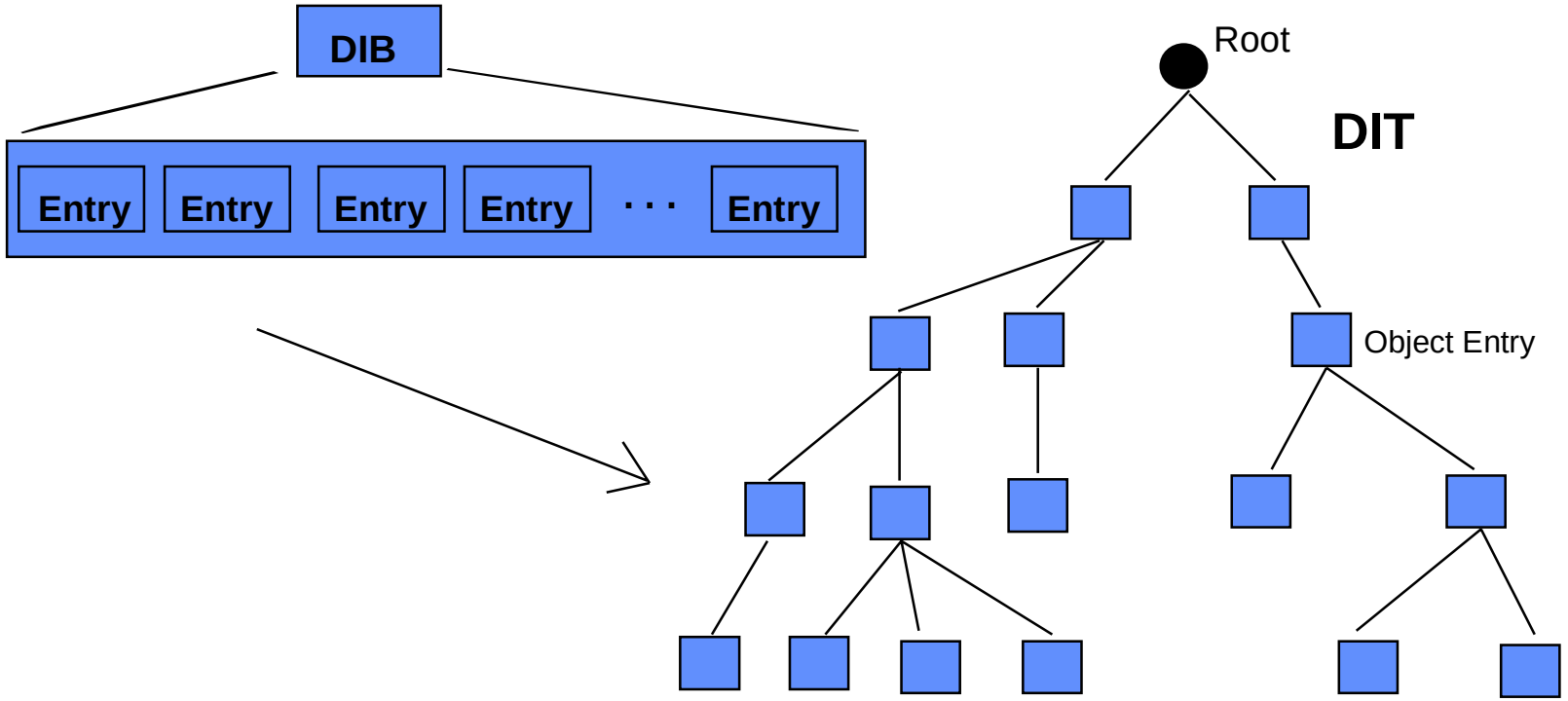


RDN	DN
	{}
C=US	{C=US}
O=Corporation	{C=US, O=Corporation}
(OU=SALES, L=San Jose)	{ C=US, O=Corporation, (OU=SALES, L=San Jose)}
CN=John L Smith	{ C=US, O=Corporation, (OU=SALES, L=San Jose), CN=John L Smith }

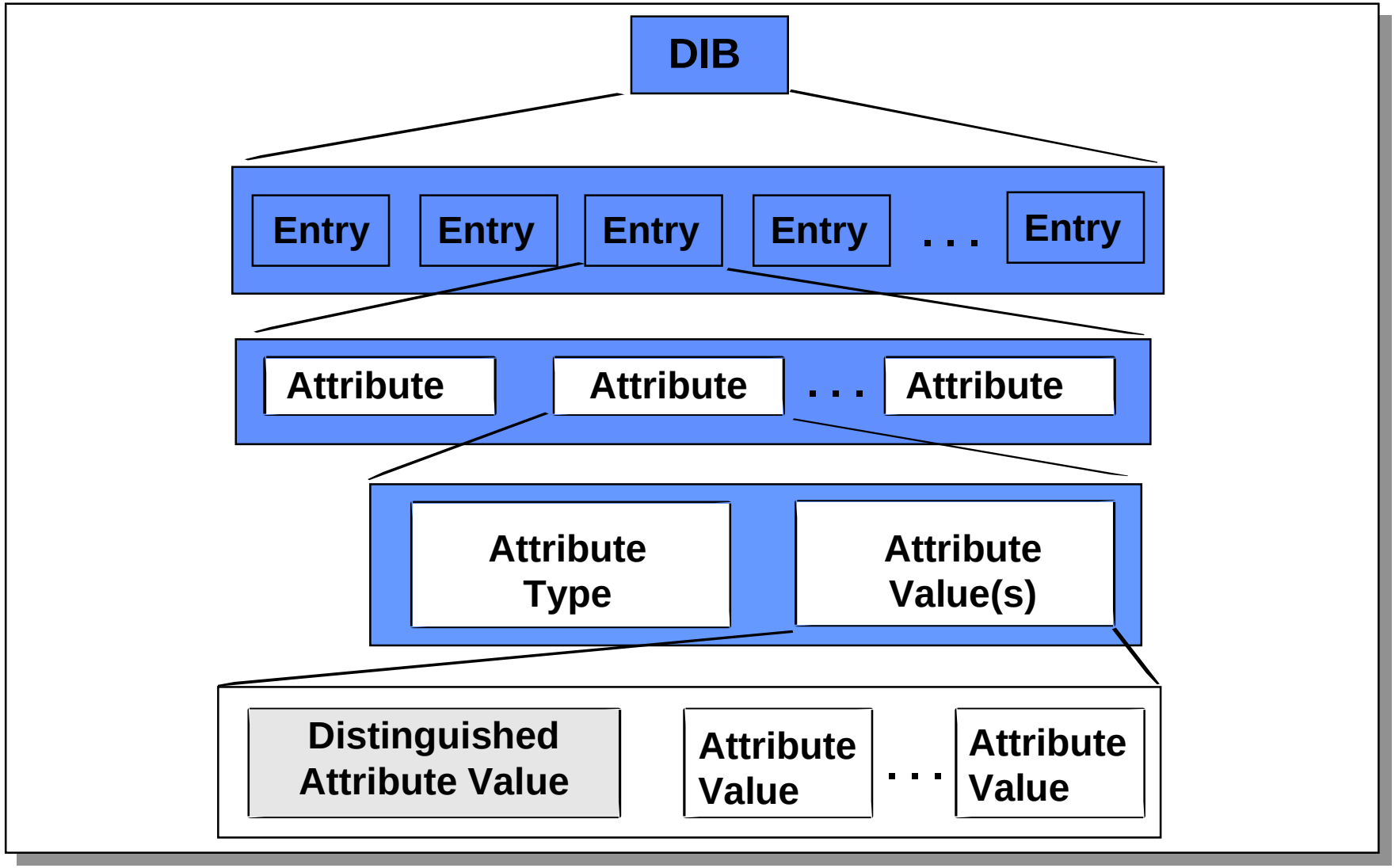
Example:Alternate values of names



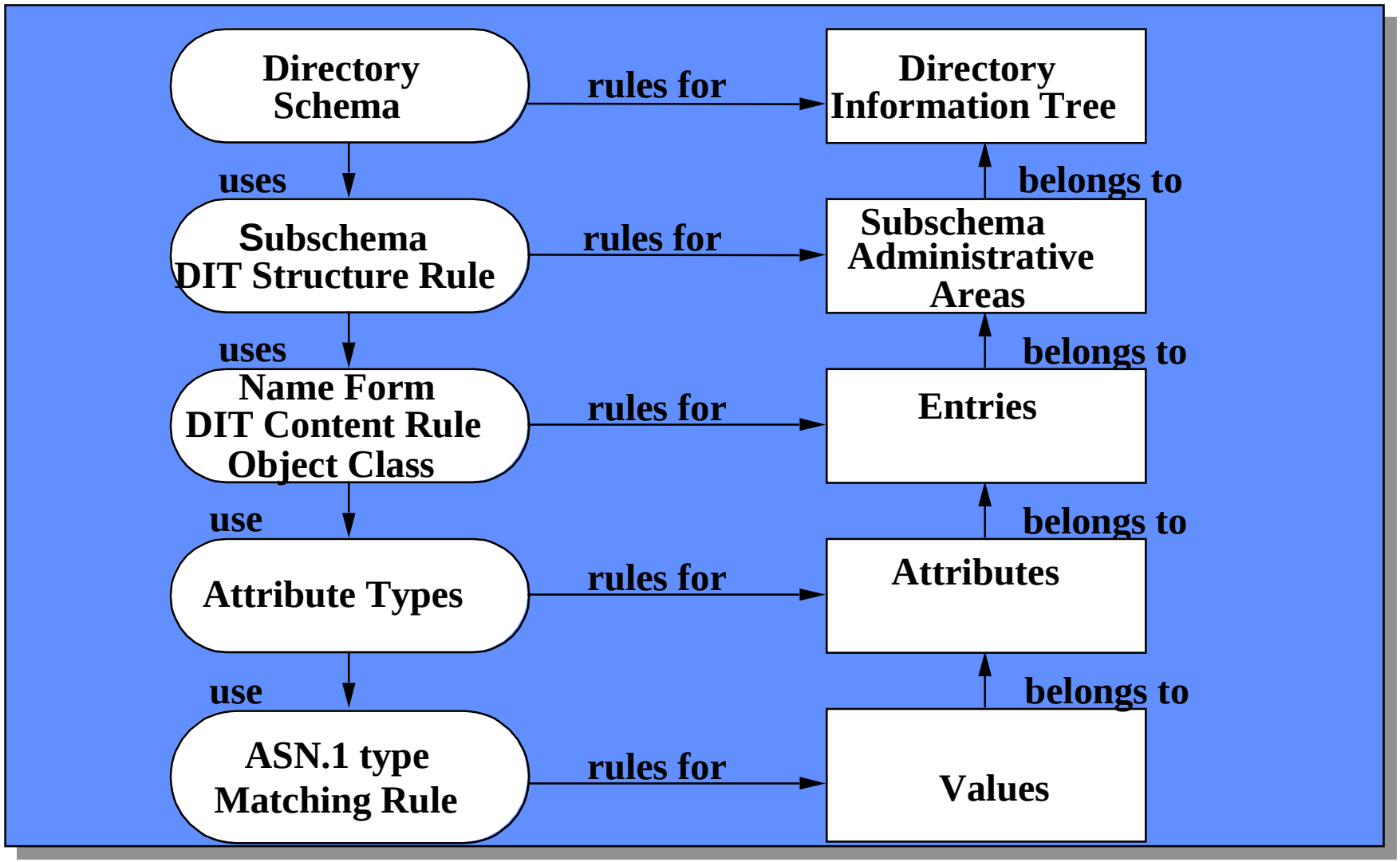
The structure of Directory entries



Directory Information Base (DIB)



Overview of the Directory schema



Object class for Certification Authority - X.521

certificationAuthority OBJECT-CLASS ::={

SUBCLASS OF	**{ top }**
KIND	**auxiliary**
MUST CONTAIN	**{ cACertificate | certificateRevocationList | authorityRevocationList }**
MAY CONTAIN	**{ crossCertificatePair }**
ID	**id-oc-certificationAuthority }**

***note that v2 CA object class may contain Delta Revocation List attribute**

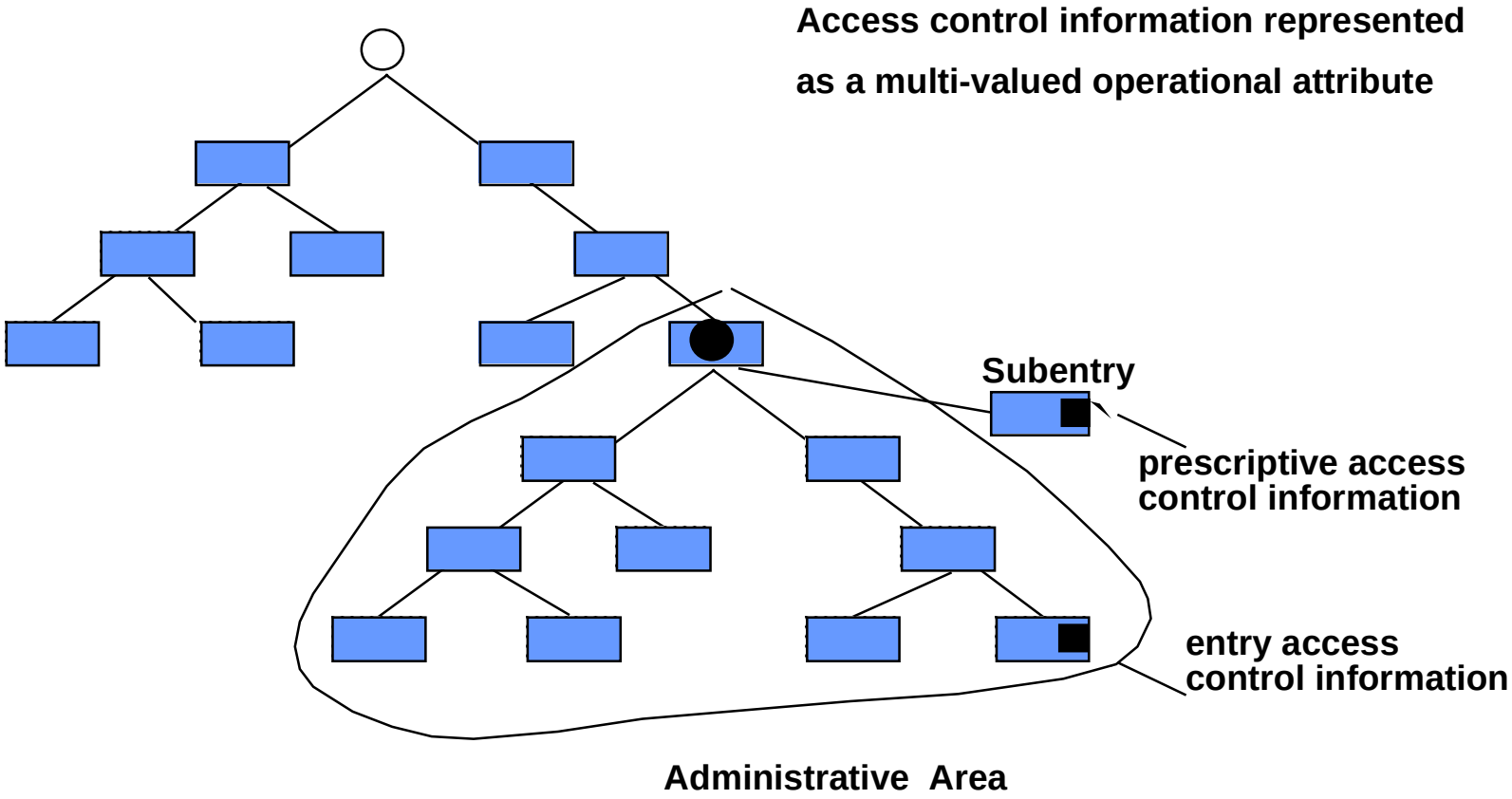
Object class for Certification Authority - draft-ietf-pkix-LDAPv2-schema-02.txt

```
pkiCA   OBJECT-CLASS   ::= {
        SUBCLASS OF            { top}
        KIND                   auxiliary
        MAY CONTAIN            {cACertificate |
                               certificateRevocationList |
                               authorityRevocationList |
                               crossCertificatePair }}
--ID   { joint-iso-ccitt(2) ds(5) objectClass(6)pkiCA(22)}
```

Matching rules

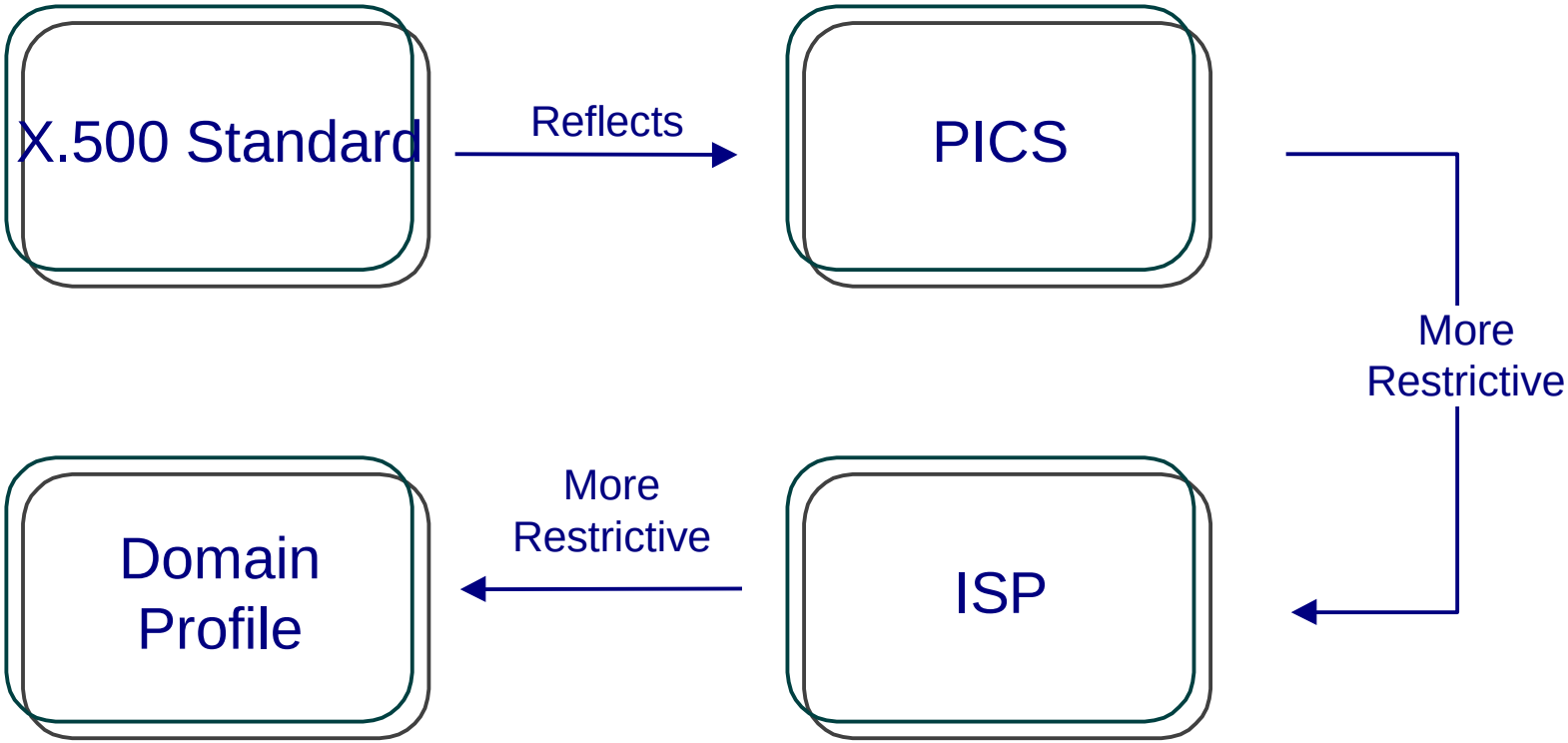
- Rules to compare a value presented by a user with a value stored in the Directory
- Each matching rule states
  - the attribute syntax that the matching rule applies to
  - the syntax of a user-presented value
  - how the comparison is performed
  - under what conditions a match is found to be True
- Built-in matching rules
  - present; equality; substrings; ordering; approximate

Security Control Model



***Presumption - anything that is in a Border DSA is read-only to any entity that has access to that network**

ISO/ITU DIRECTORY STANDARDS



Directory specifications

	ITU-T	ISO/IEC
Overview of Models, Concepts, and Services	X.500	9594-1
Models	X.501	9594-2
Authentication Framework	X.509	9594-8
Abstract Service Definition	X.511	9594-3
Procedures for Distributed Operation	X.518	9594-4
Protocol Specifications	X.519	9594-5
Selected Attribute Types	X.520	9594-6
Selected Object Classes	X.521	9594-7
Replication	X.525	9594-9
System Management	X.530	9594-10

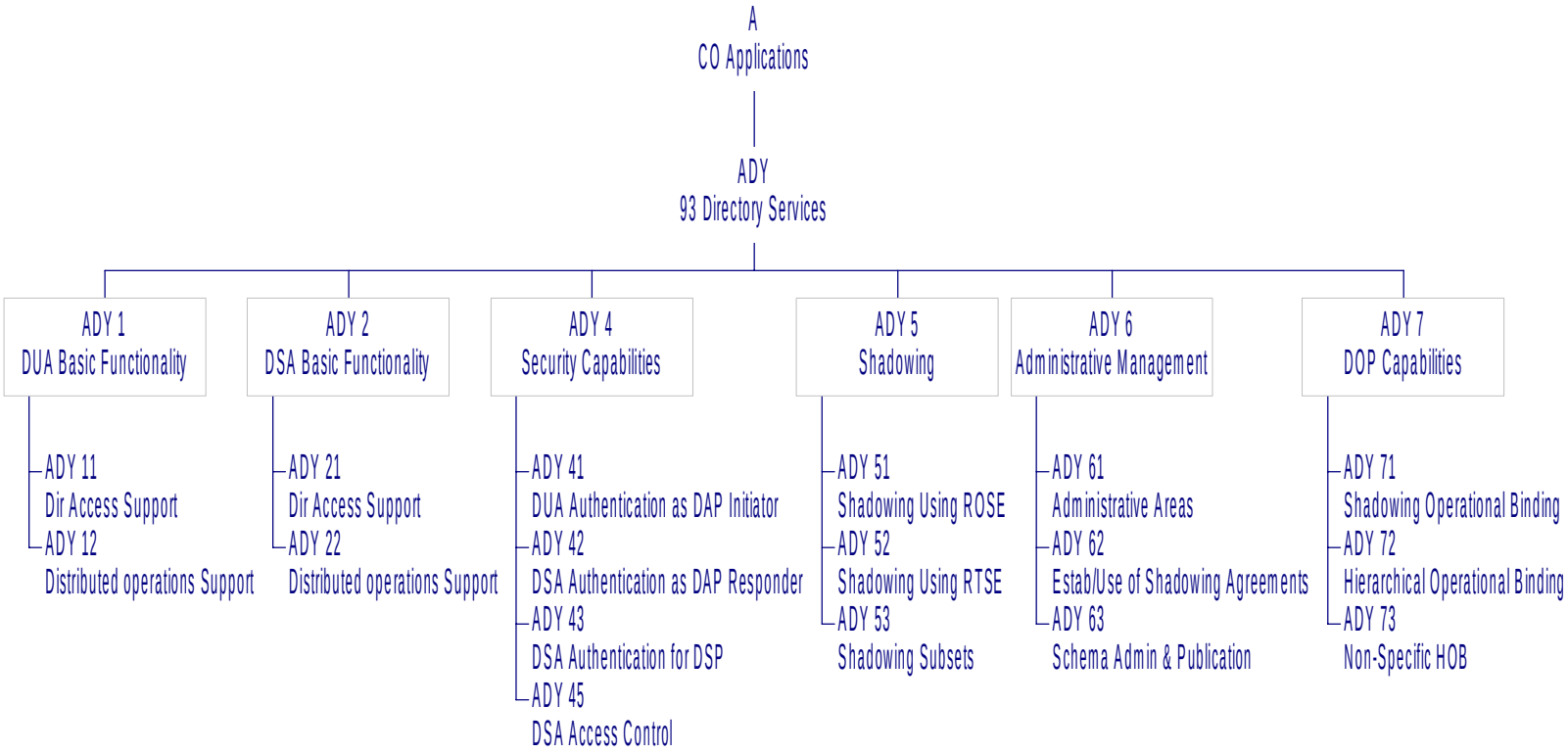
Protocol Implementation Conformance Statement (PICS)

- **Used to evaluate conformance to the standard by a particular implementation**
  - ✔ **Shows which capabilities and options have been implemented.**

- **One PICS associated with each X.500 protocol**
  - ✔ **DAP, DSP, DOP, and DISP**
    - ➪ **ITU - X.583, X.584, X.585, X.586**
    - ➪ **ISO - ISO/IEC 13248-1, 13248-2, 13248-3, 13248-4**

- **Available at URL:**
  ftp://ftp.bull.com/pub/OSIdirectory/93specification/PICSproforma

International Standardized Profiles (ISPs)
Directory A-Profile Taxonomy



ADY1-DUA Basic Functionality

- ADY 11 DUA Support of Directory Access Protocol, 16 Jun 98
- ADY 12 DUA Support of Distributed Operations, 16 Jun 98

ADY2-DSA Basic Functionality

- ADY 21 DSA Support of Directory Access Protocol, 16 Jun 98
- ADY 22 DSA Support of Distributed Operations, 20 Jan 97

ADY4-Security Capabilities

- ADY 41 DUA Authentication as DAP Initiator, 19 Jun 98
- ADY 42 DSA Authentication as DAP Responder, 19 Jun 98
- ADY 43 DSA Authentication for DSP, 22 Jul 96
- ADY 45 Simplified and Basic Access Control (combined 44 and 45), 12 Jul 98

ADY5-Shadowing

- ADY 51 Shadowing using ROSE, 12 Jul 96
- ADY 52 Shadowing using RTSE, no editor
- ADY 53 Shadowing Subsets, 12 Jul 96

ADY6-Administration Management

- ADY 61 Administrative areas, 26 Jun 98
- ADY 62 Establishment and Utilisation of Shadowing Agreements, 17 Jan 97
- ADY 63 Schema Administration and Publication, 10 Jun 98

ADY7-DOP Capabilities

- ADY 71 Shadowing Operational Binding, 30 Jul 96
- ADY 72 Hierarchical Operational Binding, Dec 97 - draft-ietf-ldapext-hobs-01.txt
- ADY 73 Non-specific Hierarchical Binding - no editor

Functional Profiles

- FDY 11 Common Directory Use, 17 Jul 96
- FDY 12 Directory System Schema, 17 Jul 96

Implementor's Guide

- Compilation of reported defects and their resolutions to the 1988 and 1993 editions of the ITU X.500 Recommendations and ISO/IEC 9594 standard
- ISO requires ballot on draft technical corrigenda
- Categories of defects
  - editorial errors
  - technical errors, such as omissions or inconsistencies
  - ambiguities
- Version 10 - March 97
  - ftp://ftp.bull.com/pub/OSIdirectory/DefectResolution/ImplementorsGuide/V10/

LDAP V3 Core documents:

- RFC 2251 : Lightweight Directory Access Protocol (v3)
- RFC 2252 : Lightweight Directory Access Protocol (v3) : Attribute Syntax Definitions
- RFC 2253 : Lightweight Directory Access Protocol (v3) : UTF-8 String Representation of Distinguished Names
- RFC 2254 : The String Representation of LDAP Search Filters
- RFC 2255 : The LDAP URL Format
- RFC 2256 : A Summary of the X.500(96) User Schema for use with LDAPv3

LDAP Extensions documents

- draft-ietf-asid-ldapv3-simple-paged-03.txt
- draft-ietf-ldapext-sorting-01.txt
- draft-ietf-asid-ldapv3-dynamic-08.txt
- draft-ietf-ldapext-lang-01.txt
- draft-ietf-ldapext-ldapv3-tls-04.txt
- draft-ietf-ldapext-ldapv3-vlv-02.txt
- draft-ietf-ldapext-acl-reqts-01.txt
- draft-ietf-ldapext-authmeth-03.txt
- draft-ietf-ladapext-ldap-c-api-01.txt
- draft-ietf-ldapext-x509-sasl-00.txt
- draft-ietf-asid-ldap-domains-02.txt

LDAP Extensions documents, con’t

- draft-ietf-ladpext-referral-00.txt
- draft-ietf-ldapext-acl-model-01.txt
- draft-ietf-ldapext-signops-03.txt
- draft-ietf-ldapext-psearch-01.txt
- draft-ietf-ldapext-java-api-02.txt
- draft-ietf-ldapext-trigger-01.txt
- draft-ietf-ldapext-c-api-vlv-01.txt
- draft-ietf-ldapext-c-api-psearch-oo.txt
- draft-ietf-ldapext-ldapv3-dupent-00.txt
- draft-ietf-ldapext-families-00.txt

www.ietf.org/ids.by.wg/ldapext.html

Other Documents ??

- draft-good-ldap-changelog-00.txt
- draft-weiser-replica-req-01.txt
- draft-ietf-asid-ldap-mult-mast-rep-02.txt
- draft-ietf-asid-ldap-repl-info-01.txt
- draft-smith-ldap-inetorgperson-00.txt
- draft-ietf-asid-ldap-rpcschema-00.txt
- draft-ietf-asid-schema-pilot-00.txt
- draft-ietf-asid-nis-schema-01.txt
- draft-good-ldap-ldif-01.txt
- draft-ietf-lsd-ldapv3-wp-00.txt
- draft-ietf-asid-ldapv3-dynatt-01.txt
- draft-ietf-ldapext-ldapv3-txn-00.txt

Open Group LDAP V3 Profiles

- Defined LDAP V3 profiles for use within the LDAP V3 test suites (http://www.opengroup.org/orc/DOCS/LDAP_PR/)
- Status of Base Documents, but are not yet Final Documents
  - RO :Read-Only LDAP Server (‘core’ documents)
  - RW:Read-Write LDAP server (‘core’ + referral + tls)
  - CERT:Certification Application Profile (RW + pkix-ipkiopp)
  - WP:White Pages Application Profile (CERT requirements + LIPS)
  - SSO:Single Sign On Application LDAP Profile (very high level requirements)