DCE Directory & LDAP

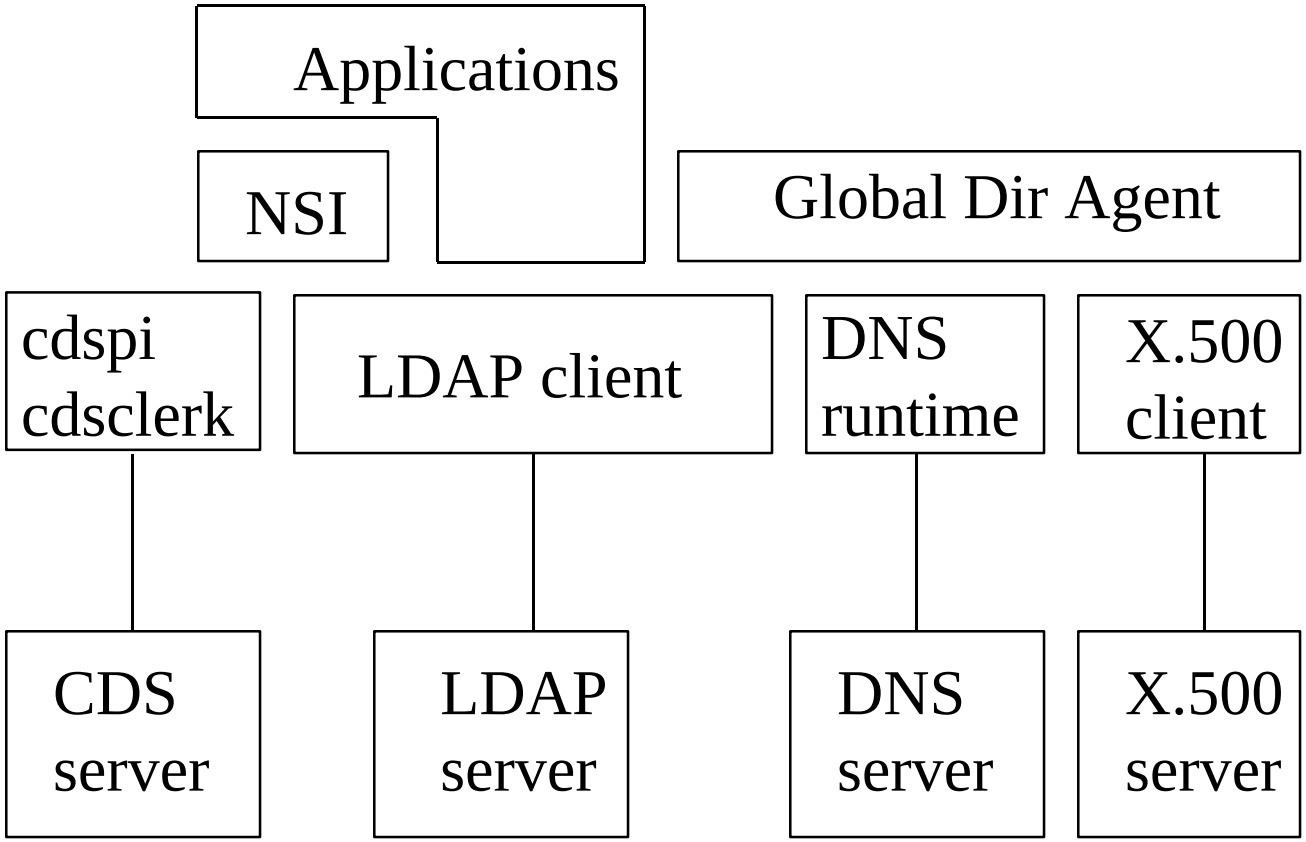
DCE Naming Task Group, 18 MAR 97

Ellen Stokes, IBM Austin
stokes@austin.ibm.com

AGENDA

- Discussion of current Naming PSTs
  - GDA
  - NSI
- Next steps
  - Other projects based on Nov 96 priorities
  - What about RFC 4.0 (Naming Requirements)
  - RFCs
  - Implications for DCE security and PKI / RFC 98

OSF: DCE and LDAP



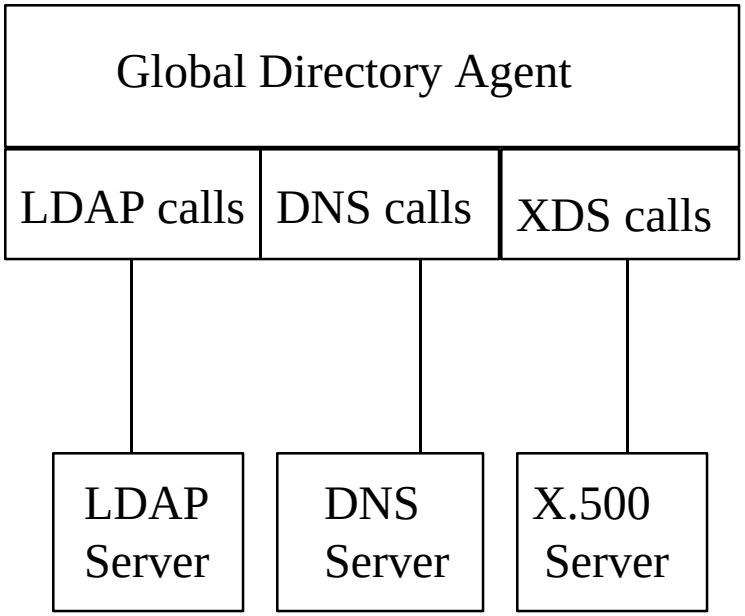
GOAL: Move DCE forward to embrace Internet technologies

Step 1: introduction of existing services to exploit ldap client services (ldap client not included)

a. GDA use of LDAP for cross cell information
b. NSI use of LDAP for binding information

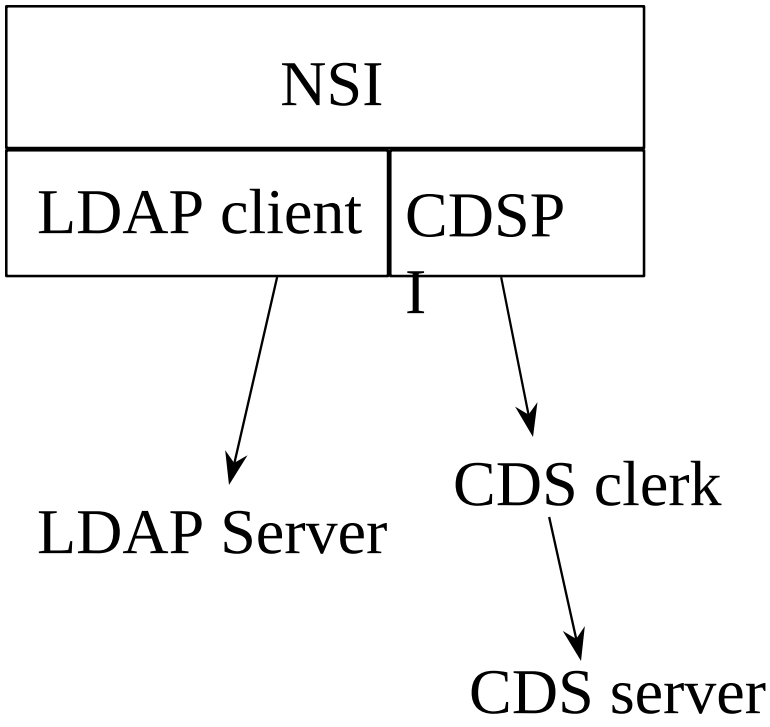
These are the two pieces of work being done via The Open Group PSTs.

GDA / LDAP



- Cross-cell information can be stored in any LDAP-based directory: re-use 2 attributes DCE GDS defines for cross-cell information
- Tool to register cell info in LDAP-based directory; similar to that for DCE GDS
- Command line extensions to gdad to enable use of LDAP service, default starts all 3 services
- Resolution of typed names: LDAP first
- Naming: cell name syntax is still X.500 or DNS. X.500 cell names algorithmically converted to LDAP names
- Security: required on LDAP flow only for registration tool (userid and password), GDA/LDAP flow is unauthenticated

NSI/LDAP Evolution



- Syntaxes:
  - pure DCE and pure LDAP
  - algorithmic translation of DCE names to LDAP syntax
- LDAP server location, translation behavior, & search order for configured name services & cell names can be:
  - globally set (DNS TXT records)
  - dynamically changed
  - overridden locally (config file)
- No Security (unauthenticated), but bindings stored in LDAP can be used for secure communication with DCE servers
- Data representation of bindings - base definition developed with Microsoft; see Internet draft ftp://ietf.org/internet-drafts/draft-ietf-asid-ldap-rpcschema-00.txt

DCE DIRECTORY PRIORITIES*

(Naming Task Group / The Open Group, 4 Nov 1996)

- NSI over LDAP, GDA over LDAP
- Directory API, may get as part of NSI & GDA work, but don't let it gate NSI & GDA delivery
- LDAP access to RGY
- LDAP V3 server
- LDAP access to CDS (probably never do, pre-empted by LDAP V3 server)

*note: don't need all bells & whistles in a first release

Proposed Projects

- LDAP access to the DCE Registry
- LDAPv3 server (& client)
- Secure NSI/LDAP
- Remove directory from the security server

***We should review RFC 4.0 (Naming Requirements) and update/track

Note: This set of projects combined with the current NSI/GDA projects has the effect of moving positioning DCE to play better in the Internet space

LDAP Access to the Registry

- Main purpose of Registry is to store security related information in secure manner
- But from end-user's view, this basically stores principal definitions among which are user definitions / profiles / groups
- Proposal: allow LDAP access to RGY to externalize PGO definitions
  - read-only: unauthenticated or authenticated
  - read-write: authenticated, algorithmic mapping of LDAP DN to DCE principal (UFN?)

LDAPv3 Server (& Client)

- Purpose: provide a complete DCE offering (instead of referencing use of components)
- Replacement (over time) for CDS (needed to fix problems that require CDS redesign)
- Model
  - separate protocol from data store
  - service provider interface (SPI) at bottom of protocol server provides framework for supporting multiple data stores at runtime
  - data store must be highly functional
    - structure capable of supporting the full protocol
    - must perform; handle high volume of writes
    - store millions of objects
    - allow storage of large objects, i.e. photos
    - <others ...>
  - authentication, access control, replication

Secure NSI/LDAP

- implies LDAPv3 client and server
- use SASL mechanism for GSSAPI (DCE & V5 Kerberos)
- use SSL (authentication via public key certificates, encrypted connection) => integration of public key into the DCE beyond DCE 1.2.2

Remove Directory from Security Svr

- Move Registry PGO tree into LDAP directory single user definition shared with DCE
  - preserve sec_rgy* protocol, interfaces?
- DCE security server becomes privilege/TGT server
- Are there some operations that one wouldn't want done over LDAP to RGY data?
- Security-related attributes appropriately ACL'd
- Access control model now unified for RGY and CDS replacements, yet different from DCE ACLs (what about host data database?)
- This proposal could pre-empt LDAP/RGY access proposal

DCE RFCs on Directory

- publish functional specs for LDAP projects
  - GDA/LDAP functional spec
  - NSI/LDAP functional spec
  - other functional specs as developed
- write/publish directional document on LDAP in the DCE, discusses:
  - NSI
  - GDA
  - Registry
  - relationship to public key based security
  - cell concepts in the LDAP
- <others ?>

So What About Public Key?

- Current and proposed projects beg this question
- Minimum: need to allow use of public key certificates for authentication in addition to current Kerberos model; define relationship
  - begs question of certificate authorities
- Suggest we work with the DCE Security Task Group