

Carrots and Sticks



Moving forward
with history and complexity

Creating The Digital Persona

- **Ownership and collection of data**
 - Security issues
 - Political issues
 - Different databases and systems holding information
- **Business Processes**
 - No clear definition of information ownership and flow
 - Tying together effects on multiple departments
- **Corporate Change**
 - Disruption in IS and other departmental systems
 - Frequency and scope of change
- **End user involvement**
 - How much end-user involvement do you want or need ?
 - What information should they own ?

Key Questions

- **Where does the information come from ?**
 - Department specific databases and applications
- **Who owns the data ?**
 - IS
 - Other departments (HR, Facilities, Telco)
 - Employees and Managers
- **Who manages the data ?**
 - IS wants to manage their own data but not all the data
 - Other departments want to own their own data but don't have access to it
- **How is it all automated ?**
- **Who uses the Directory ?**

Who uses the Directory

- **It is important to understand how the Directory fits in with the organization**
 - Existing business processes
 - Organizational/Environmental considerations
- **Scope and use of the Directory**
 - NOS vs. Extranet
 - Authentication only vs. complete profiles
 - Publishing vs. Infrastructure
 - Is the Directory only for use by IT infrastructure?
- **Implementation considerations**
 - Tree design issues
 - Access Control
 - Data sources and synchronization
 - Directory Management

What does "Directory Enabled" mean?

- **Any application that uses or stores information in the Directory**
- **Basic Information to keep in the Directory**
 - User Profile Information
 - Application Configuration Information
 - Business Rules & Policy Information
- **Directory Enabled Infrastructure**
 - Directory Enabled Networking (DEN)
 - Messaging Servers
 - Single Sign-on
 - Application Configuration Information
- **Directory Enabled Applications**
 - Messaging Clients, Address books
 - Project Management
 - Corporate Services Automation (CSA)

Directory Enabled Networking

- **Each DS uses its own tree structure**
 - Some are flexible, and some are not
 - Different between Active Directory and Netscape Directory Server
- **Policies are setup at the tree level**
 - Can setup overall policies based on organisational unit (ou), or even for specific users
- **Impact of Directory structure**
 - Access control and policy creation can be rendered useless with a flat tree structure
 - Can find alternate ways of defining membership (dynamic groups, common attributes)

Directory Enabling Your Applications

- Use Directory authentication
 - Eliminate multiple user authentication databases
- Store application configuration information in the Directory
 - Can run multiple copies of the products without having to deal with configuration information
 - Can manage configuration information through standard admin consoles (e.g. Netscape Mission Control)
- Add per-user configuration information with user object
 - Current trend is to use auxiliary classes to store this information
 - Can distribute change management of this information using applications like Oblix CSA
 - Per-user configuration is not tied down to a particular computer or workstation
 - Information can be used by other applications as well

Find the Source, Luke, Use the Source

- Identify "important" data sources (Administration, The Registry, Estates Computing Service, Departments)
- Conduct interviews with the owners
 - Data contained within
 - Feeds into the database
 - Feeds out of the database
- Loop back if "new" data sources are revealed

Find the Actors and follow them

- Admin user
 - Samba to Password on Admin box
 - Exchange username/password or Unix Samba Password
 - Senate Papers system password
 - Central Service Unix username/password (Email)
 - Central Service Unix username/password (Samba Share for Web)

Find the Actors and follow them

- Student User
 - nds Username and password (used for email, filestore, student record)
 - Surf Access to the Registry
 - Perhaps departmental Unix username password
 - Post-Graduate students... How do they fit ?

Find the Actors and follow them

- Staff User
 - Departmental Unix Username/password (Samba Share/Email)
 - Perhaps nds username password
 - Perhaps Admin Unix username and password
 - Perhaps Admin Ingress username and password
 - Perhaps Senate Papers username and password
 - How many others ??

How Many Systems

- Admin Unix/username
- Exchange Username
- NDS Username
- NT Domains
 - Desktop Support Team WinTERM Domain
 - HelpDesk Authentication System and associated NT DOMAIN
 - Departmental NT Domains.

How Many Systems

- Admin Ingress
 - Common password
 - Student Record System
 - Delphi (Personnel Payroll)
 - Agresso (Finance system)
- Reference Manager System Bibliographic Database (RAE)
- Advisors On-line.
- Senate Papers
- Department Systems
 - Modification of Central NDS
 - Unix system (Physics has NT DOMAIN)

Quality of Data (1)

- Variance
 - Pieces of an entry from different sources
 - Same data field from different sources
- Quality
 - Inconsistent/different formats (field and record)
 - Just Plain wrong data
 - Quirks (and other weird stuff)

Quality of Data (2)

- Variances
 - Look at actual data
 - Employ data experts
- Integrity
 - Correct errors within sources
 - Look for "better" sources
 - Rework schema to match data

Feeds` and Update

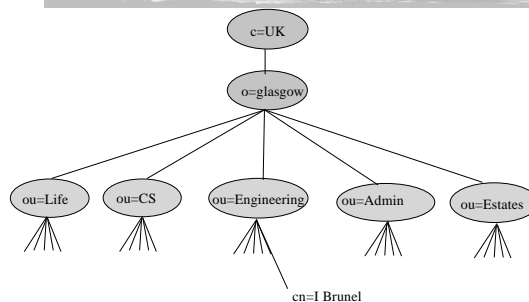
- Issue: Which of the following is the best means to feed data from existing sources into the directory
 - Continuous
 - Single load (directory absorbs source)
- Strategy - balance objectives versus difficulty
 -

Directory Tree Design

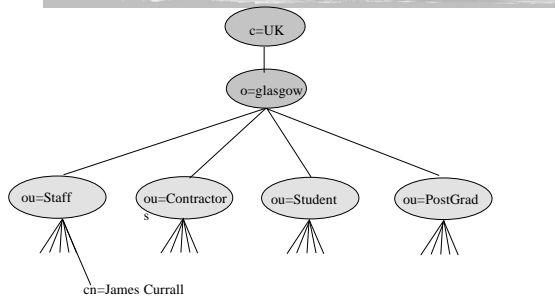
Everyone has different views of the organization

- Network Administrators
 - "Everyone in a domain" "Everyone in a subnet"
- Administration
 - "Everyone in a cost-accounting group"
- Facilities
 - "Everyone in this building"
- Telecom
 - "Everyone on a particular switch"

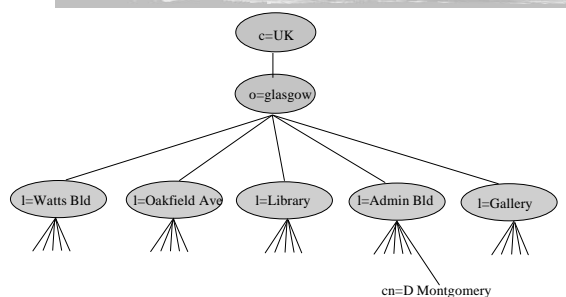
DIT Design: People By Department



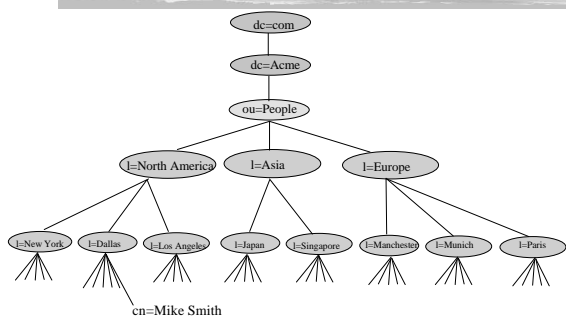
DIT Design: Types of People



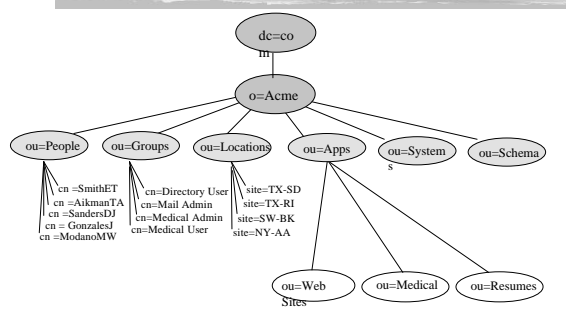
DIT Design: By Location



DIT Design: Deep Tree By Department



An Example DIT



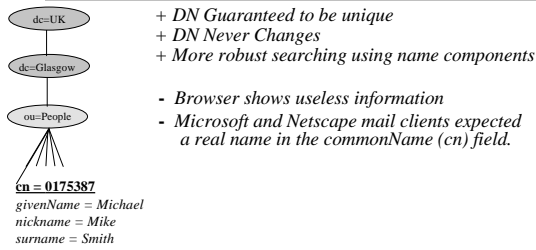
DIT Design: Deep -vs- Flat Trees

- Can result in long Distinguished Names (DN)
- May reflect your actual corporate structure
- Can result in administrative problems if your organization is constantly changing
- Better chance of having unique names within a subtree
- Works well if you want to distribute the data across multiple Directory Servers

DIT Design: Flat -vs- Deep Trees

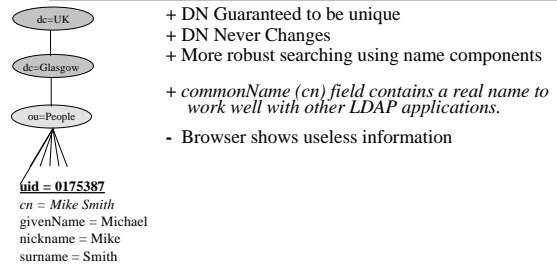
- No need to categorize people
- Short Distinguished Names, easy to type
- DIT is very stable: not affected by organizational changes, and easy to administer
- Higher chance of name collisions
- Not well suited for Browsing
- Can result in longer load times or startup times, depending on the Directory Product you use

DIT Design: Selecting a Distinguished Name



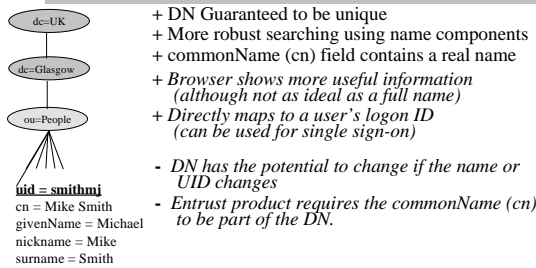
cn=0175387, ou=People, dc=Glasgow, dc=UK

DIT Design: Selecting a Distinguished Name



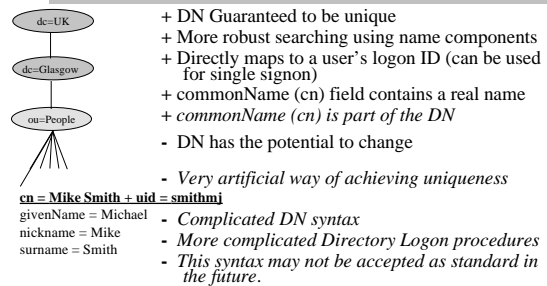
uid=0175387, ou=People, dc=Glasgow, dc=UK

DIT Design: Selecting a Distinguished Name



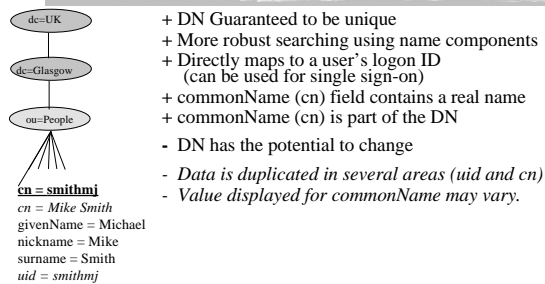
uid=smithmj, ou=People, dc=Glasgow, dc=UK

DIT Design: Selecting a Distinguished Name



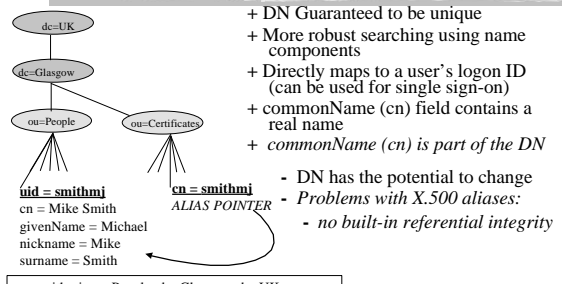
cn=Mike Smith + uid=smithmj, ou=People, dc=Glasgow, dc=UK

DIT Design: Selecting a Distinguished Name



cn=smithmj, ou=People, dc=Glasgow, dc=UK

DIT Design: Selecting a Distinguished Name



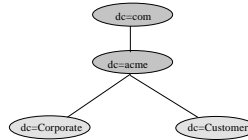
cn=smithmj, ou=People, dc=Glasgow, dc=UK
uid=smithmj, ou=Certificates, dc=Glasgow, dc=UK

DIT Design: DIT Naming Proposal (rfc2377)



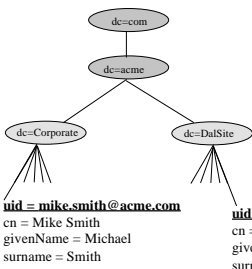
- The dc named attribute stands for *domain component*
- The idea is to map the upper levels of the tree with registered DNS Names (in this case **acme.com**)

DIT Design: DIT Naming Proposal (rfc2377)



- The dc named attribute stands for *domain component*
- The idea is to map the upper levels of the tree with registered DNS Names (in this case **acme.com**)
- Lower levels of the tree will also use the dc named attribute

DIT Design: DIT Naming Proposal (rfc2377)



- The dc named attribute stands for *domain component*
- The idea is to map the upper levels of the tree with registered DNS Names (in this case **acme.com**)
- Lower levels of the tree will also use the dc named attribute
- Each user is identified with the uid named attribute containing the email address.

Carrots and Sticks

- Robust DIT Naming and design standards are not in place yet
- There is currently no single "right way" to design your DIT that applies to everyone
- Take into consideration your organization
 - the organizational structure
 - the organization's tendency to change
 - the organization's current size and potential to grow
- Take into consideration the how you want to use the directory
 - what information will be stored in the directory
 - who will own what data and how will be mastered
 - what what other systems in the infrastructure will be using/storing the data
 - how and what applications will be accessing the data

Conclusions

- " If you think technology can solve your problems, then you don't understand the problems and you don't understand the technology. "

Bruce Schneier
- The Directory, to be useful, needs to become part of the Business Process and the repository of the highest quality and timely information.
- Remember that you are doing it FOR not TO the organisation.