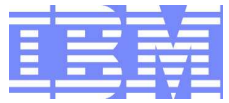


z/OS LDAP Overview and Security Function Update

Ken Morgan
IBM z/OS LDAP Development
morgankg@us.ibm.com

Disclaimer

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "as-is" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environment do so at their own risk.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used; any functionally equivalent program may be used instead.

Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly.

Users of this document should verify the applicable data for their specific environments. It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country or not yet announced by IBM. Such references or information should not be construed to mean that IBM intends to announce such IBM products, programming, or services.

Trademarks

The following are trademarks of the IBM Corporation. An asterisk following the name denotes a registered trademark.

ACF/VTAM*
ADSTAR*
Advanced Function Printing
Advanced Peer-to-Peer Networking
AIX*
AIX/6000
APL2*
APPN
Approach
AS/400*
C/VM
C/370
Callup
CICS
CICS/VSE*
Common User Access
Current
CUA
DataJoiner
DataPropagator
DB2*
DB2 Connect
DB2/2
DB2/6000
DFS
DFSMS
DFSMS/VM
DirMaint
DisplayWrite*
Distributed Relational Database Architecture
Domino
DRDA*
Enterprise Systems Connection Architecture
Enterprise Systems Architecture/390
ES/9000*
ESCON*
GDDM*
Hardware Configuration Definition
IBM*
IBM Business Partner
IBMLink
IMS
Language Environment*
Lotus Notes
Lotus SmartSuite
MQ
MQ Series
Multiprise
MVS*
MVS/ESA
MVS/SP
MVS/XA
Net.Data
NetView*
Notes
NotesPump
OfficeVision*
OfficeVision/VM
Open Blueprint
OSA
OS/2*
OS/390
Parallel Sysplex
PowerPC
PR/SM
PROFS*
QMF
RACF
RAMAC
RISC System/6000*
RS/6000
SQL/DS
SQL Master
System/390*
S/370
S/390*
S/390 Multiprise
S/390 Parallel Enterprise Server
TalkLink
Time and Place
Ultrastar
VisualAge
VisualGen
VisualLift
Visual Warehouse
VM/ESA*
VM/XA
VSE/ESA
VTAM*
Wordpro

The names listed below are trademarks or registered trademarks and are the properties of their respective companies.

ANSI
Apple
Beyond Software
C++
CATIA
CSS
DEC
DirectPC
EnterpriseWeb/VM
EnterpriseWeb Calendar
Enterprise View
Ethernet
Eudora
Gateway
Hewlett-Packard
HP
IEEE
ITAA
Java
KERBEROS
LAN Manager
Macintosh
Mortice Kern Systems InterOpen
NCR
NCE
NetWare
Network File System
Novell
NFS
Open Software Foundation
OSF, Motif
Outlook
POSIX
SAS
SnapShot
Sterling Software
Sun Microsystems
SunOS
ULTRIX
UNIX
VAX
VM:Webserver
Windows
Windows NT
XPG4
X-Windows

All statements regarding IBM's future intent are subject to change without notice, and represent goals and objectives only.

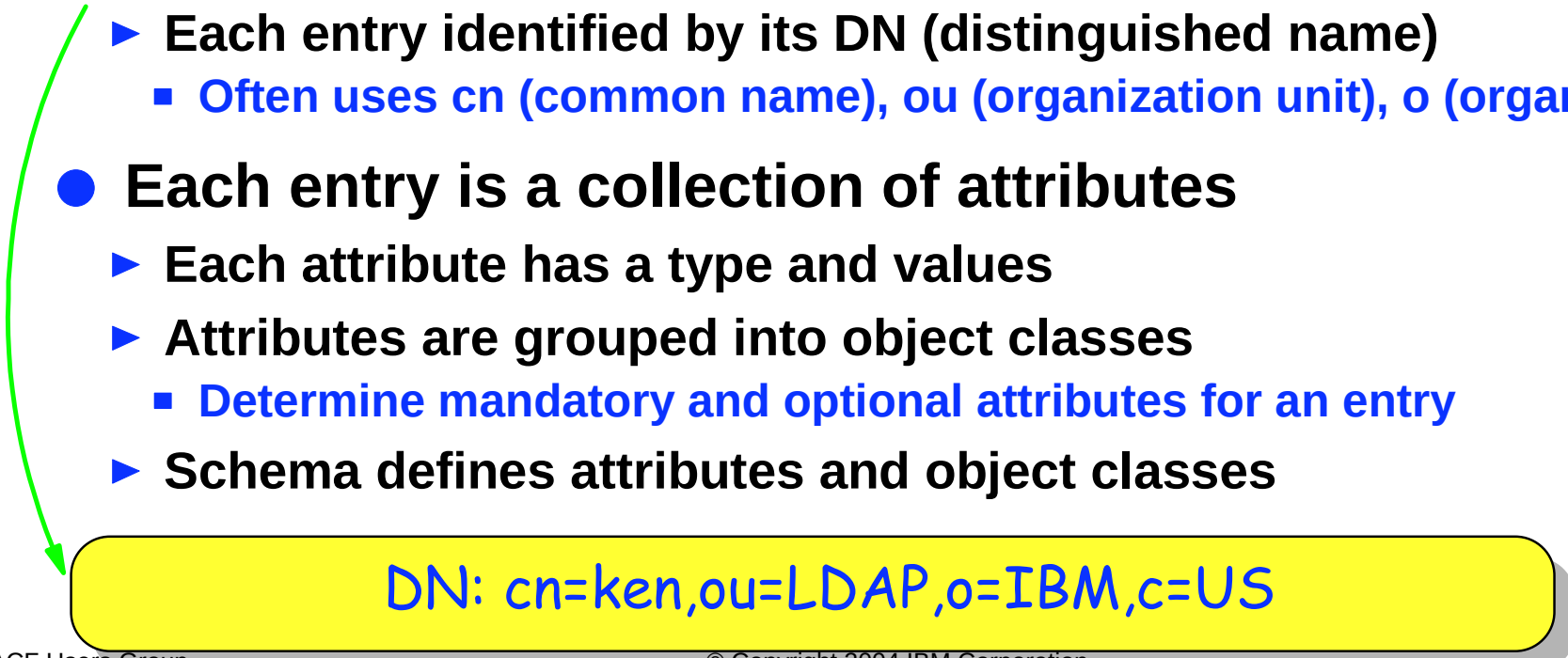
Agenda

- **LDAP Overview**
- **LDAP Authentication**
  - **Using RACF**
  - **Using TDBM**
  - **Using Native Authentication (TDBM and RACF)**
- **Accessing RACF via LDAP**
- **RACF Change Logging**
- **Access Control in TDBM**
- **The Big Picture**

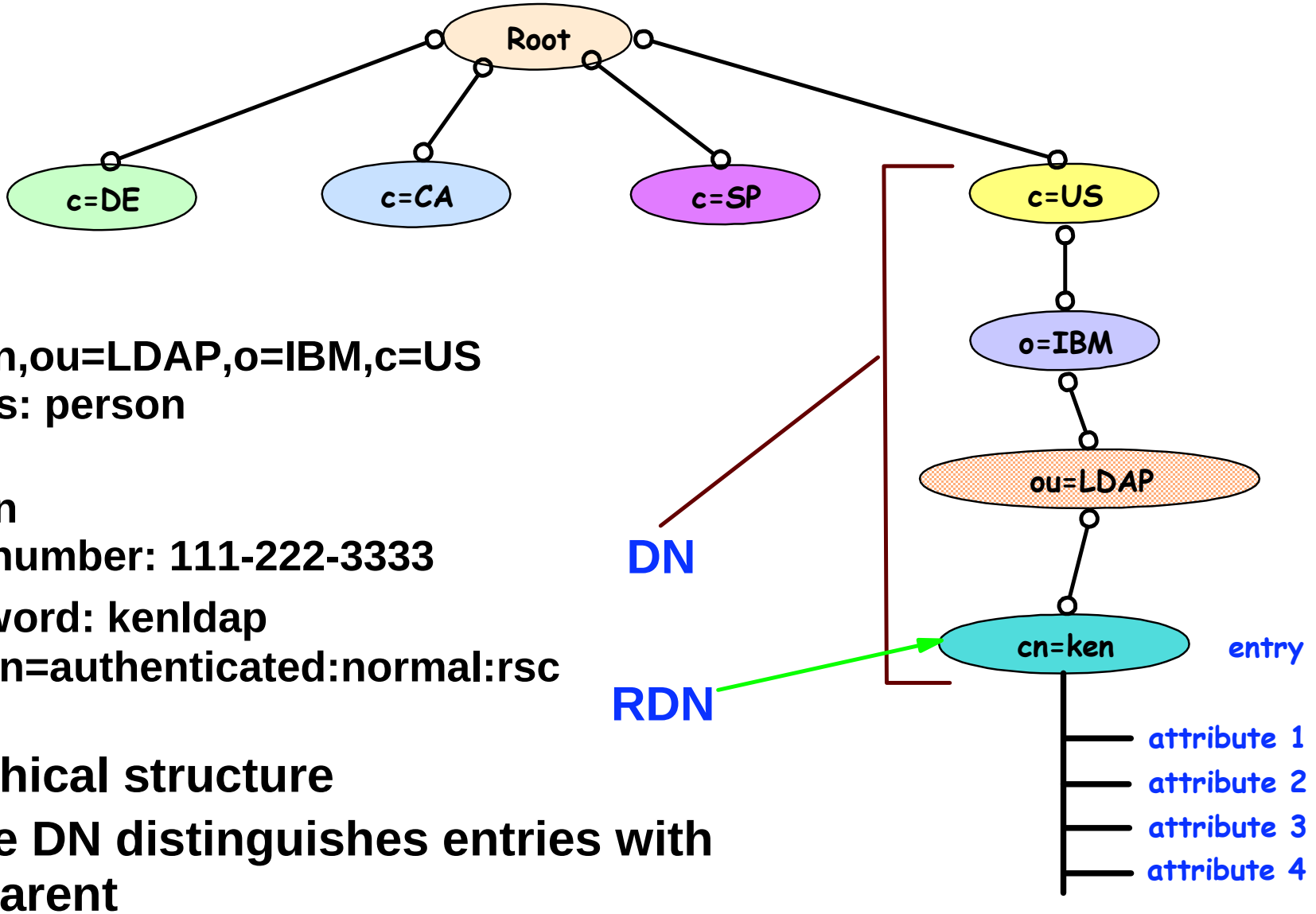
Overview of LDAP

What is LDAP?

- **Lightweight Directory Access Protocol (LDAP) is a global directory model**
- **Originally developed as front-end of X.500 (DAP)**
- **The LDAP protocol runs over TCP**
- **Global directory model is based on entries**
  - **Each entry identified by its DN (distinguished name)**
    - **Often uses cn (common name), ou (organization unit), o (organization)**
- **Each entry is a collection of attributes**
  - **Each attribute has a type and values**
  - **Attributes are grouped into object classes**
    - **Determine mandatory and optional attributes for an entry**
  - **Schema defines attributes and object classes**



LDAP Directory Structure



dn: cn=ken,ou=LDAP,o=IBM,c=US
objectclass: person
cn: ken
sn: morgan
telephonenumber: 111-222-3333
userpassword: kenldap
aclentry: cn=authenticated:normal:rsc

- **Hierarchical structure**
- **Relative DN distinguishes entries with same parent**
- **Attributes are protected by Access Control Lists (ACL)**

LDAP Parts

- **z/OS LDAP provides**
  - **LDAP server - manages the directory entries**
  - **LDAP client - C APIs to add, modify, delete, rename, compare, and search entries**
  - **Command line client utilities: ldapadd, ldapmodify, ldapdelete, ldapmodrdn, ldapsearch**
- **Any Version 3 LDAP client can be used with z/OS LDAP server**
- **z/OS LDAP client and utilities can be used with any V3 LDAP server**

Using LDAP - Examples

- **Example: add an entry**
  - **Create a file, jay.add, containing entry to be added:**

```
dn: cn=jay,ou=LDAP,o=IBM,c=US
cn: jay
sn: smith
userpassword: jaypw
```

  - **Invoke ldapadd utility:**

```
ldapadd   -h dceset3.ibm.com   -p 2803
   -D cn=ken,ou=LDAP,o=IBM,c=US   -w kenldap   -f jay.add
```

- **Example: modify an entry**
  - **Create a file, jay.mod, containing changes:**

```
dn: cn=jay,ou=LDAP,o=IBM,c=US
add: telephonenumber
telephonenumber: 555-666-7777
-
replace: sn
sn: smithson
```

  - **Invoke ldapmodify utility:**

```
ldapmodify   -h dceset3.ibm.com   -p 2803
   -D cn=ken,ou=LDAP,o=IBM,c=US   -w kenldap   -f jay.mod
```

Using LDAP - Examples cont.

- **Example: search for an entry**
  - **Display specific entry**

```
ldapsearch -h dceset3.ibm.com  -p 2803  -D cn=ken,ou=LDAP,o=IBM,c=US
 -w kenldap   -L   -s base   -b cn=jay,ou=LDAP,o=IBM,c=US   objectclass=*

 dn: cn=jay,ou=LDAP,o=IBM,c=US
 objectclass: person
 cn: jay
 sn: smithson
 telephonenumber: 111-666-7777
```

  - **Display entries with telephonenumber in 111 area code and surname starting with smith:**

```
ldapsearch  -h dceset3.ibm.com  -p 2803   -D cn=ken,ou=LDAP,o=IBM,c=US
 -w kenldap  -L  -s sub   -b c=US   "(&(telephonumber=111*)(sn=smith*))"
```

- **Example: delete an entry**

```
ldapdelete  -h dceset3.ibm.com  -p 2803   -D cn=ken,ou=LDAP,o=IBM,c=US
    -w kenldap   cn=jay,ou=LDAP,o=IBM,c=US
```

Using LDAP - Examples cont.

- **Example: display all entries in c=US directory tree**

```
ldapsearch   -h dceset3.ibm.com   -p 2803    -D cn=ken,ou=LDAP,o=IBM,c=US
    -w kenldap   -L   -s sub   -b c=US   objectclass=*
```

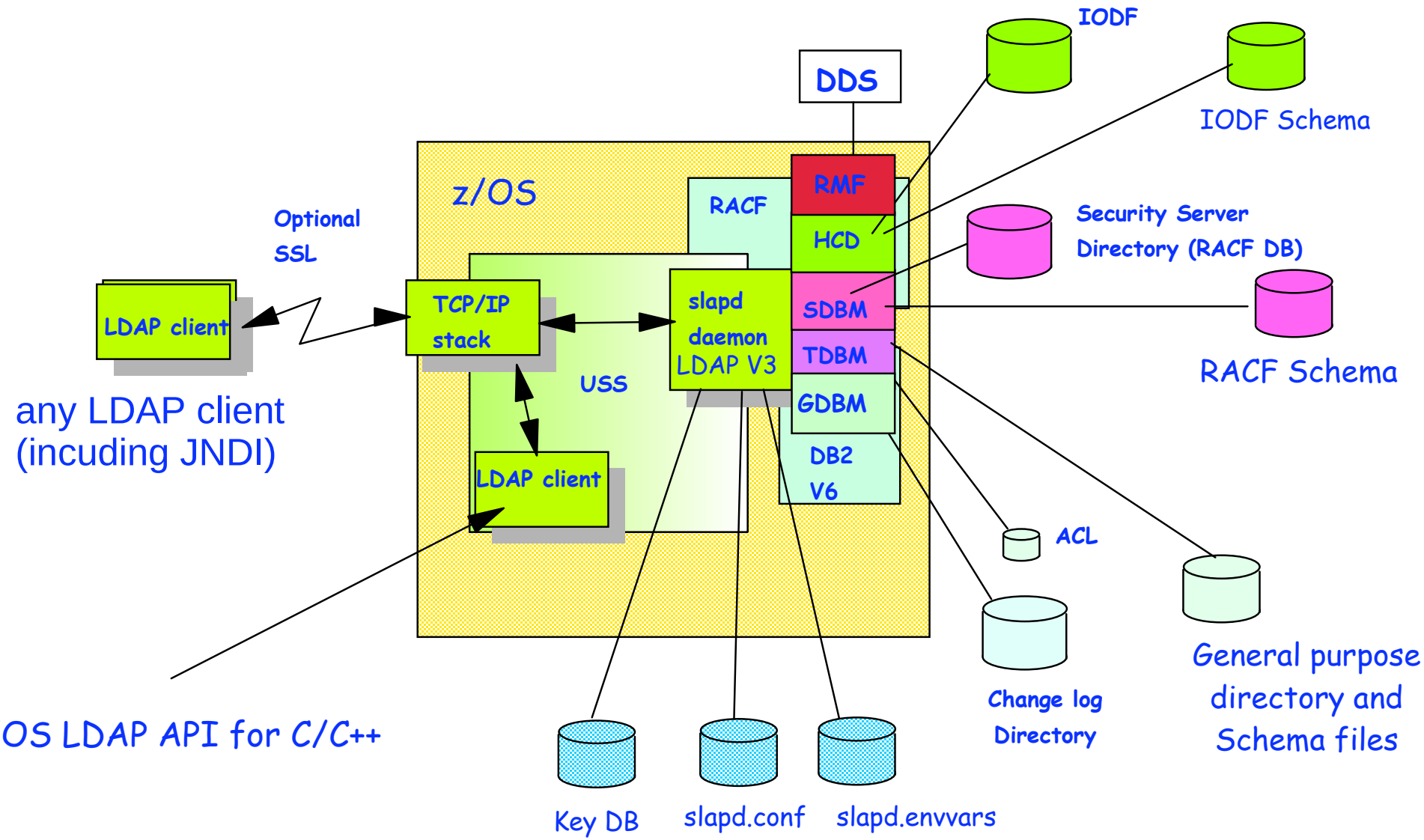
```
dn: c=US
objectclass: country
c: US

dn: o=IBM,c=US
objectclass: organization
o: IBM

dn: ou=LDAP,o=IBM,c=US
objectclass: organizationalunit
ou: LDAP

cn=ken,ou=LDAP,o=IBM,c=US
objectclass: person
cn: ken
...
```

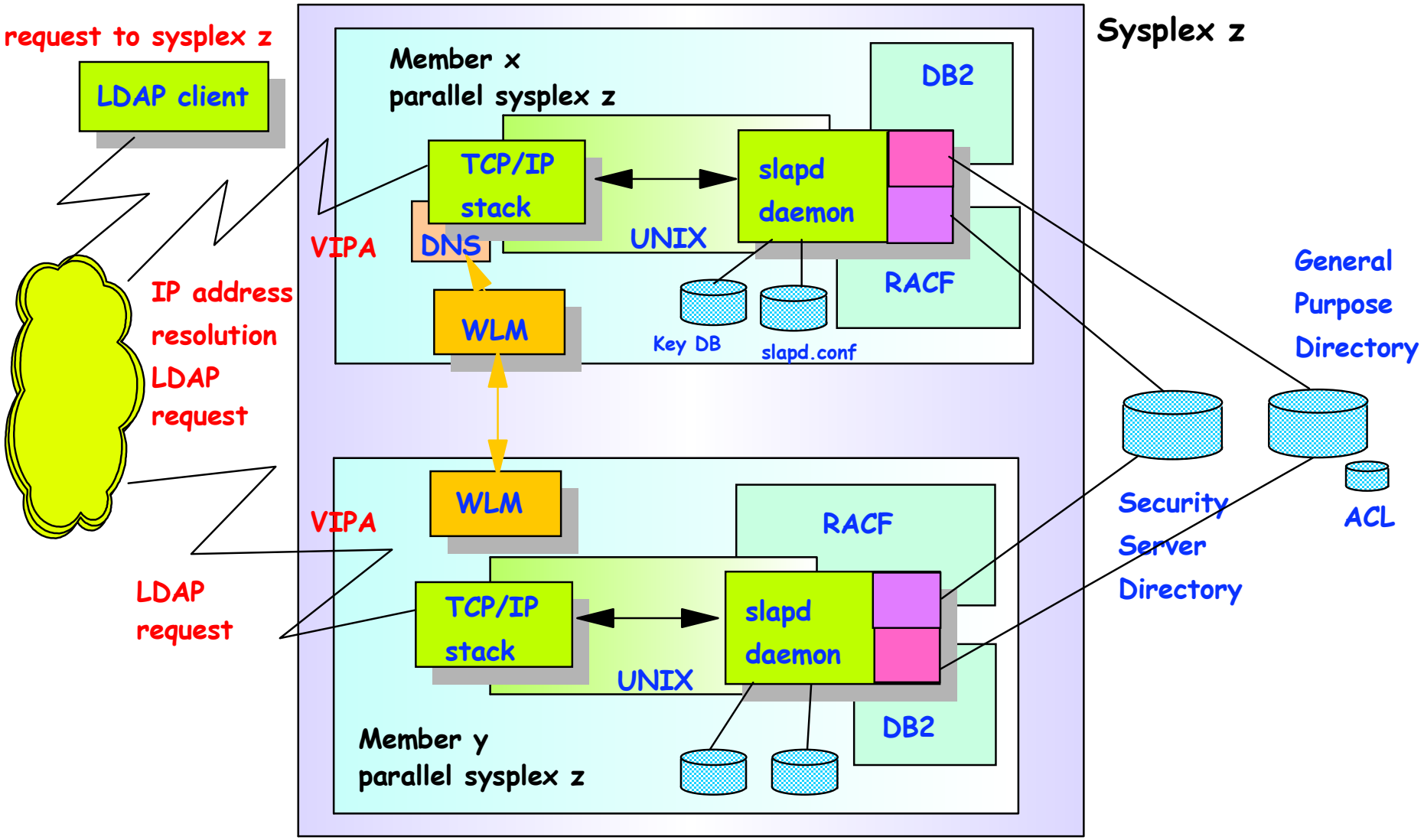
LDAP Server on z/OS



LDAP Server on z/OS...

- **LDAP Server has multiple backends (data stores)**
  - **TDBM: General purpose directory**
    - **Full LDAP V3 support, including modifiable schema**
    - **Data stored in DB2 database**
    - **Full scalability**
  - **SDBM: RACF users, groups, and user-group connections**
    - **Provides remote RACF administration and authentication**
    - **Fixed schema**
    - **Data stored in RACF database**
    - **Limited search capability**
  - **GDBM: change log directory**
    - **Similar to TDBM (DB2 based) but restricted operations**
  - **Limited function special backends**
    - **HCD: IODF definitions, data in IODF - shipped with HCD**
    - **RMF: RMF data, stored in RMF DDS server - shipped with RMF**

LDAP for z/OS Parallel Sysplex Support



LDAP Authentication

Authentication with an LDAP Server

- **LDAP is a stateful protocol**
  - **Session starts when client "binds" to server**
  - **Authentication is performed during bind**
    - **Check password or certificate**
    - **Determine groups to which user belongs (for authorization checking)**
  - **Session can be unauthenticated (anonymous bind)**
- **LDAP supports different authentication protocols**
  - **Simple bind: Distinguished Name and password**
    - **Session can optionally be protected with SSL**
    - **Passwords can be stored in LDAP directory, optionally one-way (MD5, SHA-1, crypt) or two-way (TDES) encrypted, or stored in RACF**
  - **Certificate bind: X.509 digital certificate over SSL**
    - **Distinguished name in certificate must conform with distinguished name of person authenticating - use RACF keyring or HFS keydb**
  - **Kerberos bind: Kerberos principal sends ticket for LDAP server**
    - **Attribute: ibm-kn = principal@realm**
  - **CRAM-MD5, DIGEST-MD5 binds: DN/userid and password**
    - **Client hashes password using MD5 encryption**

LDAP TDBM Authentication

Enter userid : ken
Enter password : ********

dn="cn=ken,ou=LDAP,o=IBM,c=US"
pw=kenldap
ldap_bind_s(ld,host,port,dn,pw)

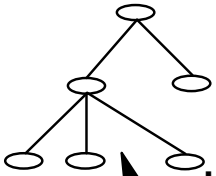
bind request

LDAP Client (API)

z/OS LDAP Server **TDBM**

find TDBM entry
verify password
get TDBM groups

successful bind



dn: cn=ken,ou=LDAP,o=IBM,c=US

objectclass: person
cn: ken
sn: morgan
userpasswd: 12Lg7tvXO

In TDBM directory

LDAP DB2 Database

LDAP Authentication with SDBM (RACF)

Enter userid : u12345
Enter password : ********

dn="racfid=u12345,profiletype=user,cn=myRACF"
pw=racfpw
ldap_bind_s(ld,host,port,dn,pw)

bind request

LDAP Client (API)

z/OS LDAP Server **SDBM**

verify user and password

__passwd(U12345,racfpw

successful bind

dn: racfid=U12345,profiletype=user,cn=myRACF

objectclass: racfUser
objectclass: racfBaseCommon
racfid: U12345
racfprogrammername: Ken Morgan
racfdefaultgroup: racfid=group1,profiletype=GROUP,cn=myRACF
racfconnectgroupname: racfid=group1,profiletype=GROUP,cn=myRACF
racfconnectgroupname: racfid=group2,profiletype=GROUP,cn=myRACF

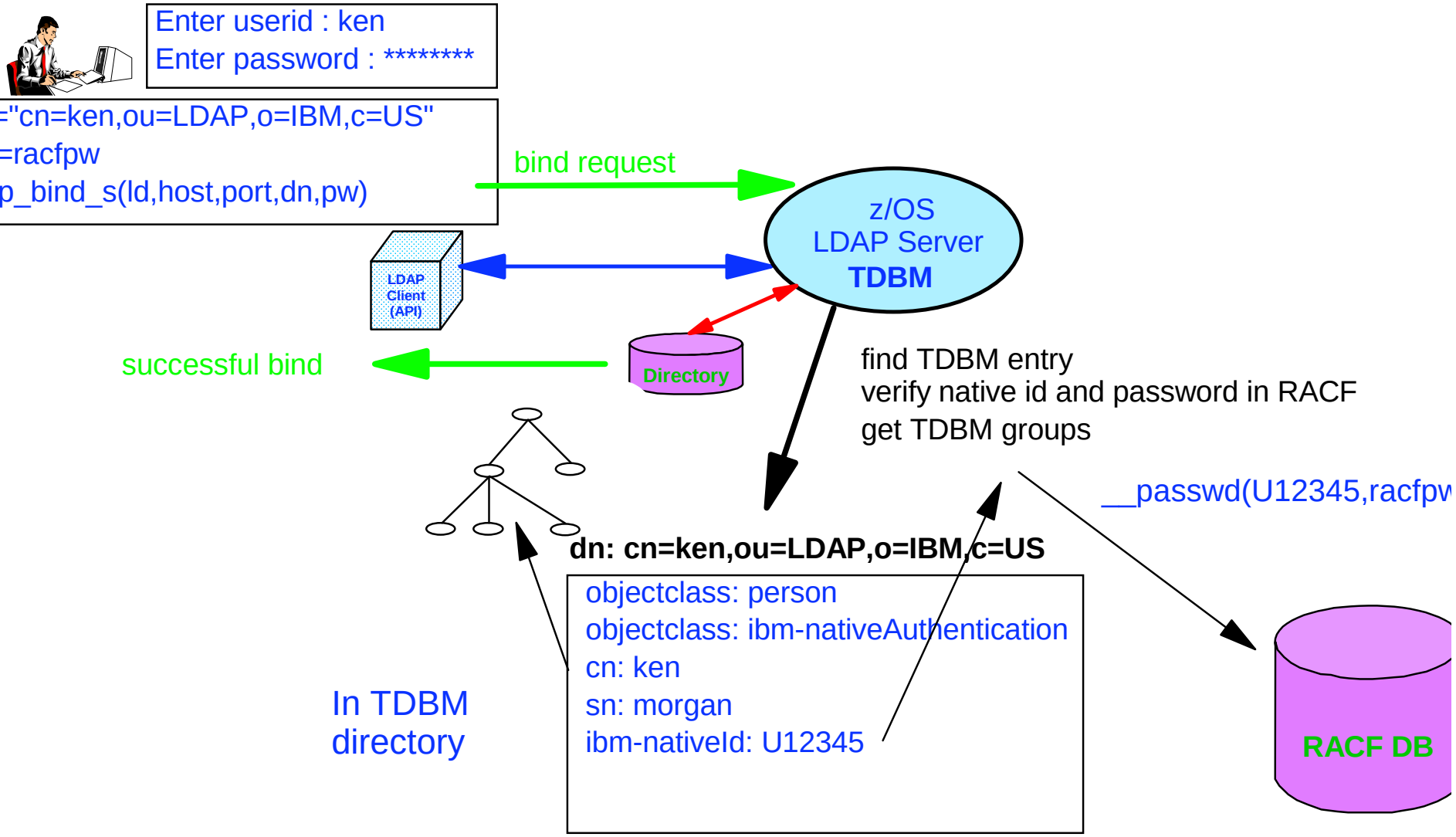
find RACF user entry
get RACF groups

RACF DB

z/OS LDAP Server Native Authentication

- **Disadvantage of authentication in RACF:**
  - **SDBM backend required**
  - **Nonstandard Distinguished Name (racfid, profiletype)**
  - **Fixed schema: only RACF information is available, cannot add attributes to contain additional information**
- **Native Authentication uses TDBM backend**
  - **Standard Distinguished Name (e.g. cn, ou, o)**
  - **Any schema supported by LDAP V3 for entry can be used**
    - **Any information supported by the schema can be retrieved**
    - **Use TDBM groups and group membership in ACLs**
  - **Authentication (password verification) performed by RACF**
    - **Password for entry is in security server (not in TDBM)**
    - **No need for administration or synchronization of multiple password registries**
    - **RACF authentication triggered by attribute ibm-nativeId in TDBM entry**
  - **Can limit native authentication to specific TDBM subtrees or entries - some entries use RACF, others have passwords in entry**

LDAP Native Authentication

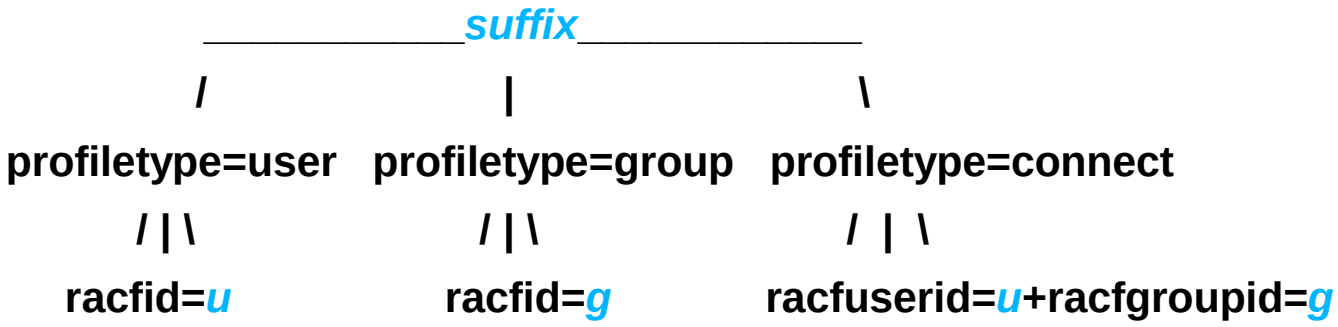


Accessing RACF via LDAP

SDBM Support of RACF

- **Use LDAP to add, modify, delete, display RACF users, groups, and user-group connections - remote admin**
  - **Equivalent to RACF commands: ADDUSER, ALTUSER, DELUSER, LISTUSER, ADDGROUP, ALTGROUP, DELGROUP, LISTGRP, CONNECT, REMOVE**

- **SDBM directory structure**



example DN: racfid=kmorgan,profiletype=user,cn=myRacf

- **Limited search capabilities - predefined by SDBM**
- **All data accessed via RACF**
  - **No RACF Data in LDAP**
  - **Authorization controled by RACF, based on bound userid**

SDBM Support of RACF- cont

- **Hard coded schema definitions**
  - **Each RACF user/group/connect profile segment mapped to an LDAP object class**
    - Example:
      User OMVS segment <---> racfUserOmvsSegment object class
    - Object class contains all the attributes in that segment
  - **Each RACF add/alt/listuser, add/alt/listgrp, connect keyword mapped to an LDAP attribute**
    - Example: OMVS UID keyword <---> racfOmvsUid attribute

Using SDBM - Examples

- **Example: add a RACF user entry**
  - **Create a file, u1234.add, containing entry to be added:**

```
dn: racfid=U1234,profiletype=user,cn=myRacf
objectclass: racfUser
objectclass: racfUserOmvsSegment
racfid: u1234
racfdefaultgroup: dce1
racfowner: radmin
racfattributes: special
racfomvsuid: 321
racfomvshome: /home/u1234
```

  - **Invoke ldapadd utility:**

```
ldapadd   -h dceset3.ibm.com   -p 2803
 -D racfid=radmin,profiletype=user,cn=myRacf  -w radminpw  -f u1234.add
```

  - **SDBM executes:**

```
ADDUSER u1234 OWNER(radmin) DFLTGRP(dce1) special
  OMVS(UID(321) HOME(/home/u1234))
```

Using SDBM - Examples cont.

- **Example: display a RACF user-group connection**
  - **Invoke ldapsearch utility:**

```
ldapsearch -h dceset3.ibm.com  -p 2803
  -D racfid=radmin,profiletype=user,cn=myRacf   -p radminpw    -L
  -b racfuserid=u1234+racfgroupid=dce1,profiletype=connect,cn=myracf
  objectclass=*
```

  - **SDBM executes LISTUSER u1234 and returns connection info for group dce1**

```
dn: racfuserid=u1234+racfgroupid=dce1,profiletype=connect,cn=myracf
objectclass: racfConnect
racfuserid: u1234
racfgroupid: dce1
racfconnectowner: racfid=RADMIN,profiletype=user,cn=myRacf
racfconnectgroupauthority=USE
racfconnectauthdate=04.279
...
```

Changing the RACF Password

- **ldapmodify can be used to change RACF password**
  - **Via SDBM:**

```
dn: racfid=u1234,profiletype=user,cn=myRACF
replace: racfPassword
racfpassword: mynewpw
racfattributes: noexpired
```

  - **Via TDBM with native authentication**

```
dn: cn=ken,ou=LDAP,o=ibm,c=us
delete: userPassword
userPassword: kenldap
-
add: userPassword
userPassword: mynewpw
-
```

    - Note: replace: userPassword cannot be used - not supported

- **LDAP SDBM or native authentication bind can be used to change a password (even if expired)**
  - **Specify *old_password/new_password*** when binding

RACF Change Logging

LDAP-RACF Change Logging

- **Provides way to propagate RACF user changes (including password changes) to other systems**
- **RACF part:**
  - **Notifies LDAP when a change to a user occurs**
  - **Creates PKCS7 envelope containing clear password**
- **LDAP part:**
  - **Creates an entry containing the RACF info in the changelog directory (in change log backend - GDBM)**
    - **Can access entry using normal LDAP operations from any LDAP client**
  - **Retrieves RACF password envelope via LDAP SDBM search**
- **Used by IBM Tivoli Directory Integrator to synchronize passwords:**
  - **Periodically does LDAP search of change log for new entries**
  - **If password changed, performs LDAP search of RACF user to retrieve enveloped password**
  - **Decrypts envelope and sets password on other systems**

Change Log SPE - continued

- **Searching the change log**

  ldapsearch … -b cn=changelog changenumber>=1023

  dn: CHANGENUMBER=1023,CN=CHANGELOG
  objectclass: CHANGELOGENTRY
  objectclass: IBM-CHANGELOG
  changenumber: 1023
  targetdn: racfid=U1234,profiletype=user,CN=MYRACF
  changetime: 20030611161820.374472Z
  changetype: MODIFY
  changes: replace: racfpassword
  racfpassword: *ComeAndGetIt*
  -

  ibm-changeinitiatorsname: racfid=radmin,profiletype=user,CN=MYRACF

- **Retrieving RACF envelope containing new password**

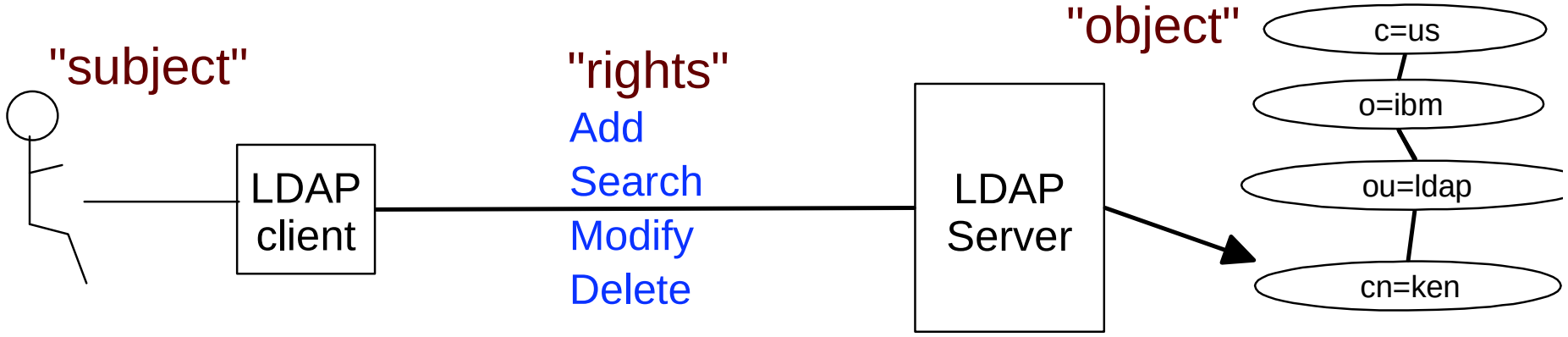
  ldapsearch –D racfid=radmin,profiletype=user,cn=myRacf
  –w radminpw –L -b racfid=U12345,profiletype=user,cn=myRacf
  “objectclass=*” racfpasswordenvelope

  racfid=U12345,profiletype=USER,cn=myRacf
  racfpasswordenvelope:: *base-64_encoded_password_envelope*

Access Control in TDBM

Access Control Checking

- **Does subject have the right to perform the requested operation on an object?**
  - **"subject" - the "bound" LDAP client identity: DN of requestor + DNs of groups to which requestor belongs**
  - **"object" - the entries or the attributes of the entries involved in the operation**
  - **"rights" - the access required to perform the requested operation (add/delete entry, read/write/search/compare attribute)**



Access Control Implementation

- **TDBM uses an Access Control List (ACL) to control access to an entry**
- **Can specify TDBM and SDBM (RACF) users and groups**
- **Can control access to individual attributes or to classes of attributes (normal, sensitive, critical, restricted and system)**
  - **Attribute's access class defined in the schema**
- **Use LDAP modify operation to set ACL and search operation to display ACL info**
  - **examples:**

    aclentry: cn=jay,ou=LDAP,o=IBM,c=US:normal:rwsc:sensitive:rsc
    aclentry: racfid=morgankg,profiletype=user,cn=myRacf:object:ad
    aclentry: group:cn=mgrs,o=IBM,c=US:at:userpassword:rwsc
    aclentry:group:racfid=g1,profiletype=group,cn=myRacf:normal:rwsc
- **Can propagate an entry's ACL to the subtree below it**

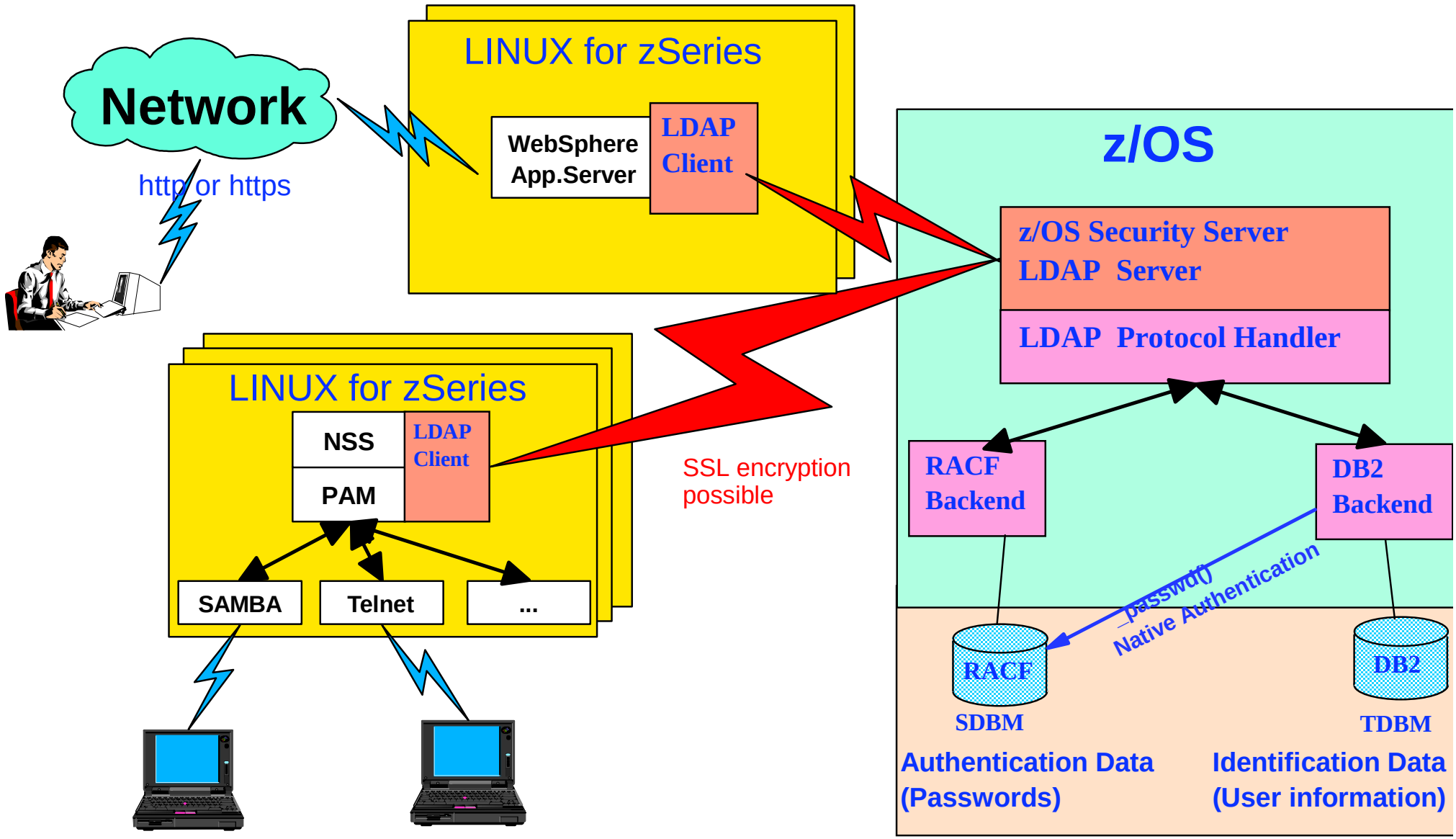
Special aclEntry "pseudo-DNs"

- **cn=anybody**
  - **Applies when no other specific ACL value applies**
- **cn=authenticated**
  - **Applies when the requestor has authenticated to the directory but no other specific ACL value applies**
  - **Meant to allow more access than cn=anybody ACL value**
- **cn=this**
  - **Applies when the requestor has authenticated with the same DN as the entry being accessed**
  - **Used to grant individuals access to their own entry**
- **Example:**

```
aclentry: cn=anybody:normal:rsc
aclentry: cn=authenticated:normal:rsc:sensitive:rs
aclentry: cn=this:normal:rscw:sensitive:rscw:critical:rsc
```

The Big Picture

User Information and Authentication in LDAP



References:

- **z/OS LDAP Documentation**
  - **SC24-5923 z/OS Integrated Security Services LDAP Server Administration and Usage Guide**
    - **http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/ICHZBK42**
  - **SC24-5924 z/OS Integrated Security Services LDAP Client Programming**
    - **http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/ICHZBK42**
- **Redpaper: Linux on IBM zSeries and S/390: Securing Linux for zSeries with a Central z/OS LDAP Server (RACF)**
  - **http://www.redbooks.ibm.com/redpapers/abstracts/redp0221.html**
- **PAM Documentation:**
  - **http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-4.html**
- **NIS Schema for z/OS LDAP Server:**
  - **ftp://www.redbooks.ibm.com/redbooks/REDP0221**
- **Contacting me**
  - **e-mail: morgankg@us.ibm.com**