IBM eServer™

Enterprise Identity Mapping

Vanguard Enterprise Security Expo

Reno, Nevada

17 June 2004

Peggy LaBelle
z/OS Security (EIM & RACF) Development and Test
IBM Poughkeepsie
plabelle@us.ibm.com

Trademarks

- The following are trademarks or registered trademarks of International Business Machines Corporation:

  AIX, CICS, DB2, DFSMS, eServer, Hiper Batch, IBM, IMS, iSeries, MVS/ESA, Open Edition, OS/390, OS/400, pSeries, PSF, RACF, Tivoli, VTAM, xSeries, z/OS, zSeries

- The following are trademarks or registered trademarks of other companies or institutions:

  BlueNotes, DCE, Distributed Computing Environment, NetWare, Novell, NT, Microsoft Corporation, Open Software Foundation, Open Software Foundation, Inc., OSF, safestone, TriAWorks, UNIX,

- Other company, product, or service names may be trademarks or service marks of others.

Disclaimer

The information contained in this document is distributed on an “as is” basis without any warranty either expressed or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in it’s own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM’s licensed programs may be used. Functionally equivalent programs 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 environment.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming, or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

Trademarks

The following are trademarks or registered trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- AIX
- DB2
- eServer
- OS/400
- pSeries
- RACF
- xSeries
- z/OS
- zSeries

The Open Group:

- UNIX is a registered trademark of The Open Group in the United States and other countries

Other company, product or service names may be trademarks or service marks of others.

Session Objectives

- **What is Enterprise Identity Mapping**
  - Purpose
  - Content
  - Benefits
- **Writing an EIM application**
- **Setting up EIM using z/OS eimadmin tool**
- **Publications and References**

Enterprise Identity Mapping

- Observation:

  There is a lot of software in an enterprise that maps one user id to another.

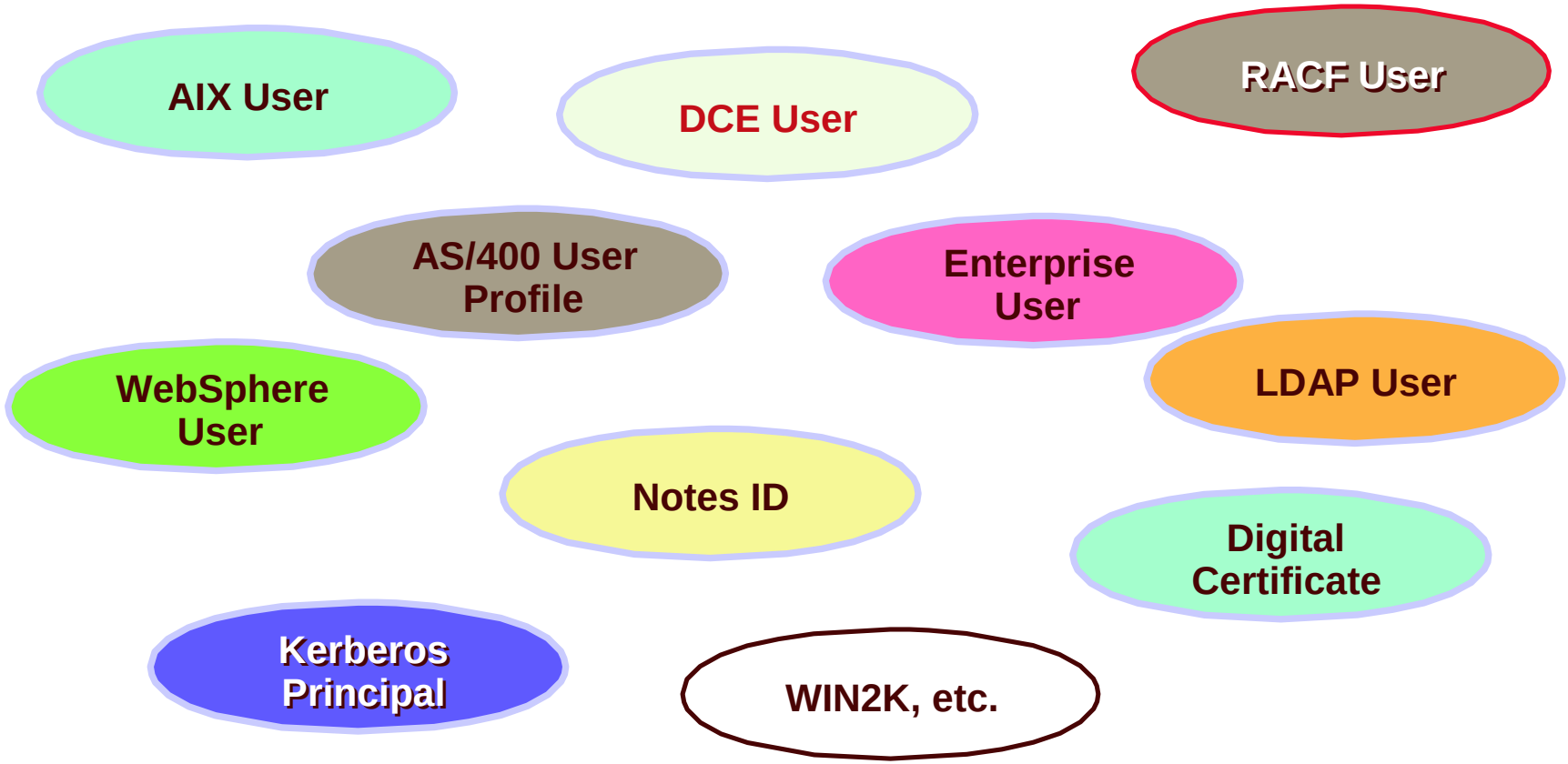
- Idea:

  Store the mappings in a central location accessible to all of the software.

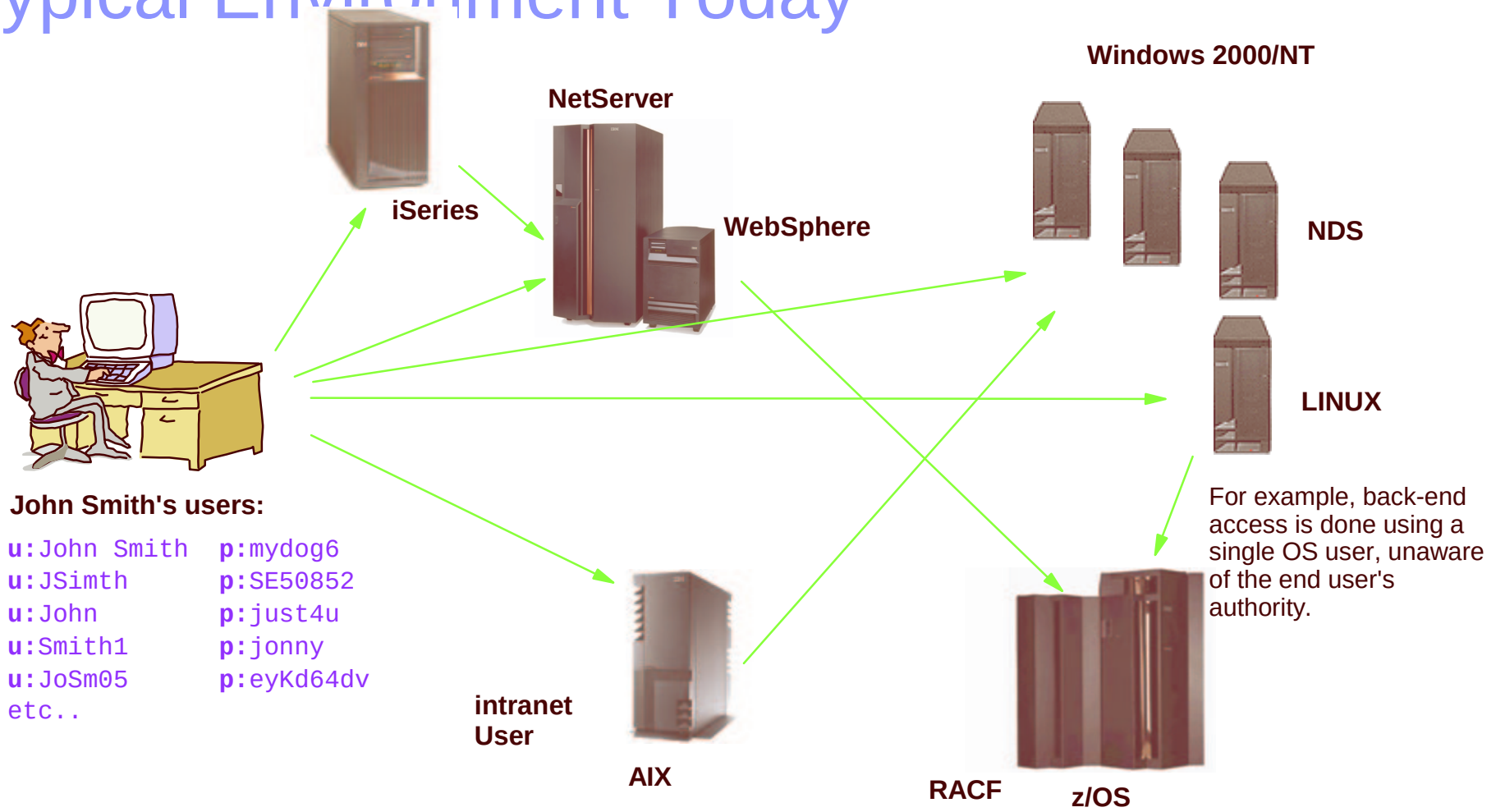
- Result:

  Seamless distributed applications with better security

Multiple User Registries Problem



Typical Environment Today

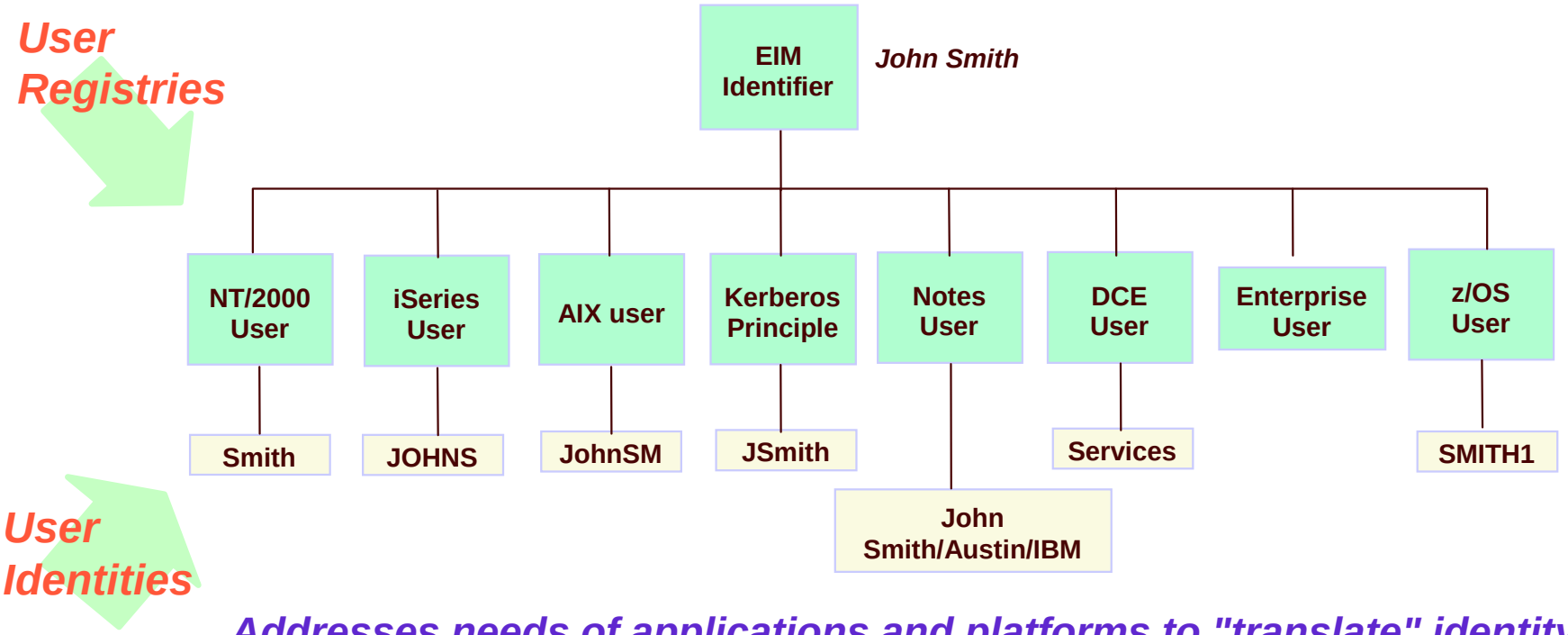


Administrative Nightmare !!
Enterprise "Trust Scope"?

X-model transactions ?
Single Sign-on?

Enterprise Identity Mapping

- **EIM defines** associations between an identifier and user ids in registries that are part of OS platforms, applications, and middle-ware.
- The identity associations (*mappings*) are stored in a well known location, e.g. LDAP, with common services across platforms to access the mappings.



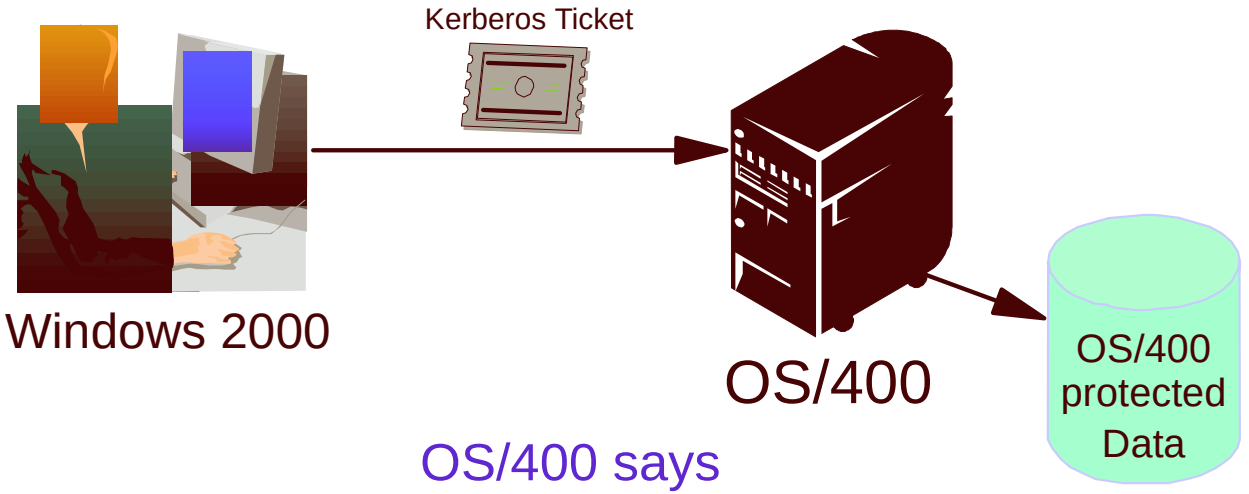
Addresses needs of applications and platforms to "translate" identity when crossing platform and registry boundaries.

Enterprise Identity Mapping Example – OS/400

Authentication vs. Authorization

Client application says
"I am 'patriciaboats@MYCOM.WIN2KDOMAIN1' and here's proof. "

Kerberos addresses
authentication only



OS/400 says
"I know who you are over **there**; but I need to know who you are over **here** to determine what you can access over here."

EIM Enhanced Kerberos Sign-on

Server B (z/OS)

EIM Domain Controller

Identifier: John N. Smith

Registry:	User:	Type	Association
DomServer	John Smith	Kerberos	Source
ServerB	JSMITH	RACF	Target
IntraNet	JohnS	AIX	Target
SysA	JS50852	OS/400	Target

IntraNet Server (AIX)

Key Distribution Center (KDC)

AS TGS

Hey, who is this Kerberos user John Smith in DomServer on SYSA?

I know, that's JS50852

Can I have a ticket For SysA? I am John Smith.

Sure.

1 2 3 4 5 6

John

Here's my ticket. Can you let me in?

Oh. Welcome JS50852

Domain Server A on OS/400
Requesting TGT steps not shown

System A (OS/400)

Ideas for EIM…

- Replace side files that contain mappings of user IDs
- Retrieve a mapping at exit points in servers where a host user ID/password is usually required (aka “single sign-on”)

  Note: ensure trusted source
- Write an application that uses EIM mappings to correlate audit data across systems

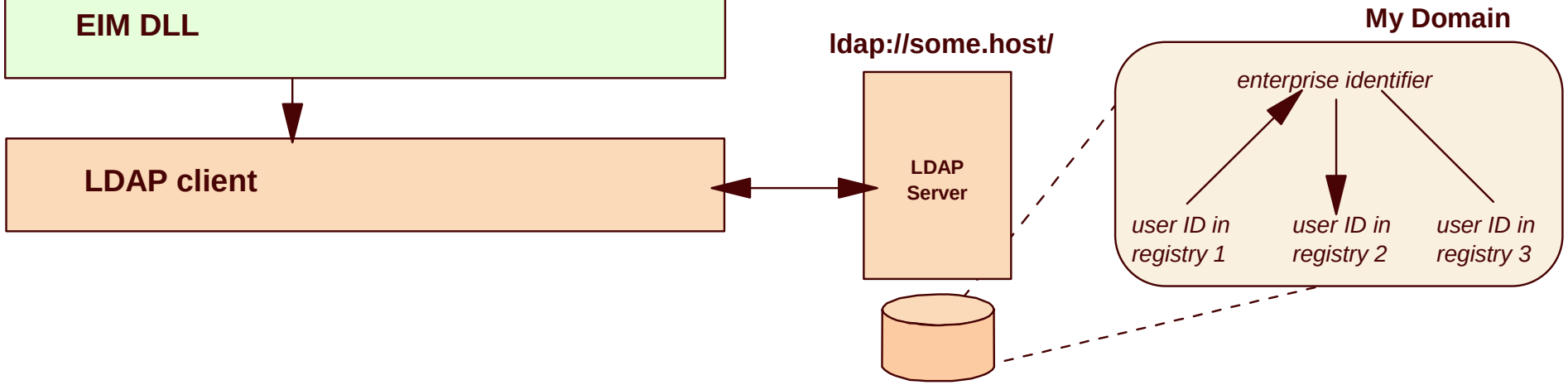
Writing EIM Applications

C/C++ Lookup Application

```
/* obtain an identity, ex. principal @ realm */
call eimCreateHandle (...)
call eimConnect(...)

call eimGetTargetFromSource(...)
/* assert the new identity */
/* access local resources */

call eimDestroyHandle(...)
```



EIM APIs

Lookup APIs

- eimGetTargetFromSource, eimGetTargetFromIdentifier, eimGetAssociatedIdentifiers

Administration APIs

- Domain operations
- Registry operations
- EIM Identifier operations
- User Management operations

Common APIs

- EIM “handle” operations

System operations

- Configure system with a default domains, bind credentials, and registry names

Planning Considerations for EIM

Recommendation:

Let applications and users drive initial deployment of EIM

Information needed about the application
The platforms you plan to run the application on
- The types and names of the local registries
Types EIM associations required and additional information
- Source, Target, Admin
Any system specific configuration requirements
- ex. IRR.EIM.DEFAULTS or IRR.PROXY.DEFAULTS profiles
EIM connection protocol required (i.e. LDAP bind protocol)
- simple, simple + CRAM-MD5, Kerberos, SSL
General idea of who in your enterprise will use the application

Planning Considerations for EIM…

Choose an IBM LDAP directory for hosting the EIM domain controller

- Must be accessible to the components of the application
- Must support the EIM connection protocol
- Options for the LDAP server
  - platform, one server, referrals, master and replicas, sysplex, dedicated directory or shared with other applications

Planning Considerations for EIM…

Administration of the EIM domain
- LDAP administrator and/or
- EIM administrator
- EIM identifier administrator
- EIM registries administrator
- EIM registry xyz administrator

Naming conventions for
- The domain
- The registries
  - type and/or system and/or location in network …
- The enterprise identifiers
  - A person's name vs employee number vs …