



# eServer Single Sign-On Enablement and More

*IBM @server iSeries*

**Patrick Botz**  
**eServer Security Architect**

© Copyright IBM Corporation, 2002. All Rights Reserved.

This publication may refer to products that are not currently available in your country. IBM makes no commitment to make available any products referred to herein.

**IBM @server. For the next generation of e-business.**

# Agenda

---

IBM  server iSeries

Multiple User Registry Problem

New eServer Approach

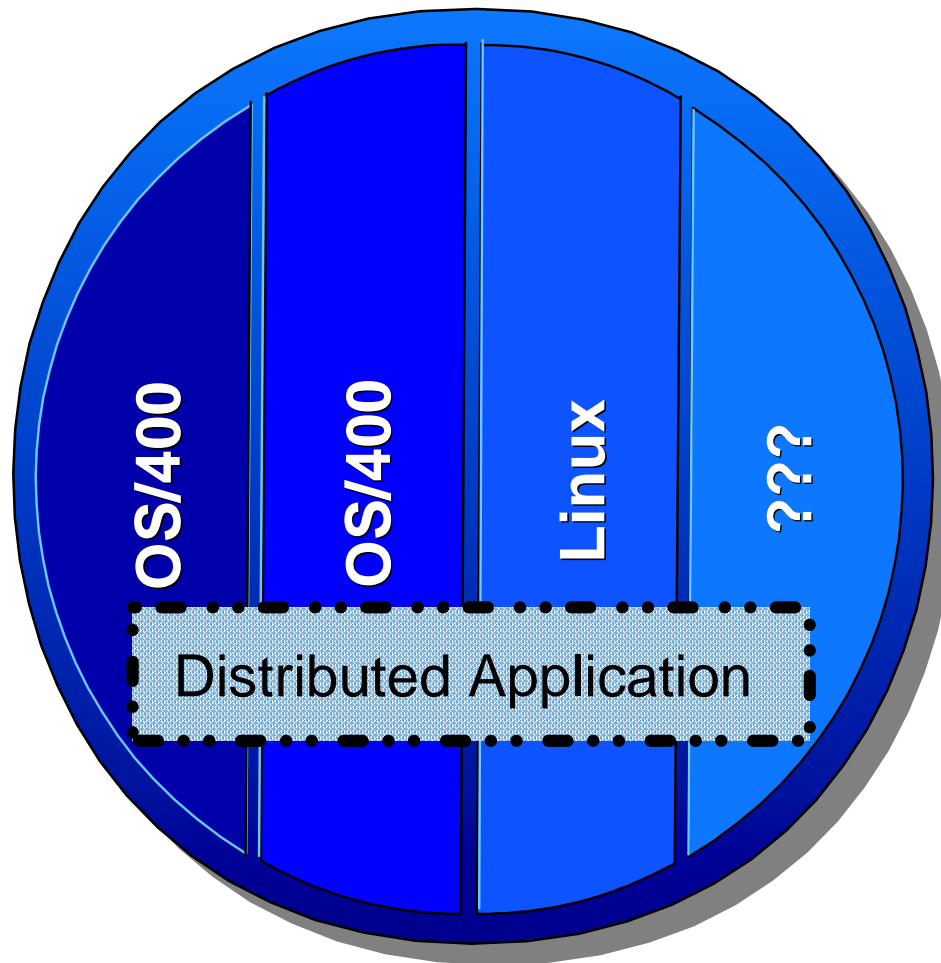
iSeries Exploitation

Architecture

Benefits for ISVs

IBM  server. For the next generation of e-business.

## Server Consolidation



Partitioned Systems

IBM  server. For the next generation of e-business.

# Problem Description

---

IBM  server iSeries

Every eServer platform (and many SWG products) have unique mechanisms for managing users (called User Registries).

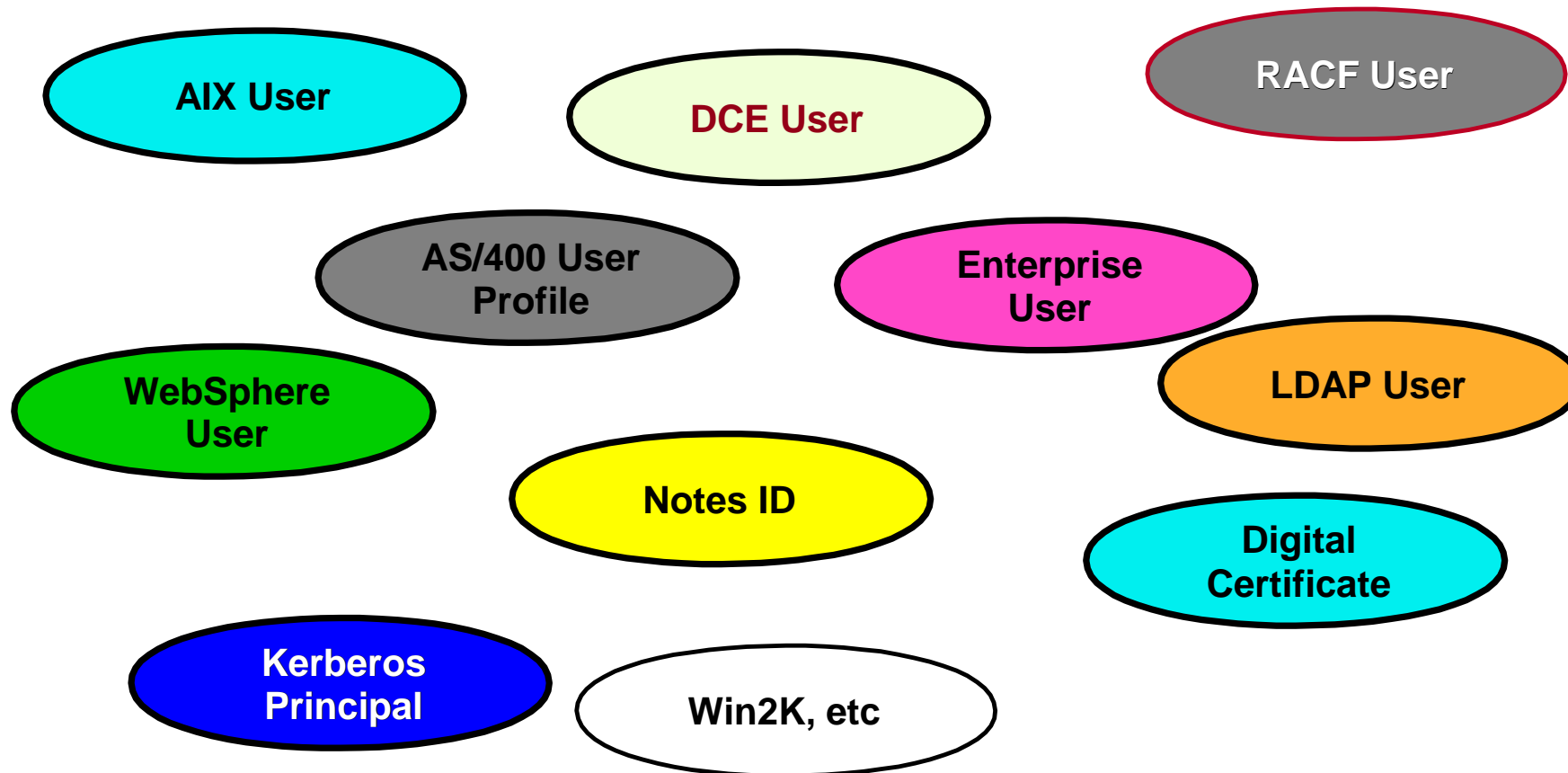
In today's world of Data/Transaction Servers, UNIX and NT servers, this becomes a severe problem for customers (and thus an opportunity to differentiate).

Systems Management application-based solutions (like Tivoli) do not meet the needs of all customers, nor do they provide any differentiation for eServer platforms - they run everywhere and manage everything.

IBM  server. For the next generation of e-business.

# Multiple User Registries Problem

IBM  server iSeries



*Administrative Nightmare !!*

*Single Signon ?*

*Enterprise "Trust Scope" ? X-model transactions ?*

IBM  server. For the next generation of e-business.

# Recommended Approach

## New Approach -- Enterprise Identity Mapping

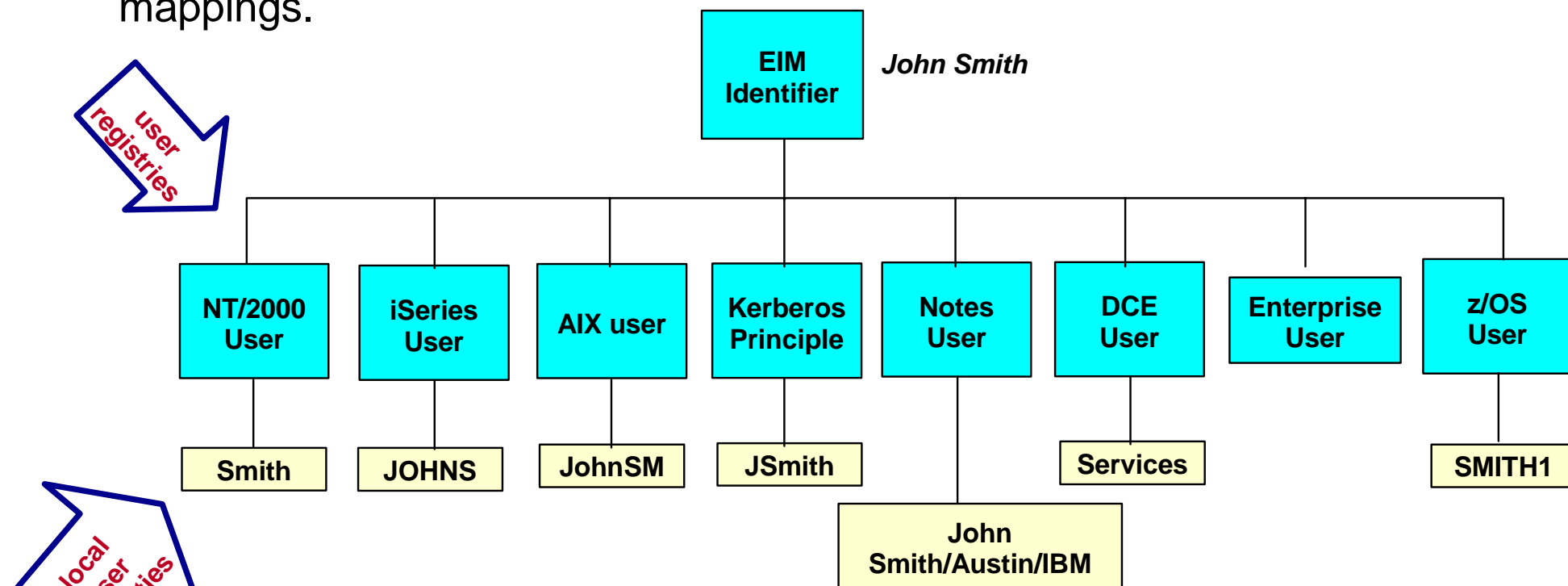
- Accept the fact that multiple registries (IBM and non-IBM) will exist in the enterprise
- Make it easy for customers to associate a user's multiple identities in the enterprise and to manage those associations
- Use IBM's platform breadth of software offerings to differentiate eServer platforms while providing a complete solution for heterogeneous environments
- Develop this in such a way that it can be extended to other facets of cross-platform management

IBM  server. For the next generation of e-business.

# Enterprise Identity Mapping

IBM  server iSeries

- **EIM defined:** Identity associations across user registries associated with 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 the run-time needs of applications and platforms which need to "translate" identity when crossing platform and registry boundaries with a set of common services.

IBM  server. For the next generation of e-business.

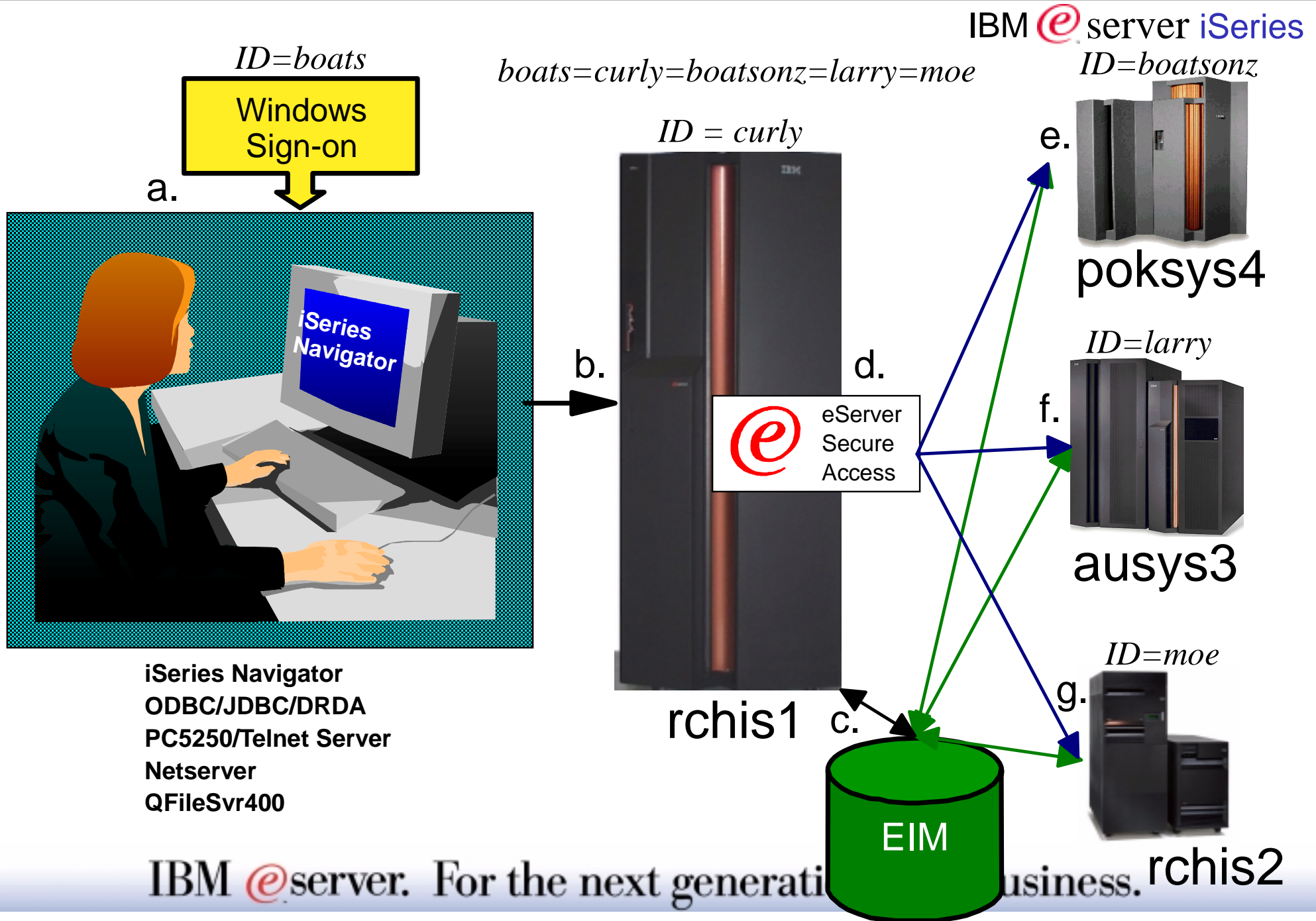
# eServer Single Sign-On

## Kerberos And EIM

IBM @server. For the next generation of e-business.



# Multi-system Security with eServer



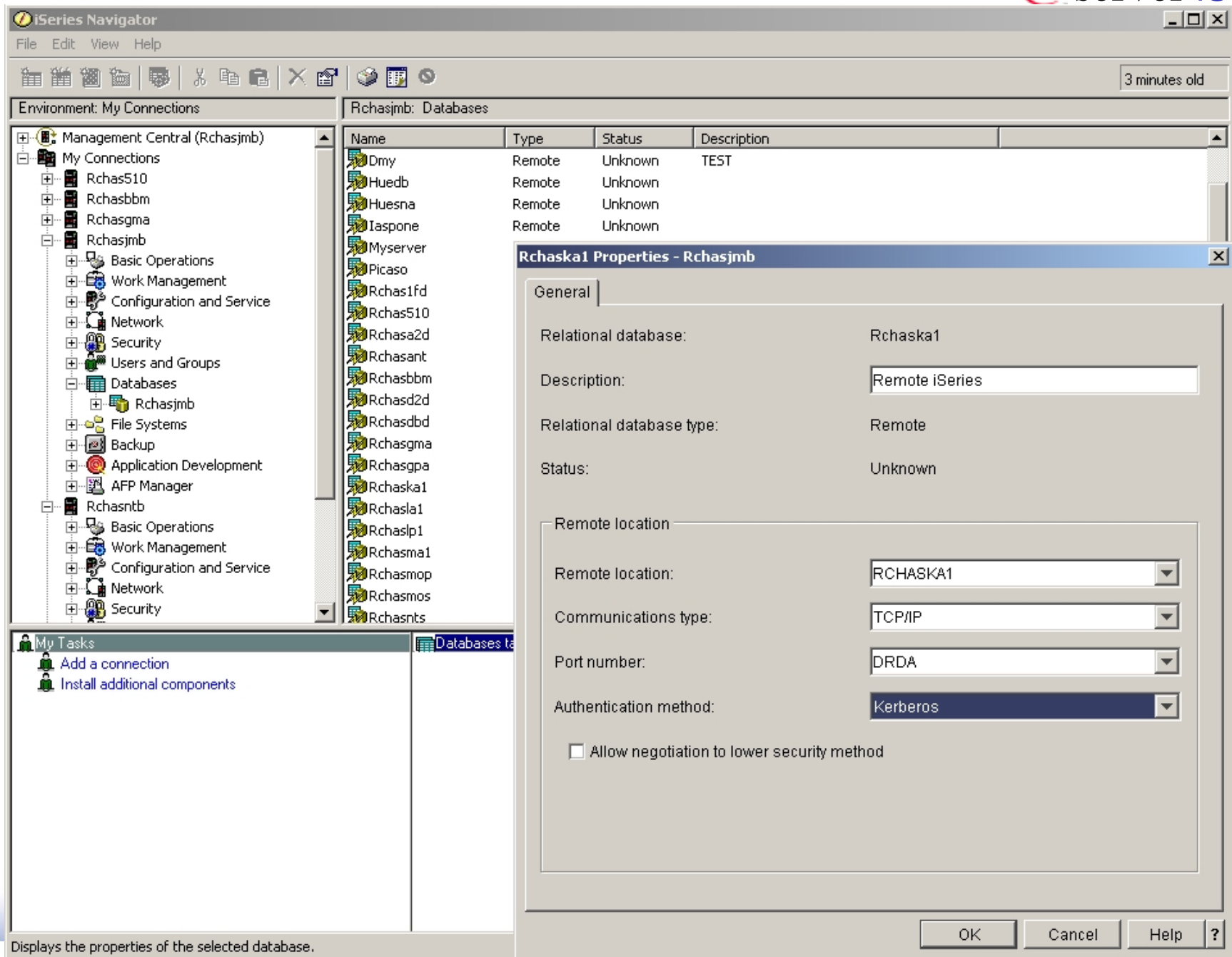
# Single Sign-On Process

- a. User signs on to Win2k as normal as "boats" (delegatable ticket)
  - Starts iSeries Navigator and points at system lpar2nzm (OS/400)
  - Navigates to Database section and pulls up the SQL Script tool.
  - SQL script
    - ▶ gets data from table **rchis1**
    - ▶ connects to system db2nsys (zOS) and gets data from table **poksys4**
    - ▶ connects to system lpar1nzm (OS/400) and gets data from table **rchis2**
    - ▶ displays all of the results
- b. Kerberos ticket flows for authentication from Win2k to lpar2nzm
- c. ODBC server validates Kerberos ticket and uses EIM to map to user CURLY and runs SQL to get data from table rchis1 on this system applying this system's security semantics (CURLY)
- d. SQL connect statement executes and the ODBC server does a DRDA connection to db2nsys flowing Kerberos ticket for authentication
- e. DRDA server on db2nsys accepts Kerberos ticket and maps to RACF ID BOATSONZ and accesses data applying RACF security semantics (BOATSONZ) and returns
- f. Same as d/e except table ausys3 and AIX user LARRY
- g. Same as d/e except lpar1nzm and table rchis2 and user profile MOE

**Retrieved data is returned to win2k system and displayed**

IBM  server. For the next generation of e-business.

# DRDA Configuration



The screenshot shows the iSeries Navigator interface. The left pane displays a tree view of 'My Connections' with 'Rchaskajmb' selected. The middle pane shows a list of databases with columns for Name, Type, Status, and Description. The right pane shows the 'Rchaska1 Properties - Rchaskajmb' dialog box with the following configuration:

Name	Type	Status	Description
Dmy	Remote	Unknown	TEST
Huedb	Remote	Unknown	
Huesna	Remote	Unknown	
Iaspone	Remote	Unknown	
Myserver			
Picaso			
Rchas1fd			
Rchas510			
Rchasa2d			
Rchasant			
Rchasbbm			
Rchasd2d			
Rchasdbd			
Rchasgma			
Rchasgpa			
Rchaska1			
Rchaska1			
Rchasp1			
Rchasma1			
Rchasmop			
Rchasmos			
Rchasnts			

**Rchaska1 Properties - Rchaskajmb**

General

Relational database: Rchaska1

Description: Remote iSeries

Relational database type: Remote

Status: Unknown

Remote location

Remote location: RCHASKA1

Communications type: TCP/IP

Port number: DRDA

Authentication method: Kerberos

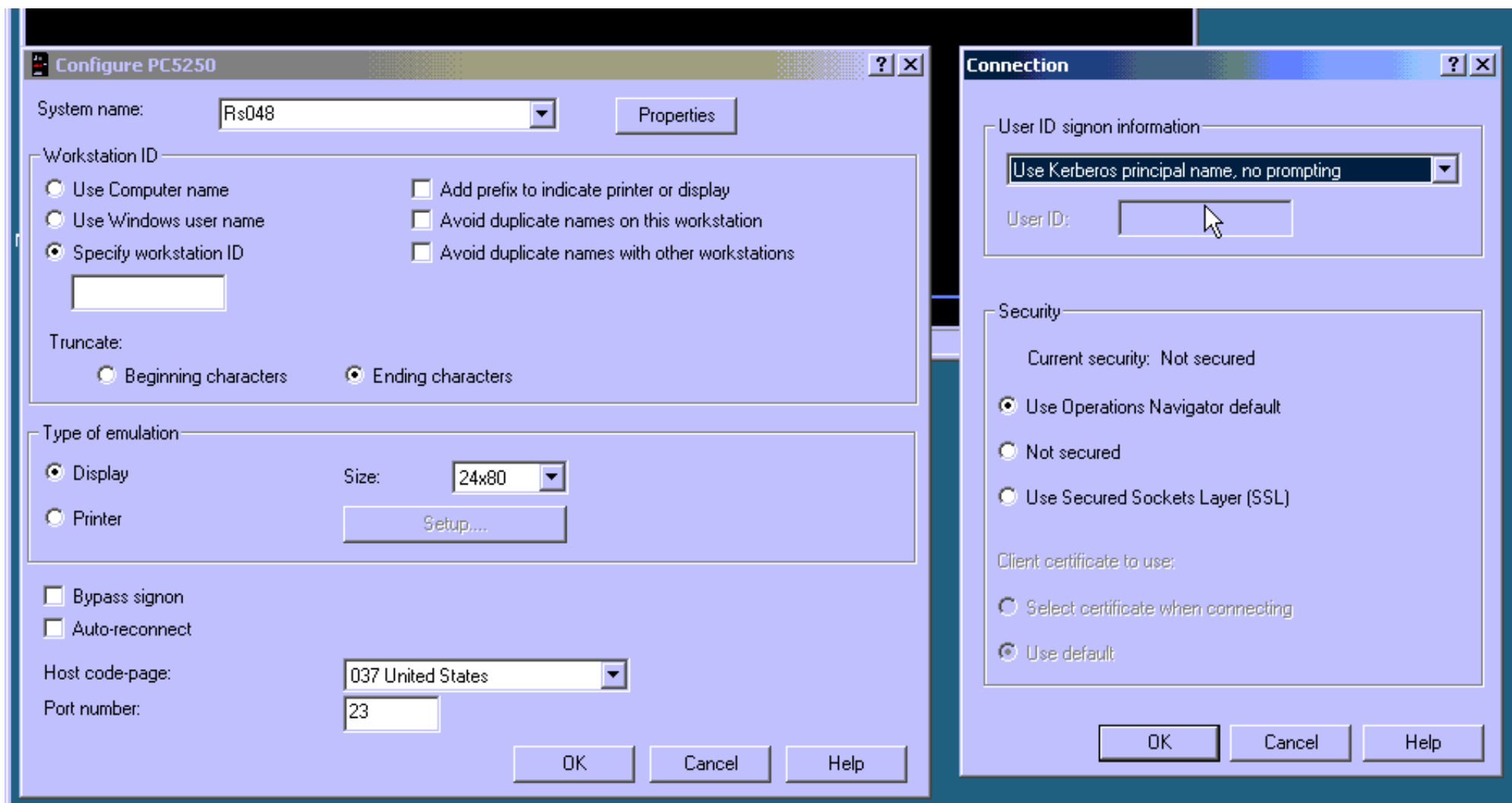
Allow negotiation to lower security method

OK Cancel Help ?

Displays the properties of the selected database.

# Client Access/PC5250 Configuration

IBM  server iSeries



The image shows two overlapping dialog boxes from the Client Access/PC5250 configuration utility. The 'Configure PC5250' dialog is on the left, and the 'Connection' dialog is on the right.

**Configure PC5250 Dialog:**

- System name:** Rs048
- Workstation ID:**
  - Use Computer name
  - Use Windows user name
  - Specify workstation ID
- Truncate:**
  - Beginning characters
  - Ending characters
- Type of emulation:**
  - Display
  - Printer
- Size:** 24x80
- Bypass signon
- Auto-reconnect
- Host code-page:** 037 United States
- Port number:** 23

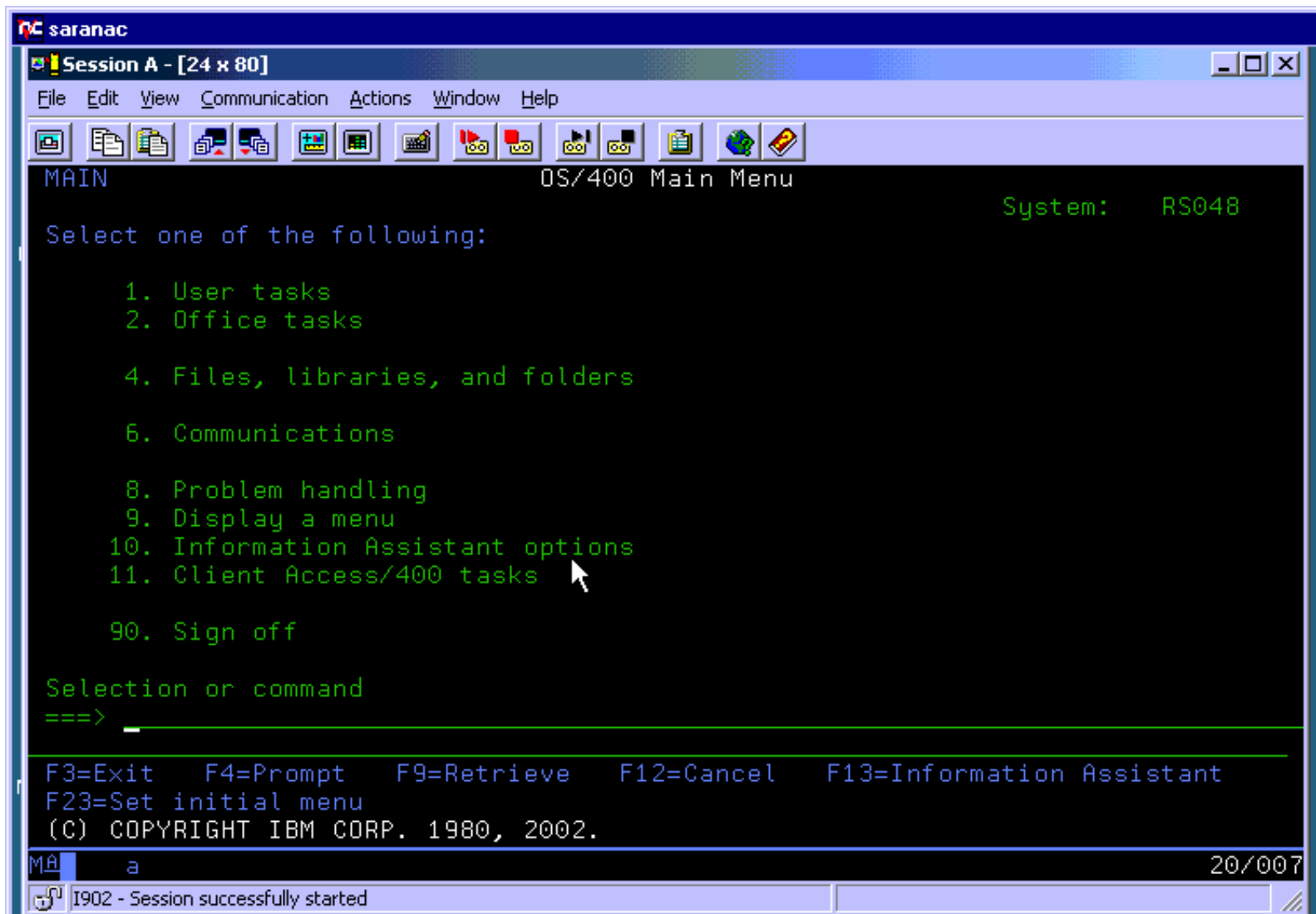
**Connection Dialog:**

- User ID signon information:**
  - Use Kerberos principal name, no prompting
  - User ID: [ ]
- Security:**
  - Current security: Not secured
  - Use Operations Navigator default
  - Not secured
  - Use Secured Sockets Layer (SSL)
- Client certificate to use:**
  - Select certificate when connecting
  - Use default

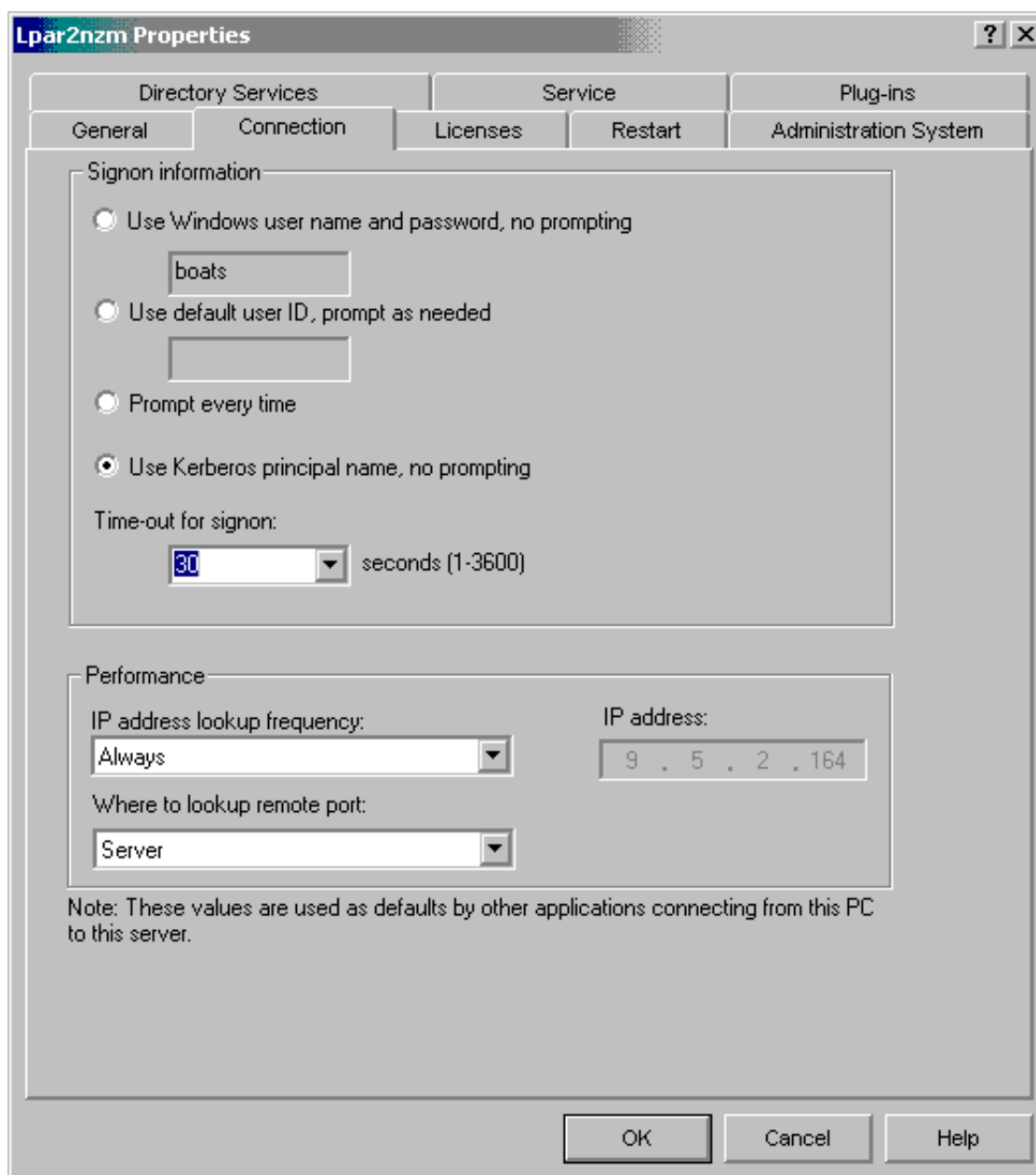
IBM  server. For the next generation of e-business.

# Telnet, Bypass Sign-On

IBM @server iSeries



IBM @server. For the next generation of e-business.



The screenshot shows the 'Lpar2nzm Properties' dialog box with the 'Connection' tab selected. The 'Signon information' section has four radio buttons: 'Use Windows user name and password, no prompting' (selected), 'Use default user ID, prompt as needed', 'Prompt every time', and 'Use Kerberos principal name, no prompting'. Below these is a 'Time-out for signon:' field set to '30' seconds. The 'Performance' section has three dropdown menus: 'IP address lookup frequency' set to 'Always', 'IP address' set to '9 . 5 . 2 . 164', and 'Where to lookup remote port' set to 'Server'. A note at the bottom states: 'Note: These values are used as defaults by other applications connecting from this PC to this server.' Buttons for 'OK', 'Cancel', and 'Help' are at the bottom right.

**Lpar2nzm Properties**

Directory Services    Service    Plug-ins

General    Connection    Licenses    Restart    Administration System

Signon information

Use Windows user name and password, no prompting  
boats

Use default user ID, prompt as needed

Prompt every time

Use Kerberos principal name, no prompting

Time-out for signon:  
30 seconds (1-3600)

Performance

IP address lookup frequency: Always

IP address: 9 . 5 . 2 . 164

Where to lookup remote port: Server

Note: These values are used as defaults by other applications connecting from this PC to this server.

OK    Cancel    Help

IBM  server. For the next generation of e-business.

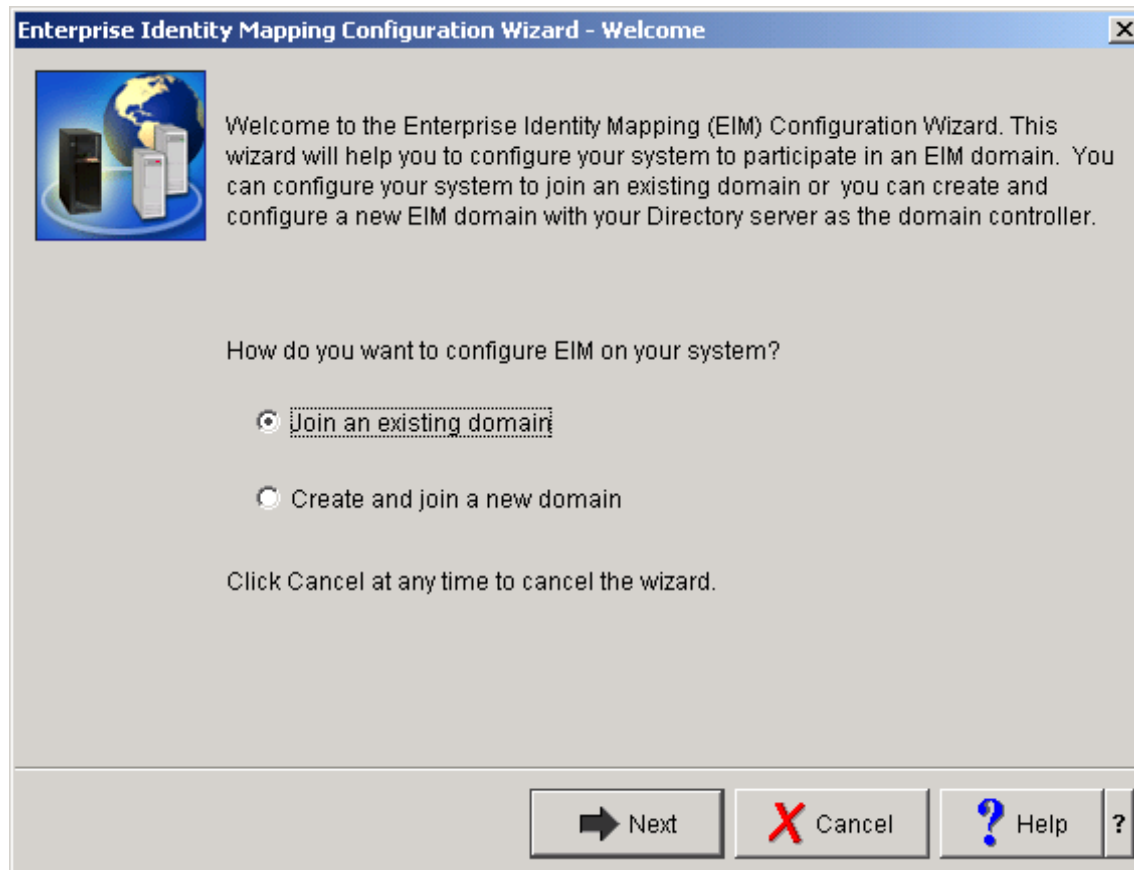
# Administering EIM

- ▶ Create EIM Domain
- ▶ Create EIM identifier for people/entities
- ▶ Define third party user registries to EIM domain
- ▶ Configure systems to participate in EIM domain
- ▶ Associate user identities with EIM identifiers
- ▶ Create replicas of EIM Domains if desired

IBM  server. For the next generation of e-business.

# EIM Domain Creation/Configuration Wizard

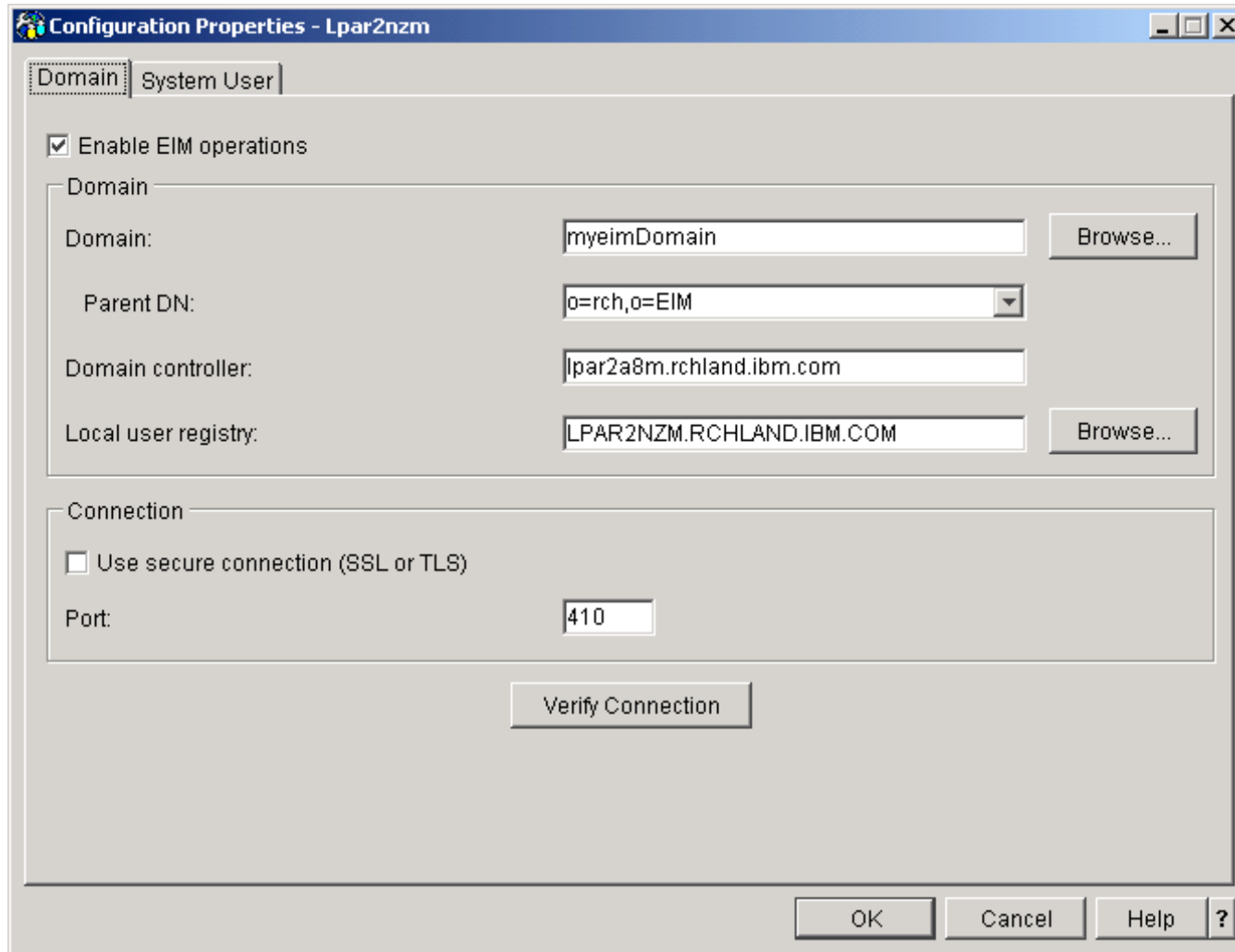
IBM  server iSeries



IBM  server. For the next generation of e-business.



# Configuring a System to Use EIM



**Configuration Properties - Lpar2nzm**

Domain | System User

Enable EIM operations

Domain

Domain: myeimDomain

Parent DN: o=rch,o=EIM

Domain controller: lpar2a8m.rchland.ibm.com

Local user registry: LPAR2NZM.RCHLAND.IBM.COM

Connection

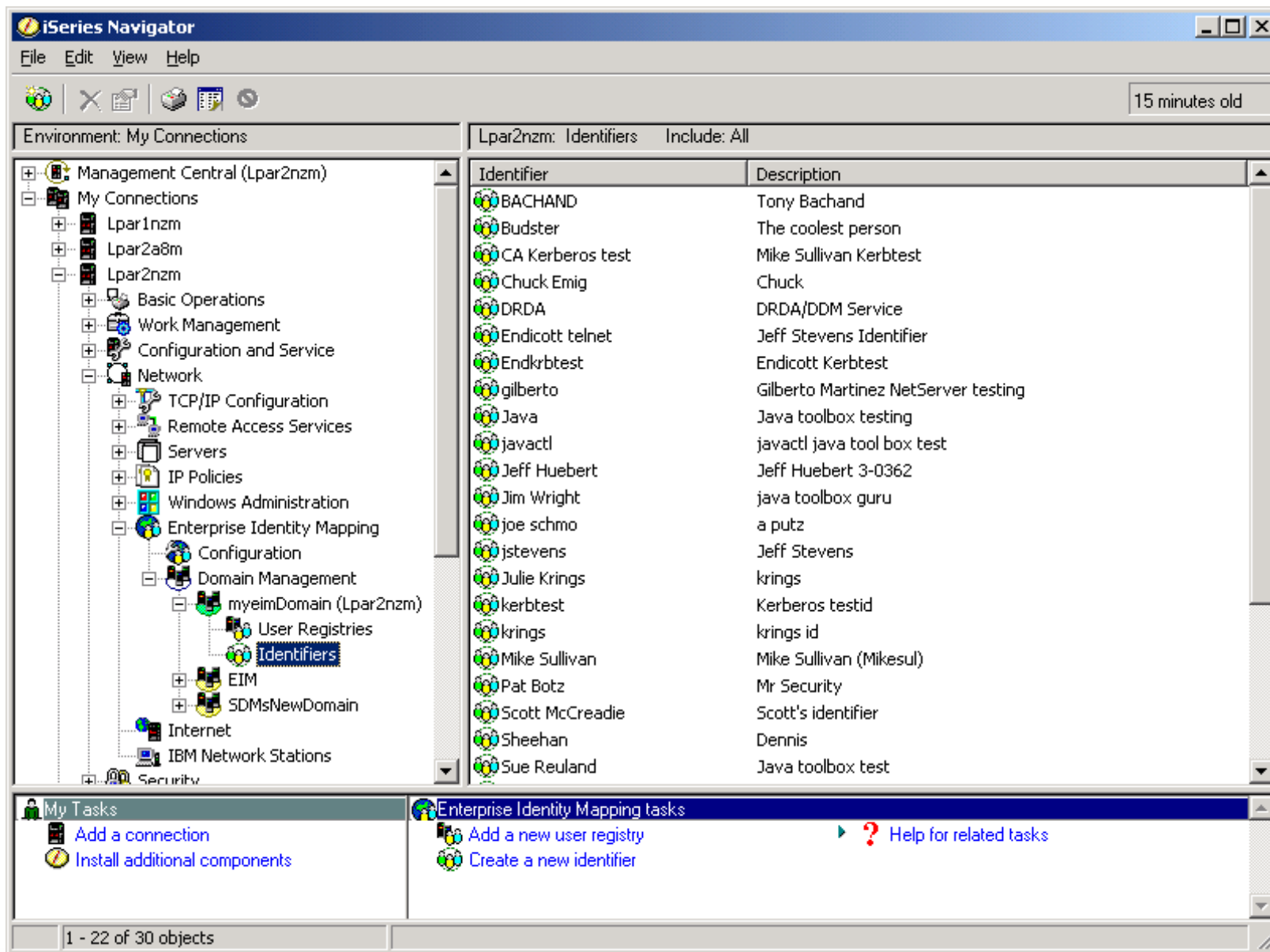
Use secure connection (SSL or TLS)

Port: 410

?

# Managing EIM

IBM  server iSeries



The screenshot displays the iSeries Navigator application window. The left pane shows a tree view of the system configuration, with 'Enterprise Identity Mapping' expanded to show 'Identifiers'. The right pane displays a table of identifiers with their descriptions.

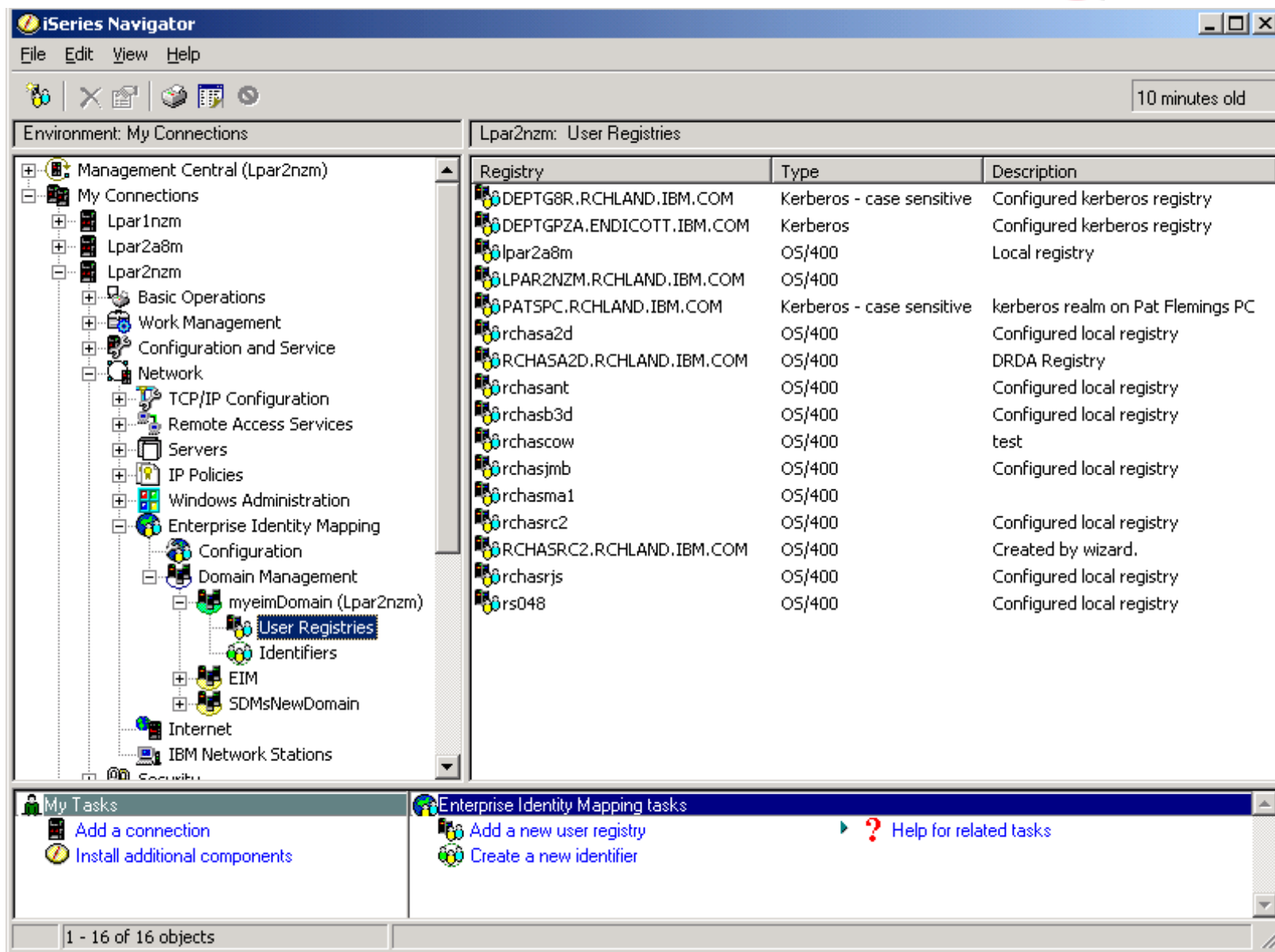
Identifier	Description
BACHAND	Tony Bachand
Budster	The coolest person
CA Kerberos test	Mike Sullivan Kerbtest
Chuck Emig	Chuck
DRDA	DRDA/DDM Service
Endicott telnet	Jeff Stevens Identifier
Endkrbtest	Endicott Kerbtest
gilberto	Gilberto Martinez NetServer testing
Java	Java toolbox testing
javactl	javactl java tool box test
Jeff Huebert	Jeff Huebert 3-0362
Jim Wright	java toolbox guru
joe schmo	a putz
jstevens	Jeff Stevens
Julie Krings	krings
kerbtest	Kerberos testid
krings	krings id
Mike Sullivan	Mike Sullivan (Mikesul)
Pat Botz	Mr Security
Scott McCreadie	Scott's identifier
Sheehan	Dennis
Sue Reuland	Java toolbox test

At the bottom of the window, the 'My Tasks' pane shows 'Enterprise Identity Mapping tasks' with options: 'Add a new user registry' and 'Create a new identifier'. A status bar at the bottom indicates '1 - 22 of 30 objects'.

IBM  server. For the next generation of e-business.

# Managing EIM

IBM  server iSeries



The screenshot displays the iSeries Navigator application window. The title bar reads "iSeries Navigator" and the menu bar includes "File", "Edit", "View", and "Help". A toolbar with various icons is located below the menu bar. The main window is divided into three panes:

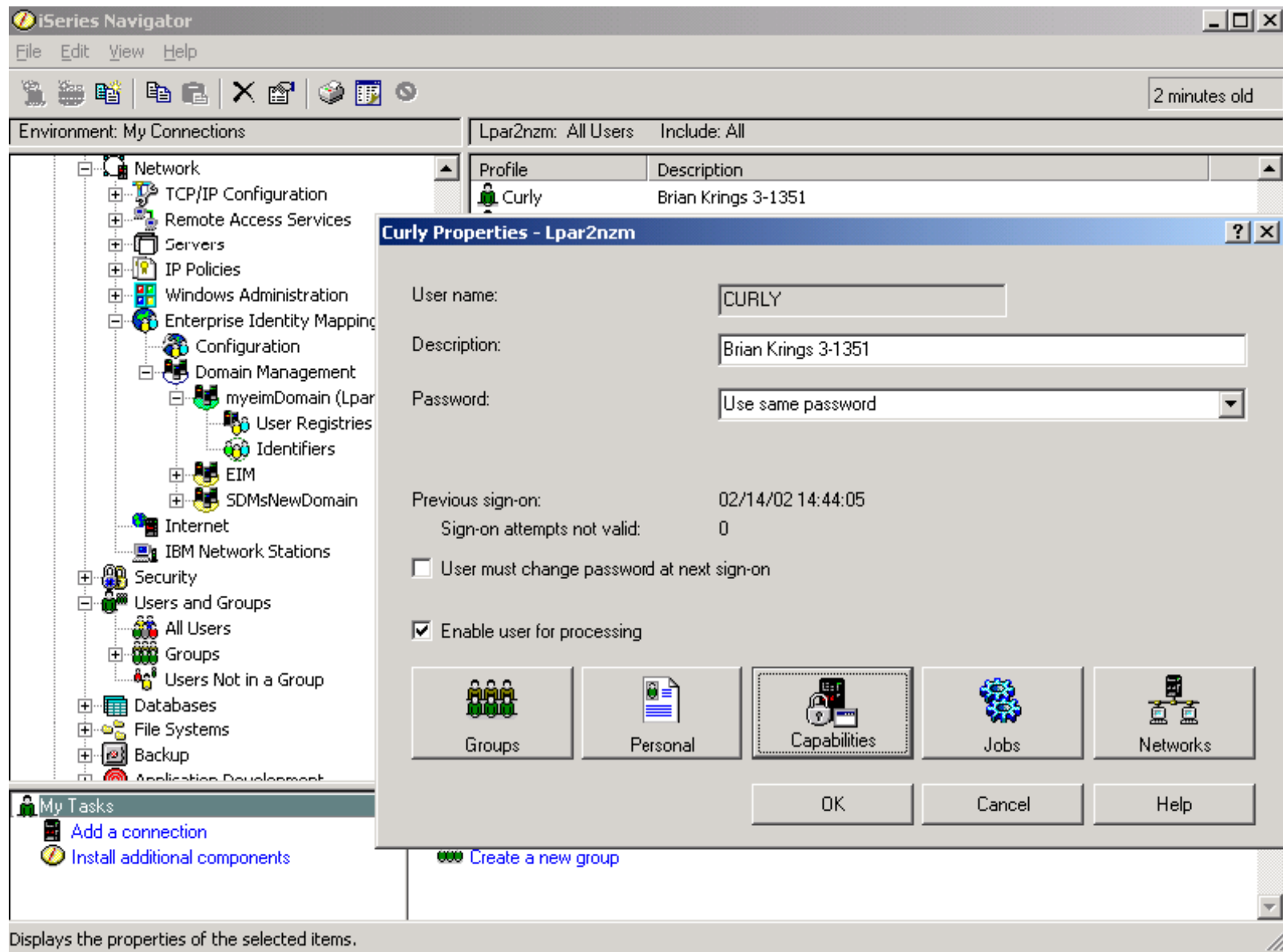
- Left Pane (Environment: My Connections):** A tree view showing the system hierarchy. The "User Registries" folder under "Enterprise Identity Mapping" is selected.
- Right Pane (Lpar2nzm: User Registries):** A table listing the configured registries.
- Bottom Pane (My Tasks):** A task pane showing "Enterprise Identity Mapping tasks" with options like "Add a new user registry" and "Create a new identifier".

Registry	Type	Description
DEPTG8R.RCHLAND.IBM.COM	Kerberos - case sensitive	Configured kerberos registry
DEPTGPZA.ENDICOTT.IBM.COM	Kerberos	Configured kerberos registry
lpar2a8m	OS/400	Local registry
LPAR2NZM.RCHLAND.IBM.COM	OS/400	
PATSPC.RCHLAND.IBM.COM	Kerberos - case sensitive	kerberos realm on Pat Flemings PC
rchasa2d	OS/400	Configured local registry
RCHASA2D.RCHLAND.IBM.COM	OS/400	DRDA Registry
rchasant	OS/400	Configured local registry
rchasa3d	OS/400	Configured local registry
rchascow	OS/400	test
rchasm1	OS/400	Configured local registry
rchasma1	OS/400	
rchasrc2	OS/400	Configured local registry
RCHASRC2.RCHLAND.IBM.COM	OS/400	Created by wizard.
rchasrjs	OS/400	Configured local registry
rs048	OS/400	Configured local registry

IBM  server. For the next generation of e-business.

# Associating User Profile/EIM Identifier

IBM  server iSeries



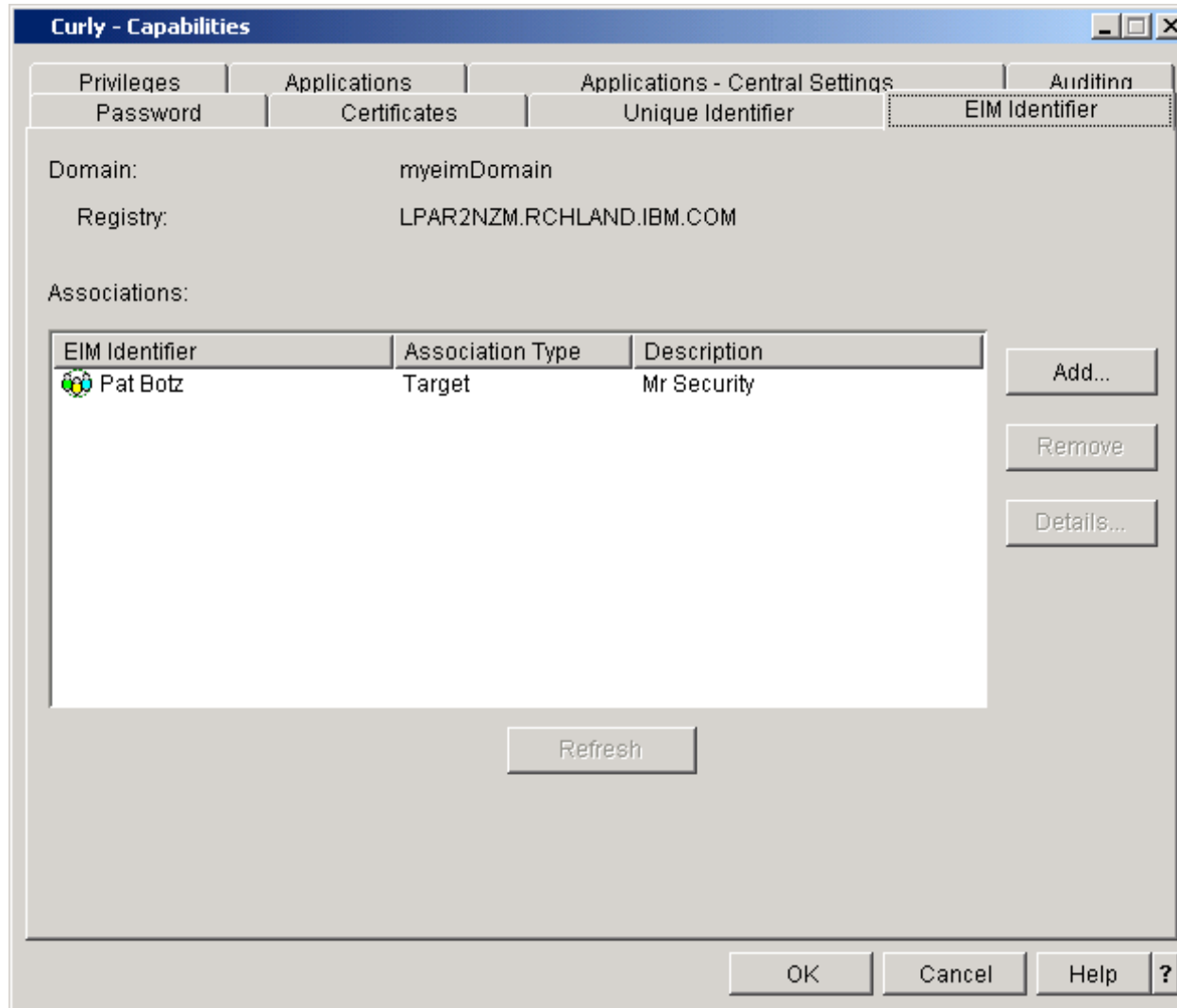
The screenshot shows the iSeries Navigator interface with a tree view on the left and a 'Curly Properties - Lpar2nzm' dialog box open. The tree view includes categories like Network, Security, and Users and Groups. The dialog box contains the following information:

Field	Value
User name:	CURLY
Description:	Brian Krings 3-1351
Password:	Use same password
Previous sign-on:	02/14/02 14:44:05
Sign-on attempts not valid:	0
User must change password at next sign-on:	<input type="checkbox"/>
Enable user for processing:	<input checked="" type="checkbox"/>

At the bottom of the dialog, there are five icons representing different user profiles: Groups, Personal, Capabilities, Jobs, and Networks. Below these icons are buttons for OK, Cancel, and Help.

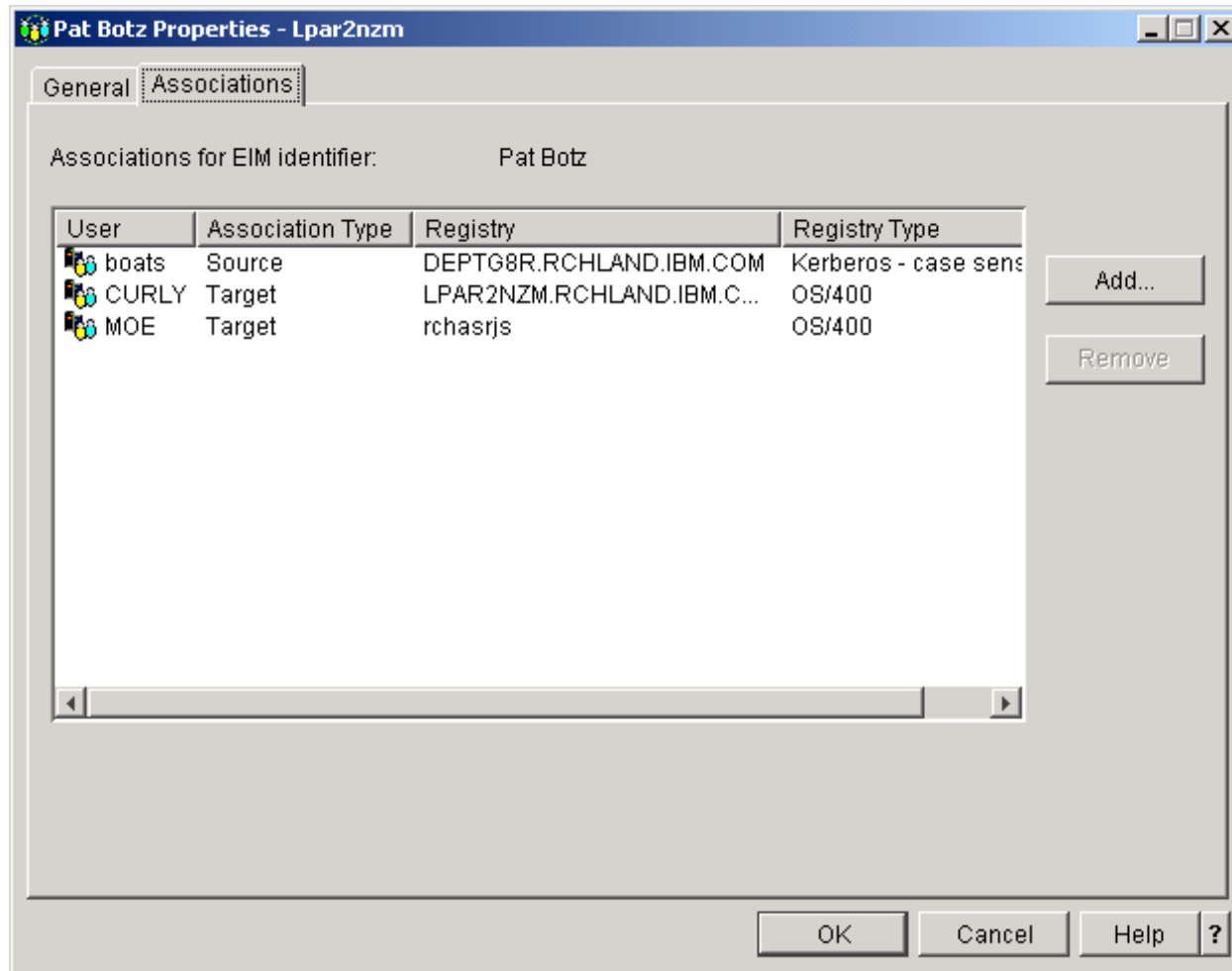
IBM  server. For the next generation of e-business.

# Associating User Profile/EIM Identifier



IBM  server. For the next generation of e-business.

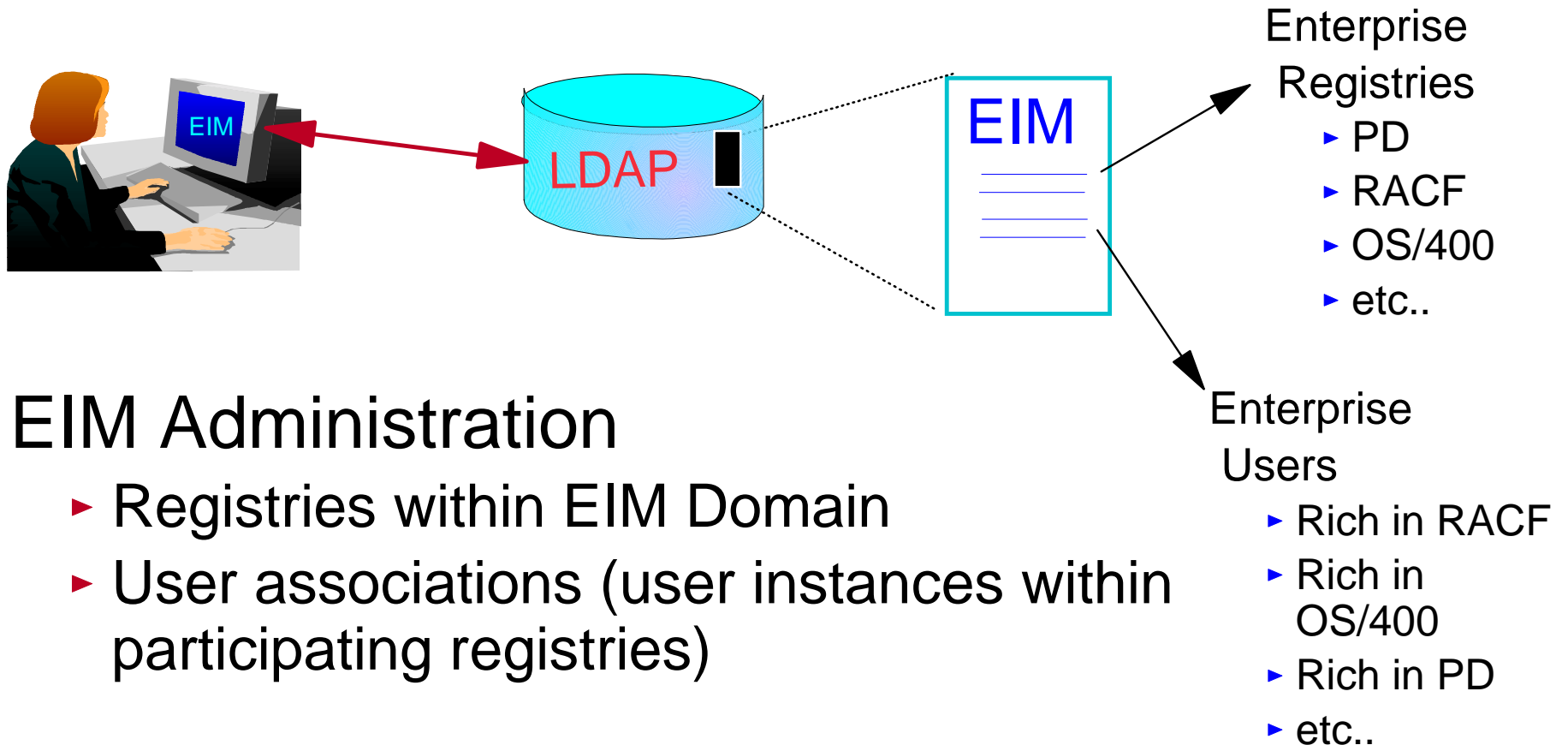
# Associating User Profile/EIM Identifier



IBM  server. For the next generation of e-business.

# EIM Administration (registries and users)

IBM @server iSeries



## EIM Administration

- ▶ Registries within EIM Domain
- ▶ User associations (user instances within participating registries)

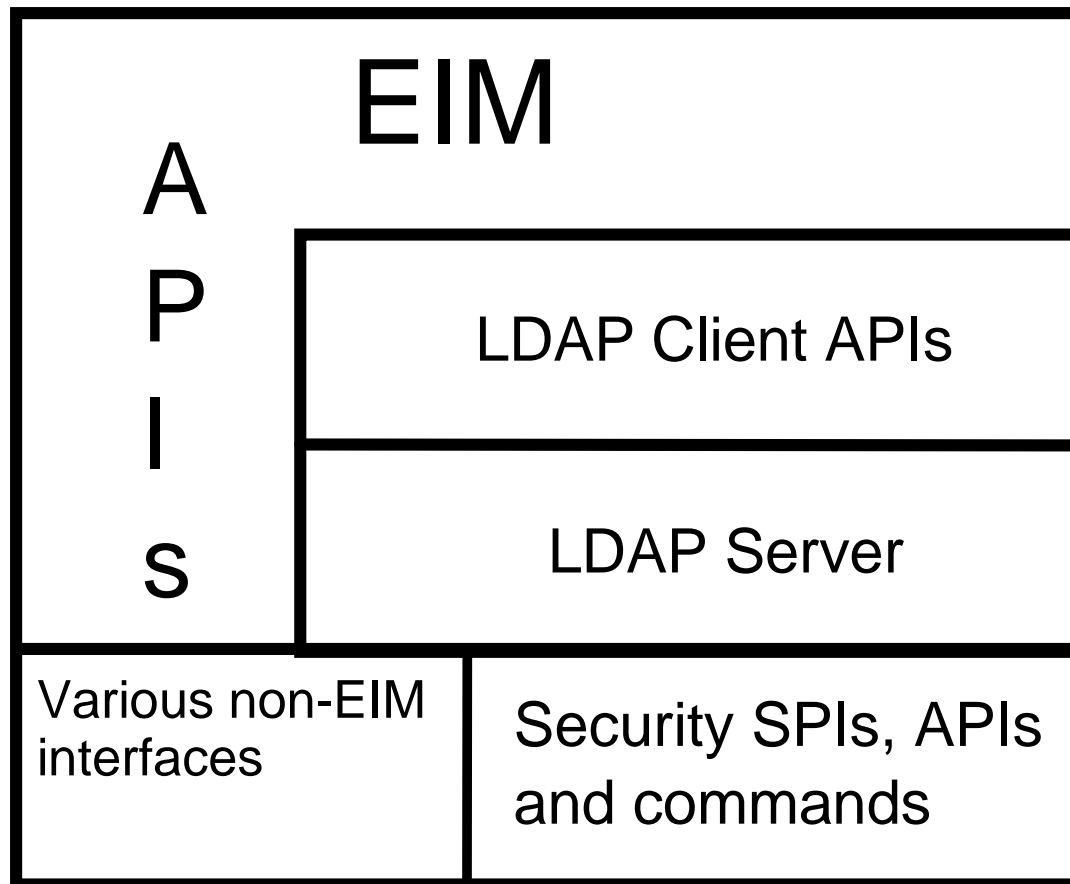
**No duplication** of registry operational information

IBM @server. For the next generation of e-business.

# EIM Architecture

IBM @server. For the next generation of e-business.





IBM @server. For the next generation of e-business.

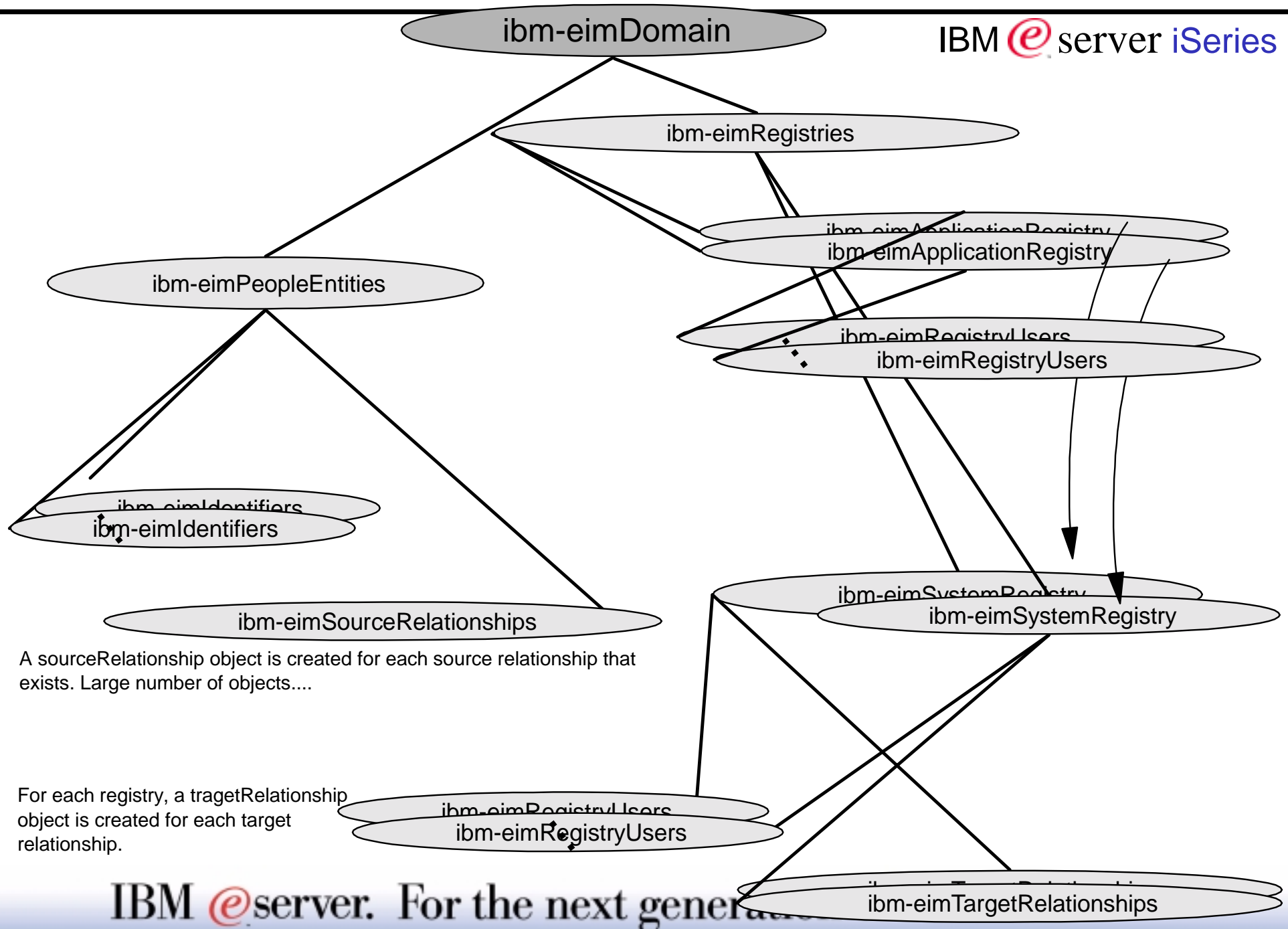
- **EIM "handle" operations - common**
  - Manages a token which is an instance of the EIM services. Similar in concept to other services in which the invoker is responsible for hanging-on to a "handle"
- **Domain operations - EIM Admin**
  - Creates a EIM domain, establishes the EIM "domain" controller...
- **Registry operations - EIM Admin**
  - System or application registries join EIM instance
- **EIM Identifier operations - EIM Admin**
  - Manages a "anchor" point for a enterprise user
- **EIM Core Mapping operations - run-time**
  - Supports determination of user's ID across disparate registries
- **System operations - System/EIM Admin**
  - Connection to an EIM domain
- **User Management operations - Admin**
  - Definition of this set of services is in progress
  - Direction is to define XML markup(s) which describe:
    - Users within registries and defines data passed on API
  - Allows add/modify/delete of users across multiple registries

Coded by application or registry security function that requires EIM services

EIM services implemented over LDAP, no new protocol

IBM  server. For the next generation of e-business.

# LDAP Directory Information Tree



# EIM Exploitation Programming Model

eimGetHandle()

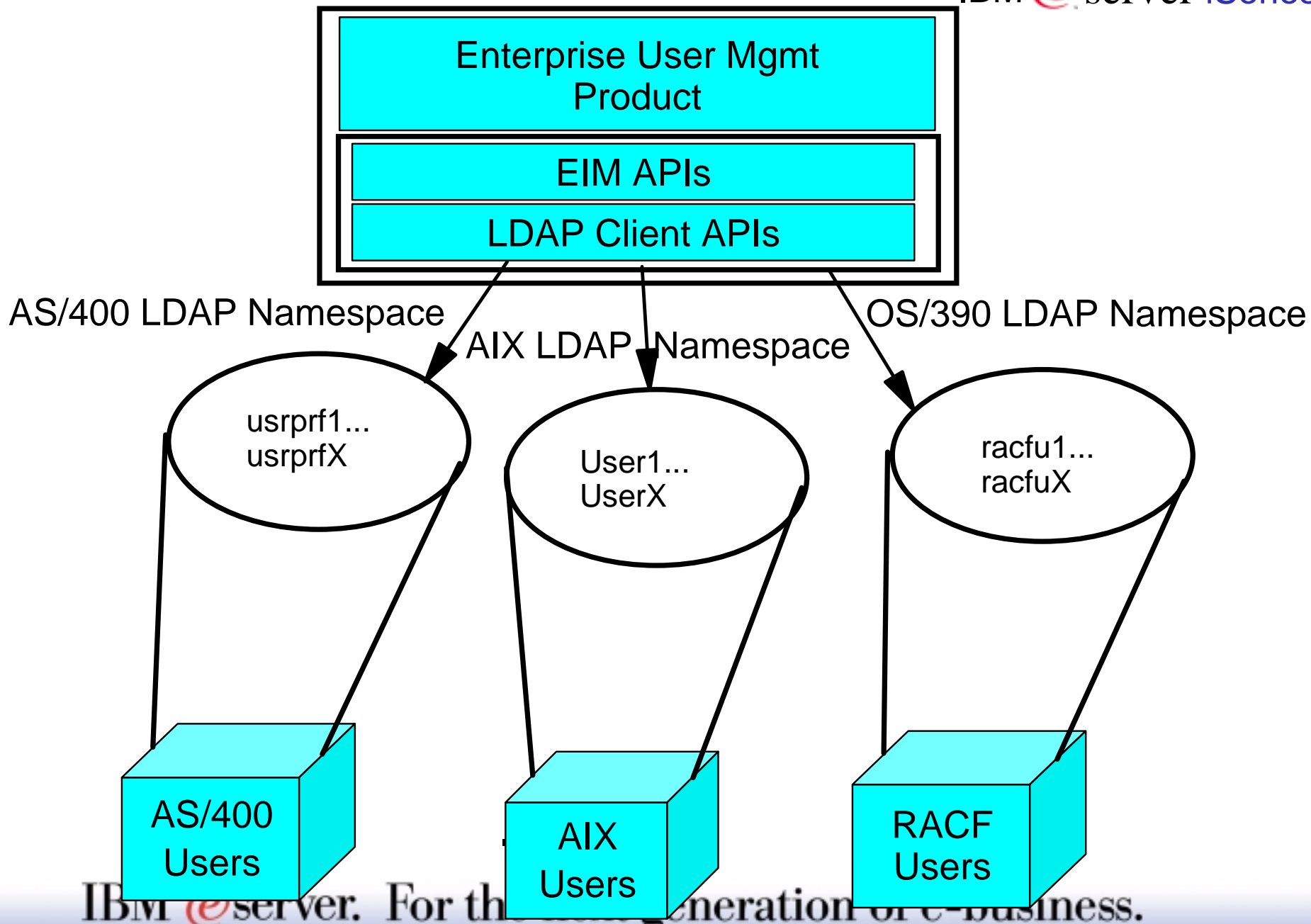
eimConnect()


- authenticate caller (U1) in registry A (REGA)
- ...
- eimGetTargetFromSource(U1, REGA, REGB, associated\_identity)
- setuid(associated\_identity)
- perform task as local identity
- get next request

eimDestroyHandle()

# Local User Projection

IBM  server iSeries



IBM  server. For the next generation of e-business.

# EIM and ISVs

IBM @server. For the next generation of e-business.

ISVs invest large amounts in building and maintaining for their applications

- application specific user registries
- associated security semantics
- pair-wise application specific identity mapping

This increases the cost of the application and cost of administering the IT environments that deploy these applications

IBM  server. For the next generation of e-business.

# ISV Exploitation of EIM (*continued*)

Today, distributed, multi-tier applications must agree to use the same authentication AND authorization mechanisms regardless of where the application executes

- this usually requires the deployment of a distributed security semantic
- which is layered on top of existing native semantics associated with the data storage mechanism
  - this creates an environment where it is easy to make a mistake that effects the security of the data in one or both of the native or distributed environments

IBM  server. For the next generation of e-business.



# EIM Reduces Development Costs

IBM  server iSeries

## EIM Significantly Reduces ISV Development Costs for Multi-tier, Heterogeneous Apps

- No need to implement new user registries
- No need to define or enforce additional security semantics
- Provides maximum flexibility for distributed, multi-tier application developers

IBM  server. For the next generation of e-business.

# EIM Reduces Administrative Costs

IBM  server iSeries

## EIM Significantly Reduces Administrative Costs -- Makes Security Easier to Administer

- Admins don't have to administer new user registries
- Rely on existing security semantics already in place for existing data
- Provides information about a person or entity and all of their associated identities

IBM  server. For the next generation of e-business.

# ISV Product Opportunities

IBM  server iSeries

Products for managing EIM from enterprise view

Products for automating "create association" and "define user registry" processes

System and user management tools that exploit the identity relationship information in EIM (e.g. delete all of a user's associated identities)

Cheaper to build multi-tier, heterogeneous applications

IBM  server. For the next generation of e-business.

IBM will make EIM widely available on eServer and non-IBM platforms by:

- Shipping EIM infrastructure on ALL IBM ^ platforms (including xSeries and Linux) within less than six months of each other (planned)
- Providing Linux opensource of EIM APIs (planned)
- Providing Java jar file on alphaworks (planned)

Licensed in a way to allow ISVs to freely bundle EIM APIs with their products!

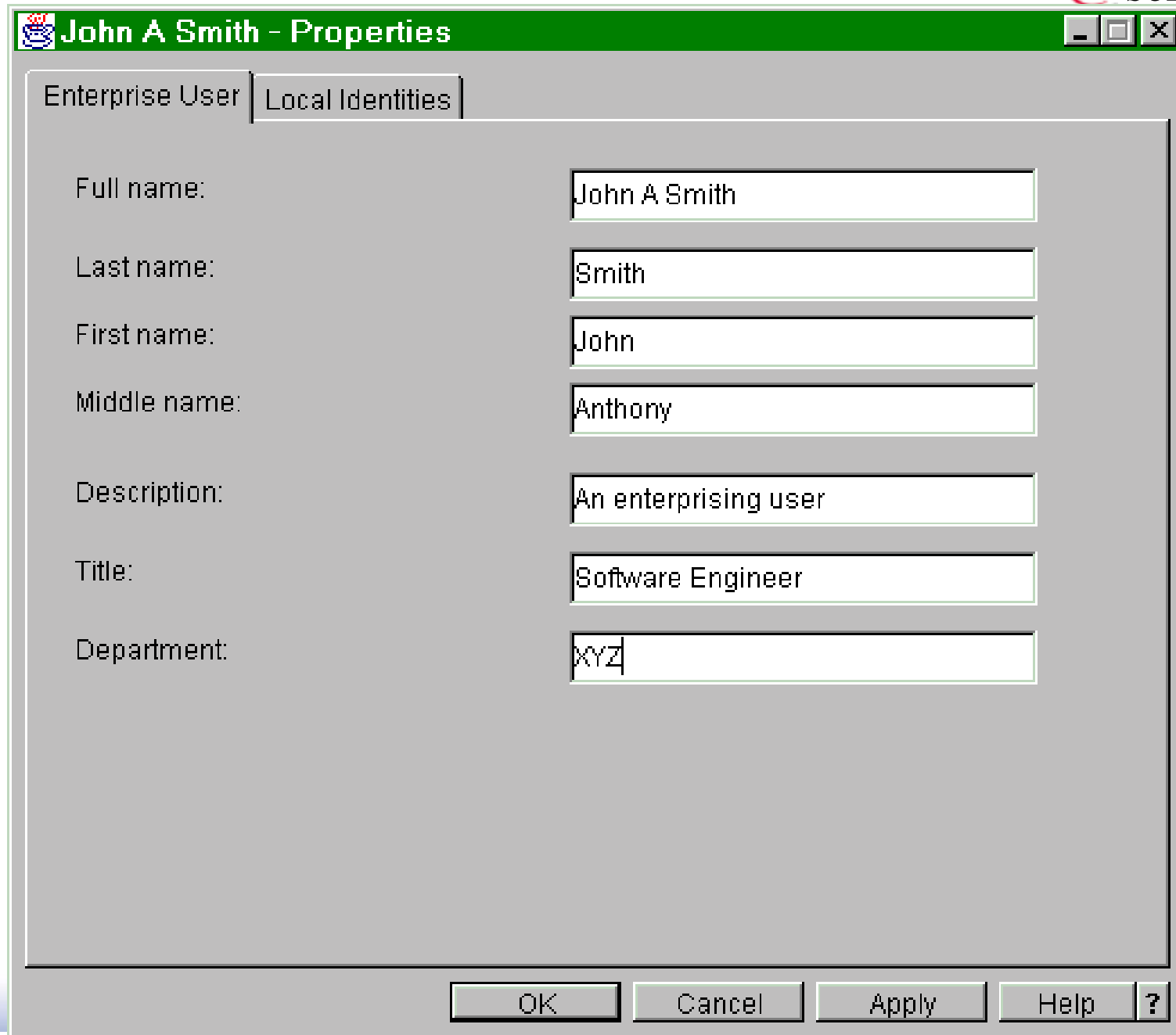
IBM is also considering industry standards body for EIM

IBM  server. For the next generation of e-business.

# Ways to Exploit EIM

IBM @server. For the next generation of e-business.

# GUI Tool View (an example)



**John A Smith - Properties**

Enterprise User | Local Identities

Full name: John A Smith

Last name: Smith

First name: John

Middle name: Anthony

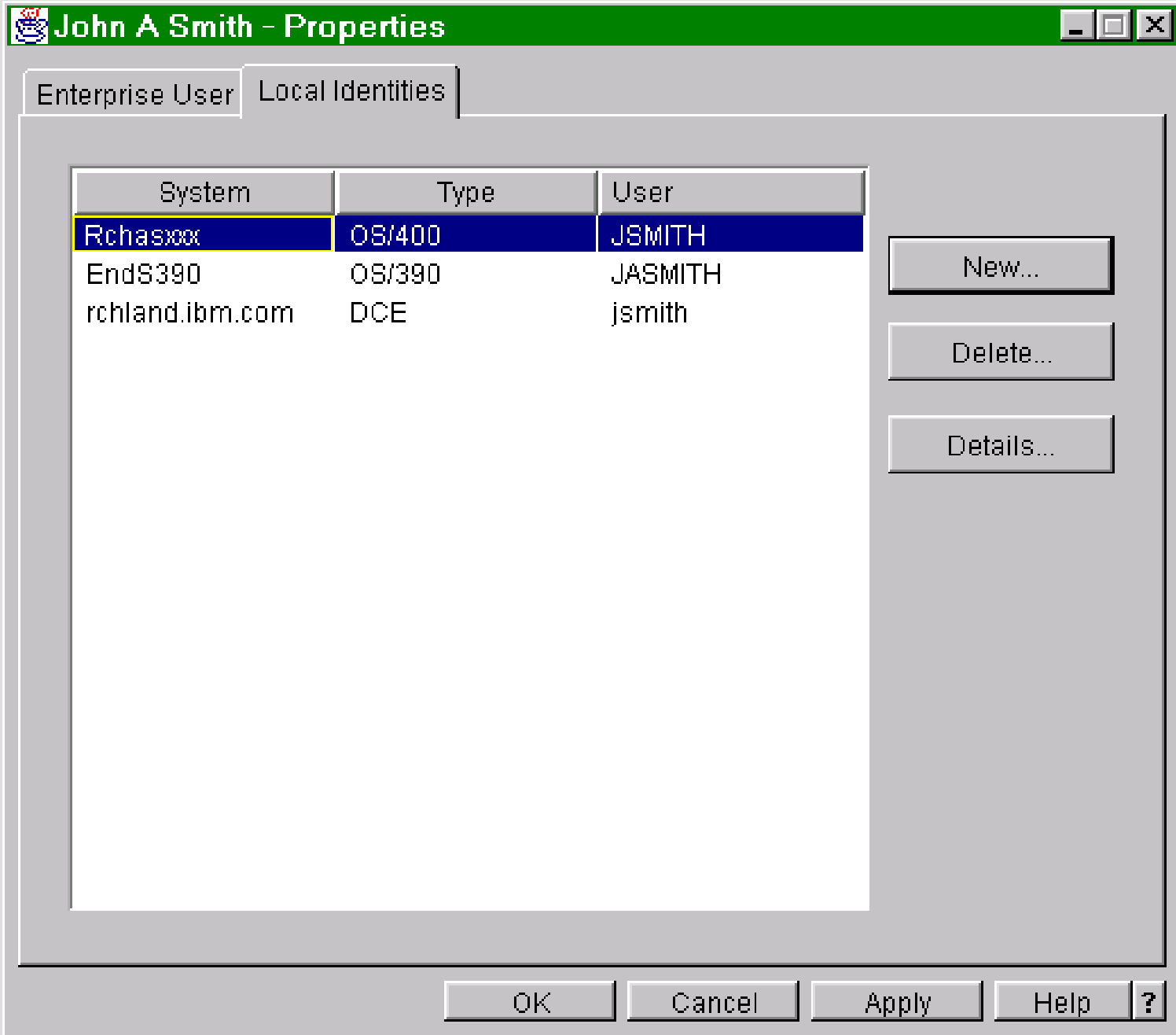
Description: An enterprising user

Title: Software Engineer

Department: XYZ

OK Cancel Apply Help ?

# GUI example (cont)



The screenshot shows a dialog box titled "John A Smith - Properties" with a green title bar. It has two tabs: "Enterprise User" and "Local Identities". The "Local Identities" tab is active, displaying a table with three columns: "System", "Type", and "User". The first row is selected, showing "Rchasmxx" for System, "OS/400" for Type, and "JSMITH" for User. To the right of the table are three buttons: "New...", "Delete...", and "Details...". At the bottom of the dialog are four buttons: "OK", "Cancel", "Apply", and "Help".

System	Type	User
Rchasmxx	OS/400	JSMITH
EndS390	OS/390	JASMITH
rchland.ibm.com	DCE	jsmith

# EIM is NOT Tivoli User Administration (TUA)

IBM @server iSeries

	EIM	TUA
Enable multi-tier heterogeneous apps	YES	NO
Enable enterprise user mgmt products	YES	NO
Single point of user mgmt product	NO	YES
Enable ESG cross-platform interoperability at OS level	YES	NO

**EIM IS an Enabler for TUA**

IBM @server. For the next generation of e-business.



# True multi-tier, heterogeneous computing at the OS

IBM @server iSeries

- ★ Users don't have multiple passwords to manage, but retain identity and authority on individual systems
- ★ Security Administrators can rely on security already in place for existing data on each system -- application level security not needed
- ★ Significantly easier for developers to build secure eBusiness applications using Enterprise Identity Mapping

**Increased productivity and security  
for the entire enterprise**

IBM @server. For the next generation of e-business.

- EIM provides "mapping" functions so that a known identity in one registry can be used to find an associated identity in another registry
  
- Make possible:
  - ✓ Applications and transactions that span across multiple, interoperable security registry domains
  - ✓ Advanced single-signon
  
- Status:
  - ✓ EIM Infrastructure and iSeries exploitation planned to be shipped in next release

IBM @server. For the next generation of e-business.

# More Information

IBM  server iSeries

<http://www.the400resource.com/content/monthly/200111/eserver11.html>

\*eServer EXTRA focuses on iSeries application development -- to subscribe, send an e-mail to:

- [serverextra@mspcommunications.com](mailto:serverextra@mspcommunications.com)

\*eServer ADMINISTRATOR focuses on security, systems management and related topics -- to subscribe, send an e-mail to:

- [eserveradministrator@mspcommunications.com](mailto:eserveradministrator@mspcommunications.com)

Look For More Articles in Industry Press (future)

IBM  server. For the next generation of e-business.

# Trademarks and Disclaimers

© IBM Corporation 1994-2002. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

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

IBM  server iSeries

AIX	IBM(logo)
RACF	iSeries
e(logo)business	OS/400
IBM	z/OS

Domino is a trademark of Lotus Development Corporation and/or IBM Corporation.

Lotus Notes and Notes are registered trademarks of Lotus Development Corporation and/or IBM Corporation.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

Information is provided "AS IS" without warranty of any kind.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information in this presentation addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

IBM  server. For the next generation of e-business.