# Don’t Synchronize! Eliminate Passwords!

## The Business Case for Password Elimination

Steve Fier

sjfier@us.ibm.com

# Agenda

Problem Definition

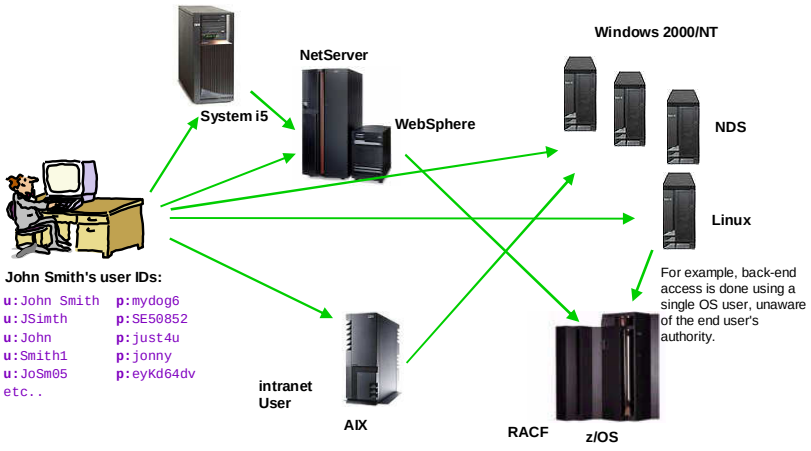
Costs of Managing Users vs. People

The i5/OS SSO Solution

Implementation Details

Benefits

# Typical Multi-Tier Heterogeneous Environment




# Multi-Tier Heterogeneous Environment

- Who is impacted by these heterogeneous multi-tier environments?
  - Users
    - productivity
  - Administrators
    - productivity
    - cost of help desk, password resets, etc...
  - Programmers
    - most cost effective way for programmers to address this environment is to add another user registry!
      - which is still very costly

# Managing Entities that Use Networks

- Do you manage “users” or “people” in your network?
- Organizations have been forced to manage users!
  - Due to the way security within OSes and applications have evolved
- Managing users in a network has multiplier effect on cost
  - users = userIDs
  - Each person has X # of userIDs
- Managing people in a network has no multiplier effect
  - A person equates to 1 userID per person
- Managing people much less expensive than managing users
  - Assuming that this could somehow be accomplished!

# Reducing the Costs of Managing a UserID

- Reducing the actual number of userIDs defined across the enterprise is not feasible today
  - Would require OSes and applications to be re-written to exploit a centralized access control mechanism
    - The cost of doing this today is prohibitive and would eliminate much of the value add of OSes (and potentially applications)
  - Today’s implementations of centralized authentication mechanisms are advisory only. They do not enforce policy, they only define it.
    - Very useful for managing access control to “virtual resources”
      - Virtual resources typically not protected by native access control mechanism
      - Typically composites of “concrete” resources that are already protected by native access control mechanisms.
  - Native access control mechanisms are already configured to protects many terabytes of data
    - Changing to a different access control mechanism would be prohibitive

## Eliminating Passwords Approaches the Cost to Manage People in the Network

- Password elimination minimizes the multipliers that drive the cost!
  - Therefore the cost of managing users when passwords are eliminated approaches the cost of managing PEOPLE in a network

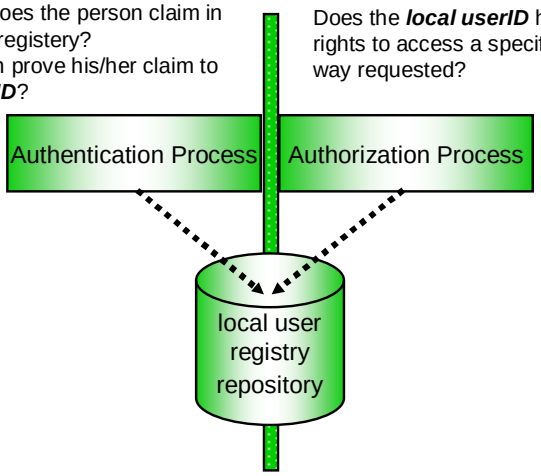
## Cost Summary

- The cost of managing userIDs in a network is the sum of the costs to manage the existence plus the changes to each userID in the network.
- The largest component of this cost is changes, not existence
- The largest component of cost of changes is the cost of changing passwords
  - Primarily due to multiplier effects of
    - The number of times it must be changed (Y)
    - The average number of userIDs per person (#UIDSPP) and the total number of userIDs (#UIDS)

# Authentication and Authorization are Related --But Different Processes

What ***userID*** does the person claim in the ***local*** user registery?
Can the person prove his/her claim to the ***local userID***?

Does the ***local userID*** have appropriate rights to access a specified resource in the way requested?

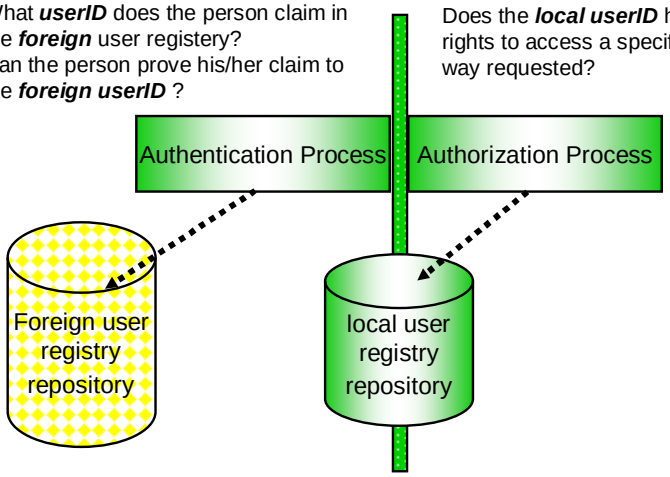



This makes the multi-tier heterogeneous problem especially difficult!

# SSO Solutions MUST address Authentication AND Authorization

What ***userID*** does the person claim in the ***foreign*** user registery?
Can the person prove his/her claim to the ***foreign userID*** ?

Does the ***local userID*** have appropriate rights to access a specified resource in the way requested?




Using different registries for AuthN and AuthZ = PROBLEM

# Comparing Traditional SSO Solutions

(a.k.a. SSO Means Different Things to Different People)

# Nirvana -- Getting there is a journey

# Common Single Sign-on Definitions

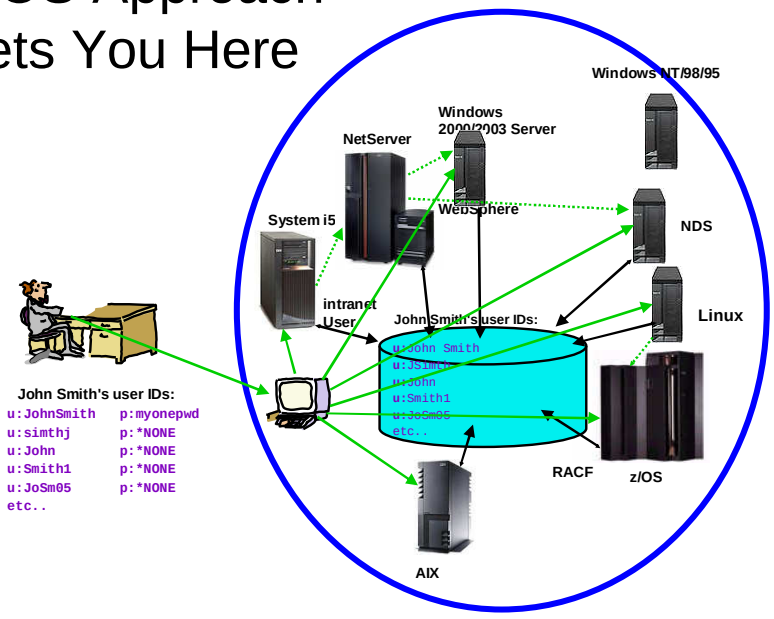
- Single Sign-on means:
  - A person has multiple IDs and passwords, but they are the same everywhere
    - User ID/password synchronization
    - User has the same ID/password everywhere
    - User still required to sign-on but always uses the same information
    - Not really SSO
    - Costly to implement and manage, prone to breakage
  - All of a person's user IDs and passwords are copied to a central location
    - Requires "front-end" applications be changed to grab the associated ID/pwd for the remote system/application
    - Costly to implement and manage, prone to breakage
    - Fragile in multi-tier environments
  - A person only has one ID and password stored in the network
    - Only one user registry exists and all systems and applications use this registry -- Users have only one ID/pwd (i.e. not synchronization)
    - e.g. "Why doesn't everyone use LDAP for authentication?"
    - Not likely because AUTHORIZATION is so closely tied to the authentication mechanism
  - A person signs-on once and never has to sign-on again regardless of which applications, systems, URLs are visited
    - Great idea but, unfortunately, not 100% achievable in the foreseeable future

# i5/OS Approach to SSO

# OS/400 V5R2 and i5/OS V5R3 Single Sign-on

- Two technologies provide a FRAMEWORK for a solution:
  - Authentication
    - Network Authentication Service (i.e. Kerberos) used for authentication
  - Authorization
    - Enterprise Identity Mapping (EIM) used to find which IDs are
- The SOLUTION is provided when the framework is exploited

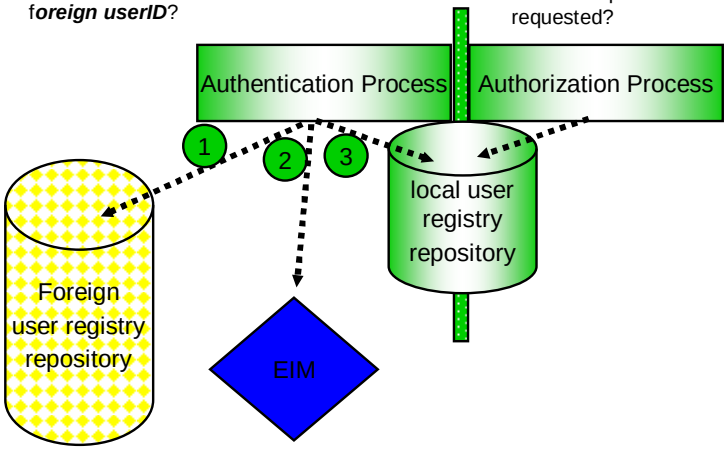
# i5/OS Approach Gets You Here



# i5/OS Approach

What ***userID*** does the person claim in a ***foreign*** user registery?
Can the person prove his/her claim to the f***oreign userID***?

Does the ***userID* on this system** have appropriate rights to
access a specified resource in the way requested?



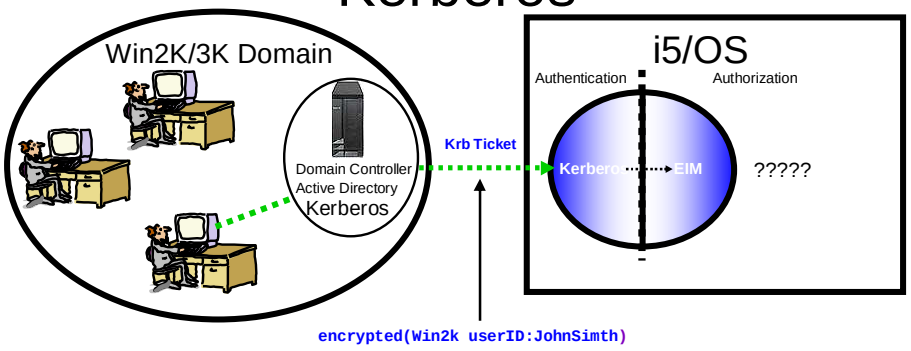

Mapping Identities from Foreign to Local = NO Problem

# Solution Components

# iSeries OS/400 V5R2 Single Sign-on Announcement Part I

- Why Kerberos?
  - Distributed 3rd party authentication mechanism
    - single repository for IDs and passwords
    - users enters password/ID once
  - Mechanism used by MS Win2K,XP and Passport
  - Designed to establish secure authentication from client to server (and vice versa) on an untrusted network
  - Can allow clients to enable cryptography to secure an established connection
    - Client dependent, iSeries Access currently does not support Kerberos encryption
  - Widespread throughout the industry, allows for interoperability between platforms
  - Simplifies trust management
  - Outlined in RCF1510
- OS/400
  - Most important OS/400 user interfaces enhanced to use Kerberos
    - Host Servers / iSeries Access for Windows / iSeries Navigator / ODBC / JDBC / DRDA / Telnet / Netserver / QFileSvr400 / Apache Web Server / Host on Demand / more clients in future

# i5/OS Single Sign-on with Kerberos




**John Smith's user IDs:**

```
u:JohSimth    p:mypassword
u:simthj      p:*NONE
```

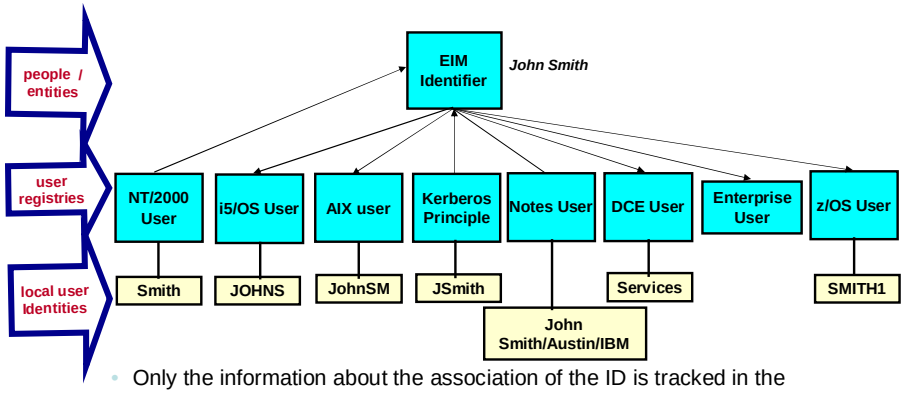
Kerberos is useful for authentication
But what about ***authorization***?

# iSeries V5R2 Single Sign-on Announcement Part II

- Enterprise Identity Mapping
- Accepts the fact that multiple registries (IBM and non-IBM) will exist in the enterprise
- Makes it easy for customers to associate a user's multiple identities in the enterprise and to manage those associations
- Focuses on eliminating the need to manage (set, change, or reset) or synchronize passwords, but not user IDs
  - Can choose to set passwords for user IDs on servers to *NONE if you wish
- Consists of
  - Native APIs shipped with all eServer supported operating systems
  - Java implementation available for download from IBM web site can run in any JVM on any IBM or non-IBM system

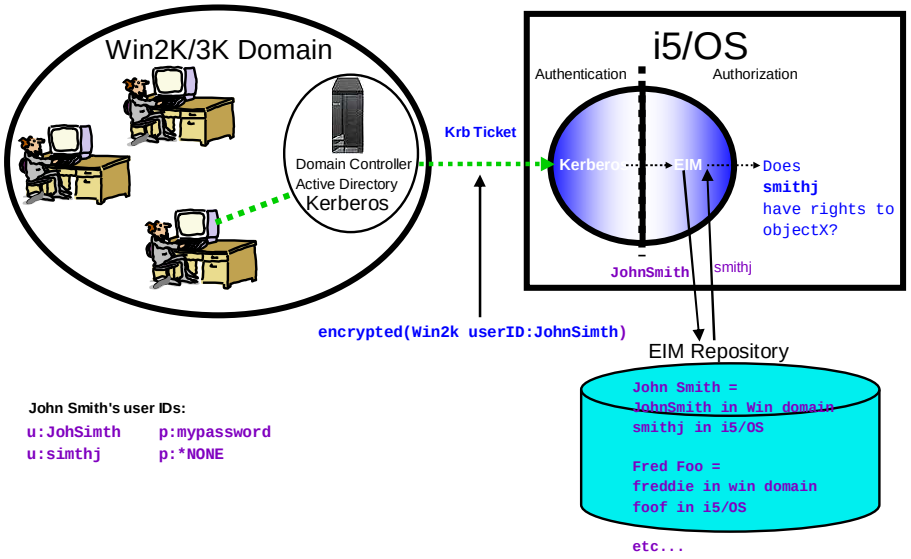
# Enterprise Identity Mapping

- EIM defined: For each person and entity in the enterprise, keep track of each of his/her/its userIDs in various user registries
- The identity associations (mappings) are stored in a well known location, i.e. LDAP, with common services across platforms to access the mappings.




- Only the information about the association of the ID is tracked in the repository; not passwords (or other attributes)

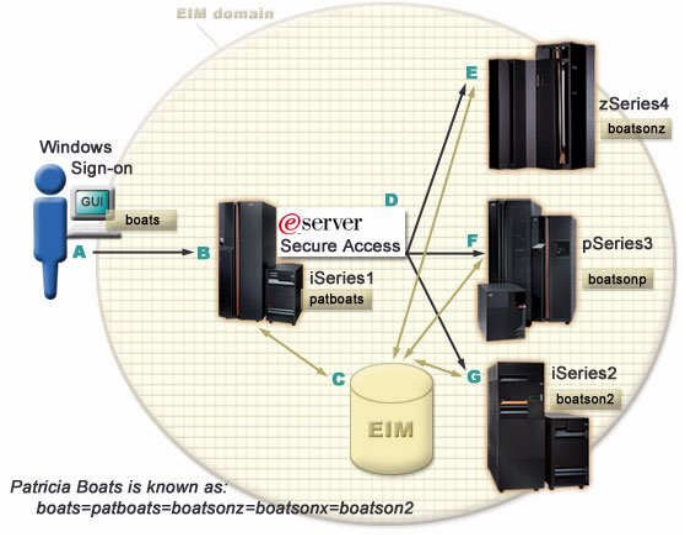
# i5/OS Single Sign-on




**John Smith's user IDs:**

`u:JohSimth` `p:mypassword`
`u:simthj` `p:*NONE`

# Multi-system Security w/ 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 (i5/OS)
   - 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 (i5/OS) 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**

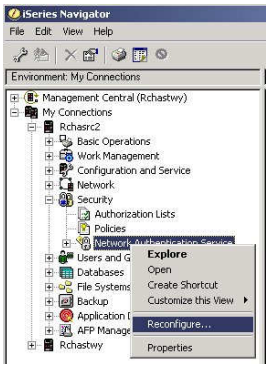
# Configuring & Administering SSO

# Requires Kerberos configuration

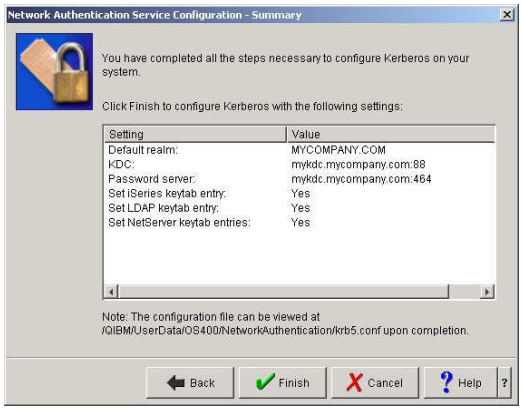
- Administrators configure i5/OS to particiate in a Kerberos "realm"
  - i5/OS is given a "user ID" (a.k.a. Kerberos service principle) to represent i5/OS in Kerberos
- Once Kerberos is configured, then configure (or write new) clients to use Kerberos to authenticate

# NAS Wizard

Launching the wizard and the welcome screen.




# NAS Wizard Summary




# Benefits

# Single Sign-on in a Single Day

- i5/OS SSO is not disruptive to implement!
  - Can implement SSO for:
    - a single user,
    - single department,
    - arbitrary group of users
    - a whole company
  - Without affecting other users
- Can easily have 1st user working in less than an hour
  - iSeries Navigator provides wizards
  - Assuming you already have a Windows 2000/2003 domain or some other Kerberos server (e.g. on Linux, AIX, etc) already configured in your network
- ROI starts with first user!
  - Available with base OS
    - Initial cost is essentially $0
  - ROI is incremental
    - Not dependent on enabling X-number of users before ROI kicks in.

# Many Interfaces Provided by i5/OS are Enabled

- V5R2 GA
  - iSeries Access/Navigator, Host Servers
  - PC5250 client, Telnet Server
  - Windows ODBC driver delivered with iSeries Access, ODBC/JDBC/DRDA servers
  - Netserver
  - QFileSrv400
- Available for V5R2 via PTFs, next release base GA, or LPP release
  - Apache Web Server (PTFs for V5R2)
  - IXS/IXA exploitation (next release)
    - New user profile attribute Local Password Management *YES/*NO
  - iNotes Access for Web (Description of solution)
  - Manage EIM associations through green screen user profile commands (next release)
  - Host on Demand (available now)
  - Others to be announced with next release

# EIM Management Issues

- Questions:
  - How do you set up all of the identity associations in EIM!!!!
  - How do you manage large numbers of identity associations over???
- Answer:
  - IBM provides a mostly manual method via iSeries Navigator
    - Great for configuring initial SSO set up and working
    - Decent for associating i5/OS user profiles
    - Not as easy for non-i5/OS user IDs and ongoing management
    - IBM Telephone Directory (ITD) (May '04 timeframe)
      - Secure self-management of EIM associations
  - Looking for Tivoli and ISVs to provide robust cross-platform life-cycle management solutions
    - Tivoli TIM-to-EIM bridge solution
    - Interim fix for 4.5.1-TIM-0010, APAR IY54871
    - http://www-1.ibm.com/support/docview.wss?rs=644&context=SSTFWV&uid=swg24006580&loc=en_US&cs=utf-8&lang=en

# EIM Management Issues

- ISV EIM Management products
  - Powertech:
    - Triaworks Identity Manager for SSO (TIM SSO)
      - Availabe today
    - http://www.triaworks.com
  - Typex
    - BlueNotes EIM Administrator
      - Available today
    - http://www.bluenotes.com
    - http://www.kimgreene.com
  - Safestone
    - AxcessIT
      - Available soon
      - DetectIT product available now
    - http://www.safestone.com

# Measuring the effectiveness of an SSO solution

$PGUAP > ($CAS + $CIS + $CMS)

PGUAP = Productivity gains for users, administrators, and programmers
CAS = Cost to aquire solution
CIS = Cost to implement solution
CMS = Cost to manage solution

PGUAP = ????? Only You Can Measure This ?????
CAS = $0
CIS = ~$100 (Estimate! of 1 hour admin time for first user)
CMS = Depends on management tools used and number of users and
number of user ID's per person

# True multi-tier, heterogeneous computing at the OS

- **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 users, administrators, and programmers**

*A 14 year track record…proven methods & techniques, worldwide results*

# STG Lab Services

To learn more about how STG Lab Services can help you attain your sales objectives, see us in the Solutions Center or contact a Lab Services Opportunity Manager:

| | |
|---|---|
| System i (WW, AG) | Mark Even, (507) 253-1313, even@us.ibm.com |
| | Pete Cornell, (507) 253-4955, pcornell@us.ibm.com |
| System p (WW, AG) | Stephen Brandenburg, (301) 803-6199, sbranden@us.ibm.com |
| | Greg Mallare, (727) 593-2228, gmallare@us.ibm.com |
| System x (WW, AG) | Michael Karchov, (919) 342-6619, michael.karchov@us.ibm.com |
| | Mike Sigl, (425) 803-5901, siglm@us.ibm.com |
| System z (WW, AG) | Jerry Koger (623) 505-4932, jerrykog@us.ibm.com |

| | |
|---|---|
| System Storage (WW, AG) | Kevin Bogart, (919) 543-7919, kbogart@us.ibm.com |
| Optimization Studies (WW, AG) | Marlin Maddy, (877) 598-9675, mmaddy@us.ibm.com |
| Solutions (WW, AG) | Mohsen Nikbakhshian, (301) 803-2947, mnikbakh@us.ibm.com |
| AP System i, z | Jenny Chen, 886-2-8170-6895, jenychen@tw.ibm.com |
| System p, x Storage | Zhe Xu, 86-10-62986677x306, xuzhe@cn.ibm.com |
| US contact for AP | Jin-Ming Liu, (507) 253-0391, jliu@us.ibm.com |
| Europe SWE & NEE IOT's | Benoit Sirot. 33-4 9211.5012, sirot@fr.ibm.com |
| | Gerard Barneaud. 33-4 9211.4231, barneaud@fr.ibm.com |

**www.ibm.com/eserver/services**





# More Information

Redbook Windows-based Single Signon and the EIM Framework on the iSeries (SG24-6975-00)

http://publib.boulder.ibm.com/eserver, select Enterprise Identity Mapping from the left-hand navigator pane: information about EIM on all IBM platforms, Windows, Linux, and Java

http://eservercomputing.com/iseries, previous issues, November 2001 "Easing the Multiple User Registry Burden"

V5R2 Information Center, Security topic

*eServer EXTRA focuses on iSeries application development -- to subscribe, send an e-mail to: eserverextra@mspcommunications.com

Experts Guide to OS/400 & i5/OS Security
Carol Woodbury and Patrick Botz
ISBN 1-58304-096-X
29th Street Press, 2003

http://www.pentontech.com/education (available early May '04)

http://www.bluenotes.com "EIM Administrator"

http://www.triaworks.com "Triaworks Identity Manager for Single Sign-On" (TIMSSO)

http://www.safestone.com "AxcessIT"

IBM Telephone Directory (ITD) for EIM end-user self-registration.

Look For More Articles in Industry Press (future)

# Trademarks and Disclaimers