iSeries Nation WebCast 9/16/04

iSeries. mySeries.

What's New in i5/OS Security

eServer Security

Patrick Botz

Assumptions and Agenda

- **This is a fire hose presentation! Get Ready ☺**
  - Session is an overview of the new security enhancements in IBM i5/OS
  - Not intended to be in depth discussion of each change
  - Lots of Notes pages with more information!

- Common Criteria Evaluation
- System Value Changes
- Dynamic Virus Scanning Enablement
- New SSO Enablement
- New Network Authentication Service Function and Enhancements
- New EIM Function
- System Integrity Enhancements
- Miscellaneous Enhancements

Common Criteria Evaluation

Common Criteria evaluation for i5/OS

- Common Criteria security evaluation of i5/OS in progress

  CAPP protection profile -- Controlled Access Protection Profile
  Protection profile describes what is being evaluated
  CAPP defined with input from US Dept. Defense
  Intended to be equivalent with the old C2

  – EAL4 – Evaluated Assurance Level
  The level of "proof" that your design and/or implementation meets the specifications defined in the Protection Profile
  1=claims, 2=some documentation, 3=high level documentation, 4=low level documentation

- Changes made in i5/OS to meet criteria
  – Must have *ALLOBJ OR *AUDIT to view audit related security values
  – Changes coming to audit failure to have special authority
    - New sbutype for AF audit records
    - Won't be fully implemented until release after i5/OS V5R3

NOTE: This work is in progress. No guarantee that this work will be completed for i5/OS

System Values

QCRTAUT Behavior Change

Change System Value

System value . . . . . : QCRTAUT
Description . . . . : Create default public authority

Type choice, press Enter.

Create default public
authority . . . . . *CHANGE
*ALL
*USE
*EXCLUDE

- Prior to i5/OS
  - Changing QCRTAUT to something other than *CHANGE required changes to device controllers in QSYS
    - AUT must be *CHANGE
- i5/OS
  - Changing QCRTAUT to *USE or *EXCLUDE does not require any other changes for the operating system itself to work properly
- Caution
  - May still require changing CRTAUT or AUT on application libraries or objects in order for the applications to work correctly.

New audit support - QAUDLVL2

- New system value QAUDLVL2
  - Support to minimize the amount of audit data
  - Subset support for the *SECURITY and *NETCMN values
    - *SECCFG (security configuration audit)
    - *SECRUN (Run time security changes)
    - *SECxxx (other values)
    - *NETBAS (Basic network audit records)
    - *NETFAIL (Network failure records)
    - *NETxxx (other values)
  - Provides room for future auditing categories

New System Value – QAUDLVL2

Work with System Values

System: XXXXXXX

Position to . . . . . Starting characters of system value
Subset by Type . . . . . F4 for list

Type options, press Enter.
2=Change 5=Display

Option	System Value	Type	Description
	QAUDLVL	*SEC	Security auditing level
	QAUDLVL2	*SEC	Security auditing level extension

Dynamic Virus Scanning Enablement

Dynamic Virus Scanning Enablement

- New System Values
  - QSCANFS
  - QSCANFSCTL
- New Exit Points
  - QIBM_QP0L_SCAN_CLOSE
  - QIBM_QP0L_SCAN_OPEN
- New Stream File Attributes
  - *CRTOBJSCAN = *YES, *NO, *CHGONLY
  - *SCAN = *YES, *NO, *CHGONLY
- CHKOBJITG
  - New SCANFS parameter

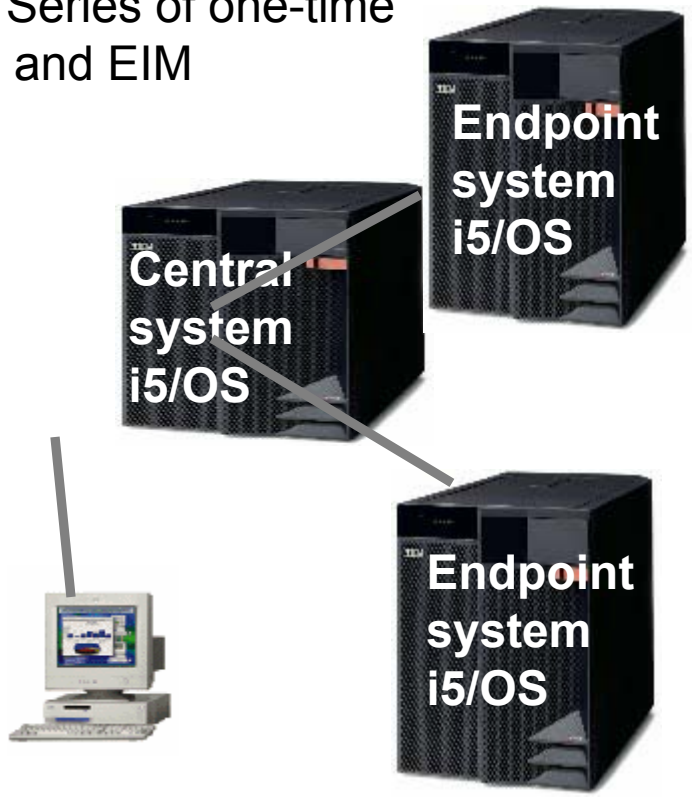
New SSO Enablement

New SSO Enablement

- Management central
- IXS/IXA Integrated Windows SSO
- Apache Web Server
  - Available in i5/OS base and V5R2 PTFs
- IBM Telephone Directory application provides end-user “self EIM registration” support.
- Integrated OS/400, i5/OS and WAS/Portal Server Application SSO
- Host-on-Demand release 8.0

Single Sign-On with Management Central

- Management Central now supports Kerberos and EIM for authentication between central and endpoint systems
- Managing users need source and target associations on central and each endpoint system they are supposed to manage Series of one-time steps need to be performed to enable Kerberos and EIM for the Management Central environment
- EIM is optional when using Kerberos authentication with Management Central



iSeries. mySeries.

Windows Integration and Single Sign-On

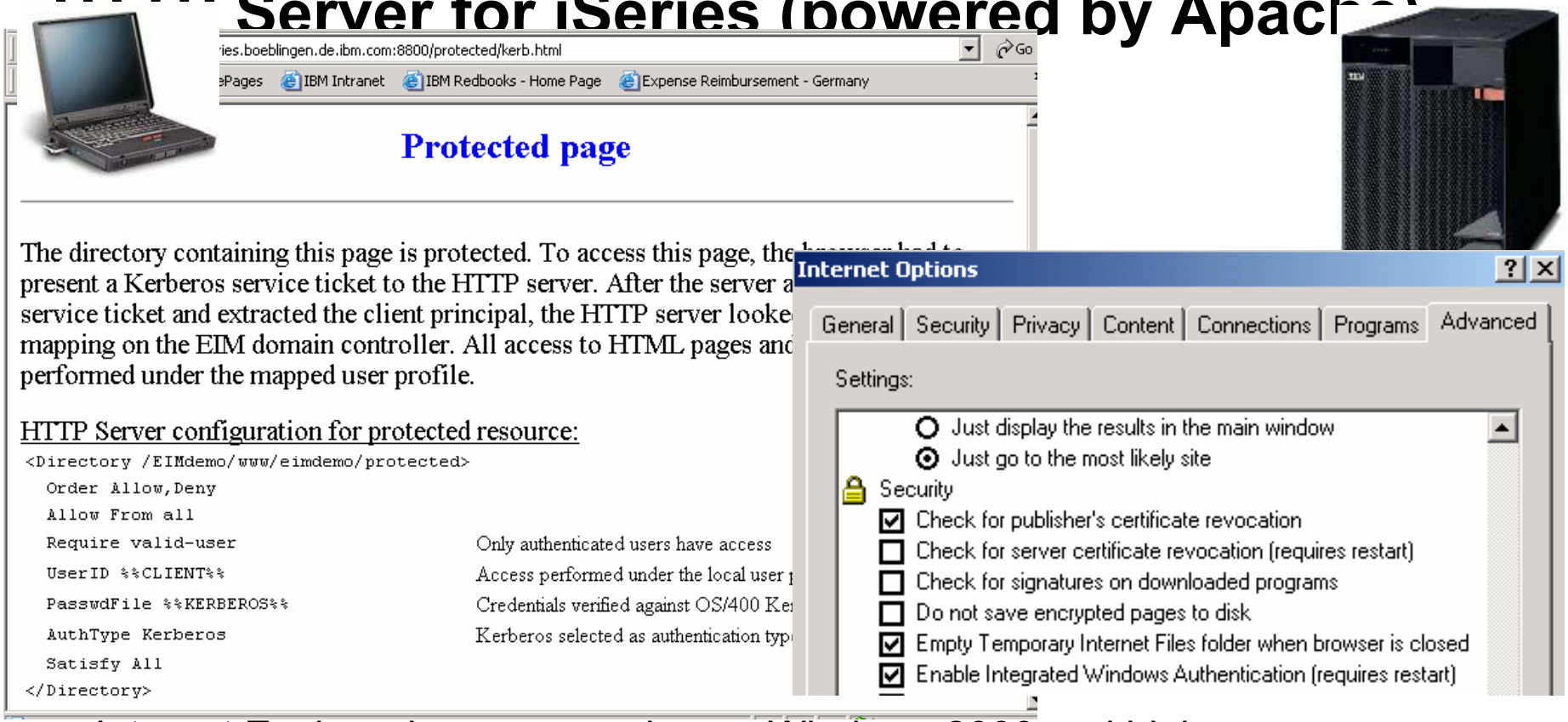
User enrollment

- User enrollment now supports EIM
- Enrollment for EIM associations can be:
  - Automatic:
    - Requires EIMASSOC parameter in user profile
    - Target and source association have the same name
  - Manual:
    - Administrator creates target and source associations manually
    - Association names can be different.

SBMNWSCMD and file level backup

- Kerberos authentication with EIM mapping only works with user profile LCLPWDMGT set to *NO
  - If set to *YES, attempt is made to authenticate with a Windows name that is equal to OS/400 name
- OS/400 and Windows server must be in the same domain

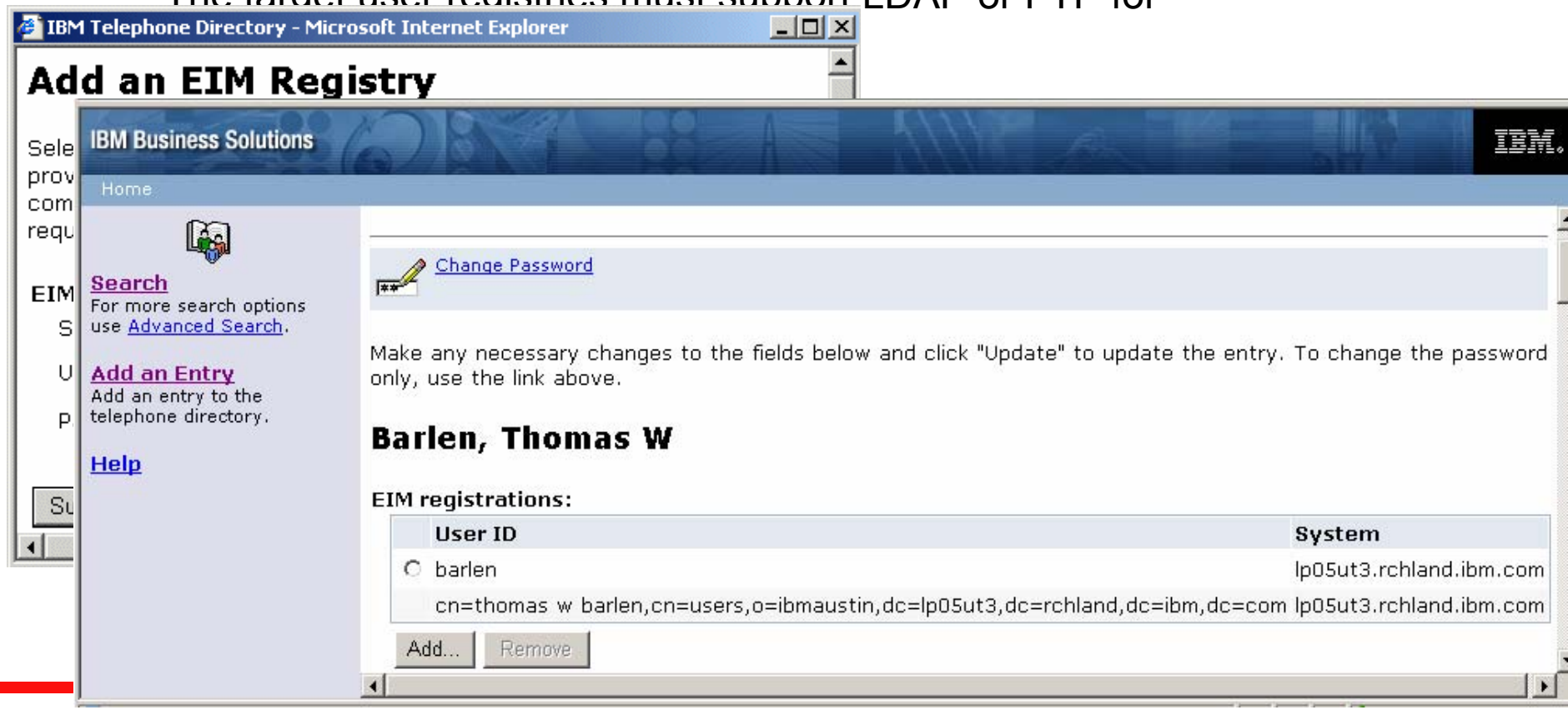
HTTP Server for iSeries (powered by Apache)



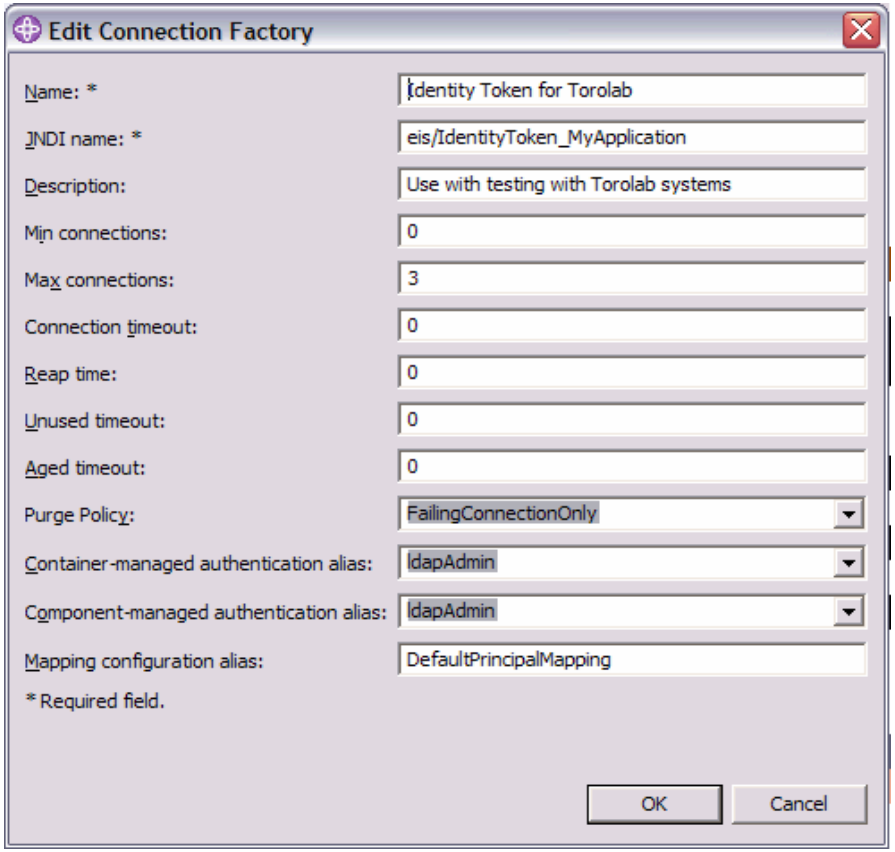
- Internet Explorer browser running on Windows 2000 and higher can authenticate Via Kerberos to protected resources on an Apache server
  - Example shows iSeries HTTP Server powered by Apache
- Requires specific options to be turned on in Internet Explorer

EIM association management – IBM Telephone Directory

- Adding associations to the EIM domain requires:
  - That the individual user knows the user and password of the association to be added
  - The target user registries must support LDAP or FTP for



Integrated SSO for OS/400, i5/OS and WAS/Portal Server Applications



SSO for WebSphere and Portal Server Applications!

Identity Token-based -- Not Kerberos!

Available in i5/OS and V5R2 via PTFs and downloads from Web (June/July '04 timeframe)

Only used through JTOpen toolbox connection -- currently

Network Authentication Service (Kerberos) Enhancements

Network Authentication Service - Kerberos

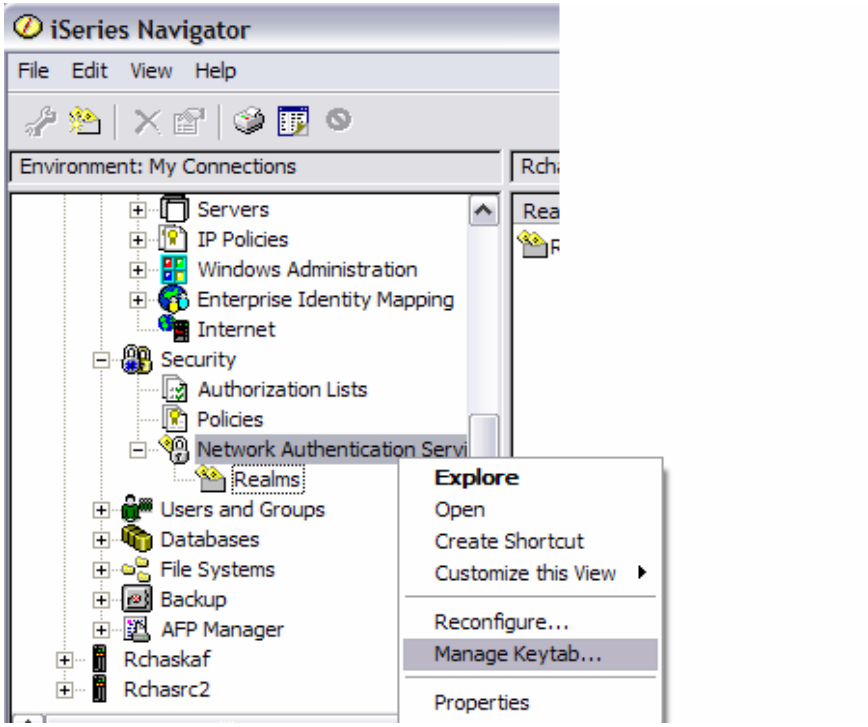
- New Kerberos Server (KDC) support on iSeries in PASE
- New Network Authentication Service function
  - Kerberos Wizard lite from EIM
  - Keytab entry display from the NAS configuration properties in Operations Navigator
  - NAS Wizard keytab batch file support
    - Allows config of Kerberos server

OS/400 Key Distribution Center (KDC) support

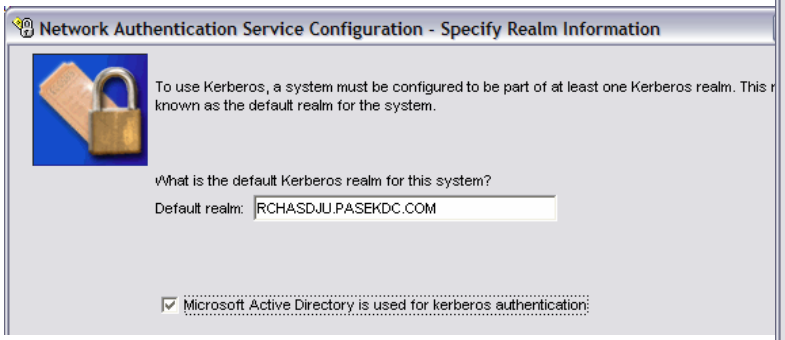
- New KDC support with OS/400 i5/OS
- Runs in PASE environment (ported from AIX)
- Based on MIT Kerberos distribution
- Configured through PASE terminal session
  - No graphical user interface
- Easy setup through IBM supplied configuration scripts

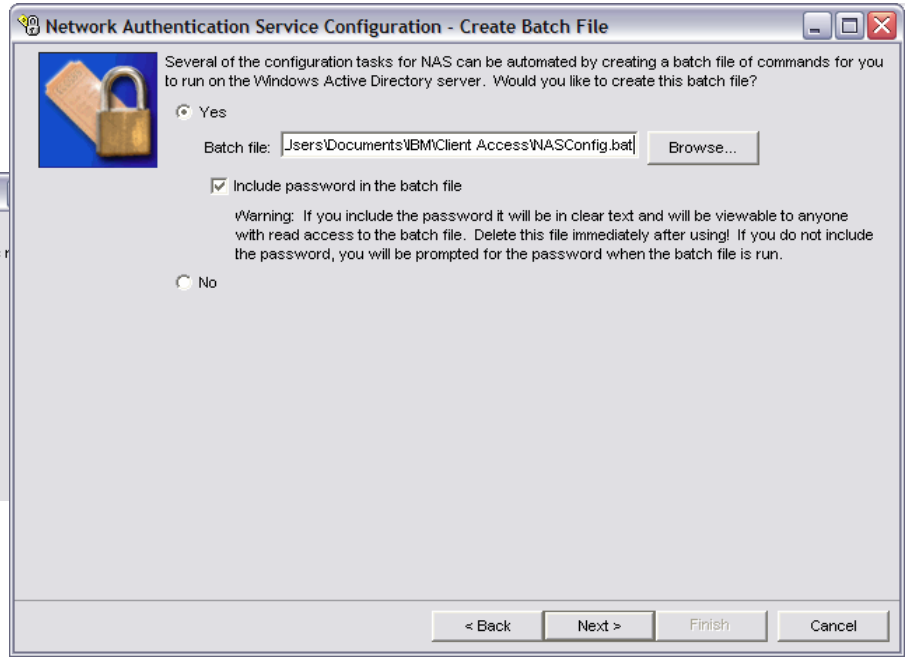
1. Start PASE shell	**Call QP2TERM**
2. Set path	**PATH=$PATH:/usr/krb5/sbin**
3. Run configuration script	**config.krb5**
4. Start the KDC	**start.krb5**
5. Configure auto start	
6. Add principals to KDC	**kadmin –p admin/admin**

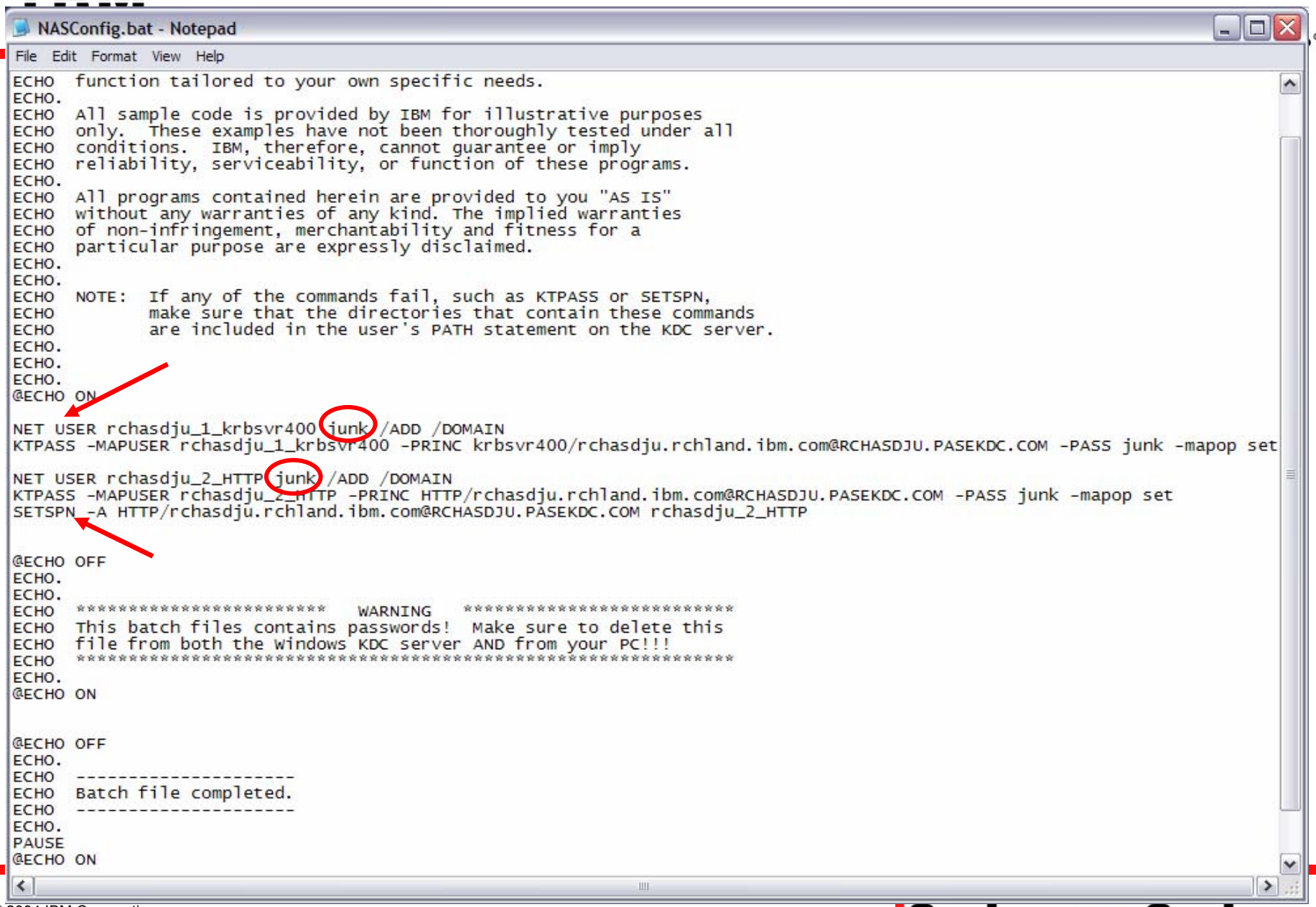
Network Authentication Service
Manage Keytab…, Properties…



Auto created batch file for Windows Server commands







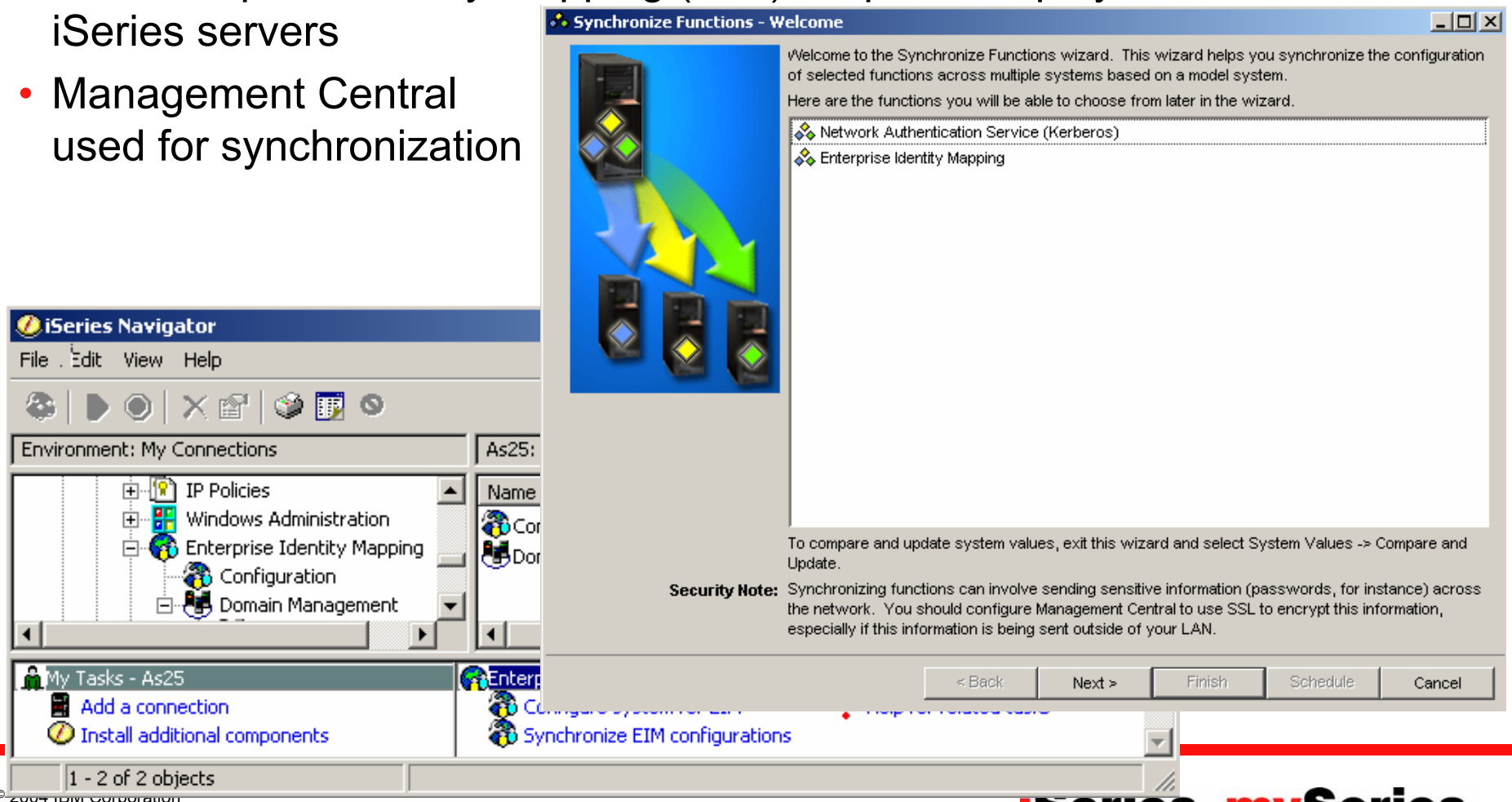
EIM Enhancements

EIM Enhancements

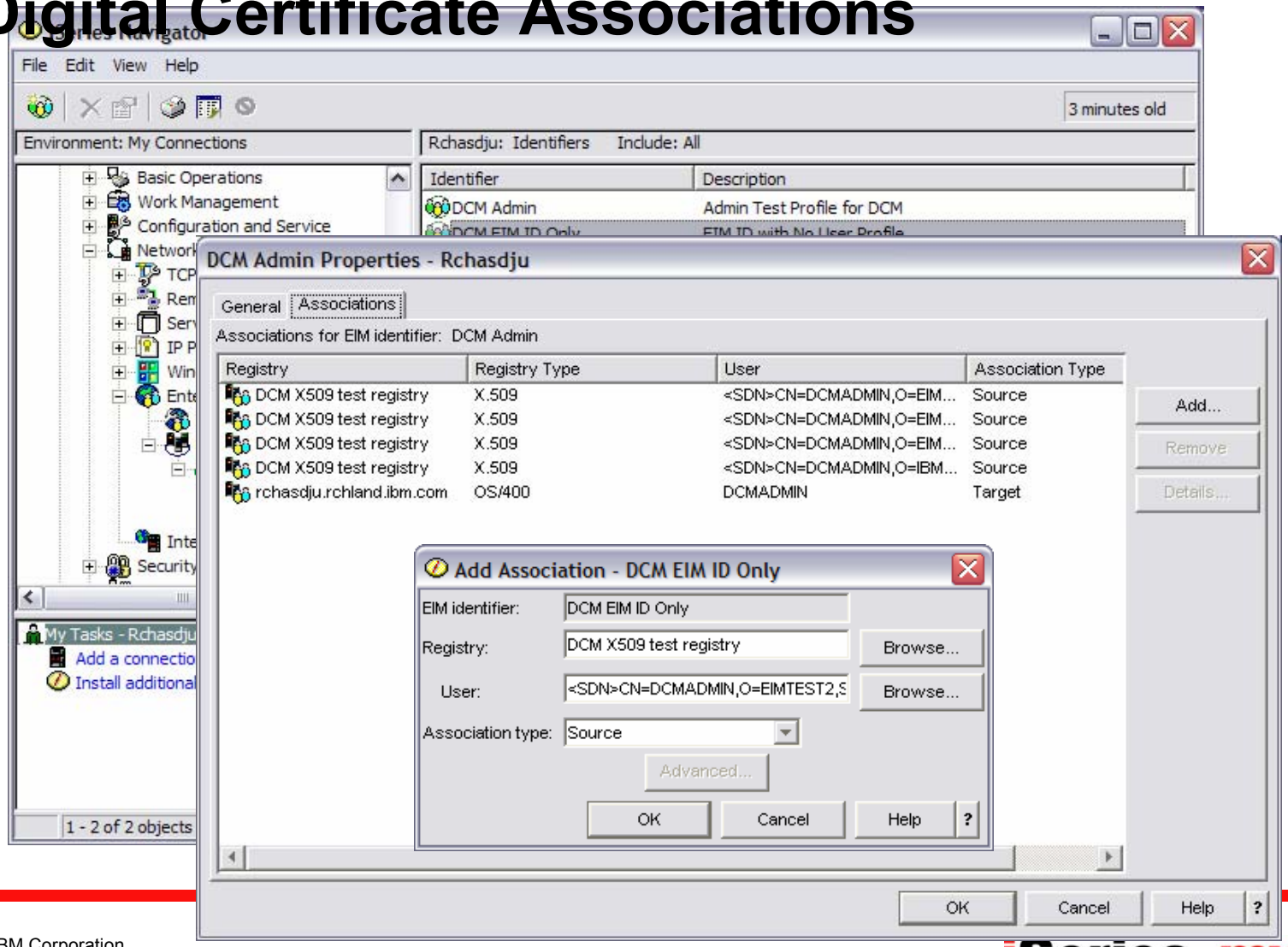
- New EIM function
  - Management Central Network Authentication Service and EIM Synchronization across platforms
  - Digital Certificate Associations
  - New EIM support for Policy Mapping (i.e. many users to one user) without requiring source associations for each user
  - EIM GUI enhancements for new function and usability
    - Mapping verification support to ensure correct user mapping
  - New parameters on crusrprf and chgusrprf
- Third-Party ISV EIM Management Support

NAS and EIM synchronization support

- New synchronization support for Network Authentication Service (NAS) and Enterprise Identity Mapping (EIM) simplifies deployment across iSeries servers
- Management Central used for synchronization

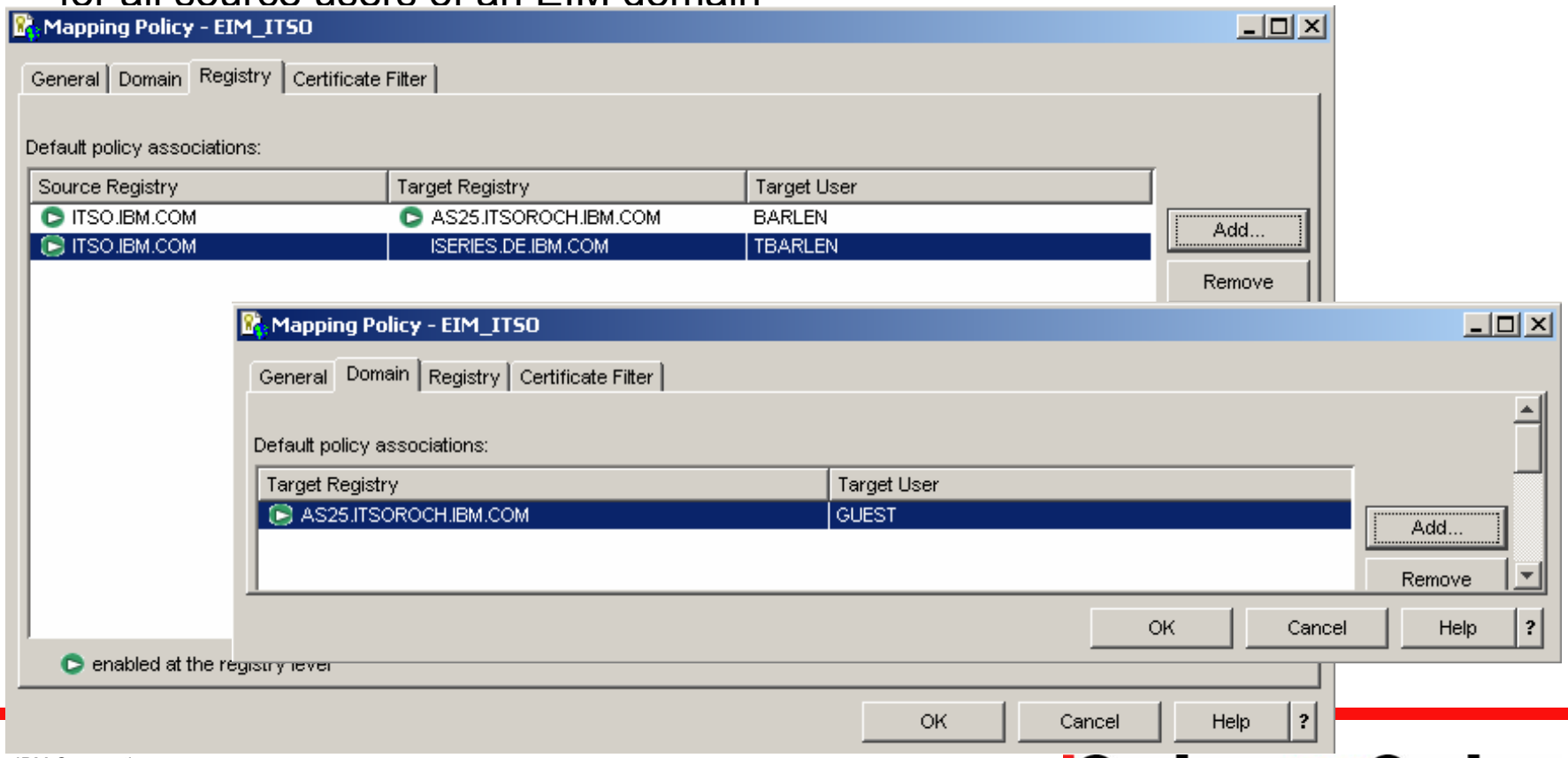


Digital Certificate Associations



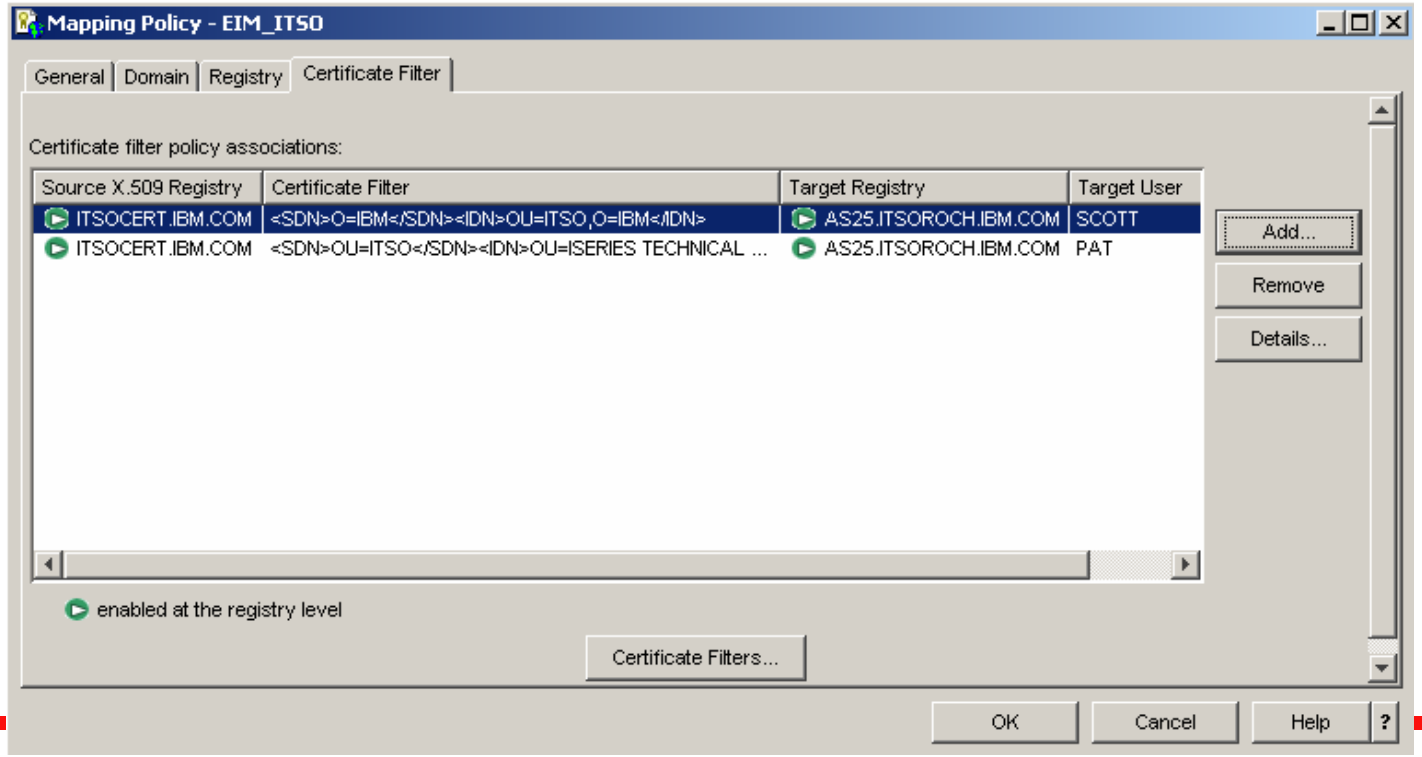
Mapping policies – Domain and registry mapping

- Registry mapping associations provide a target association for a user of a specific source registry
- Domain mapping associations provide a target association of a target registry for all source users of an EIM domain



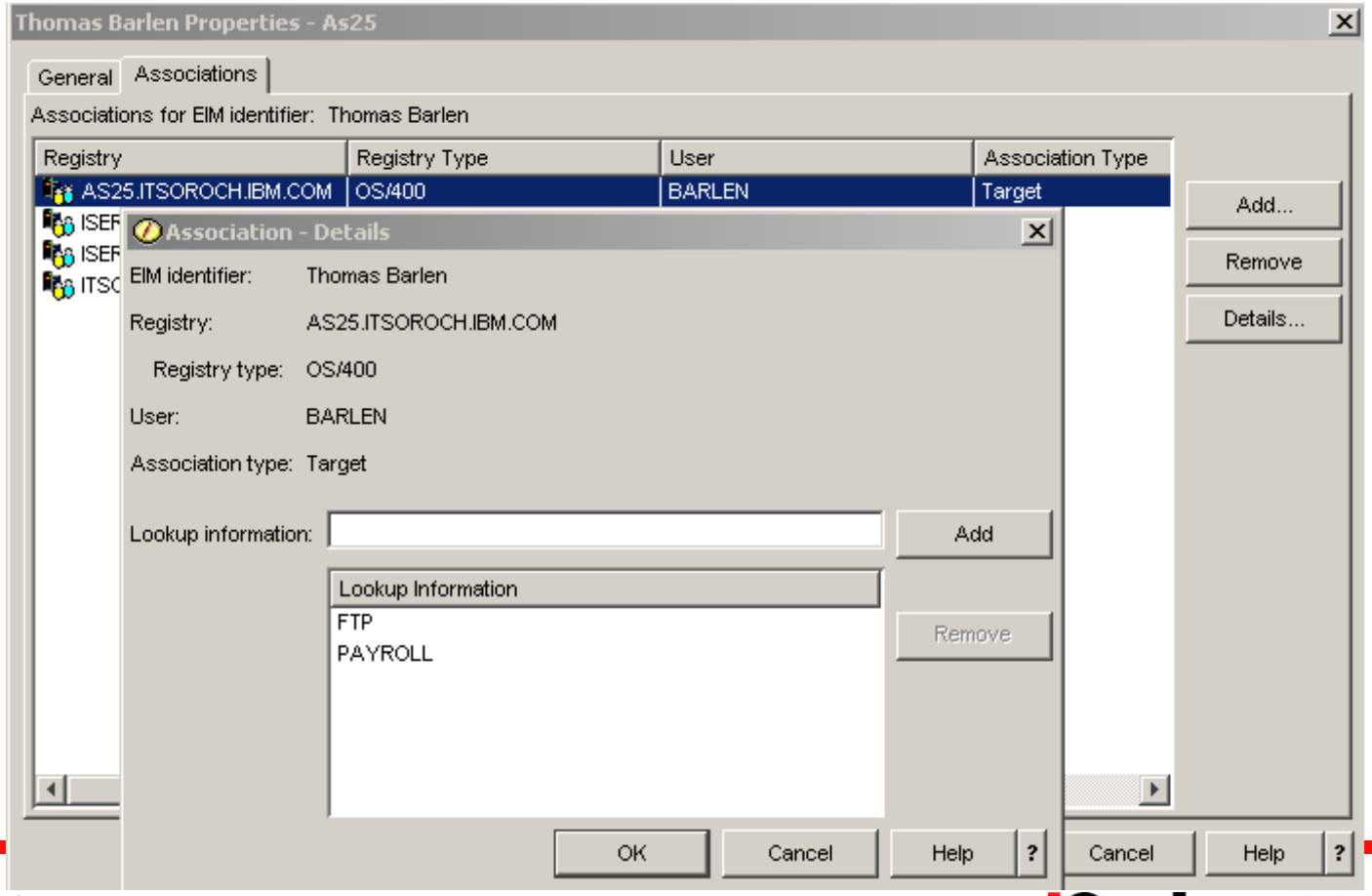
Mapping policies – Certificate filter mapping

- Certificate filter mapping can be used for mapping:
  - Entire distinguished names (DNs) from a X.509 source registry to a specific association of a target registry
  - Any part of a DN from a X.509 source registry to a specific association of a target registry
    - Filter based on entire DN or parts of issuer and subject DN



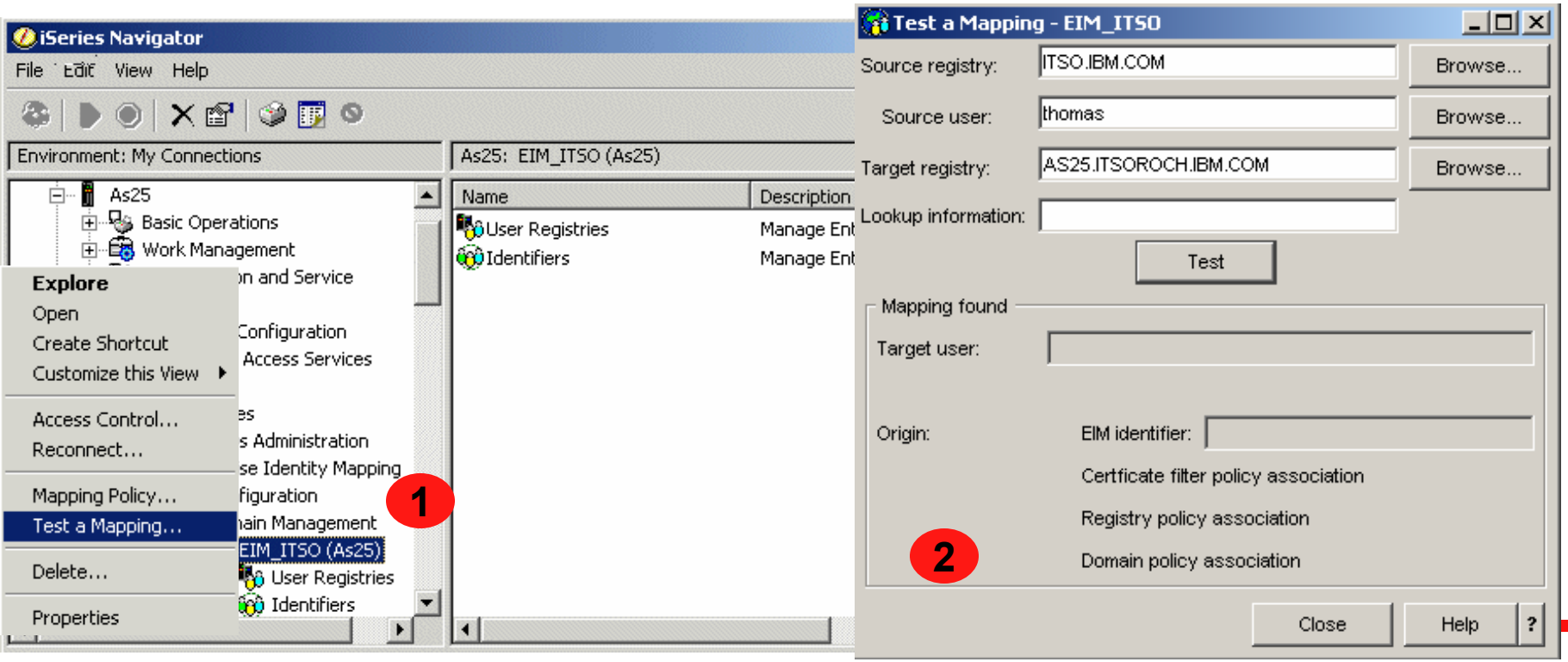
Additional lookup information

- Provides additional information to uniquely identify a target association
- Prevents lookup process from returning ambiguous results
- OS/400 applications do not consider additional lookup information



Testing mapping lookup operations

- New policy associations and lookup information introduce a more flexible way of determining a target association
- But, using all new functions in conjunction makes it more difficult to determine which target association is actually being used
- New awesome mapping test provides exact information which target association is returned based on which definition in a lookup operation



CRTUSRPRF/CHGUSRPRF EIM Parameters

Create User Profile (CRTUSRPRF)

Type choices, press Enter.

EIM association:

EIM identifier	*NOCHG
Association type	*TARGET, *SOURCE, *TGTSRC...
Association action	*REPLACE, *ADD, *REMOVE
Create EIM identifier	*NOCRTEIMID, *CRTEIMID

```
CHGUSRPRF USRPRF(DE013711) EIMASSOC('John Doe' *SOURCE *REPLACE)
```

System Integrity Enhancements

I5/OS system integrity

- New system integrity enhancements
  - Hardware storage protection of LIC control blocks
  - Enhanced Parameter Validation for LIC interfaces
  - Objects prepared for additional storage protection in the following release
  - Additional protection of LIC privileged state via stack changes

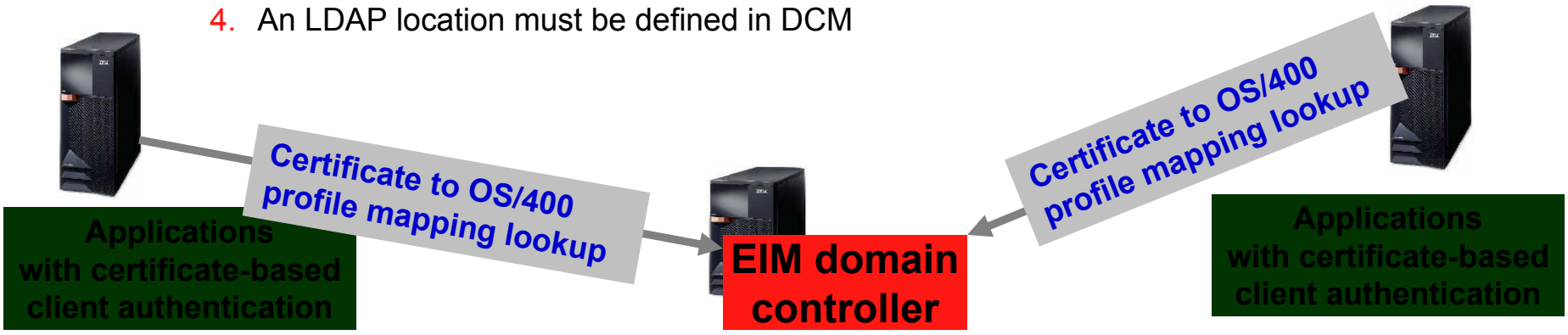
i5OS system integrity

- Check System Integrity API
  - QYDOCHKS(), QydoCheckSystem ()
  - The Check System (OPM, QYDOCHKS; ILE, QydoCheckSystem) API checks to see if any key operating system object has changed since it was signed. If any of these objects is unsigned, it is reported as an error. Only signatures from a system trusted source are valid.
  - Note: This API can take several hours to complete.

Miscellaneous Enhancements

Miscellaneous enhancements

- Digital certificates can now be published from OS/400 CA to LDAP directory
  - –If set up in DCM, OS/400 applications, such as Telnet and FTP, look up certificate to OS/400 associations via EIM
  - –The following steps need to be performed to store certificates in LDAP and support the EIM lookup for digital user certificates
    1. EIM identifier and corresponding OS/400 registry target associations must exist
    2. A X.509 registry must be added to the EIM domain
    3. The X.509 registry must be added to the EIM properties
    4. An LDAP location must be defined in DCM



User application APIs - Application Admin Commands

- New APIs for User Application support
  - New APIs that can be used to store/manage data associated with a user profile.
  - Data Saved/Restored with the user profile
  - QsyUpdateUserApplicationInfo
  - QsyRetrieveUserApplicaitonInfo
  - QsyRemoveUserApplicationInfo

New Function Usage (App Admin) CL commands

Work with Function Usage

Type options, press Enter.

2=Change usage 5=Display usage

Opt	Function ID	Function Name
	QIBM_DIRSRV_ADMIN	IBM Directory Server Administrator
	QIBM_ACCESS_ALLOBJ_JOBLOG	Access job log of *ALLOBJ job
	QIBM_ALLOBJ_TRACE_ANY_USER	Trace any user
	QIBM_QCST_SERVICE_CLUSTADMIN	Cluster Administration
	QIBM_QCST_SERVICE_CLUSTOPER	Cluster Operation
	QIBM_QYAS_SERVICE_DISKMGMT	Disk units
	QIBM_SERVICE_DUMP	Service dump
	QIBM_SERVICE_JOB_WATCHER	JOB WATCHER
	QIBM_SERVICE_THREAD	Thread control
	QIBM_SERVICE_TRACE	Service trace
	QIBM_EJB_SERVER_FUNC	
	QIBM_QBEG_OUTBOUNDMESSAGES	

More...

Crypto changes

- New set of crypto APIs for encrypt, decrypt, sign/verify, hash, hmac, mac, RSA key generation, and Diffie-Hellman key exchange.

- FIPS compliant JCE provider will be available for v5r2 and v5r3. Certification tests are currently being done.

Additional Security changes continued...

- Security toolkit commands - *AUDIT special authority allowed to run the commands
- Netserver PWD support on QSYRUPWD and QSYSUPWD APIs
- New profile handle and profile token API changes
  - New parameter(s) must be specified when verifying a password on QSYGETPH,
  - Length and CCSID of password
- Path name support on QSYRTVUA (retrieve authorized users) API

Additional Security changes continued...

- **New Open Database File Exit Point**
  - QIBM_QDB_OPEN
  - Exit program passed a list of files referenced in the open request and the open options.
  - Exit program may set a return code value to end the open request.
  - If the file being opened is a logical file or a query, multiple files may be passed to the exit program. The originally requested files will be passed in as well as any underlying physical files.
- **Only full opens will call the exit program**.
  - If the file is being opened as the result of an SQL statement, pseudo opens will not call the exit program.
  - Shared opens will not call the exit program.
  - Open Database File Exit Program can only be used with database objects. An open of a DDM file will not call the exit program on the source system, but it will call the exit program on the target system.

Backup Charts

More Granular Network Communication AUDLVL values

***NETCMN**

Networking and communications functions are audited. The following are some examples:

- Network base functions (See ****NETBAS***)
- Cluster or cluster resource group operations (See ****NETCLU***)
- Network failures (See ****NETFAIL***)
- Secure sockets functions (See ****NETSCK***)

*bold, italicized tems = new values in i5/OS

More granular Security Related AUDLVL values

***SECURITY** = All security-related functions are audited. These include:

- Security configuration (See ***SECCFG***)
- Changes or updates when doing directory service functions (See ***SECDIRSRV***)
- Changes to interprocess communications (See ***SECIPC***)
- Network authentication service actions (See ***SECNAS***)
- Security run time functions (See ***SECRUN***)
- Secure socket descriptor (See ***SECSCKD***)
- Use of verification functions (See ***SECVFY***)
- Changes to validation list objects (See ***SECVLDL***)

*bold, italicized tems=new value in i5/OS

Notes: Single Sign-On with Management Central

- Another enhancement in i5/OS is the support of Kerberos authentication for Management Central. EIM is also supported with Management Central, but not mandatory. If EIM is not used, The endpoint system authenticates only the server it receives a request from. The actual request is then performed under the user profile of the originating system (same behavior as with systems prior to i5/OS). If EIM is enabled for Management Central, you have the following choices:
  1. The endpoint system tries to find a target mapping for the source identifier, if no target mapping can be found, the request is performed under the profile of the originator.
  2. If EIM is enforced and there is no target association defined, the request will fail.
- To enable Kerberos and EIM for Management Central, an administrator must perform a series of one-time setup steps as outlined on the previous chart. Detailed implementation steps are provided in the iSeries InformationCenter under Networking->Networking Security->Network Authentication Service->Scenarios->Scenario: Use Kerberos authentication between Management Central servers and the scenario Scenario: Enable single signon
- Note that during Kerberos activation for Management Central, you temporarily set up the endpoint systems to dynamically build a trusted group. This trusted group contains the Kerberos service principals of the other Management Central servers. After all systems have been added and the trusted group is complete, you need to change the central system setting to allow only trusted connections. This change has to be synchronized to all other endpoint systems.

Notes: Windows Integration and SSO (1)

- In a typical EIM configured environment, which uses single sign-on, OS/400 target associations and Windows source associations are typically defined. With integrated Windows server user administration with i5/OS, the system administrator may decide to define enrolled Windows users to have EIM associations automatically defined. For instance, if an enrolled Windows user has EIMASSOC(*USRPRF *TARGET *ADD *CRTEIMID) specified, OS/400 will automatically create an OS/400 target and a Windows source association. The EIMASSOC information is not stored in the user profile. Also, this information is not saved or restored with the user profile. And, if the OS/400 system is not configured for EIM, then no association processing is done and the EIMASSOC information is ignored.

- If OS/400 is configured to use EIM and EIMASSOC processing is defined for the enrolled user, integrated Windows server user administration will auto create or delete Windows source associations for the user in the Windows EIM registry. For a user enrolled locally to the Windows environment, the Windows EIM registry name is the fully qualified, local Domain Name System (DNS) name. The Windows EIM registry type is defined to be Windows 2000. For users enrolled to a Windows domain, the Windows registry name is the fully qualified domain DNS name and the Windows registry type is defined to be Kerberos - case ignore. If EIMASSOC is defined for a user, and OS/400 is configured to use EIM, and the Windows EIM registry doesn't exist, integrated Windows server user administration will create the Windows EIM registry.

Notes: Windows Integration and SSO (2)

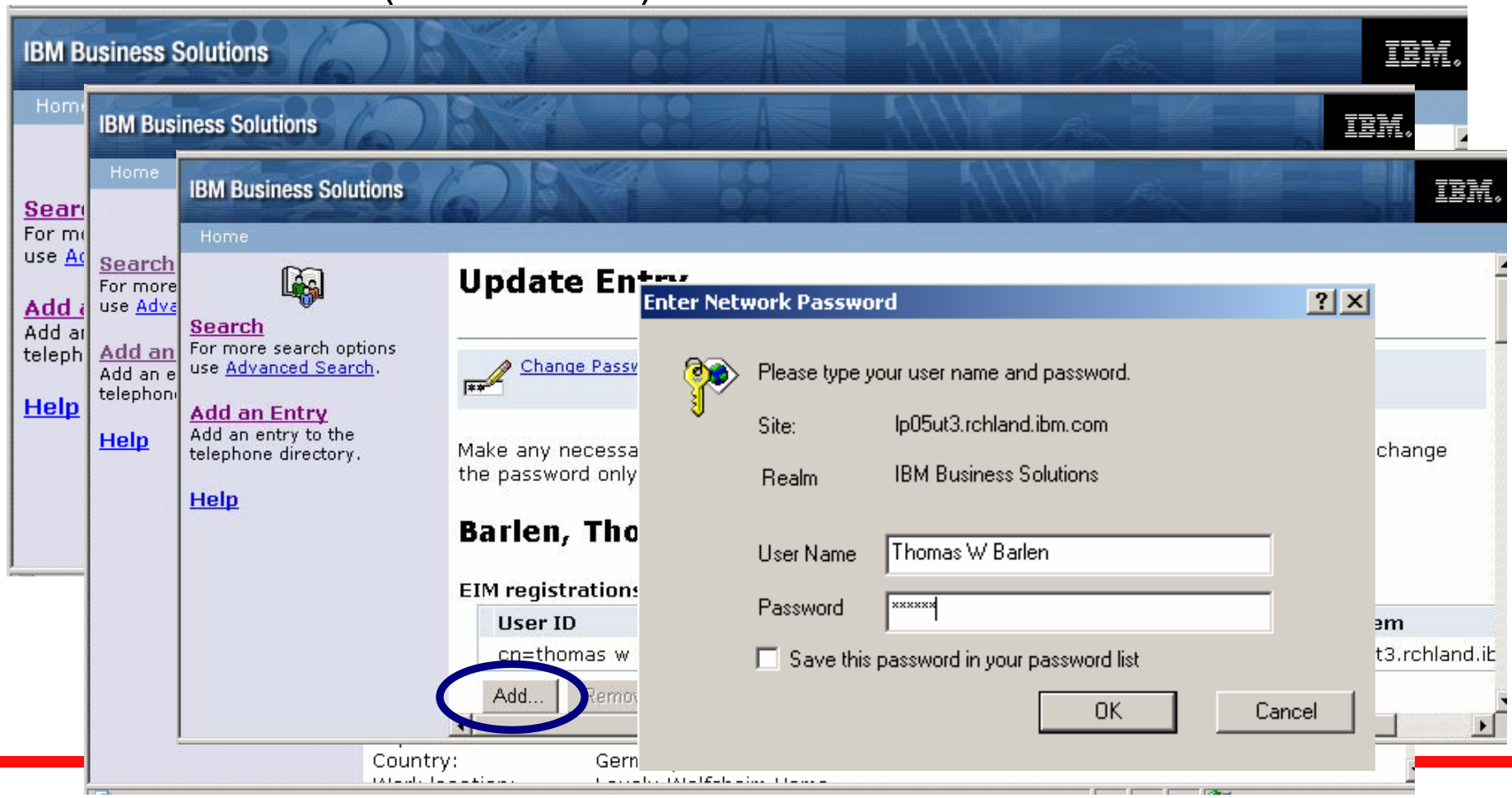
- Also new is the Kerberos support for the SBMNWSCMD command and the NetClient. There are some considerations when using the new support.
  - The iSeries NetServer should be configured to use Password/Kerberos v5 authentication and NetServer must be active.
  - The Kerberos KDC must be a Windows Active Directory domain controller .
  - Kerberos authentication will only be used when the OS/400 job's user profile has the LCLPWDMGT attribute set to *NO. When LCLPWDMGT is set to *YES, then password authentication will always be used.
  - NetClient can only successfully authenticate using Kerberos to integrated servers that are members of the same Windows domain as the OS/400 default Kerberos realm.
  - User Enrollment supports using EIM to map a Windows user name to a different OS/400 profile name. Thus, user enrollment can look for an EIM registry which is named for the Windows Active Directory domain name, or for a EIM registry which is named for the integrated server name as appropriate. User enrollment will use the EIM mapping regardless of whether Kerberos authentication can be used. However, SBMNWSCMD and NetClient will only use an EIM mapped name when Kerberos authentication is used. So, user enrollment may create a local windows user with a different name than the OS/400 profile as specified by the EIM mapping. But, SBMNWSCMD and NetClient will only use the different windows name when Kerberos authentication is performed (When LCLPWDMGT = *NO). Otherwise, they attempt to authenticate with a Windows name equal to the OS/400 profile name.
  - For SBMNWSCMD submitted windows commands to be able to connect to other network servers when Kerberos authentication is used, the target windows server must be trusted for delegation. In Windows 2000, this is enabled by default for domain controllers. However, it is disabled by default for domain member servers. It may be enabled via the Administration Tool: Active Directory User and Computers on a domain controller. Within this tool, click Computers and select the correct computer. Then click Computer properties -> General. Then check Trust computer for delegation.

Notes: HTTP Server for iSeries (powered by Apache)

- The HTTP Server for iSeries (powered by Apache) supports in i5/OS the authentication via Kerberos and identity mapping through EIM. This enhancements was also made available to V5R2 users via the HTTP server group PTF (SF99098). It allows Microsoft Internet Explorer V5 and higher browser to authenticate to a protected resource via the Kerberos authentication protocol. To leverage Kerberos authentication for the Web browser, you need to change the following setting within Internet Explorer:
  1. From the action bar select **Tools** and then **Internet Options…**
  2. Select the **Advanced** tab.
  3. Scroll down the settings window to the Security section.
  4. Check the option **Enable Integrated Windows Authentication (requires restart).**
- Within the HTTP server configuration, you have to set up security to protect a resource. This is done as usual. The only difference is, that you now have a new option (Kerberos) for authentication.

EIM association management – IBM Telephone Directory

- IBM Telephone Directory provides people the ability to manage their own user identities (associations) within an EIM domain



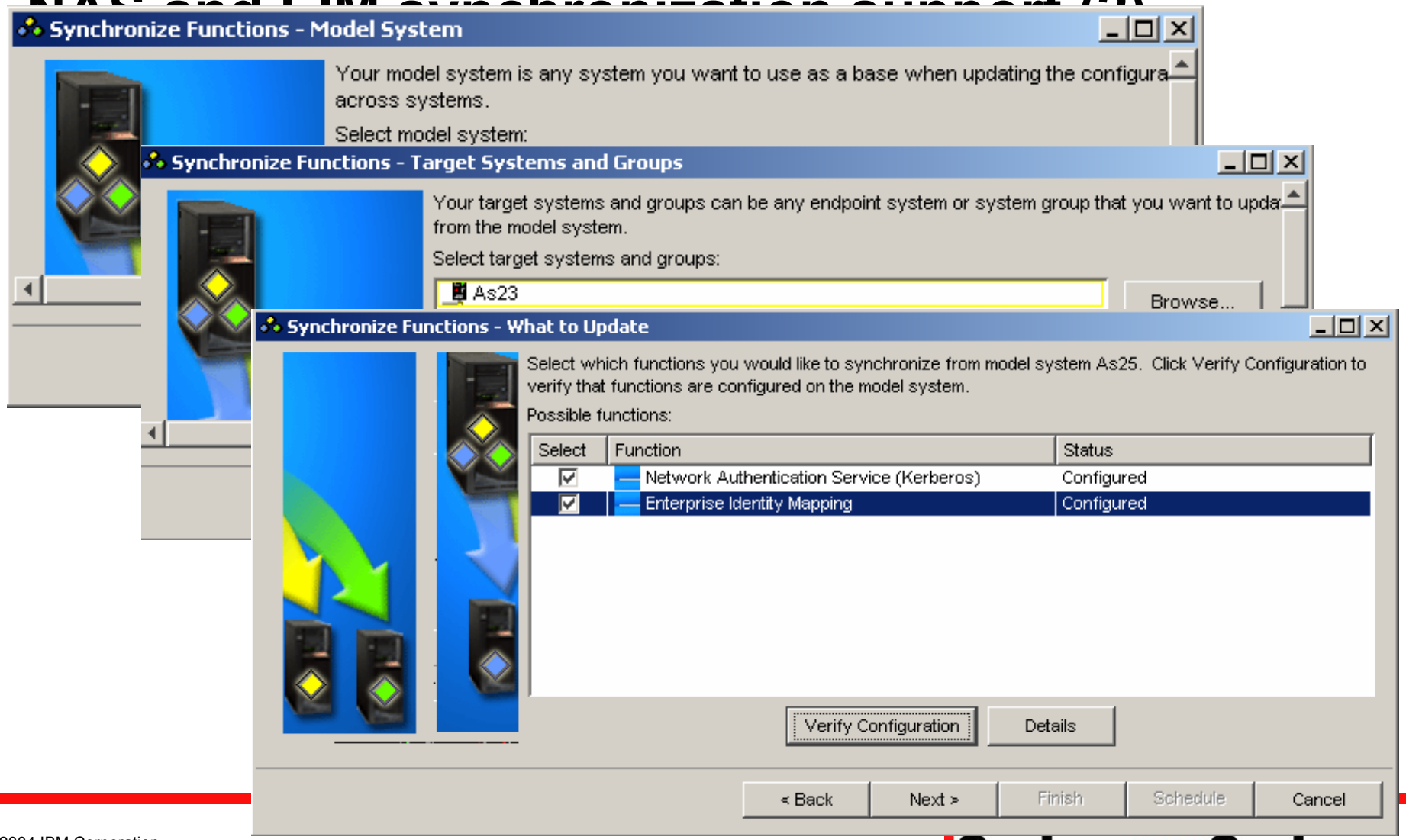
Notes: OS/400 Key Distribution Center (KDC) support

- With i5/OS, OS/400 supports a Kerberos server in the OS/400 Portable Application Solutions Environment (PASE). OS/400 PASE provides an integrated run-time environment for AIX applications.
- The Kerberos server is configured through the PASE terminal session initiated by the OS/400 command CALL QP2TERM. InformationCenter contains detailed steps on how to set up the Kerberos server.
- To establish a Kerberos environment that maximizes availability, you can install multiple secondary Kerberos servers. In this case, there is one master server and one ore more secondary servers. Updates in configuration can only be made on the master server. These changes will automatically be replicated to all secondary servers.
- Another advantage of operating an OS/400 KDC was depicted on the previous chart. If you have one or more Windows domains with their Kerberos realms, you can set up cross-realm authentication between Windows and OS/400 KDCs. If one Windows KDC fails, all other clients will still be able to authenticate with their own KDC and the iSeries KDC. You can even configure a Windows client so that it can authenticate from the Login window to different Kerberos realms.
- You need the following license programs to run the Kerberos server on iSeries in PASE environment:
  - OS/400 Host Servers (5722-SS1 Option 12)
  - OS/400 PASE (5722-SS1 Option 33)
  - Qshell Interpreter (5722-SS1 Option 30)
  - Cryptographic Access Provider (5722-AC3)
  - iSeries Access for Windows (5722-XE1)

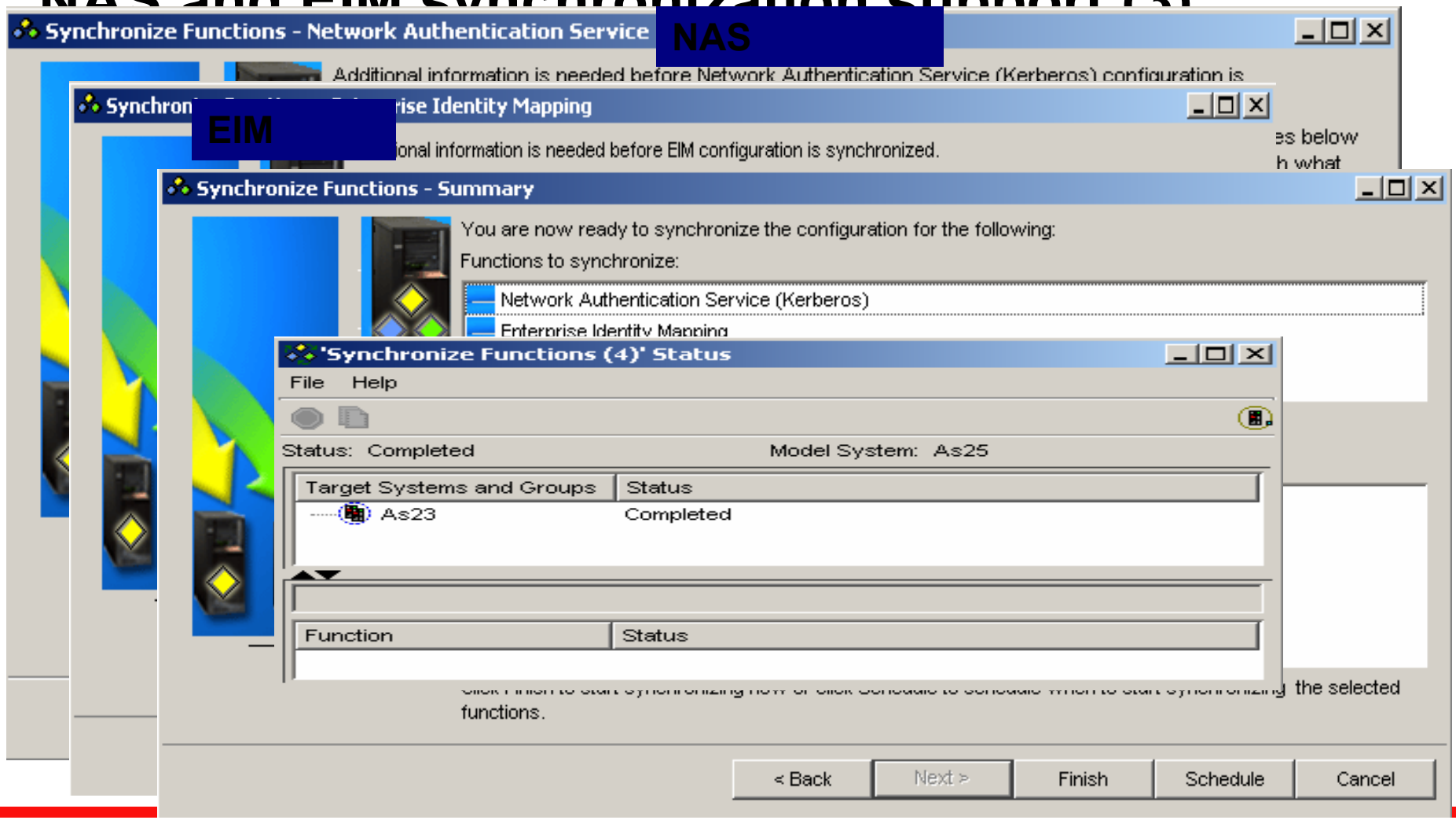
Notes: NAS wizard enhancements

- The new i5/OS wizard in iSeries Navigator allows administrators to add service principals for OS/400 Kerberos Authentication, Directory services (LDAP), IBM HTTP Server for iSeries, or iSeries NetServer interfaces. During Enterprise Identity Mapping (EIM) configuration, the EIM wizard will check if network authentication service is configured. If it is, the wizard will then check if keytab entries for any of these system interfaces are missing. The EIM wizard will then start the Kerberos service principal wizard, so that the administrator can add these services to the keytab file. See Manage keytab files for details.
- Within the network authentication service and Kerberos service principal configuration wizard, administrators will be provided with messages that alert them when host names resolved from a PC and the iSeries do not match. If host names do not resolve, administrators can optionally create multiple keytab entries for each of these host names. It is important to understand how host resolution is configured on your network before you configure network authentication service.
- During configuration of network authentication service a tool will be generated to assist an administrator to configure Microsoft Windows Active Directory to operate with iSeries server.

NAS and EIM synchronization support (2)

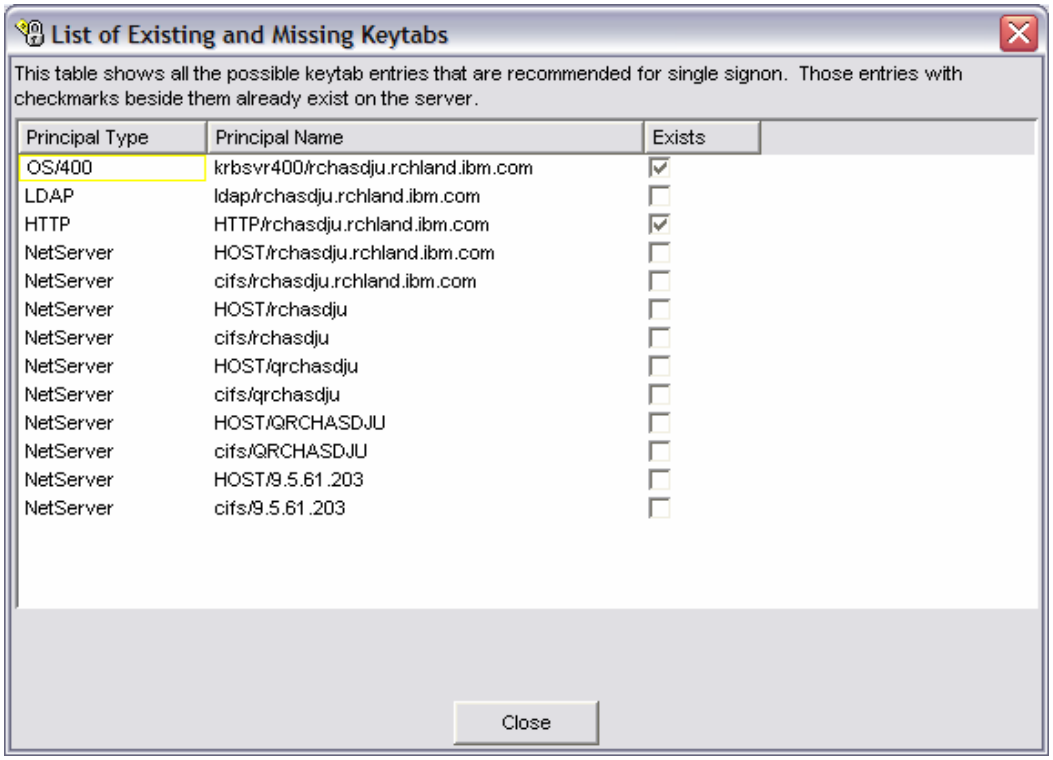


NAS and EIM synchronization support (3)



iSeries. mySeries.

Manage Keytab screen



Notes: NAS configuration batch file support

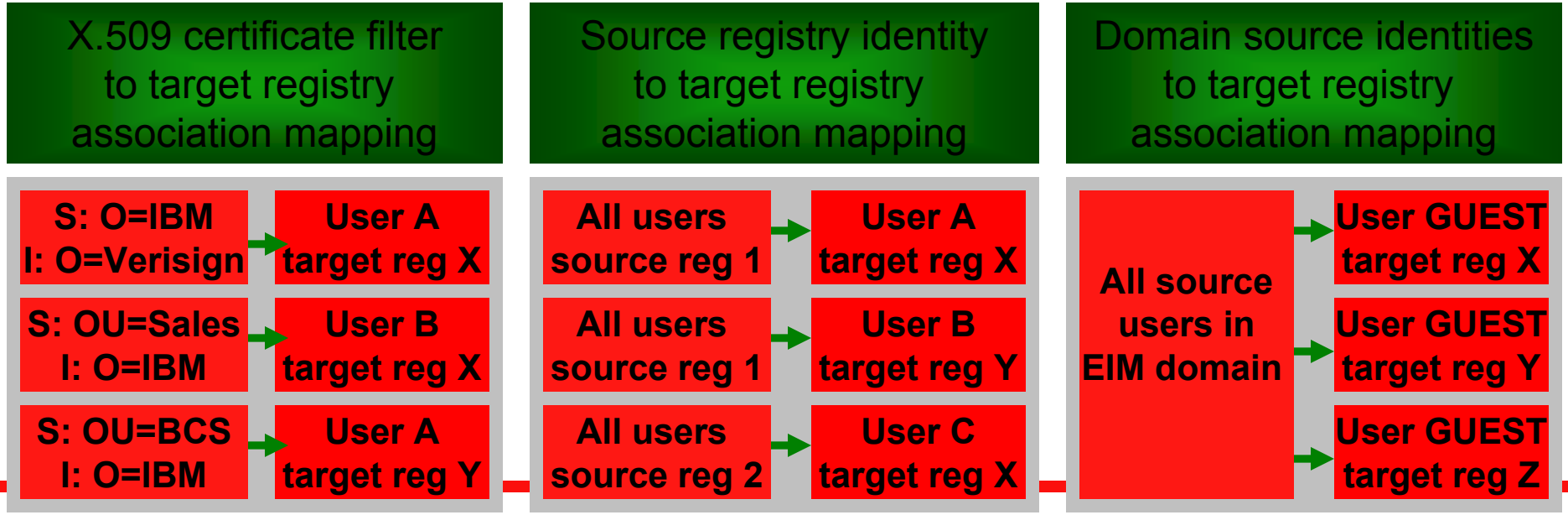
- Another enhancement that is introduced with the i5/OS NAS wizard allows administrators to easily set up the necessary configuration for OS/400 Kerberos services on a Microsoft Windows Active Directory server. When running the wizard and selecting the option that Microsoft Active Directory is used for authentication, a batch file will be created when finishing the wizard. This batch file contains the commands to set up a domain user account for a service and then map the Kerberos service principal to the corresponding account.
- The wizards prompts for a batch file name and location. It also allows an administrator to decide whether the service password are stored within the batch file. If you select not to store the passwords in the file, Windows will prompt you for the passwords when running the batch file on the Windows server.

Notes: EIM synchronization support

- You can now synchronize key functions, such as Enterprise Identity Mapping (EIM) and Network Authentication Services (NAS - Kerberos), across a group of endpoint systems. The synchronization function uses Management Central to deploy the NAS and EIM configuration across the network. You select a model endpoint system and a set of target endpoint systems, and then use the new Synchronize Functions wizard to duplicate the model system's Kerberos or EIM configurations (or both!) on the specified target systems. Synchronizing these functions from the model system saves you time by eliminating the task of individually configuring each function on each target system.

Mapping policy support

- Can solve problems where individual mappings between local associations and EIDs do not exist
- New mapping policies provide many-to-one mappings for:
  - Unknown users of the entire domain to a single user for a specific target registry
  - Unknown users from a given source registry to a single user in a specific target registry
  - Certificate distinguished names via a filter to a single user in a specific target registry



Notes: Mapping policy support

- EIM mapping policy support allows you to use policy associations as well as specific identifier associations in a domain. You can use policy associations instead of, or in conjunction with, identifier associations. EIM mapping policy support provides a means of enabling and disabling the use of policy associations for the entire domain as well as for each specific target user registry. EIM also allows you to set whether a specific registry can participate in mapping lookup operations in general. Consequently, you can use mapping policy support to more precisely control how mapping lookup operations return results.
- The default setting for an EIM domain is that mapping lookups that use policy associations are disabled for the domain. When the use of policy associations is disabled for the domain, all mapping lookup operations for the domain return results only by using specific identifier associations between user identities and EIM identifiers. The default settings for each individual registry are that mapping lookup participation is enabled and the use of policy associations is disabled. When you enable the use of policy associations for an individual target registry, you must also ensure that this setting is enabled for the domain.
- You can configure mapping lookup participation and the use of policy associations for each registry in one of three ways:
  - Mapping lookup operations cannot be used for the specified registry at all. In other words, an application that performs a mapping lookup operation involving that registry will fail to return results.
  - Mapping lookup operations can use specific identifier associations between user identities and EIM identifiers only. (Mapping lookups are enabled for the registry, but the use of policy associations is disabled for the registry.)
  - Mapping lookup operations can use specific identifier associations when they exist and policy associations when specific identifier associations do not exist. (All settings are enabled.)

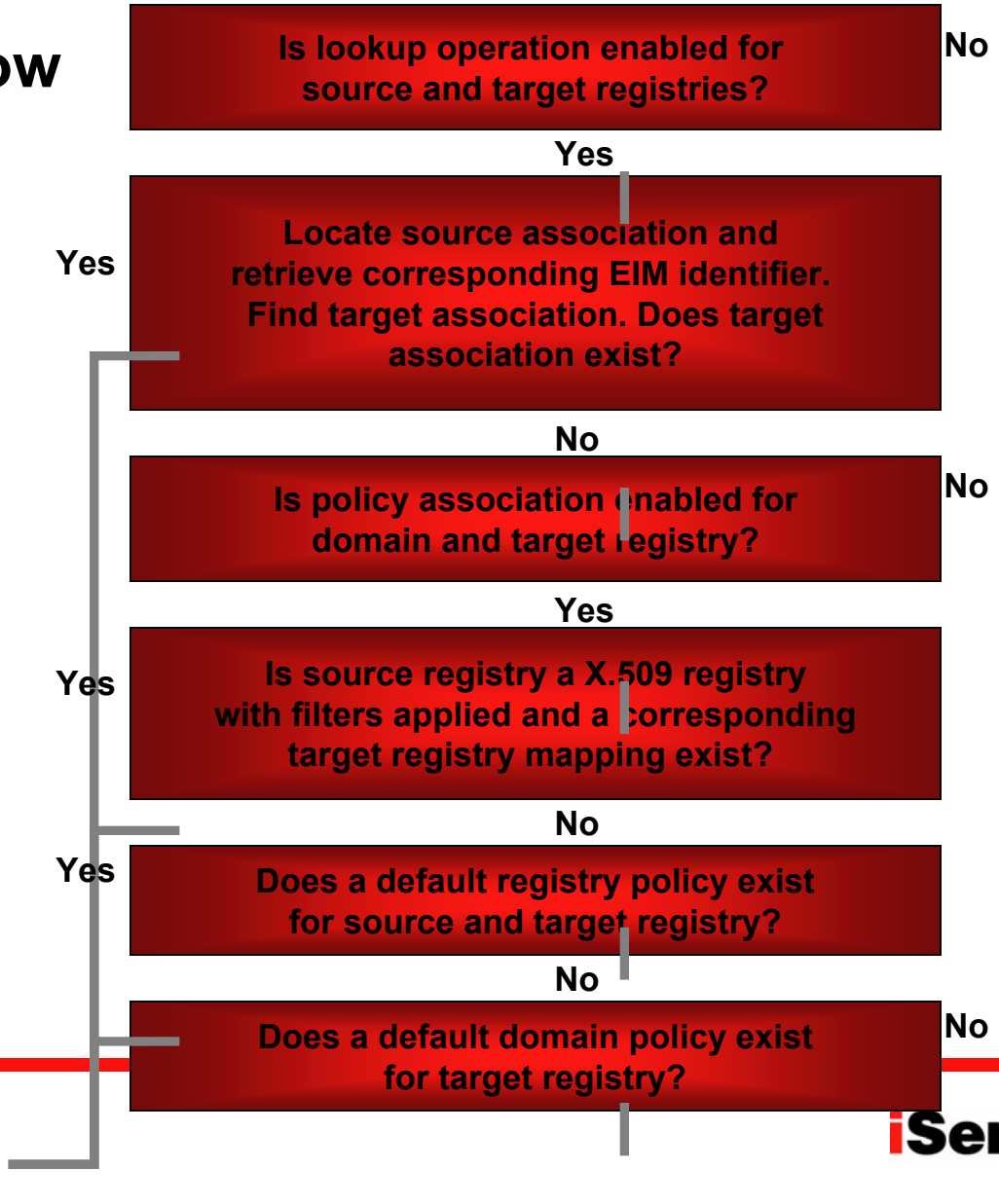
Notes: Mapping policies – Domain and registry mapping

- A policy association provides a means of creating many-to-one mappings in situations where associations between user identities and an EIM identifier do not exist. You can use a policy association to map a source set of multiple user identities (rather than a single user identity) to a single target user identity in a specified target user registry.
- In a default registry policy association, all users in a single registry are the source of the policy association and are mapped to a single target registry and target user. When you enable the default registry policy association for the target registry, the policy association ensures that these source user identities can all be mapped to a single specified target registry and target user.
- In a default domain policy association, all users in the domain are the source of the policy association and are mapped to a single target registry and target user. You can define a default domain policy association for each registry in the domain.
- Because you can use policy associations in a variety of overlapping ways, you should have a thorough understanding of EIM mapping policy support and lookup operations before you create and use policy associations.

Notes: Mapping policy support – Certificate filter mapping

- In a certificate filter policy association, you specify a set of certificates in a single X.509 registry as the source of the policy association. These certificates are mapped to a single target registry and target user that you specify. Unlike a default registry policy association in which all users in a single registry are the source of the policy association, the scope of a certificate filter policy association is more flexible. You can specify a subset of certificates in the registry as the source. The certificate filter that you specify for the policy association determines its scope.
- A certificate filter defines a set of similar distinguished name certificate attributes for a group of user certificates in an X.509 source user registry. You can use the certificate filter as the basis of a certificate filter policy association. The certificate filter in a policy association determines which certificates in the specified source X.509 registry to map to the specified target user. Those certificates that have Subject DN and Issuer DN information that match the filter are mapped to the specified target user during EIM mapping lookup operations.
- For example, when a digital certificate is the source user identity in an EIM mapping lookup operation (after the requesting application uses the eimFormatUserIdentity() EIM API to format the user identity name), EIM first checks to see if there is an identifier association with an EIM identifier for that user identity. If none exist, EIM then compares the DN in the certificate against the DN or partial DN specified in the filter for the policy association. If the DN information in the certificate matches the filter, EIM returns the target user identity that the policy association specified.
- You can specify one or both of the following to define a certificate filter:
  - Subject distinguished name (DN). The full or partial DN that you specify for the filter must correspond to the subject DN portion of the digital certificate. You can provide the full subject DN string, or you can provide one of the parent's DNs.
  - Issuer distinguished name (DN). The full or partial DN that you specify for the filter must correspond to the issuer (the Certificate Authority) subject DN portion of the digital certificate. You can provide the full issuer DN string, or you can provide one of the parent's DNs.

Mapping lookup search flow



Notes: Mapping lookup search flow

With the introduction of mapping policies and additional lookup information, the way of determining which target association will be return for a lookup operation, you need to understand the search flow. The following list describes how EIM lookups work.

1. The lookup operation checks whether mapping lookups are enabled. The lookup operation determines whether mapping lookups are enabled for both the specified source registry and the specified target registry. If mapping lookups are not enabled for one or both of the registries, then the lookup operation ends without returning a target user identity.
2. The lookup operation checks whether there are identifier associations that match the lookup criteria. The lookup operation does this by checking whether there is a specific individual source association that matches the supplied source user identity and source registry. If there is one, the lookup operation uses it to determine the appropriate EIM identifier name. The lookup operation then uses the EIM identifier name to search for an individual target association for the EIM identifier that matches the specified target EIM registry definition name. If there is an individual target association that matches, the lookup operation returns the target user identity defined in the target association.
3. The lookup operation checks whether the use of policy associations are enabled. If the lookup operation cannot return any results based on its search of identifier associations, it checks whether the domain is enabled to allow mapping lookups using policy associations. The lookup operation also checks whether the target registry is enabled to use policy associations.
4. The lookup operation checks for certificate filter policy associations. The lookup operation checks whether the source registry is an X.509 registry type. If it is an X.509 registry type, the lookup operation checks whether there is a certificate filter policy association that matches the source and target registry definition names. If there is a matching policy association, the lookup operation returns the appropriate target user identity for that policy association.
5. The lookup operation checks for default registry policy associations. The lookup operation checks whether there is a default registry policy association that matches the source registry definition name. If there is a matching policy association, the lookup operation returns the appropriate target user identity for that policy association.
6. The lookup operation checks for default domain policy associations. The lookup operation checks whether there is a default domain policy association defined for the target registry definition. If there is a matching policy association, the lookup operation returns the associated target user identity for that policy association.
7. The lookup operation is unable to return any results.

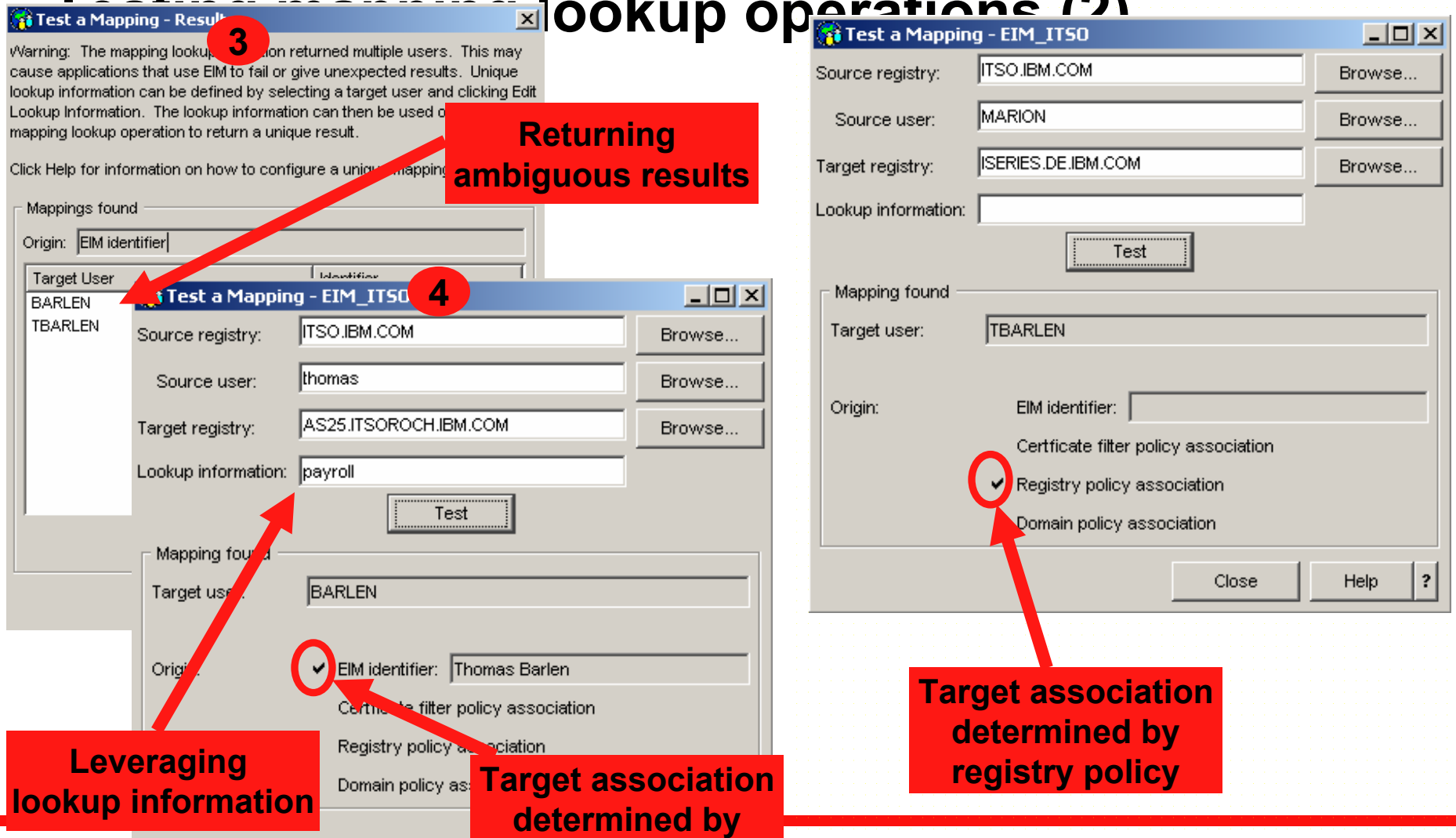
Notes: Additional lookup information

- Additional lookup information specify optional unique identifying data for the target user identity in an association. This target user identity can be specified either in an identifier association or in a policy association. Lookup information is necessary only when a mapping lookup operation can return more than one target user identity. This situation can create problems for EIM-enabled applications, including OS/400 applications and products, that are not designed to handle these ambiguous results.

- Lookup information define a unique character string that either the eimGetTargetFromSource EIM API or the eimGetTargetFromIdentifier EIM API can use during a mapping lookup operation to further refine the search for the target user identity that is the object of the operation. Data that you specify for lookup information corresponds to the registry users additional information parameter for these EIM APIs.

- You can specify multiple lookup information entries for a target association.

Testing mapping lookup operations (2)



iSeries. mySeries.

Notes: Testing mapping lookup operations

- The Test a Mapping dialog allows you to verify that a specific source user identity maps correctly to the appropriate target user identity. Such testing ensures that EIM mapping lookup operations can return the correct target user identity based on the specified information.
- The previous charts show an example as described below:
  1. From iSeries Navigator, right click on the EIM domain and select Test a Mapping…
  2. In the Test a Mapping dialog you have to specify a source registry and source association you want to lookup a target association for a specific target registry.
  3. In this case, the lookup for source user `thomas` in source registry `ITSO.IBM.COM` for target registry `AS25.ITSOROCH.IBM.COM` returned an ambiguous result (two target associations).
  4. Using additional lookup information, the lookup process returned just one target association. You can also see on the dialog windows where the returned target association originates from. In this case, the target association was returned based on the associations defined for the EIM identifier.

Notes: Miscellaneous enhancements

- By default, Digital Certificate Manager (DCM) stores the user certificates that the Local Certificate Authority (CA) issues with OS/400 user profiles. However, with i5/OS you can configure Digital Certificate Manager (DCM) in conjunction with Enterprise Identity Mapping (EIM) so that when the Local Certificate Authority (CA) issues user certificates, the public copy of the certificate is stored in a specific Lightweight Directory Access Protocol (LDAP) server directory location. A combined configuration of EIM with DCM allows you to store user certificates in an LDAP directory location to make the certificates more readily available to other applications. This combined configuration also allows you to use EIM to manage user certificates as a type of user identity within your enterprise.

- An additional parameter, called EIMASSOC, has been added to both the Create user profile (CRTUSRPRF) command and the Change user profile (CHGUSRPRF) command. The EIMASSOC parameter allows you to define EIM identifier associations for the specified user profile for the local registry. To use this parameter, you specify the EIM identifier, an action option for the association, the type of identifier association, and whether to create the specified EIM identifier if it does not already exist.

Notes: DCM, and Digital Ceritificate APIs

- By default, Digital Certificate Manager (DCM) stores the user certificates that the Local Certificate Authority (CA) issues with OS/400 user profiles. However, you can configure Digital Certificate Manager (DCM) in conjunction with Enterprise Identity Mapping (EIM) so that when the Local Certificate Authority (CA) issues user certificates, the public copy of the certificate is stored in a specific Lightweight Directory Access Protocol (LDAP) server directory location. A combined configuration of EIM with DCM allows you to store user certificates in an LDAP directory location to make the certificates more readily available to other applications on other systems. This combined configuration also allows you to use EIM to manage user certificate associations. The certificate is NOT stored in EIM, but the association of the certificate with the user is managed in EIM.
- Certificate Expiration. This new function allows you to quickly and easily view and manage certificates based on certificate expiration date. You can check certificate expiration for server or client certificates and object signing certificates on the local system. Also, you can check user certificate expiration. You can check user certificate expiration either for a specific user profile, for all user certificates on the system, or for all user certificates in an enterprise when EIM is configured on the system.

Notes: Application Information APIs

- Similar function to the provided by Windows Registry. Allows applications to save and retrieve application information specific to a particular profile. For example, the screen or view the user was in when the last exited the program so the program can start at the same screen or view when run the next time.
- Based on function that was available to the operating system prior to i5/OS.
- See Programming, APIs, What's new for i5/OS topic in the Information center for details.

Digital Certificates

- Digital Certificate Manager
  - Manage LDAP Location
    - Store user certificates in LDAP rather than in a user profile
    - Use EIM to manage certificate Associations
  - Check certificate expiration
- Digital Certificate APIs enhancements
  - Support to store certificates in LDAP
  - Certificate expiration management changes

Additional Information

The Kerberos Network Authentication Service (V5), RFC1510	http://www.ietf.org/rfc/rfc1510.txt
Microsoft's Active Directory home page	http://www.microsoft.com/activedirectory
V5R2 iSeries Information Center, Security topics	http://www.iseries.ibm.com/infocenter
Kerberos, A Network Authentication System	ISBN 0-201-37924-4
Implementation and Practical Use of LDAP on the IBM @server iSeries Server	SG24-6193
SSO Concepts in: Experts' Guide to OS/400 & i5/OS Security	http://publib.boulder.ibm.com/eserver Carol Woodbury and Patrick Botz ISBN 1-58304-096-X 29th Street Press, 2003 http://www.pentontech.com/education
Windows-based Single Signon and the EIM Framework on the IBM eServer iSeries Server, SG24-6975-00	IBM Redbook http://www.ibm.com/redbooks

For more information

- http://www.ibm.com/iseries/http
- http://www.ibm.com/iseries/clientaccess
- http://www.ibm.com/iseries/firewall
- http://www.ibm.com/iseries/ebusiness/
- http://www.ibm.com/iseries/ebusiness/security
- http://www.ibm.com/iseries/casestudies/ebiz
- http://publib.boulder.ibm.com/iseries/v5r2/ic2924/index.htm

Trademarks and Disclaimers

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 of International Business Machines Corporation in the United States, other countries, or both:

AS/400	e-business on demand	OS/400
AS/400e	IBM	i5/OS
eServer	IBM (logo)	
	iSeries	

Rational is a trademark of International Business Machines Corporation and Rational Software Corporation in the United States, other countries, or both.
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.
Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel 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.
SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.
Other company, product or service names may be trademarks or service marks of others.

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

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

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 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.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.