Test drive SSO

How to access multiple systems and services with only one signon!

Tosh Bimbra
Jim Ahrens
Dan Reusche
Dave Robertson

April 22, 2012

This article shows you how to set up Single Sign On (SSO) on the IBM i platform. SSO allows you to sign on to your primary workstation and then access other systems and applications without having to sign on again. You'll learn how to set up all the required software and how to verify each step has completed properly before continuing to the next. Soon you'll be using 5250 Emulation, NetServer, IBM System i Navigator, IBM WebSphere® Application Server and the Java™ Toolbox to access your IBM i system without having to sign on to each. Please note that there are several different components that all have to work together, so the time required to implement SSO will depend on how comfortable you are with each of the components, but generally expect to spend several days.

Prerequisites

Review the Windows-based Single Signon Redbooks title

Although the following RedBook IBM Redbooks® title was published in 2004, we recommend our readers review it in it's entirety before attempting to configure SSO. We found the documentation relevant and extremely useful and we are sure our readers will also.

Windows-based Single Signon and the EIM Framework on the IBM Eserver iSeries Server:

We would like to point out Chapter 2 - Planning for Network Authentication Service and Enterprise Identity Mapping implementation. This chapter is crucial to the successful implementation of SSO. A couple of key points in Chapter 2 are the necessary prerequisite components required and the Planning Worksheet (2.4). Do not underestimate the value of the Planning Worksheet. Appendix D has a blank Planning Worksheet for the reader's use.

Here are two links to planning for single sign-on which contain current information that the RedBook Redbooks title above lacks.

Requirements for configuring a single sign-on environment:

Single sign-on planning worksheets:

Here's the Planning WorkSheet we used, which will assist with the examples and illustrations in this article.

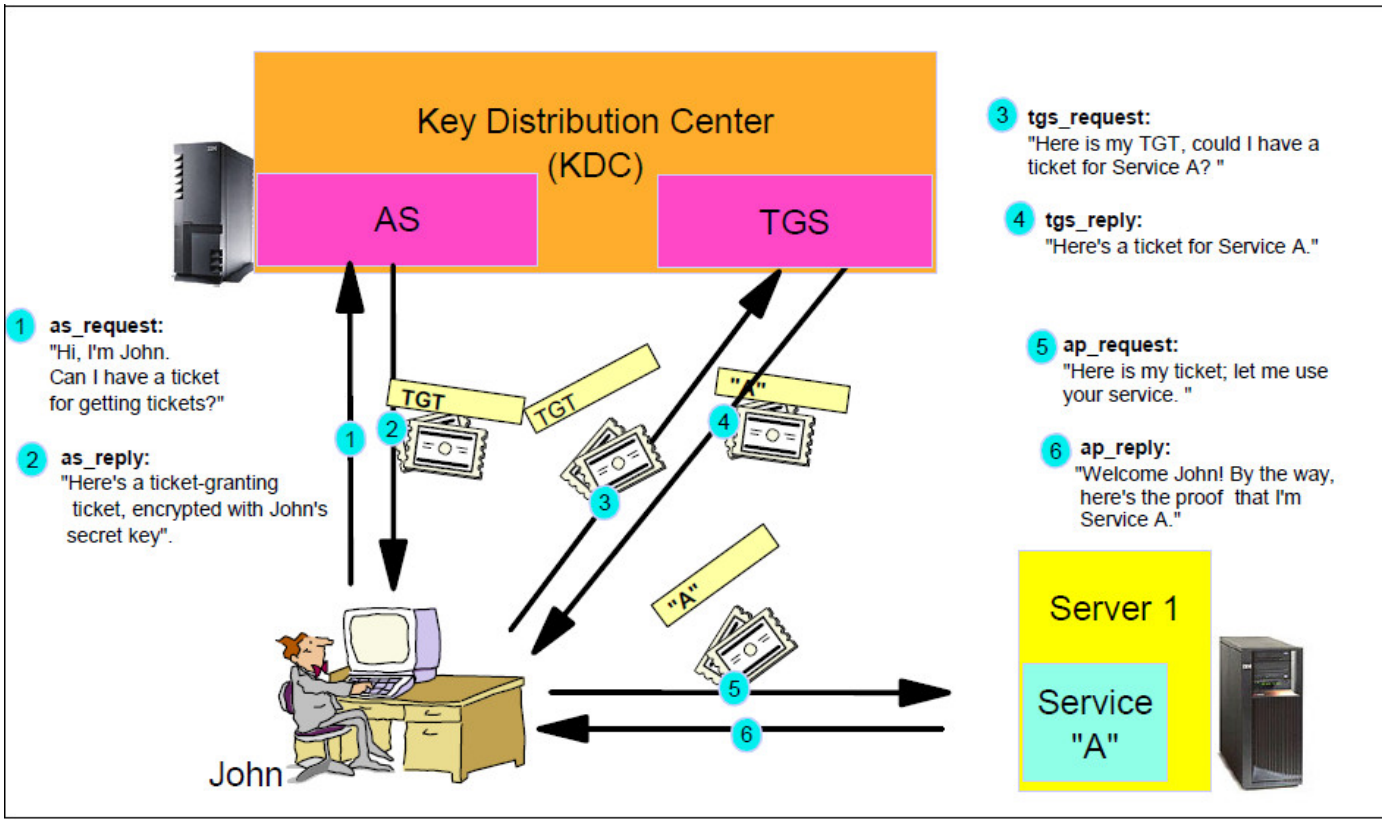
Planning WorkSheet

Item	Planning worksheet	Result
A	What is the name of the Kerberos default realm to which the iSeries will belong?	**RCHPWDI.COM**
B	What is the KDC for this Kerberos default realm?	**toshw2003**
C	What is your KDC's fully qualified host name?	**toshw2003.rchpwdi.com**
D	What is the port on which the KDC listens?	**88** - Default
E	What is name of the password server for this KDC?	Same as B above
F	What is the port of your password server?	**464** - Default
G	Password for your iSeries service principal(s)?	**pwd1sup**
	The following items will be used to create the iSeries principal on the KDC	
H	What is the name of the Kerberos principal?	**krbsvr400** (when creating the iSeries principal this name must be used)
I	What is your iSeries host name?	**rchassmb**
J	What is the fully qualified host name of the iSeries?	**rchassmb.rchland.ibm.com**
K	What is the name of the Kerberos default realm to which the iSeries server belongs? (Default: domain name converted to upper case)	**RCHPWDI.COM**
L	What is the full name of the principal? (krbsvr400/ fully.qualified.host.name@YOUR.KERBEROS.REALM)	**krbsvr400/ rchassmb.rchland.ibm.com@RCHPWDI.COM**
M	What is the password / shared secret for this principal? (Must be the same as item G)	**pwd1sup**
	The following items will be used to configure Enterprise Identity Mapping (EIM)	
N	Which type of basic EIM configuration do you want to create on your IBM i system? Join an existing domain Create and join new domain	**Create and join new domain**
O	Where do you want to configure your EIM domain, or what EIM domain you want to join?	**rchassmb.rchland.ibm.com**
P	What is the name of the EIM domain you want to create or join?	**PWDEIM**
Q	Do you want to specify a parent DN for the EIM domain? If yes - specify the parent DN	**NO**

R	What is the administrator distinguished name (DN) on the LDAP server which will be used as the EIM domain controller?	**cn=administrator**
S	What is the administrator password on the LDAP server will be used as the EIM domain controller?	**pwd1sup**

We also found that Chapter 4.2 - The components of the Kerberos protocol provided (Figure 4-1) which was very helpful illustrating how all the different Kerberos components fit together to perform a Kerberos network solution.

Figure 1. Kerberos Components



Select an Encryption Method

Originally, Kerberos only supported DES and Triple-DES encryption. DES is no longer recommended, so support for the newer encryption types AES128, AES256 and RC4 as well as new KRB5 header files in QSYSINC were added by PTF:

V7R1 SI42919, SI42919

V6R1 SI42957, SI42957

V5R4 SI43034, SI43034

If you intend to use one of the newer encryption methods provided by these PTFs, the batch file created by the NAS Wizard will have to be modified, because it defaults to using DES. See the PTF Cover Letters for details and instructions.

Active Directory

Use these instructions from Microsoft to install and create Active Directory, if it isn't already set up.

How to Install Active Directory on Windows Server 2003

How to Create an Active Directory Server in Windows Server 2003

How to Install Active Directory on Windows Server 2008

If you already have Active Directory set up, check with the Microsoft® Windows® administrator to see if they set up a specific directory structure and a place where they want the Kerberos service accounts to be placed. If so, see the section on Customizing the AD Batch File at the end of the article.

Join a Windows domain from client workstation

Note: This example uses a system running Windows Server 2003 with Active Directory as the Key Distribution Center (KDC) for the Kerberos realm, so client systems used for the initial signon must be capable of joining a Windows domain.

This does **not** mean the client has to be running Windows - we also set up an openSuSE v 11.1 workstation as a primary signon point in the Kerberos realm. YaST, the installation and configuration tool for openSuSE and the SuSE Linux® Enterprise distributions, includes a Kerberos setup wizard. Using that allowed Linux to contact Active Directory at signon time, obtain a ticket granting ticket and access other Kerberos enabled resources such as an HTTP server on the IBM i. We also used the sample Java code included in this article to create a Kerberos enabled JDBC connection to the IBM i. Since each Linux distribution is likely to be different, you may have to search on the internet for articles on configuring yours to participate as a primary workstation in a Kerberos realm.

A Windows domain is a logical group of computers that share a central directory database. This central database is known as Active Directory in Windows 2000 and Windows Server 2003, Active Directory Domain Services in Windows Server 2008 and Server 2008 R2 and NT Directory Services (NTDS) on Windows NT operating systems. It contains the user accounts and security information for the resources in that domain. Each person who uses computers within a domain receives their own unique account, or user name. This account can then be assigned access to resources within the domain.

In a domain, the directory resides on computers that are configured as "domain controllers." A domain controller is a server that manages all security-related aspects between user and domain interactions, centralizing security and administration. A Windows Server domain is generally suited for businesses and/or organizations when more than 10 PCs are in use.

Workstations and servers that want to participate in domain security need to be made domain members. Participating in domain security is often called single sign-on, or SSO for short.

This link describes the process that must be followed to have a workstation join a Windows domain:

Windowsnetworking

Perform IBM i tasks

Lightweight Directory Access Protocol

The LDAP server must support the EIM-required special object classes and attributes, which are part of the IBM Tivoli LDAP server. For example, AD and OpenLDAP do not have these schema extensions.

For our example, we chose to implement on the IBM i.

IBM Tivoli Directory Server for i5/OS (LDAP):

The LDAP server of choice simply needs to be running and accessible at this time. No further configuration is needed.

EIM configuration of your LDAP server will be completed later in the article when you run the EIM Configuration Wizard via System i Navigator.

The Knowledge Base article that discusses the EIM Configuration Wizard shows that the LDAP administrator DN should be specified in the EIM wizard in the screen to enter the LDAP administrator as well as the IBM i EIM system user DN. Although this is very easy to follow and set up, it is certainly a bad practice from a security and management point of view. The LDAP administrator is typically an account (like QSECOFR) where the password should be changed periodically. However, if you used the LDAP Admin as the IBM i EIM system user account and someone changes the LDAP Admin password, EIM stops working and no user can authenticate with Kerberos. It is better, as a preparation task, to set up an extra LDAP user entry for EIM and specify this account during the EIM wizard configuration for EIM system user. That way you can also control through access control lists ACLs the access to various parts of the LDAP directory (in case the customer wants to use the LDAP server for other purposes tool).

Also, starting with IBM V6R1, you can configure multiple instances of the LDAP server. We recommend a separate instance for the EIM domain controller. The LDAP server is a very critical component. If the EIM domain controller is not available, no user can authenticate with SSO. Therefore, splitting off the EIM part into a separate LDAP server is recommended.

An additional availability issue that we recommend is when there is a requirement to implement SSO for more than one IBM i partition. In this case, the first IBM i partition will be the EIM domain controller and the next IBM i partition will join the existing EIM domain on the first IBM i partition. If the first partition goes down, no user can authenticate to the second or other partitions as well. It is

strongly recommended to set up EIM first in the traditional way but then configure LDAP replication and create a replica of the EIM data on every IBM i partition that supports SSO. As soon as the replication is active change the local EIM configuration on each system to point to the own (local) system as the EIM domain controller. That way each partition operates independently from each other.

Network Authentication Service/Enterprise Identity Management

Earlier in this article, we discussed the Planning Worksheet in the EIM Redbook, a sample of which is in Chapter 2, and a blank copy which can be found in Appendix D. If you have properly completed this worksheet, it will be much easier to navigate through the Enterprise Identity Management (EIM) and Network Authentication Services (NAS) wizards, as several of the values in the worksheet will need to be plugged into various screens presented. An excellent resource for configuring EIM and NAS is a Knowledge Base Document that can be found at

http://www-912.ibm.com/s_dir/slkbase.NSF/DocNumber/558590066. Note that this document also contains a copy of the Planning Worksheet. We may sound redundant, but we can't emphasize strongly enough how important it is to use this planning worksheet; it has been the difference between success and failure in many configurations over the years. If you haven't completed the worksheet, you should take time NOW to do so before continuing through the Knowledge Base document. Section 2.4 of the Redbook tells you where to get the information for the worksheet. Also, you should review section 2.2.2 of the Redbooks title, entitled Time/SNTP and make sure your IBM i is communicating with an SNTP server and that it has the correct time zone configured via the QTIMZON system value. (QTIMZON automatically adjusts QUTCOFFSET to the correct value in recent releases of the IBM i).

In step J of the EIM/NAS configuration in the above referenced Knowledge Base Doc, you will use the wizard to create a batch file (.bat) that must be copied to the Active Directory machine and run. The purpose of the .bat file is to run the `ktpass` statement(s) on the Active Directory machine that will set up the service principals that you configured in NAS. This is much easier and less error prone than typing in the `ktpass` commands manually. If the Windows Administrator has already set up a specific directory structure and a place where they want the Kerberos service accounts to be placed, see the section on Customizing the AD Batch File at the end of the article before running it.

There is also a section in the Knowledge Base document about verifying your NAS configuration using the `keytab list` and `kinit -k` commands from QSH. It is VERY important to do this for each service principal that you configured (krbsvr400, http, and so on) and to correct any errors found at this time. Correcting errors might include iteratively running the NAS configuration, making DNS changes, making Active Directory changes, or fixing other issues such as time differences between your IBM i and Active Directory machines. By assuring that NAS has been properly configured at this point, you can eliminate NAS as a problem should you have trouble later in the process. If you do have problems later, you can always come back and rerun the NAS verification to make sure it is correct. The last item in the KB doc is to set up the EIM mappings, which map your IBM i user ID to the user ID that you have set up in Active Directory. Finally, you should check the system value `QRMTSIGN` on your IBM i; this value should be set to `*VERIFY`. If it is set to `*FRCSIGNON`, it will override all of your attempts to configure single sign on and always present a sign on prompt.

During NAS configuration, you may get the following warning screen. It is saying that there is a difference in how the client and the server are resolving the host name. In the example shown, note that there are two different host names listed. We found that although you can proceed with the NAS wizard after getting this error, it is best to go back and resolve the source of the conflict in DNS, or host tables on the client or the server. We encountered an error where we went past the host name conflict screen and the krbsvr400 principals worked correctly, but the HTTP principals could not connect.

Figure 2. NAS Wizard Host Name Conflict

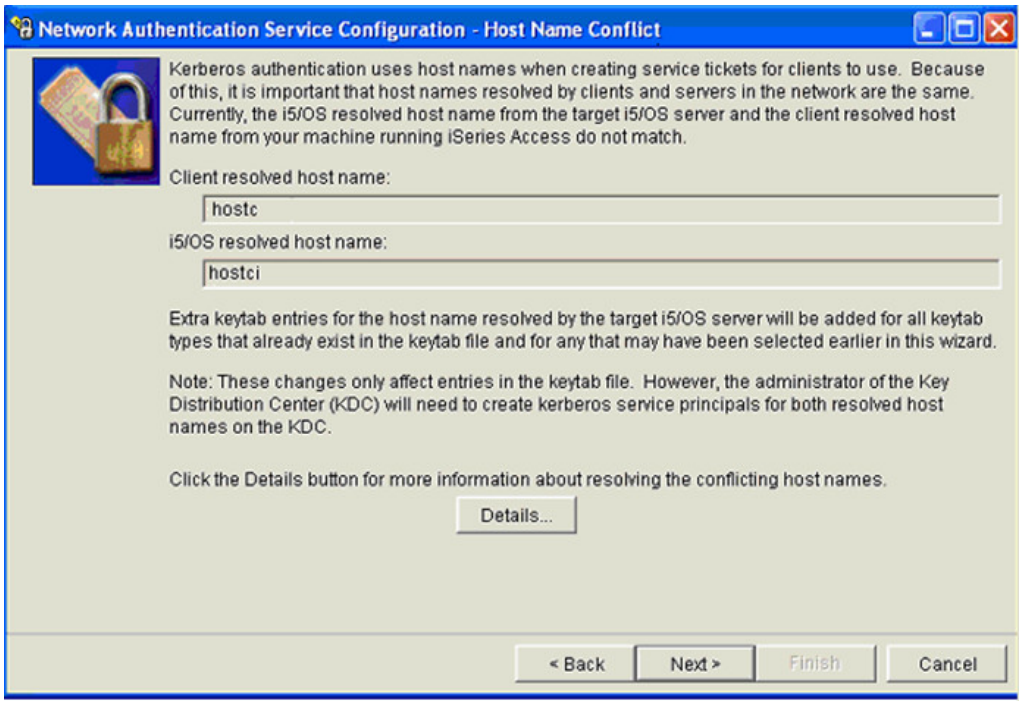


Figure 3. Some common errors when you verify your NAS configuration with kinit -k:

Error	Resolution
EUVF06014E Unable to obtain initial credentials. Status 0x8.8x - s.	In the Network Authentication Services (NAS) options, on the *General* tab, the *Use TCP* option must be checked.
EUVF06014E - other status codes	Other status codes are listed in Appendix B of the Redbook
EUVF06007E Unable to obtain name of default credentials cache	One of the things that can cause this is that the user who is running `kinit` does not have a home directory configured, for example /HOME/userid. `kinit` looks for a file called krb5ccname in that directory which contains the path to the default credentials cache.

Error CWB0999 RC8999 indicates one of three things:

1. DES encryption is not enabled.

2. The kbsvr400 account in Active Directory needs to be reset using the same password that was setup during the Network Authentication Services (NAS) configuration.

3. Verify that AD account is set to 'Use DES Encryption': http://support.microsoft.com/kb/977321

By default, Data Encryption Standard (DES) encryption for Kerberos authentication is disabled in Windows 7 and in Windows Server 2008 R2. This MS Techdoc describes various scenarios in which you may receive the following events in the Application, Security, and System logs because DES encryption is disabled:

•KDCEVENT_UNSUPPORTED_ETYPE_REQUEST_TGS

•KDCEVENT_NO_KEY_INTERSECTION_TGS

Additionally, it explains how to enable DES encryption for Kerberos authentication in Windows 7 and in Windows Server 2008 R2. For detailed information, see the "Symptoms," "Cause," and "Workaround" sections of this Techdoc.

Enabling IBM i applications

SSO 5250 Session

If you're using Windows Server 2003, before attempting to configure a 5250 Emulation session we recommend you install kerbtray. `Kerbtray` is a utility that will display the tickets that have been provided to your PC from the KDC. Here's a link to get the utility. The download (Windows Server 2003 Resource Kit Tools) includes other utilities in addition to `kerbtray`.
Windows Server 2003 Resource Kit Tools:

There is no downloadable Resource Kit for Windows Server 2008. Microsoft states "Unlike previous operating systems, in Windows Server 2008 and Windows Server 2008 R2, the resource kit tools are installed as part of the server role installation. In the past, you had to download the resource kit tools separately.

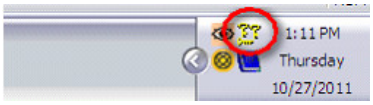
Some tools, such as `kerbtray`, have suitable replacements in the Windows Server 2008 and Windows Server 2008 R2 releases. `Kerbtray` is no longer part of the tool set, but `klist` can be used to complete many of the tasks formerly performed by it."

http://social.technet.microsoft.com/wiki/contents/articles/windows-server-2008-and-windows-server-2008-r2-support-tools-dsforum2wiki.aspx
After installing and invoking `kerbtray` on a Windows PC that is participating in a Kerberos-enabled domain, you will see a green icon in your system tray as follows:

Figure 4. Kerbtray icon

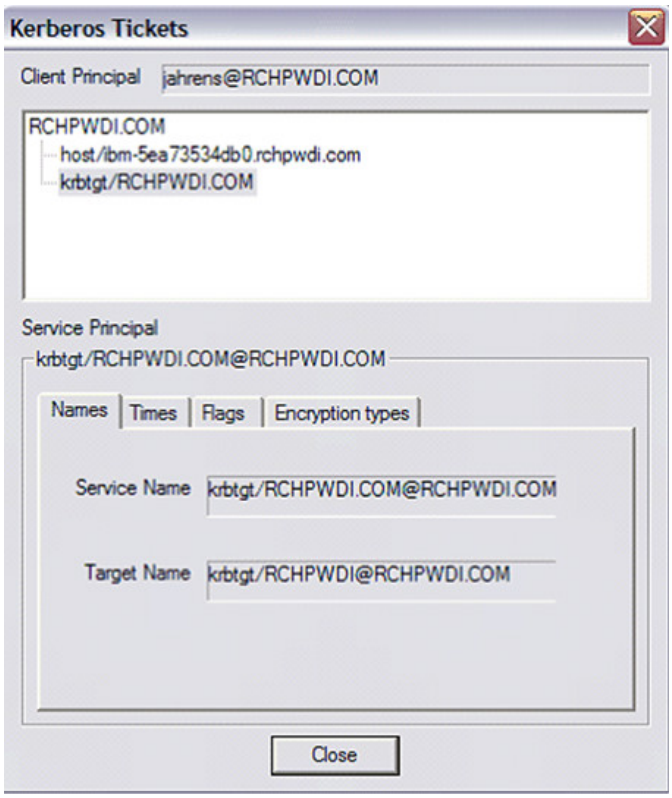
If `kerbtray` is unable to obtain the tickets from the KDC, the icon looks like this:

Figure 5. Kerbtray icon when ticket can’t be obtained



If you right-click and select list tickets, they are shown as illustrated below:

Figure 6. List of Kerberos tickets



You should see the Ticket Granting Ticket. In this case, krbtgt/RCHPWDI.COM

If you don't receive a TGT from the KDC, do NOT go on and try to configure EIM for any application since the TGT is a requirement to continue.

If you're not receiving a TGT, a Wireshark (see Resources) trace would be the most helpful tool to investigate why.

As soon as you have a TGT, follow these steps to configure a 5250 Emulation Session for Kerberos authentication:

Figure 7. Configure 5250 emulation

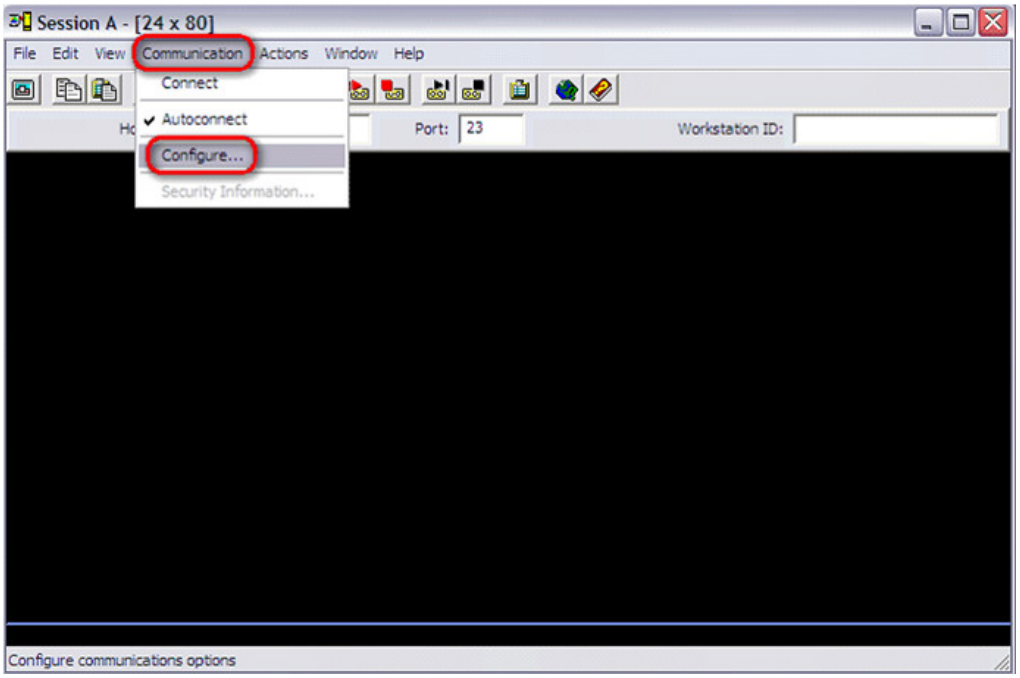


Figure 8. Configuring 5250 emulation properties

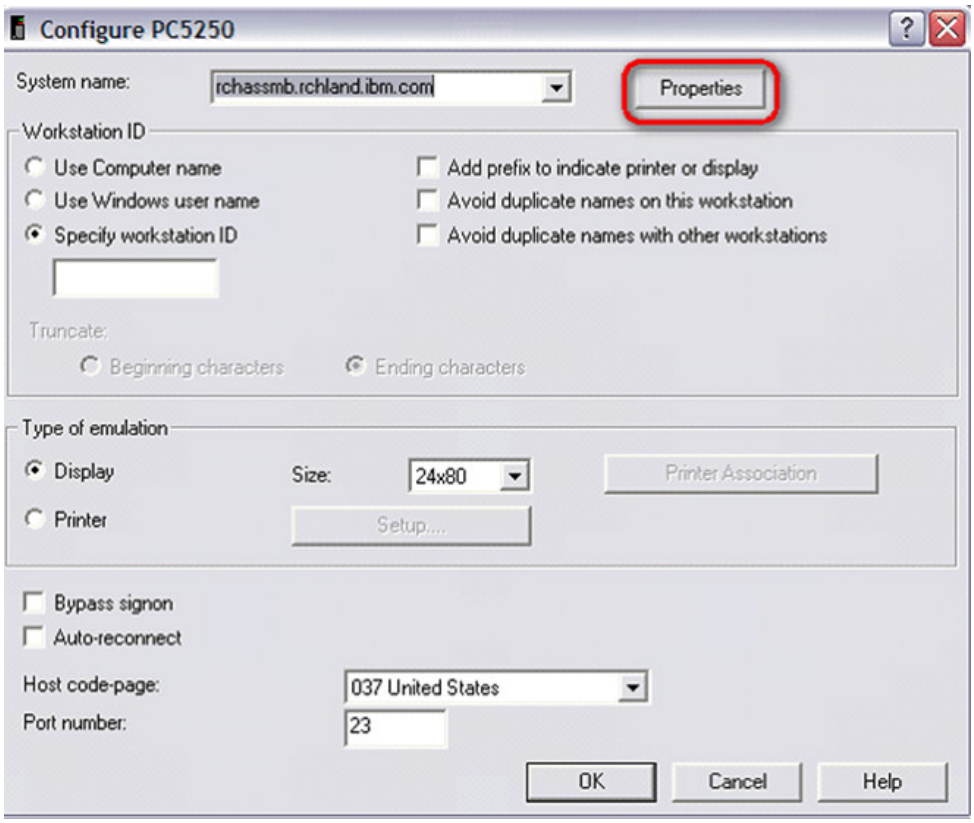
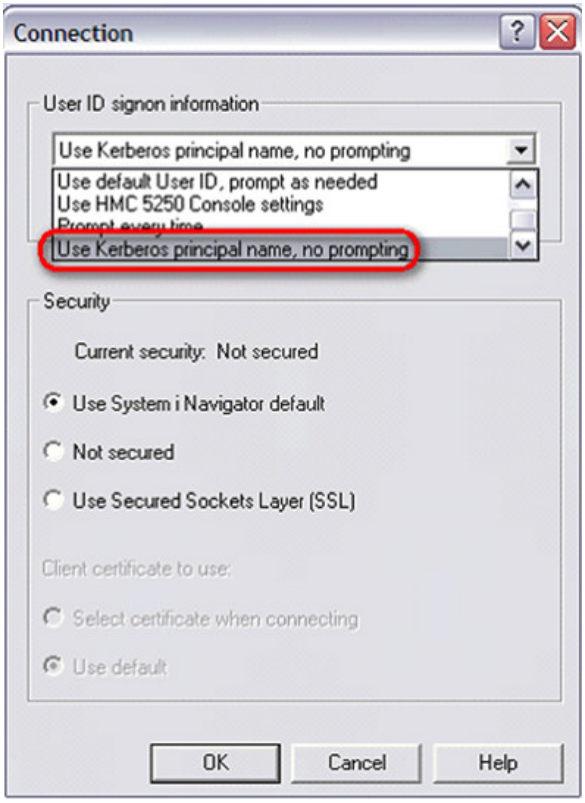


Figure 9. Configuring 5250 emulation signon



If you have further issues, a Wireshark trace is always a good idea. Also, check the event logs on the Domain Controller, AD server and your PC as well as any messages for Kerberos errors in the QZSOSIGN joblog. If the error is coming from IBM System I Access for Windows (they usually have a CWB prefix) you can get further information on the message by doing a Start > Programs > IBM System i Access for Windows > Service > Error and Trace Message Help

SSO NetServer

Enabling i5/OS NetServer support for Kerberos V5 authentication:

SSO iNav

Follow these steps to configure the System i Navigator (iNav) for Kerberos authentication:

Figure 10. Configure System i Navigator

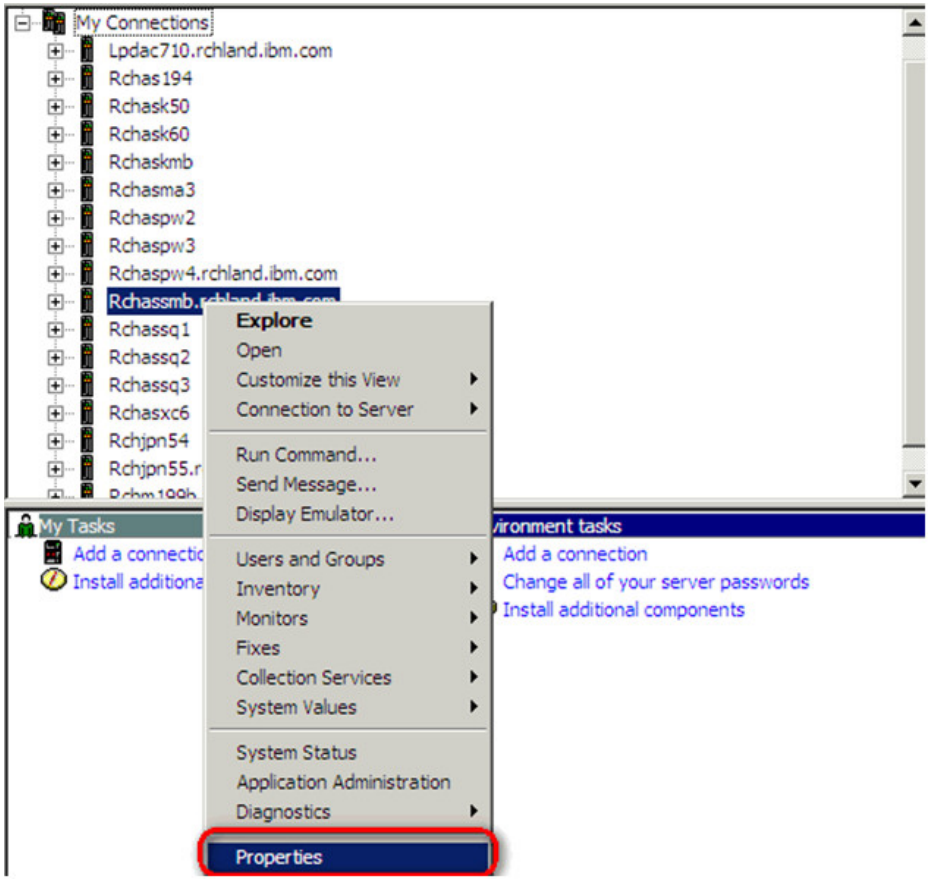
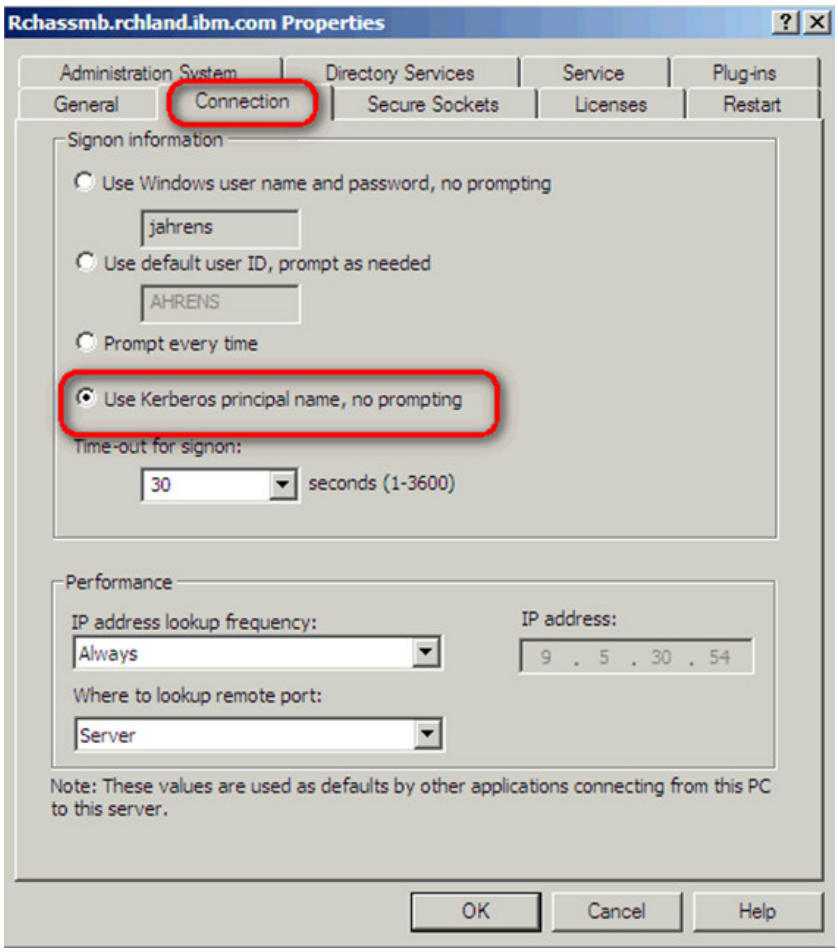


Figure 11. Configuring System i Navigator sign-on



WebSphere V6R1

At this point, EIM is configured and operational. Let's now take SSO to WebSphere. We used WebSphere V6.1 on i5/OS V6R1.

We used the following publication as a guide: *5761-XH2 V6R1 System i Access for Web*

System i Access for Web single sign-on using WebSphere SPNEGO support

Although we were not interested in enabling System i Access for Web single sign-on, the document described what needed to be accomplished for the Windows server and WebSphere.

We started with section 2.5 - Create HTTP service principal and concluded with section 3.4 - Configure SPNEGO TAI

Some items worth noting include a typo on page 19 beginning after the "Create the Kerberos config file used by JGSS: " information. The information refers to a file called "`spnego.krb5.keytab`". This file should be named `spnego.krb5.conf`. The documentation then provides values for that file. Be sure when you populate `spnego.krb5.conf`, the following is on the same line and not on separate lines as illustrated in the documentation.

```
default_keytab_name = FILE:/QIBM/UserData/OS400/NetworkAuthentication/keytab/HTTP_systemName.keytab
```

Our spnego.krb5.conf file is shown here for reference:

```
[libdefaults]
default_realm = RCHPWDI.COM
default_keytab_name =
 FILE:/QIBM/UserData/OS400/NetworkAuthentication/keytab/
 HTTP_rchassmb.keytab
default_tkt_enctypes = des-cbc-md5 rc4-hmac
default_tgs_enctypes = des-cbc-md5 rc4-hmac
kdc_default_options = 0x54800000
[realms]
RCHPWDI.COM = {
kdc = TOSHW2003.RCHPWDI.COM:88
default_domain = rchland.ibm.com
}
[domain_realm]
.rchland.ibm.com = RCHPWDI.COM
```

On page 30 there are instructions to use the Security Configuration Wizard. Security Wizard page 2 illustrates the use of Standalone LDAP registry. That is the selection you want to make whether you're using the Directory Server on i5/OS or not. In this step you want to connect to the LDAP server on Microsoft Active Directory.

We used `Ldp.exe` which is a Windows Support Tool utility you can use to perform Lightweight Directory Access Protocol (LDAP) searches against the Active Directory for specific information given search criteria.

Using `Ldp.exe` to Find Data in the Active Directory:

http://support.microsoft.com/kb/224543

This tool became useful when determining the Base and Bind distinguished name syntax.

You will next want to review section 4.6 - Configure domain account browser settings.

Once you configure WebSphere security, you can use the snoop servlet to validate. If you get challenged for username and password, that indicates SSO is not occurring.

This leads us to debug steps. We found Section 5 useful, specifically section 5.3 - Diagnostic trace settings for SPNEGO component. We found the trace information extremely helpful.

IBM Toolbox for Java

At this point, EIM is configured and operational. Now let's use IBM Java Toolbox to make an SSO connection to DB2 on IBM i V6R1.

We have made sample code available demonstrating using a Kerberos ticket in conjunction with the IBM Toolbox for Java to sign-on to the IBM i. There are two sample methods. The first sample uses the built-in Toolbox code to obtain a Kerberos ticket. The second sample uses JGSS to manually obtain a Kerberos ticket and then pass it to the Toolbox code.

You will need to change the sample code in main() to make it work for you. Specifically, the values for the following three system properties need to be updated to match your environment:

- `java.security.krb5.realm` (Planning Worksheet Item A)

- `java.security.krb5.kdc` (Planning Worksheet Item B)

- `KRB5CCNAME` (Only used in Sample 2)

Additionally, the `AS400()` constructor needs to be updated in both sample methods to use the name of your IBM i system.

Beyond the coding changes needed, the IBM i must already be configured for Kerberos. You will also want the following items in place.

1. On the PC that is running the code and has been added correctly to the Windows Domain, add a `krb5.ini` file to the `C:\WINDOWS` directory.

An example `krb5.ini` file has been added for reference.

Downloadable code: krb5.ini

2. We encountered a situation where Microsoft had restricted an interface to retrieve ticket-granting-ticket/session key pairs from the Kerberos security package. This forced us to change registry value `allowtgtsessionkey` found in `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters`. This is documented here:

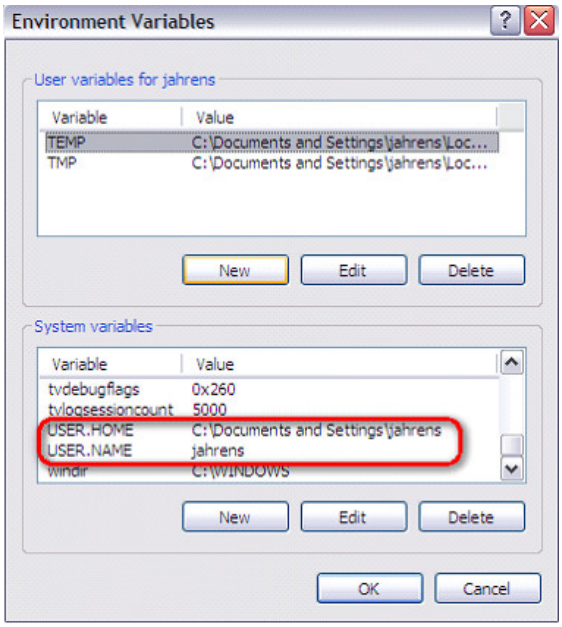
http://support.microsoft.com/kb/308339

3. Create two environment variables on the PC: USER.HOME and USER.NAME.

These are needed by the Java `kinit` command to store the principal credentials in the cache. This is a crucial requirement for running sample 2.

USER.HOME is the directory where `kinit` will place the credential file, with a file name starting with `krb5cc_` and ending with the value of the USER.NAME environment variable. The value for USER.NAME should be entered in lowercase. In the example below, the credential file will be `C:\Documents and Settings\jahrens\krb5cc_jahrens`

Figure 12. Set PC environment variables for Toolbox



4. At this point, we recommend running the `kinit` command on the PC. The `kinit` command is part of the JVM. For example, we used IBM JVM 1.6. In our case, `kinit` was located in C:\Program Files\IBM\Java60\jre\bin

Here's an example of running a successful `kinit` command (You will have to enter the password for the user).

```
C:\Documents and Settings\jahrens>kinit
Password for jahrens@RCHPWDI.COM:

Done!
New ticket is stored in cache file C:\Documents and Settings\jahrens\krb5cc_jahrens
```

If the `kinit` command is not successful, correct the error and run the command again. You will not want to continue until `kinit` completes successfully. To aid in debug, the `kinit` command will use the values found in the `krb5.ini` file found in the `C:\Windows` directory.

NOTE! Sample 2 requires a successful completion of `kinit` before it can be expected to be invoked and run successfully.

5. We were only successful using IBM's JDK/JRE. We were not successful using Sun's JDK/JRE.

The only external dependencies for these samples are the Toolbox/JTOpen jar file (`jt400.jar`) and JGSS (included in JRE 1.4 and higher).

The `jt400.jar` file can be obtained from the (JTOpen) web site, or from the IFS on your IBM i in /QIBM/ProdData/HTTP/Public/jt400/lib/.

Other sample code

Sample code using EIM APIs

The information center contains samples of many of the EIM APIs written in the C language. However, the samples typically include only one function. In reality, you normally have to put several of the functions together in a program to really accomplish something useful with the APIs.

The following is source code that puts a few of the APIs together, ultimately running the eimGetTargetFromSource API, which can be used to map the domain profile used to sign on to a client (the source) to the profile used to sign on to another platform or application (the target). You will see in the example that a number of other APIs must be used together to accomplish this.

Accessing the Windows default credentials cache

If you are writing a Windows-based application that needs to request services from a Kerberos enabled server, you may need to obtain the ticket granting ticket from the default windows credentials cache. The TGT is required on the TGS_request, to obtain a service ticket. The problem that we ran into is that there is a lack of documentation available on exactly how to get to the TGT, which by default on Windows is in a credentials cache in memory and never written to a file. We knew that there had to be a set of functions, but were spinning our wheels trying to find them via Google searches. We arrived at a conclusion, that the `klist` utility from Microsoft must have code in it that would do what we wanted (or close to what we wanted), so we focused our efforts on finding source code for `klist`. We found the source code in the sample source in the Microsoft Windows 7.0 SDK (downloadable from http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=3138) and we were on our way. If you install the Windows 7.0 SDK, the `klist.c` source code is in `C:\Program Files\Microsoft SDKs\Windows\v7.0\Samples\security\authorization\klist`.

Without copying the entire `klist` source code here, we will point out a few key elements of the source.

The function calls that were of special interest to us were:

- LsaConnectUntrusted - returns a logon handle
- LsaLookupAuthenticationPackage - using the logon handle and the name of the buffer to return, it returns a package id
- LsaCallAuthenticationPackage - using the logon handle and the package id returns a buffer of information including the ticket requested

A review of the `klist` source will show how to code these function calls.

The parms we used on the call to `klist` to get the TGT are

`get krbtgt/RCHPWDI.COM`, where RCHPWDI.COM is the name of our default realm.

There are a number of `printf` statements in the GetEncodedTicket function, which calls LsaCallAuthenticationPackage. They parse apart the Ticket structure and present it in pieces. Here is the structure for the ticket as defined by RFC 1510:

```
typedef struct _KERB_EXTERNAL_TICKET {
 PKERB_EXTERNAL_NAME ServiceName;
 PKERB_EXTERNAL_NAME TargetName;
 PKERB_EXTERNAL_NAME ClientName;
 UNICODE_STRING      DomainName;
 UNICODE_STRING      TargetDomainName;
 UNICODE_STRING      AltTargetDomainName;
 KERB_CRYPTO_KEY     SessionKey;
 ULONG               TicketFlags;
 ULONG               Flags;
 LARGE_INTEGER       KeyExpirationTime;
 LARGE_INTEGER       StartTime;
 LARGE_INTEGER       EndTime;
 LARGE_INTEGER       RenewUntil;
 LARGE_INTEGER       TimeSkew;
 ULONG               EncodedTicketSize;
 PUCHAR              EncodedTicket;
} KERB_EXTERNAL_TICKET, *PKERB_EXTERNAL_TICKET
```

Customizing the AD batch file

With regards to the batch file (.bat) that must be copied to the Active Directory machine and run, in some cases the Windows Administrator has already set up a specific directory structure and a place where they want the Kerberos service accounts to be placed. This usually does not correspond with the batch file. Below is an example that will make this point more obvious.

For example, take the following entry in our example batch file (.bat) we generated:

DSADD user cn=rchassmb_1_krbsvr400,cn=users,dc=RCHPWDI,dc=COM -pwd PWD1SUP -display rchassmb_1_krbsvr400

KTPASS -MAPUSER rchassmb_1_krbsvr400 -PRINC krbsvr400/rchassmb.rchland.ibm.com@RCHPWDI.COM -PASS PASSWORD -mapop set +DesOnly -ptype KRB5_NT_PRINCIPAL

In this case, the default location where the new account rchassmb_1_krbsvr400 is created is in this hierarchy:

```
root
     RCHPWDI.COM
        Users
                rchassmb_1_krbsvr400
```

Typically, the Windows Administrators set up a structure that organizes the LDAP entries according to organizational boundaries or other criteria.

For example:

```
root
       RCHPWDI.COM
          IT
                 Operator
                 System Administrators
                 Technical Users
          Rochester
                  Sales
                  Marketing
                  Support
etc.
```

The Windows Administrator then provides the path to the place in the directory where the Kerberos service accounts should be placed.

For example, the Technical Users. In this case, the commands from the previous example would look like:

DSADD user **"**cn=rchassmb_1_krbsvr400,**ou=Technical Users,ou=IT**,dc=RCHPWDI,dc=COM**"** -pwd PWD1SUP -display rchassmb_1_krbsvr400

KTPASS -MAPUSER rchassmb_1_krbsvr400 -PRINC krbsvr400/rchassmb.rchland.ibm.com@RCHPWDI.COM -PASS PASSWORD -mapop set +DesOnly -ptype KRB5_NT_PRINCIPAL

This always requires editing the batch file manually after the NAS wizard creates the file.

Resources

IBM Lab Services

We would like to thank Lab Services for providing the core coding techniques to implement EIM using the IBM Java Toolbox. Lab Services is available to assist with all your IBM i needs, including EIM configuration.

IBM Systems Lab Services and Training helps infuse intelligence in the way the world's information technology works. They focus on driving down costs by designing flexible infrastructures while at the same time managing risk through the use of deep technical skills and training expertise.

They can help optimize the utilization of data centers and system solutions. They are focused on new technologies emerging from IBM product development labs and delivery and training of new and important niche, mature and end-of-life market technologies.

They collaborate with other IBM service organizations such as Global Technology Services, Global Business Services, Sales & Distribution, Software Group and IBM Business Partners. For more information, visit their website at www.ibm.com/systems/services/labservices or contact them at stgls@us.ibm.com .

Lab services Offerings/Tools:

- EIM Populator Tool

- EIM management Tool
- Exit programs for automatic EIM identifier creation and deletion
- Consulting services for SSO implementation

Wireshark

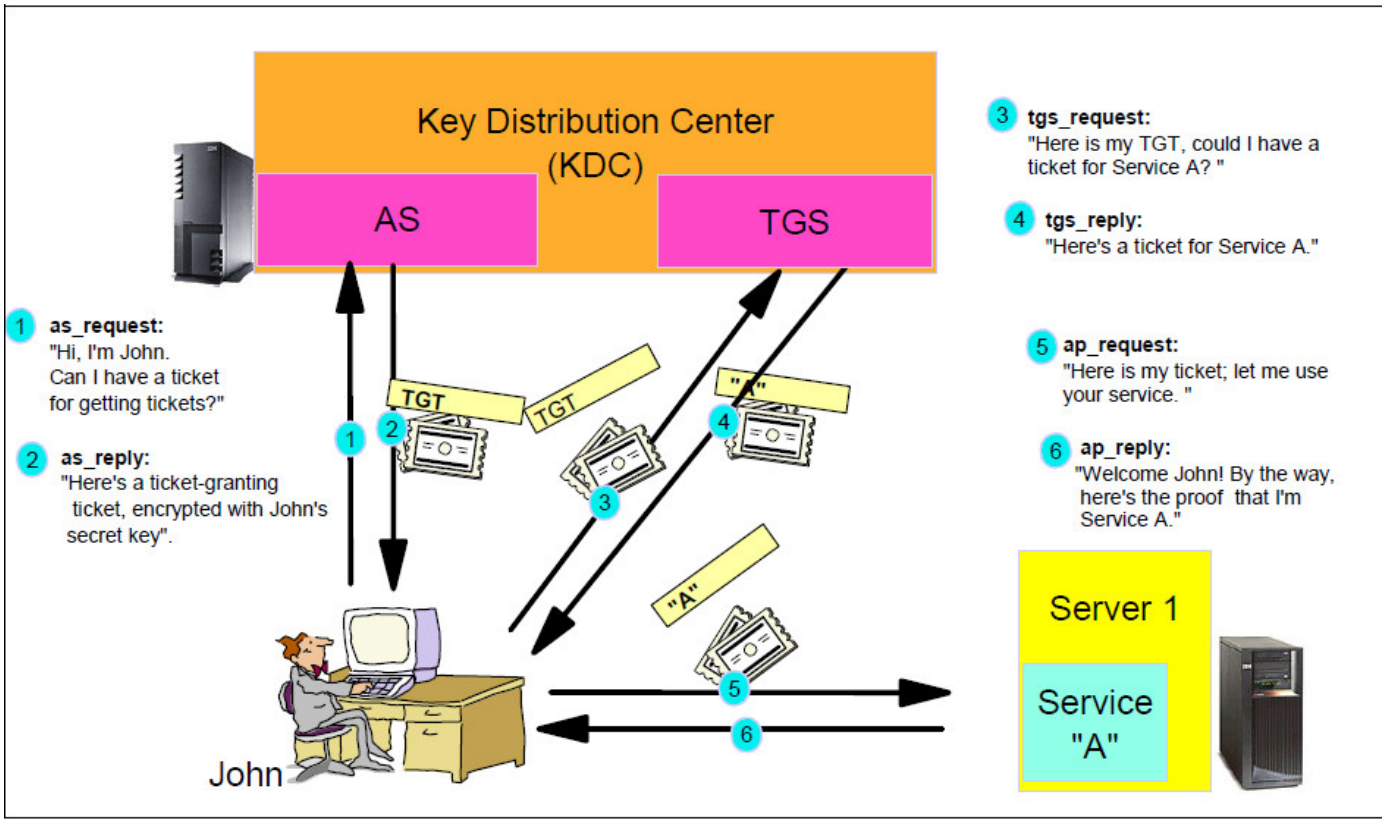
Examining the actual data sent and received across the network allows you to verify your setup is correct and you're getting tickets, not errors. Wireshark allows you to do just that, and we used it many times. It's open source and can be downloaded from:

wireshark download

Setup and operating instructions:
wireshark CaptureSetup

When reviewing a Wireshark trace, understanding the following flow will be crucial.

Figure 13. Kerberos Data Flow



Summary

This article showed you how to set up Single Sign On (SSO) on the IBM i platform and SSO enable common applications such as 5250 emulation, iSeries Navigator, WebSphere Application Server and the Toolbox for Java. Now users can sign on to their primary workstation, then access

other systems and applications without having to sign on again. Although there are several different components that have to work cooperatively, you saw how to verify each one was functioning correctly before adding the next.

Downloadable resources

Description	Name	Size
Let the Java Toolbox handle the GSS credential	KerberosSample1.java	7.0KB
Using your own GSS credential in Java	KerberosSample2.java	5.0KB
Coding the eimGetTargetFromSource API in C	EIM_APIs.txt	5.0KB