OS/390 Security Server (RACF) Interoperability with Windows 2000 Case Studies

Paul de Graaff
Field Technical Sales Specialist
E-Mail : graaff@us.ibm.com

February 28 2001 - Session Number 1732
The Westin Hotel

Agenda

OS/390 Network Authentication Service Introduction

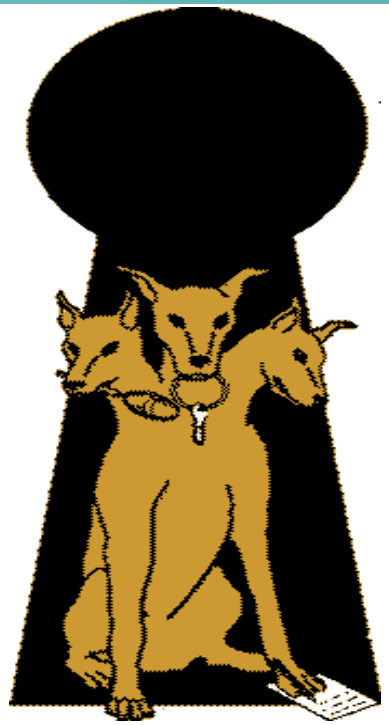
OS/390 Network Authentication Service Server Setup

- Testing the environment

Windows 2000 Setup

- Active Directory
- DNS

Greek Mythology



Kerberos (Cerberus) was the mythological three-headed dog that guarded the entrance to the underworld. Unless you could get past Kerberos, you could not enter (or leave!) the underworld

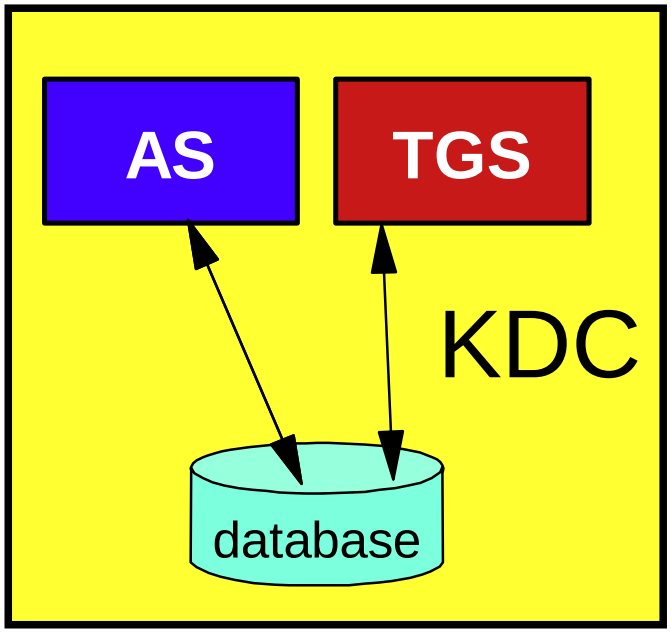
Network Authentication and Services Overview

Who will use the Network Authentication Service?

- Customers with network-based applications that use Kerberos authentication
- IBM products such as DB2 V7 and WebSphere V4

Key Distribution Center (KDC)

KDC - Key Distribution Center
Database - Contains secret keys of each user and each

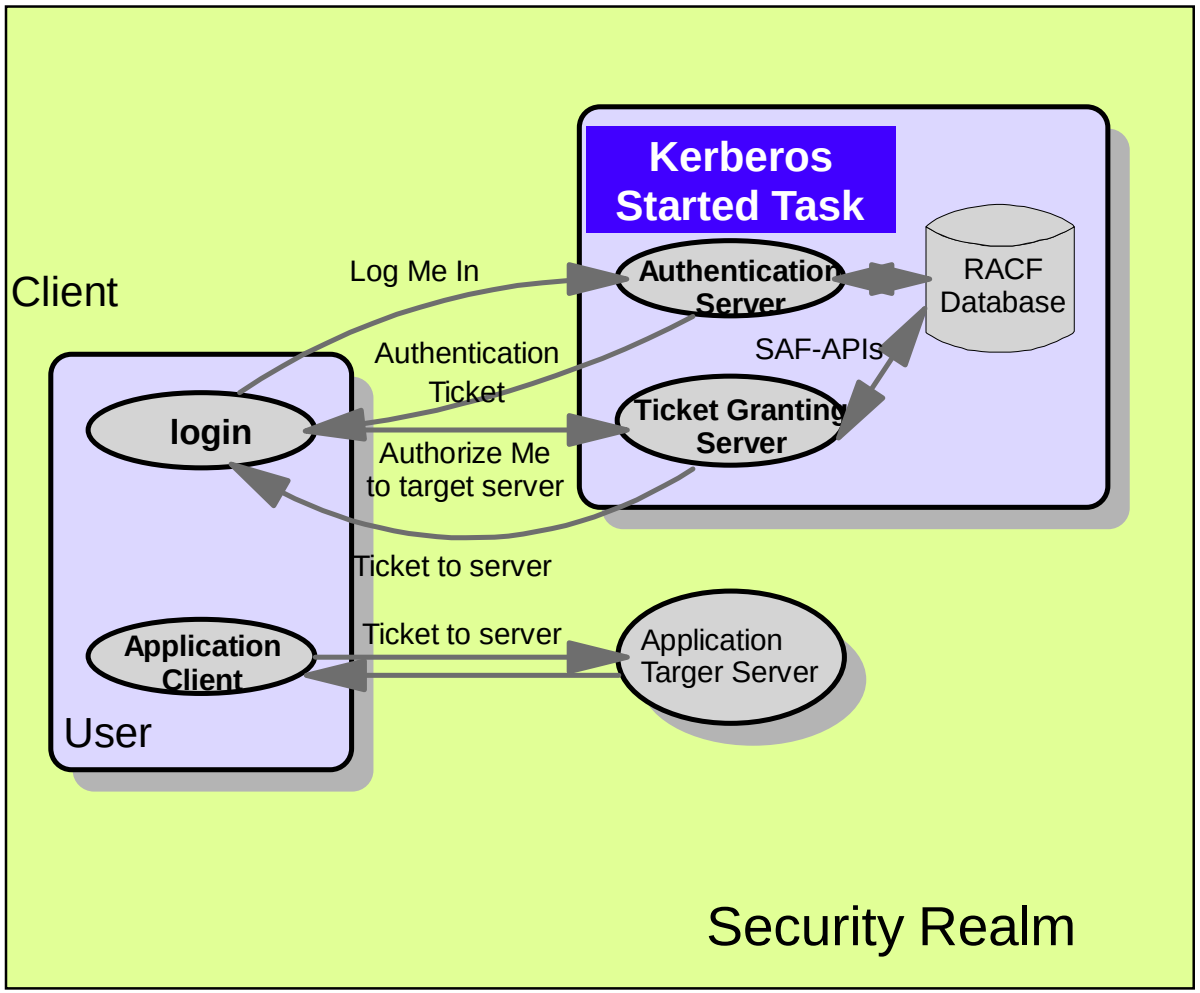


Kerberos on OS/390

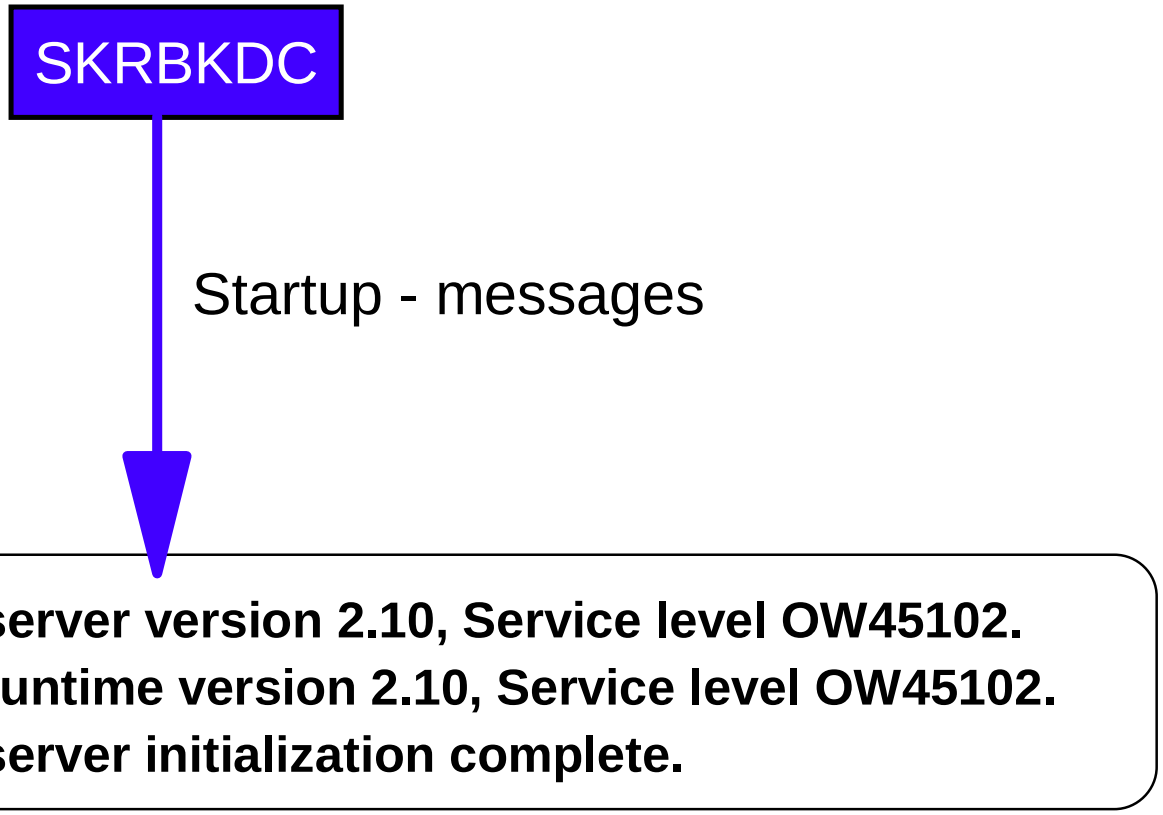
S/390 Kerberos is integrated with RACF

- Kerberos database is kept in RACF
- All administration is done through RACF
  - Define Kerberos users
  - Define passwords

Kerberos on OS/390 ....



OS/390 Kerberos Server Startup



OS/390 Kerberos - Installation

Kerberos product is installed in HFS

- /usr/lpp/skrb

System dataset changes

- Add EUVF.SEUVFLPA to LPALST
- Add EUVF.SEUVFLNK to LNKLST
- Add EUVF.SEUVFEXC to SYSEXEC DD concatenation for TSO

OS/390 Kerberos Installation ...

HFS directories needed

- /etc/skrb
- /etc/skrb/home
- /etc/skrb/home/kdc
- /var/skrb

chmod all above to 755

- /var/skrb/creds

chmod /var/skrb/creds 777

OS/390 Kerberos Installation ...

1. Set-up RRSF(RACF Remote Sharing) in local mode
2. Create SKRBKDC userid (for the Started Task)
3. Activate APPL class if not already active
4. Define SKRBKDC application
5. Set universal access to READ (if applicable)
6. Refresh APPL class

OS/390 Kerberos Installation ...

7. Define SKRBKDC started task and associate it with SKRBKDC userid
8. Refresh STARTED class
9. Copy SKRBKDC started task procedure from EUVF.SEUVFSAM to SYS1.PROCLIB
10. Copy SKRBKDC environment var. definitions to /etc/skrb/home/kdc/envar
11. Set TZ and RESOLVER_CONFIG for your installation

OS/390 Kerberos Configuration

The krb5.conf file - found by env. var. KRB5_CONFIG

- default is /etc/skrb/krb5.conf

sample in /usr/lpp/skrb/examples/krb5.conf

- permissions should be read for everyone, only administrator may modify
- modified only in code page 1047

OS/390 Kerberos Server Configuration

/etc/skrb/krb5.conf

```
Ýlibdefaults¨

default_realm = KRB390.IBM.COM
kdc_default_options = 0x40000010
use_dns_lookup = 0

Ýrealms¨

KRB390.IBM.COM = {
   kdc = wtsc57.krb390.ibm.com:88
}

KRB2000.IBM.COM = {
   kdc = tot16.itso.ibm.com:88
```

SKRBKDC

/etc/skrb/home/kdc/envar

```
SKDC_DATABASE=SAF
SKDC_PORT=88
SKDC_KPASSWD_PORT=464
SKDC_NETWORK_THREADS=15
SKDC_LOCAL_THREADS=15
SKDC_LOGIN_AUDIT=FAILURE
```

omvs(home(/etc/skrb/home/kdc))

OS/390 Kerberos Registry

RACF commands/panels are used for Kerberos administration

Local Kerberos principals are defined as RACF users with a KERB segment

Example :

adduser graaff kerb(kerbname(paul/wtsc57.itso.ibm.com))

Kerberos Registry Support ...

The RACF user password and the Kerberos local principal's password are integrated using RRSF in local mode

Kerberos keys will be generated whenever the user's password changes:

- application logon (TSO, CICS etc.)
- ALU NOEXPIRE
- PASSWORD command

The Kerberos password is subject to RACF SETROPTS rules

Both current and previous key are stored, supporting key versioning

Kerberos Registry Support ...

When the initial KERB segment is added, the RACF password is not yet synchronized with the Kerberos local principal's password:

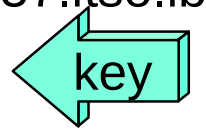
USER=GRAAFF
KERB INFORMATION

KERBNAME= paul/wtsc57.itso.ibm.com

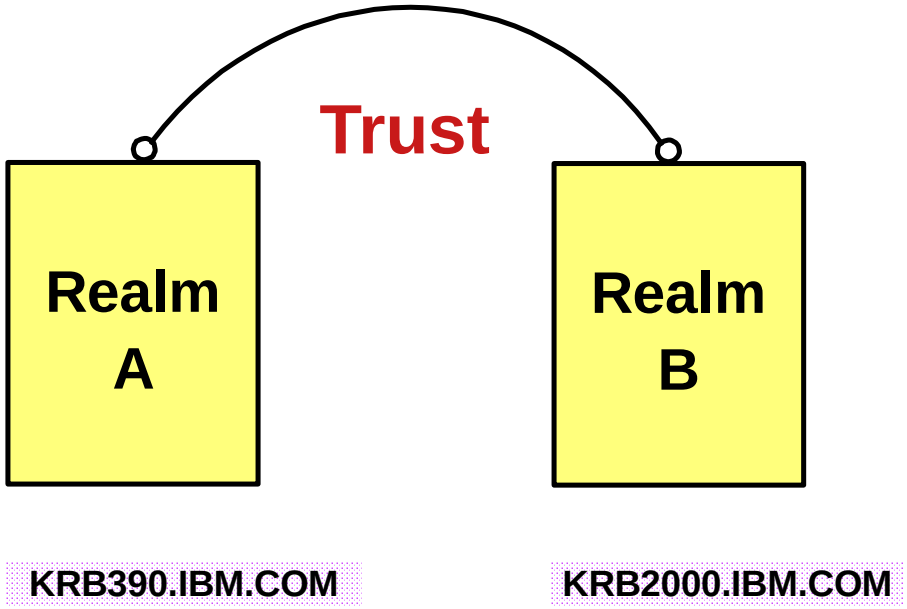
it requires a password change, and key is generated !

USER=GRAAFF
KERB INFORMATION

KERBNAME= paul/wtsc57.itso.ibm.com
KEY VERSION= 001



Realms and trust Relationships



Commands must be entered to define:

A local realm (OS/390)
Inter-realm trust relationships (between OS/390 and Win2K)
Local and foreign principals

Realm and Trust Relationships ...

REALM class profiles are used to define information about the local Kerberos realm and foreign realms

Local realm information includes name, key, and ticket lifetime (MIN, MAX, and DEFAULT in seconds)

Local Realm example:

RDEFINE REALM KERBDFLT
KERB(KERBNAME(**KRB390.IBM.COM**)
PASSWORD(xxxx) MINTKTLFE(15) DEFTKTLFE(36000)
MAXTKTLFE(86400))

Realm and Trust Relationships ...

Foreign realm trust relationships are defined in pairs (A to B and B to A) which also include a key

RDEFINE REALM /.../KRB390.IBM.COM/krbtgt/KRB2000.IBM.COM KERB(PASSWORD(password))

RDEFINE REALM /.../KRB2000.IBM.COM/krbtgt/KRB390.IBM.COM

KERB(PASSWORD(password))

Realm and Trust Relationships ...

Foreign Kerberos principals are mapped to a RACF identity using KERBLINK class profiles

- RDEFINE KERBLINK /.../foreign_realm/foreign_principal APPLDATA('racf_user')

  Maps single foreign principal to a RACF userid

- RDEFINE KERBLINK /.../foreign_realm/ APPLDATA('racf_user')

  Maps all principals for a single realm to a RACF userid

Realm names are rolled to upper case

RACF SETROPTS

Special case logic added to prevent the explicit or implicit activation of generic profile checking and generic command processing for the KERBLINK and REALM classes

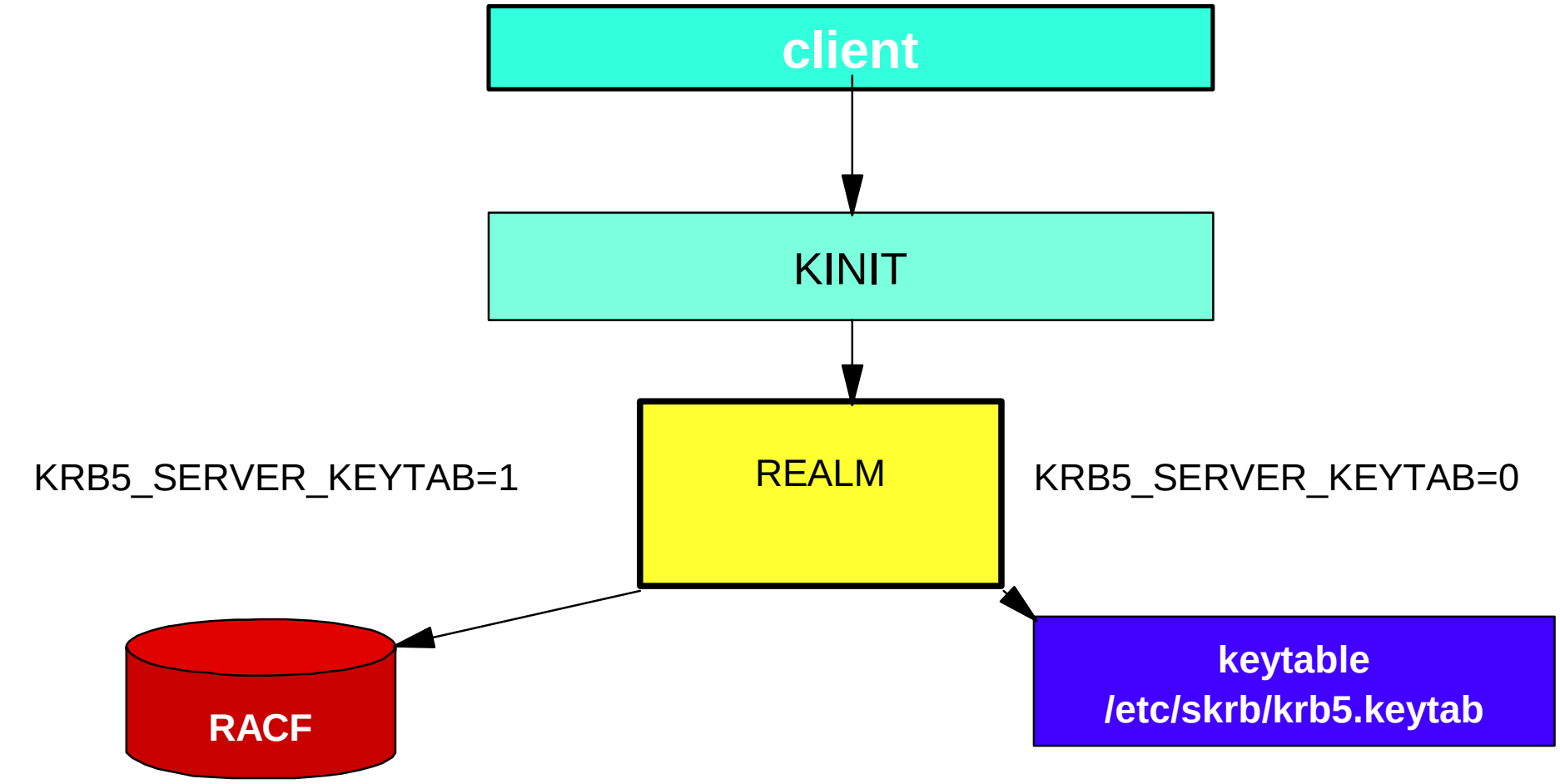
SETR GENERIC(KERBLINK REALM) GENCMD(KERBLINK REALM) will result in a new message

SETR GENERIC(*) GENCMD(*) will **ignore** the KERBLINK and REALM classes

Test the OS/390 Setup

User ID GRAAFF	User ID TESTDEL	User ID TESTSRV
Kerbname Paul	Kerbname test_delegate	Kerbname test_server
Realm krb390.ibm.com	Realm krb390.ibm.com	Realm krb390.ibm.com
skrbgss_client	skrbgss_delegate	skrbgss_server

OS/390 Kerberos - Keytab ?



User/application needs read access to IRR.RUSERMAP

Test the OS/390 Setup .... Message at Client


```
RAAFF @ SC57:/u/graaff/kerberos>kinit -s
RAAFF @ SC57:/u/graaff/kerberos>klist
Ticket cache: FILE:/var/skrb/creds/krbcred_a9b31900
Default principal: paul/wtsc57.itso.ibm.com@KRB390.IBM.COM

erver: krbtgt/KRB390.IBM.COM@KRB390.IBM.COM
 Valid 2001/02/26-23:48:16 to 2001/02/27-09:48:16
RAAFF @ SC57:/u/graaff/kerberos>skrbgss_client wtsc57.itso.ibm.com 63034
krbgss_client: GSS-API client starting
krbgss_client: Initiator credential mechanism 1: KRBV5_DES_RFC
krbgss_client: Initiator credential mechanism 2: KRBV5_DES_BETA
krbgss_client: KRBV5_DES_RFC mechanism, Mutual auth FALSE, Seq check FALSE
krbgss_client: Signature QOP=0
krbgss_client: Wrapped message QOP=0
krbgss_client: Server reply: Server greetings at Mon Feb 26 23:51:36 2001
```

Test the OS/390 Setup .... Message at the Delegate

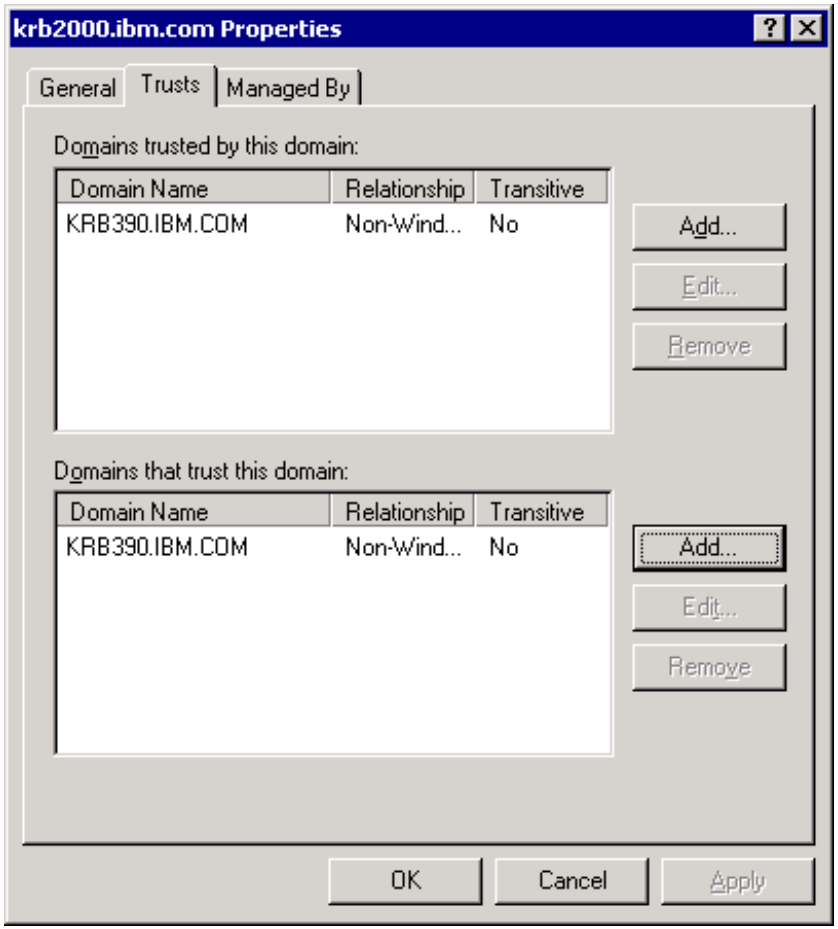

```
ESTDEL @ SC57:/u/graaff/kerberos>KRB5_SERVER_KEYTAB=1
ESTDEL @ SC57:/u/graaff/kerberos>export KRB5_SERVER_KEYTAB
ESTDEL @ SC57:/u/graaff/kerberos>skrbgss_delegate wtsc57.itso.ibm.com 63033
krbgss_delegate: GSS-API delegate starting
krbgss_delegate: Local host is wtsc57.itso.ibm.com
krbgss_delegate: Server host is wtsc57.itso.ibm.com
krbgss_delegate: Acceptor credential mechanism 1: KRBV5_DES_RFC
krbgss_delegate: Acceptor credential mechanism 2: KRBV5_DES_BETA
krbgss_delegate: Listening for requests on port 63034
krbgss_delegate: Connection received from 9.12.14.247Ý63035¨
krbgss_delegate: GSS context 1 established
   Context lifetime=35800 seconds, Context flags=000000b1
   Context mechanism=KRBV5_DES_RFC
   Mutual authentication not required
   Context initiator=paul/wtsc57.itso.ibm.com@KRB390.IBM.COM
```

Test the OS/390 Setup .... Message at the Server


```
ESTSRV @ SC57:/u/graaff/kerberos>KRB5_SERVER_KEYTAB=1
ESTSRV @ SC57:/u/graaff/kerberos>export KRB5_SERVER_KEYTAB
ESTSRV @ SC57:/u/graaff/kerberos>skrbgss_server
krbgss_server: GSS-API server starting
krbgss_server: Local host is wtsc57.itso.ibm.com
krbgss_server: Acceptor credential mechanism 1: KRBV5_DES_RFC
krbgss_server: Acceptor credential mechanism 2: KRBV5_DES_BETA
krbgss_server: Listening for requests on port 63033
krbgss_server: Connection received from 9.12.14.247Ý63036¨
krbgss_server: GSS context 1 established
   Context lifetime=35800 seconds, Context flags=000000b0
   Context mechanism=KRBV5_DES_RFC
   Context initiator=paul/wtsc57.itso.ibm.com@KRB390.IBM.COM
   Client says: Greetings from a devoted follower
   Client greeting is encrypted
```

Windows 2000 Setup

Realm and Trust Relationships ...



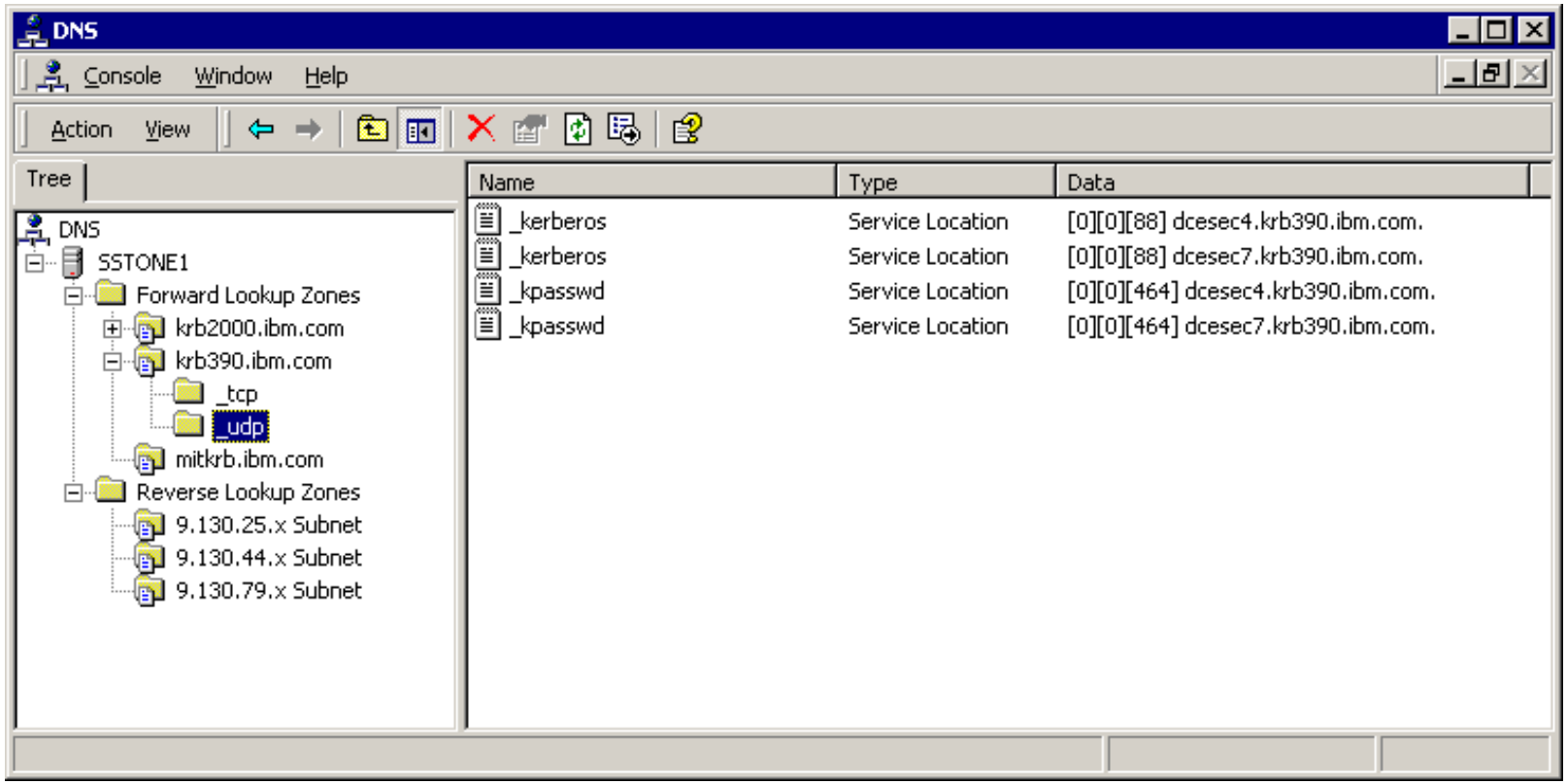
Windows 2000 Domain Controller Settings for trusted domains

DNS updates

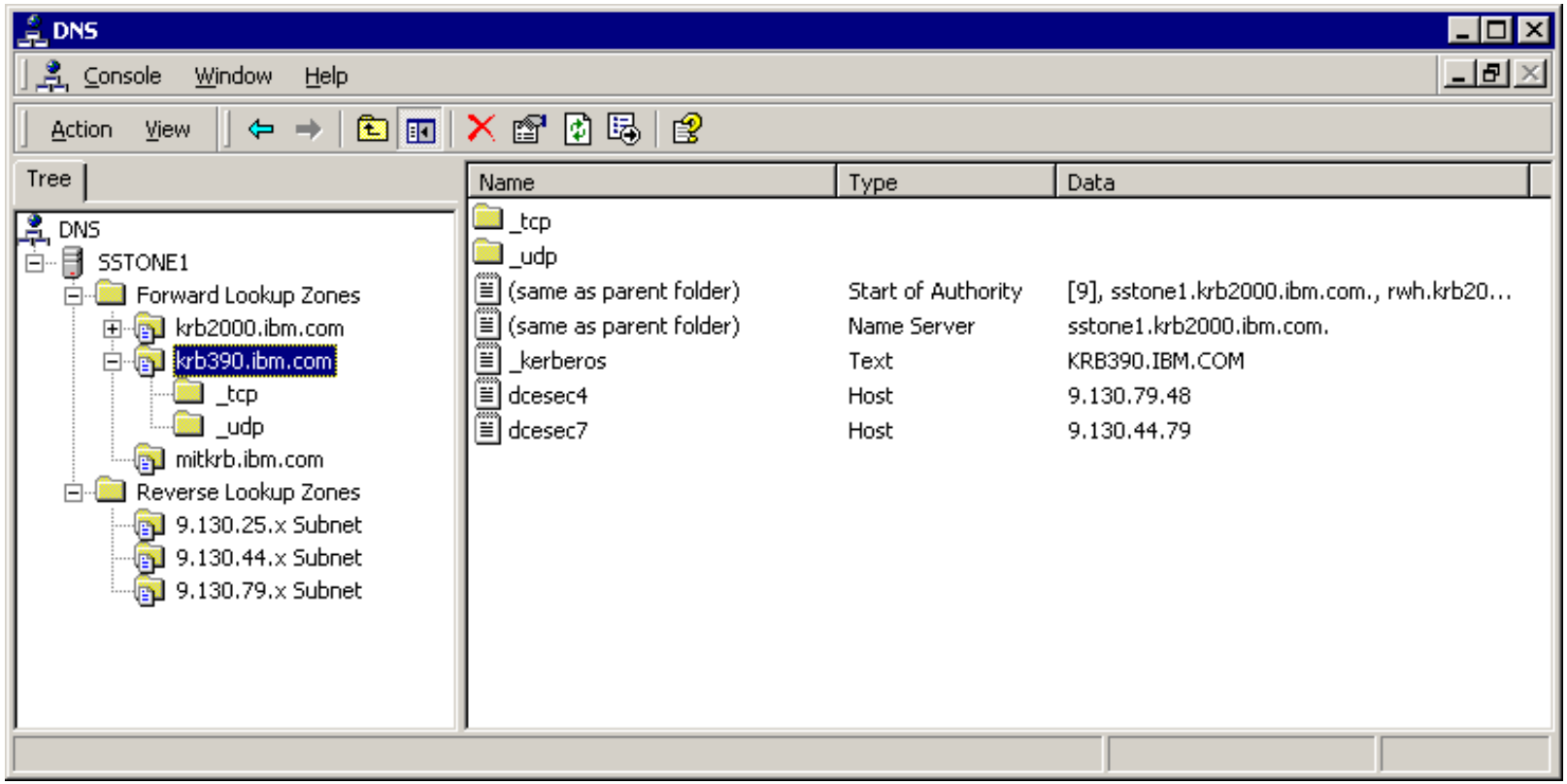
add SRV records for the _kpasswd and _kerberos service using TCP and UDP entries for the KRB390.IBM.COM (Your Domain)

Create a TXT record to map host names in the krb390.ibm.com DNS domain to the KRB390.IBM.COM Kerberos realm

DNS Updates ....

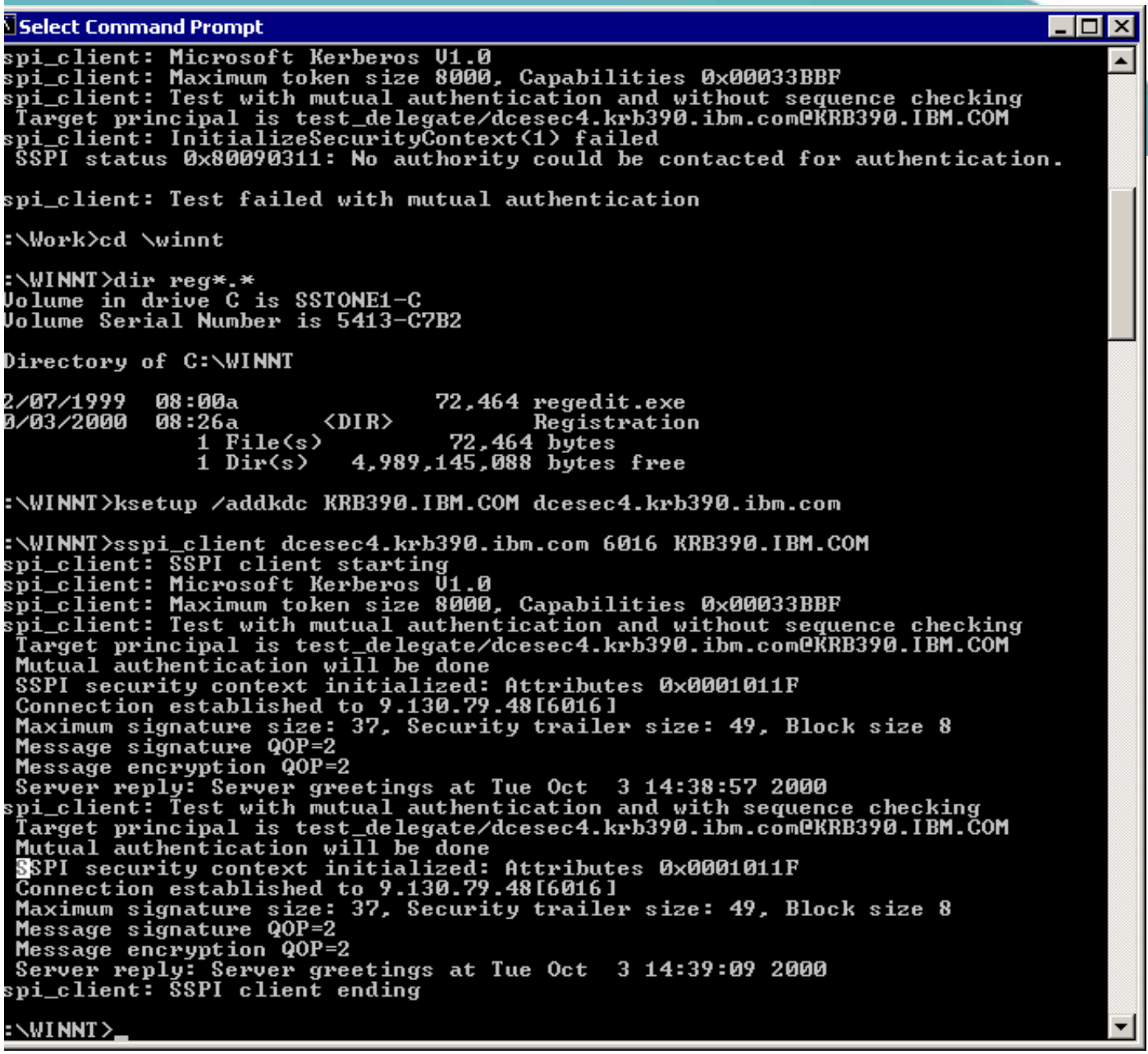

DNS
Console
Window
Help
Action
View
Tree
DNS
SSTONE1
Forward Lookup Zones
krb2000.ibm.com
krb390.ibm.com
_tcp
_udp
mitkrb.ibm.com
Reverse Lookup Zones
9.130.25.x Subnet
9.130.44.x Subnet
9.130.79.x Subnet
Name
Type
Data
_kerberos
Service Location
[0][0][88] dcesec4.krb390.ibm.com.
_kerberos
Service Location
[0][0][88] dcesec7.krb390.ibm.com.
_kpasswd
Service Location
[0][0][464] dcesec4.krb390.ibm.com.
_kpasswd
Service Location
[0][0][464] dcesec7.krb390.ibm.com.

DNS Updates ....


DNS
Console
Window
Help
Action
View
Tree
DNS
SSTONE1
Forward Lookup Zones
krb2000.ibm.com
krb390.ibm.com
_tcp
_udp
mitkrb.ibm.com
Reverse Lookup Zones
9.130.25.x Subnet
9.130.44.x Subnet
9.130.79.x Subnet
Name
Type
Data
_tcp
_udp
(same as parent folder)
Start of Authority
[9], sstone1.krb2000.ibm.com., rwh.krb20...
(same as parent folder)
Name Server
sstone1.krb2000.ibm.com.
_kerberos
Text
KRB390.IBM.COM
dcesec4
Host
9.130.79.48
dcesec7
Host
9.130.44.79

Test the OS/390-WIN2K Setup

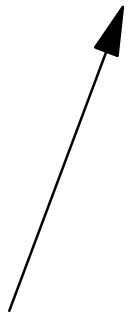
Client	Delegate	Server
User ID GRAAFF	User ID TESTDEL	User ID TESTSRV
Windows 2000	Kerbname test_delegate	Kerbname test_server
Realm krb390.ibm.com	Realm krb390.ibm.com	Realm krb390.ibm.com
sspi_client	skrbgss_delegate	skrbgss_server

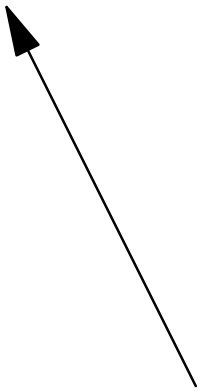

Select Command Prompt
spi_client: Microsoft Kerberos V1.0
spi_client: Maximum token size 8000, Capabilities 0x00033BBF
spi_client: Test with mutual authentication and without sequence checking
Target principal is test_delegate/dcesec4.krb390.ibm.com@KRB390.IBM.COM
spi_client: InitializeSecurityContext(1) failed
SSPI status 0x80090311: No authority could be contacted for authentication.
spi_client: Test failed with mutual authentication
:\Work>cd \winnt
:\WINNT>dir reg*.*
Volume in drive C is SSTONE1-C
Volume Serial Number is 5413-C7B2
Directory of C:\WINNT
2/07/1999 08:00a 72,464 regedit.exe
0/03/2000 08:26a <DIR> Registration
1 File(s) 72,464 bytes
1 Dir(s) 4,989,145,088 bytes free
:\WINNT>ksetup /addkdc KRB390.IBM.COM dcesec4.krb390.ibm.com
:\WINNT>sspi_client dcesec4.krb390.ibm.com 6016 KRB390.IBM.COM
spi_client: SSPI client starting
spi_client: Microsoft Kerberos V1.0
spi_client: Maximum token size 8000, Capabilities 0x00033BBF
spi_client: Test with mutual authentication and without sequence checking
Target principal is test_delegate/dcesec4.krb390.ibm.com@KRB390.IBM.COM
Mutual authentication will be done
SSPI security context initialized: Attributes 0x0001011F
Connection established to 9.130.79.48[6016]
Maximum signature size: 37, Security trailer size: 49, Block size 8
Message signature QOP=2
Message encryption QOP=2
Server reply: Server greetings at Tue Oct 3 14:38:57 2000
spi_client: Test with mutual authentication and with sequence checking
Target principal is test_delegate/dcesec4.krb390.ibm.com@KRB390.IBM.COM
Mutual authentication will be done
SSPI security context initialized: Attributes 0x0001011F
Connection established to 9.130.79.48[6016]
Maximum signature size: 37, Security trailer size: 49, Block size 8
Message signature QOP=2
Message encryption QOP=2
Server reply: Server greetings at Tue Oct 3 14:39:09 2000
spi_client: SSPI client ending
:\WINNT>

Realms

Any WIN2K workstation that wants to participate in the realm will need to add the KDC :

ksetup /addkdc KRB390.IBM.COM wtsc57.itso.ibm.com



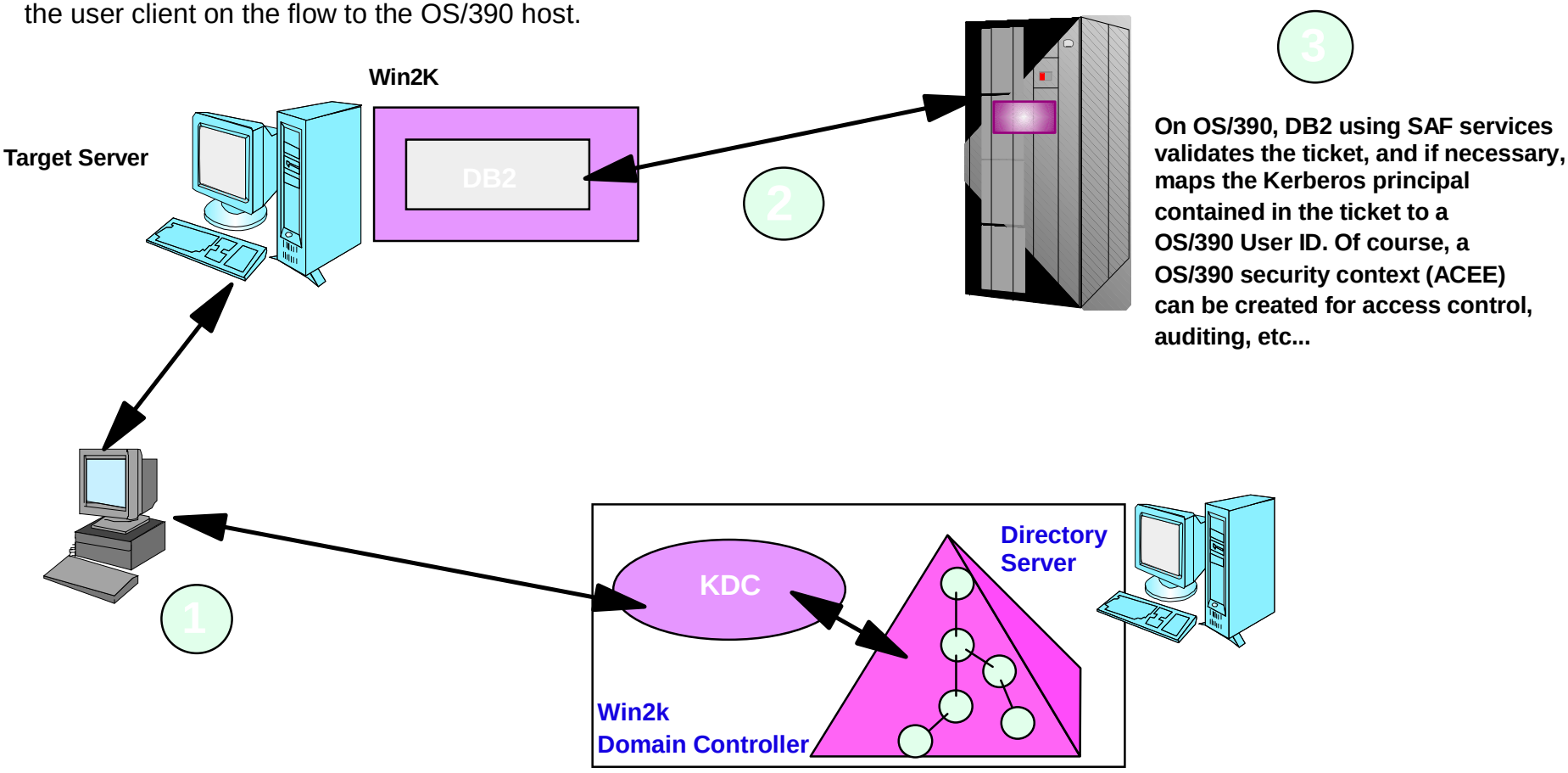


390 Realm

390 Domain

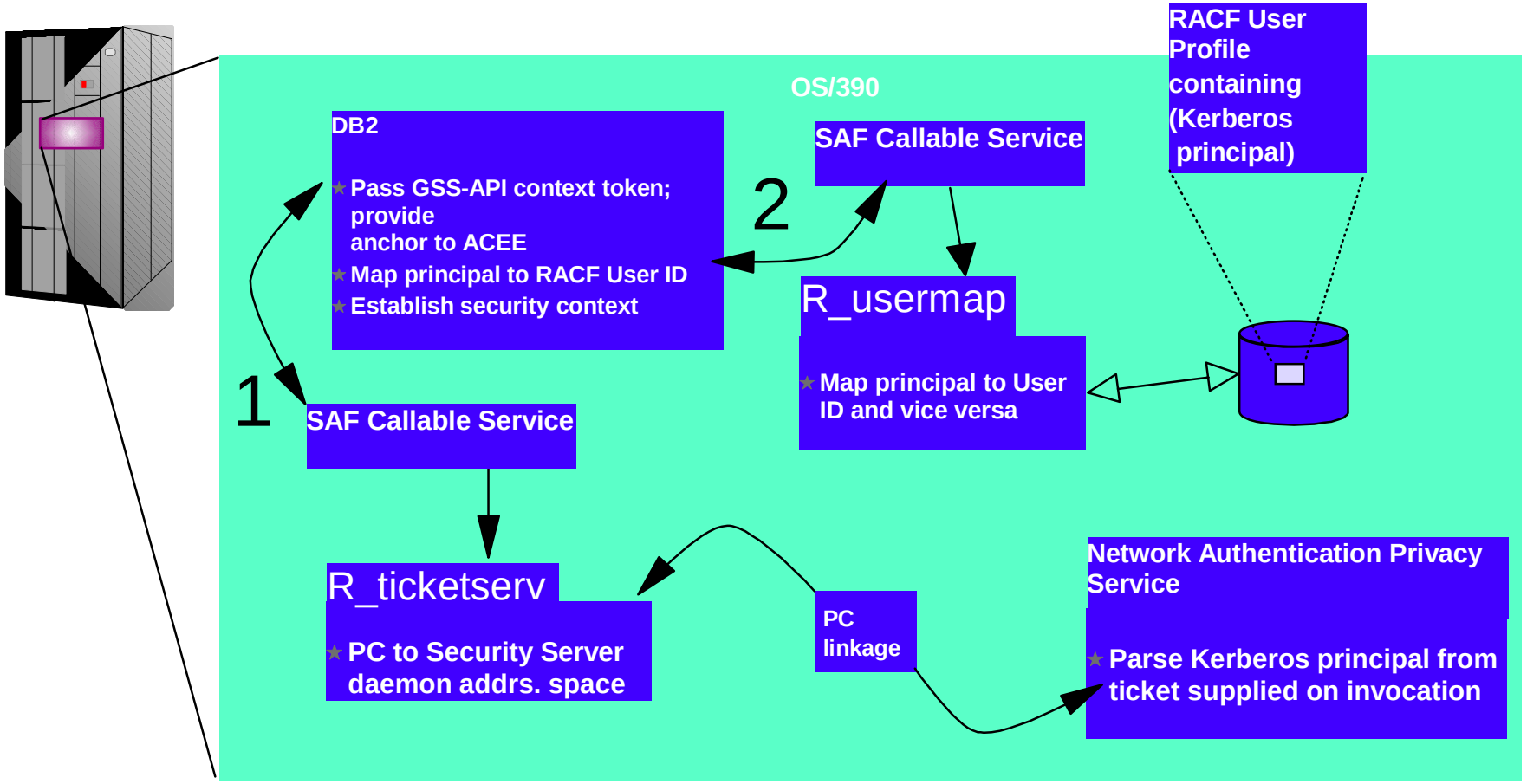
OS/390 and WIN2K Kerberos Domains

The client authenticates to the KDC, and obtains a ticket for the target server.
The assumption in this chart, is that the target server is Win2k running DB2, and the target server makes a request to a DB2 instance on OS/390. The DB2 instance on the target server passes the ticket of the user client on the flow to the OS/390 host.



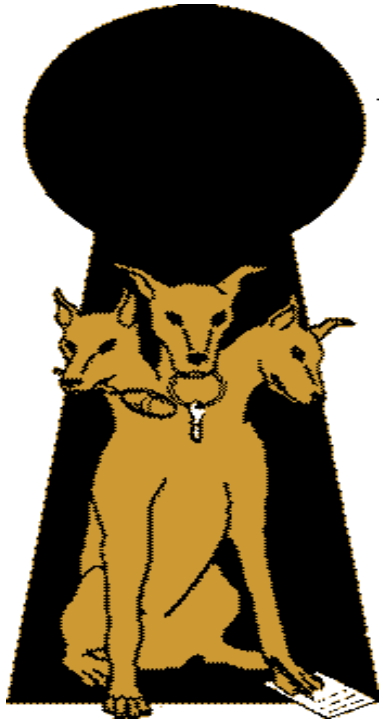
OS/390 and WIN2K Kerberos Domains...

This pictorial indicates that OS/390 needs to be a viewed as a Kerberos peer domain. Administratively, a peer trust relationship has been established between the OS/390 Kerberos domain and a Win2K kerberos domain. Local Kerberos principals must be defined to the OS/390 Security Server and a new user profile segment will hold the Kerberos principal name. Support is also provided to map a Kerberos principal name to a RACF User ID. Note that principal registration must be performed in two places, 1) to the Win2k Kerberos domain, and 2) to the OS/390 Kerberos domain.



Slogan of the day

Three heads are better than one !



Questions ???