

**SAP SINGLE SIGN-ON
AND SECURE CONNECTIONS
VIA SNC ADAPTER
BASED ON KERBEROS V5**

■
■
■
■
■
■
■
■
■
■
■
■
■

Project name : SSO SNC ABAP

Our reference : REALTECH

Project management : Manfred Stein, SAP AG
manfred.stein@sap.com

Document type : Whitepaper

Author : Matthias Schlarb, REALTECH system consulting GmbH
matthias.schlarb@realtech.com

REALTECH system consulting GmbH
Industriestrasse 39c
69190 Walldorf

Index

1	Introduction	3
1.1	General Notes	3
1.1.1	Scenario	3
1.1.2	Important SAP Notes	3
1.1.3	Helpful links	3
1.2	Prerequisites	4
2	Setup Windows-Server	4
2.1	Create service user	4
2.2	Set Service Principal Name	5
2.3	Export Keytab from Microsoft ADS	5
3	Setup Linux-Server	6
3.1	Configuration Kerberos	6
3.2	Time synchronization	7
3.3	Key import to Linux	7
3.4	Initialize Kerberos: Ticket Granting Ticket (TGT)	8
3.4.1	Set permissions	8
3.4.2	Automatic renewal of the Kerberos TGT	8
3.5	Configure SAP	9
3.5.1	Compile SNC Adapter	9
3.5.2	Configure profile parameters	10
4	Setup Windows-Client	10
4.1	Time synchronization	10
4.2	Installation of the wrapper DLLs	10
4.2.1	Manually	10
4.2.2	Automatically	11
4.3	Configure SAP Logon	11
5	Map users	12
6	Appendix	12
6.1	How Kerberos works	12
6.2	ktpass 14	

1 INTRODUCTION

SNC over the SNC Adapter enables Single Sign-On and encryption of network connections using the authentication protocol Kerberos v5.

1.1 General Notes

1.1.1 Scenario

This document is based on a test environment at the SAP LinuxLab.

System <i>hostname</i>	Operating system	Function
Linux-Server <i>linuxlabsrv</i>	SUSE Linux Enterprise 10 64-Bit SP1	SAP NW70 MaxDB (TestDrive)
Windows-Server <i>linuxlabpdc</i>	Windows 2003 32-Bit SP2	Primary Domain Controller (PDC) Key Distribution Center (KDC)
Windows-Client <i>client1</i>	Windows XP Professional 32-Bit SP2	SAP-GUI

AD-Domain: **linuxlab.com**

SAP SID: **N4S**

1.1.2 Important SAP Notes

Note [#150380](#) - Is MIT Kerberos 5 supported for use with SNC?

Note [#352295](#) - Microsoft Windows Single Sign-On options

Note [#595341](#) - Installation issues with Single Sign-On and SNC

1.1.3 Helpful links

SAP Developer Network

1) [Technology - Network Security \(BC-SNC\)](#)

SAP Library

2) [User Authentication and Single Sign-On](#)

3) [Network and Transport Layer Security](#)

Service Principal Names

4) [How Service Publication and Service Principal Names Work](#)

5) [Setspn Overview](#)

1.2 Prerequisites

The operating systems, the SAP-system and the SAP-GUI already have to be installed according to your demands before you realize the steps in this document.

The Linux server uses the MIT Kerberos implementation. By default it comes with your Linux distribution. In the present case version 1.4.3-19-17 from SUSE is used. Later versions shouldn't affect the functionality.

In addition following software should be installed. For details to SNC Adapter and wrapper DLLs see the regarding chapters.

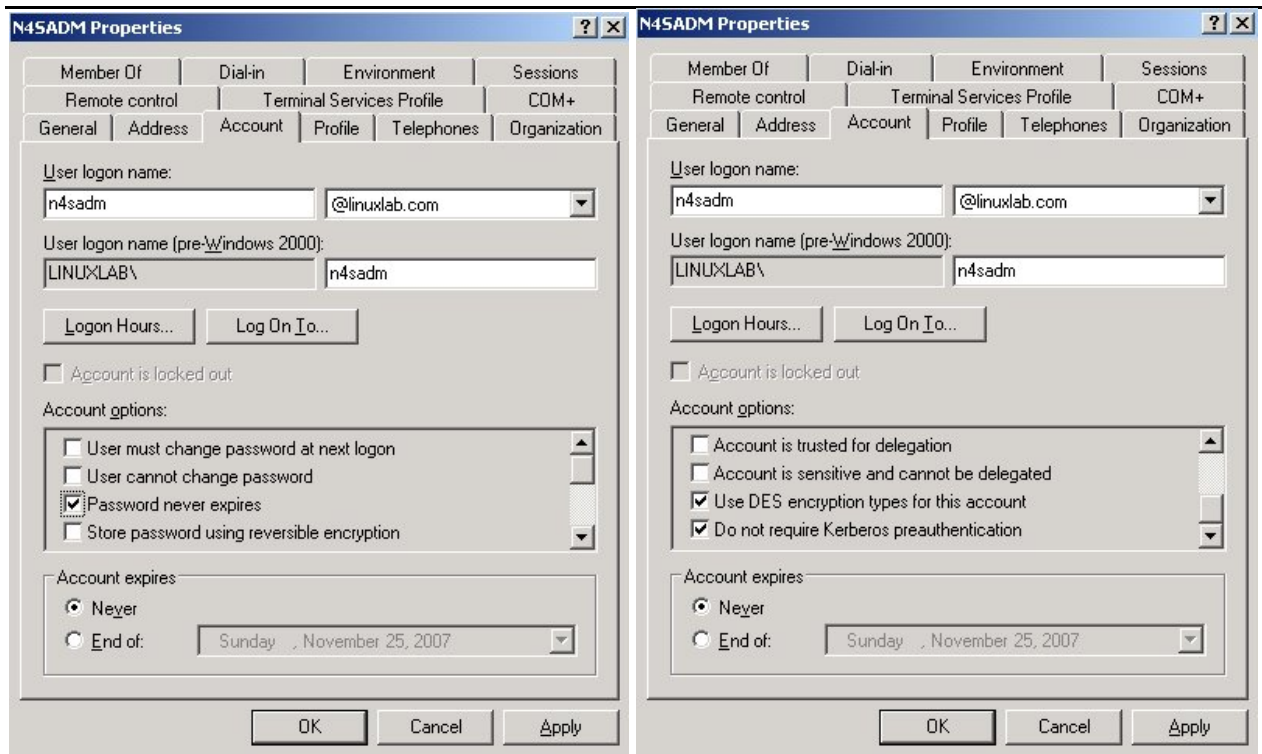
System	Software	Link
Linux-Server	MIT Kerberos5 Implementation-Libraries	(shipped)
	MIT Kerberos5 Implementation-Client	(shipped)
	SAP SNC Adapter	see Link 1
	optional: SAP GSS Test Suite	Note #150380
Windows-Server	Windows Server 2003 Resource Kit Tools	http://www.microsoft.com/downloads/
	Windows Server 2003 Service Pack 2 32-bit Support Tools	http://www.microsoft.com/downloads/
Windows-Client	Wrapper DLLs for Windows	Note #352295 or #595341

2 SETUP WINDOWS-SERVER

2.1 Create service user

Create a user which works as a Service Principal. Here the `<sid>adm` is used.

Remark: For compatibility reasons the DES-encryption has been chosen here. It depends on your system landscape if other encryption types like RC4-HMAC-NT can be chosen.



Set "Password never expires", "Use DES encryption types for this account" and "Do not require Kerberos preauthentication".

2.2 Set Service Principal Name

See [1.1.3](#): Helpful Links 4 and 5.

```
setspn -A <ServiceName>/<hostname_linux_server>.<domain_name>
<DOMAIN_SHORT>\<service_user>
```

eg:

```
setspn -A SAPService/linuxlabsrv.linuxlab.com LINUXLAB\n4sadm
```

2.3 Export Keytab from Microsoft ADS

The key export is done by `ktpass`. See [6.2](#) for help.

```
ktpass -princ
<ServiceName>/<hostname_linux_server>.<domain_name>@<DOMAIN_NAME> -mapuser
<DOMAIN_SHORT>\<service_user> -crypto <ENCRYPTION_TYPE> -ptype
<PRINCIPAL_TYPE> -mapop set +desonly -pass <your_password> -out <filename>
```

eg:

```
ktpass -princ SAPService/linuxlabsrv.linuxlab.com@LINUXLAB.COM -mapuser  
LINUXLAB\n4sadm -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -mapop set  
+desonly -pass passw0rd -out n4s.keytab
```

Targeting domain controller: linuxlabpdc.linuxlab.com

Using legacy password setting method

Successfully mapped SAPService/linuxlabsrv.linuxlab.com to n4sadm.

Key created.

Output keytab to n4s.keytab:

Keytab version: 0x502

keysize 75 SAPService/linuxlabsrv.linuxlab.com@LINUXLAB.COM ptype 1 (KRB5_NT_PRINCIPAL) **vno 3** etype 0x3 (DES-CBC-MD5) keylength 8 (0xa10746cea8df0e68)

Account n4sadm has been set for DES-only encryption.

Note the red marked number after the argument *vno*.

The file *n4s.keytab* contains the necessary key and can be copied to the linux server.

3 SETUP LINUX-SERVER

3.1 Configuration Kerberos

The configuration is held in */etc/krb5.conf* by default.

eg:

```
[libdefaults]  
    default_realm = LINUXLAB.COM  
  
[domain_realm]  
    linuxlab.com = LINUXLAB.COM  
  
[realms]  
    LINUXLAB.COM = {  
        kdc = linuxlabpdc.linuxlab.com  
        admin_server = linuxlabpdc.linuxlab.com  
        kpasswd_server = linuxlabpdc.linuxlab.com  
    }  
  
[logging]  
    kdc = FILE:/var/log/krb5/krb5kdc.log  
    admin_server = FILE:/var/log/krb5/kadmind.log  
    default = SYSLOG:NOTICE:DAEMON
```

You should give the user *<sid>adm* permissions for */var/log/krb5*:

```
chmod 777 /var/log/krb5
```

3.2 Time synchronization

The kerberos protocol marks every ticket as invalid which has more than 2 minutes (by default) time difference based on the server time. This is valid for the linux server as well as for the windows client! Both have to be synchronized to the windows server which has - as a PDC - an NTP service running by default.

Under Linux this happens with `ntpd` - the Network Time Protocol Daemon. The easiest way to install and configure it is via `YaST`.

3.3 Key import to Linux

The key from `n4s.keytab` will now be imported to `/etc/krb5.keytab`. For this the tool `ktutil` under user `root` is used.

<code>ktutil</code>	executes the program
<code>?</code>	help
<code>rkt /tmp/n4s.keytab</code>	reads the key of the imported file
<code>l -e</code>	list extended

The output should look like:

```
slot KVNO Principal
-----
  1    3 SAPService/linuxlabsrv.linuxlab.com@LINUXLAB.COM (DES cbc mode with
RSA-MD5)
```

Compare the value in the column KVNO with your number from [2.3](#): it should be the same. If not, you probably have exported the key from windows multiple times with `ktpass` and are now using an older version. In brackets you see the encryption type.

<code>wkt /etc/krb5.keytab</code>	writes the key into the key table of the system
<code>q</code>	quit

3.4 Initialize Kerberos: Ticket Granting Ticket (TGT)

Get your first TGT with:

```
kinit -V -k <ServiceName>/<hostname_linux_server>.<domain_name>@<DOMAIN_NAME>
```

eg:

```
kinit -V -k SAPService/linuxlabsrv.linuxlab.com@LINUXLAB.COM
```

Authenticated to Kerberos v5

3.4.1 Set permissions

Under the user *root* change the permissions for the key table of the system. Else *<sid>adm* can't get a valid ticket.

```
chgrp sapsys /etc/krb5.keytab
```

```
chmod 640 /etc/krb5.keytab
```

Now a (manual) *kinit* (see [3.4](#)) should also be possible under user *<sid>adm*.

Should the permissions not have been set correctly, you will receive following error on your SAP instance in the developer trace of the work process:

```
N      GSS-API(maj): Miscellaneous failure
```

```
N      GSS-API(min): Permission denied
```

3.4.2 Automatic renewal of the Kerberos TGT

Kerberos tickets have a limited lifetime (10 hours by default) and therefore have to be renewed. The easiest way is to setup a cron job. In this example the ticket will be renewed every 6th hour:

```
crontab -e
```

```
01 0,6,12,18 * * * /usr/bin/kinit -k
```

```
SAPService/linuxlabsrv.linuxlab.com@LINUXLAB.COM
```

Should the renewal of the ticket fail for any reason and therefore the linux server not possess a valid TGT, you will find following error on your SAP instance in the developer trace of the work process:

```
N      GSS-API(maj): Miscellaneous failure
```

```
N      GSS-API(min): No credentials cache found
```

3.5 Configure SAP

The SNC adapter can be downloaded from the SAP Developer Network (see [Link 1](#)). In fact it is possible to implement Single Sign-On via Kerberos without the SAP adapter, but its usage is recommended by SAP.

3.5.1 Compile SNC Adapter

There is no build for Linux, so you should create one. You can copy the build eg. from SunOS to Linux:

```
cp build.SunOS build.Linux
```

Adjust the values in your just created *build.Linux* according to your system environment, eg:

```
#!/bin/sh
OBJ=".o"
CC="gcc"
CFLAGS="-g -DXDEBUG=1"
RM="rm -f"
EXE=""
LD="$CC"
LDFLAGS="-ldl -lnsl -lpthread -lc"
LDTARGET='-o $@"
XD=""
LDLIBS="-ldl"
SHEXT=".so"
SHFLAGS="-fPIC"
LINK_SHARED='$(CC) -shared -Wl,-export-dynamic -Wl,-soname,$@"
LINK_SHARED_END=""
VENLIB="-lgssapi_krb5"
if [ "$VENLIB" = "" ] ; then
    echo "****"
    echo "**** Please edit $0 and define VENLIB to link your"
    echo "**** GSS-API v2 shared library"
    echo "****"
    exit 1
fi
export OBJ CC CFLAGS RM EXE LDLIBS LD LDTARGET LDFLAGS XD
export SHEXT SHFLAGS LINK_SHARED LINK_SHARED_END VENLIB
"$@"
```

In *Makefile* the name of the library which has to be made is written under *XNAME*. You should change it from *snctlm* to *snckrb5*.

Compile now with

```
make
```

Possibly in file *snckrb5.c* you have to comment out the function *sapgss_inquire_mechs_for_name* (line 1.000 - 1.017) because this function might not get compiled correctly which results in a corrupted library.

Copy the just created file *snckrb5.so* into your library directory (here: */usr/lib64*). Make sure that the file has the correct permissions:

```
chmod 755 /usr/lib64/snckrb5.so
```

3.5.2 Configure profile parameters

In RZ10 → Instance profile → Extended maintenance add / edit following values:

Name	Value	Description
snc/gssapi_lib	/usr/lib64/snckrb5.so	GSSAPI SNC library
snc/identity/as	p/krb5:SAPService/linuxlabshr.linuxlab.com@LINUXLAB.COM	SNC identity
snc/enable	1	Use SNC
snc/accept_insecure_cplic	1	Permit CPIC without SNC
snc/accept_insecure_rfc	1	Permit RFC without SNC
snc/accept_insecure_gui	1	Permit SAPGUI connections without SNC
snc/accept_insecure_r3int_rfc	1	Permit internal RFC connections without SNC
snc/data_protection/min	1	Min. protection level 1 (authentication)
snc/data_protection/max	3	Max. protection level 3 (encryption)
snc/data_protection/use	3	Use level of snc/data_protection/max
snc/permit_insecure_start	1	Allow execution of external programs without SNC

4 SETUP WINDOWS-CLIENT

4.1 Time synchronization

The kerberos protocol marks every ticket as invalid which has more than 2 minutes (by default) time difference based on the server time. This is valid for the linux server as well as for the windows client! Both have to be synchronized to the windows server which has - as a PDC - an NTP service running by default.

Under Windows you can configure an NTP server with `net time (help with: net help time)`.

4.2 Installation of the wrapper DLLs

In the following the both ways of installing the wrapper DLLs are described.

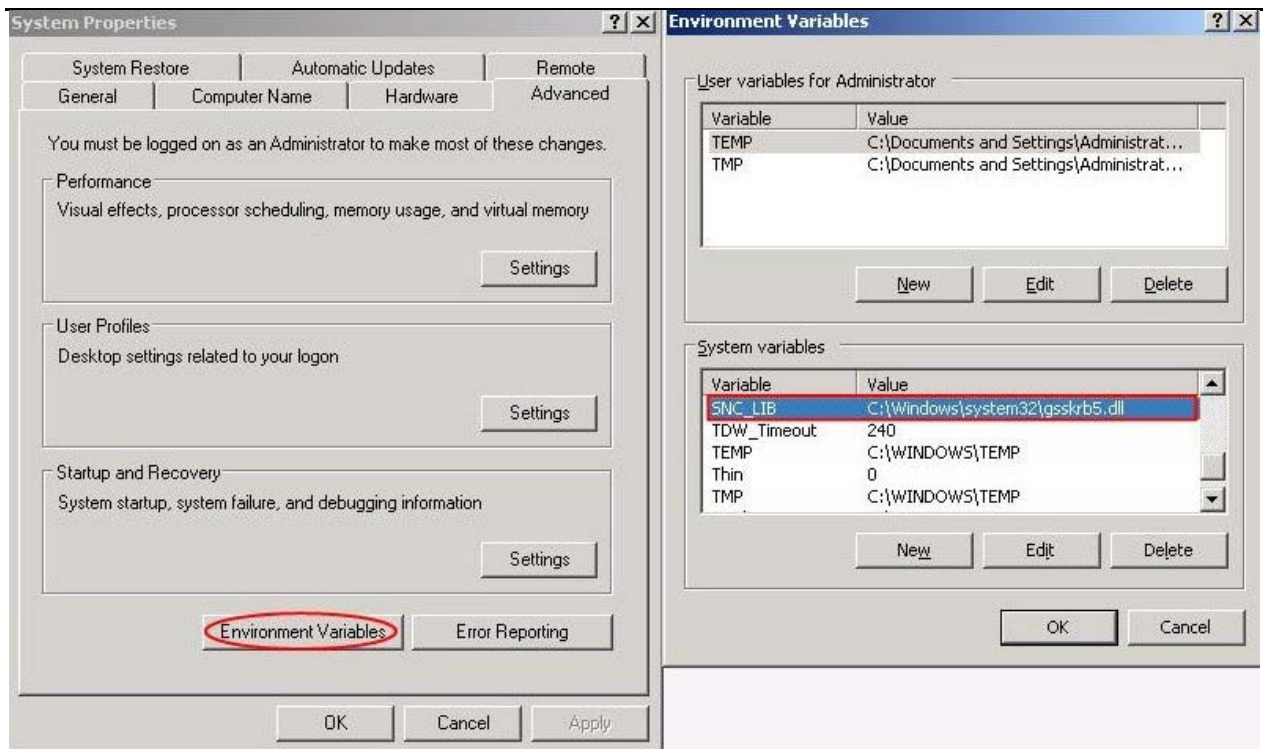
4.2.1 Manually

To install the DLLs manually follow the SAP Note [#352295](#).

Copy the file `gsskrb5.dll` in the directory `%windir%\system32`.

Add the following system variable:

Variable `SNC_LIB` with the value `%windir%\system32\gsskrb5.dll`.



4.2.2 Automatically

You can use the installer file *SAPSSO.MSI* for distributing to several clients over the windows network as of SAP Note [#595341](#).

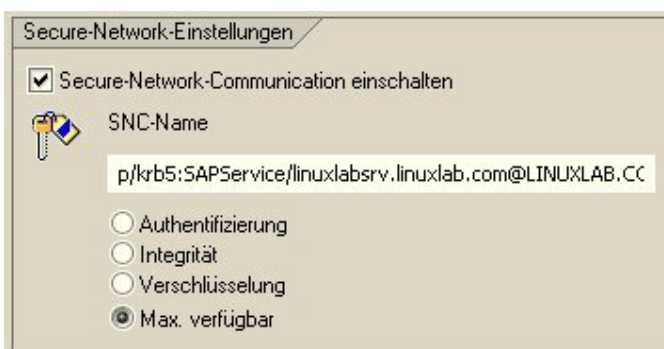
4.3 Configure SAP Logon

The logon method has to be adapted. Create with the Logon-Pad a connection to the regarding SAP system. Under *Change Item* → *Network* you activate the Secure Network Communication and add an SNC Name:

`p/krb5:<ServiceName>/<hostname_linux_server>.<domain_name>@<DOMAIN_NAME>`

eg:

`p/krb5:SAPService/linuxlabsrv.linuxlab.com@LINUXLAB.COM`



5 MAP USERS

In order to use Single Sign-On you have to map the users between the SAP system and the Windows Active Directory. You can do this with transaction **SU01**:

Tab SNC

SNC Name: p:<WindowsUser>@<DOMAIN_NAME>

6 APPENDIX

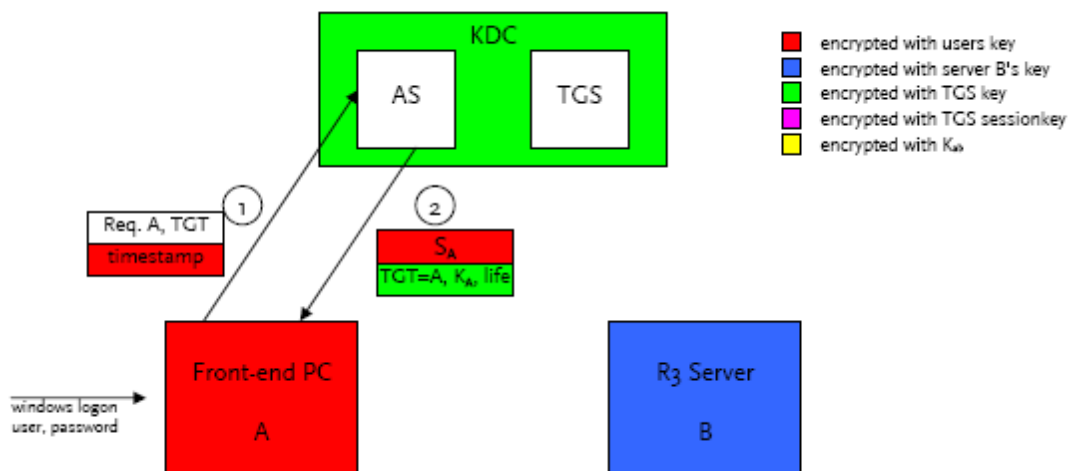
6.1 How Kerberos works

Step 1:

Logon on to Windows. The users key is generated from the password and a request for the TGT (ticket granting ticket) is sent to the KDC (key distribution centre). To prove the authenticity a timestamp encrypted with the users key is added to the request.

Step 2:

The KDC checks the request by decrypting the timestamp with the key stored in his database. Now it generates a session key S_A for the communication between A and the TGS (ticket granting service) and encrypts it with the key of user A. Afterwards it issues the TGT and encrypts it with the key of the TGS. This ticket contains the key of user A and the lifetime.

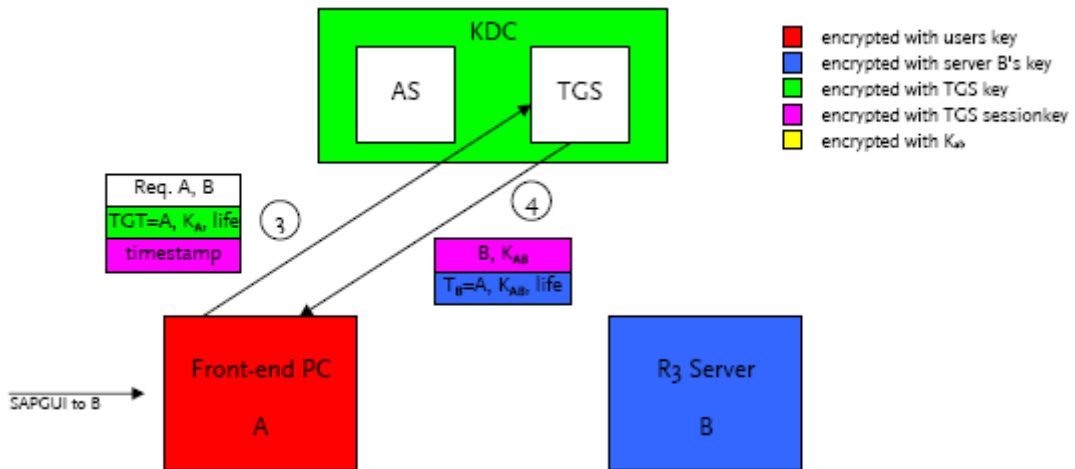


Step 3:

The user wants to log on to R/3. It requests a ticket for the communication with the Server B. It adds the TGT to provide his key to the TGS and proves his authenticity by adding a time stamp with the session key.

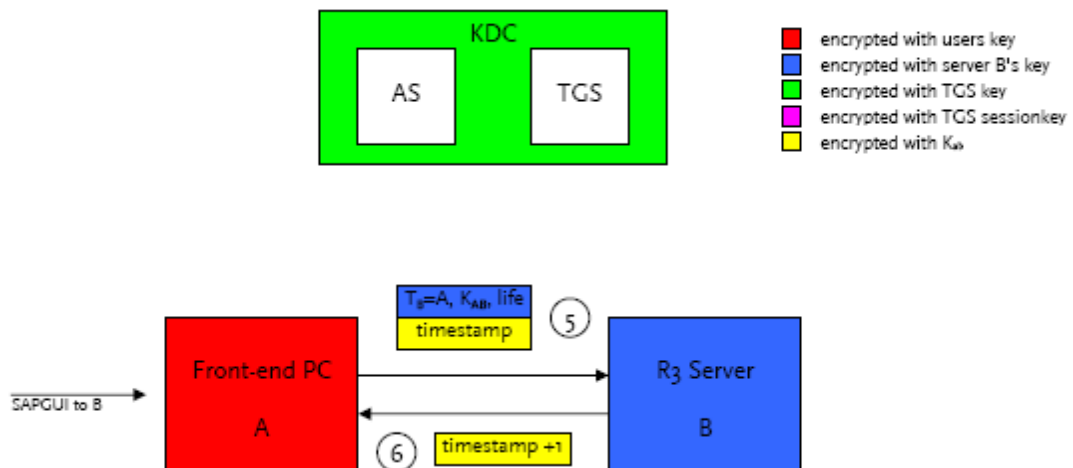
Step 4:

The TGS invents a session K_{AB} for the connection between the front-end and the R/3 server. It returns this key to the user encrypted with his session key. Afterwards it issues a ticket for server B and encrypts it with key of server B.



Step 5:
A sends the ticket to server B and adds a timestamp encrypted with the session key.

Step 6:
Server B checks the timestamp and acknowledges the connection by returning timestamp+1 encrypted with the session key.



Now both partners are sure that the other one is authentic and they have a secret key for the communication through the network.



6.2 ktpass

Command line options:

```
-----most useful args
[- /]          out : Keytab to produce
[- /]          princ : Principal name (user@REALM)
[- /]          pass : password to use
                  use "*" to prompt for password.
[- +]          rndPass : ... or use +rndPass to generate a random password
[- /]          minPass : minimum length for random password (def:15)
[- /]          maxPass : maximum length for random password (def:256)

-----less useful stuff
[- /]          mapuser : map princ (above) to this user account (default: don't)
[- /]          mapOp : how to set the mapping attribute (default: add it)
[- /]          mapOp : is one of:
[- /]          mapOp :          add : add value (default)
[- /]          mapOp :          set : set value
[- +]          DesOnly : Set account for des-only encryption (default:don't)
[- /]          in : Keytab to read/digest

-----options for key generation
[- /]          crypto : Cryptosystem to use
[- /]          crypto : is one of:
[- /]          crypto : DES-CBC-CRC : for compatibility
[- /]          crypto : DES-CBC-MD5 : for compatibliity
[- /]          crypto : RC4-HMAC-NT : default 128-bit encryption
[- /]          ptype : principal type in question
[- /]          ptype : is one of:
[- /]          ptype : KRB5_NT_PRINCIPAL : The general ptype-- recommended
[- /]          ptype : KRB5_NT_SRV_INST : user service instance
[- /]          ptype : KRB5_NT_SRV_HST : host service instance
[- /]          kvno : Override Key Version Number
                  Default: query DC for kvno. Use /kvno 1 for Win2K compat
[- +]          Answer : +Answer answers YES to prompts. -Answer answers NO.
[- /]          Target : Which DC to use. Default:detect
[- /]          RawSalt : raw salt to use when generating key (not needed)
[- +]          DumpSalt : show us the MIT salt being used to generate the key
[- +]          SetUpn : Set the UPN in addition to the SPN. Default DO.
[- +]          SetPass : Set the user's password if supplied.

-----options for trust attributes (Windows Server 2003 Sp1 Only)
[- /] MitRealmName : MIT Realm which we want to enable RC4 trust on.
[- /] TrustEncryp : Trust Encryption to use; DES is default
[- /] TrustEncryp : is one of:
[- /] TrustEncryp :          RC4 : RC4 Realm Trusts (default)
[- /] TrustEncryp :          DES : go back to DES
```