

**SAP SINGLE SIGN-ON  
UND SECURE CONNECTIONS  
VIA SNC ADAPTER  
BASIEREND AUF KERBEROS V5**

■  
■  
■  
■  
■  
■  
■  
■  
■  
■  
■  
■

**Projektname** : SSO SNC ABAP

**Unser Zeichen** : REALTECH

**Projektleitung** : Manfred Stein, SAP AG  
[manfred.stein@sap.com](mailto:manfred.stein@sap.com)

**Dokumentenart** : Whitepaper

**Verfasser** : Matthias Schlarb, REALTECH system consulting GmbH  
[matthias.schlarb@realtech.com](mailto:matthias.schlarb@realtech.com)

**REALTECH system consulting GmbH**  
**Industriestraße 39c**  
**69190 Walldorf**

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung.....</b>	<b>3</b>
1.1	<b>Allgemeine Hinweise .....</b>	<b>3</b>
1.1.1	<b>Szenario .....</b>	<b>3</b>
1.1.2	<b>Wichtige Hinweise.....</b>	<b>3</b>
1.1.3	<b>Hilfreiche Links.....</b>	<b>3</b>
1.2	<b>Softwarevoraussetzungen .....</b>	<b>4</b>
<b>2</b>	<b>Setup des Windows-Servers .....</b>	<b>4</b>
2.1	<b>Anlegen des Benutzers .....</b>	<b>4</b>
2.2	<b>Service Principal Name setzen.....</b>	<b>5</b>
2.3	<b>Export des Keytab vom Microsoft ADS.....</b>	<b>5</b>
<b>3</b>	<b>Setup des Linux-Servers.....</b>	<b>6</b>
3.1	<b>Konfiguration Kerberos .....</b>	<b>6</b>
3.2	<b>Zeit-Synchronisation.....</b>	<b>7</b>
3.3	<b>Key Import in Linux .....</b>	<b>7</b>
3.4	<b>Kerberos initialisieren: Ticket Granting Ticket (TGT).....</b>	<b>8</b>
3.4.1	<b>Berechtigung setzen .....</b>	<b>8</b>
3.4.2	<b>Automatische Erneuerung des Kerberos TGT .....</b>	<b>8</b>
3.5	<b>Konfiguration SAP.....</b>	<b>9</b>
3.5.1	<b>SNC Adapter kompilieren .....</b>	<b>9</b>
3.5.2	<b>Profilparameter anpassen .....</b>	<b>10</b>
<b>4</b>	<b>Setup des Windows-Client.....</b>	<b>10</b>
4.1	<b>Zeit-Synchronisation.....</b>	<b>10</b>
4.2	<b>Installation der Wrapper-DLLs .....</b>	<b>10</b>
4.2.1	<b>Manuell .....</b>	<b>10</b>
4.2.2	<b>Automatisch.....</b>	<b>11</b>
4.3	<b>SAP Logon anpassen.....</b>	<b>11</b>
<b>5</b>	<b>User-Mapping .....</b>	<b>12</b>
<b>6</b>	<b>Anhang.....</b>	<b>12</b>
6.1	<b>Funktionsweise Kerberos .....</b>	<b>12</b>
6.2	<b>ktpass 15</b>	

# 1 EINLEITUNG

SNC mit dem SNC Adapter ermöglicht Single Sign-On und Verschlüsselung von Netzwerkverbindungen unter Verwendung des Authentifizierungsprotokolls Kerberos v5.

## 1.1 Allgemeine Hinweise

### 1.1.1 Szenario

Dieses Dokument basiert auf einem Testszenario im SAP LinuxLab.

Bezeichnung <i>Rechnername</i>	Betriebssystem	Funktion
<b>Linux-Server</b> <i>linuxlabsrv</i>	SUSE Linux Enterprise 10 64-Bit SP1	SAP NW70 MaxDB (TestDrive)
<b>Windows-Server</b> <i>linuxlabpdc</i>	Windows 2003 32-Bit SP2	Primary Domain Controller (PDC) Key Distribution Center (KDC)
<b>Windows-Client</b> <i>client1</i>	Windows XP Professional 32-Bit SP2	SAP-GUI

AD-Domäne: **linuxlab.com**

SAP SID: **N4S**

### 1.1.2 Wichtige Hinweise

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

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

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

### 1.1.3 Hilfreiche Links

#### SAP Developer Network

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

#### SAP Library

2) [Benutzerauthentifizierung und Single Sign-On](#)

3) [Sicherheit des Netzwerks und Transport Layer Security](#)

#### Service Principal Names

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

5) [Setspn Overview](#)

## 1.2 Softwarevoraussetzungen

Die Betriebssysteme, das SAP-System sowie die SAP-GUI müssen (Ihren Bedürfnissen gemäß) bereits installiert sein, bevor Sie die in diesem Dokument beschriebenen Schritte durchführen.

Für den Linux-Server wird die MIT Kerberos Implementierung benötigt. Diese wird standardmäßig vom jeweiligen Linux-Distributor mitgeliefert. Im vorliegenden Fall wurde die Kerberos-Version 1.4.3-19-17 von SUSE verwendet. Spätere Versionen dürften die Funktionsweise nicht beeinträchtigen.

Desweiteren sollte folgende Software installiert werden. Zu den Installationen des SNC Adapter und den Wrapper-DLLs siehe jeweiliges Kapitel.

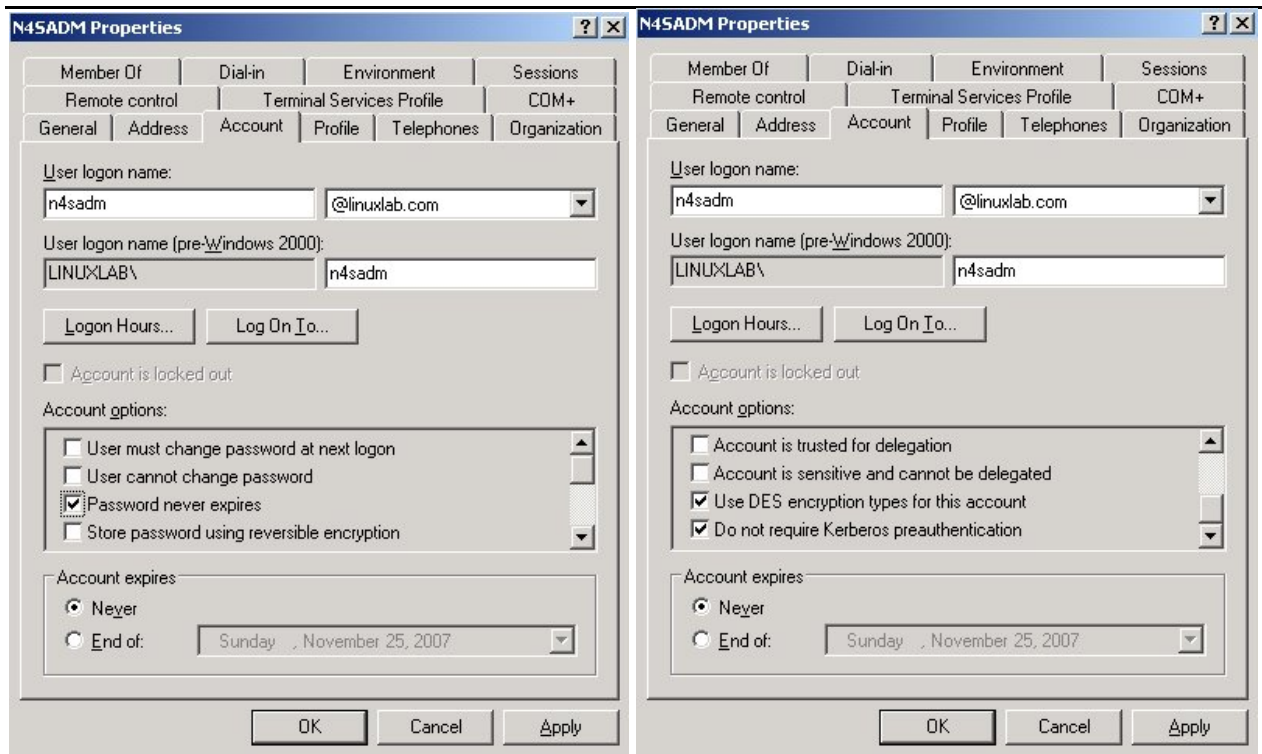
System	Software	Link
Linux-Server	MIT Kerberos5 Implementation-Libraries	(wird mitgeliefert)
	MIT Kerberos5 Implementation-Client	(wird mitgeliefert)
	SAP SNC Adapter	siehe <a href="#">Link 1</a>
	optional: SAP GSS Test Suite	Hinweis <a href="#">#150380</a>
Windows-Server	Windows Server 2003 Resource Kit Tools	<a href="http://www.microsoft.com/downloads/">http://www.microsoft.com/downloads/</a>
	Windows Server 2003 Service Pack 2 32-bit Support Tools	<a href="http://www.microsoft.com/downloads/">http://www.microsoft.com/downloads/</a>
Windows-Client	Wrapper-DLLs für Windows	Hinweis <a href="#">#352295</a> oder <a href="#">#595341</a>

## 2 SETUP DES WINDOWS-SERVERS

### 2.1 Anlegen des Benutzers

Legen Sie einen Benutzer an, der als Service Principal fungieren wird. Hier wurde `<sid>adm` verwendet.

Anmerkung: In diesem Szenario wurde aus Kompatibilitätsgründen die DES-Verschlüsselung gewählt. Ob modernere Verschlüsselungsverfahren, wie z. B. RC4-HMAC-NT, unter Ihrer Systemkonstellation verwendet werden können, muss vorher abgeklärt werden.



Setzen Sie "Password never expires", "Use DES encryption types for this account" und "Do not require Kerberos preauthentication".

## 2.2 Service Principal Name setzen

Siehe hierzu [1.1.3](#): Hilfreiche Links 4 und 5.

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

z.B.:

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

## 2.3 Export des Keytab vom Microsoft ADS

Der Keyexport wird mit `ktpass` durchgeführt. Für Hilfe zum Tool `ktpass` siehe [6.2](#).

```
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>
```

---

z.B.:

```
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.

Die rot markierte Zahl hinter dem Argument *vno* notieren.

Die Datei *n4s.keytab* enthält den benötigten Schlüssel und kann (in ein temporäres Verzeichnis) auf den Linux-Server kopiert werden.

## 3 SETUP DES LINUX-SERVERS

### 3.1 Konfiguration Kerberos

Die Konfiguration wird standardmäßig in der Datei */etc/krb5.conf* vorgenommen.

z.B.:

```
[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
```

Es sollten dem Benutzer *<sid>adm* noch Berechtigungen für */var/log/krb5* gegeben werden:

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

## 3.2 Zeit-Synchronisation

Das Kerberosprotokoll erkennt jedes Ticket als ungültig an, welches mehr als 2 Minuten außerhalb der Serverzeit liegt. Dies gilt sowohl für den Linux-Server als auch für den Windows-Client! Beide werden auf den Windows-Server, auf dem standardmäßig ein NTP-Server läuft, synchronisiert.

Unter Linux geschieht dies mit `ntpd` - dem Network Time Protocol Daemon. Dieser kann am einfachsten mit dem `YaST` installiert und konfiguriert werden.

## 3.3 Key Import in Linux

Der Key in der Datei `n4s.keytab` soll nun in die `/etc/krb5.keytab` importiert werden. Verwenden Sie hierzu das Tool `ktutil` unter dem Benutzer `root`.

<code>ktutil</code>	Ruft das Programm auf
<code>?</code>	Hilfe
<code>rkt /tmp/n4s.keytab</code>	liest den Key der importierten Datei
<code>l -e</code>	list extended

Der output sollte so aussehen:

```
slot KVNO Principal
```

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

*Vergleichen Sie den Wert KVNO mit dem notierten Wert aus [2.3](#): dieser sollte übereinstimmen. Ist dies nicht der Fall, so haben Sie wahrscheinlich mehrmals Keys unter Windows mit `ktpass` exportiert und verwenden für den Import eine veraltete Variante. In Klammern wird übrigens der Verschlüsselungsmodus angezeigt.*

<code>wkt /etc/krb5.keytab</code>	schreibt den Key in die Keytabelle des Systems
<code>q</code>	quit

---

### 3.4 Kerberos initialisieren: Ticket Granting Ticket (TGT)

Holen Sie Ihr erstes TGT mit:

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

z.B.:

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

```
Authenticated to Kerberos v5
```

#### 3.4.1 Berechtigung setzen

Ändern Sie unter dem Benutzer *root* die Berechtigungen für die Keytabelle des Systems. Andernfalls kann der *<sid>adm* kein gültiges Ticket holen.

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

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

Nun sollte ein (manueller) *kinit* (siehe [3.4](#)) auch unter dem Benutzer *<sid>adm* möglich sein.

Sollten die Berechtigungen nicht korrekt gesetzt sein, werden Sie später beim Starten der SAP-Instanz im Dev-Trace des Work-Prozesses folgenden Fehler finden:

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

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

#### 3.4.2 Automatische Erneuerung des Kerberos TGT

Kerberos Tickets haben eine begrenzte Lebenszeit (Standard 10 Stunden) und müssen erneuert werden. Der einfachste Weg ist, einen periodischen Cronjob einzurichten. Das Ticket wird alle 6 Stunden erneuert, wenn Sie folgende Zeile der Crontabelle hinzufügen:

```
crontab -e
```

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

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

Sollte die Erneuerung des Tickets aus irgendeinem Grund nicht funktioniert haben und der Linux-Server somit kein gültiges TGT besitzen, werden Sie später beim Starten der SAP-Instanz im Dev-Trace des Work-Prozesses folgenden Fehler finden:

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

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

## 3.5 Konfiguration SAP

Der SNC Adapter kann im SAP Developer Network heruntergeladen werden (siehe [Link 1](#)). Es ist zwar möglich, Single Sign-On mit Kerberos ohne den SNC Adapter zu implementieren, jedoch wird dessen Verwendung von SAP empfohlen.

### 3.5.1 SNC Adapter kompilieren

Da für die Kompilierung unter Linux kein *build.Linux* existiert, sollte dieses erstellt werden. Kopieren Sie das build z. B. von SunOS zum build von Linux:

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

Stellen Sie die Werte im soeben erzeugten *build.Linux* auf Ihr System ein, z. B.:

```
#!/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 $0 and define VENLIB to link your"
    echo "*** GSS-API v2 shared library"
    echo "****"
    exit 1
fi
export OBJ CC CFLAGS RM EXE LDLIBS LD LDTARGET LDFLAGS XD
export SHEXT SHFLAGS LINK_SHARED LINK_SHARED_END VENLIB
"$@"
```

Im *Makefile* wird unter *XNAME* der Name der zu erzeugenden Library angegeben. Sie sollten diesen Wert von *sncntlm* auf *snckrb5* abändern.

Kompilieren Sie nun die Datei mit  
make

Eventuell müssen Sie in der *snckrb5.c* die Funktion *sapgss\_inquire\_mechs\_for\_name* (Zeile 1.000 bis 1.017) auskommentieren, da diese Funktion u. U. nicht richtig kompiliert werden kann und dadurch die erzeugte Library fehlerhaft ist.

Die soeben erzeugte Datei *snckrb5.so* kopieren Sie in Ihr Library-Verzeichnis (im vorliegenden Fall */usr/lib64/*). Stellen Sie sicher, dass die Datei über die korrekten Berechtigungen verfügt:

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

### 3.5.2 Profilparameter anpassen

Unter RZ10 → Instanzprofil → Erweiterte Pflege tragen Sie folgende Werte ein:

Name	Value	Description
snc/gssapi_lib	/usr/lib64/snckrb5.so	GSSAPI SNC library
snc/identity/as	p/krb5:SAPService/linuxlab.srv.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 DES WINDOWS-CLIENT

### 4.1 Zeit-Synchronisation

Nach der Kerberosimplementierung müssen Sie unbedingt die Zeit-Synchronisation einrichten. Das Kerberosprotokoll erkennt jedes Ticket als ungültig an, welches mehr als 2 Minuten außerhalb der Serverzeit liegt. Dies gilt sowohl für den Linux-Server als auch für den Windows-Client! Beide werden auf den Windows-Server, auf dem standardmäßig ein NTP-Server läuft, synchronisiert.

Unter Windows kann mit dem Kommando `net time` ein NTP-Server eingetragen werden (Hilfe mit: `net help time`).

### 4.2 Installation der Wrapper-DLLs

Die Wrapper-DLLs für den Windows-Client - Teil des SNC Adapters - können auf zwei verschiedene Arten installiert werden.

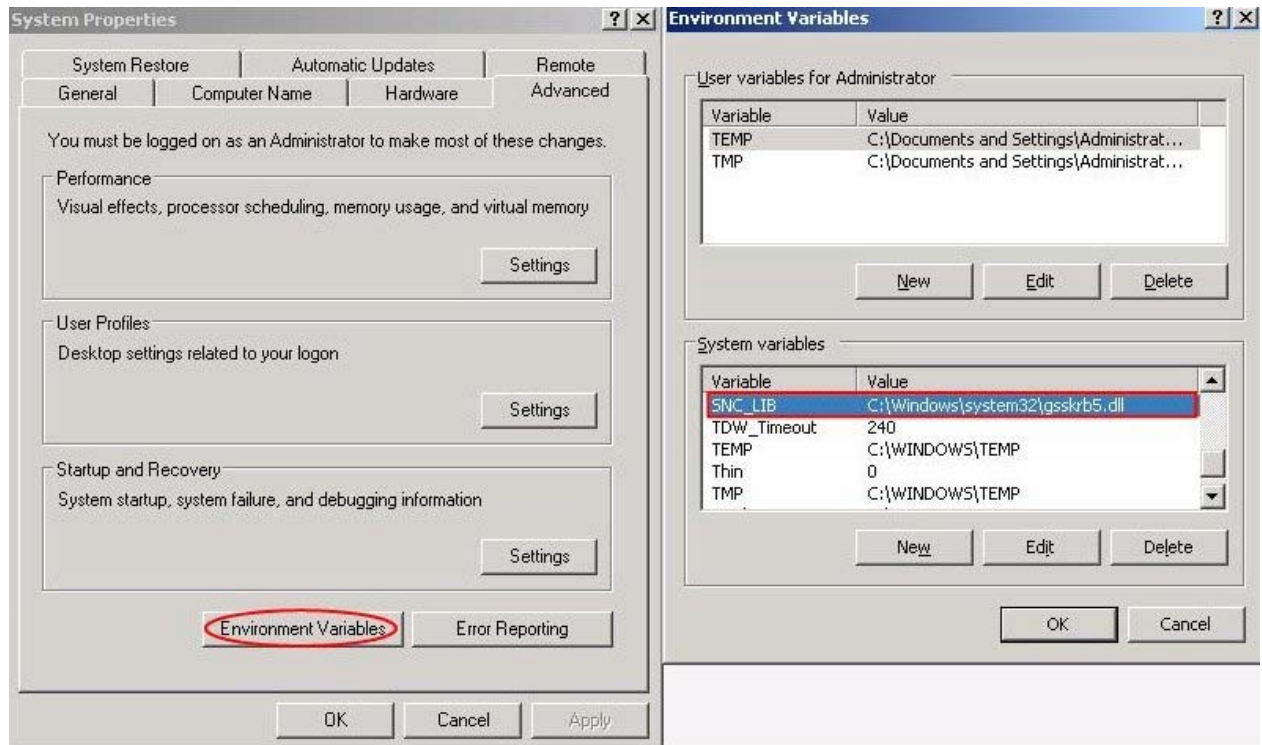
#### 4.2.1 Manuell

Um die DLLs manuell zu installieren, folgen Sie Hinweis [#352295](#).

Kopieren Sie die `gsskrb5.dll` in das Verzeichnis `%windir%\system32`.

Fügen Sie folgende System-Umgebungsvariable hinzu:

Variable `SNC_LIB` mit dem Wert `%windir%\system32\lgsskrb5.dll`.



#### 4.2.2 Automatisch

Um sich des Pakets `SAPSSO.MSI` zu bedienen (geeignet für die automatische Verteilung an viele Clients im Windows-Netzwerk) folgen Sie Hinweis [#595341](#).

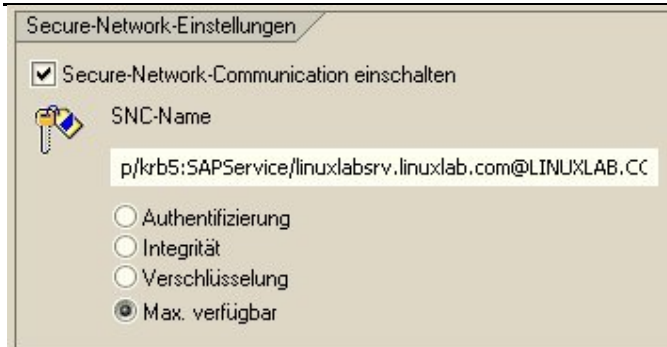
#### 4.3 SAP Logon anpassen

Das Logon-Verfahren muss angepasst werden. Erstellen Sie im Logon-Pad eine Verbindung zum entsprechenden SAP-System. Unter *Eintrag ändern* → *Weitere* aktivieren Sie die Secure-Network-Communication und fügen Sie die SNC-Identität hinzu. Hier:

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

z.B.:

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



## 5 USER-MAPPING

Damit Sie Single Sign-On benutzen können, muss ein Mapping im SAP-System zwischen dem SAP-User und dem Windows-User hergestellt werden. Dies geschieht in der Transaktion **SU01**:

Registerkarte SNC

SNC-Name: p:<WindowsUser>@<DOMAIN\_NAME>

## 6 ANHANG

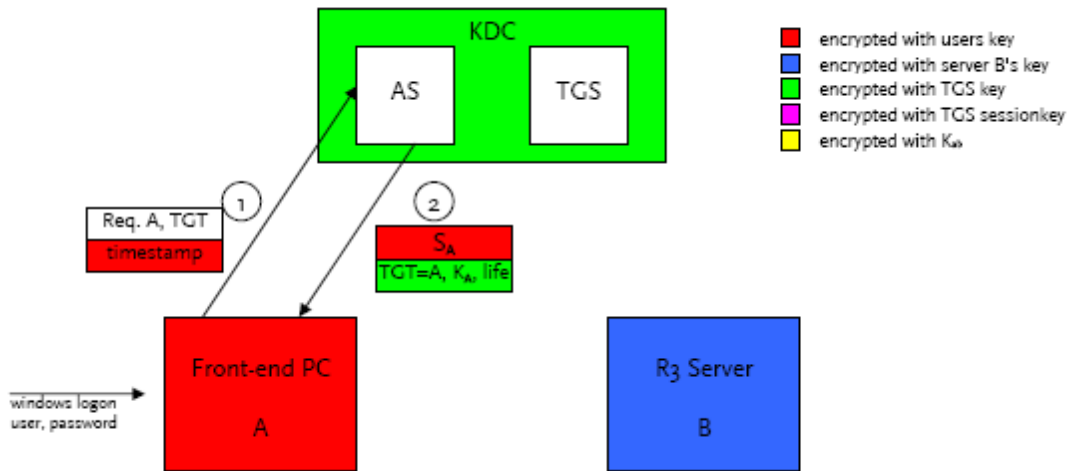
### 6.1 Funktionsweise Kerberos

Schritt 1:

Windowsanmeldung. Der Userschlüssel wird aus dem Passwort und der TGT (Ticket Granting Ticket) Anfrage gebildet, welche an den KDC (Key Distribution Center) gesendet wird. Um die Authentizität sicherzustellen, wird ein verschlüsselter Zeitstempel dem Schlüssel hinzugefügt.

Schritt 2

Der KDC überprüft die Anfrage, indem er den Zeitstempel mit dem in der Datenbank hinterlegten Schlüssel entschlüsselt. Anschließend generiert der KDC einen Sitzungsschlüssel SA für die Kommunikation zwischen User A und dem TGS (Ticket Granting Service). Dieser Sitzungsschlüssel wird zusätzlich mit dem Userschlüssel des Users A verschlüsselt. Im Anschluss wird das TGT ausgestellt und mit dem Schlüssel von User A und Gültigkeitsdauer verschlüsselt.

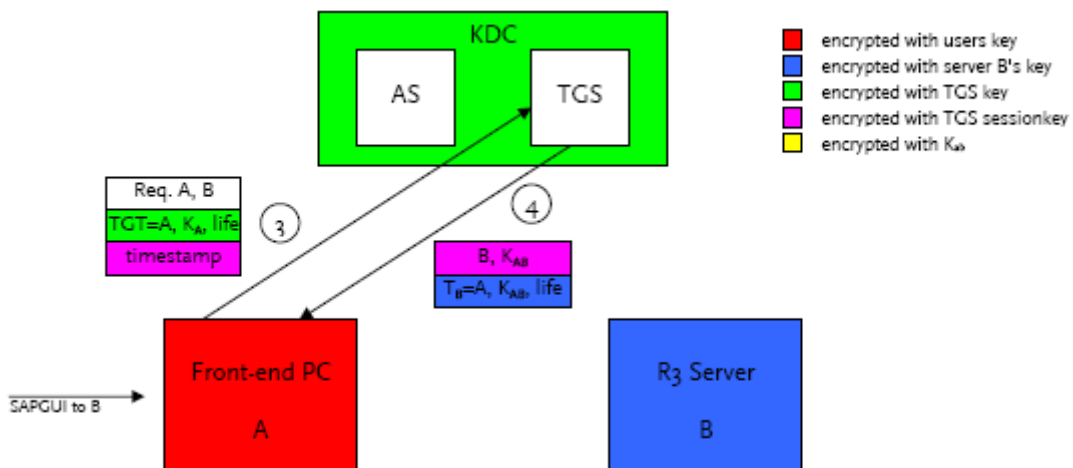


Schritt 3:

Der User versucht sich am SAP anzumelden. Er stellt eine Ticketanfrage an den TGS für die Kommunikation mit Server B. Diese Anfrage enthält das TGT und den Zeitstempel mit dem Sitzungsschlüssel.

Schritt 4:

Der TGS erstellt eine Sitzung  $K_{AB}$  für die Verbindung zwischen dem Front-End und dem SAP-Server. Der TGS sendet diesen mit seinem (durch den Sitzungsschlüssel verschlüsselten) Schlüssel zu dem User zurück. Anschließend erstellt es ein Ticket für Server B (SAP-System) und verschlüsselt es mit dem Schlüssel von Server B.

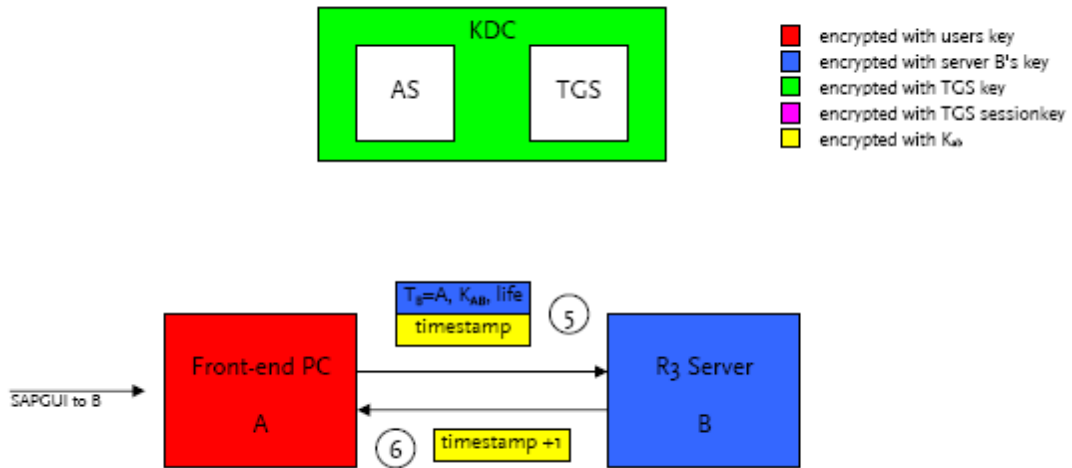


Schritt 5:

User A sendet das Ticket beim Anmeldeversuch zu Server B. Dieses Ticket ist mit einem Zeitstempel versehen, welcher mit dem Sitzungsschlüssel verschlüsselt wurde.

Schritt 6:

Server B überprüft den Zeitstempel und verifiziert die Verbindung, indem er den mit dem Sitzungsschlüssel verschlüsselten Zeitstempel+1 zurücksendet.



In diesem Moment haben sich beide Partner gegenseitig authentifiziert und eine sichere Kommunikation über das Netzwerk ist garantiert.



---

## 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
```